PHYSICAL LAYER SECURITY USING ARTIFICIAL NOISE

AKINDOYIN Olaposi Akinbiyi

Submitted in accordance with the requirements for the degree of

Master of Science (Eng.)

In

Broadband Wireless and Optical Communications

The University of Leeds

School of Electronic and Electrical Engineering

August 2012

The candidate confirms that the work submitted is his/her own and that appropriate credit has been given where reference has been made to the work of others.
Acknowledgment

I am truly indebted and thankful to my scholarship sponsor “National Information Technology Development Agency (NITDA), Nigeria” for giving me the rare privilege to study at the University of Leeds.

I am sincerely and heartily grateful to my supervisor Dr. Des McLernon for his valuable support, patience and guidance throughout the course of this dissertation. I am sure it would not have been possible without his help.

I would like to express my deep gratitude to Romero-Zurita Nabil for his enthusiastic encouragement, useful critique, recommendation and providing me with great information resources.

I also acknowledge my colleague Frempong Kwadwo for his invaluable suggestions and discussion.

Finally, I would like to appreciate my parents for their support and encouragement throughout my study at Leeds.

Above all, special thanks to God Almighty for the gift of life.
DEDICATION

This thesis is dedicated to family especially;

to my parents for inculcating the importance of hardwork and higher education
to Omobolanle for being a caring and loving sister.
to Abimbola for believing in me.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>i</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>ii</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>iii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>vi</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>viii</td>
</tr>
<tr>
<td>LIST OF ACRONYMS</td>
<td>ix</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>xi</td>
</tr>
<tr>
<td>THE WIRELESS CHANNEL</td>
<td>1</td>
</tr>
<tr>
<td>1.0 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Fading</td>
<td>2</td>
</tr>
<tr>
<td>1.1.1 Large Scale Fading</td>
<td>2</td>
</tr>
<tr>
<td>1.1.2 Small Scale Fading</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Doppler Shift</td>
<td>3</td>
</tr>
<tr>
<td>1.3 Dispersive Characteristics of the Channel</td>
<td>4</td>
</tr>
<tr>
<td>1.3.1 Doppler Spread and Coherence Time</td>
<td>5</td>
</tr>
<tr>
<td>1.3.2 Delay Spread and Coherence Bandwidth</td>
<td>5</td>
</tr>
<tr>
<td>1.3.2 Flat Fading</td>
<td>6</td>
</tr>
<tr>
<td>1.3.3 Frequency Selective Fading</td>
<td>6</td>
</tr>
<tr>
<td>1.3.4 Fast Fading</td>
<td>7</td>
</tr>
<tr>
<td>1.3.5 Slow Fading</td>
<td>7</td>
</tr>
<tr>
<td>1.4 Statistical Channel Model</td>
<td>7</td>
</tr>
<tr>
<td>1.4.1 Rayleigh Fading Distribution</td>
<td>7</td>
</tr>
<tr>
<td>1.4.2 Rician Fading Distribution</td>
<td>8</td>
</tr>
<tr>
<td>1.5 Fading Mitigation</td>
<td>8</td>
</tr>
<tr>
<td>1.6 Mitigating Frequency Selective Distortion</td>
<td>9</td>
</tr>
<tr>
<td>1.7 Orthogonal Frequency Division Multiplexing (OFDM)</td>
<td>9</td>
</tr>
<tr>
<td>OVERVIEW OF PHYSICAL LAYER SECURITY</td>
<td>10</td>
</tr>
<tr>
<td>2.1 Problem Description</td>
<td>10</td>
</tr>
<tr>
<td>2.2 Motivation for Physical Layer Security</td>
<td>10</td>
</tr>
<tr>
<td>2.3 Cryptographic Techniques</td>
<td>11</td>
</tr>
</tbody>
</table>
3.5.2 Discussion of Figure 3.15 ................................................................. 46
3.5.3 Discussion of Figure 3.16 ................................................................. 47
3.5.4 Discussion of Figure 3.17 and 3.18 .................................................. 48
3.5.5 Discussion of Figure 3.19 ................................................................. 49

PHYSICAL LAYER SECURITY OF MIMO-OFDM SYSTEMS ..................... 50

4.1 System and Signal Model...................................................................... 51
4.2 Beamforming and Artificial Noise generation ....................................... 52
4.3 Maximal Ratio Combining (MRC) at Bob ......................................... 52
4.4 Minimum Mean Square Error (MMSE) at Eve ................................... 53
4.5 Zero Forcing (ZF) at Eve .................................................................... 53
4.6 Power Allocation Strategy ................................................................. 54
4.7 Simulation Results ............................................................................. 55

CONCLUSION AND FUTURE WORK ....................................................... 60

REFERENCES ...................................................................................... 62

APPENDIX II ....................................................................................... 68
APPENDIX III ..................................................................................... 70
APPENDIX IV ...................................................................................... 71
APPENDIX V ...................................................................................... 73
APPENDIX VI ...................................................................................... 75
LIST OF FIGURES

Figure 1.1  Multipath Propagation .................................................................................. 2
Figure 1.2  Small Scale Fading ..................................................................................... 4
Figure 1.3  Intersymbol Interference (ISI) .................................................................... 4
Figure 2.1  Symmetric Data Encryption/Decryption Algorithm ...................................... 11
Figure 2.2  Symmetric Cryptography .......................................................................... 12
Figure 2.3  Asymmetric Cryptography ......................................................................... 12
Figure 2.4  Eavesdropping in Wireless Network ........................................................... 16
Figure 2.5  Encryption .................................................................................................. 17
Figure 2.6  Wiretap Model ............................................................................................ 23
Figure 2.7  Beamforming Strategy ................................................................................ 26
Figure 3.1  System Model ............................................................................................. 29
Figure 3.2  The Graph of Average SNR of Bob and Eve Against Noise Power .............. 31
Figure 3.3  The Graph of Average SNR Against Number of Transmit Antennas .......... 32
Figure 3.4  The Graph of Average SNR Against Noise Power Adding AN .................. 34
Figure 3.5  The Graph of Average SNR Against Number of Antennas Adding AN ....... 34
Figure 3.6  Graph of Average SNR Against Ratio of Power Allocated for Information ... 35
Figure 3.7  Graph of Achieved Secrecy Rate Against Ratio of Power Allocated for ... 36
Figure 3.8  Graph of Probability of Secrecy Against the Ratio of Power Allocated for ... 36
Figure 3.9  Graph of Achieved Secrecy Rate Against Power Available at Transmitter ... 38
Figure 3.10  Graph of Probability of Secrecy Against Power Available at Transmitter ... 39
Figure 3.11  Graph of Probability of Secrecy Against Power Available at Transmitter ... 40
Figure 3.12  Graph of Probability of Secrecy Against Fraction of Power Allocated for ... 40
Figure 3.13  Graph of Probability of Secrecy Against Achieved Secrecy Rate ............... 41
Figure 3.14  Graph of Achieved Probability of Secrecy Against Target Probability of ... 44
Figure 3.15  Graph of Achieved Probability of Secrecy Against Target Probability of ... 45
Figure 3.16  Graph of Achieved Probability of Secrecy Against Target Probability of ... 46
Figure 3.17  Graph of Normalized Secrecy Throughput Against the Maximum Power ... 47
Figure 3.18  Graph of Normalized Secrecy Throughput Against the Maximum Power Available at the Transmitter for Three Non-Colluding Eavesdroppers ........................................... 48

Figure 3.19  Graph of Average Power Distribution Between Artificial Noise and ................................................. 49

Figure 4.1  System Model for OFMD-MIMO Frequency Selective System with ‘k’ corresponding Flat Fading Channel for the kth subcarrier .................................................................. 50

Figure 4.2  Graph of Average SNR at Bob and Eve Against Target SNR at Bob when ........... 55

Figure 4.3  Graph of Average SNR at Bob and Eve Against Target SNR at Bob for Different Antennas at Eve, Ne = 2, 5 and 10 when Nt = Nt = 5, N = 16, and L = 4 ....................................... 57

Figure 4.4  Graph of Average SNR at Bob and Eve Against Target SNR at Bob for Different Antennas at Eve, Ne = 2, 5, 10 and 50 when Nt = Nt = 5, N = 16, and L = 4 ..................... 57

Figure 4.5  Graph of Average SNR at Bob Against the Fraction of Power Allocated for AN Generation when Nt = Ne = 5 and L = 4 ........................................................................ 58

Figure 4.6  Graph of Average SNR at Bob Against the Fraction of Power Allocated for AN when Ne = 3, 5, 8 and L = 4 for N = 16 ........................................................................... 59
### LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Comparing Physical Layer Security and Cryptography</td>
<td>14</td>
</tr>
<tr>
<td>1.2</td>
<td>Security Attacks in Wireless Network</td>
<td>14</td>
</tr>
</tbody>
</table>
## LIST OF ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACDM</td>
<td>Algebraic Channel Decomposition Multiplexing</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption System</td>
</tr>
<tr>
<td>AES-CDMA</td>
<td>Advanced Encryption Standard Code Division Multiple Access</td>
</tr>
<tr>
<td>AN</td>
<td>Artificial Noise</td>
</tr>
<tr>
<td>AOA</td>
<td>Angle of Arrival</td>
</tr>
<tr>
<td>AWGN</td>
<td>Additive White Gaussian Noise</td>
</tr>
<tr>
<td>BCC</td>
<td>Broadcast Channel</td>
</tr>
<tr>
<td>CCMP</td>
<td>Counter Cipher Mode with Block Chaining Message Authentication Code Protocol</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CSI</td>
<td>Channel State Information</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread</td>
</tr>
<tr>
<td>DFT</td>
<td>Discrete Fourier Transform</td>
</tr>
<tr>
<td>DSP</td>
<td>Digital Signal Processing</td>
</tr>
<tr>
<td>DS-CDMA</td>
<td>Direct Sequence Code Division Multiple Access</td>
</tr>
<tr>
<td>DMC</td>
<td>Discrete Memoryless Channel</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DOA</td>
<td>Direction of Arrival</td>
</tr>
<tr>
<td>EM</td>
<td>Electromagnetic</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>Extensible Authentication Protocol Tunnelled Transport Layer Security</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>Extensible Authentication Protocol Flexible Authentication via Secure Tunnelling</td>
</tr>
<tr>
<td>ESPIRIT</td>
<td>Estimation of Signal Parameters via Rotation Invariance Technique</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>FFT</td>
<td>Fast Fourier Transform</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>ISI</td>
<td>Intersymbol Interference</td>
</tr>
<tr>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol</td>
</tr>
<tr>
<td>LPI</td>
<td>Low Probability Intercept</td>
</tr>
<tr>
<td>LPD</td>
<td>Low Probability Detection</td>
</tr>
<tr>
<td>LOS</td>
<td>Line of Sight</td>
</tr>
<tr>
<td>LPF</td>
<td>Low Pass Filter</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
</tbody>
</table>

ix
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLSE</td>
<td>Maximum-Likelihood Sequence Estimation</td>
</tr>
<tr>
<td>MLE</td>
<td>Maximum Likelihood Estimator</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
</tr>
<tr>
<td>MISO</td>
<td>Multiple Input Single Output</td>
</tr>
<tr>
<td>MRC</td>
<td>Maximum Ratio Combining</td>
</tr>
<tr>
<td>MMSE</td>
<td>Minimum Mean Square Error</td>
</tr>
<tr>
<td>MUSIC</td>
<td>Multiple Signal Classification</td>
</tr>
<tr>
<td>NLOS</td>
<td>Non Line of Sight</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Density Function</td>
</tr>
<tr>
<td>PKC</td>
<td>Public Key Cryptography</td>
</tr>
<tr>
<td>PN</td>
<td>Pseudo Noise</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RSA</td>
<td>Ron Rivest, Adi Shamir and Leonard Adleman</td>
</tr>
<tr>
<td>SIMO</td>
<td>Single Input Multiple Output</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal to Noise Ratio</td>
</tr>
<tr>
<td>SVD</td>
<td>Singular Value Decomposition</td>
</tr>
<tr>
<td>SKC</td>
<td>Symmetric Key Cryptography</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>ZF</td>
<td>Zero Forcing</td>
</tr>
</tbody>
</table>
ABSTRACT

The open nature of the wireless network has raised issues of confidentiality and security of transmitted information as the wireless network continues to expand. Therefore, the need to provide a secure communication link in the presence of adversaries (eavesdroppers and jammers) cannot be over emphasized. Conventionally, the cryptographic protocols currently in use are allocated at the application layer. However, this method is associated with the problem of key management and distribution coupled with its computational complexities and cost. This research work investigates the possibility of improving the security of the system without the use of cryptographic algorithms or engaging the user. This form of secure communication is achieved on the physical layer.

This project focuses on physical layer security of MISO and OFDM-MIMO systems in the presence of passive eavesdroppers, i.e. the transmitter is unaware of the eavesdropper’s presence. The transmit strategy adopted for secure communication is artificial noise generation and spatial beamforming. This thesis investigates the possibility of ensuring a target probability of secrecy by defining a quality of service constraints at the legitimate receiver in a MISO system and then proposes an optimum power allocation scheme between the information signal and the artificial noise generated at the transmitter.

Further, this project explores the ability of the eavesdropper to make vulnerable the security of the system by extenuating the effect of the artificial noise using zero forcing as the receive beamforming strategy in OFDM-MIMO system. Results from MATLAB simulations are presented and discussed in detail.
CHAPTER ONE
THE WIRELESS CHANNEL

1.0 Introduction

One of the most important shortcomings on the performance of a communication system is the loss in signal strength (attenuation) as a result of signal transmission from the transmitter to receiver [1]. Communication can occur either through a wired or wireless channel. In wired channels, signal is transmitted via a guided media while a wireless channel uses electromagnetic waves (EM) for signal transmission [1,2]. The path the signal travels from the transmitter to the receiver can be line-of-sight (LOS) or Non-line-of-sight (NLOS) [1,2,3]. For LOS transmission, the signal loss may not be critical. However, NLOS occurs in urban environment where indirect paths are established between the transmitter and receiver. These indirect routes are as a result of scattering, diffraction, refraction and reflection from large structures, buildings, and other obstacles in the propagation path [1].

Scattering takes place when the EM waves propagate in all directions. It occurs due to propagation through a channel containing large number of objects (including vegetation, street signs, etc) that has dimension smaller than the wavelength of the EM wave [4,5]. While diffraction leads to the bending of wave as it propagates through a medium containing objects with sharp irregularities [1]. Reflection occurs due to the propagation of an EM wave through a channel containing objects with physical dimensions much larger than the wavelength of the EM wave. However, depending on the impedance on the wall and the incidence angle, refraction may also occur [1]. In mobile communication systems, these NLOS conditions describe the signal transmission from the transmitter to receiver. Therefore, the free space propagation models are inappropriate to determine the loss in signal strength (attenuation) suffered by the signal. Numerous models have been proposed to calculate the loss in signal strength as it travels to the receiver [2]. These propagation models have conventionally focused on calculating the variation of signal strength at adjacent spatial nearness to a specific position and the average strength of the signal received at a certain distance from the transmitter [2,5].

As a result of scattering, diffraction, reflection and refraction, the transmitted signal travels over multiple paths from transmitter to receiver; this is referred to as multipath propagation. Different copies of the transmitted signals arrive at the receiver out of phase from various directions with diverse propagation delays [4]. At the receiver, constructive and destructive interference of multiple copies of the transmitted signal leads to variation in the signal’s angle of arrival, phase and amplitude of the received signal [1,2,4]. This phenomenon is referred to as multipath fading.
1.1 Fading

Attenuation or loss in signal strength is not the only characteristics of signal transmitted via a wireless channel. The variability of signal strength with time and distance must also be taking into consideration. This fluctuation describes the term fading [1]. Therefore, fading describes the variability in the received signal as it propagates to the receiving antenna [2,5]. Fading can be explained in terms of period of fading (large scale or small scale) [1], statistical distribution of the received envelope (Lognormal, Rayleigh and Rician), main cause (multipath or Doppler) or slow and fast fading [1,2].

1.1.1 Large Scale Fading

This occurs as a result of path loss due to motion over large area and denotes the average loss in strength of the signal power [4]. Therefore, the statistics of large scale fading presents a method of calculating an approximation of path loss as a function of distance as well as shadowing by big objects [1,3]. Large scale fading is characteristically independent of frequency and occurs when the distance covered by a mobile is of the order of the cell size [3]. Therefore, large scale fading can be considered as a spatial average over the small-scale variations of the signal [4]. Mean path loss and lognormal distribution are used to describe large scale fading [1,4].

Figure 1.1 Multipath Propagation[6]
1.1.2 Small Scale Fading

This occurs as a result of fast variations of the phases, amplitudes or multipath delays of a radio signal over a brief period of time or distance [2]. Small scale fading is as a result of the constructive and destructive interference of several signal paths between receiver and transmitter [3,4]. Signals from different paths arriving at the receiver with different delays add up constructively or destructively producing a rapid change in the resulting received signal strength [4]. When either the transmitter or receiver move over a small distance, the received signal strength changes faster over a short duration. These fast variations in the received signal strength are termed small scale fading [1]. Small scale fading is frequency dependent and noticeable in two ways – time-variant behaviour of the channel and time-spreading of the signal (signal dispersion) [4]. Small scale fading is referred to as Rayleigh fading when there are huge numbers of multiple reflective paths and the line-of-sight signal component is zero [4]. Thus the envelope of such received signal is described by a Rayleigh pdf. However, when the line-of-sight signal component is dominant, the envelope of such received signal is described using Rician pdf [1,4].

1.2 Doppler Shift

In a typical mobile communication system, the transmitter and receiver are in relative motion. As a result of this relative motion, each of the multipath signal experiences an evident shift in frequency [Rapport]. The resulting fluctuation in the frequency of the received signal is termed Doppler shift. The maximum Doppler shift $f_d$ is expressed as:

$$f_d = f_0 \frac{v}{c} \quad 1.1$$

$$f_d = \frac{1}{2\pi} \frac{\Delta \phi}{\Delta t} = \frac{v}{\lambda} \cdot \cos \theta \quad 1.2$$

where $c$ is the free space velocity of the electromagnetic wave, $v$ is the speed of the mobile unit, $f_0$ is the transmit frequency, $\theta$ is the angle the received signal makes with source, $\Delta \phi$ is the change in phase of the received signal as a result of the difference in path length. Doppler shift therefore depends on; the relative motion between the transmitter and receiver, the angle between the direction of motion and direction in which the signal arrives.
1.3 Dispersive Characteristics of the Channel

The variation of the received signal power is not just the impact of fading. The shape of the transmitted signal may also be affected during transmission via the wireless channel [1]. The transmitted signal propagates through different paths to arrive at the receiver. Due to the different paths taken, copies of these signals arrive at different times. However, if these pulses are not resolvable at receiver, the impact of the multiple paths is to generate a broadened or overlapping pulses. Therefore, the broadening of transmitted pulse as a result of multipath causes intersymbol interference (ISI) [1].

Figure 1.2 Small Scale Fading [7].

Figure 1.3 Intersymbol Interference (ISI) [8]
1.3.1 Doppler Spread and Coherence Time

A critical parameter of the channel is the time-scale of the fluctuation of the channel [3]. The relative motion of the transmitter and receiver or even nearby objects causes the channel to fluctuate with time [1,4]. Therefore, the time dispersive characteristics of the wireless channel in a small-scale area are described by delay spread and coherence time [2]. Doppler spread ($B_D$) defines a range of frequencies such that the Doppler spectrum received is basically non-zero. Further, $B_D$ explains the frequency dispersive characteristics of the channel. Signals that arrives at the receiver experiences Doppler shift due to the relative motion between transmitter and receiver. Most often than not, this cause the bandwidth of the received signal to be larger than the transmitted signal. The amount of broadening of the Doppler spectrum is determined by Doppler spread [2].

Coherence time ($T_C$) is essentially a statistical evaluation of the duration of time over which the impulse response of the channel is basically unchanging and also measures the relationship of the response of the channel at different times [2]. The time domain dual of $B_D$ is $T_C$. Therefore, in the time domain, $T_C$ describes the time changing characteristics of the frequency dispersive nature of the channel [1,2]. $B_D$ is inversely proportional to $T_C$ and the relationship is given by:

$$T_C = \frac{1}{4B_D} \quad 1.3$$

1.3.2 Delay Spread and Coherence Bandwidth

Delay spread ($\sigma_d$) is a multipath channel parameter that defines the difference in the transmission time between the longest and the shortest paths while taking into consideration only paths with considerable energy [3]. Depending on the nature of refraction, reflection, scattering and diffraction, transmitted signals from multiple paths arrive at the receiver with different times and varying amount of power. Therefore, the impulse response of the channel is defined by the received delay copies of the multipath signals with varying powers [1]. In rural area where there are limited large structures, the impulses are expected to take shorter time to reach the receiver since the paths are close to each other. However, in an urban area, the received impulses will broaden more since there will be more diverse multiple paths [1]. Thus, a channel with high delay spread will create more time dispersion in the signal received. The delay spread can be expressed mathematically as:

$$\sigma_d = \sqrt{\langle \tau^2 \rangle - \langle \tau \rangle^2} \quad 1.4$$
where $\tau$ is the average delay experienced by the pulse as it propagates through the channel.

$$\tau = \frac{\sum_{i=1}^{N} p_i \tau_i}{\sum_{i=1}^{N} p_i}$$

And $\tau^2$ is the mean square delay given by:

$$\tau^2 = \frac{\sum_{i=1}^{N} p_i \tau_i^2}{\sum_{i=1}^{N} p_i}$$

The coherence bandwidth ($B_c$) defines the statistical measure of the range of frequencies over which the signal is transmitted without distortion. (i.e. all spectral component with almost equal line phase and gain travels through the channel). The channel can therefore be considered flat. Therefore, if two frequency components have robust amplitude correlation, the coherence bandwidth defines the range of frequencies where there is strong correlation. Considering the level of correlation of these two frequency components, the coherence bandwidth can be mathematically expressed in two ways [2]. For 0.9 and above correlation between the frequency components, the coherence bandwidth is expressed as $B_c = \frac{1}{50\sigma_d}$ whereas for 0.5 and above correlation, $B_c = \frac{1}{5\sigma_d}$

### 1.3.2 Flat Fading

Flat fading occurs when all the frequency components in the transmitted signal arrive at the receiver with little or no distortion and insignificant ISI [1]. Therefore, in flat fading, the bandwidth of the channel ($B_c$) is larger than the bandwidth of the transmitted signal ($B_s$) i.e. $B_c > B_s$. Further, in flat fading channels, the multipath delay spread is less than the symbol time i.e. $\sigma_d < T_s$. Therefore, the spectral characteristics of the transmitted signal are conserved at the receiver but the signal strength varies with time as a result of the variation in channel gain caused by multipath [2,9].

### 1.3.3 Frequency Selective Fading

In a frequency selective fading channel, the linear phase response and the constant gain over a bandwidth is less than the bandwidth of the transmitted signal [2]. In other words, the bandwidth of the transmitted signal is larger than the bandwidth of the channel i.e. $B_s > B_c$. Therefore, the various frequency components in the transmitted signal experience ISI as a result of the broadening of the pulse [1,9]. Further, in a frequency selective channel, the multipath delay
spread is greater than the symbol duration i.e. $\sigma_d > T_s$. Frequency selective fading is as a result of time dispersion of the symbols transmitted in the channel. Therefore, some frequency components in the spectrum of the received signal have higher gains than others [2].

1.3.4 Fast Fading

In a fast fading channel, the impulse response of the channel fluctuates more quickly within the symbol time [2]. Therefore, fast fading occurs if the coherence time of the channel is less than the symbol time of transmitted signal i.e. $T_c < T_s$ [1,2]. As a result of Doppler spread, fast fading causes frequency dispersion which causes signal distortion. Thus, a signal experience fast fading if the bandwidth of the signal is less than the Doppler spread i.e. $B_s < B_D$ [2].

1.3.5 Slow Fading

In a slow fading channel, the rate at which the impulse response of a channel changes is slower than the transmitted signal. Therefore, slow fading occurs if the coherence time of the channel is greater than the symbol time of transmitted signal i.e. $T_c > T_s$ [2,4]. Further, a signal will experience slow fading if the bandwidth of the signal is less than the Doppler spread i.e. $B_s > B_D$ [2]. It should be noted that whether a signal experience fast or slow fading depends on the velocity of the mobile or object in the channel.

1.4 Statistical Channel Model

In the previous sections, Doppler spread and multipath spread was defined as quantities connected to a given receiver at a time, velocity and location. Nevertheless, we are concerned about the statistical description of the number of multipath, how fast they vary and how much they fluctuate. These statistical models depend on probability density function (pdf) to express the fluctuation of the amplitude of the received signal [3].

1.4.1 Rayleigh Fading Distribution

The statistical time fluctuation of the received signal strength of a flat fading signal or the envelope of the different multipath components can be described using Rayleigh distribution [2]. The Rayleigh fading presumes that all multipath components are equal and are large enough to assume that no direct line-of-sight exist between the transmitter and receiver [1]. The envelope of the received r.f. signal $(R)$ is a Rayleigh random variable with probability density function (pdf) given by;
\[ P_R(r) = \begin{cases} \frac{r}{\sigma_R^2} \exp \left[ -\frac{r^2}{2\sigma_R^2} \right] , & 0 \leq r \leq \infty \\ 0 , & r < 0 \end{cases} \]  \hfill (1.7)

where \( \sigma_R^2 \) is the average power of the received signal and \( \sigma_R \) is the root mean square (rms) of the received voltage signal [9].

### 1.4.2 Rician Fading Distribution

Rician distribution takes into consideration the line-of-sight (LOS) component which adds a deterministic component to the multipath signal [1]. Therefore, the random received signals are superimposed on fixed main path known as the line-of-sight (LOS) [Rapport]. The pdf of the Rician distribution is given by:

\[ p(r) = \begin{cases} \frac{r}{\sigma^2} \exp \left[ -\frac{(r^2 + A^2)}{2\sigma^2} \right] I_0 \left( \frac{Ar}{\sigma^2} \right) , & r \geq 0, A \geq 0 \\ 0 , & r < 0 \end{cases} \]  \hfill (1.8)

Conventionally, the impact of the randomly located scattering points is referred to as diffuse component while steady component refers to the LOS component. Therefore, the pdf of Rician distribution can also be described as the ratio of the power of the steady component to the power of the diffuse components;

\[ K(\text{dB}) = 10 \log \left[ \frac{A^2}{2\sigma^2} \right] \]  \hfill (1.9)

### 1.5 Fading Mitigation

As mentioned in the previous sections, the impact of Rayleigh fading suffered by signal due to multipath effect is the random variation in the signal power of the received signal. Further, lognormal fading or shadowing also adds to this variation. Therefore, any methods to mitigate fading should take into account the short and long term characteristics of fading [4,5]. Diversity technique is one of the approaches employed to combat fading. This technique employs a number of receiving antenna rather than a single antenna. Diversity enhances the performance of the system at relatively low cost [4]. The concept of diversity technique entails using N different antennas at the receiver to receive the same signal in such a way that the antennas receive independent copies of the transmitted signal. By so doing, N different versions of the received signal will be produced. Thus, these N copies of the received signal can then be combined [1,10].
The N channels created will be identically Rayleigh distributed. It follows that since there are N independent channels, the possibility that all the N channel fade severely is very small. Different diversity techniques include; space, angle, time, multipath, frequency and polarization diversity. While forms of diversity combing techniques are; selection combining, maximum ratio combining and equal gain combining.

1.6 Mitigating Frequency Selective Distortion
The effect of channel induced ISI as result of frequency selective fading can be mitigated by equalization [4]. This method of equalization entails gathering the dispersed symbols energy back into its initial time interval. In fact, an inverse filter of the channel is an equalizer. The main objective of the equalizer filter is to give a linear phase and flat composite received frequency response. Equalizer filters are designed to adapt to the time varying channel characteristics of a mobile system [4,5]. In addition to ISI mitigation, adaptive equalizer filter also provide diversity. Other methods of mitigating ISI include; direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), pilot signal, maximum-likelihood sequence estimation (MLSE) equalizer, orthogonal frequency division multiplexing (OFDM), etc.

1.7 Orthogonal Frequency Division Multiplexing (OFDM)
OFDM can be viewed as either a modulation scheme or a multiplexing technique. It is a unique case of multicarrier transmission in which a single data stream is transmitted over several lower-rate subcarriers [11]. In conventional multicarrier system, high quality (thus expensive) low pass filters (LPF) are essential to preserve the orthogonality of the subcarriers at the receiver. In addition, N independent RF chains are needed. However, OFDM overcomes these limitations. OFDM is majorly used to increase robustness against narrow band interference and frequency selective fading [10]. OFDM is a digital orthogonal multicarrier modulation technique that utilizes Discrete Fourier Transform (DFT) for efficient and effective modulator and demodulator implementation. Thus, only one RF chain is required [10]. The OFDM technique is based on block transmission with guard interval and is prevalent today because it makes use of low cost digital signal processing (DSP) components that can efficiently compute the Fast Fourier Transform (FFT) [10, 11].
CHAPTER TWO

OVERVIEW OF PHYSICAL LAYER SECURITY

Wireless networks are extensively utilized in military and civil applications to accumulate real time and event driven data. Thus, it has become a crucial part of our everyday life. Wireless applications depend on the wireless network for effective transmission of vital and confidential information. However, the broadcast feature of the wireless network makes it inherently unsecured. Therefore, the need to provide a secure communication link in the presence of adversaries cannot be over emphasized. Theses adversaries may attempt to gain illegal access to and amend the information or even interrupt the flow of the information [12].

2.1 Problem Description

One of the growing concerns in wireless communication is the security of transmitted signal. Due to the open nature of the wireless network, it is intrinsically insecure [13]. The simplicity of gaining access to wireless medium makes it easy to eavesdrop communication over this medium [14]. Although encryption can be used to guarantee privacy, its computational complexities and cost could be exorbitant coupled with the problems and susceptibilities related with key distribution and management [13]. Therefore, there is a need to leverage on the unique features of the wireless medium to address these security challenges. This field of study is called physical layer security.

2.2 Motivation for Physical Layer Security

The motivations behind physical layer security are;

1. To take advantage of the physical layer of the wireless channel to improve the security of communication.

2. To provide an alternative that improves the security of the system that is presently based on cryptographic algorithms.

3. To implement security solutions to vulnerabilities (majorly Jamming and eavesdropping) in wireless network.

4. To achieve a more reliable and robust system by supplementing existing security measures.
2.3 **Cryptographic Techniques**

Generally, security methods depend on the cryptographic techniques to provide authentication, privacy/confidentiality, integrity and non-repudiation [15]. In cryptography, the sender or transmitter is named Alice while the legitimate or intended receiver is called Bob. Eve is the eavesdropper that attempt to overhear the communication between Alice and Bob. In order to prevent Eve from obtaining knowledge about the content of the message, Alice executes a sequence of mathematical operations on the original message, pre-set by the encryption key and cryptographic algorithm [16]. When the message gets to Bob, it is easily decrypted since Bob is aware of the algorithm and encryption key. However, even if Eve is aware of the algorithm, it would be difficult for her to decipher the message since she doesn’t have the key [16].

![Figure 2.1 Symmetric Data Encryption/Decryption Algorithm](image)

Cryptographic algorithms can be classified based on the number of keys used for decryption and encryption. Three types of cryptography algorithms can be identified; Harsh function, secret key (or symmetric) cryptography (SKC), public key (or asymmetric) cryptography (PKC). In secret key cryptography, a single key is used for both encryption and decryption while in asymmetric cryptography; different keys are utilized for encryption and decryption. However, harsh function employs mathematical transformation to irretrievably encrypt the information [15].

Data Encryption Standard (DES) is the most common secret key cryptography deployed today. DES is a 56 bit key that runs on a 64 bit block using a block cipher algorithm. To use DES, a common secure key must be shared by the two users [12]. However, if the key appears unavailable to any of these users, an additional channel will be required to facilitate key exchange. In place of using additional channel, physical layer methods can be used to provide location privacy, allocate private key and to augment higher layer security algorithms [12].
The conventional cryptographic method of symmetric cryptography involves duplicate keys at Alice and Bob [16]. The challenge is to transmit the key from Alice to Bob (or vice versa) in a protected and secret channel before the actual communication. To overcome this challenge, Hellman and Diffie in 1976 invented public-key cryptography. The key exchange protocol was implemented by Hellman and Diffie but the foremost real cryptographic algorithm was RSA invented by Ronald L. Rivest, Adi Shamir, and Leonard Adleman [16].

Physical layer security is a promising area of research that investigates opportunity of realizing perfect secret communication among intended nodes while perhaps malicious nodes obtain no information [17]. This is achieved by exploiting the characteristics of the wireless channel such as noise and fading to improve the secrecy of the channel [17]. Although these features have been
conventionally viewed as impairment, physical layer security makes use of these features to enhance the secrecy of the wireless channel.

2.4 Security Challenges in Wireless Network

Security is vital in wireless communication systems particularly in a multiuser wireless network where secure connection is becoming more challenging in a highly mobile and distributed environment. The next generation wireless communication networks will be distributed and ad-hoc to allow different types of mobile devices to connect and disconnect [17]. However, this will make the entire system more susceptible and at risk of attack [18]. Attacks in wireless networks can be grouped into passive (example traffic analysis and eavesdropping) and active (denial of service, replay attack, information disclosure, message modification, etc) [19]. While the aim of a passive attackers is to steal transmitted wireless information, the active attacker, habitually tries to modify the network data and could cause major disruption to normal network operation [12].

Conventionally, encryption techniques depend heavily on upper layer operation (layers above the physical layer) and utilize cryptographic protocols (AES and RSA) to provide error free link by assuming the physical layer is well-known [20]. However, in a distributed and ad-hoc networks, upper layer techniques are difficult to implement. All cryptographic algorithms are allocated to the application layer; it is therefore in the user’s hand to guarantee the secrecy of his data [16]. Invariably, in a complex environment, cryptographic methods might not work efficiently [17]. Therefore, there is a need to take advantage of the features of the wireless channel for instance noise or fading to provide a reliable and secure wireless transmission [17]. The physical layer presents the possibility of improving the security of the transmitted information without requiring cryptographic algorithms and involving the user [16]. The table 1.0 below compares physical layer security and cryptography.

2.5 Security Attacks in Wireless Network

Communications via wireless medium are vulnerable to different form of attacks as a result of the nature of deployment [21]. Generally, attacks in wireless network can be broadly categorized into two: active and passive [19]. While a passive attacker do not upset the operation of a network and the major aim of the adversary is to pilfer the information transmitted from the network, an active attacker largely disrupt the usual operation of the network by attempting to modify the network data. The table 2.0 below summarizes the different attacks in wireless network.
### Table 1.1 Comparing Physical Layer Security and Cryptography

<table>
<thead>
<tr>
<th>Physical Layer Security</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There is an accurate account about the disclosed information to the eavesdropper based on the channel’s quality.</td>
<td>The technology is not widely available and few systems are deployed.</td>
</tr>
<tr>
<td></td>
<td>Theoretically, it is possible to get close to perfect secrecy</td>
<td>A short secret key is still needed for authentication</td>
</tr>
<tr>
<td></td>
<td>There is no computational restrictions on eavesdropper</td>
<td>In the case of pure passive eavesdropping, there is only possible to have a probability of secrecy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cryptography</th>
<th>System is widely developed and available</th>
<th>It requires a secure key interchange by reliable third party supported by complex protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication can be achieved based on public keys</td>
<td>It is a complex system and thus require high computational costs</td>
</tr>
<tr>
<td></td>
<td>It is secure enough for most applications</td>
<td>System is not 100% secure, and it considers computational limitations on eavesdropper</td>
</tr>
<tr>
<td></td>
<td>Compatibility to any information. If the key is secure, the message is secure.</td>
<td>There is no precise metrics to measure the reliability and security of the system</td>
</tr>
</tbody>
</table>

### Table 1.2 Security Attacks in Wireless Network

<table>
<thead>
<tr>
<th>Security Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Attacks</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Traffic Analysis</td>
</tr>
<tr>
<td>Eavesdropping</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
2.5.1 Denial of Service Attack (DoS)

In DoS attack, the intruder tries to use up the resources which are accessible to the intended users [12]. Therefore, DoS inhibits the usual utilization or running of communications services [19]. DoS attack may be directed to a certain target; for instance, an attacker may restrain all messages meant for a specific user. On the other hand, a DoS attack could interrupt the whole network either by rendering the entire network inoperative or by congesting the network with messages in such a way that it degrades the performance of the network [19]. At the physical layer, jamming is extensively used to initiate DoS attack. In radio frequency transmission, radio frequency jamming can be utilized to attack the transmission signal band [12].

2.5.2 Masquerade Attack

This form of active attack involves an impostor pretending to be the intended user and attempts to delude the authentication system in order to seize the resources of the system. For instance, if the authentication order is jeopardized, the intruder can therefore acquire right to retrieve information illegitimately [12].

2.5.3 Message Modification and Information Disclosure

Message modification simply suggests that some segment of the lawful message is modified, belated or rearranged in order to create illegal effect [19]. However, in information disclosure, a node which has been compromised can intentionally disclose restricted and classified information to an illegal node. For instance, in military applications, information such as varying traffic patterns and traffic periodicity between certain pair of nodes can be invaluable to intruders [12].

2.5.4 Eavesdropping and Traffic Analysis

Eavesdropping involves an intruder surreptitiously listening to an ongoing communication between intended nodes to obtain information on the connection [21]. Therefore, eavesdropping is a method of attack for an authorized receiver to capture a confidential and classified message during communication [12]. However, to prevent eavedroppers, one of the well known technique to conceal confidential message is encryption. Conversely, traffic analysis is ingenious. The operation of traffic analysis is such that even if encryption was deployed, an intruder could still be able to monitor the message pattern [19]. Thus, the intruder could ascertain the position and identities of the communicating nodes [12,19] and also monitor the frequency and message segment being exchanged [19]. The information extracted by the intruder might be invaluable in speculating the nature of communication between the nodes.
Passive attacks are extremely complicated to perceive due to the fact that it doesn’t require modification of data [19]. In general, communication occurs in an evidently usual way and the communicating nodes are oblivious that an intruder has read the message or monitored the pattern of the traffic

![Eavesdropping in Wireless Network](image)

**Figure 2.4 Eavesdropping in Wireless Network**

### 2.6 Authentication and Encryption

Often when there is communication between two nodes over a wireless network, the major security objective is to provide authentication and privacy. Authentication process in most access points occurs at the Media Access Control (MAC) layer. Therefore access points provides authentication only on the hardware such that only devices with known MAC addresses are allowed to connect to the network. This method is susceptible for some reasons. One of the vulnerabilities is that some devices allow a change of MAC address. Therefore, an authenticated user can duplicate its MAC address for another user to connect to the network. Indeed, there are convincing facts that one should for no reason provide encryption without authentication [22].

Over the years, different solutions for encryption and authentication have been proposed. However, the most common form of encryption that exists now is wired equivalent privacy (WEP). The main purpose of WEP is to offer data privacy to the level of wired network as defined by IEEE 802.11 for the encapsulation of data frames [23].

WEP encapsulation has failed to meet its design objectives. This has been broadly attributed to the 40-bit RC4 used by WEP for its encryption mechanism. However, it has been proven that even if the encryption mechanism uses 104 or 128-bit RC4 keys, it is unrealistic to achieve privacy by just increasing the key size [24]. Therefore, WEP is insecure regardless of the size of the key. This flaw is as a result of WEP usage of small initialization vector [23]. This
susceptibility limits its ability to provide significant data privacy at any key size [24]. An alternative to WEP is the Virtual Private Network (VPN) which provides a much more secure encryption.

2.7 Physical Layer Security Methods

Physical layer security against different forms of attacks can be broadly categorized into five. These are; signal detection method, theoretical secure capacity, channel, power and coding.

2.7.1 Signal Detection Method

Motivated by the research carried out by Chang et al. in [25], a training-based channel estimation approach was proposed. This method allows the QoS unfairness between the intended receiver and intruder in the wireless network [25]. The authors proposed a multi-stage training based estimation approach so as to reduce the normalized mean squared error of channel estimate at the intended receiver subject to the restriction on the estimation performance of the intruder [12]. However, the main idea is to taking advantage of the channel feedback from the intended receiver at the start of each stage by adding artificial to the left null space of the intended receiver’s channel so as to demean the eavesdropper’s estimation performance [25]. The use of artificial noise restricts the quality of channel estimation achieved by the eavesdropper, whereas the channel estimation at the intended receiver can be improved after each stage [12].

2.7.2 Theoretical Secure Capacity

Currently, there has been growing concern on the subject of secure channel capacity in the information theory field [26,27]. Most research work has centred on improving the secrecy capacity of a system. The secrecy capacity is the maximum data rate realizable between the
intended transmitter-receiver pair with the restriction on the information achievable by the illegitimate receiver [26]. Wyner in [28] demonstrated that for a discrete memoryless channel, the difference between the capacities of the transmitter and intended receiver defines the perfect secrecy capacity. Gopala et al. [29] in also obtained a related result when extended to Gaussian channels.

Bloch et al. in [20] investigated the full CSI scenario where the channel gains of the intended receiver and the eavesdropper is available at the transmitter. Under the full CSI condition, the secrecy capacity is taken as the upper bound for the secrecy capacity when partial CSI (i.e. transmitter only have the CSI of the intended receiver) condition is considered [20]. Furthermore in [20], a low-complexity on/off power distribution scheme which attains the best performance only with the primary channel’s CSI was proposed. At high average SNR, the strategy was proven to be asymptotically optimal and can achieve the secrecy capacity of full CSI notion.

Based on the availability of the channel CSI at the transmitter, [20,29,30] has proven that channel fading has a positive effect on the rate adaptation and secrecy capacity of a system. The authors in [30] characterized the vital role of fading in terms of outage probability and average secrecy rate. The information-theoretic formulation of the problem was based on an imperfect CSI such that the transmitter and intended receiver communicate over a quasi-static fading channel and the eavesdropper overhears the communication over an autonomous quasi-static fading channel. To guarantee information theoretic security, the authors designed a secure communication protocol. It was then established that even in the existence of imperfect CSI, the protocol was efficient for secure key regeneration [30].

Hero in [31] pioneered the study of the use of multiple antenna in wireless communication research. The major idea in this paper was that taking advantage of space-time diversity at the transmitter can also improve the security of information [31]. Li et al. [32] in investigated single-input multiple-output (SIMO) wiretap channel. Using typical methods in communication theory, the secrecy capacity of a SIMO channel plus coloured Gaussian noise was described by converting the channel into a scalar Gaussian wiretap channel [32]. These findings can be extended to consider the effect of slow fading on the secrecy capacity of the channel and also investigate how multiple antennas at the receiver could enhance operation of communication system. In conclusion, a system may not be able to assure a security with probability of one but can be developed and regulated to a certain level of security. Moreover, the information about the channel is required which may not be perfect [12]. However, a small number of systems that uses
quantum key distribution exist, although the technology is not extensively accessible as a result of the cost of implementation.

### 2.7.3 Code Approach

The major aim of this approach is to enhance the resistance against eavesdropping and jamming. This approach consists of the use of spread spectrum coding and error correction coding.

1. Spread Spectrum Coding – This is a signalling method wherein a signal is distributed by a pseudo-noise (PN) sequence over a broad frequency band. This is an efficient way of implementing physical layer security. Spread spectrum method is well known to achieve low probability of detection (LPD) and low probability of intercept (LPI) [12]. Li et al. in [33] investigated the use of direct sequence spread spectrum (DSSS) to spread transmitted data over several frequencies. However, in frequency-hopping spread spectrum (FHSS), the frequency of the carrier is periodically modified multiple times per bit period in line with arbitrarily selected channel. This will make it tremendously difficult if not impossible to illegitimately observe the spread spectrum signal. When compared to traditional cryptography technique, the spread spectrum has a small key size due to the fact that the key space is restricted by the number of various sequences and array of carrier frequencies. However, conventional cryptographic techniques can have an extremely large key size [12].

In direct sequence code division multiple access (DS-CDMA), the same channel is divided among all users using diverse spreading codes to differentiate their signals. Initially, the transmitted signal is spread using a code sequence and in addition, to foil the detection of the signal by eavesdroppers, the spread signal is encoded using PN sequence. Hence, using moderately long PN encoding sequence is critical to physical layer security of CDMA system. Noubir in [34] proposed a technique to improve the physical layer security of CDMA using advanced encryption standard (AES) process to produce the encoding sequence. AES-CDMA technique can augment the level of security to protect the system from exhaustive-key-search attacks since AES stipulates three key sizes (256,192 and 128) [12]. However, this area of research is extensively open to both physical layer security and security/information theory experts.

2. Error Correction Coding - In traditional cryptographic technique, if there is one error in the encrypted text received, it causes a huge number of errors in the plaintext decrypted after channel decoding. However, to deal with this issue, Hwang et al. in [35] presented a technique
that combines AES and turbo coding. This method utilizes the M encoded turbo codes selected from N bits using pseudo-random number generation algorithm to establish a protected communication session [12]. The major merits of secure turbo codes include; better efficiency, lower decoder/encoder size, encryption and decryption are performed at high speed.

2.7.4 Power Approach

The security of data can be enhanced using different power methods. The common schemes involve the addition of artificially generated noise and the use of directional antennas.

1. Directional Antennas - The use of directional antennas enhance frequency reuse and increase geographical coverage due to the fact that the beam width of directional antenna is inversely proportional to the peak gain [1]. Goel and Negi in [14] examined the use of omnidirectional antennas and directional antennas when the network is subjected to different jamming situations. The authors observed that if an omnidirectional antennae is deployed, a host in the within the reach of the jammer won’t be able to obtain the data effectively. On the other hand, the use of directional antennae will ensure that nodes outside the coverage area of the jammer will still be able to obtain the transmitted data. Hence, the use of directional antennas can enhance the capacity of a wireless a network, improve the availability of data, and prevent jammers [12]. However, as the angular resolution of the antenna array improves the size of directional antenna increases. This factor limit it use and solution to this issue is yet to be found.

2. Artificial Noise Approach – Goel and Negi in [36] proposed a technique that guarantees a perfectly secure communication between legitimate nodes. The authors established that perfect secrecy is realizable when the channel of the illegitimate receiver is noisier than the channel of the legitimate receiver. The artificial noise (AN) generated is added into the null-subspace of the legitimate receiver’s channel [14,36,37]. The main idea behind this approach is to use the artificial noise to mar the channel of the illegitimate receiver while the channel of the legitimate receiver remains unaffected. Furthermore, the authors established that perfect secrecy can still be realized even though the channel of the illegitimate receiver is better than the legitimate receiver [36]. This project exploits the use of AN to achieve secrecy.

2.7.5 Channel Approach

By taking advantage of the characteristics of the channel, three techniques have been put forward. These are; randomization of MIMO transmission coefficients, algebraic channel decomposition multiplexing (ACDM) precoding, and radio frequency (RF) fingerprinting
1. Randomization of MIMO Transmission Coefficients - Li and Ratazzi in [38] presented that by randomizing the coefficients of MIMO transmission, a secure communication can be achieved. Based on the impulse response matrix of the main channel, a diagonal matrix is generated at the transmitter. The distinctive characteristics of this diagonal matrix make it imperceptible to the illegitimate receiver but clearly evident to the legitimate receiver [38]. Although this approach decreases the ability of the illegitimate receiver to intercept signal, it causes blind deconvolution issue as a result of the redundancy of MIMO transmissions [38].

2. Algebraic Channel Decomposition Multiplexing (ACDM) precoding – Sperandio and Flikkema in [39] pioneered the ACDM precoding approach. In their paper, the description of the channel between the transmitter and legitimate receiver was depicted by transmission code vectors. These code vectors were produced by the singular value decomposition (SVD) of the correlation matrix. With the aim of achieving communication with high data rate over dispersive multipath channel, symbol blocks were used to transmit the message and subsequently modulated by a complex code vector with unit energy [12]. However, even if the illegitimate user have perfect information about the transmission code vectors and channel responses, secret communication can still be achieve due to the variation in the locations of the intended user and illegitimate user [12].

3. RF Fingerprinting - This approach was proposed by Tomko et. al in [40]. The authors presented a technique that detects wireless local area network (WLAN) intrusion. The method was based on employing several sensor systems to obtain and extract the physical layer RF characteristics from each received signal [40]. A dynamic fingerprint for individual internal source identifier (for instance MAC address) was generated from the processed RF features by an intrusion detector [40]. The sequential development of each fingerprint is observed and whenever any inconsistencies are detected in several components of the fingerprint, intrusion warnings are issued. The author demonstrated the practicality of the system using data obtained from a set IEEE 802.11b transceiver. However, the proposed system does not operate in real time. It stores and post-process digitalized packets [40]. But to realize real-time physical layer intrusion detection and combine it with the traditional intrusion detection system (IDS), further research works are required.

2.8 Wiretap Channel and Secrecy Capacity
Wyner in 1975 pioneered the wiretap channels to model secret systems [28]. In the typical wiretap model, Alice attempts to communicate with Bob via a main channel while Eve overhears
this communication through a wiretap channel. Wyner in [28] was able to establish the possibility of an almost perfect secure link between Alice and Bob without depending on private or secret keys. Wyner was able to show that perfect secrecy is achievable if the eavesdropper’s channel is a degraded version of the Bob’s channel. In contrast to the cryptography approach to secrecy which presumes that the eavesdropper is unable to resolve some computational problems, Wyner approach ensures the secrecy of transmitted message at the physical layer without making any assumption about the eavesdropper’s competence. This forms the theoretical foundation for information theoretic approach which builds on the Shannon’s concept of perfect secrecy. However, to describe the perfect secrecy capacity of a discrete memoryless channel (DMC), Csiszar and Korner in [41] simplified Wyner’s methodology by considering the transmission of secret messages over a broadcast channel where all forms of messages can be transmitted. It was established that positive perfect secrecy capacity is achievable when the main channel is less noisy than the eavesdropper’s channel (wiretap channel). However in practice, positive secrecy capacity is not always obtainable. Csiszar and Korner were able to establish that there are channel codes that ensure both a certain level of data secrecy and sturdiness to transmission errors. It was shown in [26] that if both Alice and the Eavesdropper’s channel are additive white Gaussian noise (AWGN) channel and the main channel has higher capacity than the wiretap channel, the secrecy capacity can then be expressed as the difference between these capacities. The secrecy capacity was defined in [30] as the maximum transmission rate at which the eavesdropper is unable to decode any information. Thus, secret communication is not possible except the Gaussian Alice-to-Bob channel has a better signal to noise ratio (SNR) than the Gaussian Alice-to-Eavesdropper’s channel. Figure 2.3 show a wiretap model and the secrecy capacity of the system can be expressed as:

$$C_S(P) = C_M - C_W = \left[ \log_2 \left( 1 + \frac{|h_M|^2 P}{\sigma^2} \right) - \log_2 \left( 1 + \frac{|h_W|^2 P}{\sigma^2} \right) \right]^+$$

where, $[ \cdot ]^+$ implies that only positive values are considered.

Barros and Rodriguez in [30] considered a broader view of the challenges of securing transmission over a wireless channel by examining the effect of quasi-static fading on the secrecy capacity. The authors defined secrecy capacity in terms of the outage probability and offer a comprehensive characterization of the highest rate of transmission at which the eavesdropper is not able to decode the information. Result in [30] shows that under fading condition, information
theoretic security is realizable even when the average SNR of the eavesdropper is larger than that of the primary channel.

![Wiretap Model](image)

**Figure 2.6 Wiretap Model**

Current research work on information theoretic security by Maurer in [42] revealed that even when Alice-to-Bob channel is worse than the Alice-to-Eve channel; it is viable to generate a secret key via public communication over an unprotected channel. Space-time signal processing methods to secure the wireless network was introduced in [31]. The secrecy capacity of different degraded slow fading channels was determined in [43]. The authors studied the secrecy capacity of a Single Input Multiple Output (SIMO) channel under Gaussian noise. In their study, standard communication theory methods were used to convert the SIMO channel into a scalar Gaussian wiretap channel which invariably represents an extension of Wyner’s model. The authors concluded that under slow fading condition, employing multiple antennas at the receiver offers an advantage over a single antenna channel. However, with the scenario considered, the authors were not able to establish that antenna diversity improves secrecy. In [27,44,45] the authors explored the contribution of multiple antennas to provide secrecy. Khristi and Wornel in [44] investigated the secrecy capacity of a Gaussian wiretap channel when there are multiple antennas at the Alice, Bob and Eve. The authors proposed a quantifiable description of the secrecy capacity as a saddle point solution to a minimax problem. Further, to achieve secrecy at high SNR, it was shown that by concurrently diagonalizing the channel matrices through Singular Value Decomposition (SVD), and separately coding across the subsequent parallel channels, the related capacity can be expressed in terms of the generalized singular values [27]. In conclusion, the author provided the required and adequate condition for zero secrecy capacity. The condition
requires that Eve needs three times as many antennas as Alice and Bob mutually have and that the best ratio of antennas at Alice to that at Bob should be 2:1 to prevent secure communication.

In [29,46], the ergodic secrecy capacity, optimal power and rate allocation strategies to achieve a secure communication over slow fading channel was proposed. Gopala et al in [29] investigated the secrecy capacity of a slow fading channel in the presence of eavesdropper considering different notions on the availability of CSI at the transmitter. The result of this work concludes that fading can actually be exploited to improve the secrecy capacity of the system. This corroborates the result from [30] but in contrast with the conventional AWGN scenario described in [26]. Further, the authors proposed a low-complexity on/off power transmission strategy and also verified that the best asymptotic performance occurs when the SNR approaches infinity [29]. It was further established that at high SNR levels, the presence of the eavesdropper CSI at the transmitter does not provide extra gain in the secrecy capacity for slow fading channel [29]. However, the CSI of the primary channel is important since the nonexistence of this information makes the system more vulnerable when the eavesdropper is more capable than the intended receiver [29]. Liang et al. in [46] investigated the fading broadcast channel with confidential messages (BCC). The authors established the secrecy capacity region of for the parallel Gaussian BCC as well as the best power allocation strategy for this region. The results obtained were further used to derive the ergodic secrecy capacity region for the fading BCC [46]. However, the outage performance of BCC was not presented in this paper.

Furthermore, to guarantee secrecy, the system information accessible at the transmitter plays an important role. In fact, it is possible to calculate the secrecy capacity if the channel state information of both the Alice-to-Bob and Alice-to-Eve links are accessible at Alice. However, in passive eavesdropping scenario which is the most common, the eavesdropper’s CSI is unknown at Alice. Therefore, secrecy capacity cannot be computed and invariably, we cannot guarantee perfect secrecy. To define secrecy capacity in a passive eavesdropping situation, Barros and Rodbrigues in [30] introduced the notion of outage probability of secrecy. The authors defined outage probability of secrecy as the probability that the secrecy capacity at a particular instant falls below a pre-specified target secrecy rate. An alternative method to define secrecy capacity in a passive eavesdropper situation was presented in [47] and [13]. In [47], secret communication is guaranteed using quality-of-service (QoS) viewpoint. The design formulation established a maximum allowable SNR at the eavesdropper while guaranteeing a minimum acceptable SNR at the intended receiver [47].
Beamforming as the best strategy to maximize the secrecy capacity of a MISO system in both fading and non-fading was presented in [48,49]. The authors established that beamforming achieves the largest secrecy rate and that the direction of beamforming depends on the CSI available at the transmitter [48]. Negi and Goel in [14,37] investigated how secrecy can be achieved by intelligently adding artificially generated noise to the signal conveying the information in such a way that the primary link remain unaffected while the eavesdropper’s channel degrades. The main idea in these papers was to transmit artificially generated noise over the null space of the legitimate receiver so as to confuse the eavesdropper and in turn, enhance the secrecy of the system [14,37].

Therefore, exploiting the use of beamforming and artificial noise generation as transmit strategy to ensure secrecy in a passive eavesdropper system, numerous research works has been proposed to distribute the available transmit power between artificial noise and information signal. However, the goal is to guarantee a given SNR to fulfil the QoS constraint or minimize the outage probability of secrecy as described in [30] and [13,47] respectively.

Zhou and Mckay in [50,51] proposed that for the case of non-colluding passive eavesdropper, equal power distribution between the information signal and artificial noise is an easy but near-optimal power allocation strategy. However, as the number of colluding eavesdroppers rises, additional power should be utilized to produce artificial noise [50]. Further in [50], the effect of imperfect CSI at both the transmitter and receiver was investigated. It was shown that generating more artificial noise to obscure the eavesdropper is more intelligent than to increase the strength of the signal for the legitimate receiver since the CSI is imperfect. Furthermore, the authors concluded that the when the CSI of the eavesdropper is not accessible at the transmitter, the lower bound secrecy capacity is maximized [50,51]. However, in [13], a fraction of the transmit power was used to broadcast the information signal to guarantee a specific SNR while the remaining power was used to generate artificial noise. Comparing the strategy in [13] to [47], the later extended the security constraint to also ensure a predefined SNR at the eavesdropper. Further in [47], the power allocation between the information signal and the noise was converted to a joint optimization problem which was resolved using convex optimization and semidefinite relaxation methods in order to establish the optimum artificial noise and beamformer spatial distribution.

In [52], a security constraint of maintaining a predefined SNR at the intended receiver was used to establish a robust beamforming strategy for multiple-input-multiple-output (MIMO) configuration as a technique to surmount the imperfect CSI at the transmitter.
2.9 Beamforming

This is a signal processing technique that can be used for directional signal transmission or reception. It is otherwise known as spatial filtering. Beamforming uses suitable digital or analogue signal processing methods to cause an array of antennas to be turned in such a way that will impede the reception of radio signal coming from a particular direction [53]. Beamforming uses multiple antenna elements to adapt strength of the received and transmitted signals based on their mathematical direction (eigenbeamforming) or physical direction (direction of arrival - DOA). The beamformer combines energy over its space in such a way that a specific antenna gain is achieved in a particular direction while attenuation occurs in other directions [53]. This convergence of energy is realized by selecting appropriate weights for each antenna elements with a specific criterion [54].

Figure 2.7 Beamforming Strategy

In DOA-based beamforming, each of the received signals is characterized in terms of its angle of arrival (AOA) of direction of arrival (DOA). Signal processing techniques such as multiple signal classification (MUSIC), maximum likelihood estimator (MLE), and estimation of signal parameters via rotation invariance technique (ESPRIT) algorithms can be used to estimate each of the DOAs. A beamformer is then used to extract a weighting vector for the antenna elements from the acquired DOAs. The beamformer uses these extracted weighting vectors to transmit or receive signal the desired signal of a particular user while the unwanted signal is suppressed. DOA-based beamformer is also known as null-steering beamformer [54]. A major drawback of
this approach is that antenna gain is not maximized in the direction of the intended user due to the presence of a null in the direction of the interferer. Eigenbeamforming presents a more feasible approach in a realistic broadband wireless environment. Rather than using the array-response vector from various users’ AOAs, eigenbeamforming take advantage of the channel-impulse response of each antenna element to obtain the array weight that fulfil a required condition (for instance, maximizing SNR or minimizing MSE). Therefore, if the CSI is known at the transmitter, eigenbeamforming can make use of eigendecomposed channel response to direct the transmit signal to the required user even in the presence of co-channel interfering signals with several AOAs [54]. Traditional beamformers utilize fixed array of phase-shifters (or time-delays) and weightings to merge the signals. However, adaptive beamformers combines the characteristics of the signal received by the array and the information about the location of the sensor in the array to enhance the rejection of undesired signals from other directions.
CHAPTER THREE

PHYSICAL LAYER SECURITY OF MISO SYSTEM

The advantages of using multiple antennas to ensure secure communication was investigated in [27,44,45]. This chapter work focuses on a MISO configuration. That is the transmitter has multiple antennas while the eavesdropper and intended receiver is assumed to have just one antenna. Secrecy in MISO system was studied in [55]. Further in [48], beamforming was proven to be an optimal transmit strategy to maximize the secrecy capacity in a MISO system. In the previous chapter, we have discussed the use of artificial noise as adopted in [14,37] as a transmission scheme to achieve secure communication. This research work therefore takes advantage of the positive contribution of artificial noise and beamforming to provide secure communication in a flat fading channel. However, chapter four will expand the scope of this project to investigate frequency selective fading channel. It is also assumed that the eavesdropper is passive. That is; the transmitter is unaware of the eavesdropper’s channels.

This research work investigates the optimum power allocation scheme between the artificial noise and transmitted information in a power constrained and unconstrained systems. Further, we study a QoS based secure communication scheme where a minimum SNR is enforced at Bob to guarantee a certain probability of secrecy and ensure probabilistically that the SNR at all the eavesdropper does not exceed a maximum permissible value. This chapter presents the system models and simulation results of these models are discussed.

The following notations is used throughout this write-up, vectors and matrices are represented using bold face lower and upper case letters respectively, $\mathbf{x}^H$ represent the conjugate transpose of the complex vector $\mathbf{x}$ while $||\mathbf{x}||$ denote the norm of the complex vector $\mathbf{x}$. $\text{Tr}(\mathbf{X})$ represents the trace of the square matrix $\mathbf{X}$ which is the sum of the diagonal elements of matrix $\mathbf{X}$.
3.1 System Model

The system model is as shown in figure 3.1 above. Let $\mathbf{x}$ represent the beamformed signal transmitted from Alice to Bob and nth Eves. The signal received at Bob and at Alice can be represented as;

$$y_b = \mathbf{h}_{ab}^H \mathbf{x} + n_b$$  \hspace{0.5cm} 3.1

$$y_{en} = \mathbf{h}_{en}^H \mathbf{x} + n_{en}$$  \hspace{0.5cm} 3.2

where $n_b$ is the zero mean complex Guassian noise term with variance $\sigma_b^2$ in Alice-to-Bob’s channel such that $\mathbb{E}(|n_b|^2) = \sigma_b^2$ and $n_{en}$ is the zero mean complex Guassian noise term with variance $\sigma_{en}^2$ in Alice-to-Eve’s channel such that $\mathbb{E}(|n_{en}|^2) = \sigma_{en}^2$.

Figure 3.1 System Model
The covariance matrix of $\mathbf{x}$ is expressed by $\mathbf{C}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$ and let $P_t = \text{Tr}\{\mathbf{C}_x\}$ denotes the total transmitted power such that; $P_t = c + d$. Where $c$ and $d$ represent the absolute power allocated for information and artificial noise respectively. Therefore, the signal vector $\mathbf{x}$ can be modelled as;

$$\mathbf{x} = \sqrt{c}\mathbf{w}\mathbf{s} + \sqrt{d}\mathbf{\eta}$$  \hspace{1cm} 3.3

where $\mathbf{\eta}$ is the $(N_t \times 1)$ artificial noise vector with a covariance matrix $\mathbf{C}_\eta = \mathbb{E}\{\mathbf{\eta}\mathbf{\eta}^H\}$ and $\text{Tr}\{\mathbf{C}_\eta\} = 1$. $\mathbf{w}$ is the normalized $(N_t \times 1)$ beamforming vector $||\mathbf{w}|| = 1$.

As previously stated in chapter two, the objective of artificial noise generation as adopted in [14, 37,55,56] is to obscure the eavesdropper by broadcasting artificially generated noise in all direction aside from Bob. Therefore as described in [56], Alice picks the beamforming vector $\mathbf{w}$ as the principal eigenvector $\mathbf{w}_1$ corresponding to the largest eigenvalue of $\mathbf{h}_{ab}\mathbf{h}_{ab}^H$. Further, the linear combination of the remaining $(N_t - 1)$ eigenvectors are employed to compute the artificial noise vector $\mathbf{\eta}$ such that $\mathbf{\eta}$ will lie in the nullspace of $\mathbf{h}_{ab}$. Thus, orthogonality between the beamformer $\mathbf{w}_1$ and the artificial noise $\mathbf{\eta}$ is conserved $\mathbf{w}_1^H\mathbf{\eta} = 0$. If we assume a uniform power distribution among the $N_t - 1$ remaining eigenvectors, we can obtain $\mathbf{\eta}$ as follow:

$$\mathbf{\eta} = \frac{1}{\sqrt{N_t - 1}} \sum_{i=2}^{N_t} \mathbf{w}_i \mathbf{\eta}_i$$  \hspace{1cm} 3.4

where $\mathbf{\eta}_i$ denotes a unit magnitude random complex scalar and $\mathbf{w}_i$ represents the $i$th eigenvector of $\mathbf{h}_{ab}\mathbf{h}_{ab}^H$. The covariance matrix of the artificial noise is thus expressed as;

$$\mathbf{C}_\eta = \frac{1}{N_t - 1} \sum_{i=2}^{N_t} \mathbf{w}_i\mathbf{w}_i^H$$  \hspace{1cm} 3.5

As derived in the Appendix I, the SNR received at Bob and Eve can be expressed as;

$$\text{SNR}_b = \frac{c||\mathbf{h}_{ab}||^2}{\sigma_{ab}^2}$$  \hspace{1cm} 3.6

$$\text{SNR}_e = \frac{c\mathbf{w}_1^H(\mathbf{h}_{en}\mathbf{h}_{en}^H)\mathbf{w}_1}{d\mathbf{h}_{en}^H\mathbf{C}_\eta\mathbf{h}_{en} + \sigma_{en}^2}$$  \hspace{1cm} 3.7
Using the equations above, the positive contribution of using beamforming without artificial noise was investigated then add artificial noise (AN) was later added to the system to further establish the impact of beamforming and artificial noise on the system performance.

### 3.2 Simulation I: Beamforming without Artificial Noise

The aim of this simulation is to investigate the impact of beamforming at the transmitter. From equation (3.3) above, since we are transmitting without artificial noise, we set $\eta = 0$. Therefore, the beamformed transmitted signal vector becomes;

$$x = \sqrt{c} w_s$$  \hspace{1cm} (3.8)

From the equations for SNR above, only the SNR of Eve has noise term in it. Therefore, with or without noise addition, the SNR of Bob remains unaffected. However, without artificially generated noise addition, $C_\eta = 0$ also assuming $c = 1$. Equation 3.7 simplifies to;

$$\text{SNR}_{e_n} = \frac{c w_1^H (h_{e_n} h_{e_n}^H) w_1}{\sigma_{e_n}^2}$$  \hspace{1cm} (3.9)

Using equations 3.6 and 3.9, the variation of the SNR of Bob and Eve with the number of transmit antennas and noise power was investigated. The main strategy is to choose the principal beamforming eigenvector $w_1$ corresponding to the largest eigenvalue of $h_{ab} h_{ab}^H$ to transmit toward Bob. The simulation results are presented in the next section.

![Graph of Average SNR of Bob and Eve Against the Noise Power](image)

**Figure 3.2** The Graph of Average SNR of Bob and Eve Against Noise Power
3.2.1 Discussion of Figure 3.2 and 3.3

By implementing $10^5$ iterations of Monte Carlo simulations in MATLAB, the results are as shown above. From figure 3.2, the separation of the SNR curve of Bob and that of Eve explains the secrecy capacity of the system. It can be observed the 6dB separation of the two curves is maintained. At low noise power, Bob achieves higher SNR but as the noise power increases, the SNR of Bob and Eve degrades but the distance between the two curves remains constant. Therefore, the system can guarantee a secrecy of 6dB by employing beamforming at the transmitter. Figure 3.3 shows the variation of average SNR of Bob and Eve as the number of antennas at Alice increases. It can be observed from the graph that the SNR of Eve remains constant at 0dB no matter the number of antennas employ at Alice. However, the SNR of Bob increase linearly as the number of antennas at Alice increases. This is expected since Alice is beamforming in the direction of Bob using the principal eigenvector corresponding to $h_{ab}h_{ab}^H$. Therefore, to achieve better secrecy, we employ more antennas at Bob. To further improve the performance of the system, we can either improve the SNR of Bob or degrade that of Eve. The next simulation investigates the addition of artificially generated noise to further degrade the SNR of Eve while the SNR of Bob remains unaffected.

3.3 Simulation II: Beamforming with Artificial Noise

The objective of this simulation is to investigate the effect of adding artificially generated noise on the secrecy of the system. It was assumed that Alice has perfect knowledge of Bob’s channel.
but not that of Eve. Therefore, the strategy is to transmit the artificial noise in the null space of Bob while the information signal in its space range. This ensures that Bob’s channel nulls out the artificial noise thereby making it unaffected by the noise generated. However, Eve’s channel degrades with probability due to the fact that the artificial noise lies in its range space. From the formulations above, we implement equations 3.6 and 3.7 in MATLAB with the assumptions that $c = d = 1$.

### 3.3.1 Discussion of Figure 3.4 and 3.5

By implementing $10^5$ iterations of Monte Carlo simulations in MATLAB, the results are as shown below. Figure 3.4 shows the variation of SNR with AWGN noise power in the presence of artificially generated noise. From the graph, the impact of adding of artificial noise can be observed. In presence of AN, the SNR of Eve worsens while that of Bob remains unchanged. The multiple antennas at Alice provide a degree of freedom that intelligently generates an artificial noise in order to degrade Eve’s channel while Bob’s channel is unaffected. This is because the artificial noise lies in the null space of Bob’s channel but in the range space of Eve. The secrecy of the system is thus enhanced since the SNR of Eve reduces. However, the price we pay for this is the extra power needed to generate the artificial noise. The next simulation considers this issue.

In figure 3.5, we further assume that $\sigma_n^2 = \sigma_0^2 = 1$ and then observe in the presence of noise, the impact of increasing the number of transmit antennas on the secrecy of the system. From the graph, it is evident that the SNR of Eve degrades further in the presence of artificially generated noise. A loss of 2.2dB in the SNR of Eve is observed. Therefore, the secrecy capacity of the system increases by 2.2dB.

### 3.4 Simulation III: Manual Allocating a Fraction of the Total Power for Information Signal

The objective of this simulation is to manually allocated the available transmit power between the artificial noise and information signal. This simulation can be studied in two different ways. Firstly, allocating a fraction of the available transmit power for information signal while the remaining is used to generate artificial noise and then examine the impact of this strategy on the secrecy capacity of the system. Secondly, by defining a ratio of the power allocated for AN to the power allocated for information signal (i.e. $d/c$). The first strategy will be considered in this project.
The Graph of Average SNR of Bob and Eve Against the Noise Power

Figure 3.4  The Graph of Average SNR Against Noise Power Adding AN

The Graph of Average SNR of Bob and Eve Against Number of Tx Antennas

Figure 3.5  The Graph of Average SNR Against Number of Antennas Adding AN
Let $\rho \in (0,1]$ be the fraction of the total power $P_t$ allocated for the information signal. Then,

$$c = \rho P_t$$ \hspace{1cm} 3.10

and

$$d = (1 - \rho) P_t$$ \hspace{1cm} 3.11

Substituting these into equations 3.6 and 3.7 gives,

$$\text{SNR}_b = \frac{\rho P_t \|h_{ab}\|^2}{\sigma_b^2}$$ \hspace{1cm} 3.12

$$\text{SNR}_{e_n} = \frac{\rho P_t w_{1}^H (h_{e_n} h_{e_n}^H) w_1}{(1 - \rho) P_t h_{e_n}^H c_{e_n} h_{e_n} + \sigma_{e_n}^2}$$ \hspace{1cm} 3.13

For a single eavesdropper, the secrecy rate of the system can be expressed as;

$$R_s = \log_2 (\text{SNR}_b + 1) - \log_2 \left(\text{SNR}_{e_1} + 1\right)$$ \hspace{1cm} 3.14

$$R_s = \left[ \log_2 \left(\frac{\rho P_t \|h_{ab}\|^2}{\sigma_b^2} + 1\right) - \log_2 \left(\frac{\rho P_t w_{1}^H (h_{e_1} h_{e_1}^H) w_1}{(1 - \rho) P_t h_{e_1}^H c_{e_1} h_{e_1} + \sigma_{e_1}^2} + 1\right) \right]^{+}$$ \hspace{1cm} 3.15

Further, under this formulation, the system is said to be secured if $R_s > 0$. The probability of secrecy can thus be defined as;

$$\text{Probability of Secrecy} = \frac{\text{Number of channel realization (when } R_s > 0\text{)}}{\text{Number of Channel Realization}}$$ \hspace{1cm} 3.16

![Graph of Average SNR Against Ratio of Power Allocated for Information Signal](image)

**Figure 3.6** Graph of Average SNR Against Ratio of Power Allocated for Information Signal ($\rho$).
Figure 3.7  Graph of Achieved Secrecy Rate Against Ratio of Power Allocated for Information Signal ($\rho$)

Figure 3.8  Graph of Probability of Secrecy Against the Ratio of Power Allocated for Information Signal ($\rho$).
By implementing $10^5$ iterations of Monte Carlo simulations in MATLAB, the results obtained are discussed below.

### 3.4.1 Discussion of Figure 3.6

Figure 3.6 shows the variation of the average SNR at Bob and Eve with the ratio of power allocated for information signal. At low fraction of power allocated for information ($\rho = 0.1$), the system uses more power to transmit artificial noise (AN) but little power is available for the information signal. The transmitted AN will degrade Eve’s channel but has no effect on Bob’s channel as explained previously. The implication of this as observed from the graph is that at low $\rho$, we achieve high secrecy rate but the SNR at Bob is very low. As $\rho$ increases, the SNR at Bob and Eve also increases. At high value of $\rho = 1$, all the power is used to transmit information signal and none to generate AN. This leads to a decrease in the secrecy rate of the system due to the fact that no power to transmit AN. However, it can be observed that at $\rho = 1$, secrecy was still achievable. This achieved secrecy is as a result of the beamforming strategy employed by Alice. It can therefore be concluded that there exist a trade-off between achieving high SNR and fraction of power allocated for AN generation.

### 3.4.2 Discussion of Figure 3.7

Figure 3.7 above shows the graph of achieved secrecy rate against ratio of power allocated for information ($\rho$) for different total transmit power. The aim of this graph is to investigate and establish the optimal power allocation between information signal and AN that achieves the best secrecy rate. As observed from the graph, as $\rho$ increases, the secrecy rate also increase but get to a maximum where it begins to drop. This maximum can be observed at $\rho = 0.5$. Therefore, the optimum power allocation between the information signal and AN is to divide the power equally between them. This result supports the findings of [51].

### 3.4.3 Discussion of Figure 3.8

Figure 3.8 above shows the graph of probability of secrecy against ratio of power allocated for information ($\rho$) for different total transmit power. As previously stated, under this formulation, we defined the probability of secrecy as the ratio of number of channel realizations when ($R_s > 0$) to the total number of channel realizations. At low value of $\rho$, we observed that the system achieves high probability of secrecy. This is due to the fact that at low $\rho$, more power is available to generate AN which will degrade the eavesdropper’s channel. Therefore, the
probability of achieving secrecy will be high. However, as $\rho$ increases, less power becomes available to degrade the eavesdropper’s channel. This will eventually reduce the probability of achieving secrecy. It can also be observed that when $\rho = 1$, i.e. no power was allocated for AN generation, the probability of secrecy was 0.9688. This achieved probability of secrecy is due to beamforming strategy employed at the transmitter rather than AN generation.

The next set of simulation results investigate how the available transmit power varies with the achieved secrecy rate and probability of secrecy. The simulation was performed for different fraction of power allocated for information signal ($\rho = 0.25, 0.5$ and 0.75).

![Graph of Achieved Secrecy Rate Against Power Available at Transmitter](image)

**Figure 3.9** Graph of Achieved Secrecy Rate Against Power Available at Transmitter

### 3.4.4 Discussion of Figure 3.9

Figure 3.9 shows the graph of the achieved probability of secrecy against the power available at the transmitter. The simulation was carried out for different values of $\rho = (0.25, 0.5, 0.75)$. It can be observed from the graph that at low power available at transmitter, $P_t < 6$, using 75% of $P_t$ for information signal achieves better secrecy rate than using 50% of $P_t$. However, when the total power available at the transmitter is $6 \leq P_t \leq 10$, using 75% of $P_t$ for information signal achieves the same secrecy rate as using 50% of $P_t$. Nonetheless, at $P_t > 10$, using 50% of $P_t$ for information signal achieves better secrecy rate than using 75% of $P_t$. This implies that at $P_t > 10$,
the optimal strategy to achieve better secrecy is to split the available power equally between the information signal and the noise. The result further support the simulation result presented in figure 3.7.

![Graph of Probability of Secrecy Against Power Available at Transmitter](image)

**Figure 3.10** Graph of Probability of Secrecy Against Power Available at Transmitter

### 3.4.5 Discussion of Figure 3.10

Figure 3.10 presents the graph of the probability of secrecy against total power available at the transmitter. Here, the probability of secrecy is defined as the ratio of the number of channel realization when $Rs > 0$ to the total number of channel realizations. The simulation was carried out for different values of $\rho = 0.25, 0.5, \text{ and } 0.75$. From the graph, it can be observed that at low power available at the transmitter ($P_t$), when 25% of $P_t$ is used for information signal i.e. $\rho = 0.25$, the system achieves better probability of secrecy. This is due to the fact that most of the power (75% of $P_t$) will be used to generate AN so as to degrade the eavesdropper’s channel. However, as $P_t$ increases, the probability of secrecy when 25% of $P_t$ is used for information signal approaches the same value as when 50% of $P_t$ is used.

By re-defining the probability of secrecy based on a QoS constraint as the ratio of the number of channel realization when $Rs \geq 4$ to the total number of channel realization, we can re-design the system such that a minimum secrecy rate of 4 is guaranteed. Figure 3.11 and 3.12 below
investigates the maximum probability of secrecy achievable and minimum power required to achieve the QoS constraint placed on the system.

Figure 3.11 Graph of Probability of Secrecy Against Power Available at Transmitter when Rs ≥ 4

Figure 3.12 Graph of Probability of Secrecy Against Fraction of Power Allocated for Information Signal when Rs ≥ 4
3.4.6 Discussion of Figure 3.11 and 3.12

Figure 3.11 shows how the probability of secrecy varies with the power available at the transmitter for different values of $\rho = 0.25, 0.5, 0.75$. It can be observed from the graph that to achieve a probability of secrecy of 0.1, a minimum power of 4 is required when $\rho = 0.75$, for $\rho = 0.5$, a minimum power of 5.8 is required while for $\rho = 0.25$, a minimum power of 9.8 is required. Therefore, as the fraction of power allocated for information signal decreases, more power is required at the transmitter to achieve a given probability of secrecy. However, from the graph, when $P_t \geq 10$, allocating 50% of available power for information signal achieves better probability of secrecy than allocating 75%. Thus, to achieve high probability of secrecy, allocating 50% of available power for information signal and 50% for AN generation is optimal. This result is in conformity with results from figure 3.7 and figure 3.10. Figure 3.12 shows the variation of the probability of secrecy with the fraction of power allocated for the information signal. It can be observed that when $P_t = 1$, the probability of secrecy remains at zero no matter the fraction of power allocated for information signal. This is due to the fact that when $P_t = 1$, the system does not meet the minimum power requirement to achieve the QoS secrecy constraint. However, when $P_t = 5$, at least 30% of the fraction of the available power must be allocated for information signal to achieve probability of secrecy greater than 0.

![Graph of Probability of Secrecy Against Secrecy Rate](image)

Figure 3.13 Graph of Probability of Secrecy Against Achieved Secrecy Rate
3.4.7 Discussion of Figure 3.13

Figure 3.13 above shows the graph of the probability of secrecy against the achieved secrecy rate when $P_t = 10$ for different values of $\rho = 0.25, 0.5, 0.75$. From the graph, it can be observed that high probability of secrecy is achieved at low secrecy rate but as the demand on the system (secrecy rate) increases at fixed transmit power, the probability of secrecy decreases. It can also be observed that when $\rho = 0.5$, the system achieves better performance as the demand on the system increases. Comparing figures 3.13 and 3.11, it can be observed that at $P_t = 10$ on figure 3.11, a probability of secrecy of 0.4 is achieved for both $\rho = 0.5$ and $\rho = 0.75$. Similarly, from figure 3.13, a probability of secrecy of 0.4 is achieved when the secrecy rate is 4 for both $\rho = 0.5$ and $\rho = 0.75$. Therefore, these two results show similarities.

3.5 Simulation IV: Power Allocation Problem and Secrecy Constraint

The generation of artificial noise adds to the power requirement of the system since additional power is needed at the transmitter to generate the artificial noise. Therefore, we need to investigate the optimal way of allocating the available power between the information signal and AN in order to guarantee a given SNR to fulfil a pre-defined QoS constraint or minimize the outage probability of secrecy. In this formulation, a QoS constraint is defined at both Bob and Eve. The objective of this formulation as described in [55] is to propose a given probability of secrecy by imposing a minimum SNR at Bob and probabilistically making sure that the SNR at each eavesdropper does not exceed a maximum set value. Therefore, the task is to compute the best power allocation strategy that minimizes the transmitted power ($P = c + d$) bounded by ensuring a certain probability of secrecy $\beta \in [0,1)$, fulfilling the set QoS constraint. The formulation is mathematically expressed below;

$$\min_{c,d} \quad (c + d) \quad \text{s.t} \quad \text{SNR}_b \geq \gamma_b \quad 3.18$$

$$P \{ \text{SNR}_{e_1} \leq \gamma_e , \ldots , \text{SNR}_{e_n} \leq \gamma_e \} \geq \beta \quad 3.19$$

where $P \{ \cdot \}$ refers to the probability of an event

By assuming that all the $h_{en}$ are mutually independent, equation 3.19 simplifies to

$$\left( P \{ \text{SNR}_e \leq \gamma_e \} \right)^n \geq \beta \quad 3.20$$

Substituting equations 3.6 and 3.7 into 3.18 and 3.20 respectively, we obtain;
We consider both constraint and unconstraint power allocation scenarios. By power constraint system, we imply that the total transmit power \((P_{\text{max}})\) at Alice is fixed. However, if the total power requirement of the system (i.e. \(c + d\)) is more than the maximum power \(P_{\text{max}}\) at the transmitter, the system is declared unrealizable. In this condition, no information is transmitted for that specific channel realization and the system declares an outage.

Equation 3.22 above can be re-written in terms of a random Hermitian form as described below:

\[
\begin{align*}
\mathbb{P} \left\{ \frac{cw_i^H(h_e^Hh_e)w_1}{dh_e^HC_nh_e + \sigma_e^2} \leq \gamma_e \right\} \geq \beta^{1/n}
\end{align*}
\]

The equations above can easily be solved for optimum value of \(c\) and \(d\) to give;
In this simulation, a passive eavesdropper scenario is considered. The mean and the covariance matrix of the CSI of Eve are zero and respectively. Also, the channel variances is .

The simulation results evaluate the power allocation, achieved secrecy probability as well as the normalized secrecy throughput both for constrained and unconstrained cases.

Figure 3.14 Graph of Achieved Probability of Secrecy Against Target Probability of Secrecy

3.5.1 Discussion of Figure 3.14

The graph above shows the plot of the achieved probability of secrecy against the target probability of secrecy. The plot was obtained from the formulation in equations 3.26 and 3.27 above. By assuming that the distance from Alice to Bob is equal to the distance from Alice to Eve
and that both Bob and Eve are affected by similar noise characteristics, therefore the noise power is the same: $\sigma^2_b = \sigma^2_e = 1$. The target probability of secrecy ($\beta$), in equation 3.27 varies from 0.05 to 0.95. For this simulation, one eavesdropper was considered (i.e. $n = 1$) and the maximum available power at Alice is $P_{\text{max}} = 5$. In the power unconstrained scenario, transmission will always take place since there is no restriction placed on the power. Therefore, the target probability of secrecy is continuously guaranteed. However, for power constrained system, transmission will only occur when equations 3.18 and 3.19 are both fulfilled and the solution of equations 3.26 and 3.27 require that $P_t = c + d \leq P_{\text{max}}$. From the graph, it can be observed that at low target probability of secrecy, the achieved probability of secrecy is higher. This is as a result of the positive contribution of beamforming. But as the target probability of secrecy increases, the achieved probability of secrecy increases linearly. For instance, at 0.5 and above target probability of secrecy, the achieved probability of secrecy is approximately equal to the target probability of secrecy. This proves that the design meets the target probability of secrecy.

The next simulation investigates the variation of normalized secrecy throughput against the target probability of secrecy for both constrained and unconstrained power condition.

**Figure 3.15** Graph of Achieved Probability of Secrecy Against Target Probability of Secrecy.
3.5.2 Discussion of Figure 3.15

Figure 3.15 above shows the plot of normalized secrecy throughput against target probability of secrecy for both constrained and unconstrained power system when the total power available is 5. In this simulation, the normalized secrecy throughput is defined as the ratio between the number of channel realization with secure transmission and the total number of channel realization times the achieved probability of secrecy.

\[
\text{Normalized Sec. Throughput} = \text{Prob. of Sec} \times \frac{\text{Number of Channel Realization with Secure Transmission}}{\text{Total number of Channel Realizations}}
\]

As observed from the graph, for the power unconstrained scenario, the target probability of secrecy is always assured since power is readily available. However, for the constrained system, as the target probability of secrecy increases (for instance as \( \beta \) approaches 1), the normalized secrecy throughput decreases. This is because as the security condition place on the system becomes more demanding, information is transmitted for fewer number of channel realization. Therefore, there is a trade-off between ensuring high probability of secrecy and normalized secrecy throughput. However, to improve the secrecy throughput of the system, additional power is needed at the transmitter. Figure 3.16 below present the scenario where the available power at the transmitter was increased to 10.

![Graph of Normalized Secrecy Throughput Against Target Probability of Secrecy](image.png)

**Figure 3.16** Graph of Achieved Probability of Secrecy Against Target Probability of Secrecy.
3.5.3 Discussion of Figure 3.16

Figure 3.16 above presents the plot of normalized secrecy throughput against the target probability of secrecy for both constrained and unconstrained power system when the available power at the transmitter is 10. The simulation was performed for similar condition as that of figure 3.15 except that the available power at the transmitter has been increased to 10. As observed from the graph, the normalized secrecy throughput curve for the power constrained scenario moves closer to the unconstrained case when compared to figure 3.15. This is because as the power available at the transmitter is increased, the secrecy throughput of the system also increases for the power constrained system. Furthermore, the next simulation investigate the effect of increasing the maximum power at the transmitter for two values of the target probability of secrecy $\beta = 0.8$ and 0.9.

![Graph of Normalized Secrecy Throughput Against Maximum Power Available at Transmitter](image-url)

Figure 3.17 Graph of Normalized Secrecy Throughput Against the Maximum Power Available at the Transmitter for a Single Eavesdropper
Discussion of Figure 3.17 and 3.18

Figure 3.17 and 3.18 above shows the plot of normalized secrecy throughput against the maximum power available for two values of the target probability of secrecy $\beta = 0.8$ and 0.9. Figure 3.17 considered just one eavesdropper while figure 3.18 presents the result for three non-colluding eavesdroppers. It can be observed from figure 3.17 that for target probability of 0.8, a minimum power of 20 is required at the transmitter while the minimum power required to achieve a target secrecy probability of 0.9 is 30. This result explains that higher secrecy throughput can be achieved by increasing the power at the transmitter. However for the case of three eavesdroppers as presented in figure 3.18, to achieve a target secrecy probability of 0.8, a minimum power of 30 is required at the transmitter but for a target of 0.9, additional power greater than 30 is required at the transmitter. It can therefore be deduced that by providing more power at the transmitter, it is possible to guarantee a target probability of secrecy when the number of eavesdropper is greater than three (i.e. $n > 3$)
Figure 3.19  Graph of Average Power Distribution Between Artificial Noise and Information Signal Against Target Probability of Secrecy in an Unconstraint Power System.

3.5.5  Discussion of Figure 3.19

Figure 3.18 above presents the plot of the average power allocated between the information signal and AN against the target probability of secrecy. The average value of power was computed using equations 3.26 and 3.27 by taking the mean value of the power over the Monte Carlo simulations where there is transmission(i.e. $P \leq P_{\text{max}}$).
CHAPTER FOUR

PHYSICAL LAYER SECURITY OF MIMO-OFDM SYSTEMS

In [13,47,50–52,56], the authors investigated the secrecy in flat fading channel using beamforming and AN generation as transmit strategy in the presence of passive eavesdroppers. However in [57], the authors revealed the concept of improving the secrecy of a frequency selective multiple-input-multiple-output (MIMO) system based on OFDM signalling using spatial beamforming and AN as transmit strategy for secure communication. The authors in [57] investigated the potential of the eavesdropper to make vulnerable the security of the system. To achieve this, zero forcing was employed as the receive beamforming strategy at the eavesdropper. By using zero forcing, the interfering effect of the AN is alleviated by the eavesdropper thereby making the system more vulnerable. This project work investigates the power allocation scheme across the subcarriers and then for each subcarrier, the power distribution between the AN and information bearing signal.

Figure 4.1 System Model for OFMD-MIMO Frequency Selective System with ‘k’ corresponding Flat Fading Channel for the kth subcarrier.
4.1 System and Signal Model

The system model is as shown in figure 4.1 above. The system assumes a single eavesdropper with multiple antennas and OFDM signalling was taken into account. Alice, Bob and Eve has $N_t$, $N_b$, and $N_e$ antennas respectively. The Alice-to-Eve and Alice-to-Bob MIMO frequency selective channel of $L$ multipath taps are represented by $H_e$ and $H_{ab}$. Further, this channel taps are modelled as $(N_e \times N_t)$ and $(N_b \times N_t)$ matrices respectively. The frequency selective channels of $L$ multipath taps are denoted by a corresponding OFDM system of $N$ parallel frequency flat fading channel.

The beamformed signal vector $(x_{(k)})$ transmitted by Alice over the $m$th subcarrier is received by Bob and Eve on their $m$th subcarrier respectively as;

$$u_{(k)} = H_{ab(k)}x_{(k)} + n_{ab(k)} \quad 4.1$$

$$v_{(k)} = H_{e(k)}x_{(k)} + n_{e(k)} \quad 4.2$$

where $H_{ab(k)}$ and $H_{e(k)}$ represents the frequency-domain channel matrices of the channel between Alice-to-Bob and Alice-to-Eve respectively. Further, $n_{e(k)}$ and $n_{ab(k)}$ denotes the zero mean, mutually independent, complex AWGN with covariance matrices $\sigma^2_{e(k)}I$ and $\sigma^2_{b(k)}I$.

The signal vector transmitted by Alice is modelled as;

$$x_{(k)} = \sqrt{\rho_{(k)}} \left( \left( 1 - \epsilon_{(k)} \right) t_{(k)}s_{(k)} + \sqrt{\epsilon_{(k)}} \eta_{(k)} \right) \quad 4.3$$

where the covariance matrix of $x_{(k)}$ is given by $C_{x(k)} = \mathbb{E}\{x_{(m)}x_{(k)}^H\}$. Further, the power allocated to the $k$th subcarrier is given by $\rho_{(k)} = \text{Tr}\{C_{x(k)}\}$ while the total power constraint condition is given by;

$$\sum_{k=0}^{N-1} \rho_{(k)} = P \quad 4.4$$

A fraction $\epsilon_{(k)} \in [0,1]$ of power allocated to each of the subcarrier is committed for AN generation. $t_{(k)}$ is the $(N_t \times 1)$ normalized beamforming vector such that $\|t_{(k)}\| = 1$, while $d_{(k)}$ represents the transmitted scalar complex information symbol such that $\mathbb{E}\{|s_{(k)}|^2\} = 1$. Finally, $\eta_{(k)}$ is the AN vector with a covariance matrix given by $C_{\eta_{(k)}} = \mathbb{E}\{\eta_{(k)}\eta_{(k)}^H\}$. 
4.2 Beamforming and Artificial Noise generation

In order to increase the secrecy of the system, beamforming and AN generation are adopted as the transmit strategy. As previously stated in chapter two, the objective of artificial noise generation as adopted in [14,37,55,56] is to confuse the eavesdropper by broadcasting artificially generated noise in all direction aside from Bob. Therefore, as described in [56], Alice picks the beamforming vector \( \mathbf{t} \) as the principal eigenvector \( \mathbf{t}_{1(k)} \) corresponding to the largest eigenvalue of \( \mathbf{H}_{ab(k)}^H \mathbf{H}_{ab(k)} \). Further, the linear combination of the remaining \( (N_t - 1) \) eigenvectors are employed to compute the artificial noise vector \( \mathbf{n}_{(k)} \) such that \( \mathbf{n}_{(k)} \) will lie in the nullspace of \( \mathbf{H}_{ab(k)} \). Thus, orthogonality between the beamformer \( \mathbf{t}_{1(k)} \) and the artificial noise \( \mathbf{n}_{(k)} \) is conserved \( \left( \mathbf{t}_{1(k)}^H \mathbf{n}_{(k)} = 0 \right) \). If we assume a uniform power distribution among the \( N_t - 1 \) remaining eigenvectors, we can obtain \( \mathbf{n} \) as follow;

\[
\mathbf{n}_{(k)} = \frac{1}{\sqrt{N_t - 1}} \sum_{i=2}^{N_t} \mathbf{t}_{i(k)} \eta_i
\]

where \( \eta_i \) denotes a unit magnitude random complex scalar and \( \mathbf{w}_i \) represents the \( i \)th eigenvector of \( \mathbf{H}_{ab(k)}^H \mathbf{H}_{ab(k)} \). The covariance matrix of the artificial noise \( \mathbf{C}_{\eta} \) is thus expressed as;

\[
\mathbf{C}_{\eta_{(k)}} = \frac{1}{N_t - 1} \sum_{i=2}^{N_t} \mathbf{t}_{i(k)} \mathbf{t}_{i(k)}^H
\]

4.3 Maximal Ratio Combining (MRC) at Bob

At Bob, the optimal strategy employ in order to maximize the received SNR is maximal ratio combining (MRC). The received SNR at Bob is given by;

\[
y_{(k)\text{MRC}} = \mathbf{w}_{(k)\text{MRC}}^H \mathbf{u}_{(k)}
\]

The optimum beamforming vector at the \( k \)th subcarrier is given by;

\[
\mathbf{w}_{(k)\text{MRC}} = \mathbf{H}_{ab(k)} \mathbf{t}_{1(k)}
\]

As derived in Appendix III, the SNR on the \( k \)th subcarrier at Bob can be expressed as;

\[
\text{SNR}_{b(k)} = \frac{(1 - \epsilon_{(k)})\rho_{(k)} \mathbf{t}_{1(k)}^H \mathbf{H}_{ab(k)}^H \mathbf{H}_{ab(k)} \mathbf{t}_{1(k)}}{\sigma_{b(k)}^2}
\]
Eve can receive the transmitted signal using either minimum mean square error (MMSE) to maximise the received SNR as proposed in [13,52,56] or zero forcing (ZF) to reduce the effect of the interfering AN as presented in [57].

4.4 Minimum Mean Square Error (MMSE) at Eve

As proposed in [13,52,56], Eve uses MMSE to retrieve the maximum likely information from the primary link (i.e. MMSE is used as the optimum multiple antennas combining strategy to maximize the SNR). It is assumed that $H_{e(k)}$, $t_{1(k)}$, $C_{n(k)}$, and the power allocated for AN ($\rho_{(k)}E_{(k)}$) are known by Eve. Therefore, using MMSE at Eve the beamformer at the $k$th subcarrier can be expressed as:

$$w_{e(k)}^{\text{MMSE}} = \varphi H_{e(k)}^H t_{1(k)}$$

where:

$$\varphi = \left(\epsilon_{(k)}\rho_{(k)}H_{e(k)} C_{n(k)} H_{e(k)}^H + \sigma_{e(k)}^2 I\right)^{-1}$$

The received scalar signal at the output of the beamformer is given by the expression;

$$y_{e(k)}^{\text{MMSE}} = w_{e(k)}^{H\text{MMSE}} v(k)$$

As derived in appendix IV, the SNR at the $k$th subcarrier is given by:

$$\text{SNR}_{e(k)\text{MMSE}} = (1 - \epsilon_{(k)})\rho_{(k)} t_{1(k)}^H H_{e(k)}^H \varphi H_{e(k)} t_{1(k)}$$

4.5 Zero Forcing (ZF) at Eve

This technique as proposed in [57] assumes that Eve is aware of the transmit strategy employed by Alice (i.e. Eve is aware of $H_{e(k)}$ and $t_{1(k)}$). With the knowledge of this information, Eve is able to ease the effect of the AN. Using ZF, the beamformer vector of Eve is computed as follows:

$$w_{e(k)}^{\text{ZF}} = \left(H_{e(k)}^\dagger\right)^H t_{1(k)}$$

where: $H_{e(k)}^\dagger = \left(H_{e(k)}^H H_{e(k)}\right)^{-1} H_{e(k)}^H$ represents the Moore-Penrose inverse.

The received scalar signal at the output of the beamformer is given by the expression:

$$y_{e(k)\text{ZF}} = w_{e(k)\text{ZF}}^H v(k)$$

As derived in appendix V, the SNR at the $k$th subcarrier is given below;

when $N_e \geq N_t$, the SNR can be computed thus

$$\text{SNR}_{e(k)\text{ZF}} = (1 - \epsilon_{(k)})\rho_{(k)} \Phi$$
where
\[ \Phi = \left[ \sigma^2_{e(k)} t^H_{1(k)} H^H_{e(k)} \left( H^H_{e(k)} \right)^H t_{1(k)} \right]^{-1} \]

However, when \( N_e < N_t \), mitigating the AN process will not be entirely successful. The SNR can be computed by;

\[
\text{SNR}_{e(k)ZF} = \frac{\left( 1 - \epsilon_{(k)} \right) \rho_{(k)} \left| t^H_{1(k)} H^H_{e(k)} H_{e(k)} \rho_{(k)} t_{1(k)} \right|^2}{H^H_{e(k)} H_{e(k)} H_{e(k)} \epsilon_{(k)} + \sigma^2_{e(k)} I \left( H^H_{e(k)} \right)^H t_{1(k)}}
\]

### 4.6 Power Allocation Strategy

Allocating power in a frequency selective OFDM-MIMO system involves distributing power among the subcarriers and subsequently for each subcarrier, allocates power between the information signal and AN. The optimal power allocation strategy among the subcarriers is to use the water-filling approach since the CSI of Bob is known perfectly by Alice. However, a less complicated approach is to uniformly distribute the available power among the subcarriers. In addition, to allocate power between the information signal and AN, three different schemes can be identified. Firstly, as introduced in [13], the power allocated for AN generation \( \epsilon_{(k)} \) is fixed so as to guarantee a minimum target SNR on the kth subcarrier at Bob. \( \epsilon_{(k)} \) is computed using the expression below;

\[
\epsilon_{(k)} = 1 - \frac{\text{SNR}_{(k)}}{\rho_{(k)} v_{1(k)}}
\]

where \( \text{SNR}_{(k)} \) is the minimum target SNR at Bob on the kth subcarrier, \( v_{1(k)} \) is the principal eigenvalue of \( H^H_{ab(k)} H_{ab(k)} \).

The second approach to allocate power between information signal and AN was proposed in [51]. According to [51], to maximize the ergodic secrecy capacity of the system, power should be equally distributed between the information signal and AN. The last approach investigates the impact of AN on the secrecy of the system. To achieve this objective, the fraction of power dedicated for AN generation is gradually varied.

#### 4.6.1 Allocating Power among Subcarriers

As stated early, waterfilling approach is the optimal strategy to allocate power among the subcarriers. However, the implementation of waterfilling is complicated. The approach adopted in this study is to uniformly allocate power among only half of the subcarriers with the highest
power to noise ratio ($\gamma$). This is a suboptimal method and easy to implement. The channel’s power to noise is given by:

$$\gamma(i) = \frac{\|H(i)\|_F^2}{N_t N_b \sigma^2_{(k)}}$$

where $\| . \|_F$ represents the Frobenius norm.

The strategy is to divide the power equally among only half of the total subcarrier with the highest power to noise ratio. The remaining half is allocated zero power. By so doing, this strategy select best half of the subcarriers to transmit the information signal. Therefore, $(1 - \epsilon_{(k)})\rho_{(k)}$ is used to transmit the information signal and $\epsilon_{(k)}\rho_{(k)}$ is allocated to broadcast AN.

4.7 Simulation Results

![Graph of Average SNR at Bob and Eve Against Target SNR at Bob](image)

Figure 4.2 Graph of Average SNR at Bob and Eve Against Target SNR at Bob when $N_t = N_b = 5$ and $L = 4$
4.7.1 Discussion of Figure 4.2

Figure 4.2 above shows the graph of average SNR at Bob and Eve against the target SNR at Bob when all nodes are equipped with 5 antennas and considering 4 channel taps. The power allocation among the subcarriers is as explained in 4.6.1 while the power is allocated between information signal and AN in order to guarantee a minimum target SNR at Bob. The target SNR at Bob is varied from −10dB to 60dB. The power allocated for AN generation follows equation 4.19. This graph investigates the effect of increasing the number of OFDM subcarriers on the secrecy of the system. In order to compare the two receive beamforming strategies, the simulation was performed for both MMSE and ZF. It can be observed from the graph that when the system demands low SNR, MRC at Bob achieves the target SNR at Bob. Although MMSE and ZF at Eve do not achieve the target SNR at Bob, ZF outperforms MMSE. This is due to the fact that at low target SNR, more power is used to broadcast AN and ZF can mitigate the effect of AN better than MMSE. However, as the system demands higher SNR, the power required to broadcast AN is lower. At this point, MMSE outperforms ZF as observed by the decrease in gap between the MMSE-Eve curve and MRC-Bob curve. It can also be observed that above 30dB target SNR, MRC at Bob cannot achieve the minimum target SNR. This is because the available power at Alice is exhausted therefore the system cannot attain the minimum target SNR at Bob. The gap between the SNR at Bob and Eve remain even when there is no power to transmit AN because of the positive contribution of beamforming strategy.

4.7.2 Discussion of Figure 4.3 and 4.4

Figure 4.3 and 4.4 below shows the graph of average SNR at Bob and Eve against the target SNR at Bob for different number of antennas at Eve for 16 OFDM subcarriers. The same power allocation scheme as explained previously was employed. The graph investigates the effect of increasing the number of antennas at Eve when $N_t = N_b = 5$. It can be observed from the graph that the SNR of Eve increases as the number of antennas at Eve increases. This is due to the additional spatial diversity available to weaken the security of the system. It can also be observed from figure 4.3 that when $N_e = 2, 5$ and $10$, MRC at Bob performs better than both MMSE and ZF at Eve. However from figure 4.4, when $N_e = 50$, ZF outperforms MRC and MMSE both at low and high target SNR. Further, it can be observed that at certain point when the system demands high SNR, MMSE at Eve performs better than MRC at Bob; however, $N_e = 50$ is practically unrealistic.
Figure 4.3 Graph of Average SNR at Bob and Eve Against Target SNR at Bob for Different Antennas at Eve, $N_e = 2, 5$ and $10$ when $N_t = N_t = 5$, $N = 16$, and $L = 4$.

Figure 4.4 Graph of Average SNR at Bob and Eve Against Target SNR at Bob for Different Antennas at Eve, $N_e = 2, 5, 10$ and $50$ when $N_t = N_t = 5$, $N = 16$, and $L = 4$. 
**4.7.3 Discussion of Figure 4.5**

Figure 4.5 above shows the graph of average SNR at Bob and Eve against the fraction of power allocated for AN generation when $N_t = N_e = 5$ and $L = 4$. 

This implies that at low fraction of power allocated for AN generation ($\epsilon_{(k)} < 0.1$), MMSE performs better than ZF since there is little AN to cancel.
Figure 4.6   Graph of Average SNR at Bob Against the Fraction of Power Allocated for AN when \( N_e = 3, 5, 8 \) and \( L = 4 \) for \( N = 16 \)

4.7.4 Discussion of Figure 4.6

Figure 4.6 above show the variation of SNR of Bob and Eve against the fraction of power allocated to AN generation for different number of antennas at Eve. The aim of this graph is to investigate the relation between the number of antennas at Eve and the ability of Eve to cancel AN. As observed from the graph, when \( N_e \geq N_t \), i.e. \( N_e = 5 \) or \( 8 \), Eve can efficiently null the AN. Even though MMSE outperforms ZF at low \( \epsilon_k \), as \( \epsilon_k \) increases, ZF at Eve achieves higher SNR which proves that ZF can effectively null the AN. However, when \( N_e < N_t \), i.e. \( N_e = 3 \), Eve employs ZF to partially cancel the AN.
CHAPTER FIVE

CONCLUSION AND FUTURE WORK

This research work has investigated the physical layer security of both MISO and OFDM-MIMO communication systems. This project explored the use of beamforming and artificial noise generation as transmit strategy to achieve secure communication. In the MISO system, a probabilistic approach for achieving secrecy was studied. This method ensures a target probability of secrecy characterised by QoS constraint at the eavesdropper and the legitimate receiver. Further, this research work considers the optimum power allocation strategy between the information signal and artificial noise. Results from MATLAB simulation show that this scheme achieves the target probability of secrecy by allocating the minimum power for both constrained and unconstrained transmit power scenarios. It was established that for power constraint scenario, there exist a trade-off between attaining a high probability of secrecy and the secrecy throughput. Further, it was proven that the secrecy throughput of the system can be increased by augmenting the available power at the transmitter.

In the OFDM-MIMO system, the contribution of frequency selectivity to the secrecy of the system was investigated. A sub-optimal power distribution scheme among the subcarriers was adopted. This power distribution strategy uniformly allocates power only to half of the subcarriers with the highest power to noise ratio while the other half is not used for transmission. In addition, this research work explored the possibility of the eavesdropper to mitigate the effect of the added artificial noise by assuming that the eavesdropper is aware of the CSI of the main channel. In fact, it was proven that the security of the system is at risk if the eavesdropper has a large number of antennas and whether it also knows the Alice-to-Bob’s link CSI and uses ZF as the receive beamforming strategy. Further, even though ZF mitigates the AN at the eavesdropper, it does not maximize the SNR when compares to MRC since it amplifies the AWGN. However, the MMSE approach achieves a balance between AN cancellation and AWGN improvement.

One of the major issues that need to be addressed in physical layer security is the optimization of the physical layer transmit strategies. Using the expression for secrecy capacity or the achievable secrecy rate, the transmit strategies such as beamforming, subcarrier power allocation need to be optimized in order to select a particular point of operation. Considering a single user situation, if additional secrecy constrained is placed on the system design, the secrecy capacity expressions obtained are generally non-convex in the transmit strategies. This leads to a non-convex transmit optimization problem. On the contrary, in a multi-user scenario, the resulting transmit optimization problem can be reduced to a convex optimization problem and can be computed.
effectively. Therefore, by speculation, the MIMO scenario will be entirely resolved in the near future. Furthermore, assumptions such as having the perfect CSI of the receivers and transmitters are unrealistic and need to be addressed. Also, the effect of limited channel feedback and channel estimation errors on the achieved secrecy rate
In the future, this research work will be extended to address the resource allocation and transmit optimization problem in MIMO scenarios i.e. multiple antenna at transmitter, receiver and at the eavesdropper as well as considering malicious user and complex attacks.
REFERENCES


Physical Layer Security Using Artificial Noise by AKINDOYIN Akinbiyi 2012


APPENDIX I

Derivation of the SNR at Bob and Eve

The transmitted beamformed vector $\mathbf{x}$ modelled as;

$$\mathbf{x} = \sqrt{c} \mathbf{w} s + \sqrt{d} \mathbf{\eta}$$

The SNR received at Bob is derived below;

$$y_b = \mathbf{h}_{ab}^H \mathbf{x} + n_b$$

$$y_b = \mathbf{h}_{ab}^H (\sqrt{c} \mathbf{w} s + \sqrt{d} \mathbf{\eta}) + n_b$$

$$y_b = \sqrt{c} \mathbf{h}_{ab}^H \mathbf{w} s + \sqrt{d} \mathbf{h}_{ab}^H \mathbf{\eta} + n_b$$

Since $\mathbf{\eta}$ lies in the null space of $\mathbf{h}_{ab}^H$, therefore, $\mathbf{h}_{ab}^H \mathbf{\eta} = 0$. The above expression simplifies to:

$$y_b = \sqrt{c} \mathbf{h}_{ab}^H \mathbf{w} s + n_b$$

$$\text{SNR}_b = \frac{E\left\{ |\sqrt{c} \mathbf{h}_{ab}^H \mathbf{w} s|^2 \right\}}{E\{ |n_b|^2 \}}$$

$$\text{SNR}_b = \frac{c |\mathbf{h}_{ab}^H \mathbf{w}|^2 E\{|s|^2 \}}{E\{ |n_b|^2 \}}$$

$$\text{SNR}_b = \frac{c \mathbf{w}^H \mathbf{h}_{ab} \mathbf{h}_{ab}^H \mathbf{w}}{\sigma_b^2}$$

Alice will always select the beamforming vector as the principal eigenvector that correspond to the largest eigenvalue of $\mathbf{h}_{ab} \mathbf{h}_{ab}^H$. Therefore, $\text{SNR}_b$ is maximized when $\mathbf{w}$ is the maximum eigenvector of $\mathbf{h}_{ab} \mathbf{h}_{ab}^H$. The maximum eigenvector is $\mathbf{h}_{ab}$ and the maximum eigenvalue is $||\mathbf{h}_{ab}||^2$

$$\text{SNR}_b = \frac{c ||\mathbf{h}_{ab}||^2}{\sigma_b^2}$$

The SNR at the $n$th Eve is derived below;

$$y_{en} = \mathbf{h}_{en}^H \mathbf{x} + n_{en}$$

Substituting the expression for $\mathbf{x}$,

$$y_{en} = \mathbf{h}_{en}^H (\sqrt{c} \mathbf{w} s + \sqrt{d} \mathbf{\eta}) + n_{en}$$

$$y_{en} = \sqrt{c} \mathbf{h}_{en}^H \mathbf{w} s + \sqrt{d} \mathbf{h}_{en}^H \mathbf{\eta} + n_{en}$$
\[
\text{SNR}_{en} = \frac{E\left\{ |\sqrt{d} h_{en}^H w s|^2 \right\}}{E\left\{ (\sqrt{d} h_{en}^H \eta + n_{en})^2 \right\}}
\]

\[
\text{SNR}_{en} = \frac{c (h_{en}^H w)^2 E\left\{ |s|^2 \right\}}{E\left\{ |\sqrt{d} h_{en}^H \eta|^2 \right\} + E\left\{ |n_{en}|^2 \right\}}
\]

\[
\text{SNR}_{en} = \frac{c w^H (h_{en}^H h_{en}^H) w}{d E\left\{ (\eta^H h_{en}^H h_{en}) \right\} + E\left\{ |n_{en}|^2 \right\}}
\]

\[
\text{SNR}_{en} = \frac{c w^H (h_{en}^H h_{en}^H) w}{d h_{en}^H E\left\{ (\eta \eta^H) h_{en} \right\} + E\left\{ |n_{en}|^2 \right\}}
\]

But, \( E\left\{ (\eta \eta^H) \right\} = C_\eta \) and \( E\left\{ |n_{en}|^2 \right\} = \sigma_{en}^2 \), substituting these expressions give;

\[
\text{SNR}_{en} = \frac{c w^H (h_{en}^H h_{en}^H) w}{d h_{en}^H C_\eta h_{en} + \sigma_{en}^2}
\]
APPENDIX II  

Derivation of the Optimum Power Allocation Strategy  

From equation 3.23, 

\[ P \left[ h_e^H A h_e \leq \sigma_e^2 \right] \]

where  

\[ A = \frac{c w_i w_i^H}{Y_e} - d C_\eta \]

The equation above relates to the CDF of an indefinite Hermitian quadratic form \( Y = h_e^H A h_e \)

where \( E\{h_e h_e^H\} = \sigma_{h_e}^2 I \). The equation can be re-written as; \( Y = \frac{h_e^H A h_e}{\sigma_{h_e}^2} \), where \( h_e = h_e / \sigma_{h_e} \) and \( E\{h_e h_e^H\} = I \). Therefore, \( \bar{A} = \frac{\sigma_{h_e}^2}{\sigma_{h_e}^2} A \) also the eigenvalues of \( \bar{A} \) are \( \lambda_1 \sigma_{h_e}^2 A \).

From 

\[ A = \frac{c w_i w_i^H}{Y_e} - d C_\eta \]

Substituting the expression for \( C_\eta \) and \( A \) into the equation above; 

\[ \frac{\bar{A}}{\sigma_{h_e}^2} = \frac{c w_i w_i^H}{Y_e} - d \left( \frac{1}{N_t - 1} \sum_{i=2}^{N_t} w_i w_i^H \right) \]

\[ \bar{A} = \sigma_{h_e}^2 \left[ \frac{c w_i w_i^H}{Y_e} - d \left( \frac{1}{N_t - 1} \sum_{i=2}^{N_t} w_i w_i^H \right) \right] \]

\[ \bar{A} = \sigma_{h_e}^2 \left[ \frac{c w_i w_i^H}{Y_e} - \frac{d}{N_t - 1} w_2 w_2^H - \frac{d}{N_t - 1} w_2 w_2^H \ldots - \frac{d}{N_t - 1} w_{N_t} w_{N_t}^H \right] \]

The eigendecomposition \( N_t \) eigenvalues of \( \bar{A} \) are \( \lambda_1 \) and \( \lambda_2 \) with order of multiplicity of one and \( N_t - 1 \) respectively. 

\[ [\lambda_1, \lambda_2, \ldots, \lambda_{N_t}] = \left[ \frac{c}{Y_e} \sigma_{h_e}^2, \frac{d}{N_t - 1} \sigma_{h_e}^2, \frac{d}{N_t - 1} \sigma_{h_e}^2, \ldots, \frac{d}{N_t - 1} \sigma_{h_e}^2 \right] \]

The CDF of \( Y \) is 

\[ F_Y(y) = u(y) + \frac{\alpha_1}{\lambda_1} e^{-\frac{y}{\lambda_1}} u \left( \frac{y}{\lambda_1} \right) + \sum_{k=1}^{N_t-1} \frac{\alpha_{n+1}}{(n-1)!} |\lambda_2|^n e^{-\frac{y}{\lambda_2}} u \left( \frac{y}{\lambda_2} \right) \]
where \( \alpha_1 = -\frac{\lambda_1}{\left(1 - \frac{\lambda_2}{\lambda_1}\right)^{N_t-1}} \)

The expression above can be simplified for only positive values of \( y \). Since \( \sigma_e^2 \geq 0 \), therefore \( \{\alpha_{k+1}\}_{k=1}^{N_t-1} \) can be ignored. The CDF of \( Y \) simplifies to:

\[
F_Y(y) = 1 - \frac{1}{\left(1 + \frac{d}{c} \frac{Y_e}{N_t - 1}\right)^{N_t-1}} e^{-\frac{Y_e - \sigma_e^2}{c\sigma_{\text{he}}}} \geq \beta^{-1} \]

From equation 3.25 above,

\[
F_Y(y) = 1 - \frac{1}{\left(1 + \frac{d}{c} \frac{Y_e}{N_t - 1}\right)^{N_t-1}} e^{-\frac{Y_e - \sigma_e^2}{c\sigma_{\text{he}}}} \leq 1 - \beta^{-1}
\]

\[
\frac{e^{-\frac{Y_e - \sigma_e^2}{c\sigma_{\text{he}}}}}{1 - \beta^{-1}} \leq \left(1 + \frac{d}{c} \frac{Y_e}{N_t - 1}\right)^{N_t-1}
\]

\[
\left(\frac{e^{-\frac{Y_e - \sigma_e^2}{c\sigma_{\text{he}}}}}{1 - \beta^{-1}}\right)^{N_t-1} \leq 1 + \frac{d}{c} \frac{Y_e}{N_t - 1}
\]

Therefore,

\[
d = d^* = \max \left\{0, c'(N_t-1) \frac{Y_e}{\gamma_e} \left(\sqrt{\frac{\left(\frac{Y_e - \sigma_e^2}{c\sigma_{\text{he}}}ight)^{N_t-1}}{1 - \beta^{-1/n}} - 1}\right)\right\}
\]
APPENDIX III

Derivation of SNR at Bob Using MRC

From equation 4.7 and 4.8,

\[ y_{(k)\text{MRC}} = w_{(k)\text{MRC}}^H u_{(k)} \]

The optimum beamforming vector at the kth subcarrier is given by;

\[ w_{(k)\text{MRC}} = H_{ab(k)} t_{1(k)} \]

Substituting equation 4.8 into 4.7,

\[ y_{(k)\text{MRC}} = \left( H_{ab(k)} t_{1(k)} \right)^H u_{(k)} \]

Substituting the expression for \( u_{(k)} \),

\[ y_{(k)\text{MRC}} = \left( H_{ab(k)} t_{1(k)} \right)^H [H_{ab(k)} x_{(k)} + n_{b(k)}] \]

\[ y_{(k)\text{MRC}} = t_{1(k)}^H H_{ab(k)}^H [H_{ab(k)} x_{(k)} + n_{b(k)}] \]

Finally, substituting the expression for \( x_{(k)} \),

\[ y_{(k)\text{MRC}} = \sqrt{\rho(k)} \left( \sqrt{1 - \epsilon_{(k)}} t_{1(k)} s_{(k)} + \sqrt{\epsilon_{(k)}} \eta_{(k)} \right) + n_{b(k)} \]

\[ y_{(k)\text{MRC}} = \sqrt{\rho(k)} \left( 1 - \epsilon_{(k)} \right) t_{1(k)}^H H_{ab(k)}^H H_{ab(k)} t_{1(k)} s_{(k)} + \sqrt{\rho(k)} \epsilon_{(k)} t_{1(k)}^H H_{ab(k)}^H H_{ab(k)} \eta_{(k)} \]

\[ y_{(k)\text{MRC}} = \left( t_{1(k)}^H H_{ab(k)}^H \right) n_{b(k)} \]

But \( t_{1(k)}^H \eta_{(k)} = 0 \),

\[ y_{(k)\text{MRC}} = \sqrt{\rho(k)} \left( 1 - \epsilon_{(k)} \right) t_{1(k)}^H H_{ab(k)}^H H_{ab(k)} t_{1(k)} s_{(k)} + t_{1(k)}^H H_{ab(k)}^H n_{b(k)} \]

\[ \text{SNR}_{b(k)\text{MRC}} = \frac{\mathbb{E} \left| \sqrt{\rho(k)} \left( 1 - \epsilon_{(k)} \right) t_{1(k)}^H H_{ab(k)}^H H_{ab(k)} t_{1(k)} s_{(k)} + t_{1(k)}^H H_{ab(k)}^H n_{b(k)} \right|^2}{\mathbb{E} \left| t_{1(k)}^H H_{ab(k)}^H n_{b(k)} \right|^2} \]

\[ \text{SNR}_{b(k)\text{MRC}} = \frac{\rho(k) \left( 1 - \epsilon_{(k)} \right) \left| t_{1(k)}^H H_{ab(k)}^H H_{ab(k)} t_{1(k)} s_{(k)} \right|^2}{\mathbb{E} \left| s_{(k)} \right|^2 + \mathbb{E} \left| n_{b(k)} \right|^2} \]

\[ \mathbb{E} \left| s_{(k)} \right|^2 = 1 \quad \text{and} \quad \mathbb{E} \left| n_{b(k)} \right|^2 = \sigma_{b(k)}^2 \]

\[ \text{SNR}_{b(k)\text{MRC}} = \frac{\rho(k) \left( 1 - \epsilon_{(k)} \right) \left| t_{1(k)}^H H_{ab(k)}^H H_{ab(k)} H_{ab(k)} t_{1(k)} \right|^2}{\mathbb{E} \left| s_{(k)} \right|^2 + \mathbb{E} \left| n_{b(k)} \right|^2} \]

Therefore, the SNR at Bob can be expressed as;

\[ \text{SNR}_{b(k)\text{MRC}} = \frac{\rho(k) \left( 1 - \epsilon_{(k)} \right) t_{1(k)}^H H_{ab(k)}^H n_{b(k)}^2}{\sigma_{b(k)}^2} \]
APPENDIX IV
Derivation of the SNR at Eve Using MMSE

From equations 4.10, 4.11 and 4.12 above,

\[ \mathbf{w}_{e(k)}^{\text{MMSE}} = \mathbf{\varphi} \mathbf{H}_{e(k)} \mathbf{t}_{1(k)} \]

where:

\[ \mathbf{\varphi} = \left( \varepsilon(k) \rho(k) \mathbf{H}_{e(k)} \mathbf{C}_{\eta(k)} \mathbf{H}_{e(k)}^{H} + \sigma_{e(k)}^{2} \mathbf{I} \right)^{-1} \]

The received scalar signal at the output of the beamformer is given by the expression;

\[ y_{e(k)}^{\text{MMSE}} = \mathbf{w}_{e(k)}^{H} \mathbf{v}_{(k)} \]

Substitute the expressions for \( \mathbf{v}_{(k)} \),

\[ y_{e(k)}^{\text{MMSE}} = \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{v}_{(k)} + \mathbf{n}_{e(k)} \]

\[ y_{e(k)}^{\text{MMSE}} = \left[ \sqrt{1 - \varepsilon(k)} \sqrt{\rho(k)} \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{t}_{1(k)} + \sqrt{\varepsilon(k)} \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{t}_{1(k)} \mathbf{s}_{(k)} + \mathbf{w}_{e(k)}^{H} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} \right] \]

\[ \text{SNR}_{e(k)}^{\text{MMSE}} = \frac{\mathbb{E} \left[ \left| \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{t}_{1(k)} \mathbf{s}_{(k)} \right|^{2} \right]}{\mathbb{E} \left[ \left| \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} \right|^{2} \right] + \mathbb{E} \left[ \mathbf{w}_{e(k)}^{H} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} \right]^{2}} \]

\[ \text{SNR}_{e(k)}^{\text{MMSE}} = \frac{\rho(k) \left( 1 - \varepsilon(k) \right) \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{t}_{1(k)} \mathbf{s}_{(k)}^{H}}{\rho(k) \varepsilon(k) \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} + \mathbf{w}_{e(k)}^{H} \mathbf{w}_{e(k)}^{H} \sigma_{e(k)}^{2} \mathbf{I}} \]

\[ \text{SNR}_{e(k)}^{\text{MMSE}} = \frac{\rho(k) \left( 1 - \varepsilon(k) \right) \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{t}_{1(k)} \mathbf{s}_{(k)}^{H} \mathbf{H}_{e(k)}^{H} \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} + \mathbf{w}_{e(k)}^{H} \mathbf{w}_{e(k)}^{H} \sigma_{e(k)}^{2} \mathbf{I}}{\rho(k) \varepsilon(k) \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} \mathbf{n}_{e(k)}^{H} \mathbf{H}_{e(k)}^{H} \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{w}_{e(k)}^{H} \sigma_{e(k)}^{2} \mathbf{I}} \]

\[ \text{SNR}_{e(k)}^{\text{MMSE}} = \frac{\rho(k) \left( 1 - \varepsilon(k) \right) \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{t}_{1(k)} \mathbf{s}_{(k)}^{H}}{\rho(k) \varepsilon(k) \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{n}_{e(k)} \mathbf{n}_{e(k)}^{H} \mathbf{H}_{e(k)}^{H} \mathbf{H}_{e(k)} \mathbf{w}_{e(k)}^{H} \mathbf{w}_{e(k)}^{H} \sigma_{e(k)}^{2} \mathbf{I}} \]
\[ SNR_{e(k)MMSE} = \frac{\rho(k) (1 - \epsilon(k)) t_{1(k)}^H H_{e(k)}^H H_{e(k)} t_{1(k)}}{\rho(k) \epsilon(k) H_{e(k)} C_{\eta(k)} H_{e(k)}^H + \sigma_{e(k)}^2 I} \]

Let \( \varphi = \left( \epsilon(k) \rho(k) H_{e(k)} C_{\eta(k)} H_{e(k)}^H + \sigma_{e(k)}^2 I \right)^{-1} \)

Therefore,

\[ SNR_{e(k)MMSE} = \rho(k) (1 - \epsilon(k)) t_{1(k)}^H H_{e(k)}^H \varphi H_{e(k)} t_{1(k)} \]
APPENDIX V

Derivation of the SNR at Eve Using Zero Forcing

From equations 4.14 and 4.15,

\[ w_{e(k)}^{ZF} = \left( H_{e(k)}^H \right)^H t_{1(k)} \]

where: \( H_{e(k)}^+ = \left( H_{e(k)}^H H_{e(k)} \right)^{-1} H_{e(k)}^H \) represents the Moore-Penrose inverse.

The received scalar signal at the output of the beamformer is given by the expression;

\[ y_{e(k)}^{ZF} = w_{e(k)}^{ZF} v_{(k)} \]

Substituting the expressions for \( w_{e(k)}^{ZF} \) and \( v_{(k)} \),

\[ y_{e(k)}^{ZF} = \left( H_{e(k)}^H \right)^H t_{1(k)} \]

\[ y_{e(k)}^{ZF} = t_{1(k)}^H H_{e(k)}^+ \left[ H_{e(k)} \sqrt{\rho(k)} \left( \sqrt{1 - \epsilon(k)} t_{1(k)} S_{(k)} + \sqrt{\epsilon(k)} \eta_{(k)} \right) + n_{e(k)} \right] \]

\[ y_{e(k)}^{ZF} = \sqrt{\rho(k)} \sqrt{1 - \epsilon(k)} S_{(k)} t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} + \sqrt{\rho(k)} \sqrt{\epsilon(k)} t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \]

\[ y_{e(k)}^{ZF} = \sqrt{\rho(k)} \sqrt{1 - \epsilon(k)} S_{(k)} t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} + \sqrt{\rho(k)} \sqrt{\epsilon(k)} t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \]

Therefore, \( y_{e(k)}^{ZF} = \sqrt{\rho(k)} \sqrt{1 - \epsilon(k)} S_{(k)} t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} + \sqrt{\rho(k)} \sqrt{\epsilon(k)} t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \)

\[ SNR_{e(k)}^{ZF} = \frac{\mathbb{E} \left[ \sqrt{\rho(k)} \sqrt{1 - \epsilon(k)} S_{(k)} t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} \right]^2}{\mathbb{E} \left[ t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \right]^2} \]

\[ SNR_{e(k)}^{ZF} = \frac{\rho(k)(1 - \epsilon(k)) \left( H_{e(k)}^+ \right)^H t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} \mathbb{E} \left[ S_{(k)} \right]^2}{\mathbb{E} \left[ t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \right]^2} \]

\[ H_{e(k)}^+ H_{e(k)} = I \quad H_{e(k)}^+ \left( H_{e(k)}^+ \right)^H = I \]

\[ SNR_{e(k)}^{ZF} = \frac{\rho(k)(1 - \epsilon(k)) \left( H_{e(k)}^+ \right)^H t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} \mathbb{E} \left[ S_{(k)} \right]^2}{\mathbb{E} \left[ t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \right]^2} \]

\[ SNR_{e(k)}^{ZF} = \frac{\rho(k)(1 - \epsilon(k)) \left( H_{e(k)}^+ \right)^H t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} \mathbb{E} \left[ S_{(k)} \right]^2}{\mathbb{E} \left[ t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \right]^2} \]

\[ SNR_{e(k)}^{ZF} = \frac{\rho(k)(1 - \epsilon(k)) \left( H_{e(k)}^+ \right)^H t_{1(k)}^H H_{e(k)}^+ H_{e(k)} t_{1(k)} \mathbb{E} \left[ S_{(k)} \right]^2}{\mathbb{E} \left[ t_{1(k)}^H H_{e(k)}^+ n_{e(k)} \right]^2} \]
\[
\text{SNR}_{e(k)ZF} = \frac{\rho(k) \left( 1 - \epsilon(k) \right)}{\sigma_e^2(k) t_1^H(k) H_e^H(k) \left( H_e^H(k) \right)^H t_1(k)}
\]

Let \( \Phi = \left[ \sigma_e^2(k) t_1^H(k) H_e^H(k) \left( H_e^H(k) \right)^H t_1(k) \right]^{-1} \)

Therefore,

\[
\text{SNR}_{e(k)ZF} = \rho(k) \left( 1 - \epsilon(k) \right) \Phi
\]

For \( N_e < N_t \),

\[
y_{e(k)ZF} = \sqrt{\rho(k)} \sqrt{1 - \epsilon(k)} s(k) t_1^H(k) H_e^H(k) H_e(k) t_1(k) + \sqrt{\rho(k)} \sqrt{\epsilon(k)} t_1^H(k) H_e^H(k) H_e(k) \eta(k) + t_1^H(k) H_e^H(k) n_e(k)
\]

\[
\text{SNR}_{e(k)ZF} = \frac{E \left[ \sqrt{\rho(k)} \sqrt{1 - \epsilon(k)} s(k) t_1^H(k) H_e^H(k) H_e(k) t_1(k) \right]^2}{E \left[ \sqrt{\rho(k)} \sqrt{\epsilon(k)} t_1^H(k) H_e^H(k) H_e(k) \eta(k) \right]^2 + E \left[ t_1^H(k) H_e^H(k) n_e(k) \right]^2}
\]

\[
\text{SNR}_{e(k)ZF} = \frac{\rho(k) \left( 1 - \epsilon(k) \right) \left| t_1^H(k) H_e^H(k) H_e(k) t_1(k) \right|^2 E \left| s(k) \right|^2}{\epsilon(k) \rho(k) H_e^H(k) \left( H_e^H(k) \right)^H t_1(k) t_1^H(k) H_e^H(k) H_e(k) E \left| \eta(k) \right|^2 + \left( H_e^H(k) \right)^H t_1(k) t_1^H(k) H_e^H(k) E \left| n_e(k) \right|^2}
\]

\[
\text{SNR}_{e(k)ZF} = \frac{\rho(k) \left( 1 - \epsilon(k) \right) \left| t_1^H(k) H_e^H(k) H_e(k) t_1(k) \right|^2}{t_1^H(k) H_e^H(k) \left[ \rho(k) \epsilon(k) H_e^H(k) C_\eta(k) H_e(k) + \sigma_e^2(k) I \right] \left( H_e^H(k) \right)^H t_1(k)}
\]
APPENDIX VI
Some Linear Algebra Fundamentals

Eigen Value Decomposition (EVD) and Singular Value Decomposition (SVD)

Let $A \in \mathbb{R}^{m \times m}$ be a square and diagonalizable. A vector $v \in \mathbb{C}^m$ which is non-zero and a scalar $\lambda \in \mathbb{C}$, satisfying $Av = \lambda v$ are called the eigenvectors and eigenvalues of $A$ respectively. The eigenvectors can also be characterised by a non-trivial solution of the homogenous system of linear equation of:

$$p(\lambda) = \det(A - \lambda I) = 0 \implies (A - \lambda I) \text{ is singular}$$

where $p(\lambda)$ is the $m$th order polynomial in $\lambda$ called the characteristics polynomial of $A$.

Zero-eigenvalues are special in that they can only occur in rank-deficient and non-invertible matrices. Therefore, there associated non-zero eigenvectors must lie in the nullspace of $A$.

Let $T \in \mathbb{R}^{m \times m}$ be a matrix whose columns are the eigenvectors of (i.e.) $T = (v_1, v_2, ... v_m)$ and $A = \text{diag}(\lambda_1, \lambda_2, ... \lambda_m)$ a diagonal matrix holding the corresponding eigenvalues. Then we can write:

$$AT = TA$$

Assuming $A$ has $m$ independent eigenvectors and $T$ is invertible,

$$A = T\Lambda T^{-1}$$

The expression above is called the eigen value decomposition (EVD) or spectral factorization of $A$. SVD decomposes a matrix $A \in \mathbb{R}^{m \times m}$ into the product of two orthonormal matrices, $U \in \mathbb{R}^{m \times m}$ and $V \in \mathbb{R}^{m \times m}$ and a pseudo-diagonal matrix $\Sigma = \text{diag}(\sigma_1, \sigma_2, ... \sigma_p) \in \mathbb{R}^{m \times m}$, with $p = \min(m, n)$ such that all components except the first diagonal are zero. Therefore,

$$A_{m \times n} = U_{m \times m}\Sigma_{m \times n}V_{n \times n}^T = \sum_{i=1}^{p} \sigma_i u_i v_i^T \text{ and } p = \min(m, n)$$

where the diagonal elements of $\Sigma$ are called the singular values which are always non-negative, $u_i$ are the columns of $U$ and referred to as the left singular vectors, and $v_i^T$ are the columns of $V$ and referred to as the right singular vectors.

$$Av_i = \sigma_i u_i , Au_i^T = \sigma_i v_i^T \text{ where } 1 \leq i \leq p$$

$(A^TA)v_i = \sigma_i^2 v_i$ , $A^TA$ has $n$ eigenvalues and $\sigma_i^2$ are the largest eigenvalues of $A^TA$.

$(AA^T)u_i = \sigma_i^2 u_i$ , $AA^T$ has $m$ eigenvalues and $\sigma_i^2$ are the largest eigenvalues of $AA^T$.

Therefore,

$$A^TA = V\Sigma^TU^TU\Sigma V^T = V(\Sigma \Sigma)V^T$$

$$AA^T = U\Sigma V^TV\Sigma U^T = U(\Sigma \Sigma)U^T$$

From
\[ A_{m \times n} = U_{m \times m} \Sigma_{m \times n} V_{n \times n}^T = \sum_{i=1}^{p} \sigma_i u_i v_i^T \quad \text{and} \quad p = \min(m, n) \]

If \( m \geq n \implies p = n \), then \((A^T A)x_i = \lambda_i x_i \) \quad i = 1, 2, 3, \ldots n

\[ v_i = x_i, \quad \sigma_i = \sqrt{\lambda_i} \quad \text{i} = 1, 2, 3, \ldots p \]

Also, \((A A^T)y_i = \lambda_i y_i \) \quad i = 1, 2, 3, \ldots m

\[ u_i = y_i, \quad \sigma_i = \sqrt{\lambda_i} \quad \text{i} = 1, 2, 3, \ldots p \quad \text{and} \quad u_i = y_i, \quad \lambda_i = 0, \quad i = p + 1, p + 2, p + 3, \ldots m \]

If \( m < n \implies p = m \), then \((A^T A)x_i = \lambda_i x_i \) \quad i = 1, 2, 3, \ldots n

\[ v_i = x_i, \quad \sigma_i = \sqrt{\lambda_i} \quad \text{i} = 1, 2, 3, \ldots p \quad \text{and} \quad v_i = x_i, \quad \lambda_i = 0, \quad i = p + 1, p + 2, p + 3, \ldots n \]

Also, \((A A^T)y_i = \lambda_i y_i \) \quad i = 1, 2, 3, \ldots m \quad \text{and} \quad u_i = y_i, \quad \sigma_i = \sqrt{\lambda_i} \quad \text{i} = 1, 2, 3, \ldots p

SVD clearly constructs the orthonormal bases of range and nullspace of \( A \). If the range space of \( A \) is defined by the vector \( r \), then all vectors \( r = Ax \) that can be obtained as the linear combination of the columns of \( A \), lie in the span of the first \( p_o \) column of \( U \). On the other hand, if \( w \) defines all vectors in the null space of \( A \), then all vectors satisfying \( Ax = 0 \) must be orthogonal to the first column \( p_o \) of \( V \). These are the rows non-zero singular values of \( V^T \). We can therefore conclude that \( w \) lies in the subspace spanned by the last \( (n - p_o) \) columns of \( V \) which are the nullspace of \( A \) i.e \( v_{p_o+1} \ldots v_n \) forms the orthonormal basis of the nullspace of \( A \). (Ref: Melzer, T. (2004) SVD and its Application to Generalized Eigenvalue Problems. p.1 -15.)