Master of Science in Telecommunication Systems
January 2024

Physical Layer Security for MIMO Transmission of Short Packet Communications

Varun Duvva
Bharath Reddy Anugu

Faculty of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Telecommunication Systems. The thesis is equivalent to Weeks weeks of full time studies.

The authors declare that they are the sole authors of this thesis and that they have not used any sources other than those listed in the bibliography and identified as references. They further declare that they have not submitted this thesis at any other institution to obtain a degree.

Contact Information:
Author(s):
Varun Duvva
E-mail: vadv21@student.bth.se

Bharath Reddy Anugu
E-mail: bhan21@student.bth.se

University advisor:
Mrs.Thi My Chin Chu
Department of Department of Computer Science

Faculty of Computing
Blekinge Institute of Technology
SE–371 79 Karlskrona, Sweden

Internet	:	www.bth.se
Phone	:	+46 455 38 50 00
Fax	:	+46 455 38 50 57

Abstract

This thesis explores the practical application of Physical Layer Security (PLS) in Multiple-Input Multiple-Output (MIMO) systems, particularly focusing on Short Packet Communication (SPC). The aim is to enhance the security of wireless communications against eavesdropping threats. By employing advanced techniques such as Maximum Ratio Transmission (MRT) and Maximum Ratio Combining (MRC), along with Beamforming, the study demonstrates how these methods can significantly strengthen the signal integrity in MIMO systems.

In developing a comprehensive system model that integrates PLS into MIMO, the research provides a dual approach of evaluation. Rigorous theoretical analysis coupled with MATLAB simulations are utilized to validate the effectiveness of the proposed model. These methods not only underscore the feasibility of PLS in real-world applications but also highlight the potential improvements in wireless communication security, offering a valuable contribution to the field.

Keywords: Physical Layer Security, Multiple-Input Multiple-Output, Short Packet communication, Maximum Ratio Combining, Maximum Ratio Transmission, and Beamforming

Acknowledgments

We extend our heartfelt gratitude to Dr. Thi My Chinh Chu, our dedicated thesis supervisor. Her unwavering support and invaluable guidance have played an indispensable role in the successful completion of our study. Collaborating with her has not only been an honor but also a continuous source of inspiration throughout our research journey. Dr. Chu's relentless advice and constructive feedback have been instrumental in helping us overcome various challenges and obstacles.

We would also like to express our profound appreciation to our family and friends for their unwavering support and encouragement. Their belief in us has been a driving force in our academic endeavors.

Furthermore, we would like to acknowledge the exceptional quality of instruction and commitment to nurturing student success at BTH, which has significantly contributed to our growth and achievement.

Contents

List of Figures

List of Abbreviations

AN	Artificial Noise
BLER	Block Erorr Rate
CDF	Cumulative Distribution Function
CSI	Channel State Information
IoT	Internet of Things
ML	Machine Learning
MIMO	Multiple Input Multiple Output
MRT	Maximum Ratio Transmission
MRC	Maximum Ratio Combining
MISO	Multiple-Input Single-Output
NLOS	Non-Line-of-Sight
PDF	Probability Distribution Function
PLS	Physical Layer Security
SC	Selection Combining
SPC	Short Packet Communication
SNR	Signal-to-Noise Ratio
SISO	Single-Input Single-Output
SIMO	Single-Input Multiple-Output
TAS	Transmit Antenna Selection
URLLC	Ultra-Reliable and Low-Latency Communication

Chapter 1

Introduction

1.1 Wireless Communication

Wireless communication can be traced back to the late 19th century. This initial foray into wireless technology led to the development of the first generation of wireless communications (1G) in the 1980s, which was characterized by analog transmission and used primarily for voice communication.

The evolution from 1G to 2G marked the transition from analog to digital communications, introduced text capabilities, and paved the way for more efficient and secure data This period also saw the advent of 2.5G and 3G, increased data numbers, and multimedia services [1]. It was important in the emergence of Internet usage and video calling activity.

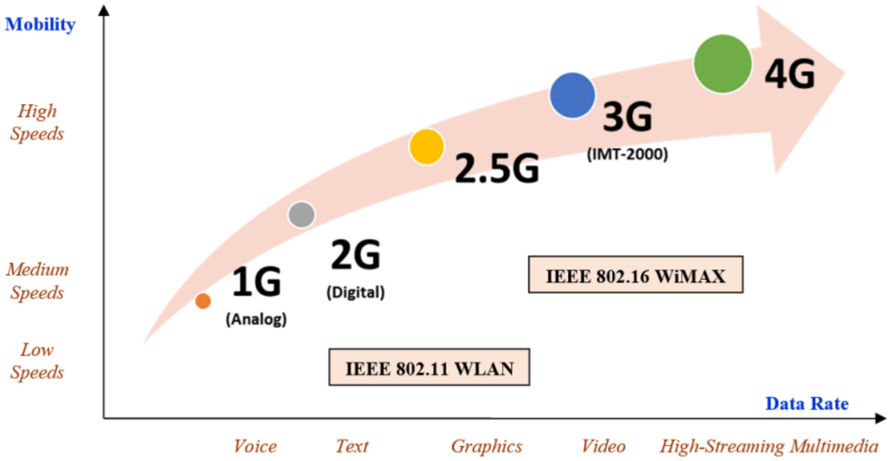

Figure 1.1: Evolution of Wireless Communication

Figure 1.1 encapsulates this historical progression, highlighting the milestones in wifi conversation generation from 1G via 4G [2]. The x-axis represents growing record prices, signifying the boom in the quantity of statistics that can be transmitted in keeping with units of time. The y-axis illustrates mobility, indicating the potential to maintain incredible conversation across various speeds of consumer movement. Each era is marked by its ability to deal with one-of-a-kind types of media, from voice and text in the younger generations to pictures, video, and high-streaming multimedia in the later generations [2].

With the arrival of 4G, a full-size tower turned into a finished wireless communication generation, presenting customers with a mobile broadband network to get into. This generation introduced the Multiple Input Multiple Output (MIMO) era, which utilizes multiple antennas at both the transmitter and receiver to improve communication's overall performance. MIMO lets in higher record fees and more dependable transmission, which is vital for the bandwidth-intensive packages that have grown to be indispensable to trendy life, which include streaming high-definition videos and engaging in excessive-velocity cell gaming [3].

Security is a major concern in wireless communication because, unlike wired connections, where the transmission medium can be physically protected, wireless signals are broadcast through the air and can be intercepted by unauthorized parties. Because wireless communication is so prevalent, especially with the rising ubiquity of smartphones, Internet of Things (IoT) devices, and mobile Internet services, a massive quantity of sensitive data is continually exchanged. This data includes personal conversations, financial activities, and sensitive health and vital infrastructure information. It is critical to preserve confidence, safeguard privacy, and secure economic and national interests by ensuring this information's integrity, confidentiality, and availability. As a result, robust encryption, safe authentication procedures, and advanced security algorithms must be included in the architecture of modern wireless communication systems to mitigate the risks of eavesdropping, data theft, and unauthorized access [4].

1.2 Fading

In wireless communications, fading is a fundamental phenomenon that describes the variation of received signal strength over time due to multiple propagation paths. It is an important factor that affects the performance and design of wireless systems, as it can cause signal amplitude and phase fluctuations, consequently reducing communication and quality, which can be degraded by various factors such as the physical environment, user mobility, and inherent characteristics of radio wave propagation. There are two different fading techniques used in our work [5]. Figure 1.2 below shows the classification of fading [6].

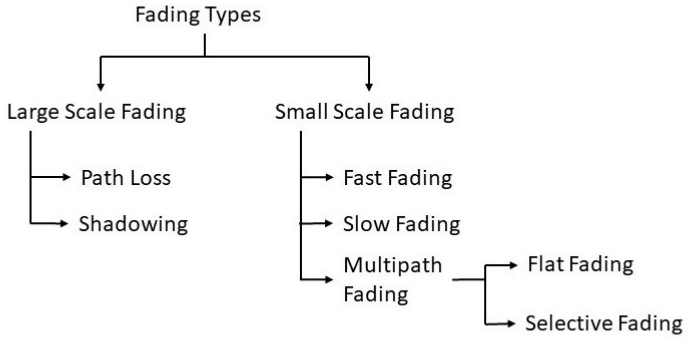

Figure 1.2: Types of Fading

1.2.1 Large Scale Fading

The attenuation or loss of a radio signal during long-distance propagation is referred to as large-scale fading. The main causes of it include things like free-space path loss, which happens as the signal spreads out as it gets farther away from the transmitter. Obstacles that can attenuate or disperse the signal include topography, buildings, and atmospheric conditions. To lessen the effects of large-scale fading and guarantee dependable signal transmission over long distances, wireless communication systems must employ strategies including power regulation, diversity reception, and the use of numerous antennas [7].

1.2.2 Small Scale Fading

The term "small-scale fading" describes the abrupt changes in a radio signal's amplitude, phase, or frequency that occur when it experiences multi-path propagation over short distances. A signal between the transmitter and the receiver might take many pathways when it comes into contact with different reflecting surfaces [8]. The signals that arrive at the receiver may interfere either constructively or destructively due to the differences in the length of these routes.

1.2.3 Types of Fading

- **Rayleigh Fading**
  Rayleigh Fading is typically used to model environments where there's no line of sight between the transmitter and receiver and the signal has been contemplated using multiple surfaces earlier than accomplishing the receiver. The received sign's amplitude is characterized by a Rayleigh distribution [9]. The Probability Distribution Function (PDF) of the received signal amplitude r in Rayleigh fading can be expressed as [10]

$$p(r) = \begin{cases} -\frac{r}{2\sigma^2} exp\left(-\frac{r^2}{2\sigma^2}\right), & 0 \leq r \leq \alpha \\ 0, & \text{r} < 0 \end{cases} \tag{1.1}$$

  where σ is $r_r ms (r_r ms$ is square root of mean value) value of received signal, σ^2 time average power of received signal. Cumulative Distribution Function (CDF) of rayleigh distribution is given by [10],

$$P(r) = 1 - \exp\left(-\frac{r^2}{2\sigma^2}\right) \tag{1.2}$$

  The mean of rayleigh distribution is given by [10],

$$E[r] = \sigma\sqrt{\frac{\pi}{2}} \tag{1.3}$$

  Rayleigh Fading is chosen for the main channel to accurately represent Non-Line-of-Sight (NLOS) conditions typical in urban environments and indoors, where signals undergo multiple reflections. This model is effective in depicting the statistical nature of wireless channels with no dominant signal path, using the gamma distribution to realistically simulate the channel's fading severity and mean power. This approach ensures a realistic portrayal of typical wireless communication scenarios, essential for analyzing system performance.

- **Nakagami-m Fading**

  Nakagami-m fading is another statistical model used to symbolize a huge variety of fading conditions, from intense fading environments (like Rayleigh) to much less intense and even line-of-sight situations [10]. The pdf of the received sign amplitude r for Nakagami-m fading is given by

$$f(r) = \frac{2m^m r^{2m-1}}{\Gamma(m)\Omega^m} e^{-\frac{m}{\Omega}r^2} \tag{1.4}$$

  where m is the fading parameter, Ω is the average power of the received signal, and $\Gamma(m)$ is the gamma function for m.

  Nakagami-m Fading is used for the eavesdropper channel due to its flexibility in modeling a wide range of fading conditions. This choice allows for a more accurate representation of various eavesdropping scenarios, which might differ significantly from the main channel's environment. Employing Nakagami-m Fading enables a nuanced analysis of the system's security aspects, like secrecy capacity, under diverse and realistic conditions, providing valuable insights into the system's robustness against eavesdropping.

1.3 Multiple Input Multiple Output Wireless Communications

In the realm of wireless communication, MIMO, or Multiple-Input Multiple-Output, stands as a transformative technology that has revolutionized the efficiency and performance of wireless systems. At its core, MIMO harnesses the power of multiple antennas at both the transmitting and receiving ends of a communication link. This departure from traditional single-antenna systems unlocks a wealth of possibilities, offering significant improvements in data rates, reliability, and spectral efficiency. The key principle of MIMO lies in exploiting spatial diversity. Unlike conventional systems where a single antenna handles data transmission, MIMO systems utilize multiple antennas to simultaneously transmit or receive multiple data streams. This spatial diversity allows MIMO to combat challenges like signal fading and interference, significantly enhancing the quality of wireless communication [3]

MIMO technology has found widespread application across various communication standards, including Wi-Fi, cellular networks, and emerging technologies like 5G. By intelligently managing multiple streams of data, MIMO enables faster data rates, more reliable connections, and improved utilization of available bandwidth. In essence, MIMO has become a cornerstone technology, propelling wireless communication into a new era of efficiency and performance. Its impact is felt in everyday

technologies, from the seamless streaming of high-definition content to the reliable connectivity of mobile devices, illustrating the pervasive influence of MIMO in our interconnected world [3].
Physical Layer Security (PLS) is especially critical in MIMO communication systems, where the increased capabilities and complexity of using many antennas for both transmitting and receiving pose security concerns. Because MIMO systems are frequently used to transmit huge amounts of sensitive data in high-throughput applications, the inherent weaknesses of wireless channels, which are vulnerable to interception and unauthorized access, demand sophisticated security measures. PLS takes advantage of the wireless medium's particular qualities, like as channel noise and fading, to protect data transmission at the most fundamental level. This strategy is critical for protecting communication, especially in situations when standard cryptographic approaches may be insufficient, preserving the privacy and integrity of information in an increasingly wireless and networked world [11].

1.3.1 Different Models of MIMO System

These MIMO systems come in a variety of configurations. Several configurations each have their own set of pros and drawbacks. So, in this thesis, we will go over the various forms.MIMO systems with examples of how each format affects the system's efficiency.

- **Single-Input Single-Output**

  It is the simplest MIMO system format. Single-Input Single-Output (SISO) is a radio system with a single antenna on both the transmitter and receiving sides. Because there is no need for variety, this system suffers from fading and interference [12].
  The channel capacity of SISO is given by [13]

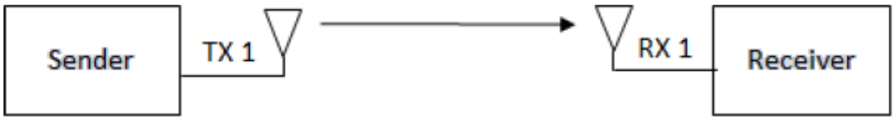

Figure 1.3: SISO System

$$C_{\text{SISO}} = B\log_2\left(1+\frac{S}{N}\right) \tag{1.5}$$

Where, C_{SISO} is the capacity of the SISO system, B is the Bandwidth of the signal and $\frac{S}{N}$ is the Signal-to-Noise Ratio (SNR).

- **Single-Input Multiple-Output**

There is a single transmit antenna and multiple receiving antennas. This Single-Input Multiple-Output (SIMO) is also known as receive diversity. This SIMO system is simple to construct and suitable for a wide range of applications. The primary use of this SIMO is mobile communications, in which the base station (BS) serves as a transmitter and the mobile phones serve as receivers (uplink). Because it is difficult to install multiple antennas, especially of small size, in mobile devices, SIMO is limited in both price and size [12].

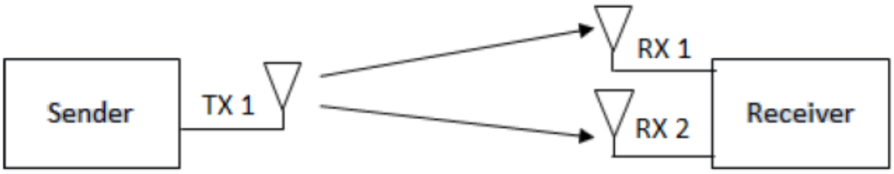

Figure 1.4: SIMO System

The channel capacity of SIMO is given by [13]

$$C_{\text{SIMO}} = M_r \log_2\left(1 + \frac{S}{N}\right) \tag{1.6}$$

Where C_{SIMO} is the capacity of the SIMO system, M_r is the number of receiving antennas and $\frac{S}{N}$ is the SNR.

- **Multiple-Input Single-Output**

There are multiple transmit antennas and a single receiving antenna. Transmit Diversity is another name for this Multiple-Input Single-Output (MISO). This technique is utilized in mobile communications, where the base station receives data from various mobile devices. When compared to SIMO systems, this has no size or cost limits [12].
The channel capacity of MISO is given by [13]

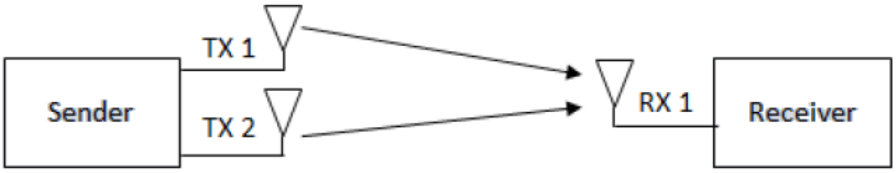

Figure 1.5: MISO System

$$C_{\text{MISO}} = M_t \log_2\left(1 + \frac{S}{N}\right) \tag{1.7}$$

Where C_{MISO} is the capacity of the MISO system, M_t is the number of receiving antennas, and $\frac{S}{N}$ is the SNR.

- **Multiple-Input Multiple-Output**

  It is a system where there are multiple transmit antennas and multiple receive antennas. This system is an expansion of the MISO systems that can contain N numbers of transmit and receive antennas. This MIMO system is used to improve channel robustness and channel capacity [12]. The channel capacity of MIMO system [13]

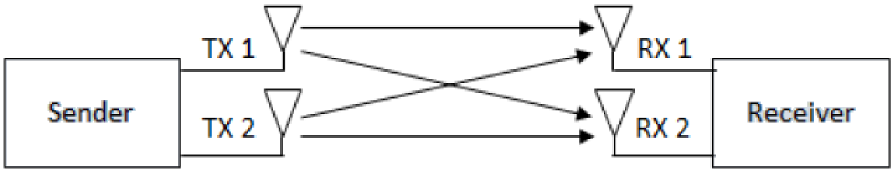

Figure 1.6: MIMO System

$$C_{\text{MIMO}} = M_t M_r \log_2 \left(1 + \frac{S}{N}\right) \tag{1.8}$$

  Where C_{MIMO} is the capacity of the MIMO system, M_t and M_r are the number of transmit and receive antennas, and $\frac{S}{N}$ is the SNR.

1.3.2 MIMO Transmission Techniques

In wireless communication, the quest for higher data rates, improved reliability, and efficient use of available resources has given rise to sophisticated transmission techniques within MIMO systems. There are two main transmitting techniques that are Maximum Ratio Transmission (MRT) and Transmit Antenna Selection (TAS).

- **Maximum Ratio Transmission**

  MRT is a MIMO transmission technology that optimizes transmission by utilizing Channel State Information (CSI). It modifies the phases and amplitudes of signals sent by numerous antennas such that they constructively merge at the receiver, leveraging the diversity given by multiple antennas. This strategy seeks to maximize the received signal power, hence enhancing the dependability and quality of the communication channel [14].

- **Transmit Antenna Selection**

  TAS is a MIMO transmission technique designed to enhance the efficiency of data transmission by judiciously selecting the antennas at the transmitter. In a MIMO system equipped with multiple antennas, TAS involves choosing a subset of antennas for transmitting data based on certain criteria. The selection is dynamically adjusted to optimize the transmission for current channel conditions [15].

In this research, MRT was chosen as the transmitting technique for its ability to optimize transmission using CSI. MRT effectively modifies the phases and amplitudes of signals from multiple antennas to ensure they constructively merge at the receiver. This method leverages the diversity of multiple antennas to maximize the received signal power, thereby enhancing both the dependability and quality of the communication channel.

1.3.3 MIMO Receiving Techniques

There are two main Receiving techniques in the MIMO system are Maximum Ratio Combining (MRC) and Selection Combining (SC).

- **Maximum Ratio Combining**
  On the receiving end of a MIMO system, the MRC technique is employed to maximize the strength of the received signals. In MRC, the signals from multiple receive antennas are combined with different weights, and these weights are adjusted to maximize the SNR of the combined signal [16].

- **Selection Combining**
  Selection combining is a diversity technique that improves signal quality and reliability by selecting and utilizing the strongest or best signal from multiple available antennas at the receiver [16].

In this thesis, MRC was selected as a receiving technique in MIMO systems due to its efficacy in maximizing the strength of received signals. By combining signals from multiple antennas with carefully adjusted weights, MRC significantly enhances the SNR of the received signal. This approach not only improves signal quality but also contributes to achieving high secrecy capacity.

1.4 Short Packet Communication

Short Packet Communication (SPC) in the context of 5G networks is designed to address the demands of Ultra-Reliable and Low-Latency Communication (URLLC), particularly useful for the IoT and mission-critical applications. In SPC, data is transmitted in small-sized packets to ensure minimal latency and high reliability, a significant deviation from traditional methods that emphasize large packet sizes for efficiency [17].

Incorporating SPC in MIMO systems enhances capacity and reliability, leveraging the spatial diversity of MIMO to counteract the high error rates typically associated with short packets [18].

PLS becomes crucial in SPC to safeguard against eavesdropping and other security threats. This is especially relevant in URLLC scenarios, where data integrity and confidentiality are paramount. PLS mechanisms can provide an additional layer of protection by exploiting the physical properties of the wireless channel, thus enhancing the overall security of short packet transmissions in 5G networks [17].

The integration of these technologies aims to meet the stringent requirements of URLLC, ensuring not only rapid and reliable communication but also high levels of security, essential for emerging applications in 5G networks.

1.5 Eavesdropper

In the context of wireless communication, an eavesdropper is an unauthorized party that intercepts and possibly decodes signals intended for authorized receivers, hence posing a serious risk to the communication's secrecy and integrity. The open-air aspect of wireless transmission, where signals can travel beyond the intended recipient and be available to anybody with the correct equipment, makes eavesdroppers a particularly serious obstacle. PLS, which is intended to protect against such attacks by making use of the intrinsic characteristics of the communication channel itself, is necessary in light of this vulnerability.PLS methods like noise exploitation and channel-aware encoding are designed to make sure that the data is safe even if an eavesdropper intercepts the signal, thereby maintaining the privacy and security of data in an environment where traditional encryption methods alone may not suffice [19].

1.6 Physical Layer Security

PLS is a strategic shift in wireless communication security that leverages the naturally random nature of the communication channel instead of depending only on encrypted codes. PLS attempts to secure data transfers at the physical layer by making use of the stochastic characteristics of wireless channels, such as noise, signal fading, and interference. With the exponential growth of wireless communication and the accompanying development in sophisticated eavesdropping capabilities, this technology is extremely important. PLS offers a strong defense against interception by adding an extra layer of security that works in conjunction with existing cryptographic techniques and, in certain cases, can function independently of them [20].

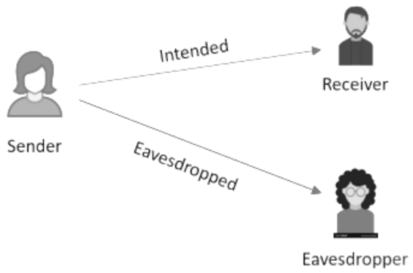

Figure 1.7: Typical Eavesdropper scenario

From Figure 1.7, we see a simplified depiction of a communication scenario where PLS plays a pivotal role. The sender sends out a signal meant for the authorized recipient, but there's a chance that an eavesdropper may intercept it. PLS makes use of strategies like channel variation and signal obfuscation to make sure the data gets to the right person while being incomprehensible to outsiders. PLS may considerably lessen the possibility that an eavesdropper will be able to decode the transmission by adjusting the signal's phase and amplitude, protecting the communication's anonymity.

To fully utilize the enhanced capabilities of MIMO technology, PLS must be included in the system. The MIMO's array of many antennas offers a large number of independent data transmission channels, which expands the potential applications of PLS. PLS benefits greatly from this spatial dimension, which is a feature of MIMO systems and enables the use of sophisticated methods like generated noise and spatial beamforming. By adapting the signal to the unique propagation characteristics of the targeted channel and adding an amount of uncertainty for potential eavesdroppers, these approaches are essential to protecting communication lines. The necessity to protect the increased data rates and enhanced communication capabilities from possible interception and unauthorized access is what motivates the use of PLS in MIMO. PLS can increase the secrecy rate by focusing the signal intensity at the receiver's position by making use of the multipath propagation and spatial diversity provided by MIMO. This deliberate focus on signal strength not only maximizes the quality of the signal received by the intended recipient but also greatly reduces the capacity of the eavesdropper to intercept the conversation, thereby making good use of the physical characteristics of the wireless channel to reinforce security [21].

PLS seems to be particularly beneficial for the transmission of SPC in MIMO systems. SPC is made to carry out small-scale data packet transmissions under high latency and reliability criteria, which is in accordance with the goals of URLLC [17], which is essential for vital applications such as telemedicine and driverless cars. PLS facilitates the achievement of high secrecy capacity and low block error rate, two essentials for quick and safe information sharing. Beamforming is a crucial PLS method in MIMO SPC that focuses the transmission beam on the target receiver, improving the quality of the signal for the receiver while making eavesdropping more difficult. Since beamforming is effective in concurrently enhancing the security and reliability of critical and time-sensitive communication, it is the selected PLS approach for MIMO SPC in this thesis.

1.6.1 Beamforming

In MIMO systems, beamforming is a signal processing method that maximizes the signal's focus on a particular receiver while reducing its reception by an eavesdropper. Beamforming uses the numerous antennas at the transmitter in a MIMO setting to control and steer the signal's phase and amplitude. Through this method, the signal strength and quality at the receiver position are successfully increased by creating a constructive interference pattern in the direction of the target receiver [22].

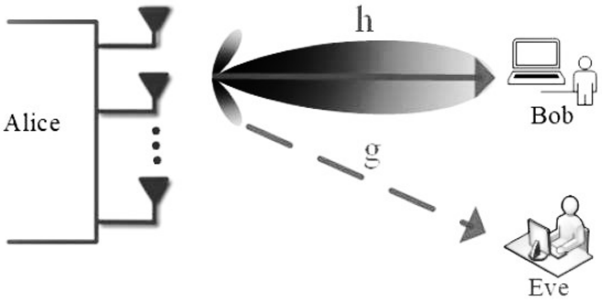

Figure 1.8: Beamforming

Figure 1.8 illustrates the concept of beamforming with Alice's multiple antennas directing a focused beam, indicated by 'h', towards Bob's receiver. To maximize the SNR at Bob's location, the system cleverly modifies the signals from each antenna such that they combine to produce a coherent wavefront at Bob's receiver. Concurrently, the method seeks to reduce the signal intensity in unintended directions, indicated by 'g', so lowering the signal quality that Eve can intercept. By reducing the possibility of eavesdropping, this strategic control over the directionality of the signal not only enhances communication with the intended recipient but also plays a vital role in preserving security in wireless communications.

1.7 Background

Our goal in this thesis is to investigate and improve the use of PLS in MIMO systems, with a specific focus on SPC. The integration of many essential wireless communication technology components is the primary objective of the research. MIMO systems, which are renowned for their spatial diversity and multiplexing capacities, are being deployed as part of this integration, along with the thoughtful application of beamforming techniques. Beamforming is crucial in this context as it facilitates targeted signal transmission, which is particularly advantageous in scenarios with potential eavesdropping threats. Furthermore, we employ MRT and MRC for transmitting and receiving techniques of MIMO. It is hypothesized that this dual implementation will reduce the possibility of eavesdropping and increase signal strength at the target receiver, hence optimizing the system's efficiency overall.

The methodology of this research comprises both theoretical analysis and practical simulation. Theoretical work involves computing performance parameters that are essential for evaluating PLS in MIMO systems, such as secrecy capacity and Block Erorr Rate (BLER). These measures contribute to our understanding of how PLS, particularly in SPC, might improve wireless communication security. There will be comprehensive simulations conducted with MATLAB and other tools to validate theoretical conclusions. The purpose of these simulations is to illustrate the signal intensity in terms of BLER and secrecy capacity. The thesis seeks to demonstrate how modern techniques such as beamforming in MIMO systems support secure wireless communications in SPC.

1.8 Motivation

Ensuring data transmission security is crucial in today's society, where wireless technology is prevalent. Eavesdroppers and new dangers present a challenge to conventional tactics. The desire to innovate by fusing MIMO transmission with MRT and MRC methodologies is the driving force behind this thesis. Short-packet communication is more efficient when MRT maximizes transmission and MRC improves reception. Adding Physical Layer Security creates an extra layer that strengthens integrity and secrecy. This fusion aspires to redefine secure, efficient wireless communication for the digital age.

1.9 Aim and Objectives

1.9.1 Aim

This thesis aims to investigate the implementation of physical layer security techniques to enhance the security of MIMO transmission of SPCs. Specifically, the study aims to explore the effectiveness of designing the beamforming vector for MRT and MRC of MIMO transmission for SPCs in PLS, in the presence of an eavesdropper. The ultimate goal is to identify the optimal combination of PLS and MIMO techniques that can provide reliable and secure communication for short packet transmissions in a wireless network.

1.9.2 Objectives

- Implementation of physical layer security for short packet communications.
- Designing an effective beamforming vector for MIMO transmission for short packet communications.
- Quantifying the performance of MIMO transmission of SPCs by deriving the mathematical expressions for BLER and secrecy capacity.
- Performing simulations to present the performance of the concerned system in MATLAB.

1.10 Research Questions

- **RQ1**: What is an effective transmission method to provide the secrecy capacity of MIMO transmission for SPC in the physical layer?
- **RQ2**: How are the transmitting and receiving beamforming vectors designed and optimized based on the channel condition to achieve low BLER and high secrecy capacity?
- **RQ3**: What are the mathematical expressions for the BLER and secrecy capacity of MIMO transmission for SPC in the PLS?
- **RQ4**: How can we simulate the performance of the system in Matlab and represent the results by plotting?

1.11 Outline of the Report

The structure of the thesis report is outlined as follows:

- **Chapter 1:** This chapter provides an introduction to the technologies employed in the research, encompassing the aim, objectives, and research questions, as well as the background information for the study and reasons for selecting the subject.

- **Chapter 2:** This chapter outlines the research methodology, incorporating elements such as a comprehensive literature review, theoretical analysis, simulation, performance evaluation, contributions, and an examination of related work.
- **Chapter 3:** In this chapter, the system design is presented along with detailed theoretical calculations of SNR, PDF, and CDF for both the receiver and the potential eavesdropper.
- **Chapter 4:** In this chapter, a performance analysis of the system is conducted, focusing on theoretical calculations for BLER and secrecy capacity.
- **Chapter 5:** In this chapter, the results obtained from MATLAB simulations are presented, showcasing the calculated BLER and secrecy capacity across various scenarios and cases.
- **Chapter 6:** In this chapter, an in-depth discussion is presented, addressing the outcomes concerning the challenging research questions posed earlier in the study.
- **Chapter 7:** This chapter provides the conclusions and gives a scope for future research in this area

Chapter 2

Methodology

2.1 Research Methodology

This section discusses the research method used to carry out the research, the literature review procedure, theoretical calculation, simulation, and performance evaluation.

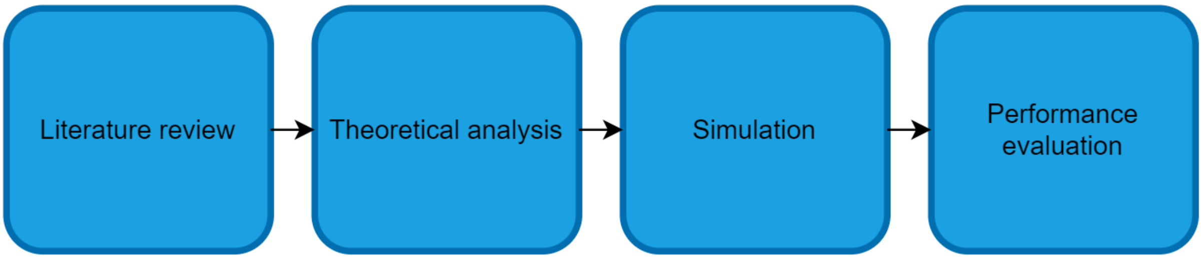

Figure 2.1: Methodology

2.1.1 Literature Review

We will perform a comprehensive review and literature review of the existing works on PLS, MIMO transmission techniques, and SPCs to see the landscape and achieve the background. This includes studying various research papers, conference proceedings, and textbooks to gain an understanding of the different techniques used in the field.

2.1.1.1 Data Sources

Our research predominantly utilized several authoritative and comprehensive databases to procure primary studies. These included academic databases such as IEEExplorer, Google Scholar, Diva Portal, and some science databases to determine the quality of the study.

2.1.1.2 Inclusion criteria

- Articles should be in English.
- Articles can be conference papers, journal articles, or books.
- Articles that are related to the current research are considered.

2.1.1.3 Exclusion Criteria

- Studies that are not associated with the research questions.
- Studies that are not written in the English language.
- Duplicate articles and repeated articles.
- Studies with unclear results and findings.

2.1.1.4 Work Division

At the outset, each author independently performed searches using various search engines to gather relevant articles. Subsequently, a collaborative effort ensued, with both authors pooling together the gathered papers. A mutual exchange of these papers between the authors was conducted to verify their relevance and filter out any that did not align with the research objectives. Throughout the process, both authors contributed equally to all facets of this work.

2.1.2 Theoretical Analysis

- **Importance of Theoretical Analysis:** Theoretical analysis is key for predicting system performance and guiding design in MIMO systems, especially in PLS and SPC, without extensive physical experimentation.
- **Mathematical Models and Equations:** Introduces mathematical frameworks for signal processing in MIMO systems, including BLER and secrecy capacity calculations.
- **Significance of BLER and Secrecy Capacity:** The importance of BLER is highlighted as a measure of system reliability, especially in SPC, where data transmission is brief and must be highly reliable. Similarly, the secrecy capacity is discussed as a vital metric for assessing the system's security capabilities against potential eavesdropping, which is central to PLS.
- **Computational Approach:** This section details the computational methods used for calculating these metrics, including the algorithms, assumptions, and any simulation tools employed. The step-by-step computational process provides clarity on how these metrics are derived from the mathematical models.
- **Implications of Theoretical Findings:** The section concludes by discussing how these theoretical findings can influence the design and optimization of MIMO systems for both efficiency and security in the context of PLS and SPC. This analysis is crucial for advancing the field of secure wireless communication.

2.1.3 Simulation

The simulation aspect is meticulously designed to complement the theoretical analysis. Using MATLAB, a series of simulations are conducted to empirically test the performance of MIMO systems in various scenarios relevant to PLS and SPC. These simulations help in visualizing the real-world applicability of the theoretical models, focusing on how different variables impact the system's performance. This approach not only validates the theoretical findings but also provides practical insights into the system's behavior under different conditions, which is crucial for developing robust and secure communication systems.

2.1.4 Performance Evaluation

The performance evaluation of MIMO systems for PLS and SPC is conducted through a blend of theoretical analysis and simulation studies. Theoretical analysis, involving mathematical modeling, provides insights into system performance under various theoretical conditions, focusing on metrics like BLER and secrecy capacity. Simulations, likely performed in MATLAB, complement this by offering empirical evidence and visualizing the system's performance in practical scenarios. This dual approach ensures a comprehensive evaluation, validating the theoretical models and offering practical insights for the advancement of secure and efficient wireless communication systems.

2.2 Related Work

In recent years, the field of PLS in MIMO systems, especially in the context of SPC, has witnessed significant advancements. Key studies have explored various aspects, including MIMO MRT/MRC techniques and beamforming.

The findings from the research paper [23], which delves into the complexities of MIMO systems in the context of SPC, are instrumental to my thesis. By offering a near estimate for the average BLER and a tight lower constraint on the average attainable rate in flat uncorrelated Rayleigh fading channels, this paper provides a crucial theoretical foundation. The utilization of Jensen's inequality and eigenvalue analysis of a Wishart matrix in their analytical approach, validated by closely matching simulations, offers valuable insights. This enhances the understanding of system performance in realistic scenarios, directly contributing to the robustness and applicability of the security techniques explored in our thesis work.

The research in [20] by Joseph R. Childress, focusing on the application of beamforming and Artificial Noise (AN) for enhancing security in MIMO wireless communication systems, is highly relevant to our work. The MATLAB simulations and analysis of various techniques in this study underscore the effectiveness of directing information signals toward the intended receiver while simultaneously degrading signal quality for potential eavesdroppers. This approach aligns with the objectives of our work to improve secure communication in MIMO systems, demonstrating practical strategies to safeguard against adversaries through the strategic use of beamforming and AN.

The study in [24] provides a valuable perspective for our thesis by examining the impact of an active eavesdropper on the secrecy performance of SPC. Their scenario, involving an eavesdropper with full-duplex capabilities capable of simultaneous eavesdropping and jamming, offers critical insights. The closed-form formula for secrecy outage probability and the Monte-Carlo simulations assessing system security against various jamming powers and eavesdropper proximities, contribute significantly to understanding and enhancing the security aspects in our research.

The paper cited as [25] is instrumental to our thesis, as it delves into optimizing beamforming for URLLC within cell-free massive MIMO systems. Their approach to solving the non-convex optimization problem, considering power and backhaul constraints, aligns with the objectives of our work. The user-centric techniques they develop and the demonstrated enhancement in system performance through simulations underscore the effectiveness of their beamforming architecture. This research provides pivotal insights into improving SPC, significantly contributing to the deployment of URLLC in next-generation wireless networks, a key focus of our thesis.

The research in [26] is crucial for our thesis as it investigates the enhancement of system performance in MIMO systems using MRT and MRC techniques under the assumption of perfect CSI. Their comparative analysis showing MIMO outperforming SISO, SIMO, and MISO configurations, especially with increasing antenna numbers, provides a strong theoretical basis for our work. The mathematical models they develop for outage probability and symbol error rate, supported by simulations, are pivotal in demonstrating how MRT and MRC can significantly improve the reliability and overall performance of MIMO systems, a central theme in our research.

The investigation of PLS in MIMO systems for SPC has advanced remarkably in the last several years. Important topics, including channel capacity and signal processing methods, have been covered in detail in the papers above. The books mentioned above provide an in-depth understanding of secure communication techniques and draw attention to issues like eavesdroppers and signal interference. By building on these basic findings, our research hopes to further the continuously developing area by addressing the optimization of security algorithms for effective data transmission in MIMO systems.

Chapter 3

System Model

MIMO refers to multiple antennas at the transmitter and receiver, which allow the data to be transmitted over multi-path propagation. We can implement MIMO by using MRTT and MRC at the transmitter and receiver, respectively. In the MRT technique, the signal is sent from all transmit antennas with different weights based on the channel condition. In the MRC technique, the received signals are combined at the receiver over the different channels are combined at the receiver with different weights.

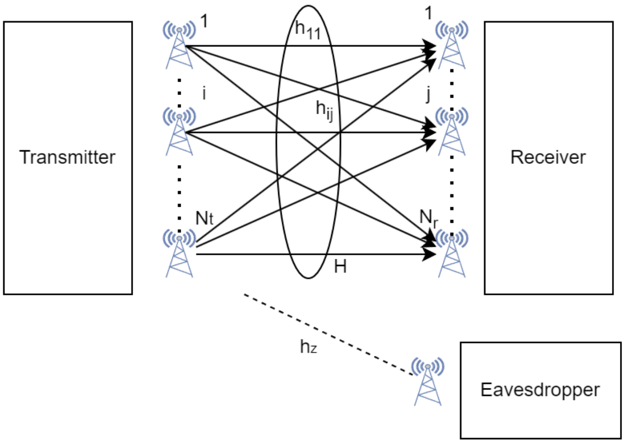

Figure 3.1: System model of MIMO transmission

3.1 Signal Expression

We consider a MIMO with N_t transmitting antennas and N_r receiving antennas. MRT technique is applied at the transmitter to transmit signal x using beam stearing vector $\mathbf{v}$ with size $N_t \times 1$. The received signal at the receiver is given by.

$$\mathbf{y} = \sqrt{P}\mathbf{H}\mathbf{v}x + \mathbf{n} \tag{3.1}$$

where $\mathbf{y}$ is the receiving signal vector over N_r antennas at the receiver with size $N_r \times 1$. Furthermore, $\mathbf{H}$ denotes the channel matrix with size $N_r \times N_t$, $\mathbf{n}$ denotes Gaussian noise with size $N_r \times 1$, and P is the total power transmitted at the transmitter.

Finally, based on the principle of the MRT, the beam stearing vector is selected as an eigenvector corresponding to the largest value of the Wishart matrix. i.e.,

$$\mathbf{H}^{+}\mathbf{H}\mathbf{v} = \lambda_{\max}\mathbf{v} \tag{3.2}$$

where $\lambda_{\max}$ is the largest value in the Wishart matrix $\mathbf{H}^{+}\mathbf{H}$.The received signal after using the MRT technique at the receiver is obtained as

$$\overline{s} = \mathbf{w}\mathbf{y} \tag{3.3}$$

where $\mathbf{w}$ is a weighting vector with size $1\times$ N_r at the receiver. Based on the principle of MRC, the weighting vector is selected to achieve the maximum SNR.

$$\mathbf{w} = (\mathbf{H}\mathbf{v})^{+} = \mathbf{v}^{+}\mathbf{H}^{+} \tag{3.4}$$

Thus, the combined signal at the receiver is obtained by substituting 3.1 and 3.4

$$\overline{s} = \mathbf{v}^{+}\mathbf{H}^{+}(\sqrt{P}\mathbf{H}\mathbf{v}x + \mathbf{n}) \tag{3.5}$$

$$\overline{s} = \sqrt{P}\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v}x + \mathbf{v}^{+}\mathbf{H}^{+}\mathbf{n} \tag{3.6}$$

The instantaneous SNR at the receiver is obtained as,

$$\gamma_R = \frac{(\sqrt{P}|\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v}x|)^2}{|\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{n}|^2} \tag{3.7}$$

$$\gamma_R = \frac{P(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v}x)(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v}x)^{+}}{(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{n})^{+}(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{n})} \tag{3.8}$$

$$\gamma_R = \frac{P(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v}xx^{+}\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v})}{(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{n}\mathbf{n}^{+}\mathbf{v}^{+}\mathbf{H}^{+})} \tag{3.9}$$

We know that x is the transmit signal with unit power, i.e., $E|xx^{+}| = 1$, $E|\mathbf{v}\mathbf{v}^{+}| = 1$ and $E|\mathbf{n}\mathbf{n}^{+}| = N_0$. Thus, the SNR at the receiver is obtained as

$$\gamma_R = \frac{P(\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v}\mathbf{v}^{+}\mathbf{H}^{+}\mathbf{H}\mathbf{v})}{(\mathbf{v}^{+}\mathbf{H}^{+}N_0\mathbf{v}\mathbf{H})} \tag{3.10}$$

substituting (3.2) in (3.10), we can rewrite the SNR as

$$\gamma_R = \frac{(P\mathbf{v}^{+}\lambda_{\max}\mathbf{v}\mathbf{v}^{+}\lambda_{\max}\mathbf{v})}{(\mathbf{v}^{+}\lambda_{\max}N_0\mathbf{v})} \tag{3.11}$$

$$\gamma_R = \frac{P\lambda_{\max}^2}{\lambda_{\max}N_0} \tag{3.12}$$

$$\gamma_R = \frac{P\lambda_{\max}}{N_0} \tag{3.13}$$

$$\gamma_R = \gamma_{\max}\bar{\gamma}, \quad \bar{\gamma} = \frac{P}{N_0} \tag{3.14}$$

3.1.1 Statistic Derivation Functions of γ_R

By definition, the CDF of γ_R is given by [27]

$$F_\gamma(\gamma) = P_{\mathrm{r}}\{\gamma_{\mathrm{R}} \leq \gamma\} \tag{3.15}$$

$$F_{\gamma_{\mathrm{R}}}(\gamma) = P_{\mathrm{r}}\{\bar{\gamma}\lambda_{\max} \leq \gamma\} \tag{3.16}$$

$$P_{\mathrm{r}}\{\lambda_{\max} < \frac{\gamma}{\bar{\gamma}}\} \tag{3.17}$$

$$F_{\gamma_{\mathrm{R}}}(\gamma) = F_{\lambda_{\max}}(\frac{\gamma}{\bar{\gamma}}) \tag{3.18}$$

As a result, the PDF of γ_R is obtained as

$$f_{\gamma_{\mathrm{R}}}(\gamma) = \frac{1}{\bar{\gamma}} f_{\lambda_{\max}}(\frac{\gamma}{\bar{\gamma}}) \tag{3.19}$$

From (3.18), (3.19) CDF and PDF of $\lambda_{\max}$ is obtained as [27]

$$F_{\lambda_{\max}}(\lambda) = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)k} \frac{d_{k,l}}{k(l+1)} [\Gamma(l+1) - \Gamma(l+1, k\lambda)] \tag{3.20}$$

$$f_{\lambda_{\max}}(\lambda) = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)k} d_{k,l}(\lambda)^l e^{-k\lambda} \tag{3.21}$$

where,
$M = min(N_t, N_r)$
$N = max(N_t, N_r)$
From [23], K is given as

$$\frac{1}{K} = \prod_{i=1}^{M} (N-i)!(M-i)! \tag{3.22}$$

Determining the weighting coefficient, $d_{k,l}$ involves numerical computation via the algorithm introduced in [28], $\Gamma(n)$ denotes the gamma function, and $\Gamma(n,x)$ is the incomplete gamma function, as given by [27].
Substituting (3.20) into (3.18) and (3.21) into (3.19) the CDF and PDF are given by

$$F_{\gamma_{\mathrm{R}}}(\gamma) = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)k} \frac{d_{k,l}}{k(l+1)} \left[\Gamma(l+1) - \Gamma(l+1, k(\frac{\gamma}{\bar{\gamma}}))\right] \tag{3.23}$$

$$f_{\gamma_{\mathrm{R}}}(\gamma) = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)k} d_{k,l} \frac{\gamma^l}{\bar{\gamma}^{l+1}} e^{-k(\frac{\gamma}{\bar{\gamma}})} \tag{3.24}$$

For the integer value of n, the gamma function and incomplete gamma functions $\Gamma(n+1)$ and $\Gamma(n+1, x)$

$$\Gamma(n+1) = n! \tag{3.25}$$

$$\Gamma(n+1,x) = n!e^{-x}\sum_{m=0}^{n}\frac{x^m}{m!} \tag{3.26}$$

Then, the CDF and PDF of γ_R are rewritten as

$$F_{\gamma_\mathrm{R}}(\gamma) = K\sum_{k=1}^{M}\sum_{l=N-M}^{(N+M-2k)k}\frac{d_{k,l}}{k(l+1)}l!\left[1-e^{-k\frac{\gamma}{\bar{\gamma}}}\sum_{m=0}^{l}\frac{k\frac{\gamma^m}{\bar{\gamma}^m}}{m!}\right] \tag{3.27}$$

$$f_{\gamma_\mathrm{R}}(\gamma) = K\sum_{k=1}^{M}\sum_{l=N-M}^{(N+M-2k)(k)} d_{k,l}\frac{\gamma}{\bar{\gamma}^{l+1}}e^{-k(\frac{\gamma}{\bar{\gamma}})} \tag{3.28}$$

3.1.2 Eavesdropper Signal Expression

An active eavesdropper with a single antenna. The received signal (z) at the receiver can be written as

$$z = \sqrt{P}\mathbf{h_z}\mathbf{v}x + n_z \tag{3.29}$$

Where, z is the receiving signal at the eavesdropper with size 1× 1, $\mathbf{h_z}$ is the channel matrix of size $N_t \times 1$, n_z denotes Gaussian noise with size 1× 1, and P is the total power transmitted at the transmitter. The instantaneous SNR at the Eavesdropper is obtained as,

$$\gamma_E = \frac{|\sqrt{P}\mathbf{h_z}\mathbf{v}x|^2}{|n_z|^2} \tag{3.30}$$

$$\gamma_E = \frac{P(\sqrt{P}\mathbf{h_z}\mathbf{v}x)(\sqrt{P}\mathbf{h_z}\mathbf{v}x)^+}{(n_z)(n_z)^+} \tag{3.31}$$

$$\gamma_E = \frac{P(\mathbf{h_z}\mathbf{v}xx^+\mathbf{v}^+\mathbf{h_z}^+)}{(n_z{n_z}^+)} \tag{3.32}$$

$$\gamma_E = \frac{P|\mathbf{h_z}|^2}{N_0} \tag{3.33}$$

$$\gamma_E = \frac{P\sum_{i=1}^{N_t}|h_{z,i}|^2}{N_0} \tag{3.34}$$

$$\gamma_E = \bar{\gamma}X_z \tag{3.35}$$

where $X_z = \sum_{i=1}^{N_t}|h_{z,i}|^2$

It can be seen that $h_{z,i}$ is an i.i.d. complex Gaussian random variable with zero mean and variance ω_z. Thus, X_z is a sum of the square of N_t i.i.d. complex Gaussian random variables with zero mean and variance ω_z. Therefore, X_z is a Gamma random variable with parameter set (N_t ; ω_z) whose PDF can be written as The CDF of the channel power gain $X_{k,h}$ of Nagakami-m fading channel [29]

$$\alpha_z = \frac{n_T}{\omega_z} \tag{3.36}$$

By definition, the CDF of γ_E is given by

$$F_{\gamma_E}(\gamma_z) = P_\mathrm{r}\{\gamma_E \leq \gamma_z\} \tag{3.37}$$

$$F_{\gamma_{\mathrm{E}}}(\gamma) = P_{\mathrm{r}}\{\bar{\gamma}X_z \leq \gamma_z\} \tag{3.38}$$

$$P_{\mathrm{r}}\{X_z < \frac{\gamma_z}{\bar{\gamma}}\} \tag{3.39}$$

$$F_{\gamma_{\mathrm{E}}}(\gamma) = F_{X_z}(\frac{\gamma_z}{\bar{\gamma}}) \tag{3.40}$$

As a result, the PDF of γ_E is obtained as

$$f_{\gamma_{\mathrm{E}}}(\gamma) = \frac{1}{\bar{\gamma}} f_{X_z}(\frac{\gamma}{\bar{\gamma}}) \tag{3.41}$$

The CDF and CDF of X_z are given by

$$F_{X_z}(x) = 1 - \exp(-\alpha_z x) \sum_{i=0}^{N_t-1} \frac{\alpha_z^i x^i}{i!} \tag{3.42}$$

$$f_{X_z}(x) = \frac{\alpha_z^{N_t}}{\Gamma(N_t)} x^{N_t-1} \exp(-\alpha_z x) \tag{3.43}$$

By Substituting (3.42) into (3.40) and (3.43) into (3.41), The CDF and PDF of γ_E can be written as

$$F_{\gamma_E}(\gamma_z) = 1 - \exp\left(-\alpha_z \frac{\gamma_z}{\bar{\gamma}}\right) \sum_{i=0}^{N_t-1} \frac{\alpha_z^i \frac{\gamma_z}{\bar{\gamma}}^i}{i!} \tag{3.44}$$

$$f_{\gamma_E}(\gamma_z) = \frac{\alpha_z^{N_t}}{\Gamma(N_t)} \left(\frac{\gamma_z}{\bar{\gamma}}\right)^{N_t-1} \exp\left(-\alpha_z \frac{\gamma_z}{\bar{\gamma}}\right) \tag{3.45}$$

Chapter 4

Performance Analysis

4.1 BLER Analysis

We assume that the transmitter transmits σ bits of information with m block length to the receiver over the channel used during each packet transmission. The coding rate is given by $r = \frac{\sigma}{m}$
let ϵ denote the instantaneous BLER of the legitimate communication from transmitter to receiver at instantaneous received SNR $\gamma_R = \gamma$

$$\varepsilon(\gamma_R) = Q\left(\frac{C(\gamma_R) - r}{\sqrt{\frac{V(\gamma_R)}{m}}}\right) \tag{4.1}$$

$C(\gamma_R)$ is the Shannon capacity, and $V(\gamma_R)$ is the channel dispersion, which measures the stochastic variability of the channel relative to a deterministic channel with the same capacity. It is hard to characterize ϵ in a closed form due to the complicated Q-function and we are thus motivated to use a linear approximation of $Q\left(\frac{C(\gamma_R)-r}{\sqrt{\frac{V(\gamma_R)}{m}}}\right) \approx \varepsilon(\gamma_R)$ is given by [30] and [31]

$$\varepsilon(\gamma) = \begin{cases} 0, & \gamma \geq \gamma_{\mathrm{RH}} \\ \frac{1}{2} - v\sqrt{m}(\gamma - \theta), & \gamma_{\mathrm{RL}} < \gamma < \gamma_{\mathrm{RH}} \\ 1, & \gamma \leq \gamma_{\mathrm{RL}} \end{cases} \tag{4.2}$$

Where,

$v = \frac{1}{2\sqrt{2^{2r}-1}}$, $\theta = 2^{2r} - 1$,

$\gamma_{\mathrm{RL}} = \theta - \frac{1}{2v\sqrt{m}}$, $\gamma_{RH} = \theta + \frac{1}{2v\sqrt{m}}$

With the above approximation, $\bar{\epsilon}$ can be evaluated as

$$\bar{\epsilon} \approx \int_0^\infty \varepsilon(\gamma_R) f_{\gamma_R}(x)\, dx \tag{4.3}$$

Substituting (3.28) into (4.3) can be evaluated as

$$\bar{\epsilon} = \int_0^\infty \varepsilon(\gamma_R) K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)(k)} d_{k,l} \frac{\gamma^l}{\bar{\gamma}^{l+1}} e^{-k(\frac{\gamma}{\bar{\gamma}})} d\gamma \tag{4.4}$$

$$\begin{aligned}\bar{\epsilon} = &\int_0^{\gamma_{\mathrm{RL}}} K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)(k)} d_{k,l} \frac{\gamma^l}{\bar{\gamma}^{l+1}} e^{-k(\frac{\gamma}{\bar{\gamma}})} d\gamma + \\ &\int_{\gamma_{\mathrm{RL}}}^{\gamma_{\mathrm{RH}}} \left(\frac{1}{2} - v\sqrt{m}(\gamma - \theta)\right) K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)(k)} d_{k,l} \frac{\gamma^l}{\bar{\gamma}^{l+1}} e^{-k(\frac{\gamma}{\bar{\gamma}})} d\gamma\end{aligned} \tag{4.5}$$

$$\begin{aligned}\bar{\epsilon} = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)(k)} &\left(\frac{(1 - 2v\sqrt{m}\theta)}{2} \int_0^{\gamma_{RL}} d_{k,l} \frac{\gamma^l}{\bar{\gamma}^{l+1}} e^{-k(\gamma/\bar{\gamma})} d\gamma \right. \\ &+ \frac{(1 + 2v\sqrt{m}\theta)}{2} \int_0^{\gamma_{RH}} d_{k,l} \frac{\gamma^l}{\bar{\gamma}^{l+1}} e^{-k(\gamma/\bar{\gamma})} d\gamma \\ &\left. - v\sqrt{m} \int_0^{\gamma_{RH}} d_{k,l} \frac{\gamma^{l+1}}{\bar{\gamma}^{l+1}} e^{-k(\gamma/\bar{\gamma})} d\gamma \quad + v\sqrt{m} \int_0^{\gamma_{RH}} d_{k,l} \frac{\gamma^{l+1}}{\bar{\gamma}^{l+1}} e^{-k(\gamma/\bar{\gamma})} \right)\end{aligned} \tag{4.6}$$

By leveraging the formula provided in Equation (3.351, [32]), we can effectively compute the integration as

$$\begin{aligned}\bar{\epsilon} = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)(k)} d_{k,l} &\left(\frac{(1 - 2v\sqrt{m}\theta)}{2} \frac{l!\bar{\gamma}^{l+1}}{k^{l+1}} \left(1 - e^{-\frac{k\gamma_{RL}}{\bar{\gamma}}} \sum_{i=0}^{l} \frac{l!}{i!} \frac{\bar{\gamma}^{(l-i+1)}\gamma_{RL}^{i}}{k^{(l-i+1)}} \right) \right. \\ &+ \frac{(1 + 2v\sqrt{m}\theta)}{2} \frac{l!\bar{\gamma}^{l+1}}{k^{l+1}} \left(1 - e^{-\frac{k\gamma_{RH}}{\bar{\gamma}}} \sum_{i=0}^{l} \frac{l!}{i!} \frac{\bar{\gamma}^{(l-i+1)}\gamma_{RH}^{i}}{k^{(l-i+1)}} \right) \\ &- v\sqrt{m} \frac{(l+1)!\bar{\gamma}^{(l+2)}}{k^{(l+2)}} \left(1 - e^{-\frac{k\gamma_{RL}}{\bar{\gamma}}} \sum_{i=0}^{(l+1)} \frac{(l+1)!}{i!} \frac{\bar{\gamma}^{(l-i+2)}\gamma_{RL}^{i}}{k^{(l-i+2)}} \right) \\ &\left. + v\sqrt{m} \frac{(l+1)!\bar{\gamma}^{(l+2)}}{k^{(l+2)}} \left(1 - e^{-\frac{k\gamma_{RH}}{\bar{\gamma}}} \sum_{i=0}^{(l+1)} \frac{(l+1)!}{i!} \frac{\bar{\gamma}^{(l-i+2)}\gamma_{RH}^{i}}{k^{(l-i+2)}} \right) \right)\end{aligned} \tag{4.7}$$

$$\begin{aligned}\bar{\epsilon} = K \sum_{k=1}^{M} \sum_{l=N-M}^{(N+M-2k)(k)} d_{k,l} &\left(\frac{l!\bar{\gamma}^{l+1}}{k^{l+1}} - \frac{1 - 2v\sqrt{m}\theta}{2} e^{-\frac{k\gamma_{RL}}{\bar{\gamma}}} \sum_{i=0}^{l} \frac{l!}{i!} \frac{\bar{\gamma}^{l-i+1}\gamma_{RL}^{i}}{k^{l-i+1}} \right. \\ &- \frac{1 + 2v\sqrt{m}\theta}{2} e^{-\frac{k\gamma_{RH}}{\bar{\gamma}}} \sum_{i=0}^{l} \frac{l!}{i!} \frac{\bar{\gamma}^{l-i+1}\gamma_{RH}^{i}}{k^{l-i+1}} + v\sqrt{m} \Big(e^{-\frac{k\gamma_{RL}}{\bar{\gamma}}} \sum_{i=0}^{l+1} \frac{(l+1)!}{i!} \frac{\bar{\gamma}^{l-i+2}\gamma_{RL}^{i}}{k^{l-i+2}} \\ &\left. - e^{-\frac{k\gamma_{RH}}{\bar{\gamma}}} \sum_{i=0}^{l+1} \frac{(l+1)!}{i!} \frac{\bar{\gamma}^{l-i+2}\gamma_{RH}^{i}}{k^{l-i+2}} \Big) \right)\end{aligned} \tag{4.8}$$

4.2 Secrecy Capacity

To ensure reliable communication between the transmitter and the receiver, the secrecy capacity should be determined. The secrecy capacity of the transmission from the transmitter to the receiver in the presence of an eavesdropper is given as the difference between the channel capacity of the main channel from the transmitter to the receiver and the eavesdropper channel from the transmitter to the eavesdropper. Mathematically, it can be written as [33]

$$C = \log_2(1+\gamma_R) - \log_2(1+\gamma_E) \tag{4.9}$$

where γ_R, γ_E denote the SNRs at Reaceiver and Eavesdropper respectively. This rate can be achieved by a coding scheme for infinite block length. The scheme involves two rates, namely, codeword rate R_y, and secrecy rate R_z separately.

$$R = R_y - R_z \tag{4.10}$$

The rate difference, called rate redundancy, reflects the cost of securing the message transmission against eavesdropping. For systems with infinite blocklength, both R_y and R_z can be designed separately to achieve a possible secrecy rate R that is close to C.

The data rate of SPC needs to be adapted based on the channel conditions to guarantee a desired reliability level. In particular, based on [34], [31], the maximum achievable secrecy rate of SPC can be formulated as a function of BLER ε and the information leakage probability, i.e. Secure constraint δ is given by [35]

$$R(m,\varepsilon,\delta) = C - \sqrt{\frac{\vartheta(\gamma_R)}{m}}\frac{Q^{-1}(\varepsilon)}{ln2} - \sqrt{\frac{\vartheta(\gamma_E)}{m}}\frac{Q^{-1}(\delta)}{ln2} \tag{4.11}$$

$\vartheta(\gamma)$ is the channel dispersion at the instantaneous SNR for infinite blocklength m

$$\vartheta(\gamma) = 1 - (1+\gamma)^{-2} \tag{4.12}$$

$$\vartheta(\gamma) = 1 - \frac{1}{(1+\gamma)^2} \tag{4.13}$$

$$\vartheta(\gamma) = \frac{\gamma^2 + 2\gamma}{(1+\gamma)^2} \tag{4.14}$$

$Q^{-1}(.)$ is the reserve Gaussian Q-function at the block error rate ε and secure constraint δ. Q-function is given by

$$Q(i) = \frac{1}{\sqrt{2\pi}} \int_i^\infty \exp\left(-\frac{t^2}{2}\right) dt \tag{4.15}$$

Based on Shannon's theory [36], Secrecy capacity C is given by

$$C = \int_0^\infty \left[\log_2(1+\gamma_R) - \log_2(1+\gamma_E)\right] f_\gamma(\gamma) d\gamma \tag{4.16}$$

$$C = \int_0^\infty \log_2(1+\gamma_R) f_{\gamma_R}(\gamma_R)\, d\gamma_R - \int_0^\infty \log_2(1+\gamma_E) f_{\gamma_E}(\gamma_E)\, d\gamma_E \tag{4.17}$$

The Secrecy Rate R is given by

$$R = C - \int_0^\infty \sqrt{\frac{\gamma_R^2 + 2\gamma_R}{m(1-\gamma_R)^2}} \frac{Q^{-1}(\varepsilon)}{ln2} f_{\gamma_R}(\gamma_R)\, d\gamma_R - \int_0^\infty \sqrt{\frac{\gamma_E^2 + 2\gamma_E}{m(1-\gamma_E)^2}} \frac{Q^{-1}(\delta)}{ln2} f_{\gamma_E}(\gamma_E)\, d\gamma_E \tag{4.18}$$

$$\begin{aligned} R =& C - \log_2(e) Q^{-1}(\varepsilon) \int_0^\infty \sqrt{\frac{\gamma_R^2 + 2\gamma_R}{m(1-\gamma_R)^2}} f_{\gamma_R}(\gamma_R)\, d\gamma_R \\ & - \log_2(e) Q^{-1}(\delta) \int_0^\infty \sqrt{\frac{\gamma_E^2 + 2\gamma_E}{m(1-\gamma_E)^2}} f_{\gamma_E}(\gamma_E)\, d\gamma_E \end{aligned} \tag{4.19}$$

The Secrecy rate is given by

$$\begin{aligned} R =& \int_0^\infty \log_2(1+\gamma_R) f_{\gamma_R}(\gamma_R)\, d\gamma_R - \int_0^\infty \log_2(1+\gamma_E) f_{\gamma_E}(\gamma_E)\, d\gamma_E \\ & - \log_2(e) Q^{-1}(\varepsilon) \int_0^\infty \sqrt{\frac{\gamma_R^2 + 2\gamma_R}{m(1-\gamma_R)^2}} f_{\gamma_R}(\gamma_R)\, d\gamma_R \\ & - \log_2(e) Q^{-1}(\delta) \int_0^\infty \sqrt{\frac{\gamma_E^2 + 2\gamma_E}{m(1-\gamma_E)^2}} f_{\gamma_E}(\gamma_E)\, d\gamma_E \end{aligned} \tag{4.20}$$

4.3 Simulation setup

4.3.1 SNR Computation for Main Channel

The simulation begins with generating a channel matrix under Rayleigh Fading conditions, determined by the number of transmit (Nt) and receive (Nr) antennas. The SNR for the main channel is calculated using the largest eigenvalue obtained from the channel covariance matrix, which is derived from the generated channel matrix. This calculation incorporates both transmit power and noise power to accurately represent the communication system's environment.

4.3.2 SNR Computation for eavesdropper

Parallel to the main channel analysis, an eavesdropper channel is modeled using Nakagami-m fading. This step involves computing another set of SNR values for the eavesdropper channel, which is essential for determining the channel capacity and secrecy rate.

4.3.3 BLER simulation

With the SNR of the main channel computed, the focus shifts to simulating the BLER. This simulation is essential for evaluating the system's reliability and robustness under different channel conditions. By varying the SNR levels and assessing the corresponding BLER, the simulation provides insights into the performance of the MIMO system in maintaining data integrity during transmission.

4.3.4 Secrecy rate

The final phase involves simulating the secrecy capacity. This is achieved by calculating the difference between the channel capacity and the data rate for both the main and eavesdropper channels. The channel capacities are computed based on their respective SNRs, and the secrecy rate is derived from these values. This step is critical for assessing the system's capability to maintain secure communication, a key aspect in the context of PLS.

4.3.5 Parameter Variation Analysis

The simulations also involve altering various factors, such as the number of transmitting and receiving antennas, the number of bits, and the block length in different scenarios. This comprehensive approach allows for a detailed understanding of how each parameter impacts the overall system performance, with a specific emphasis on both BLER and secrecy capacity.

Chapter 5

Results and Analysis

In this chapter, we'll delve into an examination of the system performance of the PLS technique within the context of the MIMO system of SPC. We'll explore its behavior across different simulation cases to gain comprehensive insights.

5.1 BLER Performance

In this section, we will check the performance of BLER by varying different parameters such as the number of transmitters Nt, number of receivers Nr, number of bits σ, and block length m in three different cases.

5.1.1 Case I

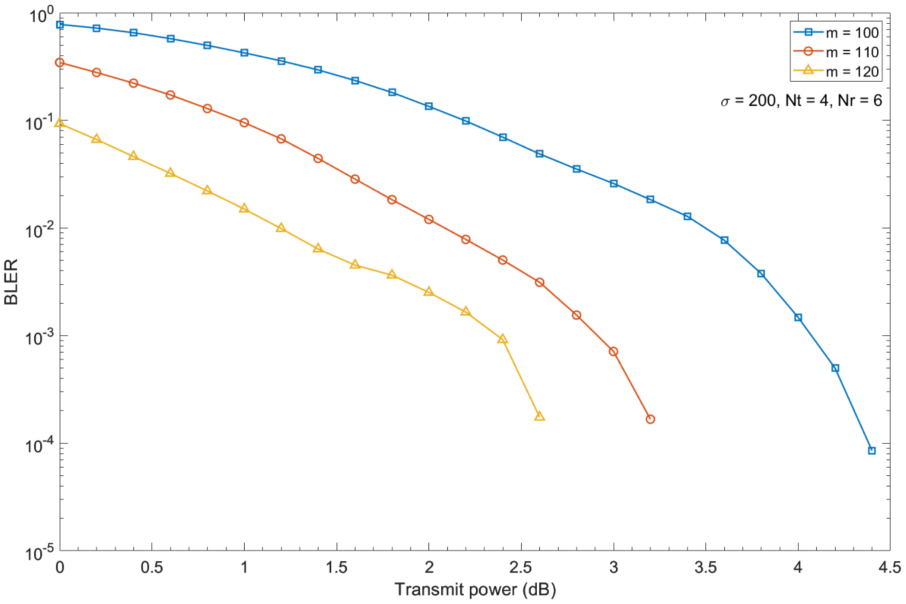

Figure 5.1: BLER versus transmit power with different number of block length

Figure 5.1 demonstrates the impact of block length on the BLER in a MIMO communication system, maintaining constants such as 4 transmit antennas Nt, 6 receive antennas Nr, and number of bits σ of 200. It shows that with increasing transmitted power, the BLER decreases across all considered block lengths $m = 100$, 110, 120. This trend aligns with the expectation that higher transmit power should enhance the SNR, thus reducing the error rate. Notably, the graph reveals that an increase in the block length leads to a more significant decrease in BLER. This suggests that longer block lengths provide benefits such as improved error correction capabilities and enhanced diversity gain, which contribute to more reliable signal transmission. The results imply a trade-off where longer blocks improve error rates at the possible expense of increased latency and computational demands, highlighting the need for careful system design to optimize both performance and efficiency.

5.1.2 Case II

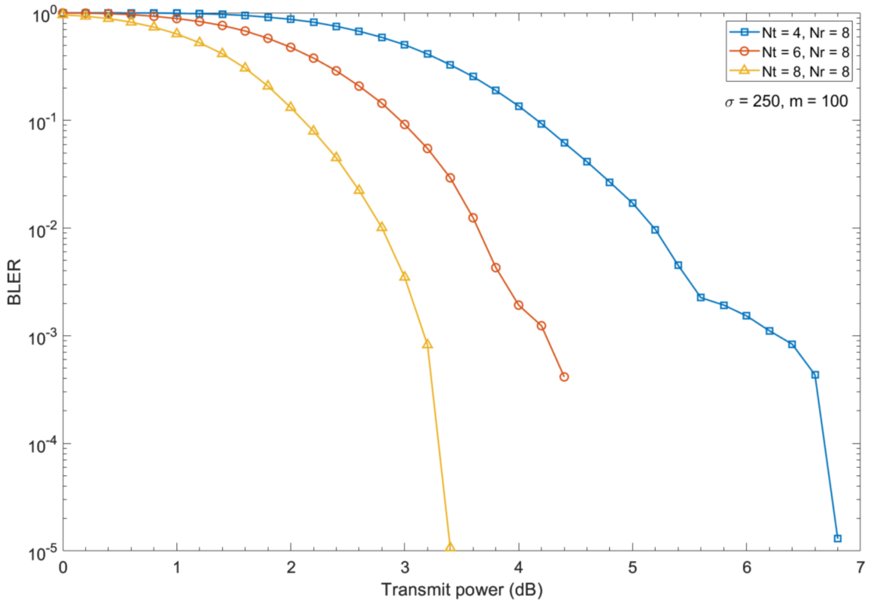

Figure 5.2: BLER versus transmit power with different number of transmit antennas

Figure 5.2 represents the impact of increasing transmit antenna numbers on BLER in a MIMO system with a constant number of receive antennas $Nr = 8$, block length $m = 100$, and number of bits $\sigma = 250$. The graph shows three curves for transmit antennas $Nt = 4$, 6, 8.

As the transmit antenna increases, BLER decreases, indicating that having more transmit antennas can effectively lower the rate of block errors. This is consistent with MIMO technology's benefits, which include increased spatial diversity and capacity. These enable more sophisticated signal processing techniques, leading to improved signal reception and a decreased likelihood of errors. However, the graph also hints at diminishing returns as antenna numbers grow, an essential consideration for system design where complexity and cost must be balanced with performance gains.

5.1.3 Case III

Figure 5.3 captures the variation of BLER with respect to the transmitted power while holding the number of transmit antennas $Nt = 8$, the number of receive antennas $Nr = 6$, and the block length $m = 120$ constant and altering the value of the number of bits $\sigma = [270, 300, 330]$.

The graph delineates a clear trend where an increase in the number of bits σ leads to a rise in the BLER. This indicates that transmitting a larger number of bits under the same conditions of power and antenna configuration leads to a higher probability of errors occurring during transmission. This could be because as the number of bits increases, there is more information to transmit over the same channel, which may result in a higher chance of bit errors, particularly if the channel conditions or the system's error correction capabilities are not adequately optimized to handle the increased load.

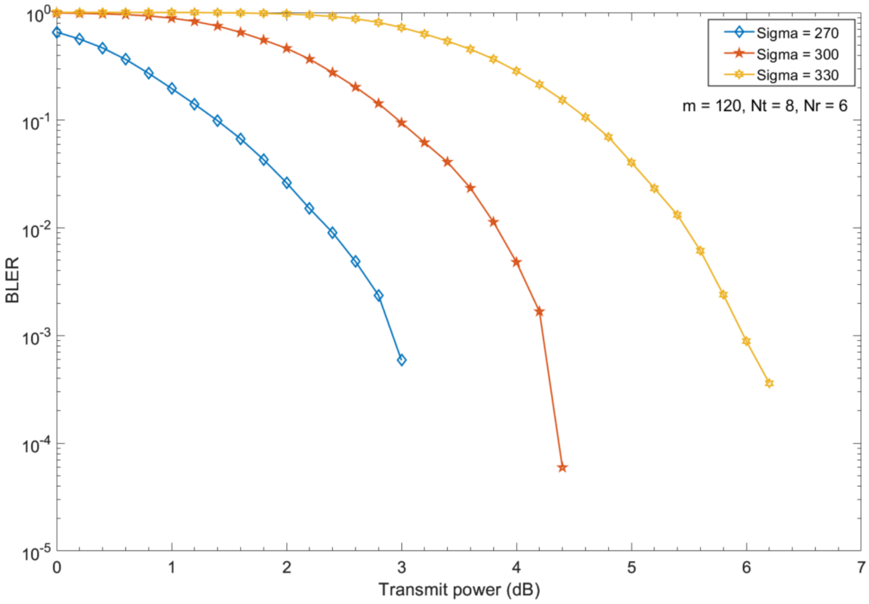

Figure 5.3: BLER versus transmit power with a different packet length of data

The results from this graph show a direct correlation between the number of bits and the error performance of the system, highlighting the need for careful consideration of the bit rate in system design. The findings emphasize the importance of optimizing the number of bits to balance between the desired throughput and the BLER for reliable communication within a MIMO system. This balance is crucial for designing systems that can effectively manage the trade-off between high data rates and error-free transmission, which is especially significant in the context of secure physical communication in MIMO systems.

The simulated results provide valuable insights into the performance of BLER concerning various system parameters. Across these scenarios, it becomes evident that certain factors significantly influence BLER. Increasing the number of channels (as observed in Figure 5.1) and the number of transmit antennas (as seen in Figure 5.2) tends to lower BLER, suggesting a positive correlation between these parameters and error rate reduction. Conversely, the number of bits (as shown in Figure 5.3) demonstrates an inverse relationship with BLER, wherein a higher bit count corresponds to an increase in error rate. These findings underscore the critical role that factors like channel count, antenna numbers, and bit allocation play in shaping BLER performance within communication systems. Understanding and optimizing these parameters are pivotal for achieving improved error rates and system reliability.

5.2 Secrecy Capacity Performance

In this section, we will check the performance of secrecy capacity by varying different parameters, such as the number of transmit antennas Nt, the number of receive antennas Nr, and the block length m in three different cases.

5.2.1 Case I

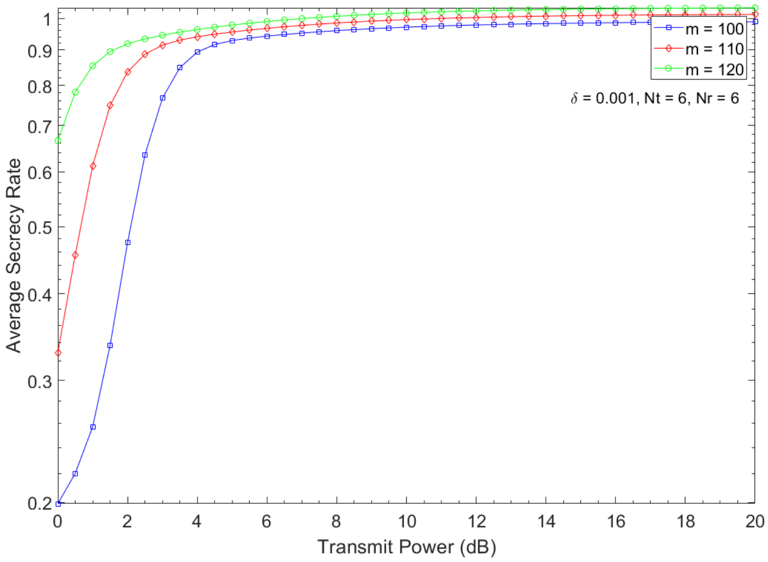

Figure 5.4: Average secrecy rate versus transmit power for different number of block lengths

Figure 5.4 displays simulated results depicting the relationship between Transmitted power and Secrecy Rate while maintaining constants such as $Nt = 6$, $Nr = 6$ and varying the block length $m = [100, 110, 120]$.

The graph in Figure 5.4 demonstrates a direct relationship between the block length and the average secrecy rate, signifying that as the block length increases, the average secrecy rate also increases. This indicates that longer block lengths contribute to enhancing the security of the transmission. The reason behind this might be that longer blocks allow for better coding schemes, which can improve the reliability of the transmitted signal while also making it more difficult for an eavesdropper to decode it successfully.

5.2.2 Case II

Figure 5.5 displays simulated results depicting the relationship between transmitted power and secrecy rate while maintaining constants such as $m = 120$, and varying the number of transmit and receive antennas $Nt = [4, 6, 8]$ and $Nr = 8$.

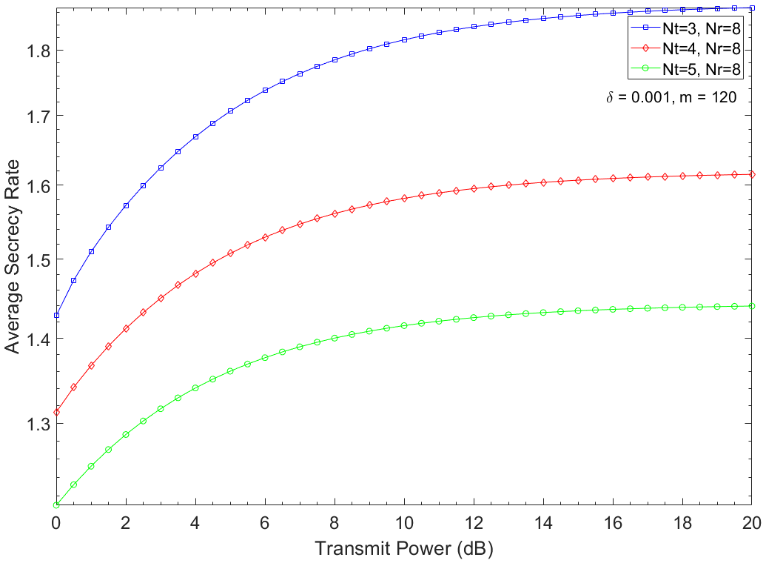

Figure 5.5: Average secrecy rate versus transmit power with different number of transmit antennas

With an increase in transmitted power, the average secrecy rate initially rises sharply and then begins to plateau, suggesting a diminishing return on increasing power in terms of enhancing the secrecy rate. Interestingly, the graph shows that systems with fewer transmit antennas $Nt = 3$ achieve a higher secrecy rate than those with more $Nt = 4$ and $Nt = 5$, which could imply that beyond a certain point, adding more transmit antennas might not necessarily contribute to an increased secrecy rate. This could be due to a variety of factors, such as increased channel correlation or the potential for more sophisticated eavesdropping capabilities as the number of transmission paths increases. The leveling off of the secrecy rate at higher power levels indicates that there is an optimal range of transmit power for maximizing the secrecy rate, beyond which the benefits are marginal. This highlights a nuanced aspect of MIMO system design, where the number of transmit antennas must be carefully selected to balance the trade-offs between system capacity, complexity, and secrecy.

The simulated results highlight key factors impacting the secrecy capacity. When the block length (m) increases, the secrecy rate also increases (as seen in Figure 5.4). Conversely, an increase in transmit antennas (Nt) leads to a decrease in the secrecy rate (as shown in Figure 5.5). These findings emphasize the intricate relationship between system parameters and the secrecy rate, underscoring the importance of optimizing these variables to enhance security in communication systems.

From the analysis, it was observed that the performance of the MIMO system, particularly in terms of BLER and secrecy capacity, had significant implications for URLLC and secure communication. The BLER results illuminated the system's reliability, showing how error rates varied under different conditions, a key factor for URLLC applications. Similarly, the analysis of secrecy capacity sheds light on the system's ability to maintain confidentiality, which is crucial in scenarios where secure data transmission is a priority. This comprehensive evaluation demonstrated the system's capacity to handle the demands of high reliability and security.

Chapter 6

Discussion

In our mathematical analysis, we derived formulas for key performance measures like BLER and secrecy capacity. To reach these expressions, we began by obtaining signal expressions, SNR, PDFs, and CDFs for both the receiver and the potential eavesdropper, all based on our system model. In our simulations, we generated a channel matrix reflecting the Rayleigh fading environment using the gamma distribution, considering factors like fading severity and channel mean power. These channel coefficients were then used in the derived SNR expressions. For the eavesdropper's channel coefficient, we simulated the Nakagami-m fading, employing gamma distribution based on channel mean power. These coefficients were integrated into the SNR expression for the eavesdropper. From these derived expressions, we calculated the secrecy capacity and BLER for users within our system. Essentially, we used these mathematical models to mimic real-world scenarios and gauge system performance accurately.

RQ1: What is an effective transmission method to provide the secrecy capacity of MIMO transmission for SPC in the physical layer?

Ans: Beamforming is identified as the preferred method for enhancing secrecy capacity in MIMO transmission for SPC within the physical layer. This choice is grounded in the unique capabilities of beamforming in a MIMO system, where it effectively maximizes the signal's focus on the intended receiver while significantly reducing its reception by potential eavesdroppers. This is achieved by utilizing the multiple antennas at the transmitter to control and direct the signal's phase and amplitude, thereby creating a constructive interference pattern aimed precisely at the target receiver. Such a method is particularly effective in the context of PLS, as it concurrently bolsters both the security and reliability of critical and time-sensitive communications. By improving signal quality and strength at the receiver's position and diminishing it elsewhere, beamforming emerges as an optimal approach in scenarios that demand high levels of confidentiality and data integrity, especially in environments vulnerable to eavesdropping.

RQ2: How are the transmitting and receiving beamforming vectors designed and optimized based on the channel condition to achieve low BLER and high secrecy capacity?

Ans: The design of optimal transmitting and receiving beamforming vectors is centered on the vectors $\mathbf{v}$ and $\mathbf{w}$ as weights at the transmitter and receiver, respectively. On the transmitting side, the beam steering vector $\mathbf{v}$ is selected based on the MRT principle, chosen as an eigenvector corresponding to the largest eigenvalue of the Wishart matrix $\mathbf{H}^{+}\mathbf{H}$, effectively aligning the transmitted signal to maximize signal strength at the receiver. Conversely, at the receiver, the weighting vector $\mathbf{w}$ is determined by the MRC principle, aimed at achieving the maximum SNR. This vector is calculated as $\mathbf{w} = (\mathbf{Hv})^{+} = \mathbf{H}^{+}\mathbf{v}^{+}$, incorporating the beam steering vector used at the transmitter. This methodological approach in beamforming, by optimizing vectors $\mathbf{v}$ and $\mathbf{w}$ according to the channel conditions, is tailored to reduce the BLER and enhance the secrecy capacity, thus bolstering both the reliability and security of the MIMO system for SPC.

RQ3: What are the mathematical expressions for the BLER and secrecy capacity of MIMO transmission for SPC in the PLS?

Ans: The mathematical derivation of the BLER and secrecy capacity for MIMO transmission in SPC involves integrating beamforming vectors and channel fading models. The beamforming vectors $\mathbf{v}$ and $\mathbf{w}$ at the transmitter and receiver, respectively, are crucial in optimizing signal direction and strength. For the main channel, Rayleigh fading is considered to model the signal fluctuations in a typical wireless environment, while for the eavesdropper's channel, Nakagami-m fading is employed to represent a range of fading conditions. With these models, the SNR is calculated for both the legitimate receiver and the eavesdropper. From the SNR, PDFs, and CDFs are derived, which are instrumental in understanding the likelihood of different SNR values. Finally, using these derived statistical functions and considering the effects of the beamforming vectors and fading models, the BLER and secrecy capacity are mathematically calculated.

RQ4: How can we simulate the performance of the system in Matlab and represent the results by plotting?

Ans: In our discussion on simulating the performance of a MIMO system for SPC in MATLAB, the primary focus lies on the BLER and secrecy capacity analysis. The process begins with the computation of SNR for the main channel. This involves generating a channel matrix under Rayleigh Fading conditions, sized according to the number of transmit (Nt) and receive (Nr) antennas. The largest eigenvalue extracted from the channel covariance matrix, derived from this matrix, plays a crucial role in the SNR calculation, which is influenced by both transmit and noise power. This step sets the stage for the subsequent BLER analysis, which is conducted across various modulation orders to understand the system's reliability under different channel conditions and modulation techniques. Additionally, the simulation includes an eavesdropper channel, modeled using Nakagami-m fading, to calculate another set of SNR values. These values are integral in determining the channel capacity and achievable rate, leading to the simulation of secrecy capacity based on the derived equations. The MATLAB simulations aim to thoroughly assess the performance of PLS techniques within the MIMO system context, particularly focusing on how the system behaves under varying conditions and parameters. By altering different factors such as the number of transmitting and receiving antennas, the number of bits, secure constraints, and the block length in various simulation scenarios, we gain valuable insights into the system's behavior and its efficiency across a range of scenarios. This comprehensive analysis is vital in understanding the impact of each parameter on the overall performance of the system, with a specific emphasis on both BLER and secrecy capacity.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

In this thesis, a comprehensive investigation into PLS in MIMO systems was carried out, with a specific focus on SPC. A significant portion of the study was dedicated to rigorous mathematical derivation, forming a robust theoretical base for our research. This foundational work involved the development of complex mathematical models and formulas, which were crucial in understanding the dynamics of PLS in MIMO systems.

Building on this theoretical groundwork, the study then applied practical techniques such as MRT and MRC, along with Beamforming. These techniques were employed to strengthen the security and reliability of wireless communications, especially in the face of potential eavesdropping threats. Through extensive simulations conducted in MATLAB, we assessed critical performance indicators like the BLER and Secrecy Capacity under various conditions. The results from these simulations demonstrated that incorporating MRT, MRC, and Beamforming significantly enhances the efficiency and security of communication systems.

The insights gained from both the mathematical derivations and practical simulations provide a comprehensive understanding of the efficacy of PLS in MIMO systems for SPC. This research contributes to the advancement of more robust and secure wireless communication strategies, marking a significant step forward in the field of secure communications. The findings lay a strong foundation for future research, offering pathways for further exploration and development in enhancing communication security across different scenarios.

7.2 Future Work

A key area for future exploration is the integration of advanced Machine Learning (ML) algorithms into the realm of PLS for MIMO systems in SPC. This approach holds the promise of dynamically optimizing PLS strategies based on real-time data and channel behavior predictions. By employing ML algorithms, future research could focus on developing adaptive beamforming techniques that respond to instantaneous changes in the communication environment, thereby significantly enhancing both the security and efficiency of MIMO systems in SPC scenarios. Such an advancement would not only improve the robustness of current systems against eavesdropping threats but also pave the way for smarter, AI-driven wireless communication technologies in future 5G and beyond networks.

References

[1] Rajiv. History of wireless communication - morse code to 5g technology. [Online]. Available: https://www.rfpage.com/history-of-wireless-communication-morse-code-to-5g-technology/

[2] M. Adnan and S. M. Hilles, “An evolution to next generation heterogeneous cellular networks.”

[3] D. W. Bliss, K. W. Forsythe, and A. M. Chan, “MIMO wireless communication,” vol. 15, no. 1.

[4] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” vol. 114, no. 1, pp. 19–26, publisher: Proceedings of the National Academy of Sciences. [Online]. Available: https://www.pnas.org/doi/10.1073/pnas.1618130114

[5] E. Biglieri, J. Proakis, and S. Shamai, “Fading channels: information-theoretic and communications aspects,” *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2619–2692, 1998.

[6] What are the different types of fading? - everything RF. [Online]. Available: https://www.everythingrf.com/community/what-are-the-different-types-of-fading

[7] E. Tanghe, W. Joseph, L. Martens, H. Capoen, K. Van Herwegen, and W. Vantomme, “Large-scale fading in industrial environments at wireless communication frequencies,” in *2007 IEEE Antennas and Propagation Society International Symposium*, 2007, pp. 3001–3004.

[8] H. Tataria, “Wireless communications channels lecture 3: Fading.”

[9] W. Lee, “Estimate of channel capacity in raleigh fading environment,” in *38th IEEE Vehicular Technology Conference*, 1988, pp. 582–584.

[10] A. Goldsmith, “WIRELESS COMMUNICATIONS.”

[11] J. Tang, L. Jiao, K. Zeng, H. Wen, and K.-Y. Qin, “Physical layer secure mimo communications against eavesdroppers with arbitrary number of antennas,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 466–481, 2021.

[12] M. DRISSI, N. BENJELLOUN, P. DESCAMPS, and A. GHARSALLAH, “Analysis & implementation of SISO, SIMO, MISO and MIMO in 5g communication systems based on SDR,” vol. 23, no. 2, pp. 140–146. [Online]. Available: https://doi.org/10.22937/IJCSNS.2023.23.2.15

[13] N. C. Giri, A. Sahoo, J. R. Swain, P. Kumar, A. Nayak, and P. Debogoswami, “Capacity & performance comparison of SISO and MIMO system for next generation network (NGN),” vol. 3, no. 9.

[14] T. Lo, “Maximum ratio transmission,” *IEEE Transactions on Communications*, vol. 47, no. 10, pp. 1458–1461, 1999.

[15] T. M. C. Chu, H. Phan, and H.-J. Zepernick, “Mimo incremental af relay networks with tas/mrc and adaptive modulation,” in *2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, 2013, pp. 1–5.

[16] M. Kang and M.-S. Alouini, “Performance analysis of mimo mrc systems over rician fading channels,” in *Proceedings IEEE 56th Vehicular Technology Conference*, vol. 2, 2002, pp. 869–873 vol.2.

[17] Y. Gu, H. Chen, Y. Li, and B. Vucetic, “Ultra-reliable short-packet communications: Half-duplex or full-duplex relaying?” *IEEE Wireless Communications Letters*, vol. 7, no. 3, pp. 348–351, 2018.

[18] N. H. Tu and K. Lee, “Performance analysis and optimization of multihop mimo relay networks in short-packet communications,” *IEEE Transactions on Wireless Communications*, vol. 21, no. 6, pp. 4549–4562, 2022.

[19] D. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[20] J. R. Childress, “Physical layer security for mimo wireless systems.”

[21] R. Melki, H. Noura, M. Mansour, and A. Chehab, “Physical layer security schemes for mimo systems:an overview,” *Wireless Networks*, vol. 26, 04 2020.

[22] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, “An overview of key technologies in physical layer security,” vol. 22, no. 11, p. 1261. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7711494/

[23] J. Zheng, Q. Zhang, and J. Qin, “Average achievable rate and average bler analyses for mimo short-packet communication systems,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12 238–12 242, 2021.

[24] N. Arı, N. Thomos, and L. Musavian, “Active eavesdropping in short packet communication: Average secrecy throughput analysis,” in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.

[25] J. Fu, P. Zhu, J. Li, Y. Wang, and X. You, “Beamforming design in short-packet transmission for urllc in cell-free massive mimo system,” *IEEE Systems Journal*, vol. 17, no. 3, pp. 4715–4724, 2023.

[26] M. Chaitanya and I. S. P. Reddy, “System performance of MIMO MRT/MRC system under perfect CSI.”

[27] T. M. C. Chu, T. Q. Duong, and H.-J. Zepernick, "Outage probability and ergodic capacity for mimo-mrt systems under co-channel interference and imperfect csi," in *2011 IEEE Swedish Communication Technologies Workshop (SweCTW)*, 2011, pp. 46–51.

[28] A. Maaref and S. Aissa, "Closed-form expressions for the outage and ergodic shannon capacity of mimo mrc systems," *IEEE Transactions on Communications*, vol. 53, no. 7, pp. 1092–1095, 2005.

[29] H. M. Elkamchouchi and A. M. Medra, "Performance comparison of mimo space-time block coded mc-cdma systems in nakagami-m fading channel," in *2009 National Radio Science Conference*, 2009, pp. 1–7.

[30] B. Makki, T. Svensson, and M. Zorzi, "Finite block-length analysis of the incremental redundancy harq," *IEEE Wireless Communications Letters*, vol. 3, no. 5, pp. 529–532, 2014.

[31] O. L. Alcaraz Lopez, E. M. G. Fernandez, R. D. Souza, and H. Alves, "Ultra-reliable cooperative short-packet communications with wireless energy transfer," vol. 18, no. 5, pp. 2161–2177. [Online]. Available: http://ieeexplore.ieee.org/document/8246490/

[32] I. S. Gradštejn, J. M. Ryžik, A. Jeffrey, D. Zwillinger, and I. S. Gradštejn, *Table of integrals, series and products*, 7th ed. Elsevier Acad. Press.

[33] Z. Li and S. Han, "Research on physical layer security of mimo two-way relay system," in *ICC 2022 - IEEE International Conference on Communications*, 2022, pp. 3311–3316.

[34] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Quasi-static multiple-antenna fading channels at finite blocklength," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 4232–4265, 2014.

[35] N. Arı, N. Thomos, and L. Musavian, "Performance analysis of short packet communications with multiple eavesdroppers," *IEEE Transactions on Communications*, vol. 70, no. 10, pp. 6778–6789, 2022.

[36] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

Faculty of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden