Performance Analysis of Artificial Noise-aided Physical Layer Security in Multi-antenna Wireless Networks

Genet Amde Chewiecha

A Thesis Submitted to the Department of Electronics and Communication Engineering

School of Electrical and Computing Engineering

Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

June 2023

Adama, Ethiopia

Performance Analysis of Artificial Noise-aided Physical Layer Security in Multi-antenna Wireless Networks

Genet Amde Chewiecha

Major Advisor: Dr. Demisse Jobir

Co-Advisor: Eshetu Tessema

A Thesis Submitted to the Department of Electronics and Communication Engineering

School of Electrical and Computing Engineering

Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

June 2023

Adama, Ethiopia

Declaration

I hereby declare that this Master Thesis entitled “Performance Analysis of Artificial Noise-aided Physical Layer Security in Multi-antenna Wireless Networks” is my original work. That is, it has not been submitted for the award of any academic degree, diploma, or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

Name of student	Signature	Date

Recommendation of Advisors

We, the major advisor and co-advisor of this thesis, hereby certify that we have read the revised version of the thesis entitled “Performance Analysis of Artificial Noise-aided Physical Layer Security in Multi-antenna Wireless Networks” prepared under our guidance by Genet Amde Chewiecha submitted in partial fulfillment of the requirements for the degree of Mater’s of Science in Communication Engineering. Therefore, we recommend the submission of revised version of the thesis to the department following the applicable procedures.

Major Advisor	Signature	Date
Co-advisor	Signature	Date

Approval Page of M.Sc Thesis

We, the major advisor and co-advisor of the thesis entitled “Performance Analysis of Artificial Noise-aided Physical Layer Security in Multi-antenna Wireless Networks” and developed by Genet Amde Chewiecha, hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

Major Advisor	Signature	Date
Co-advisor	Signature	Date

Approval of Board of Reviewers

We, the undersigned, members of the Board of Examiners of the thesis by Genet Amde Chewiecha have read and evaluated the thesis entitled “Performance Analysis of Artificial Noise-aided Physical Layer Security in Multi-antenna Wireless Networks” and examined the candidate during open defense. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of Master of Science in Communication Engineering.

Chairperson	Signature	Date
Internal Examiner	Signature	Date
External Examiner	Signature	Date

Finally, approval and acceptance of the thesis is contingent upon submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

Department Head	Signature	Date
School Dean	Signature	Date
Office of Postgraduate Studies, Dean	Signature	Date

ACKNOWLEDGEMENT

In the beginning, I am grateful for the assistance I received from God and his Mother Virgin Mary. The simulation and documentation for this thesis were completed during a challenging time that necessitated frequent requests for your assistance. I appreciate your support and everything you do to show me that you care.

Next, my appreciation and gratefulness go to the Ministry of Education (MoE) and Adama Science and Technology University in Ethiopia for funding and supporting this study. I also would like to give my sincere gratitude to my advisor, **Dr. Demisse Jobir (Ph.D.),** for his patient guidance, useful advice, and encouragement during my study. I have been tremendously lucky to be advised by him; accomplishing my research in time would have been substantially more challenging without his support and understanding. I also very much appreciate that he allowed me to decide upon the subject matter of the research for this thesis on my own. I would also like to give sincere thanks to my co-advisor, **Mr. Eshetu Tessema (MSc)**, for his valuable suggestions and continuous support.

I'd want to express my heart felt gratitude to my husband, **Mr. Abebe Hailu,** for being there for the entire journey of the study and for your patience while I am far apart from you and our child by being responsible for him like mother and father this is all your support, I would like to express you my big respect and love. Also am grateful for my child **Naol Abebe;** you make me do hard and better.

Also, I value and am most grateful for the support I have received from all my family members, **Ada**, **Abiye**, **Deje**, **Babi**, **Reho**, **Mimi,** and **Tewabu**; your inspiration and love have motivated me greatly in the pursuit of successful research outcomes and entire study.

I would like to show my gratitude to my friends **Ms. Misgana Zelalaem**, **Mrs. Sewinet Bora**, **Ms. Sosina Abiyot,** and **Mr. Yidnekachew Solomon** for the remarkable support and encouragement you have given me throughout my study.

Finally, I'd like to express my gratitude to my colleagues, Gender office staff, neighbors, and all of those I have had the pleasure to work with, for they have given me continuous encouragement towards completing this thesis.

Table of Contents

List of Tables iii
List of Figures iv
List of Acronyms vii
Abstract x
CHAPTER ONE 1
INTRODUCTION 1
1.1 Research Background 1
1.2 Statement of the problem 7
1.3 Objective 7
1.4 Significant of the study 7
1.5 Scope and limitation of the study 8
1.6 Thesis Contribution 8
1.7 Thesis Outline 8
CHAPTER TWO 10
LITERATURE REVIEW 10
2.1 Information-Theoretic Security 10
2.2 Multi-antenna Wireless Network 16
2.3 Beamforming 21
2.4 Artificial Noise 22
2.5 Modulation Schemes 23
2.6. Related Work 27
CHAPTER THREE 34
MATERIALS AND METHODS 34
3.1 Introduction 34
3.2 Materials 34
3.3 Methods 34
3.4 Mathematical Model of Modulation Schemes 36
3.5 Mathematical Model of Transmit Beamforming 36
3.6 Mathematical Model of Artificial Noise 38

CHAPTER FOUR 41
Result and Discussion 41
4.1 Introduction 41
4.2 Simulation Parameter 42
4.3 Transmit Beamforming Simulation Results 43
4.4 Artificial Noise Simulation Results 47
CONCLUSIONS AND RECOMMENDATIONS 52
Conclusions 52
Recommendations 53
Reference 54

List of Tables

Table 2.1 Related Works……33

Table 4.1 Simulation Parameters……...……42

Table 4.2 BER performance comparison for BPSK and QPSK modulation techniques for Bob and Eve channel with and without TX beamforming for two three and four antennas at SNR of 10dB……...46

Table 4.3 BER performance comparison for BPSK and QPSK for Eve's channel at 20%, 40%, 60%, and 80% Artificial Noise at SNR value of 20dB…….…….51

List of Figures

Figure 1.1 Security techniques for different layers……..……3

Figure 1.2 Eavesdropper scenario passive attack (Childress, n.d.)…….….4

Figure 1.3 Artificial noise effect in PLS active attack…….6

Figure 2.1 Binary Symmetric Channel Model(Cover & Thomas, 2005)…….……..10

Figure 2.2 Wyner Wiretap channel (special case) (Wyner, 1975)…….…11

Figure 2.3 Wyner Wiretap channel (general case) (Wyner, 1975)……....13

Figure 2.4 Wyner Achievable Wiretap Code Region (Wyner, 1975)……14

Figure 2.5 SISO Model……..20

Figure 2.6 SIMO Model…….20

Figure 2.7 MISO Model…….21

Figure 2.8 MIMO Model……...21

Figure 2.9 (a) Multi-antenna AN generation (b) amplifier relay AN generation (Negi & Goel, 2005)……..23

Figure 2.10 BPSK constellation diagram (Xiong, 2016)……...24

Figure 2.11 Block diagram of BPSK (Wu et al., 2018)…….25

Figure 2.12 Constellation diagram of QPSK (Xiong, 2016)……..25

Figure 2.13 Block diagram of QPSK (Wu et al., 2018)…….26

Figure 2.14 Constellation graph of 8-PSK bit arrangement in a Gray code (Xiong, 2016).....27

Figure 3.1 AN- aided passive attack PLS system model……...35

Figure 3.2 Transmit beamforming model……..37

Figure 4.1 Simulation result plot for Bob and Eve with and without TX beamforming in BPSK modulation technique with two transmit antenna transmitter side.…….…….43

Figure 4.2 Simulation result plot for Bob and Eve with and without TX beamforming in QPSK modulation technique with two transmit antenna transmitter side.……..…43

Figure 4.3 Simulation result plot for Bob and Eve with and without TX beamforming in BPSK modulation technique with three transmit antenna transmitter side..……....44

Figure 4.4 Simulation result plot for Bob and Eve with and without TX beamforming in BPSK modulation technique with three transmit antenna transmitter side.……....44

Figure 4.5 Simulation result plot for Bob and Eve with and without TX beamforming in BPSK modulation technique with four transmit antenna transmitter side.……....45

Figure 4.6 Simulation result plot for Bob and Eve with and without TX beamforming in BPSK modulation technique with four transmit antenna transmitter side...…….…...45

Figure 4.7 BER versus SNR Simulation plot for Bob and Eve in BPSK modulation and 20% AN of total transmit power ……...……47

Figure 4.8 BER versus SNR simulation plot for Bob and Eve in QPSK modulation and 20% AN of total transmit power……...…….47

Figure 4.9 BER versus SNR simulation plot for Bob and Eve in BPSK modulation and 40% AN of total transmit power……...…….48

Figure 4.10 BER versus SNR simulation plot for Bob and Eve in QPSK modulation and 40% AN of total transmit power.……...……...….48

Figure 4.11 BER versus SNR simulation plot for Bob and Eve in BPSK modulation and 60% AN of total transmit power……...…….49

Figure 4.12 BER versus SNR simulation plot for Bob and Eve in QPSK modulation and 60% AN of total transmit power……...…….49

Figure 4.13 BER versus SNR simulation plot for Bob and Eve in BPSK modulation and 80% AN of total transmit power……...…….50

Figure 4.14 BER versus SNR simulation Plot for Bob and Eve in QPSK modulation and 80% AN of total transmit power……...…….50

List of Acronyms

AM	Amplitude Modulation
8-PSK	8-Phase Shift Keying
AM	Analog Modulation
AM	Adaptive Modulation
AN	Artificial Noise
ASK	Amplitude Shift Keying
AWGN	Additive White Gaussian Noise
BCD	Block Coordinate Descent
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BS	Base Station
CCP	Convex-Concave Procedure
CQI	Channel Quality Indicator
CSI	Channel State Information
CSIT	Channel State Information at Transmitter
DDM	Dynamic Directional Modulation
EGC	Equal Gain Combining
EH	Energy Harvesting
EMF	Electromotive Force
Eve	Eavesdropper

FD	Full Duplex
FM	Frequency Modulation
FSK	Frequency Shift Keying
GSSK	Generalized Space Shift Keying
IoT	Internet of Things
IR	Information Receiver
IRS	Intelligent Reflection Surface
LED	Light Emitting Diode
LIS	Large Intelligent Surface
LM	Lagrangian Multiplier
LU	Legitimate User
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
MM	Majorization Minimization
MRC	Maximal Ratio Combining
NOMA	Non-Orthogonal Multiple Access
OOBE	Out of Band Emission
OSI	Open System Interconnect
PAPR	Peak-to-Average Power Ratio
PEAK	Phase-Enciphered Alamouti Coding
PL	Physical Layer

PLS	Physical Layer Security
PM	Phase Modulation
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
SC	Selection Combining
SCD	Spatial Constellation Design
SDR	Software Defined Radio
SIC	Successive Interference Cancellation
SIMO	Single Input Multiple Output
SISO	Single Input Single Output
SM	Spatial Multiplexing
SNR	Signal to Noise Ratio
SR	Secrecy Rate
SRM	Secrecy Rate Maximization
TDD	Time Division Duplex
TPC	Transmit Precoding
URLLC	Ultra-Reliable and Low Latency Communication
VLC	Visible Light Communication
ZFP	Zero Forcing Precoding

Abstract

Wireless communication is the most dynamic and rapidly expanding technology area in the communication industry. Data can be transmitted wirelessly from one location to another without the use of physical mediums like cables or wiring, or other connections. Because of the continued universal development of wireless communication networks, privacy and security concerns have anticipated a greater impact. The broadcast nature of wireless communication makes it vulnerable to security attacks such as data loss, hijacking, and eavesdropping. Conventionally, cryptography-based security solutions have been made where a secret key is generated and shared over the wireless channel. This technique suffers from the problem of key sharing and key management, making the future wireless network create a time delay in operation. The physical layer security (PLS) technique overcomes this problem which is based on Claude Elwood (C.E) Shannon's everlasting information-theoretic security. By using the basic principle of the inherent randomness of wireless channel and noise, then degrading the listening capability of the attacker, without the need for secret key generation security, is achieved. Different physical layer security techniques have been investigated by different researchers. In this thesis, artificial noise-aided (AN-aided) physical layer security technique over the multi-antenna system on Rayleigh fading and additive white Gaussian noise (AWGN) channel in passive eavesdropper scenario performance is analyzed. Transmit beamforming is used for the multi-antenna system, which is two transmit and single receive antenna for both the eavesdropper and the legitimate receiver. The system is analyzed by using binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK) modulation techniques, based on performance evaluation techniques bit error rate (BER) and signal-to-noise ratio (SNR), at 20dB SNR and 40% AN, better performance is achieved the legitimate user (Bob with AN) is not affected significantly, while the eavesdropper BER value with AN is increased 140 times at BPSK modulation, and on QPSK modulation only 38 times BER value is increased this making BPSK modulation better. Also, by increasing the number of transmit antennas from two to three and then to four and applying them to transmit beamforming for the two modulation technique and four transmit antennas, for bob without transmit beamforming and eavesdropper with and without transmit beamforming,793 times increased BER value for BPSK and 630 times BER value increase for QPSK. This makes BPSK better.

***Key words**: Eavesdropper, PLS, BER, SNR, QPSK, BPSK, AN, AWGN, Transmit Beamforming*

CHAPTER ONE

INTRODUCTION

1.1 Research Background

A common model for computer networking is the OSI model. It is a fictitious networking architecture that employs particular protocols and methods at each layer (*OSI Security Layers and Their Significance*, n.d.). By segmenting the entire communication process into a 7-layer model and using several protocols at each layer, this model provides the standards for communication between the devices (*OSI Security Architecture - Detailed Explanation - InterviewBit*, n.d.). The seven layers are the Physical layer, Datalink layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer. The OSI model continues to play a significant role in standardizing protocols (Simoneau, 2006).

The physical layer (PL) is the first and lowest layer of the OSI reference model. It is in charge of regulating the transmission and reception of raw, unstructured bit stream data through a physical channel. The data link layer, a raw and unreliable bit transmission service offered by the physical layer, is built upon by the data link layer, which offers reliable data transmission (frames) between nearby nodes. It prepares the information for transport and reconfiguration at the network layer. In simple terms, logical routing and route selection are the main responsibilities of this layer. This layer aids the receiving packets' navigating by providing them with logical addresses. In the transport layer, between processes running on various machines, end-to-end communication is made possible by it. Both parties can sustain an ongoing communication process over a network, thanks to the session layer. The programs on both sides of the session can exchange packets as long as it is active. Before heading to the application layer, the information is organized at the presentation layer. It could be viewed as the interpreter for the network. Users often interact alongside the application layer. It facilitates end-user and application processes (Simoneau, 2006).

The data travels from the sender's application layer to the layers below, where each layer adds a header to the data that may include details such as the sender's and receiver's addresses. The headers from all the preceding layers are appended to the data when it gets to the sender's physical layer. The data now flows to the receiver across a physical medium and reaches the

physical layer of the receiver. The data is then sent from the receiver to the upper layers, where each layer processes the header and removes it from the data so that the data is in its original form when it reaches the application layer of the receiver.

This realization leads to the understanding that information travels through the sender's application layer to its PL and through the sender's PL into the receiver's PL. As a result, an attacker could modify, steal, or simply read the data for a later purpose. This is unsafe because the data might also be used for illegal purposes, and in any large organization, the possibility of data theft or modification is a serious worry. The attack may be active or passive. During a passive attack, an intruder analyzes the information that has been communicated through the transmitter to the receiver during the communication. During this case, it's crucial to remember that a passive attack is one whereby the intruder does not alter or modify the information being accessed. No changes are made to the information in any manner. Conversely, in an active attack, the intruder's main objective is to alter communicated information between the sender and receiver. The most dangerous feature of this attack is that both the transmitter and receiver aren't typically aware that an attack has occurred (Engli, 2020).

For the transferred data to possess a successful transmission from the sender to the receiver, different security techniques have been studied by different researchers on the different OSI layers. (Alfardan, 2014; Deccio, 2004) , both papers studied security techniques on the Network layer. (Dilloway, 2008; van der Merwe, 2018) , both papers studied the transport layer protocol for secured communication between the sender and receiver. (Siddique et al., 2015), discussed some of the security problems found in the datalink layer and the respected solutions. (Krontiris, 2018; Report et al., 2016; Vadlamani, 2013) those papers studied different techniques used in the security of the application layer of the OSI model. (Alotaibi, 2016; Jennifer, n.d.) , both papers discussed physical layer security (PLS) techniques. Figure 1.1 below shows some security techniques of the OSI model.

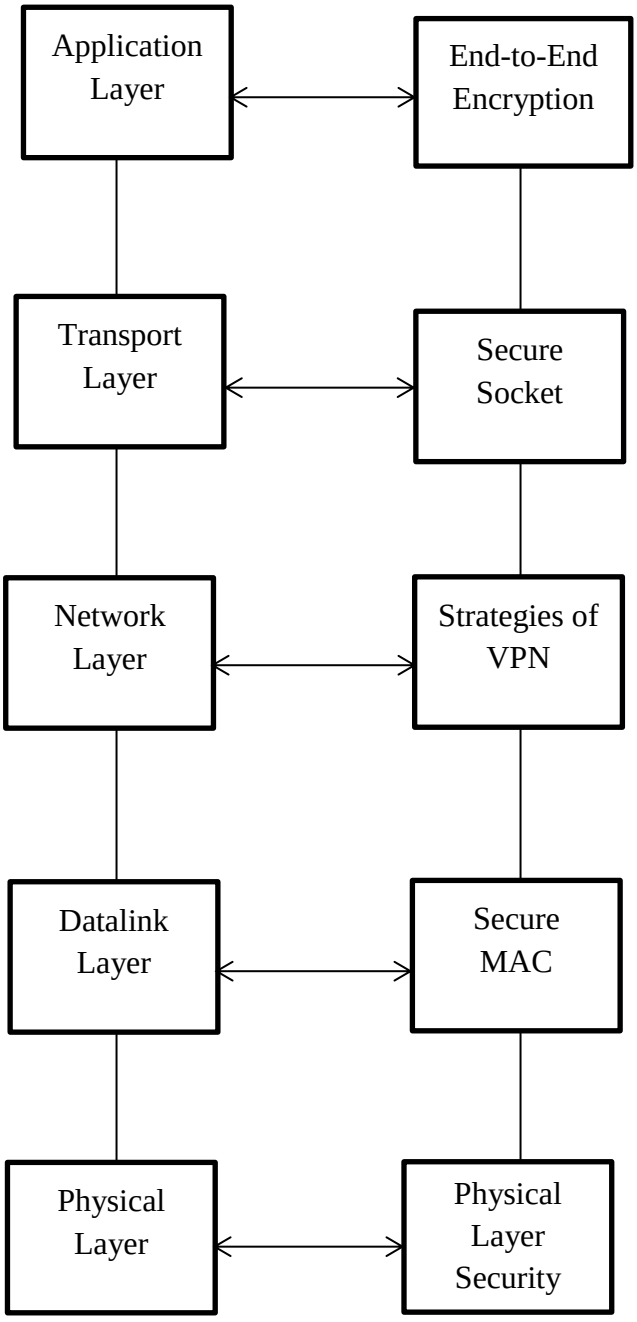

Figure 1.1 Security techniques for different layers

The OSI model's PL layer is the topmost and bottommost layer. The physical medium is supported by it, and it is connected to electronic or physical connectors for synchronized interaction, while the PL deals with bit-level transmission between various devices. The PL is in charge of transmitting data packets across the network across many devices. Its function is to describe the way physical links to the network are configured and how bits are represented

into predictable signals during transmission across electrical, optical, or radio waves; it does not understand the bits (R. Chen et al., 2019). To achieve this, the PL performs a variety of functions, such as defining bits and deciding how to transform bits from 0s and 1s to a signal. The data rate, measured in bits per second, dictates how quickly the data travels. The sending and receiving devices are synchronized. The kind of transmission—simplex, half-duplex, or full-duplex— regulates how information is carried and if it is simplex (one signal is sent out in one way), half-duplex, or full-duplex (data is simultaneously transmitted in both directions). The interface controls how devices are coupled to a communication medium, such as Ethernet or radio waves. The higher levels interact with the external world using the PL. Particularly for newer technologies like the internet of things, machine-to-machine communication, vehicular communication, and so forth, this layer's security is of utmost importance.

PLS is a technique for achieving perfect security that was created from information theory and examines the fundamental properties of the channel. Given the broadcast nature of wireless systems and the quick technological developments available to possible eavesdroppers, as seen in figure 1.2 Eavesdropper Scenario, it is becoming more difficult to deliver secure communications using wireless networks.

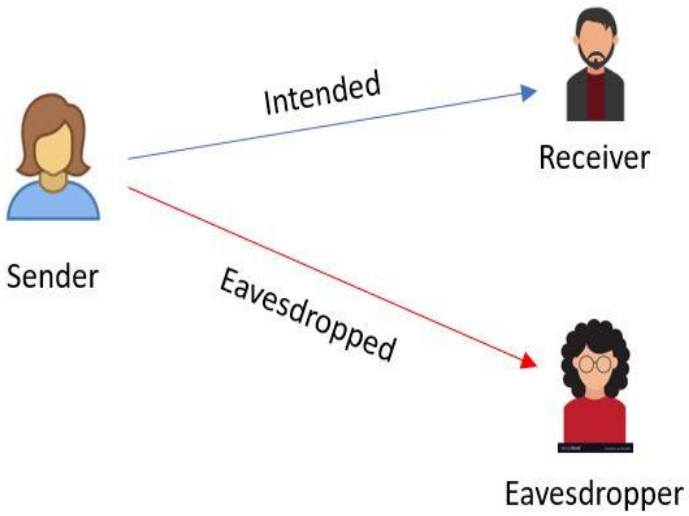

Figure 1.2 Eavesdropper Scenario passive attack(Childress, n.d.)

Security methods are primarily separated into two categories: computational security and information-theoretic security (Umebayashi et al., 2014). Computational-based security assesses security based on how long it takes to crack a code (Bloch et al., 2008; Massey, 1986). The second strategy, on the other hand, uses the physical properties of the wireless channel and is based on Shannon's early research on the mathematical theory of communication. Additionally, there are two subcategories within information theoretic security: Key-based (Csiszár, 1993; Shannon, C.E., 1949) and keyless, according to Wyner's wiretap channel (Wyner, 1975). Key-based security establishes secure keys among genuine users through the use of wireless channels' unpredictability (Mukherjee et al., 2014). In contrast, keyless security solutions need complete or incomplete CSI of the usually unreachable eavesdropper's channel (Bloch & Barros, 2011). PLS, which is based on information-theoretic security, has gained a lot of interest as a result. Utilizing the physical channel's inherent unpredictability to enable secure communication is the main concept of PLS.

The following standout qualities and benefits of PLS technology over conventional encryption technologies are noteworthy. First, PLS comprises keyless techniques (i.e., no encryption or decryption operations are necessary) in addition to secure key generation techniques. Second, PLS methods can benefit from the erratic and time-varying characteristics of wireless channels. The PLS technology may successfully prevent unauthorized parties from reading the contents of private communications transmitted by the transmitter, as well as through observing how the signal is transmitted or discovering the user's location (X. Chen et al., 2017; Hu et al., 2018). In particular, the key generation-based PLS solution primarily relies on the unpredictability and openness of the wireless channel to produce channel keys so authorized users can constantly have the appropriate keys while keeping an eye on the transceiver link (Chou et al., 2013). The research on keyless PLS approaches is based on the Wyners Wire-tap wireless communication eavesdropping channel model. It shows that there's an approach to maximize the speed of communication from the transmitter to the genuine receiver, not giving any information to Eve when Eve's channel is the degraded channel of the genuine receiver. Broadcast Gaussian channels have been added to this eavesdropping channel model (Csiszár & Körner, 1978; Leung-Yan-Cheong & Hellman, 1978). Signal processing methods are specifically utilized to create appropriate beamforming or power distribution methods from the

transmitter's side to improve the confidentiality of wireless communication networks (Wang et al., 2019). Due to the aforementioned benefits, tackling the communication security issue from the PL has caused considerable concern among researchers.

Different PLS techniques have been studied by different researchers; some of them are Security key generation and distribution, Physical Layer Authentication, Antenna Selection (MIMO), Beamforming/Pre-coding, AN addition, IRS, Modulation for Secrecy, and Coding-polar code. From all mentioned above and other techniques, artificial noise(AN)-aided PLS technique is the best and attracted researchers by its better performance and increased efficiency of security.

AN aided PLS is a physical Layer Security approach based on orthogonal blinding. Blinding is the process of purposefully hiding the signal of the intended user by bombarding any possible listeners with useless transmissions. An interfering AN signal is added to the transmission medium utilizing the null space of the authorized receiver's channel in orthogonal blinding-based secure communication. The interfering sign ensures that there is little to no negative impact on the reception at the legitimate receiver while degrading the attacker's performance (because the attacker perceives a superposition of noise and signal).

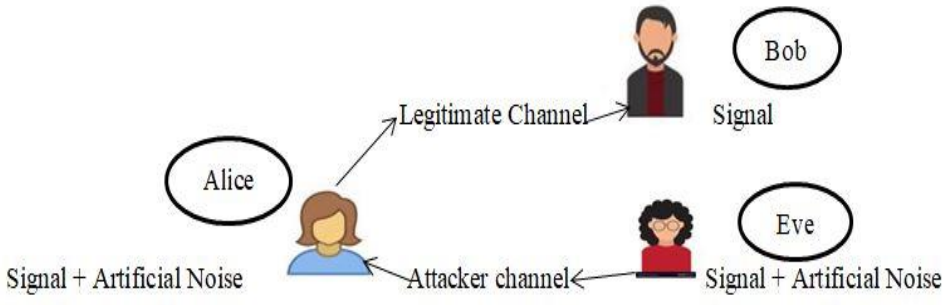

Figure 1.3 Artificial noise effect in PLS active attack

In this thesis, AN-aided PLS technique has been studied in multiple wireless channel, transmit beamforming (TX BF), AWGN, and Rayleigh fading channel, considering passive Eavesdropper and three different modulation schemes, BPSK and QPSK. Where the performance of each modulation scheme in the presence and absence of AN is discussed, and the result is presented.

1.2 Statement of the problem

The interception of communications is typically restricted to unauthorized users who are situated in the same narrow beam as the authorized user since the transmitted signals are highly directed, and the propagation environment is severe. An unauthorized receiver may decrypt signals in line of sight (LoS) broadcasts even while using extremely narrow beams. As a result of its broadcasting nature and line-of-sight channel features, physical layer security is difficult to establish. Wireless channels are broadcast, making it easy for any unintentional user to pick up the signal and eavesdrop on an unencrypted or inadequately secured wireless communication link. Due to the nature of wireless communication, security risks such as information corruption, hijacking, and eavesdropping arise. Conventionally, cryptography-based security solutions have been made where a secret key is generated and shared over the wireless channel. This technique suffers from the problem of key sharing and key management, making the future wireless network create a time delay in operation. Therefore, a PLS technique that performs with the keyless technique plus the key-based one, guided by AN is proposed to raise the level of security in a wireless network.

1.3 Objective

1.3.1 General Objective

The general objective of this thesis is to analyze the performance of artificial noise-aided physical layer security in a Multi-antenna wireless network.

1.3.2 Specific Objective

- To analyze the performance of AN-aided PLS with two different modulation techniques, BPSK and QPSK.
- To evaluate the effectiveness of AN in improving the performance of PLS.
- To compare the security performance of the proposed algorithm considering the criteria BER, SNR.

1.4 Significant of the study

The shortcoming of upper layer secrecy makes room for physical layer security, which benefits from mathematical security level measurement that can determine how confidential

data is transmitted and significantly impacts key management and distribution of cryptography. This study will develop a solution using AN-aided PLS using multi-antenna in a wireless system and evaluate the performance.

1.5 Scope and limitation of the study

Scope

This thesis work has a scope of:

- Analyzing the performance of the proposed work on additive white Gaussian noise (AWGN), Rayleigh fading channel, considering two modulation techniques, binary phase shift keying (BPSK) and quadrature phase shift keying (QPSk), passive eavesdropper scenario with the application of transmit beamforming for the legitimate receiver Bob.

Limitations

This thesis work:

- It is limited to simulation-based investigation, which relies on theoretical analysis.

1.6 Thesis Contribution

- We are analyzing the performance of AN-aided PLS with two different modulation techniques BPSK and QPSK.
- Analyzing the BER performance of transmit beamforming with two, three, and four transmitter antennas with BPSK and QPSK modulation technique for Bob and Eve channel.

1.7 Thesis Outline

The outline is summarized as follows:

- Chapter two discusses various definitions and conceptions of basic information theory concept, MIMO, AN, Transmit beamforming, and Modulation techniques, which several researchers have provided.

- Chapter three analyses the research techniques employed in this thesis, involving the mathematical model.
- Chapter four is devoted to talking about the suggested discussions and results.
- Chapter five outlines the conclusions and suggestions.

CHAPTER TWO

LITERATURE REVIEW

2.1 Information-Theoretic Security

Information theory is the foundation for how a receiver recognizes a signal and correctly decodes it, and it is the basic building block for PLS. Numerous information theory concepts make use of random variables and various outcome probabilities. Digital communication systems include identifying whether a 0 or a 1 has been transmitted through a channel, similar to a coin toss that has potential results becoming heads or tails. Figure 2.1, Information-Theoretic Secrecy, illustrates the Binary Symmetric Channel, a conventional framework for representing the likelihood of events connected to a communication system.

The BSC's result is a random variable that can be either 0 or 1. The representation of data transmission across a channel with the possibility of errors is made simpler by this paradigm. F is a representation of the likelihood of estimating the initial value incorrectly. The impact that a real physical communication channel exerts on the information transmitted across it is connected to the error probability F.

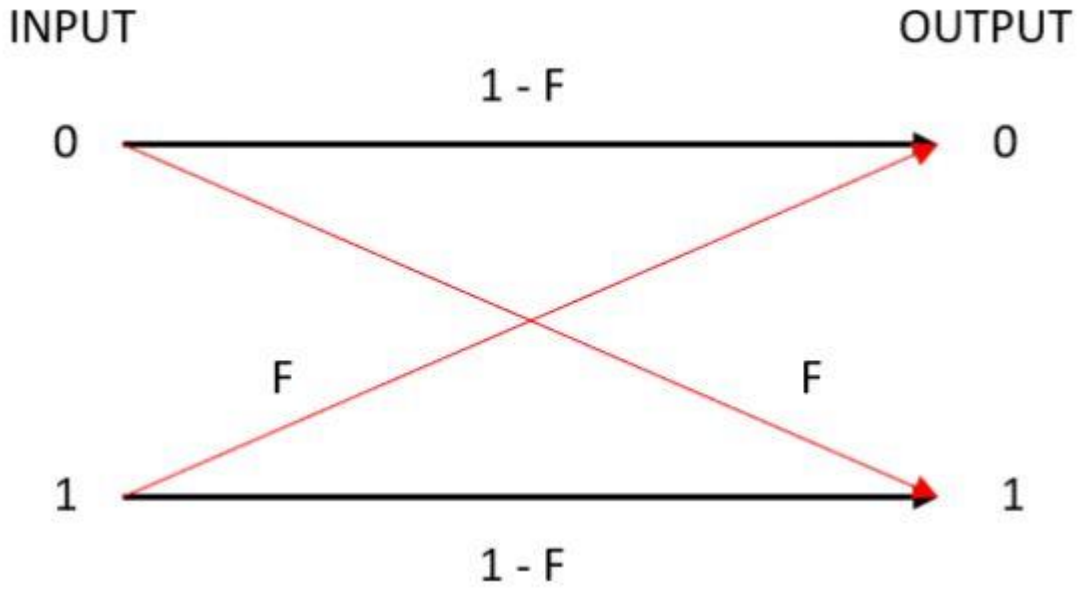

Figure 2.1 Binary Symmetric Channel Model(Cover & Thomas, 2005)

2.1.1 Wyner's Wiretap Channel

The wiretap channel model, which Wyner developed in 1975, is the fundamental idea of PLS(Wyner, 1975). By "tapping" the primary communication channel among the users using a "wiretap" channel, the wiretapper (also known as the eavesdropper) seeks to obtain the data being transmitted among authorized users within this paradigm. A quantifiable number of data can be successfully transferred between the transmitter and the legitimate receiver throughout times when the legitimate receiver's channel is "more reliable" compared to that used by the eavesdropper. According to this theory, confidentiality is only maintained by taking advantage of the random characteristics of the wiretap channel used by the eavesdropper. Wyner described the particular case and the general case of the wiretap channel (Wyner, 1975).

In the unique scenario depicted in figure 2.2, the transmitter and the legitimate recipient converse through a noiseless channel. Via a memoryless BSC, the eavesdropper likewise receives the same message. Blocks of K bits are supplied to the encoder from the input depicted as, $S^k = (S_1, \dots, S_k)$ which encodes S^kinto a binary N vector $X^N = (X_1, \dots, X_N)$ with length N. Error likelihood, transmission speed, and uncertainty rate are significant factors in Wyner's wiretap channel.

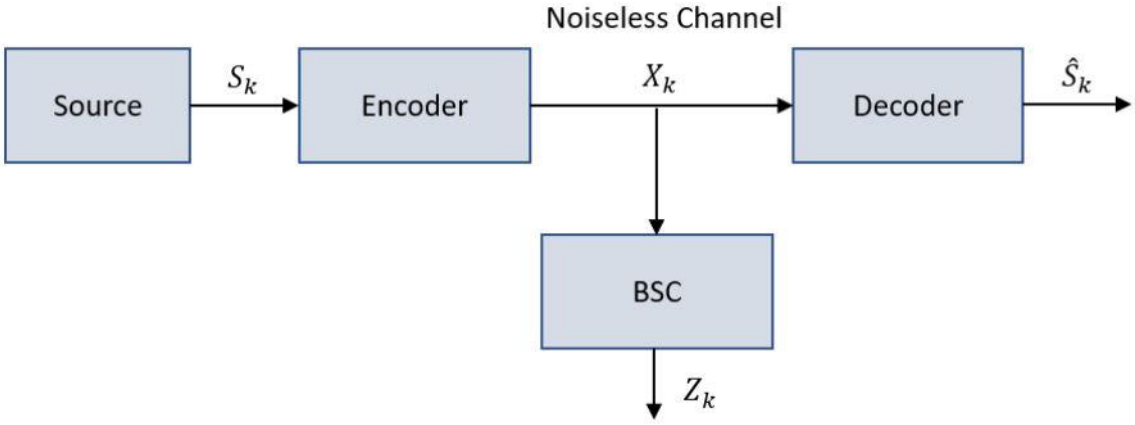

Figure 2.2 Wyner Wiretap channel (special case) (Wyner, 1975)

The error probability is:

$$p_e = \frac{1}{k} p_r \sum_{k=1}^{k} p_r \{s_k \neq \hat{s}_k\}. \quad (2.1)$$

With the BSC (also known as the wiretap channel), the listener can view the encrypted string X^N. The chance of a bit of flipping is $p_o \left(0 < p_o \leq \frac{1}{2}\right)$. The order of the data from the wiretap channel

$$Z^N = (Z_1, \ldots, Z_N). \tag{2.2}$$

The transmission rate of the channel is written as:

$$R = \frac{K}{N} \tag{2.3}$$

expressed in source bits per transferred symbol. The ambiguity rate, which measures the eavesdropper's level of bewilderment, is defined as

$$\Delta = \frac{1}{K} H(S^K | Z^N) \tag{2.4}$$

The goal is for the channel to deliver an excellent transmission rate, a small error probability, and a high confusion rate.

Both the primary and wiretap channels are discrete and memoryless in the general case of Wyner's wiretap channel, where the source's entropy is H_s. The probability of their corresponding transitions are Q_M as well as Q_W, correspondingly. While the data transfer rate is different from that of the exceptional case, the error probability and confusion rate do. The entropy of the source H_s is now factored into the data transfer rate for Wyner's wiretap channel in the general case. So,

$$R = \frac{kH_s}{N} \tag{2.5}$$

in source bits per transmitted symbol is the definition of the rate of transmission for the general case. Figure 2.3 shows how the source transmits a binary message S^k to an encoder, which creates a codeword X^N with N bits. Before being read as Y^N at the appropriate receiver, the codeword travels via the main channel, wherein it is subject to noise and various kinds of error. Yet, the wiretap channel allows the eavesdropper to obtain an even larger deteriorated portion of Y^N, which results in Z^N being provided to the eavesdropper. It is crucial to keep in mind the fact that the wiretap channel disregards any presumptions regarding the

eavesdropper's processing power and that no real encryption keys are being sent between the transmitter and the legitimate recipient. The wireless channels' internal properties serve as the only basis for the wiretap channel model.

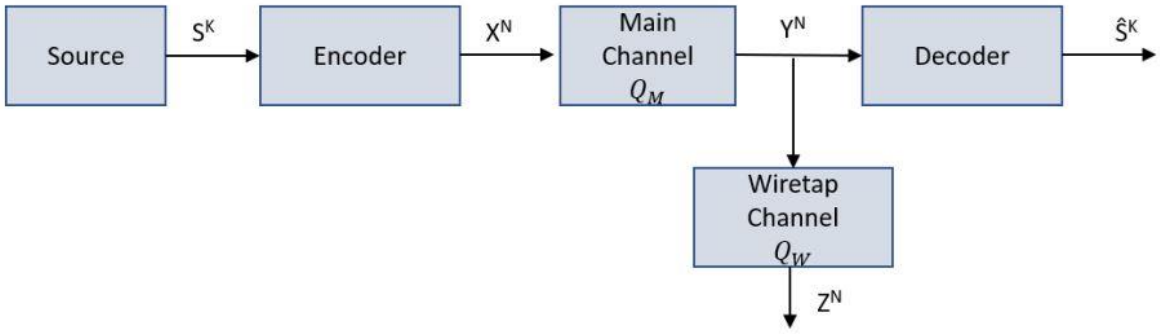

Figure 2.3 Wyner Wiretap channel (general case) (Wyner, 1975)

2.1.2 Wyner's Equivocation-Rate Region

Wyner proposes a secret capacity area $\bar{R}$ in (Wyner, 1975) for a pair of communication and confusion rates (R, d). This region is shown in figure 2.4. The rate R denotes the speed at which Alice and Bob can reliably communicate, whereas the ambiguity d denotes the degree of perplexity Eve feels as a result of her perceptions of the message being exchanged (Yener & Ulukus, 2015). The area has the following definition:

$$\bar{R} \triangleq \{(R,d): 0 \leq R \leq C_M\ ,\ 0 \leq d \leq H_s\ ,\ Rd \leq H_s\ \Gamma(R)\} \qquad (2.6)$$

In Wyner's wiretap channel method, the data transfer rate reaches the main channel QM's channel's capacity at the spots on $\bar{R}$ where

$$R = C_M. \qquad (2.7)$$

Indicate the points in Wyner's wiretap channel model where the data transfer rate reaches the channel capacity for the primary channel Q_M. The eavesdropper's confusion reaches H_s, which corresponds to full concealment (Wyner, 1975) for places across the line

$$d = H_s. \qquad (2.8)$$

In Wyner's wiretap channel model, the primary channel and the wiretap channel are represented by the points on the line C_s, which stands for the security capacity of the channel pair (Q_M, Q_W) Wyner reminds out that at this rate, a wiretap confusion near

$$H_s\,\Gamma C_M/C_M \tag{2.9}$$

is possible. Keep in mind that a lower rate of transmission is necessary for an increase in confusion (Wyner, 1975). The location on $\bar{R}$ where the confusion rate

$$R_e = \lim_{n\to\infty}\frac{1}{n}H(W|Z^n)\ \ , \tag{2.10}$$

where W is the information sent from Alice to Bob and Zn comprises Eve's observations, equivocates with a trustworthy transmission rate

$$R = \lim_{n\to\infty}\frac{1}{n}H(W) \tag{2.11}$$

This rate is the maximum at which Eve receives a data without learning anything. Wyner demonstrates the possibility of a maximum difference in mutual information, denoted by

$$\Gamma(R) = SUP_{p_{x\epsilon p(R)}}I(X;\tfrac{Y}{Z}) \tag{2.12}$$

provided the given input probability distribution is optimized. The greatest rate of transmission at which full secrecy is attained is at the point (C_s) (Ryland et al., 2017).

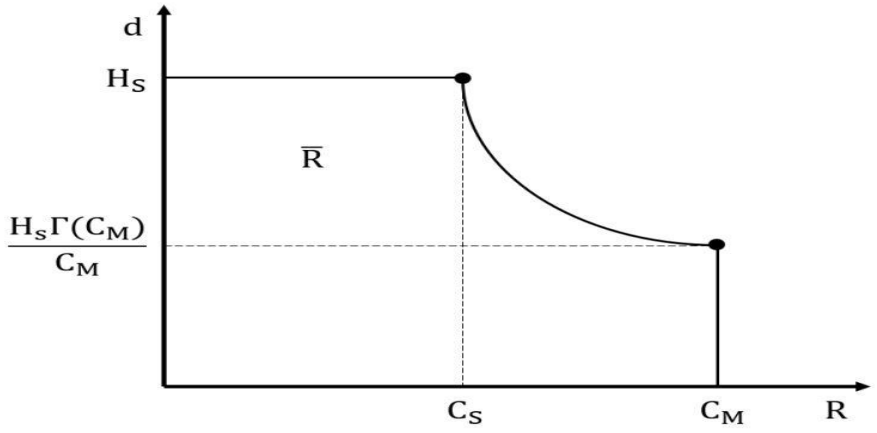

Figure 2.4 Wyner achievable Wiretap code region (Wyner, 1975)

2.1.3 Information Measurements

A discrete random variable with a probability distribution is called X's average data measurement. The entropy of X, is defined as

$$H(X) = -\sum p(X) \log p(X). \tag{2.13}$$

It is also known as the level of ambiguity regarding X (Bloch & Barros, 2011). Entropy is a basic idea in both PLS and information theory (Cover & Thomas, 2005).

The joint entropy of two discrete random variables X and Y with a joint probability distribution p_{XY} is:

$$H(X,Y) = -\sum\sum p(X,Y) \log p(X,Y) \tag{2.14}$$

and reflects the level of ambiguity surrounding X and Y. The measure of X's level of uncertainty given Y is known as conditional entropy, and its formula is

$$H(X/Y) = -\sum\sum p(X/Y) \log p(X/Y). \tag{2.15}$$

The ideas of entropy and conditional entropy have now been discussed, allowing the idea of reciprocal information to be discussed. A measurement of the knowledge that one random variable imparts about another random variable is known as shared data.

The quantity of information provided about a random variable X would result in several data regarding X given Y, for instance, if Y is a series of observations performed. The formula for this is

$$I(X;Y) = H(X) - H(X/Y). \tag{2.16}$$

The following definition of

$$I(Y;X) = H(Y) - H(Y/X) \tag{2.17}$$

also exists because of symmetric. It's also important to remember that

$$I(X;Y) = I(Y;X). \tag{2.18}$$

Based on mutual information as a foundation, its relationship to secrecy may be considered. The maximization of the mutual information gap between the mutual information among Alice and Bob and the mutual information between Alice and Eve determines the secret capacity (Yener & Ulukus, 2015) of the generic wiretap channel as

$$C_s = max_{p(u,x)} I(X;Y) - I(X;Z) \tag{2.19}$$

A DMC (Cover & Thomas, 2005)capacity can also be expressed as

$$C = max_{p(x)} I(X;Y) \tag{2.20}$$

The information supplied per symbol must go to zero, given the weakened confidentiality restriction (Subramanian et al., 2010). Poor secrecy is defined as:

$$\lim_{n\to\infty} \frac{1}{n} I(X;Y)=0 \tag{2.21}$$

corresponds to an encoded bit stream of length n delivered by Alice, and Z^n denotes the information viewed by Eve.

However, the powerful secrecy limitations, which is expressed as

$$\lim_{n\to\infty} \frac{1}{n} I(X^n;Z^n)=0 \tag{2.22}$$

demands that all information sent to an observer goes to zero (Subramanian et al., 2010).

2.2 Multi-antenna Wireless Network

2.2.1 Basics of Antenna

A metallic item termed an antenna serves as an avenue for electromagnetic energy transmission and reception. It serves as a bridge between the transmitting devices and the open space. Electromagnetic waves are created by the movement of electrons in the antenna. The transmitter that is used to produce current as an expression of time is connected to the antenna. An EMF created by this current pushes free charge in the antenna's conducting element to move around through the transmitting antenna. In the metallic element of the receiving antenna, there is a spontaneous charge. The movement of charge in the transmitting antenna

has an impact on them. The motion of charge in the antenna that receives signals is far less than the amount of charge and mobility in the transmitting antenna since there is typically an extensive distance between them. The receivers then enhance this weak, slightly distorted signal (Anon, 1983).

Various factors have been considered to comprehend the fundamental antenna principle. Radiation pattern, radiation power density, radiation intensity, antenna efficiency, bandwidth, directivity, directional patterns, beam efficiency, polarization, input impedance, antenna temperature, and antenna gain are some of the fundamental antenna properties (Balanis, 1997).

James Clerk Maxwell is credited with uniting the theories of electricity and magnetism and elegantly illustrating how they relate through a series of complex calculations that have come to be known as Maxwell's Equations. His initial publication of his writings appeared in 1873. Additionally, he demonstrated that light is electromagnetic and that both electromagnetic and light waves move at an identical pace due to wave disruptions (JC, 1954).

A desire for improved services, enhanced security, and faster data rates is generated as technology develops. In the past, physical connections were mostly used for high-speed data needs, while wireless networks were mainly employed for voice. Antenna constructions must also be modified to satisfy the varying demands of different wireless systems. Combining numerous antenna components with data processing capabilities is one option. The creation of "intelligent antennas" follows. Their traits and roles can change depending on the particular system requirements. They may significantly enhance the antenna's capacity, quality, and level of service. The antenna in wireless systems nowadays has to work as a directed device to enhance or increase the energy sent or received in certain paths while inhibiting it in others (Balanis, 1997). This leads us to the concept of MIMO.

2.2.2 MIMO

2.2.2.1 MIMO Basics

MIMO communication uses many antennas to convey identical information as multiple signals concurrently while only using one broadcast channel. This type of antenna selection employs numerous antennas to enhance the intensity and quality of the movement. At the moment of

transmission point, the data is divided into several data streams, which a second MIMO then recombines on the receiving side. The signal receiver is built to account for any additional noise or interference, lost signals, and even the little lag in timing between each signal's receipt (Wrulich, 2008).

The MIMO radios add resilience to transmitting information that traditional single antenna systems can't broadcast identical information across several streams. Due to this, MIMO devices have several benefits over conventional mono antenna configurations. As MIMO radios receive and combine numerous streams of the same data that are received at somewhat different times apart, MIMO radios can use multipath propagation to improve signal strength even without a clear line-of-site. This is especially useful in urban environments. Overall throughput can be increased, allowing for more video or other data to be sent over the network in higher quality and quantity. Using multiple data streams can reduce problems like fading caused by lost or dropped data packets, improving the quality of the video or audio (Krumbein, 2016).

MIMO systems can significantly outperform conventional single antenna structures in terms of efficiency. These enhancements are due to several advances, including interference reduction and array, diversity, and spatial multiplexing (ROHIT U. NABAR, 2015).

For the needed antenna gain and radiation pattern, single-element antennas are not always adequate. An array of single-element antennas offers a far superior option. An antenna array is created when several operational antennas are connected to a single source to produce a directed radiation pattern. The components of an array antenna are each of the antennas. The vector addition of all of the electromagnetic fields emitted from each of the antennas or elements yields the distribution of radiation from the array in a linear medium. The principle of superposition is another name for this procedure. The dimensions of antenna arrays might be one, two, or three (Alejandro, 2017). It brings up the notion of array gain.

2.2.2.2 Array Gain

Array gain can be used to improve the mean obtained SNR. For providing a harmonic mixing impact, adaptive synthesis using numerous antennas is used in array gain. The transmitter and/or receiver may carry out the analysis. Gain from an array requires an understanding of the

channel state information at the transmitter or receiver. The overall antennas used at the transmitter and receiver are an additional variable. As attaining CSIT necessitates a larger degree of network difficulty, it is more practicable to have CSI at the receiver than the transmitter.

2.2.2.3 Interference Resistance

MIMO can also increase resistance to interference. Multi-antenna receivers will more effectively screen off undesirable information caused by subscribers of common or repeated channels by analyzing the received signals through every receiving antenna (Jankiraman, 2016). The receiver nonetheless needs a certain degree of channel awareness about what signals it intends to keep while reducing the remainder to provide meaningful choice.

2.2.2.4 Spatial Multiplexing

Since several antennas can be employed to transmit distinct bits over every antenna, utilizing concurrent transmission lines and various channels, a multi-antenna technology may also improve its data throughput in comparison with that of a single antenna system. The process is known as spatial multiplexing (Gesbert & Akhtar, 2002). Under this instance, numerous sequences of information are received by the receiver, and they subsequently merge to optimize spectral effectiveness. For instance, the throughput of a MIMO system having three transmit antennas and three receive antennas is going to be triple times better than that of a conventional single antenna system.

Basically, in most literature, multiple input multiple output (MIMO) systems are classified into four general groups. Single input single output (SISO), single input multiple output (SIMO), multiple input single output (MISO), MIMO.

A. SISO

The SISO model, which is depicted in Figure 2.5, represents a very fundamental antenna arrangement. One transmit antenna, and one receive antenna are present in a SISO system. Because SISO is restricted by one transmission route, therefore can’t deliver array gain or diversity gain.

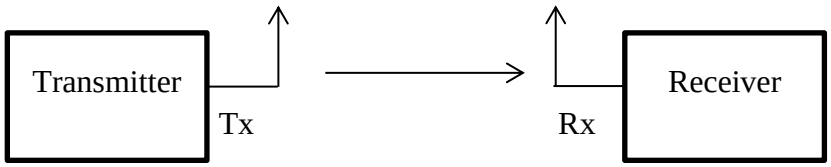

Figure 2.5 SISO Model

B. SIMO

SIMO, which is depicted in Figure 2.6, refers to an architecture where a single antenna broadcasts and many antennas receive. In this case, just one message is sent, and more than one signal is received. The SIMO antenna technology employs receive diversity. Receiving a message with receive diversity implies the antenna can choose the most powerful signal or combine all of the signals received by several antennas. The received signals can be combined using a few different methods. The following are the top three of them: equal gain combining (EGC) here, multiple antenna beams are mixed and combined, selection combining (SC) which is the easiest method and merely changes among all of them based on the quality of its signals; and maximal ratio combining (MRC) here, incoming signals are merged, to maximize the whole signal's SNR.

Figure 2.6 SIMO Model

C. MISO

Just one antenna is employed in the receiver when using the MISO antenna approach, whereas many antennas are employed on the transmitter. That is a fairly new piece of technology. Transmit beamforming is a popular method applied within a MISO system that enables the transmitter to concentrate the strength of the data signal in the path of the intended receiver or receivers. Figure 2.7 below shows the MISO model.

Figure 2.7 MISO Model

D. MIMO

Several antennas are used by MIMO on each transmitter and receiver. The two may simultaneously combine SIMO and MISO techniques. Additionally, they can boost throughput by employing SM. Compared to SISO approaches, the MIMO method offers several certain benefits. Spatial diversity significantly reduces fading, and in contrast with alternative MIMO systems, minimal power is needed (Persson et al., 2012). Figure 2.8 below shows the MISO model.

Figure 2.8 MIMO Model

Different researchers have enjoyed and researched further due to the advancement of antenna technology which is MIMO.

2.3 Beamforming

Beamforming approaches offer an effective method for transmitting messages that yield improved spectrum utilization in multiuser networks of communication. The BS has numerous antennas, allowing beam vectors to physically structure the electromagnetic waves for various applications (Gershman et al., 2010). There are different beamforming techniques used for

different multi-antenna techniques. As mentioned earlier, MRC can be used for the case of SIMO multi-antenna systems, whereas transmit beamforming is used for MISO systems, and in the MIMO system, both transmit and receive beamforming can be utilized. When we deal with the case of MISO, we can see the transmit beamforming.

Transmit Beamforming

Currently, transmit beamforming has received higher interest from researchers. Transmit BF, which makes use of either little or complete awareness regarding CSI on the sender side, can significantly improve wireless communication's energy utilization and security (Mudumbai et al., 2009; Narula et al., 1998).

2.4 Artificial Noise

It is a PLS approach based on orthogonal blinding. Blinding is the process of purposefully hiding the signal of the intended user by bombarding any possible listeners with useless transmissions. An intruding AN signal is introduced into a broadcast utilizing the null space of the authorized receiver's channel in orthogonal blinding-based encrypted communication. The intervening indication ensures that it has little to no negative impact on what is received at the authorized receiver yet degrades the intruder's effectiveness because the intruder perceives a combination of noise and signal (Hong et al., 2020).

AN can be generated using different techniques, as discussed by different researchers. (Negi & Goel, 2005) this paper studies two different techniques for the generation of AN. The first one is using the multiple antenna techniques at the transmitter side, and the second case scenario is where even if we didn’t use multiple antennas, AN generation could be achieved by using many amplifying relays. Figure 2.10 below shows these two different cases.

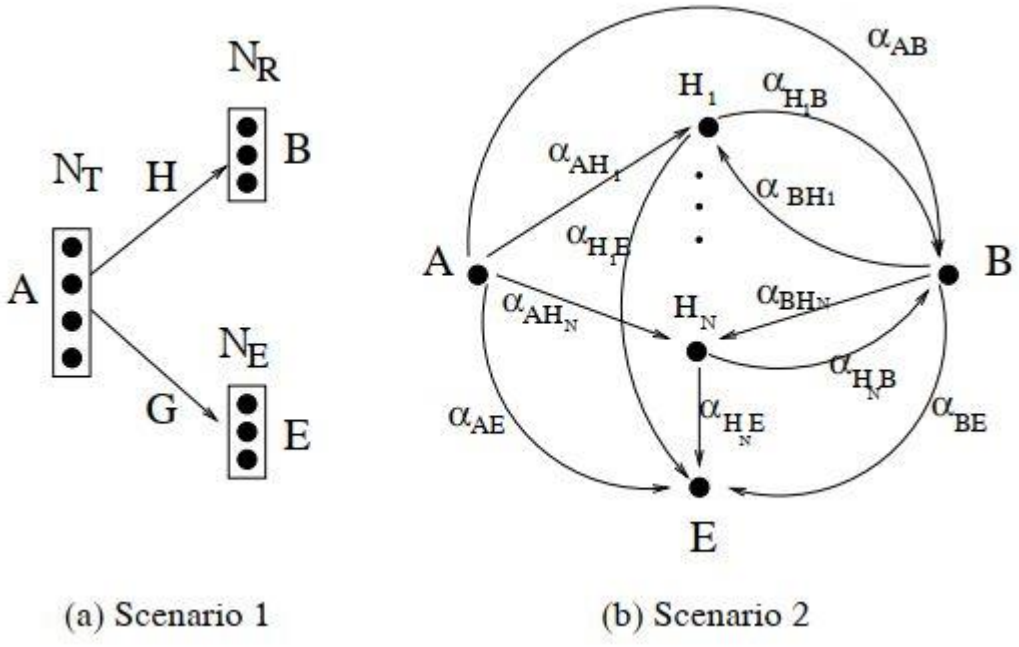

Figure 2.9 (a) Multi-antenna AN generation (b) amplifier relay AN generation (Negi & Goel, 2005)

2.5 Modulation Schemes

There are two types of modulation schemes in communication which are analog modulation (AM) and digital modulation (DM). AM technique is used for analog message signals, and the DM is used for digital signals transmitted over a communication channel which can be wired or wireless. DM is the most popular and highly used wireless communication channel. Further, the DM technique is classified as frequency modulation (FM), amplitude modulation (AM), and phase modulation (PM), where each of them is classified again into different categories depending on the number of bits that are modulated at once. Binary amplitude shift keying (BASK), binary phase shift keying (BPSK), and binary frequency shift keying (BFSK), where one bit is modulated at once. Quadrature amplitude shift keying (QASK), quadrature phase shift keying (QPSK), and quadrature frequency shift keying (QFSK), where two-bit sequences are modulated once and M-ASK, M-PSK, and M-FSK where three or more bits are modulated at ones. QAM modulation is a modulation scheme where both the amplitude and phase are modulated. All types of modulation schemes have their area of application. PSK modulation

scheme is highly used in wireless communication for the increased security it provides and less complexity compared to QAM, where both phase and amplitude are modulated.

BPSK, QPSK, 8-PSK, and QAM Modulation

A. BPSK

The most basic kind of PM is called BPSK, and under this method, the carrier phase merely represents a pair of phase states. It is distinguished by using a constellation graph with a single-dimensional data point and binary signal nodes.

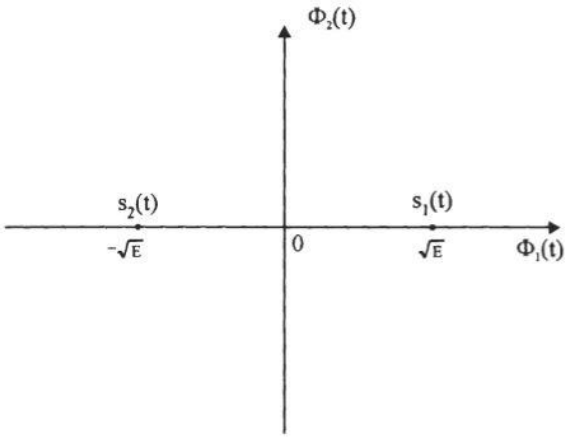

Figure 2.10 BPSK constellation diagram (Xiong, 2016)

Both of the phases, which have a distance of 180^0, are referred to as 2-PSK. One carrier is modulated in BPSK by altering its polarity under the information in the binary input that will be broadcast. The greatest amount of power that can be provided is increased because the BPSK message's magnitude is maintained fixed.

The two-byte code in polarized form having symbols 1 and 0 is denoted by constant magnitude values of $-\sqrt{E}$ and$+\sqrt{E}$, accordingly resulting in a BPSK signal. The modulator receives the consequent binary pulse in a polarised state and a sinusoidal carrier $\phi_1(t)$, a frequency that is determined as $f_{c=}({}^{n_c}/_{T_b})$ with a given variable nc. Typically, a typical master clock is utilized for obtaining the carrier and clock pulses needed to produce the binary wave. You can get your preferred PSK signal from the modulator's output (Barnela, 2014).

A simplified block diagram of the BPSK modulation technique is shown in the below figure.

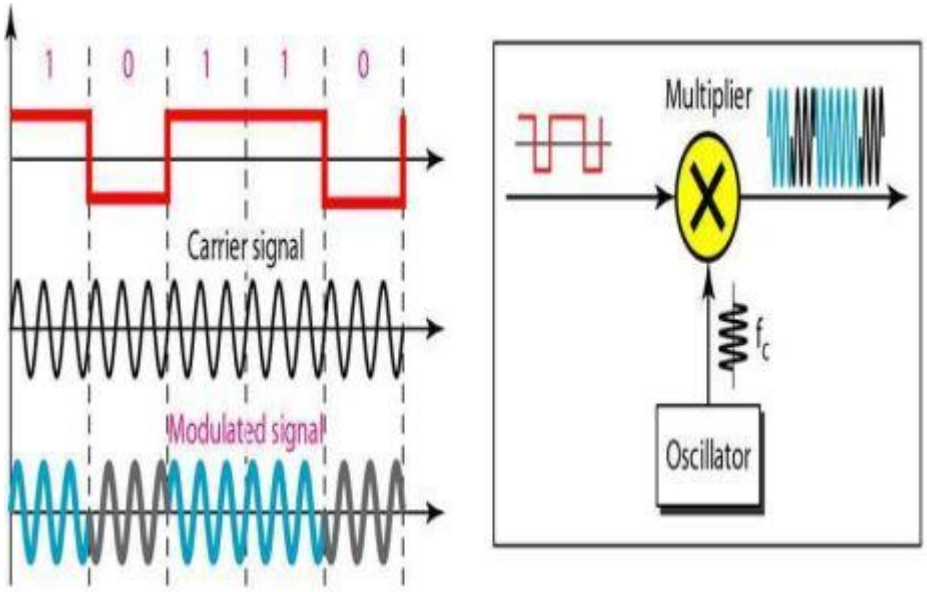

Figure 2.11 Block diagram of BPSK (Wu et al., 2018)

B. QPSK

In the QPSK modulation technique, each pulse signal phase is segregated between four evenly separated intervals for the phase angle of 45^0, 135^0, $-45^{0,}$ and -135^0. The QPSK DM method gives it an important benefit above BPSK by doubling its data storage.

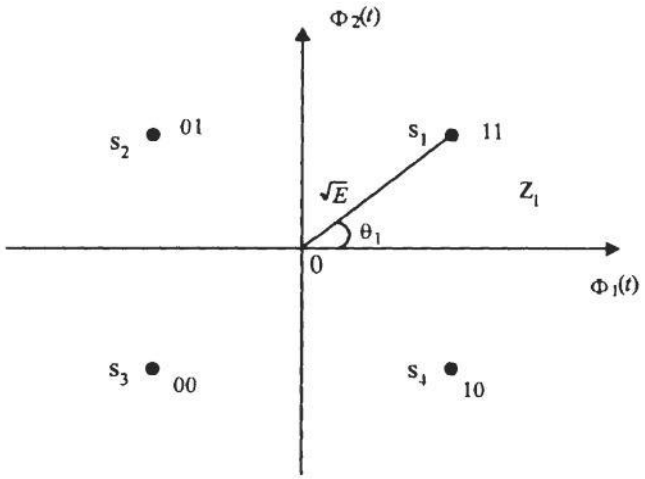

Figure 2.12 Constellation diagram of QPSK (Xiong, 2016)

Since there are a total of quadruple data nodes within QPSK's constellation graph, this makes it an incredibly bandwidth-efficient DM technology. Every single symbol in QPSK contains a pair of bits of information that need to be communicated, and every symbol may include any of four potential values: 00, 01, 10, or 11 (Das et al., 2013). Since additional information may be conveyed utilizing several phases and just one carrier, QPSK requires a smaller bandwidth and power (Taware, 2013). The QPSK approach can be utilized either to conserve the bandwidth of the message by doubling its information rate relative to a BPSK modulation method or to keep the information rate of BPSK yet halving the bandwidth need (Mishra et al., 2012).

A simplified block diagram of the QPSK modulation scheme is shown in the below picture.

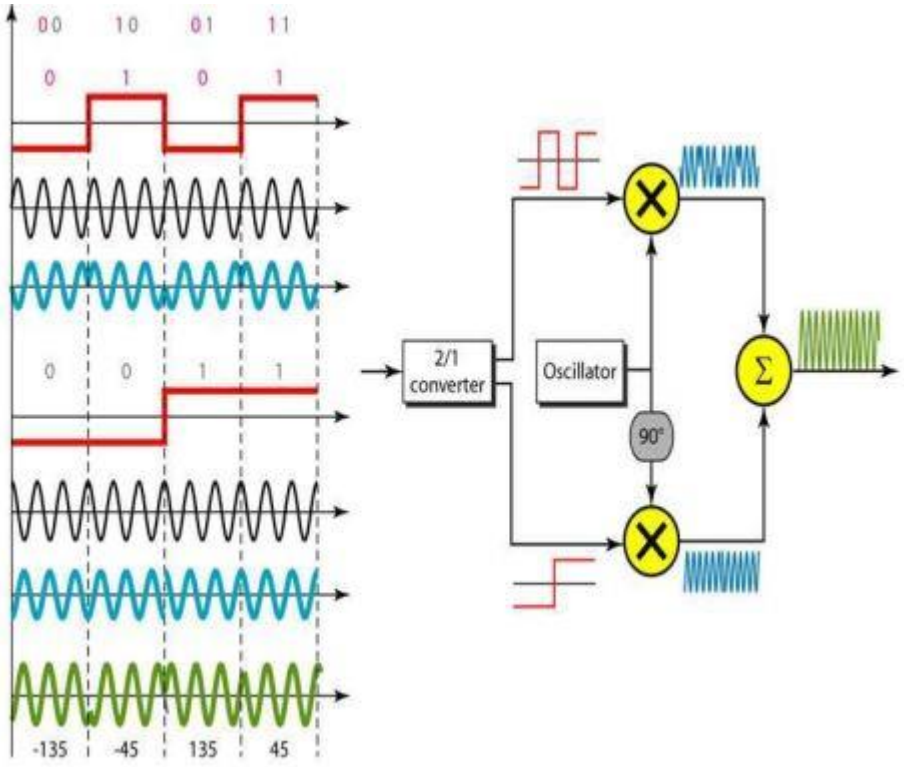

Figure 2.13 Block diagram of QPSK (Wu et al., 2018)

C. 8-PSK

Every single symbol in 8-PSK contains three bits of information that need to be communicated, and every symbol may include any of eight potential values: 000, 001, 010, 011, 100, 101, 110, or 111. The eight potential values listed above take these 8 angles in the constellation diagram 0^0,45^0, 90^0, 135^0, 180^0, 225^0, 270^0, and 315^0.

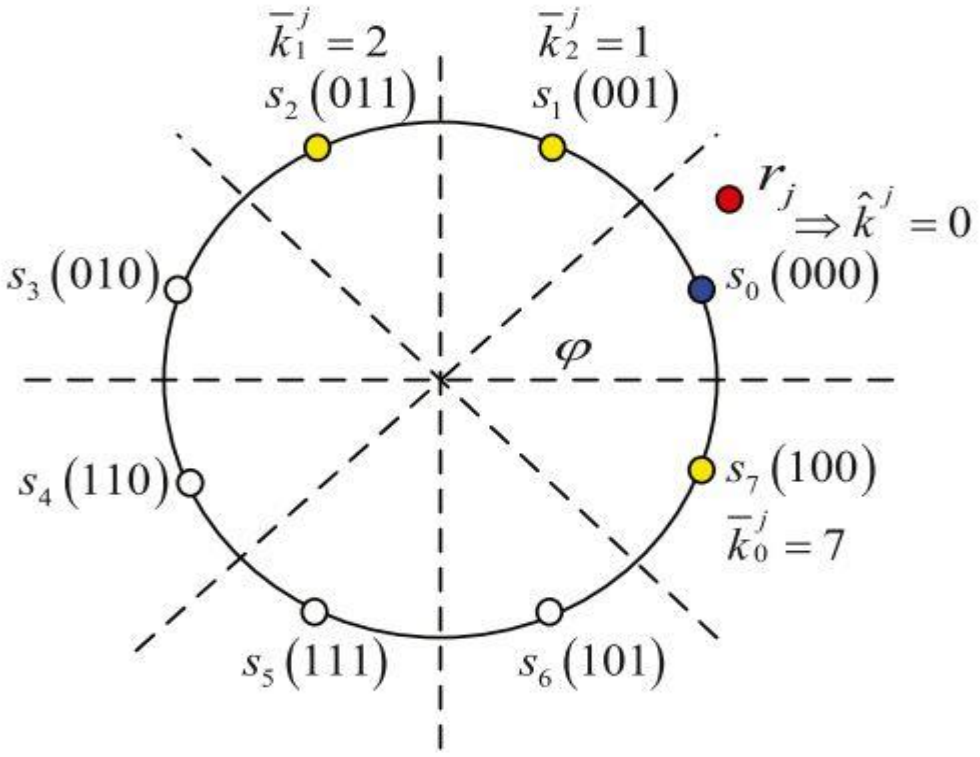

Figure 2.14 Constellation graph of 8-PSK bit arrangement in a Gray code(Li et al., 2016)

Since additional information may be conveyed utilizing several phases and just one carrier, 8-PSK requires a smaller bandwidth and power also from the QPSK modulation scheme.

All of the modulation techniques that are listed and not listed here have their area of application. When we come to security in our case, BPSK has got a better performance; if our focus is shifted to increased communication speed, we will choose 8-PSK since three bits are being modulated at a time but creating a higher inter symbol interference and creating a higher BER value and making it not highly selected for security.

2.6. Related Work

In (X. Chen et al., 2015), the authors provided a lesson about different multi-antenna relaying systems. Modern studies have been performed on multi-antenna relay-supported by PLS. Special attention is given to massive MIMO relaying technology because it is efficient in addressing several difficult problems regarding wireless PLS, like narrow surveillance despite

eavesdropper CSI as well as inadequate valid CSI. The case of multiuser access and mobile relay is not considered.

In (Parrón et al., 2021), the transmission of a stream of symbols for each measurement angle is commonly used to test the DM's BER efficiency; however, this method can be tedious. This research developed a method for precisely and effectively determining the DDM BER for typical modulation schemes; to demonstrate the advantages and constraints of the assessment approach, various DDM setups are evaluated. Additionally, a non-iterative DDM analysis having limitations in the BER response is presented using the suggested methodology. The system performs only under an omnidirectional antenna.

In (Jin et al., 2021), the authors designed to reduce the amount of BS sent power; this research suggested a NOMA PLS communication approach. The user close to the BS is used in this system as a helpful conduit to enhance the efficiency of the user away from the base station. A SWIPT employing the EH technique is deployed close to the user to gather energy that can be deployed in the collaborative phase. To combat this issue, AN is employed at the BS to improve the confidentiality of secrecy information. This is because eavesdroppers within the downlink of a NOMA scheme can employ the SIC technique to access the receiver's secret data. Additionally, to address the aforementioned non-convex issue, the SDR approach and SCA methodology are merged. Considers only one passive Eavesdropper and one legitimate user.

In (Hong et al., 2020), the authors designed an efficient MIMO wireless communication system with AN support is discussed. The enhanced IRS is activated, and the BS, real IR, and Eve are outfitted with many antennae to improve the security of the system's effectiveness. The TPC vector of BS, covariance matrix used with AN, also phase shifts of IRS are simultaneously improved to maximize the SR, subject to limitations of the transmission power limit and unit modulus of IRS phase shifts. The SRM issue, a non-convex problem with numerous coupled variables, is then formulated. To address the issue, we suggest using the BCD algorithm to concurrently modify the parameters when maintaining SR. In particular, the LM method is used to produce the best TPC matrix and AN covariance matrix, while the MM algorithm is used to determine the best phase shifts. The suggested approach is extremely effective because all variables can be estimated in closed form. A BCD technique is proposed

to resolve the SRM problem, which is also expanded to include the more common multiple-IRS scenario. TPC matrix is not optimized at the user side, only considered at the BS.

In (Makin et al., 2022), authors investigated intelligent surfaces that have recently been promoted as a ground-breaking method and acknowledged as one of the contenders for wireless networks that go beyond the fifth generation. This study examines the PLS of a wireless system with LIS assistance over Nakagami channels. LIS's phase-shift optimization approach is successfully used in the suggested phase-based AM strategy to improve the security of systems. Additionally, the effectiveness of the architecture is studied concerning the Nakagami fading parameter (m), correlation parameter (ρ), and several passive LIS components (M). While assessing the BER efficiency of the suggested system, a substantial advancement in security is demonstrated. Didn't consider the case for multiple users and eavesdroppers.

Here (Gong et al., 2021), the effectiveness of a large-scale downlink system using FD NOMA communication assisted by AN is examined in this research concerning confidentiality outages. The structure's LUs are dispersed arbitrarily based on homogenous Poisson point techniques, but an active Eve is undoubtedly present. In our new safe collaborative interaction approach, NOMA users running close in FD mode serve as jammers and produce AN to improve the PLS of the genuine broadcast. A user couple is given closed-form phrases in terms of the SOP. The secrecy variations sequence assessment is then performed for two different situations, fixed transmit SNR at the Eve and transmit SNR at the Eve being proportionate in terms of LUs, in light of the analytical findings. For both circumstances, asymptotic SOP closed-form equations are discovered as well. Only passive Eavesdropper is considered.

In (Okeke & Asianuba, 2019), the authors study a WiMAX framework developed and examined using various modulation methods and encoding ratios. Didn't show the best modulation technique in the physical layer security technique.

In (Lemayian & Hamamreh, 2021), the authors analyzed and measured the privacy efficiency of hybrid MIMO. The data interference-canceling vectors in this work offer complete security (no data escape) contrary to external as well as internal intrusions, according to the reliability

assessment that was done. Furthermore, consumers receive the desired information straight as a result of the novel MIMO technology, which avoids the requirement for any sort of analysis at the point of reception and reduces sophistication and power usage there. For upcoming IoT, in addition to 6G and further innovations, they are very important features. The propo performs in the presence of AWGN noise without considering fading channel.

In (Zeng et al., 2022), the authors investigated the PLS of a wirelessly polar-coded transmission network is investigated in this work. To be very precise, a frozen-bit pattern-generating approach founded on CQI is proposed that utilizes the special characteristics of polar code generation. By the immediate CQI of the valid link, the sender uses the Gaussian estimation approach to construct the associated frozen bit pattern. At the destination, CQI is mapped to the matching frozen bit sequence and accurately decodes the received bits by taking advantage of the complete channel reciprocal in the TDD mode. Eve, on the other hand, failed to gain information about the lawful channel, so it was impossible to ascertain the frozen bit pattern of the polar-coded bit sequence. Doesn't consider the keyless technique of physical layer security; only a key generation scheme is applied.

In (R. Chen et al., 2019), the authors analyzed the overall setting of URLLC, PLS being the main topic of the paper. For achieving confidentiality, the PLS approach primarily relies on communication schemes that take advantage of the wireless medium's inherent unpredictability. PLS has fewer features and delays than conventional encryption as a result. This article explains the disparity between delay, dependability, and privacy by introducing relevant benchmarks to assess PLS in URLLC. The contribution that CSI may play in potentially offering remedies to these difficulties is then examined once the main tough issues for establishing PLS for URLLC have been highlighted.

In (Arfaoui et al., 2020), the authors have investigated the majority of PLS for VLC's facets covered, encompassing several channel designs, data ranges, system setups, precoding/signaling tactics, privacy capability, and data speeds. Additionally, to fully exploit the capabilities of these advancements, here a variety of immediate and accessible areas of study for PLS-VLC structures, including the implementation of measurement-based both inside and outside channel designs, the incorporation of user movement and equipment

positioning through the channel framework, as well as the combination of VLC and RF networks.

In (Pham et al., 2023), the authors developed AN to improve PLS in VLC networks is examined in this study in the situation of input data lacking a specified amplitude limitation (like multicarrier devices). For keeping the input messages inside the constrained linear limits of the light-emitting diodes in these kinds of networks, cutting is required. The AN architecture has to consider non-linear clipping deformation consideration as a result of this clipping procedure. The CCT and the CCP are used to propose a sub-optimal layout plan that will help solve this issue. The confidentiality degree is greatly reduced by clipping deformation, according to statistical information, and adopting AN has a benefit against a no-AN method in terms of enhancing secrecy function. Clipping without modulation technique is deployed.

In (Panayirci et al., 2020), the authors investigated a newly developed SCD approach is put out to improve the optical GSSK's PLS while retaining certain SM advantages. Since there is no small-scale fading, the data received on the authorized user's end is tailored using the visual channel's quasi-static properties. The correct choice of the power distribution parameters for arbitrarily triggered LEDs ensures the PLS of the system. The bit error ratio (BER) of Bob is reduced with the use of the CSI from Bob at the transmitter, but the BER efficiency of Eve dramatically deteriorates.

In (Shi et al., 2022), the authors presented an overview of the PLS studies on many prospective emerging mobile innovations, such as secure key generation, DM, SM, covert communication, and IRS-aided communication. It also discusses keyless and secure key generation strategies. PLS for mobile communications is provided as the final topic, along with excellent complications with technology.

In (Ari et al., 2022), the authors examined the effectiveness of short packet transmissions in the circumstances of numerous eavesdroppers. The examination began by looking at the faded wiretapping channel, wherein the conversation can be listened to through numerous single-antenna hackers who are not cooperating. Assuming the sender has just one antenna, a closed-form calculation for the mean secrecy capacity is obtained. The findings of the Monte-Carlo

computations closely correspond to the mathematical formulation. Additionally, the best block length quantity is identified while both one and numerous hackers are monitoring the conversation to maximize secrecy performance. The study is expanded to account for multiple antenna transmitters and considers AN to fool listeners. In the case of a dual-antenna sender and dual hackers with just one antenna, a closed-form equation for the mean secrecy capacity is found. When contrasted with Monte-Carlo modeling, the outcomes show the approximation's reliability. A short packet without the best modulation technique is deployed.

In (Ryland et al., 2017), the author's work on the development of a pair of PLS approaches upon SDRs is covered in the present paper. PLS is a group of safety procedures that use the tangible features of the signal or channel of transmission to safeguard transmission. The initial approach uses a 2 1 MISO in which the sender injects AN onto the recipient's null space using CSI by the legitimate receiver. The additional version, known as PEAC, uses a single-carrier Alamouti coding system with implemented pseudorandom phase shifts for every broadcast antenna. The Alamouti equalization performed by the legitimate receiver, who is aware of the pseudo-random sequence, can reverse these phase shifts, but an illegitimate receiver who is unaware of it is going to be incapable of deciphering the message.

Table 2.1 Related Works

Authors	Tittle	Contribution	Gap
N.Arı, N.Thomos, and L.Musavian(2022)	Performance Analysis of Short Packet Communications With Multiple Eavesdroppers	Short packet communications in the presence of multiple eavesdroppers considering AN is studied.	A short packet without the best modulation technique is deployed.
T.V. Pham, S.Hranilovic, and S.Ishihara(2022)	Design of Artificial Noise for Physical Layer Security in Visible Light Systems With Clipping	The design of AN to enhance PLS in visible light systems is studied in the context of input signals with no explicit amplitude constraint (such as multicarrier systems).	Clipping without modulation technique is deployed.
Childress, J. R.(2019)	Physical Layer Security for MIMO Wireless Systems	MISO system PLS with AN is achieved with the QPSK modulation technique	The system is employed only on the QPSK modulation technique. Only 2 Tx and 1 Rx antenna for TX BF are employed.

CHAPTER THREE

MATERIALS AND METHODS

3.1 Introduction

In this thesis work, the performance of PLS in the addition of AN is analyzed and discussed with a multi-antenna MISO 2X1, two transmit, and one receive antenna system with Transmit beamforming applied to the legitimate receiver Bob. And the performance is evaluated in two different modulation techniques, BPSK and QPSK.

3.2 Materials

The simulation in this thesis is done using the MATLAB/R2020a MEX file package software. The packages required for the simulation in MATLAB form.

3.3 Methods

As mentioned above, this work analyzes the performance of the AN-aided PLS technique. The system incorporates multi-antenna MISO and uses Transmit Beamforming approach from the two antennas of the transmitter to the intended receiver Bob; having one receive antenna increases the security performance of Bob. The multi-antenna system here, having two transmit antenna and one receive antenna for both Bob and Eve, generates an AN and send it to the null space of Bob's channel, making Bob secure and only receiving the transmitted message while letting passive Eve receive both the generated AN and message that makes it get a higher BER. The system performance is analyzed in the presence of AWGN and Rayleigh fading channel.

Also, the performance of transmit beamforming is discussed for two, three, and four transmit antenna is discussed for two modulation techniques, BPSK and QPSK.

3.3.1 System Design

It involves the following

- Analyzing the mathematical model of AN.

- Analyzing the mathematical model for the Transmit beamforming weights for increased secrecy.
- Analyzing the BER formulas for the two modulation techniques used.

3.3.2 System Model

The System model is shown in the figure below:

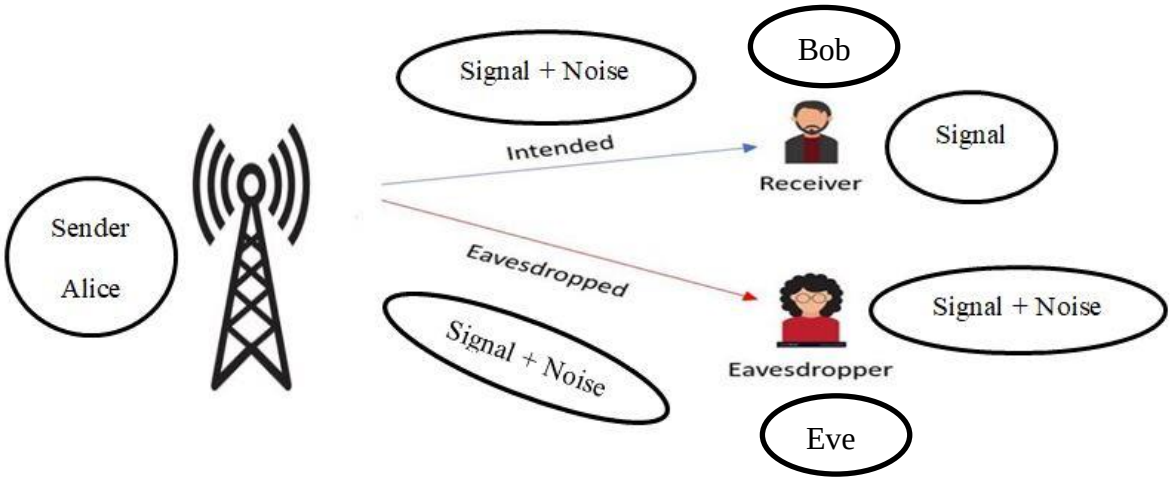

Figure 3.1 AN- aided passive attack PLS system model

3.3.3 Simulation Methods

It involves the following:

- AWGN noise generation in Rayleigh fading channel.
- Design a MATLAB code for the modulation technique used.
- Transmit Beamforming generation and application in legitimate Bob's channel, AN generation and allocation of 20%, 40%, 60%, and 80% power from the total transmitted power.
- Evaluation and comparison of the BER performance of the system with and without the presence of AN.

3.4 Mathematical Model of Modulation Schemes

As mentioned earlier here, we used two types of PSK modulation schemes, BPSK and QPSK. In this thesis, since our objective is to achieve a better SNR performance of increased PLS, we will analyze the mathematical model for theoretical calculation of the BER performance of all the two modulation schemes, of which their performance has been analyzed in the MATLAB software simulation.

Theoretically, the BER calculation of the two modulation schemes equations is listed below. Where BPSK and QPSK have the same BER formula and almost the same BER while simulating since the BPSK modulation technique has a better performance of SNR since a single bit is modulated once while looking at QPSK two bits are modulated ones where it increases the case of ISI. This makes BPSK better when we need a short-distance transmission and better BER performance(Golam Sadeque, 2015).

$$BER = \frac{BITS\ WITH\ ERROR}{BITS\ SENT} \tag{3.1}$$

BER for BPSK and QPSK calculation is the same, but there is a better performance of BER of BPSK in real; the equation over Rayleigh fading channel with AWGN noise is shown below:

$$p_b = \frac{1}{2}\left(1 - \sqrt{\frac{E_b/N_0}{1+E_b/N_0}}\right) \tag{3.2}$$

Where, E_b/N_0 is SNR per bit

3.5 Mathematical Model of Transmit Beamforming

Unlike SIMO systems using MRC here, since the system used is MISO, transmit beamforming is used. Two transmit antenna with a single receive antenna system model is depicted in this thesis. In terms of PLS, the goal of beamforming is to make certain that Bob, the legitimate receiver, has a higher SNR over Eve, the illegitimate receiver(Khisti & Wornell, 2010). By scaling the data signals carried over every transmit antenna with a complex conjugate of the channel of the legitimate receiver, transmit beamforming directs the information in the

direction of the desired recipient. This has the effect of combining each piece of information obtained at the legitimate receiver in a way that enhances the receiver's SNR.

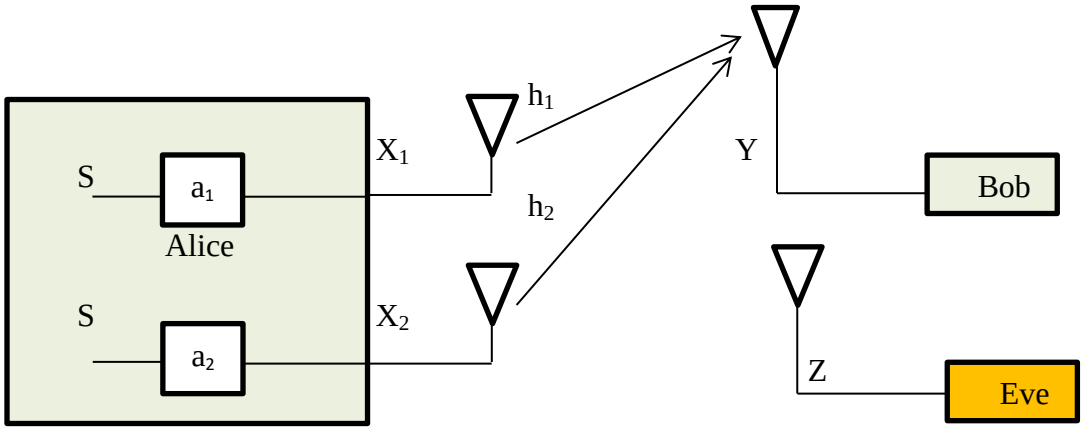

Figure 3.2 Transmit beamforming model (Zhou & Giannakis, 2004)

In the aforementioned Transmit beamforming situations, Alice beam forms the information-bearing message to Bob using a pair of transmit antennas while Bob and Eve each use just one receive antenna. Alice beam forms beamforming weights using Bob's CSI and sends the message data throughout the appropriate sender antenna in Alice's dual antenna array as:

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_1 s \\ a_2 s \end{bmatrix} \tag{3.3}$$

x is the sent data vector comprising a combination of the data signals and the beamforming weights created by Alice depending upon Bob's CSI (Khisti & Wornell, 2010).

The complex channel parameters h_1, and h_2, are included in Bob's channel matrix H; thus, the data obtained at Bob is transformed into:

$$y = [h_1 \; h_2 \;] \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \; n \tag{3.4}$$

$$y = h_1 x_1 + h_2 x_2 + n \tag{3.5}$$

$$y = h_1 a_1 s + h_2 a_2 s + n \tag{3.6}$$

$$y = \frac{h_1 h_1^* s}{|h_1|} + \frac{h_2 h_2^* s}{|h_2|} + n \quad (3.7)$$

the shifted phase of the formed beams are

$$a_1 = \frac{h_1^*}{|h_1|} \quad (3.8)$$

and

$$a_2 = \frac{h_2^*}{|h_2|}. \quad (3.9)$$

The simplified form of information perceived by Bob is:

$$y = (|h_1| + |h_2|)s + n \quad (3.10)$$

As we increase the number of the transmitter to N antennas, equation (3.10) can be expanded to:

$$y = (\sum_{n=1}^{N} |h_1| + |h_2| + \cdots |h_n|)s + n \quad (3.11)$$

3.6 Mathematical Model of Artificial Noise

The sender (Alice) creates AN and transmits it throughout every path besides the path of the legitimate receiver Bob. This is the AN approach. When Alice is aware of the CSI for Eve's channel, that usually can't be applicable in the scenario of a passive eavesdropper, Alice may increase the total impact of the AN on Eve. The goal of creating AN is to lower the overall performance of the channel for illegitimate receivers without lowering the performance of the channel for legitimate Bob.

Multi-antenna technique is studied where two transmit antennae and one receive antenna for both Bob and Eve. The multi-antenna generates the AN that is being transmitted throughout the channels of both Eve and Bob's null space. It is presumed that the eavesdropper is passive, meaning it isn't sending out anything but hears. Therefore, the sender might not be aware of its CSI. AWGN channel and Rayleigh fading with a transmit beamforming are considered here.

When the data signal is broadcast in the spectrum of the receiver's channel, AN is created so that it falls within the null space of the recipient's channel. The receiver's channel must be known for this system to work, while the illegitimate channel is not. The receiver is unaffected by the noise because the recipient's channel cancels out the AN. Yet, its coverage space will differ from that of the recipient's channel; the illegitimate Eve channel will generally deteriorate still, and certain artificial noise will therefore be present in its range space.

We will now go over how the multi-antenna transmitter, in our case two antennas, can produce AN to weaken the illegitimate receiver's channel. The transmitter selects x_k as the result of adding the information-bearing signal s_k and the Artificial Noise-generating signal w_k as well as the beamforming weight a_k. w_k , is assumed to be a complex Gaussian symbol vector.

$$x_{k=}a_k s_k + w_k \tag{3.12}$$

w_k , is made to lie in the null space of Bob's channel where the bellow equation holds.

$$H_k w_k = 0 \tag{3.13}$$

is met by Alice selecting w_k ensuring it falls under Bob's channel H_k's null space.

The received signal by Bob is:

$$y_k = H_k x_k + n_k \tag{3.14}$$

$$y_k = H_k(s_k a_k + w_k) + n_k \tag{3.15}$$

$$y_k = H_k a_k s_k + n_k \, . \tag{3.16}$$

For an increased number of antennas and multiple users, equation 3.16 will expand to:

$$y_k = s_k \sum_k^N a_k H_k + n_k \tag{3.17}$$

Being observed, the signal that Bob obtained has lost the AN-related part. In contrast, Eve detected the following signal where G_k is eavesdropper's channel:

$$z_k = G_k x_k + e_k \tag{3.18}$$

$$z_k = G_k(a_k s_k + w_k) + e_k \tag{3.19}$$

$$z_k = G_k a_k s_k + G_k w_k + e_k \quad (3.20)$$

For an increased number of antennas and multiple eavesdroppers, equation 3.20 will expand to:

$$z_k = s_k \sum_k^N G_k a_k + w_k + \sum_k^N G_k w_k + e_k \quad (3.21)$$

Whereas Eve's channel G_k suffers greatly from the existence of the AN symbolized by $G_k w_k$ in the signal she receives. As the AN vector w_k is located in Bob's null space, Bob is not aware of the AN element. This causes the AN to affect possible eavesdroppers, such as Eve, in all parts but not Bob's.

The transmitted signal is designed as when the entire transmission power allotted to the creation of AN compared to that data signal is depicted by:

$$\mathrm{x_k} = \sqrt{(1-\mathrm{r})}\mathrm{s_k} + \mathrm{e^r w_k} \quad (3.22)$$

in which r is a proportion of the AN's amplitude versus the overall amplitude from the signal being transmitted. Here the values taken for the simulation of the designed model is r: 0.2, 0.4, 0.6, and 0.8.

Equation 3.21 is designed here for creating a better BER performance to be achieved even at 20% AN is added where the value of r is 0.2.

CHAPTER FOUR

Result and Discussion

4.1 Introduction

Here, the simulation result of the proposed algorithm is discussed in two sections. In section one, the simulation result of transmit beamforming on BPSK and QPSK modulation technique for both Bob and Eve is discussed. Transmit beamforming is performed for two, three, and four transmitter antennas and a single receive antenna for both Eve and Bob. In section two, the simulation result of AN-aided transmit beamforming on Rayleigh fading, and AWGN channel is analyzed considering passive eavesdropper on the two modulation techniques. The results are performed considering the 2X1 MISO system.

In section one, the performance of the two modulation techniques, while transmit beamforming, is applied is analyzed. Figures 4.1 to 4.6 show simulation results for both BPSK and QPSK modulation techniques. **Table 4.2** shows the overall simulation result for transmit beamforming at 10dB SNR. Considering two, three, and four transmitter antenna for creating a strong beam on the main lobe for Bob's channel while increasing interference for Eve's channel and making the BER of Eve's channel more worst. For both BPSK and QPSK modulation techniques, it is analyzed that Eve has got no advantage over the TX beamforming having the same BER value of $10^{-1.9}$ for BPSK and 10^{-1} at SNR value of 10dB for any number of transmitter antennas deployed. And also, Bob's channel without beamforming has got the same BER to SNR plot as Eve.

In section two, we analyzed the performance of the two modulation schemes based on different AN power allocations from the overall transmit power used for the message signal transmission, which is 20%, 40%, 60%, and 80%. **Table 4.3** shows the overall simulation result for AN at 20dB SNR. Figures 4.7 and 4.8 show the simulation result of the two modulation schemes and 20% AN power from the total transmitted power. Figures 4.9 and 4.10 shows the simulation result of the two modulation schemes and 40% AN power from the total transmitted power. Figures 4.11 and 4.12 shows the simulation result of the three modulation schemes and 60% AN power from the total transmitted power. Figures 4.13 and

4.14 shows the simulation result of the three modulation schemes and 80% AN power from the total transmitted power.

4.2 Simulation Parameter

The simulation parameter used in this Thesis work is found in Table 3.1:

Table 4.1: Simulation Parameters(Childress, n.d.)

Simulation Parameter	Parameter Value
Number of transmit antennas of Alice	2
Number of symbols	10^6
Number of receive antennas of Bob	1
Number of receive antennas of Eve	1
SNR in dB range	-25 to 35
Number of Passive Eavesdroppers	1
AN parameter r value	0.2, 0.4, 0.6, and 0.8

4.3 Transmit Beamforming Simulation Results

As shown in **Figure 4.1** and **Figure 4.2** for two transmitter antenna, BPSK modulation results have got a better BER performance for Bob's channel with transmit beamforming. At SNR of 10dB, BPSK has a lower BER of $10^{-2.9}$ while QPSK has a higher BER of 10^{-2}.

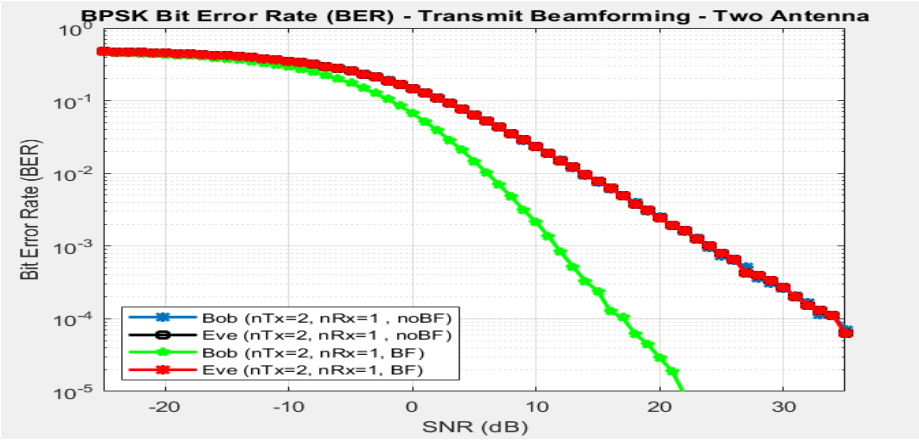

Figure 4.1 Simulation result plot for Bob and Eve with and without TX Beamforming in BPSK modulation technique with two transmit antenna transmitter side.

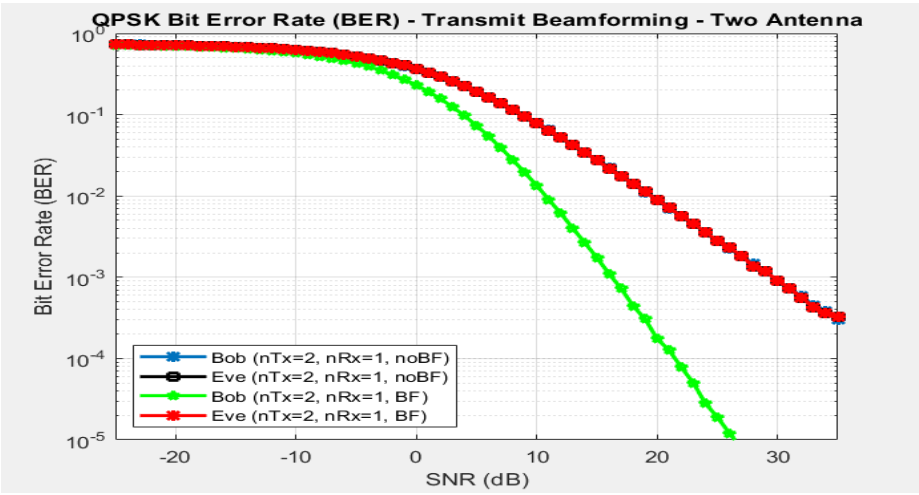

Figure 4.2 Simulation result plot for Bob and Eve with and without TX Beamforming in QPSK modulation technique with two transmit antenna transmitter side.

As shown in **Figure 4.3** and **Figure 4.4** for three transmitter antenna it is shown that the BER curve has decreased related to the two transmitter antenna case. At SNR of 10dB, BPSK modulation results have got a better BER performance for Bob's channel. BPSK has a lower BER of $10^{-3.9}$ while QPSK has a higher BER of $10^{-2.9}$.

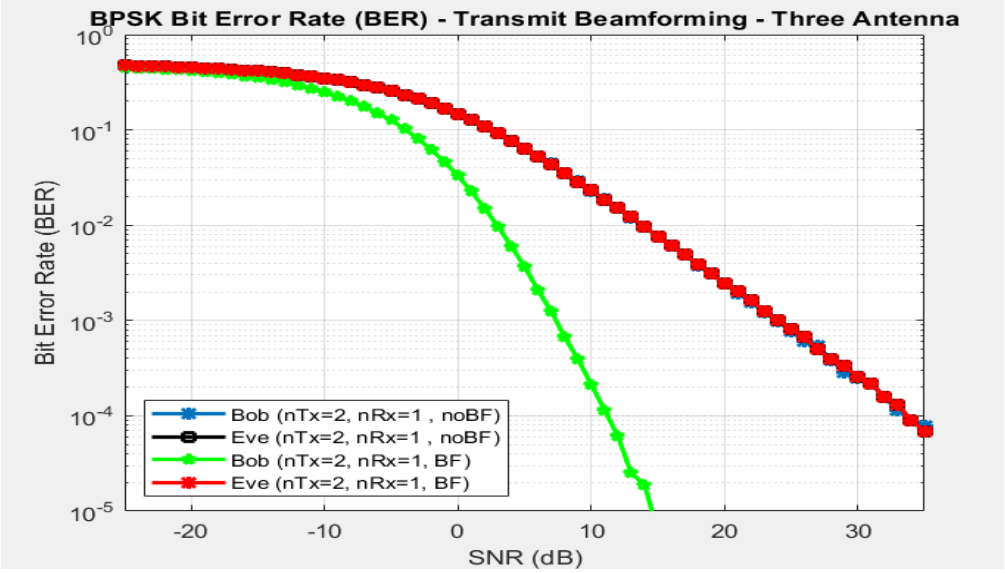

Figure 4.3 Simulation result plot for Bob and Eve with and without TX Beamforming in BPSK modulation technique with three transmit antenna transmitter side.

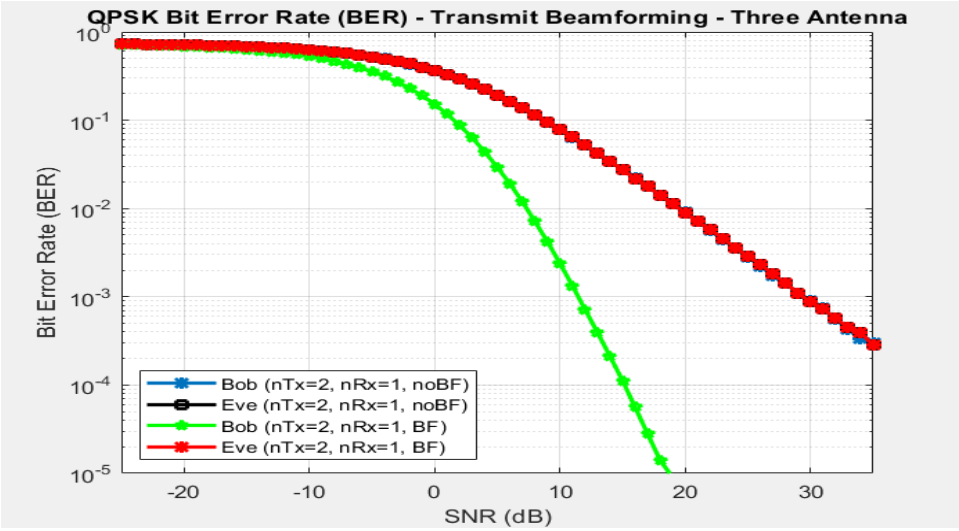

Figure 4.4 Simulation result plot for Bob and Eve with and without TX Beamforming in BPSK modulation technique with three transmit antenna transmitter side.

As shown in **Figure 4.5** and **Figure 4.6** for four transmitter antenna it is shown that the BER curve has decreased related to the three transmitter antenna case. At SNR of 10dB, BPSK modulation results have got a better BER performance for Bob's channel. BPSK has a lower BER of $10^{-4.8}$ while QPSK has a higher BER of$10^{-3.8}$.

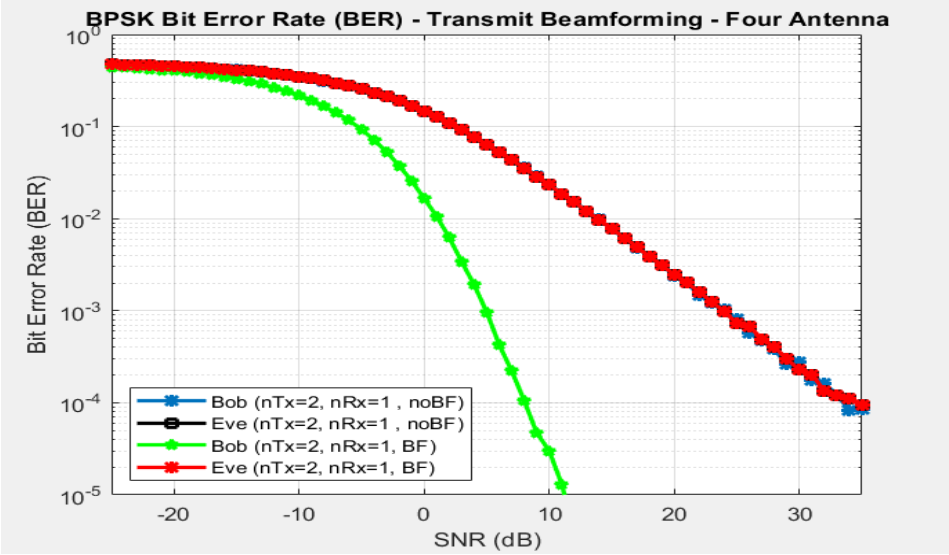

Figure 4.5 Simulation result plot for Bob and Eve with and without TX Beamforming in BPSK modulation technique with four transmit antenna transmitter side.

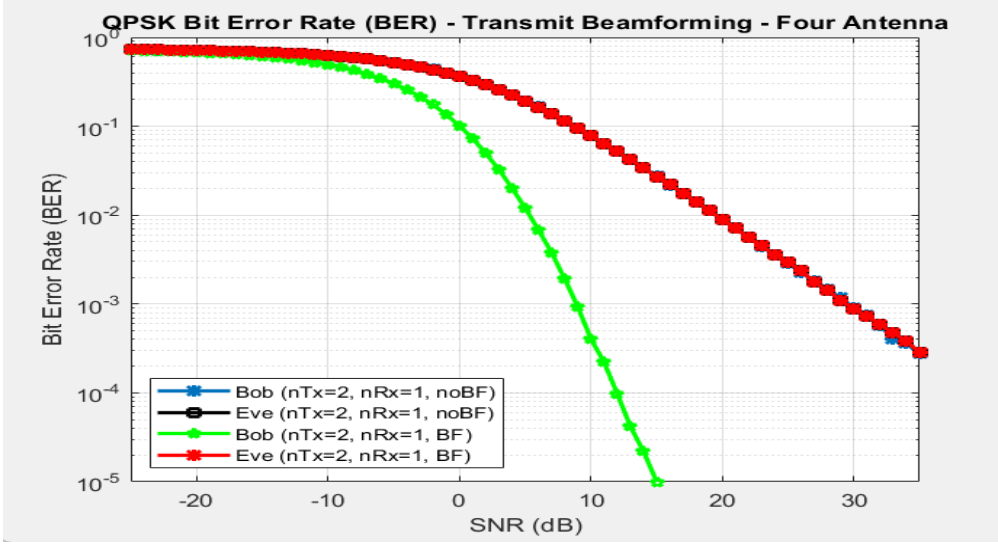

Figure 4.6 Simulation result plot for Bob and Eve with and without TX Beamforming in BPSK modulation technique with four transmit antenna transmitter side.

Table 4.2 BER performance comparison for BPSK & QPSK modulations for Bob and Eve channel with and without TX beamforming for two, three, and four antennas at SNR of 10dB.

No of Tx antenna	Modulation Technique	BER value with BF for Bob	BER of Eve and Bob without BF	BER value increased by	Remark
2	BPSK	$10^{-2.9}$	$10^{-1.9}$	9 times	The same BER performance
	QPSK	10^{-2}	10^{-1}	9 times	
3	BPSK	$10^{-3.9}$	$10^{-1.9}$	99 times	BPSK has got a better BER performance in the presence of transmit beamforming
	QPSK	$10^{-2.9}$	10^{-1}	78 times	
4	BPSK	$10^{-4.8}$	$10^{-1.9}$	793 times	
	QPSK	$10^{-3.8}$	10^{-1}	630 times	

4.4 Artificial Noise Simulation Results

From **Figure 4.7** and **Figure 4.8,** we can analyze that Eve's BER is significantly increased in the presence of AN. The BER of Bob is also slightly affected and increased in the presence of AN, which is the effect that comes in the decrease of the total allocated transmitted power from a mere 100% to 80% while 20% is being allocated to the AN also Bob has got a better BER performance in BPSK modulation technique than QPSK. Eve's BER increased from $10^{-2.95}$ to $10^{-0.9}$ for BPSK and 10^{-2} to $10^{-0.7}$ for QPSK modulation.

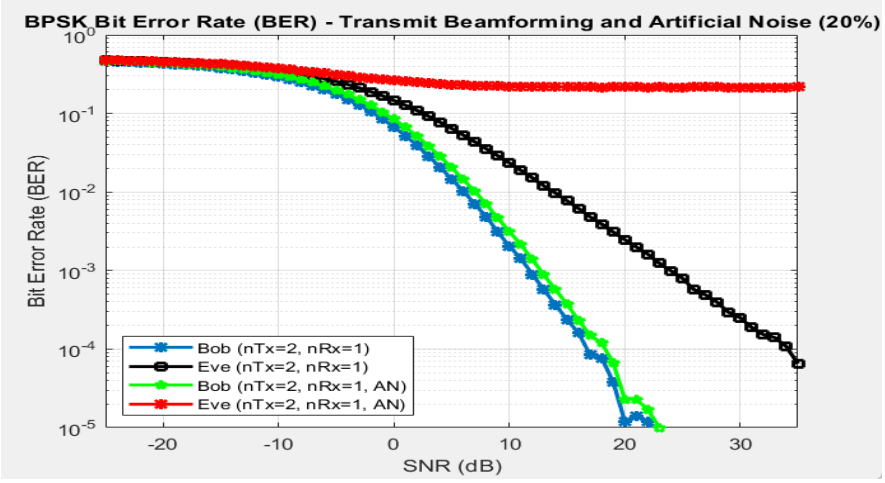

Figure 4.7 BER versus SNR simulation plot for Bob and Eve in BPSK modulation and 20% AN of total transmit power

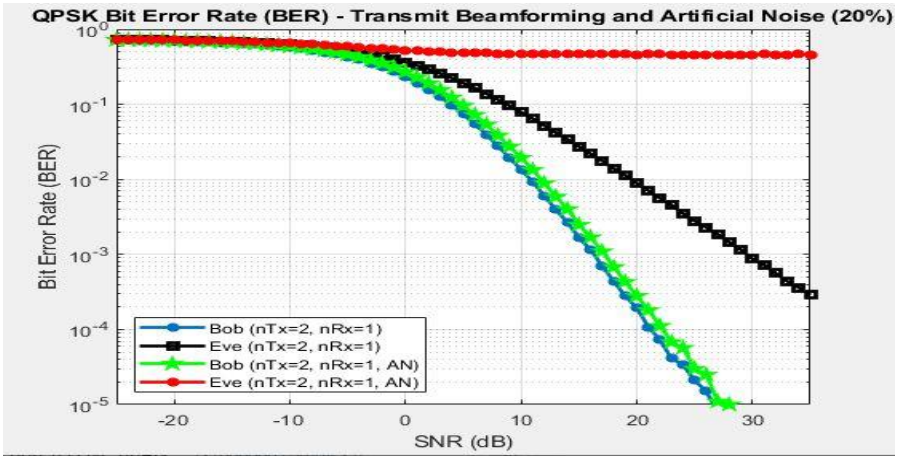

Figure 4.8 BER versus SNR simulation plot for Bob and Eve in QPSK modulation and 20% AN of total transmit power

From **Figure 4.9** and **Figure 4.10,** we can analyze that Eve's BER is significantly increased in the presence of AN. The BER of Bob is also slightly affected and increased in the presence of AN, which is the effect that comes in the decrease of the total allocated transmitted power from a mere 100% to 60% while 40% is being allocated to the AN also Bob has got a better BER performance in BPSK modulation technique than QPSK. Eve's BER increased from $10^{-2.95}$ to $10^{-0.8}$ for BPSK and 10^{-2} to $10^{-0.6}$ for QPSK modulation.

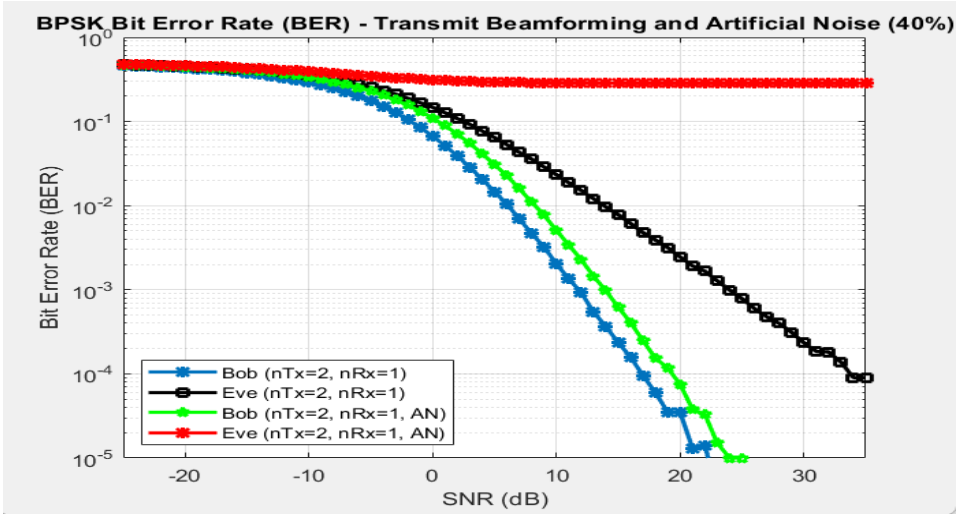

Figure 4.9 BER versus SNR Simulation Plot for Bob and Eve in BPSK modulation and 40% AN of Total Transmit Power

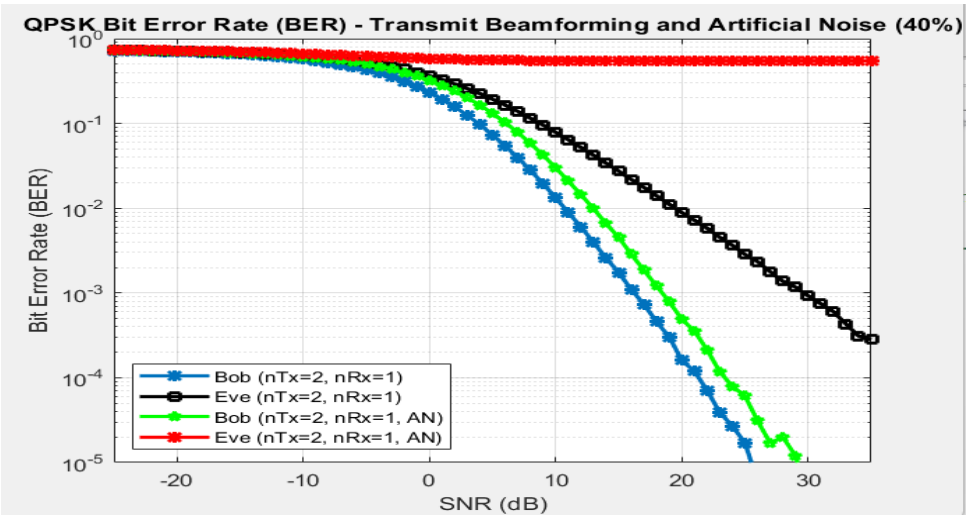

Figure 4.10 BER versus SNR simulation plot for Bob and Eve in QPSK modulation and 40% AN of total transmit power

From **Figure 4.11** and **Figure 4.12,** we can analyze that Eve's BER is significantly increased in the presence of AN. The BER of Bob is also significantly affected and increased in the presence of AN, which is the effect that comes in the decrease of the total allocated transmitted power from a mere 100% to 40% while 60% is being allocated to the AN also Bob has got a better BER performance in BPSK modulation technique than QPSK. Eve's BER increased from $10^{-2.95}$ to $10^{-0.75}$ for BPSK and QPSK modulation from 10^{-2} to $10^{-0.5}$.

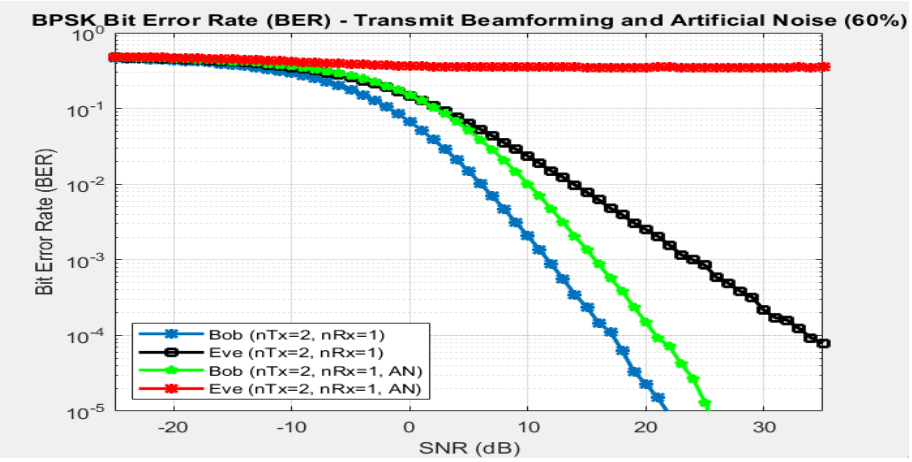

Figure 4.11 BER versus SNR simulation plot for Bob and Eve in BPSK modulation and 60% AN of total transmit power

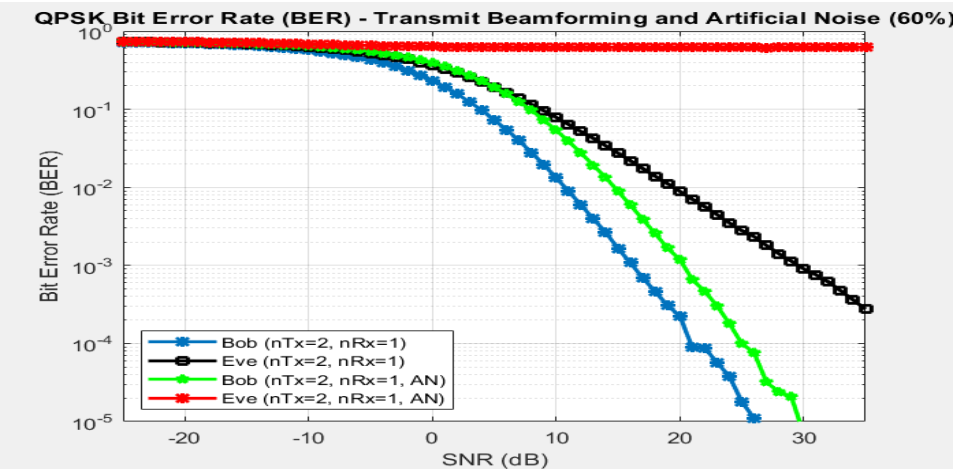

Figure 4.12 BER versus SNR Simulation plot for Bob and Eve in QPSK modulation and 60% AN of total transmit power

From **Figure 4.13** and **Figure 4.14,** we can analyze that Eve's BER is significantly increased in the presence of AN. The BER of Bob is also significantly affected and increased in the presence of AN, creating a worst-case performance scenario for Bob, which is the effect that comes in the decrease of the total allocated transmitted power from a mere 100% to 20% while 80% is being allocated to the AN also Bob has got a better BER performance in BPSK modulation technique than QPSK. Eve's BER increased from $10^{-2.95}$ to $10^{-0.7}$ for BPSK and QPSK modulation from 10^{-2} to $10^{-0.4}$.

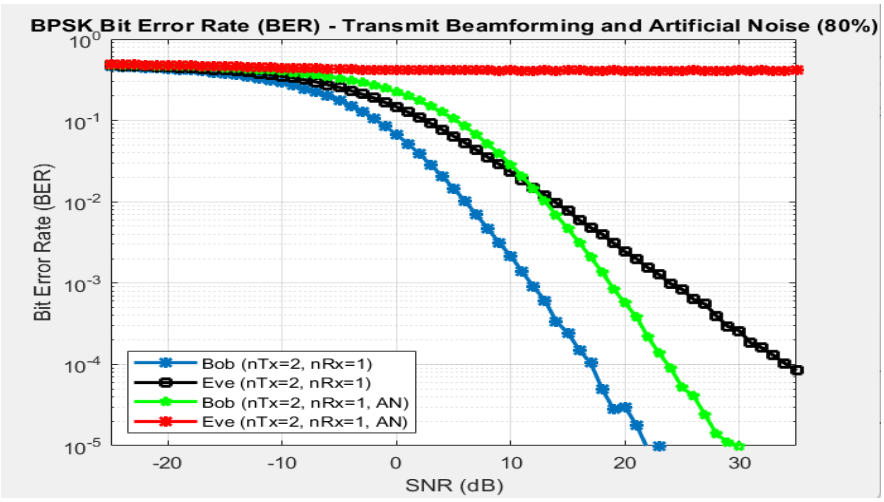

Figure 4.13 BER versus SNR simulation plot for Bob and Eve in BPSK modulation and 80% AN of total transmit power

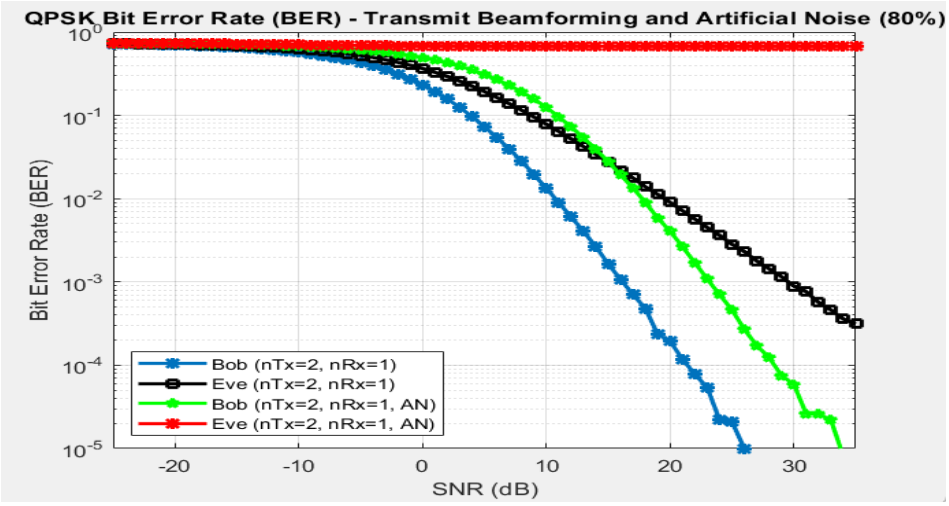

Figure 4.14 BER versus SNR simulation plot for Bob and Eve in QPSK modulation and 80% AN of total transmit power

Table 4.3 BER performance comparison for BPSK and QPSK for Eve's channel at 20%, 40%, 60%, and 80% Artificial Noise at an SNR value of 20dB

% of AN	Modulation Techniques	BER value With AN	BER value without AN	BER value increased by	Remark
20	BPSK	$10^{-2.95}$	$10^{-0.9}$	111 times	BPSK shows a higher BER increase
	QPSK	10^{-2}	$10^{-0.7}$	19 times	
40	BPSK	$10^{-2.95}$	$10^{-0.8}$	140 times	BPSK shows a higher BER increase
	QPSK	10^{-2}	$10^{-0.6}$	24 times	
60	BPSK	$10^{-2.95}$	$10^{-0.75}$	157 times	BPSK shows a higher BER increase
	QPSK	10^{-2}	$10^{-0.5}$	30 times	
80	BPSK	$10^{-2.95}$	$10^{-0.7}$	177 times	BPSK shows a higher BER increase
	QPSK	10^{-2}	$10^{-0.4}$	38 times	

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

In this research, to investigate a better performance and increased security, successive simulation has been made to analyze the performance of AN-aided PLS technique considering Transmit Beamforming, AWGN, and Rayleigh faded channel and two different modulation techniques considering passive eavesdropper. Here it is found that with the above-mentioned situations all for getting better security, the BPSK modulation technique has got a better BER performance in all percentage power allocated, 20%, 40%, 60%, and 80% for AN generation from the total transmitted power creating a lower BER for Bob in BPSK modulation compared with QPSK modulation scheme.

While analyzing the simulation result, it has been noticed that the BER performance of the intended receiver Bob, is also being altered in the presence of AN which is because of that the total transmitted power for the message has been reduced for the generation of AN. While we allocate 60% of the power for the AN generation, it has been seen that the BER curve of Bob with AN overlaps with Eve's BER curve for the SNR range from -10 dB up to 5dB for BPSK, -10dB up to 10dB for QPSK, which still making BPSK better. When we look at the power allocated for AN generation is 80%, it highly affects the BER performance of Bob, the legitimate receiver, which becomes the worst-case scenario.

As discussed in the simulation result for Transmit beamforming, while increasing the number of transmit antennas from two to three and four, Bob's channel with TX beamforming has got a better BER result as compared to Eve's channel and Bob's without TX beamforming for both modulation techniques performed. Also, a better BER performance is achieved with the BPSK modulation technique.

In general performance evaluation of the two modulation schemes, it is found that BPSK performs better, and also it has been seen that at 40% power allocation, better performance is investigated, making Eve more affected by the AN and also letting Bob not be affected to the worst.

Recommendations

This thesis deals with the performance analysis of AN-aided PLS technique with multi-antena wireless network. The following issues are the future recommendation of this work.

- An active Eavesdropper scenario is recommended, which creates an increased complication in the system, unlike the passive eavesdropper one.
- Both transmit and Receive beamforming techniques application for better-increased secrecy.

Reference

Alejandro. (2017). *The Basics of Antenna Theory*. 167–213.

Alfardan, N. J. (2014). *On the Design and Implementation of Secure Network Protocols*.

Alotaibi, E. (2016). *Physical layer security in wireless communications*. 295.

Anon. (1983). Ieee Standard Definitions of Terms for Antennas. In *IEEE Transactions on Antennas and Propagation: Vol. AP-31* (Issue 6).

Arfaoui, M. A., Soltani, M. D., Tavakkolnia, I., Ghrayeb, A., Safari, M., Assi, C. M., & Haas, H. (2020). Physical Layer Security for Visible Light Communication Systems: A Survey. *IEEE Communications Surveys and Tutorials*, *22*(3), 1887–1908. https://doi.org/10.1109/COMST.2020.2988615

Ari, N., Thomos, N., & Musavian, L. (2022). Performance Analysis of Short Packet Communications With Multiple Eavesdroppers. *IEEE Transactions on Communications*, *70*(10), 6778–6789. https://doi.org/10.1109/TCOMM.2022.3198111

Balanis, C. A. (1997). *[ENG_C.A.Balanis]_Antenna.Theory.Analysis.and.Design_2ed_(Wiley_1997).pdf*.

Barnela, M. (2014). Digital Modulation Schemes Employed in Wireless Communication: A Literature review. *International Journal of Wired and Wireless Communications*, *2*(2), 15–21. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.676.7402&rep=rep1&type=pdf

Chen, R., Li, C., Yan, S., Malaney, R., & Yuan, J. (2019). Physical layer security for ultra-reliable and low-latency communications. *IEEE Wireless Communications*, *26*(5), 6–11. https://doi.org/10.1109/MWC.001.1900051

Chen, X., Ng, D. W. K., Gerstacker, W. H., & Chen, H. H. (2017). A Survey on Multiple-Antenna Techniques for Physical Layer Security. *IEEE Communications Surveys and Tutorials*, *19*(2), 1027–1053. https://doi.org/10.1109/COMST.2016.2633387

Childress, J. R. (n.d.). *Physical Layer Security for Mimo Wireless Systems*.

https://digitalcommons.latech.edu/theses

Chou, T. H., Draper, S. C., & Sayeed, A. M. (2013). Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage. *IEEE Journal on Selected Areas in Communications*, *31*(9), 1751–1764. https://doi.org/10.1109/JSAC.2013.130909

Cover, T. M., & Thomas, J. A. (2005). Elements of Information Theory. In *Elements of Information Theory*. https://doi.org/10.1002/047174882X

Csiszár, I., & Körner, J. (1978). Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, *24*(3), 339–348. https://doi.org/10.1109/TIT.1978.1055892

Das, S. M., Kumar, P. U., & Engineering, C. (2013). A Verilog Design in FPGA Implementation Of Quadrature Phase Shift Keying (QPSK) Digital Modulator. *International Journal of Engineering Science & Technology*, *2*(7), 1–6.

Deccio, C. T. (2004). *Network-layer Selective Security*.

Dilloway, C. (2008). On the Speci cation and Analysis of Secure Transport Layers. *Computing*.

Engli, W. F. (2020). *Factors Determining Cyber Strategy: the Differences Between Active and Passive Cyber Attacks*. 113.

Gershman, A., Sidiropoulos, N., Shahbazpanahi, S., Bengtsson, M., & Ottersten, B. (2010). From receive to transmit and network designs]. *IEEE Signal Processing Magazine*, *May*, 62–75.

Gesbert, D., & Akhtar, J. (2002). Breaking the barriers of Shannon's capacity: An overview of MIMO wireless systems. *Signal Processing*, 1–9. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.18.3414&rep=rep1&type=pdf

Golam Sadeque, M. (2015). Bit Error Rate (BER) Comparison of AWGN Channels for Different Type's Digital Modulation Using MATLAB Simulink. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS) ISSN (Print)*,

13(1), 61–71. http://asrjetsjournal.org/

Gong, C., Yue, X., Zhang, Z., Wang, X., & Dai, X. (2021). Enhancing Physical Layer Security with Artificial Noise in Large-Scale NOMA Networks. *IEEE Transactions on Vehicular Technology*, *70*(3), 2349–2361. https://doi.org/10.1109/TVT.2021.3057661

Hong, S., Pan, C., Ren, H., Wang, K., & Nallanathan, A. (2020). Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface. *IEEE Transactions on Communications*, *68*(12), 7851–7866. https://doi.org/10.1109/TCOMM.2020.3024621

Hu, J., Yan, S., Zhou, X., Shu, F., Li, J., & Wang, J. (2018). Covert communication achieved by a greedy relay in wireless networks. *IEEE Transactions on Wireless Communications*, *17*(7), 4766–4779. https://doi.org/10.1109/TWC.2018.2831217

Jankiraman, M. (2016). *Space-Time Codes and MIMO Systems*.

JC, M. (1954). *1891 - Maxwell A Treatise On Electricity and Magnetism Volume 2.pdf*.

Jennifer, J. (n.d.). *downloaded from Explore Bristol Research , Physical Layer Security for Next Generation Wireless Systems*.

Jin, Y., Hu, Z., Xie, D., Wu, G., & Zhou, L. (2021). Physical layer security transmission scheme based on artificial noise in cooperative SWIPT NOMA system. *Eurasip Journal on Wireless Communications and Networking*, *2021*(1). https://doi.org/10.1186/s13638-021-02020-3

Khisti, A., & Wornell, G. W. (2010). Secure transmission with multiple antennas-part II: The MIMOME wiretap channel. *IEEE Transactions on Information Theory*, *56*(11), 5515–5532. https://doi.org/10.1109/TIT.2010.2068852

Krontiris, A. P. (2018). *Evaluation of Certificate Enrollment over Application Layer Security*.

Krumbein, A. (2016). Understanding the Basics of MIMO Communication Technology Introduction to MIMO. *Rfmw.Com*.

Lemayian, J. P., & Hamamreh, J. M. (2021). Hybrid MIMO: A New Transmission Method

For Simultaneously Achieving Spatial Multiplexing and Diversity Gains in MIMO Systems. *RS Open Journal on Innovative Communication Technologies*, *2*(4). https://doi.org/10.46470/03d8ffbd.549d270b

Leung-Yan-Cheong, S. K., & Hellman, M. E. (1978). The Gaussian Wire-Tap Channel. *IEEE Transactions on Information Theory*, *24*(4), 451–456. https://doi.org/10.1109/TIT.1978.1055917

Li, C., Wang, J., Cheng, Y., & Huang, Y. (2016). Low-complexity soft-decision aided detectors for coded spatial modulation MIMO systems. *Eurasip Journal on Wireless Communications and Networking*, *2016*(1), 1–11. https://doi.org/10.1186/s13638-015-0509-9

Makin, M., Arzykulov, S., Celik, A., Eltawil, A. M., & Nauryzbayev, G. (2022). Enhancing Physical Layer Security in Large Intelligent Surface-aided Cooperative Networks. *IEEE Vehicular Technology Conference*, *2022-June*. https://doi.org/10.1109/VTC2022-Spring54318.2022.9860850

Mishra, B. K., Singh, S. K., Sharma, M., & Sharma, U. (2012). *Enhancing quality of service using OFDM technique for next generation network* . *2*, 286–292.

Mudumbai, R., Brown, D. R., Madhow, U., & Poor, H. V. (2009). Distributed Transmit Beamforming : Raghuraman Mudumbai , University of California at Santa Barbara. *IEEE Communications Magazine*, *February*, 102–110.

Narula, A., Lopez, M. J., Trott, M. D., & Wornell, G. W. (1998). Efficient use of side information in multiple-antenna data transmission over fading channels. *IEEE Journal on Selected Areas in Communications*, *16*(8), 1423–1436. https://doi.org/10.1109/49.730451

Negi, R., & Goel, S. (2005). Secret communication using artificial noise. *IEEE Vehicular Technology Conference*, *3*, 1906–1910. https://doi.org/10.1109/VETECF.2005.1558439

Okeke, R. O., & Asianuba, I. B. (2019). *Performance Evaluation of WiMAX Physical Layer Using Matlab Simulink American Journal of Engineering Research (AJER)*. *6*, 34–43.

OSI Security Architecture - Detailed Explanation - InterviewBit. (n.d.). Retrieved May 24,

2023, from https://www.interviewbit.com/blog/osi-security-architecture/

OSI Security Layers and Their Significance. (n.d.). Retrieved May 24, 2023, from https://www.w3schools.in/cyber-security/osi-security-layers-and-their-significance

Panayirci, E., Yesilkaya, A., Cogalan, T., Poor, H. V., & Haas, H. (2020). Physical-Layer Security with Optical Generalized Space Shift Keying. *IEEE Transactions on Communications*, *68*(5), 3042–3056. https://doi.org/10.1109/TCOMM.2020.2969867

Parrón, J., Cabrera-Hernandez, E., & Tennant, A. (2021). Accurate and efficient evaluation of bit error rate for dynamic directional modulation for standard modulation schemes. *Electronics (Switzerland)*, *10*(7), 1–14. https://doi.org/10.3390/electronics10070776

Persson, D., Lau, B. K., & Larsson, E. G. (2012). Scaling Up MIMO. *IEEE Signal Processing Magazine, january 2013*, 40–60.

Pham, T. V., Hranilovic, S., & Ishihara, S. (2023). *Design of Artificial Noise for Physical Layer Security in Visible Light Systems With Clipping*. *m*, 1054–1059. https://doi.org/10.1109/ccnc51644.2023.10060251

Report, A. P., Technology, M. O. F., & Technology, I. (2016). *APPLICATION LAYER SECURITY IN DATA PLANE OF SDN* (Issue December).

ROHIT U. NABAR, A. J. P. F. I. D. A. G. (2015). An Overview of MIMO Communications—A Key to Gigabit Wireless AROGYASWAMI. *IEEE Transactions on Vehicular Technology*, *63*(1), 2115–2126. http://dx.doi.org/10.1016/j.compeleceng.2015.01.011%0Ahttp://dx.doi.org/10.1016/j.neucom.2015.08.083%0Ahttp://dx.doi.org/10.1016/j.dcan.2015.09.001

Ryland, K. S., Clancy, T. C., Buehrer, R. M., & Dietrich, C. B. (2017). *Software-Defined Radio Implementation of Two Physical Layer Security Techniques*. https://vtechworks.lib.vt.edu/bitstream/handle/10919/82055/Ryland_KS_T_2018.pdf?sequence=1

Shi, W., Jiang, X., Hu, J., Abdelgader, A. M. S., Teng, Y., Wang, Y., He, H., Dong, R., Shu, F., & Wang, J. (2022). Physical layer security techniques for data transmission for future

wireless networks. *Security and Safety*, *1*, 2022007. https://doi.org/10.1051/SANDS/2022007

Siddique, N., Ali, M., & Zubair, M. (2015). *Data link layer security problems and solutions*. 56. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A783188&dswid=-202

Simoneau, P. (2006). The OSI Model : Understanding the Seven Layers of Computer Networks. *Global Knowledge E-Series*, *4*(3), 1–11.

Subramanian, A., Suresh, A. T., Raj, S., Thangaraj, A., Bloch, M., & McLaughlin, S. (2010). Strong and weak secrecy in wiretap channels. *6th International Symposium on Turbo Codes and Iterative Information Processing, ISTC 2010*, 30–34. https://doi.org/10.1109/ISTC.2010.5613867

Taware, R. (2013). *BER Performance Analysis of SSB-QPSK over AWGN and Rayleigh Channel*. 21–25.

Vadlamani, N. S. (2013). A Survey on Detection and Defense of Application Layer DDoS Attacks. *University of Nevada, Las Vegas*, 1800–1805.

van der Merwe, T. (2018). *An Analysis of the Transport Layer Security Protocol*. 225. http://www.isg.rhul.ac.uk/~kp/theses/TvdMthesis.pdf

Wang, D., Bai, B., Zhao, W., & Han, Z. (2019). A Survey of Optimization Approaches for Wireless Physical Layer Security. *IEEE Communications Surveys and Tutorials*, *21*(2), 1878–1911. https://doi.org/10.1109/COMST.2018.2883144

Wrulich, M. (2008). Capacity Analysis of MIMO Systems. *Nttuwienacat*, 112. http://www.nt.tuwien.ac.at/fileadmin/users/mwrulich/capacity_analysis.pdf

Wu, Y., Zhou, F., Li, Z., Zhang, S., Chu, Z., & Gerstacker, W. H. (2018). Green Communication and Networking. In *Wireless Communications and Mobile Computing* (Vol. 2018). https://doi.org/10.1155/2018/1921353

Wyner, A. D. (1975). The Wire-Tap Channel. In *Bell System Technical Journal* (Vol. 54, Issue 8, pp. 1355–1387). https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

Xiong, F. (2016). *Digital Modulation Techniques*.

Yener, A., & Ulukus, S. (2015). Wireless Physical-Layer Security: Lessons Learned from Information Theory. *Proceedings of the IEEE*, *103*(10), 1814–1825. https://doi.org/10.1109/JPROC.2015.2459592

Zeng, Y., Tang, Y., & Xiang, L. (2022). Physical Layer Security Design for Polar Code Construction. *Cryptography*, *6*(3). https://doi.org/10.3390/cryptography6030035

Zhou, S., & Giannakis, G. B. (2004). *How Accurate Channel Prediction Needs to be for Transmit-Beamforming With Adaptive Modulation Over Rayleigh MIMO Channels ? 3*(4), 1285–1294.

Research Fund Acknowledgement

This research project is funded by Adama Science and Technology University under the grant number ASTU/SM-R/737/23, Adama, Ethiopia.