DOCTORAL THESIS

Physical layer of Security with NOMA in mixed RF/FSO systems

By: Amani Alged Fetaha Osman

Supervisor:

Prof. Fambirai Takawira

Co-Supervisor:

Prof. Jules Moualeu

A thesis submitted to the Faculty of Engineering and the Built Environment, University of the Witwatersrand, Johannesburg, in fulfillment of the requirements for the degree of Doctor of Philosophy

September 2024

Declaration

I, **Amani Alged Fetaha Osman**, declare that this Dissertation titled, "**Physical Layer Security with Non-Orthogonal Multiple Access in Mixed RF-FSO Systems**" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this dissertation is entirely my own work.
- I have acknowledged all main sources of help.

Signed: ______________________________

Date: 10.09.2024

I dedicate this to my Dearest Parents and Siblings,

Acknowledgements

My utmost gratitude goes to the ALLAH, the author of life who has enabled me and provided opportunity to embark on this journey of acquisition of knowledge. My heartfelt appreciations and deepest thanks goes to my supervisor, Professor Fambirai Takawira, whose guidance and mentorship have been valuable throughout this journey. Your dedication to the field is truly inspiring, and I am grateful for your encouragement and support in my growth as a researcher.
I would like to express my heartfelt gratitude to my co-supervisor, Professor Jules Moualeu for his time and commitment invested in guiding me and my research, the knowledge and skills that you have imparted on to me is immeasurable, without your support this research would have not been possible.
I extend my sincere appreciation to all the academic staff and administrative staff at EIE for their unwavering assistance have been indispensable throughout my PhD study.
My deepest gratitude to my parents, Alged Fetaha and Raya Jaber, for their unwavering love, endless sacrifices, and unwavering support. Your prayers and blessings have shaped me into the person I am today, and I am profoundly grateful for the privilege of having you as my parents. I am determined to continue striving to make you proud.
To my sisters and brothers, I would like to thank you for the constant support and words of encouragement. I am very fortunate to have siblings like you, thank you for being my guiding light.
I would especially like to thank my lovely fiancé, Ahmed Abdelgader for his supports and believe in me, motivation, laughs and encouragement over the years. In moments when I felt like giving up, your unwavering support lifted me up and kept me going. I am endlessly grateful for the strength you've given me.
To my Friends in Sudan, for keeping me in your prayers and the constant support you have given me over the years.
To all my colleagues at EIE School for their continuous assistance, support and encouragement and definitely friendship.
The financial assistance of the Centre for Telecommunications Access Services (CeTAS)-Telkom Centre of Excellence (CoE) Program, University of the Witwatersrand, Postgraduate Merit Award (PMA) toward this research is hereby acknowledged and greatly appreciated.

Publications

- A. A. Osman, J. M. Moualeu, and F. Takawira, "Secrecy Performance of Uplink MIMO-NOMA with Antenna Selection in a Mixed RF-FSO System", *in 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, 2023, pp. 1–6, Morocco.*
- A. A. Osman, J. M. Moualeu, and F. Takawira, "Secrecy Capacity Analysis of Uplink MIMO-NOMA in a Hybrid RF-FSO System", Submitted for possible publication in *IEEE Signal Processing Letters.*
- A. A. F. Osman, J. M. Moualeu, F. Takawira, K. Yadav, and P. K. Upadhyay, "On secure hybrid RF-FSO MIMO-NOMA systems with colluding and non-colluding eavesdroppers," *IEEE Wireless Communication Letters*, pp. 1–1, 2024.

Abstract

The ever-increasing demand for spectrum resources, driven by the surge in high data traffic poses a significant challenge to the efficiency of wireless communication systems. In response, non-orthogonal multiple access (NOMA) has been proposed as a pivotal technique designed to address the spectral challenges inherent to traditional multiple access schemes. NOMA, through its ability to allow multiple users to share the same time-frequency resources non-orthogonally, represents a promising avenue for improving spectral efficiency (SE).

To further improve connectivity and enhance efficiency, NOMA can seamlessly be integrated with multiple-input-multiple-output (MIMO) systems. MIMO, a cornerstone technology in modern wireless communication, utilizes multiple antennas at both the transmitter and receiver to exploit spatial diversity, thereby achieving substantial gains in terms of capacity and reliability. The integration of MIMO with NOMA not only addresses the escalating demand for connectivity but also unlocks the potential for massive connectivity and enhanced spectral efficiency in wireless networks. However, the distribution of radio resources within the MIMO-NOMA framework brings forth security challenges owing to the intrinsic characteristics of wireless transmissions. In this regards, this thesis tackles the security aspect of MIMO-NOMA systems from an information theoretic viewpoint. The information theoretic security or physical layer security (PLS) effectively mitigates vulnerabilities stemming from eavesdropping and interception, thereby fortifying the overall security of wireless communication in the present case of MIMO-NOMA systems. Another challenge that requires some attention is ensuring reliability over long distances. Although the radio frequency (RF) spectrum band is recognized for its reliability in diverse weather conditions, its inherent nature renders it susceptible to security concerns. To address the imperative for secure long-distance communications, it is essential to explore innovative solutions that harness the inherent reliability of the RF spectrum while concurrently mitigating its vulnerabilities through enhanced security measures. Integrating technologies such as free-space optical (FSO) communication, acknowledged for its secure transmission capabilities, along with the implementation of advanced security protocols stands as a promising solution to achieving reliability and security in long-distance communications.

In this work, PLS of a MIMO-NOMA based system in a mixed RF-FSO communications is investigated. Additionally, this thesis delves into the injection of

artificial noise (AN) in an effort to explore other features of the proposed system from a PLS perspective. The last part of the work investigates the secrecy performance of the proposed system in the presence of multiple colluding and non-colluding eavesdroppers. To this end, the statistical properties are examined by deriving the statistical characteristics of the underlying system model, which will subsequently be used to establish both the analytical and asymptotic frameworks for evaluating secrecy performance measures. Finally, Monte Carlo simulations are adopted to validate the accuracy of our proposed mathematical derivations.

Contents

List of Figures

List of Tables

List of Symbols

U_i	RF NOMA Users
b_i^*	Best selected antenna at User i
N_{U_i}	Number of antenna at User i
X_{U_iR}	Average SNR at the j-th antenna of the relay node
X_{U_iE}	Average SNR at the j-th antenna of the eavesdropper
$\sigma^2_{U_i}$	Noise power at U_i signal (variance)
N_R	Number of antenna at the relay
m_R	Nakagami fading parameter at the relay
y_{R_j}	Received signal at the j-th antenna of the relay node
x_{U_i}	Transmit sample by U_i
x_{AN_i}	Artificial noise signal generated by U_i
a_i	Power coefficient of U_i
a_{AN}	Power coefficient of the artificial noise signal
L_i	Path-loss gain of the radio frequency link
P_t	Total transmit power
n_{R_j}	AWGN at the j-th antenna of the relay node
$G_{t,i}^{RF}$	Transmit antenna gain of the radio frequency link
$G_{r,i}^{RF}$	Receive antenna gain of the radio frequency link

λ^{RF}	Wavelength of the radio frequency signal
d_{ref}^{RF}	Reference distance of the antenna far-field
v	Path-loss exponent
d_i^{RF}	radio frequency link distance between U_i and the relay node
N_E	Number of antenna at the eavesdropper
m_E	Nakagami fading parameter at the eavesdropper
y_{E_j}	Received signals at the j-th antenna of the eavesdropper
N_E	Number of antennas at the eavesdropper
N_{U_i}	Number of antennas at U_i
N_R	Number of antennas at the relay node
$h_{U_i^{b*}R_j}$	Channel gain between the best at U_i and the j-th antenna at the rela
n_{E_j}	AWGN at the j-th antenna of the eavesdropper
S_R	Transmitted optical signal by the relay node
$\mathcal{G}$	Fixed gain-amplification factor
μ	Electrical-to-optical conversion coefficient
r	Detection technique used at the destination
h_l	Path loss gain of the free space optical link
ρ	Responsivity of the photodetector
K	Weather dependent attenuation coefficient

h_{RD}	Overall FSO channel fading coefficient
ξ	Pointing error coefficient
h_a	Optical turbulence coefficient
γ_1	The CDF of the Equivalent SNR associated with U_1
γ_2	The CDF of the Equivalent SNR associated with U_2
$\mathbb{E}(\bullet)$	Expectation operator
$\mathbb{P}(\bullet)$	Probability operator
$\Gamma(\bullet)$	Gamma function
$\Upsilon(\bullet,\bullet)$	Lower incomplete gamma function
$G_{p,q}^{m,n}\left(\bullet \mid \begin{matrix}\bullet\\ \bullet\end{matrix}\right)$	Meijer G-function
$G_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}(\bullet)$	Extended generalized bivariate Meijer's G-function
n_R	AWGN at the relay
n_E	AWGN at the eavesdropper
n_D	AWGN at the destination

List of Acronyms

PLS	Physical layer security
RF	Radio frequency
FSO	Free space optics
AF	Amplify-and-forward
DF	Decode-and-forward
TAS	Transmit antenna selection
RAS	Receive antenna selection
BS	Base station
NOMA	Non-orthogonal multiple access
PD-NOMA	Power domain-non-orthogonal multiple access
CD-NOMA	Code domain-non-orthogonal multiple access
OMA	Orthogonal multiple access
MIMO	Multiple input multiple output
SIMO	Single input multiple output
CSI	Channel state information
SNR	Signal-to-noise ratio
SINR	Signal-to-interference-plus-noise ratio
MRC	Maximum ratio combining
EGC	Equal gain combining
IM/DD	Intensity modulation/direct detection
OWC	Optical wireless communications
SOP	Secrecy outage probability
SPSC	Strictly positive secrecy capacity
ASC	Average secrecy capacity
SIC	Successive interference cancellation
JUPPA	Joint user pairing and power allocation
JUCPA	Joint user clustering and power allocation
IUI	Inter-user interference
ICRI	Inter-cluster interference
FU	Far-user
NU	Near-user

RIS	Reconfigurable intelligent surface
VLC	Visible light communication
Wi-Fi	Wireless-fidelity
LTE	Long-term evolution
5G	fifth-generation
IoT	Internet-of-things
QoS	Quality-of-service
OSI	Open system interconnect
BW	Band width
OP	Outage probability
SC	Selection combining
CS	Combining scheme
HS	Hybrid selection
BER	Bit error rate
ML	Machine learning
AN	Artificial noise
ESC	Ergodic sum capacity
EC	Ergodic capacity
SCC	Sum channel capacity
PA	Power allocation
SWIPT	Simultaneous wireless information and power transfer
EST	Effective secrecy throughput
SER	Symbol error rate
RB	Resource block
LOS	Line-of-sight
NLOS	Non line-of-sight
i.i.d.	Identically and independently distributed
AWGN	Additive white gaussian noise
PDF	Probability density function
CDF	Cumulative distribution function

CHAPTER 1

Introduction

1.1 Thesis Motivation

The combination of mixed radio frequency (RF) and free-space optical (FSO) systems has emerged as a promising avenue. These mixed systems present an exciting frontier for enhancing communication performance by leveraging the reliability of RF transmissions and the high data rates of FSO communications [1, 2]. Within this realm, the introduction of the multiple-input-multiple-output (MIMO) technology has provided significant advantages over its single-antenna counterpart. It brings forth the potential for enhanced system capacity and low error rates by exploiting spatial diversity [3–5]. Simultaneously, a promising paradigm in the non-orthogonal multiple access (NOMA) has shown an improved spectral efficiency (SE) [6]. At its core, NOMA harnesses the power domain for multiplexing, enabling multiple users to access the same time-frequency slot using different power levels. This innovative strategy effectively allocates multiple users with varying quality-of-service (QoS) requirements in a more efficient manner compared to the traditional orthogonal multiple access (OMA). Integrating NOMA with MIMO systems has the potential to further enhance the SE, as MIMO technology leverages a spatial diversity to improve overall system capacity and performance [7]. However, a notable concern pertains to the security challenges posed by the shared utilization of channel resources in NOMA-based systems, compounded with the inherent broadcast nature of RF transmissions [8]. One promising approach is to integrate the FSO link with the RF link. This integration introduces distinctive interception vulnerabilities. For instance, while eavesdroppers can potentially attack the RF link, targeting the FSO link poses greater challenges. This difficulty arises from factors like the narrow beam divergence and high directivity inherent in FSO communication, which significantly limit interception opportunities to the mixed RF-FSO system. Traditional security measures rely on encryption-based techniques, which may not be robust against security attacks given the increasing computational power available to attackers [9]. To address this issue, physical layer security (PLS) has emerged as a novel and promising alternative security mechanism to ensure a secure communication to authorized users by leveraging the inherent characteristics of wireless communication channels [10]. Additionally, it can also be employed to distribute secret keys instead of using an additional layer in the upper layers of the open system interconnect (OSI) model [11–13]. The application of PLS more challenging for attackers to decipher transmitted information [14–16]. In the light of above, the exploration of PLS in mixed RF/FSO systems across various architectures has recently garnered significant attention in the literature [17–21]. However, a significant gap exists with the improvement of SE is seldom considered, especially in the context of future wireless systems. Driven by the prospective advantages of MIMO-NOMA technology, this research focuses on the information theoretic security of a mixed RF-FSO systems. Specifically, the presence of multiple passive and active eavesdroppers is considered with and without the injection of artificial noise, and the obtained findings provide useful insights to the current state-of-the-art.

1.2 Thesis Contributions

The main contributions of this thesis are summarized as follows.

- A two-user MIMO-NOMA with transmit antenna selection (TAS) in a mixed RF-FSO system utilizing fixed gain relaying scheme is considered. The antenna selection scheme is adopted at each user to further reduce the hardware complexity at the transmitter. Next, the statistics of the underlying system model are derived in terms of the probability density function (PDF) and cumulative distribution function (CDF). The analytical expressions of the secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), average secrecy capacity (ASC) and the asymptotic ASC are obtained by capitalizing on the derived statistics.
- Building upon the system model presented previously, the analysis extends to a two-user MIMO-NOMA aided by the injection of artificial noise (AN) in a mixed RF-FSO system with a variable gain relaying scheme. The incorporation of AN in the underlying system serves to confound the eavesdropper while bolstering the transmission to the intended receiver. The analytical and asymptotic expressions of secrecy performance metrics are obtained in closed form after deriving the channel statistics.

- The secrecy performance of the two-user MIMO-NOMA-aided AN for mixed RF-FSO transmissions in the presence of multiple eavesdroppers is investigated. To begin with, the statistical properties of the underlying system model are studied. Using the derived expressions of the channel statistics, we obtain the analytical expressions of the SOP, asymptotic SOP, probability of the SPSC and the ASC in a closed form.

1.3 Thesis Outline

The subsequent chapters of the thesis are structured as follows.

Chapter 2 provides a comprehensive review of the existing works in the literature relevant to the PLS with a focus on mixed RF-FSO systems. These works encompass different approaches proposed to enhance the security and reliability of diverse system architectures. These approaches include MIMO, NOMA, TAS, cooperative relaying and mixed/hybrid systems.
Chapter 3 investigates the PLS of a two-user MIMO NOMA with TAS in mixed RF-FSO systems. Considering fixed gain relaying scheme, the channel statistics for the underlying system model are presented and then used to derive the analytical expressions for the SOP, the probability of the SPSC, ASC, and asymptotic ASC.
Chapter 4 builds upon the system model established in Chapter 3, this chapter extends the investigation to incorporate an AN signal and assume a variable gain at the relay node. The secrecy performance is analyzed under varying pointing errors, detection techniques and turbulence conditions. Considering this system model, the channel statistics are studied for the mixed RF-FSO links. Finally, the analytical expressions for the SOP, the probability of SPSC, and ASC are derived in a closed forms. Moreover, the asymptotic expression for SOP is derived in terms of the expansion of Meijer's G-function.
Chapter 5 extends the investigation of the two-user MIMO-NOMA system with TAS in a mixed RF-FSO system in the presence of multiple colluding and non-colluding eavesdroppers. Moreover, the secrecy performance of the underlying system model is analyzed considering different RF and FSO link conditions. To enhance the secrecy performance of the underlying system, the injection of AN from both users is adopted to counteract the deleterious influence of multiple eavesdroppers. Finally, the numerical analysis is presented for different RF and

FSO link conditions.

Chapter 6 provides a comprehensive summary of the work presented in this thesis, highlighting key findings and contributions. Following the summary, some concluding remarks are offered to reflect on the significance of the research and its implications. Finally, potential avenues for future research based on the completed work are discussed, identifying areas where further investigation could expand upon the current findings and address remaining challenges.

CHAPTER 2

Literature Survey

2.1 Introduction

In this chapter, we present a comprehensive review of the emerging wireless technologies explored in this thesis. To begin with, we introduce the principles of non-orthogonal multiple access (NOMA) and multiple-input-multiple-output (MIMO) technologies. Then, we present the benefits offered by integrating NOMA in MIMO systems. Subsequently, we present challenges of MIMO-NOMA systems associated with resource allocation, signaling, and security challenges. Next, the discussion shifts to the physical layer security (PLS) recognized as a promising security solution within MIMO-NOMA systems. Furthermore, the discussion will be extended to the PLS wherein the security aspect of standalone radio frequency (RF) and free-space optical (FSO) systems are considered as well as mixed and hybrid RF-FSO systems. In addition, a general review of the recent related works investigating PLS in a mixed/hybrid RF-FSO systems under different system architectures and performance metrics is presented.

2.2 Non-Orthogonal Multiple Access

In the last decade, there has been a substantial surge in the demand for high-data rates and continuous connectivity in wireless communication systems, essential for supporting a wide array of applications ranging from video streaming, voice calls, email to file transfers and internet browsing [22]. To accommodate this, upcoming wireless applications face various challenges that require careful considerations. One of these challenges is bandwidth scarcity, as the availability of this resource to service providers is often constrained [23]. In order to address these challenges, NOMA has recently been introduced as a promising solution to tackle the bandwidth scarcity. It facilitates concurrent service of multiple users within the same time, code and frequency resource block (RB) through superposition coding (SC) at the transmitter [24]. This inherent characteristic of NOMA provides connectivity, enhances spectral efficiency (SE), and handles the high data traffic [25, 26]. Many works have validated the superior performance of NOMA over orthogonal multiple access (OMA) [27–29]. In [27], it is demonstrated that the NOMA scheme for a simple two-user scenario outperforms OMA in terms of both sum rate and ergodic sum rate. Moreover, It is indicated in [28] that NOMA enhances both the capacity and throughput of cell-edge users in terms of the system-level evaluation. Furthermore, the authors in [29] demonstrates that NOMA can achieve a better performance in scenarios involving randomly deployed users.

2.2.1 Fundamental Principles of NOMA

There exists two main categories of NOMA: **(1) power domain (PD)-NOMA**; and **(2) code domain (CD)-NOMA**. In PD-NOMA, users are permitted to share the same resources but with different power levels. This power allocation strategy enables simultaneous transmission to multiple users within the same RB, thereby enhancing spectral efficiency [30]. On the other hand, CD-NOMA enables the simultaneous transmission of multiple user signals over the same time-frequency resource, leveraging unique codebooks assigned to each user [31]. Next, we provide an overview of NOMA in both downlink and uplink transmissions.

2.2.2 Downlink NOMA Transmission

Figure 2.1 depicts a downlink NOMA transmission where the base station (BS) transmits a composite signal consisting of the desired signals of both the near-user (NU) and far-user (FU). The users are allocated different power levels with more power to the FU due its bad channel conditions and less power to the NU due to it good channel conditions. At the receiver side, the NU first decodes the signal of the FU, and then removes the FU's signal before decoding its own signal.

2.2.3 Uplink NOMA Transmission

In the uplink NOMA transmission illustrated in Figure 2.2, each user transmits its signal to the BS. Then, the BS first decodes the FU's signal while treating NU's

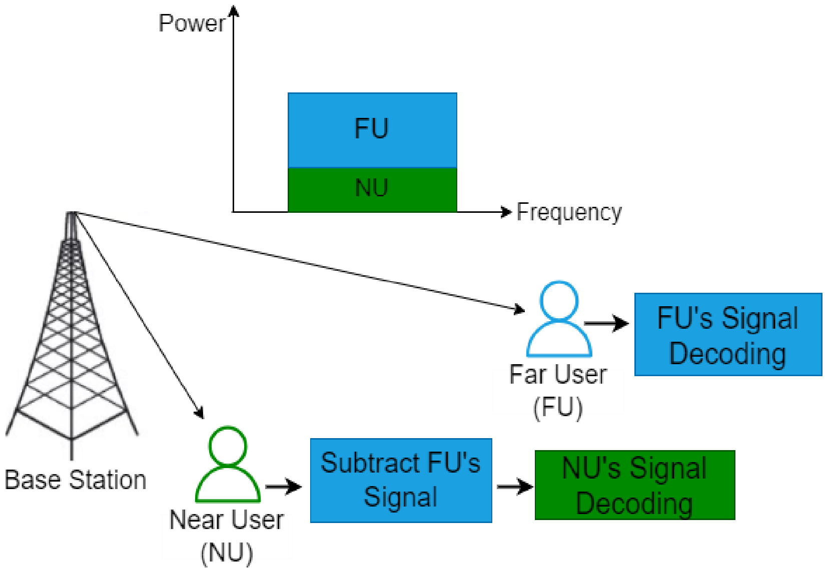

FIGURE 2.1: illustration of two-users down link NOMA

signal as noise, and subsequently apply the successive interference cancellation (SIC) to decode NU's signal.

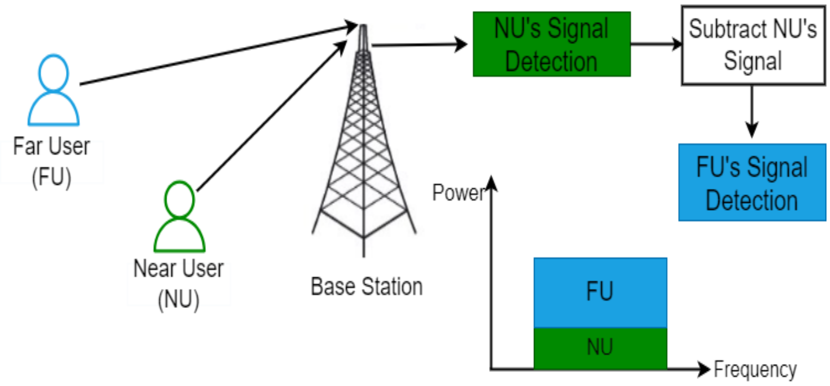

FIGURE 2.2: illustration of two-users uplink NOMA

2.3 Multiple-Input Multiple Output

Multiple-input multiple-output (MIMO) is a pivotal technology in wireless communication that enhances data transfer rates and system reliability. By employing multiple antennas at both the transmitter and receiver ends, MIMO exploits spatial diversity, allowing for the simultaneous transmissions of multiple data streams to reduce the probability of errors. This technique provides robustness of signal transmissions against multi-path fading leading to an improvement of the system performance via high capacity, low error rate, and transmit/receive diversity. As a result, MIMO has become a fundamental component of modern wireless communication standards including wireless-fidelity (Wi-Fi), long-term evolution (LTE), and fifth-generation (5G) [32,33]. For instance, in modern Wi-Fi standards such as 802.11ac and 802.11ax, MIMO has enabled significant improvements in data rates and network coverage by allowing multiple data streams to be transmitted simultaneously. Recently, the advent of MIMO technology has revolutionized various communication systems. In the realm of cellular networks, operators like Verizon and American Telephone and Telegraph (ATT) have successfully deployed MIMO in their LTE and 5G networks, resulting in enhanced spectral efficiency and better user experience [34]. Furthermore, the synergy between MIMO and beamforming techniques has proven invaluable in smart home ecosystems. MIMO facilitates robust and reliable connectivity between a multitude of devices, ensuring seamless communication within a connected home environment. Beamforming further optimizes signal transmission by directing it towards specific devices, mitigating interference and improving overall network performance [35]. In addition, field trials conducted by leading telecom equipment manufacturers have consistently demonstrated the superior performance of MIMO systems in real-world environments, solidifying its role as a cornerstone of modern communication technology [36]. Despite these advantages, MIMO suffers from some limitations such as an increase of the computational complexity and hardware cost. This is due to the fact that additional antenna elements not only increases hardware costs but also necessitates additional computational power [37]. Therefore, it is crucial to employ some techniques capable of overcoming the aforementioned limitations and leveraging spatial diversity. Some common approaches provided in the existing literature are discussed subsequently.

2.4 Antenna Selection

Antenna selection is an efficient technique in MIMO systems that enables complexity and hardware cost reduction. This approach allows for a single or a subset of antennas among several antennas to be selected to transmit or receive. In this regards, there exist two categories of antenna selection techniques: transmit antenna selection (TAS) and receive antenna selection (RAS) [38]. In what follows, we provide some discussion on these techniques.

2.4.1 Transmit Antenna Selection

Transmit antenna selection (TAS) is adopted at the transmitter side by selecting a single antenna or a set of antennas based on a given criterion. This leads to a reduction in the number of RF chains, and therefore reduction in the hardware cost and computational complexity for a more viable system [39]. In TAS, a feedback of the channel state information (CSI) is required between the receiver and transmitter to inform the latter about the selected antenna, enabling the transmitter to choose the optimal antenna configuration for transmission. It is well-established that TAS achieves maximum capacity when the transmitter has complete CSI knowledge [40]. This capability is crucial in improving system performance by optimizing antenna selection based on real-time channel conditions, thereby enhancing throughput and reliability in MIMO communication systems.

2.4.2 Receive Antenna Selection

In receive antenna selection (RAS), the receiver perceives multiple replicas of the transmitted signal, each subject to distinct fading coefficients. To capitalize on this diversity, a subset of receive antennas is strategically selected to capture the signal variations [41]. These antennas are then combined in order to improve the signal-to-noise ratio (SNR) of the received signal, thereby enhancing the overall performance of the communication system. Through this process, RAS effectively mitigates the impact of fading and noise, resulting in more reliable and robust signal reception [42].

2.5 Combining Schemes (CS)

The multiple replicas of the transmitted information need to be combined at the receiver before the demodulation process. In what follows, we discuss the different combining schemes that have been widely reported in the existing literature.

2.5.1 Selection Combining

The selection combining (SC) is a sub-optimal combining scheme and the simplest of the combining schemes [43]. In this scheme, only one receive antenna with the maximum SNR is active to demodulate the original modulated signal sent by the transmitter yielding reduction of the hardware complexity at the receiver [44]. Assuming N received antenna at the receiver, the instantaneous SNR denoted by γ_{SC} for the selected antenna can be expressed as [45, Eqn. (3)]

$$\gamma_{SC} = \max_{i=0,\ldots,N} \gamma_i, \tag{2.1}$$

where $i \in \{1, \ldots, N\}$. One of the key advantages of SC is its ability to accommodate both differentially coherent and noncoherent modulation techniques without the need for co-phasing multiple receiver outputs, thus simplifying the receiver design [45]. This makes SC particularly attractive for applications where simplicity and hardware efficiency are prioritized. However, despite its simplicity and hardware efficiency, SC suffers from the performance degradation compared to other combining schemes such as maximum ratio combining (MRC) and equal gain combining (EGC). Since SC only uses the branch with the highest SNR, it does not fully exploit the diversity gain available from multiple antennas. Consequently, the system performance is sub-optimal particularly in environments with severe fading and interference. In the context of a mixed RF-FSO systems, SC can offer a balance between hardware simplicity and performance. While it may not provide the highest possible secrecy performance, its ease of implementation and reduced complexity make it a suitable option for scenarios where these factors are critical [46].

2.5.2 Maximum Ratio Combining

Unlike the SC wherein a single branch is used at the receiver output, in MRC scheme, the received signals are combined with the gain of their respective channels in order to maximize the output SNR at the receiver [42]. This is achieved by adjusting the weights assigned to each received signal in such a way that the amplitudes of the signals are combined coherently, taking into account the respective channel gains and phases [47]. MRC works by assigning a weight to each received signal proportional to its SNR, ensuring that stronger signals have a greater influence on the combined output. Mathematically, for L received branch, the total combined instantaneous SNR denoted by γ_{MRC} for equally transmitted signals at the output of the MRC combiner is given as [48, Eqn. (9.1)]

$$\gamma_{MRC} = \sum_{l=1}^{L} \gamma_l, \tag{2.2}$$

where $l \in \{1, \dots, L\}$. This coherent combination effectively amplifies the desired signal while minimizing the impact of noise and interference, leading to an optimal improvement in the overall system performance. Although MRC achieves the best possible performance, it requires knowledge of the SNR on each receiving antenna. This requirement is intricate to obtain in real-world scenarios due to the dynamic nature of wireless channels and the complexity of achieving accurate channel estimation. Furthermore, implementing MRC increases the computational complexity and hardware requirements at the receiver. In the context of underlying mixed RF-FSO systems, employing MRC could significantly enhance secrecy performance by optimally combining the received signals. However, the complexity and need for accurate CSI must be carefully managed to realize these benefits in practical implementations.

2.5.3 Hybrid Selection

Hybrid selection combining, also termed as EGC strikes a balance between both the SC and MRC schemes. To address the challenge of obtaining the time-varying SNR on each branch, a simpler combining technique in the EGC can combine signals from co-phased branches with equal gain [47]. In EGC, the received signals from multiple antennas are co-phased and then summed with equal weighting. This approach avoids the need for precise SNR measurements for each branch, simplifying the implementation compared to MRC [49]. The EGC ensures that the signals are added constructively, enhancing the overall SNR at the receiver [46]. Mathematically, the instantaneous SNR at the receiver's EGC output, denoted by γ_{EGC} can be expressed as [48, Eqn. (9.46)]

$$\gamma_{\mathrm{EGC}} = \frac{\left(\sum_{l=1}^{L} \alpha_l\right)^2 E_s}{\sum_{l=1}^{L} N_l}, \tag{2.3}$$

where α_l represents the channel gain between the transmitter and the l-th received branch, E_s is the power per symbol and N_l is the AWGN power spectral density on the l^{th} path. This scheme offers a trade-off between performance and hardware complexity. While it does not achieve the optimal performance of MRC, it performs better than SC by utilizing signals from multiple branches. This makes EGC suitable for practical scenarios where hardware complexity is a concern but improved performance is desired [42]. In the context of the proposed system model, EGC is particularly relevant as it provides a viable solution for enhancing the secrecy performance of mixed RF-FSO systems without incurring the high complexity and stringent CSI requirements of MRC.

2.6 MIMO-NOMA Systems

To further optimize the performance gains of NOMA and leverage additional spatial degrees of freedom alongside the power domain, MIMO can be incorporated into NOMA. This holds particular advantages in scenarios where multiple users are positioned in the same spatial direction but at different propagation distances [50]. Moreover, MIMO-NOMA systems can serve multiple users utilizing shared resources, thereby enhancing the overall system capacity [51]. Numerous studies have consistently demonstrated the superior performance of MIMO-NOMA over the single-antenna OMA. In this regards, early work such as [52] focus on maximizing the ergodic sum capacity (ESC) of a rayleigh fading MIMO-NOMA/MIMO-OMA systems with statistical CSI at the transmitter. This work proposed both optimal and low complexity sub-optimal power allocation schemes to maximize the ergodic capacity (EC) of both MIMO-NOMA/MIMO-OMA systems with total transmit power and minimum rate constraint. It is demonstrated that MIMO-NOMA achieves a larger ergodic sum capacity compared to MIMO-OMA. In addition, [53, 54] have validated the superiority of MIMO-NOMA over MIMO-OMA in terms of sum channel capacity and the number of the allocated users. In [53], it is illustrated that MIMO-NOMA surpasses MIMO-OMA in terms of sum channel capacity, except when communicating with only one user. Specifically, for any rate pair achievable by MIMO-OMA, there exists a power split for which MIMO-NOMA can achieve rate pairs that are strictly greater. This finding extends to the sum EC, confirming that MIMO-NOMA can achieve a larger sum EC compared to MIMO-OMA. Moreover, the performance of MIMO-NOMA is investigated in [54] when multiple users are grouped into a cluster. The superiority of MIMO-NOMA over MIMO-OMA in terms of both sum channel capacity (SCC) and ESC is proved analytically in this work. Additionally, it is demonstrated that the more users are admitted to a cluster, the lower is the achieved sum rate, which illustrates the trade-off between the sum rate and maximum number of admitted users. Next, we present the main categories of MIMO-NOMA systems as outlined in [26]:

- The cluster-based MIMO-NOMA structure organizes users into clusters, where multiple users within a cluster share the same resources simultaneously [55]. This approach aims to optimize resource allocation, enhance spectral efficiency, and improve overall system capacity by exploiting diversity in users' channel conditions within each cluster.

- The beamformer-based MIMO-NOMA structure employs advanced beamforming techniques to optimize signal transmission through strategic beamformer design [56]. These techniques manipulate antenna array weights to direct the transmitted signal in specific directions, enhancing signal quality at intended receivers while mitigating interference from other users. Leveraging the spatial domain, beamforming enables MIMO-NOMA systems to achieve improved spectral efficiency and enhanced signal reliability, making it indispensable in modern wireless communication networks.

The design of the MIMO-NOMA system encountered certain challenges summarized in subsequent subsections

2.6.1 Resource Allocation Challenges

The adoption of multiple antennas at both the transmitter and receiver introduces intricate interference challenges in MIMO-NOMA transmissions. This interference is particularly notable in cluster-based MIMO-NOMA systems where both intra-cluster and inter-cluster interference issues may arise [26]. To effectively address these interference challenges and optimize system performance, various resource allocation strategies are employed in MIMO-NOMA systems. These strategies can effectively mitigate interference effects and enhance overall system efficiency, with the goal of minimizing power consumption while improving SE. User clustering/user pairing, power allocation (PA), and joint user pairing and power allocation techniques are encompassed in these strategies. Different approaches have been employed to address resource allocation challenges in the context of the aforementioned issues [54, 57, 58], and will be elaborated in the sequel.

2.6.1.1 User Pairing

In NOMA, users with varying channel gains are grouped within a single RB in the power domain. This allocation involves assigning higher power to users with weaker channel gains and lower power to those with stronger channel gains, promoting user fairness [59]. The weak users decode the superimposed signal by treating signals from strong users as noise, while the strong user employs SIC in down-link to decode its own signal. In the context of MIMO-NOMA where multiple antennas are employed, the spatial dimension is leveraged through spatial multiplexing to simultaneously transmit multiple data streams. However, the allocation of users and power in MIMO-NOMA requires more intricate strategies. Specifically, user pairing in MIMO-NOMA involves the strategic of assigning users to different spatial streams considering their channel conditions. This ensures that each user's signal is optimally transmitted using the available spatial resources. For instance, weaker users may be paired with stronger users to achieve better overall system performance. This strategic pairing optimizes the utilization of the spatial dimension, resulting in enhanced system capacity through spatial multiplexing gains. In [54], the optimal user admission scheme is proposed in terms of both the sum rate and the number of admitted users when the signal-to-interference-plus-noise ratio (SINR) thresholds of users are equal. Even in scenarios where these thresholds vary, the proposed scheme maintains a commendable performance by effectively balancing both criteria.

2.6.1.2 Power Allocation

Achieving optimal PA poses significant challenges in MIMO-NOMA systems. These challenges stem from the complexity of multi-antenna users in NOMA where users are separated by different power levels within a single RB [52,60]. One major challenge is the computational complexity associated with implementing PA strategies, considering the numerous antennas, user pairs, and interference conditions. Additionally, managing interference becomes crucial for maximizing system capacity while minimizing interference levels among users [57]. Ensuring fairness in data rate distribution among paired users presents another challenge, requiring careful consideration of user channel conditions and PA strategies. Moreover, the robustness of PA techniques is essential to address performance degradation due to imperfect channel estimation, user mobility, and varying interference levels. In the light of above, the implementation of suitable PA strategies is essential to optimize the overall performance of the communication system [61]. Overcoming these challenges is crucial to optimize the overall performance of MIMO-NOMA systems. For instance, artificial intelligence (AI) holds significant potential to PA strategies in MIMO-NOMA systems [62]. AI algorithms can dynamically optimize PA by analyzing real-time data and adapting to changing network conditions, thereby improving overall system performance and efficiency. One key advantage of AI in PA is its capacity to handle the computational complexity associated with MIMO-NOMA systems. By employing machine learning techniques, AI can efficiently manage the numerous antennas and interference conditions, reducing the computational demands and enabling more accurate PA decisions.

2.6.1.3 Joint User Pairing and Power Allocation

The combination of multi-antenna user pairing and power allocation in MIMO-NOMA systems presents a strategic approach to efficiently manage resources and optimize system performance. This consists of pairing users with varying channel conditions and dynamically allocating power within shared RB [58]. However, this integrated strategy introduces several challenges, including computational complexity, interference management, and fairness in resource allocation [63]. The computational complexity arises considering multiple factors such as user channel conditions, interference levels, and system constraints while optimizing user pairing and power allocation. Moreover, managing interference becomes crucial to maximize system capacity and ensure fair data rate distribution among paired users. Additionally, ensuring robustness in power allocation techniques is essential to address performance degradation due to imperfect channel estimation and varying interference conditions [64]. Despite these challenges, the integration of multi-antenna user pairing and power allocation holds significant promise for enhancing spectral efficiency and overall system capacity in MIMO-NOMA-enabled wireless communication systems [26]. In [65], the joint user clustering and power allocation (JUCPA) strategy combined with robust beamforming design is proposed to mitigate inter-user interference (IUI) and inter-cluster interference (ICRI) in MIMO-NOMA systems. In this algorithm, the optimal user pair is selected as a cluster in order to achieve a higher sum-rate. It is demonstrated that the proposed robust beamforming design, in conjunction with the JUCPA algorithm, notably enhances system performance in terms of sum-rate compared to existing MIMO-NOMA schemes.

2.6.2 Signaling Challenges

The combination of MIMO and NOMA technologies introduces intricate signaling challenges due to its design complexity. Addressing these signaling challenges in

MIMO-NOMA systems is crucial for enabling reliable and efficient communication. The utilization of SIC and efficient feedback systems are key components in overcoming these challenges [66].

2.6.2.1 Successive Interference Cancellation

The implementation of SIC faces challenges related to receiver complexity, which can lead to system performance degradation due to incorrect decoding of signals from weaker users. In MIMO-NOMA, the main challenge faced by SIC arises from the non-orthogonal transmission where multiple users utilize the same time-frequency resource. Moreover, incorporating multiple antennas at both the transmitter and receiver can increase the hardware complexity and the number of interfering signals. Addressing these challenges requires advanced signal processing techniques, adaptive algorithms, and efficient coordination of user pairing and power allocation strategies [26]. While SIC is a powerful tool for interference mitigation, its effectiveness in the context of MIMO-NOMA depends on addressing the complexities introduced by non-orthogonal transmission and multi-antenna configuration. In [66, 67], the issue related to the imperfect SIC has been solved by adopting machine learning (ML) approach. Specifically, a deep learning-based approach is adopted in [66] while a deep neural network-based algorithm is proposed in [67].

2.6.2.2 Channel State Information

Utilizing partial CSI that incorporates path loss information with employing constrained feedback mechanisms for precoding matrices represent potential strategies to mitigate the challenges associated with overhead and signaling in the context of CSI [68]. These strategies enable efficient utilization of available channel information while minimizing the feedback overhead. Additionally, techniques such as feedback compression and codebook-based feedback can further enhance the efficiency of CSI utilization in MIMO-NOMA systems. These methods ensure that the transmitted signals are adapted to the varying channel conditions, thereby optimizing system performance and spectral efficiency. Considering the accuracy of channel information at the transmitter, CSI can be categorized as either perfect or imperfect. Both perfect and imperfect CSI play crucial roles in context of MIMO-NOMA systems performance [69]. In perfect CSI, accurate channel information is available at the transmitter enabling optimal power allocation and beamforming strategies. However, perfect CSI requires extensive feedback and signaling overhead, which can be impractical in real-world scenarios due to limited resources and channel estimation errors [70]. On the other hand, imperfect CSI reflects the practical limitations and uncertainties associated with channel estimation and feedback mechanisms. Imperfect CSI can result in suboptimal power allocation, ineffective interference management, and overall degradation in system performance. Consequently, a performance gap emerges between practical MIMO-NOMA systems with imperfect CSI and ideal MIMO-NOMA systems with perfect CSI. This performance gap can directly be proportional to the transmit power of the information signal and inversely proportional to the accuracy of CSI. To ensure consistent performance, the transmit energy of the pilot sequence for channel estimation should increase alongside the transmit power of the information signal [71]. Additionally, AI-based learning algorithms can be utilized for channel estimation to achieving better performance compared to conventional techniques [72]. These AI-assisted channel estimation are highly relevant to 5G/6G communications, as AI is considered a foundational element of future networks [73, 74]. For instance, 5G/6G networks will operate in millimeter and terahertz frequencies to overcome bandwidth limitations and increase throughput. However, this introduces greater channel complexity due to higher attenuation and atmospheric absorption. Furthermore, key technologies such as massive MIMO will add to the complexity of transceiver architecture, creating new challenges for channel estimation. While the multicarrier systems can mitigate some of early-mentioned effects, advanced channel estimation techniques are still needed for diverse architectures and environments. Therefore, the use of AI to enhance these techniques is essential, as it can help create an intelligent physical layer and optimize system performance through virtualized tools [75–78].

2.6.3 Security in MIMO-NOMA

The inherent design of MIMO-NOMA introduces vulnerability of wireless transmissions to potential eavesdropping threats [79]. Traditionally, secure communication relies on cryptography methods, introducing heightened computational complexity to ensure security. One promising approach is the PLS which leverages the intrinsic characteristics of wireless channels. By exploiting some features pertaining to the MIMO-NOMA technology such as spatial multiplexing and power domain multiplexing, PLS can be designed to mitigate eavesdropping attempts and unauthorized access. This approach provides an additional layer of protection beyond traditional encryption methods [14], making it particularly relevant in the context of MIMO-NOMA's security challenges.

2.7 Physical Layer Security

The key idea behind information theory-based PLS is to exploit the fading properties of the wireless channel for secure message transmission in the presence of an eavesdropper which is an unauthorized user that tries to intercept or gather the confidential information transmitted to an authorized user [14, 80]. Unlike traditional approaches, PLS operates autonomously irrespective of computational complexity. In addition, the system can still ensure secure and dependable communications even in the presence of sophisticated computational devices wielded by potential eavesdroppers in 5G networks [81]. There exists two types of eavesdropping attacks which may differently impact the wireless communications:

- Passive eavesdropping: In this scenario, the eavesdropper(s) can adeptly intercept communication without actively manipulating or tampering with the signals. This type of attack enables the eavesdropper(s) to quietly listen the wireless transmission and gather information without being detected. Generally, the adoption of some techniques such as the multi-antenna at the transmitter or the intended user(s) can help improve the potential presence of passive eavesdropper in the system.
- Active eavesdropping: This type of attack is more intrusive and more detrimental to the security performance of wireless system as the eavesdropper(s) are actively involved in the interception of the transmitted data with the aim to modify them. To counter such attacks, an efficient method consists of injecting artificial noise (AN) [82, 83], where the noise is carefully designed to enhance the signals intended for authorized users while confounding and disrupting the eavesdroppers' efforts.

As above mentioned, it is possible to combat the eavesdropping attacks (regardless of their nature) through efficient techniques that will make it challenging for unauthorized users to listen or intercept the transmitted data, let alone decipher the original information [11,84]. In what follows, we delve into the security aspect of various systems such as RF, FSO, and mixed/hybrid RF-FSO.

2.7.1 Physical Layer Security in RF systems

The inherent characteristics of RF signals enabling them to effectively penetrate obstacles and adapt to a variety of atmospheric conditions, contribute to their resilience against turbulence. This quality is advantageous, particularly in scenarios where environmental factors, such as atmospheric turbulence might pose challenges to the communication systems [85]. However, the problem with such transmissions is that the RF spectrum has become congested due to the proliferation of wireless applications and services. Moreover, these transmissions can be compromised by the potential eavesdropping attacks due to the broadcast nature of the wireless channels, and therefore pose a security threat to the overall system. Many studies have recently analyzed the security of MIMO-NOMA over the RF spectrum band [86–90]. These studies have extensively investigated PLS by employing various approaches to enhance the secrecy performance. One crucial approach involves AN injection [32,90], introducing uncertainty into transmitted signals and thereby complicating the decoding process for potential eavesdroppers. Moreover, the utilization of accurate CSI enables adaptive strategies, dynamically adjusting transmission parameters to counteract real-time eavesdropping attempts. Furthermore, the MIMO technology can be exploited to improve the capacity, making it more challenging for eavesdroppers to intercept the transmitted information [89,91]. In NOMA systems, PA optimization aims to maximize the secrecy rate of legitimate users and thereby enhance security, this power allocation strategy enhances security and defends against external eavesdropping [92,93]. However, NOMA-based networks face potential threats from both internal and external eavesdropping where the former involves an unauthorized access by other users within the NOMA system posing a significant security challenge, while external eavesdropping entails interception attempts from users outside NOMA network [94–97].

2.7.2 Physical Layer Security in FSO Systems

The FSO technology has emerged as an attractive and promising technique for optical wireless communications (OWC) since they can be used in the unlicensed spectrum band and can also provide high-data rates and high security [79]. On the latter, FSO systems are notably secure due to the nature of a high-directional beam. Due to these characteristics, the FSO technology can be used as an alternative to its RF counterpart where the latter is limited (spectrum scarcity, hardware cost, power consumption, interference, etc..) as it is shown in Table

2.1. Despite these advantages, FSO is very susceptible to atmospheric turbulence which can lead to the degradation of the system performance. In addition, thermal expansion and fluctuating wind forces contribute to the occurrence of building sway, inducing vibrations in the transmitter beam. This phenomenon can result in misalignment between the transmitter and receiver, commonly referred to as a pointing error [98, 99]. In urban environments particularly on high-rise buildings where FSO transmitter and receiver are generally placed, pointing errors are prevalent and pose a significant challenge as they have the potential to cause substantial degradation in system performance. Another challenge with FSO systems is the security concerns in scenarios wherein an eavesdropper is placed close to the receiver [100]. In such a scenario, it is possible for the eavesdropper to intercept the communication between the transmitter and the intended receiver due the pointing errors. In response, PLS can be adopted in the context of FSO systems to mitigate security threats using different approaches including beam direction control and utilization of narrow beam-width to minimize signal exposure. Additionally, the mechanism for pointing error correction ensure the accurate alignment of FSO transceivers and further reduces vulnerabilities [98, 101–104].

Table 2.1: A comparison of RF and FSO Spectrum Bands.

Characteristics	**RF**	**FSO**
Device size	Small	Large
Power consumption	Low	Moderate
EM Interference	High	No
Spectrum	Licensed	Unlicensed
Security	Low	High
Transmission	NLOS	LOS
Limitation	Spectrum	Environment

2.7.3 Physical Layer Security in Mixed/Hybrid RF-FSO Systems

In the evolving landscape of wireless communication, RF and FSO systems have emerged as pivotal technologies, each offering distinct advantages. RF systems, renowned for their robustness and extensive range, are widely utilized in various communication applications. In contrast, FSO systems are highly valued for their high data rates and wide bandwidth, making them ideal for high-capacity point-to-point communication [79]. However, both technologies face certain limitations—RF systems can suffer from spectrum congestion, security vulnerabilities and interference, while FSO systems are highly susceptible to atmospheric conditions such as fog, rain, and turbulence [105]. To tackle the inherent challenges faced by the standalone RF and FSO systems (see Table 2.1), mixed and hybrid RF-FSO systems have emerged as a good candidate to provide robust link availability, reliability and high level of security particularly in severe weather conditions [85, 106]. These mixed/hybrid networks find their applications in effective long-distance communication scenarios such as in inter-satellite, satellite-to-earth or earth-to-satellite, airplane-to-satellite, airplane-to-ground, airplane-to-airplane, and ship-to-ship communications where a relay node can be adopted to extend the network coverage. In the following subsections, the definitions and functionalities of hybrid RF-FSO systems and mixed RF-FSO systems are presented, emphasizing their roles in modern communication infrastructures.

2.7.3.1 Hybrid RF-FSO Systems

Hybrid RF-FSO systems combine the advantages of both RF and FSO communication technologies to improve the overall performance and reliability of wireless communication networks [85]. In a hybrid RF-FSO system, both RF and FSO links are used simultaneously or selectively to ensure a robust communication link. The RF link is typically used as a backup to the FSO link, which can be affected by atmospheric conditions such as fog, rain, and turbulence. This hybrid approach leverages the high data rates and wide bandwidth of FSO communication while maintaining the reliability and extended range provided by RF communication.

2.7.3.2 Mixed RF-FSO Systems

Mixed RF-FSO systems refer to communication networks where RF and FSO links are used in a complementary manner within different parts of the network. In such systems, the first and second link (transmitters to relay and relay to intended receiver, respectively) can either be FSO or RF link depending on the specific requirements and environmental conditions [107]. For example, FSO links might be used for high-capacity point-to-point communication between buildings, while RF links provide coverage and connectivity in areas with obstacles or in adverse weather conditions. The mixed RF-FSO approach allows for optimized network performance by using the most suitable technology for each segment of the network. Driven by the potential of mixed RF-FSO systems, the investigation of PLS has garnered significant attention in the existing literature [17,20,108,109].

As concluded in [17], the secrecy performance under weak atmospheric turbulence conditions is superior to that under strong turbulence conditions. Moreover, the secrecy performance has shown less influence in the RF link with variable gain relaying, and the pointing error deteriorates the secrecy performance of mixed systems. In [108], the secrecy performance of a mixed RF-FSO dual-hop communication system with both fixed-and variable-gain relaying schemes has been investigated wherein eavesdropping is assumed to be closed to RF link due to the high security of optical links.

The integration of NOMA in mixed/hybrid RF-FSO systems represents a promising step towards the optimization of SE in mixed/hybrid systems. In this regard, the performance analysis of these mixed/hybrid systems with downlink NOMA has recently been investigated in [110,111]. Particularly, the BS as an FSO source communicating with two RF NOMA users via an intermediate amplify-and-forward (AF) relay in the presence of an eavesdropping attack are assumed in [110]. To analyze the secrecy performance, the closed-form expression of the secrecy outage probability (SOP) is derived for the NU. To this end, it is indicated that the secrecy performance improves as the PA ratio dedicated to the NU user increases. To get more insights, closed forms of the SOP and strictly positive secrecy capacity (SPSC) for the overall NOMA system "NU and FU users" are derived in [111]. Additionally, the asymptotic analysis of SOP is analyzed at high SNR. It is shown that the SOP is approximately constant in the high-SNR regime, while the overall secrecy performance is independent of the channel conditions of the weak user.

The incorporation of MIMO in hybrid RF-FSO systems can improve the confidentiality and integrity of transmitted information, making the hybrid system well-equipped to operate securely in different challenging environments [112]. The performance of hybrid MIMO-RF/FSO systems is analyzed in [113] where four TAS schemes are proposed. The closed-form expressions for SOP and asymptotic effective secrecy throughput (EST) are obtained considering imperfect CSI. Additionally, the secrecy performance of mixed RF-hybrid RF-FSO and hybrid RF-RF/RF-FSO systems is analyzed in [21] under the presence of multiple eavesdroppers. It is shown that the hybrid RF-RF/RF-FSO scenario outperforms the mixed FSO-RF and mixed RF-hybrid RF-FSO systems, highlighting the effectiveness of the proposed system configurations.

2.8 Conclusion

This chapter provides a comprehensive review of the key concepts discussed throughout this thesis. Initially, the fundamental principles of NOMA and MIMO systems are explored, emphasizing the substantial advantages of combined MIMO-NOMA systems. Following this, potential challenges within MIMO-NOMA systems such as resource allocation, signaling intricacies, and security concerns are examined to highlight the complexities inherent in this advanced communication paradigm. The chapter further explore PLS as a promising security solution within MIMO-NOMA systems, underscoring its significance in ensuring the security of wireless communications. Extending the discourse to encompass PLS in the mixed and hybrid RF-FSO spectrum bands provides a comprehensive understanding of the challenges associated with securing communication in diverse environments. Finally, the inclusion of a broad review of recent works investigating PLS in mixed/hybrid RF-FSO systems, considering various system architectures and performance metrics, is presented.

CHAPTER 3

Secrecy Performance of Uplink MIMO-NOMA with Antenna Selection in a Mixed RF-FSO System

3.1 Introduction

In recent years, the surge in data traffic has led to an unprecedented demand for spectrum resources, creating an environment of spectrum congestion. This issue has been further exacerbated by the continuous advancements in future wireless technologies, indicating that the demand for spectrum resources is likely to persist in the foreseeable future. The overcrowded spectrum band poses significant challenges to accommodate the ever-growing communication needs. In response to this pressing concern, non-orthogonal multiple access (NOMA) has emerged as a promising technology. NOMA holds the potential to address the spectrum scarcity issue efficiently and provide a pathway for achieving massive connectivity. It allows multiple users to be served concurrently in the same time, code, and frequency resource block (RB) through superposition coding (SC) at the transmitter and successive interference cancellation (SIC) at the receiver [24]. This approach effectively eliminates interference within the NOMA framework, enhances spectrum efficiency and supports large number of connected devices simultaneously. The adoption of NOMA represents a strategic step towards optimizing spectrum utilization and meeting the escalating demand for wireless connectivity in the evolving landscape of modern communication systems [114, 115].

To further bolster the system performance, the multiple-input-multiple-output (MIMO) technology has been incorporated into NOMA [3]. This integration lies in the recognition that the utilization of multiple antennas introduces additional degrees of freedom to the system. MIMO technology exploits spatial diversity by employing multiple antennas at both the transmitter and receiver ends, allowing

for the simultaneous transmission of multiple data streams. This spatial multiplexing capability not only enhances the overall spectral efficiency of NOMA but also contributes to improved reliability and increased data throughput [116].
The sharing of radio resources among users, as mentioned earlier, is anticipated to introduce security concerns owing to the inherent nature of wireless transmissions. Consequently, in the context of the aforementioned considerations, security has become a notable concern in the development of upcoming wireless systems. Traditionally, users' confidentiality has been addressed in the upper layer of the open system interconnect (OSI) model through the use of complex encryption-based protocols that require a secret key [117]. With the development of sophisticated mathematical algorithms, these secret key-based protocols are no longer reliable. In light of the above, physical layer security (PLS) offers an alternative approach and/or a complement to the secret key-based mechanisms [11–13]. This technique is used to ensure secure communication with the intended receiver by taking advantage of the intrinsic characteristics of wireless channels. Some research studies have recently investigated the secrecy performance of MIMO-NOMA systems in the radio frequency (RF) spectrum band [4, 5, 60, 118, 119]. The problem with the RF spectrum band is that it has now become overcrowded due to the exponential growth of wireless devices and applications, and is vulnerable to security threats. In contrast to the RF communications, free-space optical (FSO) transmissions operate in the unlicensed band and are inherently more secure and can offer high data rates making them suitable for future wireless applications. Numerous studies have analyzed the secrecy performance in FSO systems, recognizing their potential for secure communication [100, 102, 120–123]. However, it is crucial to note that FSO systems come with inherent challenges, particularly sensitivity to atmospheric turbulence conditions and pointing errors. These factors can significantly impact the performance of FSO systems, introducing complexities that need to be carefully addressed to ensure the reliability and security of wireless communication links [99, 100]. To take advantage of both RF and FSO spectrum bands, a few works have studied the secrecy performance of mixed or hybrid RF-FSO systems in various scenarios (see [19, 20, 124] and the references therein). Particularly, the secrecy performance of mixed RF-FSO systems is investigated in [19] considering both fixed and variable gain amplify-and-forward (AF) relaying schemes. Unlike AF, decode-and-forward (DF) involves more sophisticated processing at the relay by decoding the original signal for error correction. Therefore, the secrecy outage performance of downlink mixed RF-FSO simultaneous wireless information and power transfer (SWIPT) systems with DF relaying schemes is studied in [20]. This study explores the impact of misalignment, different detection schemes, SWIPT,

and multiple antenna techniques. Additionally, the secrecy outage performance of a MIMO RF-FSO system is analyzed in [124], It is assumed that the channel state information (CSI) of the RF links is outdated due to delay in feedback transmission, and the CSI of the FSO link is imprecise due to channel estimation errors. However, none of the aforementioned studies have adopted the MIMO-NOMA technology to further reap the benefits of the spectral efficiency (SE) improvement. Motivated by the potential of the mixed RF-FSO system, the work in this chapter investigates the information-theoretic security of an uplink MIMO-NOMA mixed RF-FSO system. To the best of the knowledge, the performance of the underlying system has not been reported in the literature from the PLS approach; this is the gap the proposed work aims to partly fill. The main contributions in this chapter are as follows:

(a) We propose an uplink two-user MIMO-NOMA system in mixed RF-FSO transmission, where an antenna selection is adopted at the transmitter to reduce the hardware complexity of the underlying system. Moreover, we obtain the closed-form expressions of the corresponding statistical features consisting of the probability density function (PDF) and cumulative distribution function (CDF).

(b) Using the expressions of the derived PDF and CDF of the proposed system, we subsequently obtain the analytical expressions of the secrecy outage probability (SOP), the probability of the strictly positive secrecy capacity (SPSC) and the average secrecy capacity (ASC).

(c) Moreover, to approximate the ASC in the high signal-to-noise ratio (SNR) regime, the corresponding asymptotic analysis is presented;

(d) We provide Monte Carlo simulations to validate the accuracy of the proposed analytical framework.

The rest of the chapter is structured in the following manner. Section 3.2 describes the proposed system model followed by the channel statistics in Section 3.3. In Section 3.4, the secrecy performance metrics of the underlying system are derived in terms of the SOP, probability of the SPSC, and the ASC while the corresponding asymptotic analytical framework is studied in Section 3.5. The ensuing discussion of the results are presented in 3.6. Finally, concluding remarks are drawn in Section 3.7.

3.2 System Model

We study a two-user MIMO-NOMA dual-hop mixed RF-FSO system as depicted in Figure 3.1. The uplink RF transmissions take place between two users U_i with $i = \{1, 2\}$ both equipped with N_U antennas[1], and a legitimate receiver (relay node) mounted with N_R antennas in the presence of an N_E-antenna eavesdropper. To reduce the complexity associated with the number of RF chains at the transmitter, transmit antenna selection (TAS) is applied at each user before the information is sent to the destination via the AF relay node in a NOMA fashion. The selection

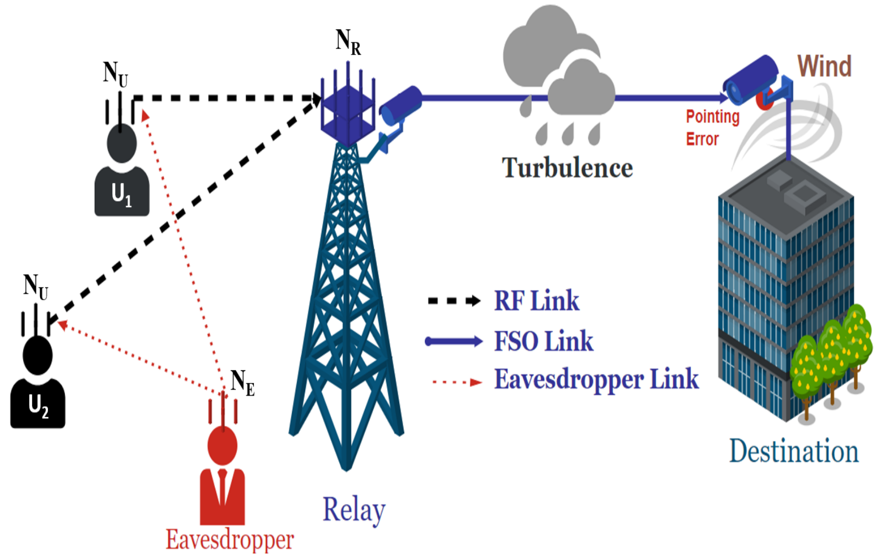

FIGURE 3.1: Illustration of an uplink MIMO-NOMA Mixed RF-FSO System.

criterion of the best antenna at each user is given by [13]

$$b_i^* = \arg\max_k \sum_{j=1}^{N_R} |h_{U_i^{(k)} R_j}|^2, \tag{3.1}$$

where $h_{U_i^{(k)} R_j}$ is the fading coefficient of the $U_i^{(k)}$-R_j link with $k \in \{1, \ldots, N_U\}$ and R_j being the j-th antenna at the relay. Subsequently, the received signal at the j-th antenna of the relay node is given by

$$y_{R_j} = \left(\sum_{i=1}^{2} x_{U_i} h_{U_i^{(b_i^*)} R_j} \sqrt{a_i L_i P_t} \right) + n_{R_j}, \tag{3.2}$$

[1]Subsequently, we assume that $N_{U_i} = N_U$, i.e., the number of antennas at each user is equal throughout this thesis. It is worth noting that this assumption does not change our proposed analysis.

where $E\left[|x_{U_i}|^2\right] = 1$, the signal power transmitted by U_1 is $a_1 P_t$ and the signal power transmitted by U_2 is $a_2 P_t$, P_t denotes the average power transmitted by U_i, a_i is the power allocation coefficient with $\sum_{i=1}^{2} a_i = 1$ and $a_2 > a_1$, n_{R_j} is the additive white Gaussian noise (AWGN) at the j-th antenna of the relay node with zero mean and variance σ_R^2, and L_i is the path-loss gain [125]. It is assumed that the equal gain combining (EGC) is employed at the relay node to improve the received signals from the various antennas[2]. Hence, the combined received signal at the relay node can be expressed as [13, 126]

$$y_R = \sqrt{a_1 L_1 P_t} x_{U_1} h_{U_1^{(b_1^*)} R} + \sqrt{a_2 L_2 P_t} x_{U_2} h_{U_2^{(b_2^*)} R} + n_R, \tag{3.3}$$

where $y_R = \sum_{j=1}^{N_R} y_{R_j}$, $h_{U_i^{(b_i^*)} R} = \sum_{j=1}^{N_R} h_{U_i^{(b_i^*)} R_j}$, where $h_{U_i^{(b_i^*)} R_j}$ are modeled according to the Nakagami-m distribution, $n_R = \sum_{j=1}^{N_R} n_{R_j}$, and n_{R_j} are assumed to be i.i.d. complex Gaussian random variables with zero mean and variance $\sigma_{R_j}^2$, i.e., $n_{R_j} \sim \mathcal{CN}(0, \sigma_{R_j}^2)$. In the FSO link[3], the composite signal at the relay node is first converted to optical signal using either intensity–modulation direct detection (IM/DD) or heterodyne detection (HD). Consequently, the transmitted optical signal to the destination is given by $S_R = \mathcal{G}(1 + \mu y_R)$, where μ is the electrical-to-optical conversion coefficient, $\mathcal{G}$ is the amplification factor [127]. At the destination, the optical received signal given by $h_{RD} S_R$ is filtered out to remove the direct current (DC) component in order to improve the signal quality with the removal of unwanted signals. The resulting received signal is given by

$$y_D = h_{RD} \mathcal{G} \mu y_R + n_D, \tag{3.4}$$

where $h_{RD} = h_l h_a h_p$ is the composite channel gain coefficient with h_l, h_a and h_p denoting the deterministic path loss of the optical link, the fading induced by the atmospheric turbulence, and the fading due to the pointing errors, respectively, and n_D is the AWGN variable at the destination node with mean zero and variance σ_D^2. In what follows, we present the average electrical SNR at the relay node and the signal-to-interference-plus-noise ratio (SINR) at the destination node. According to the NOMA principle, the destination node[4] will first decode the strongest user's signal x_{U_2} while treating U_1's signal as noise, and subsequently apply the SIC to decode x_{U_1}. After substituting (3.3) in (3.4) and performing some mathematical

[2]It is worth mentioning that EGC is employed throughout this thesis with the assumption that phase correction has been applied.

[3]This link is characterized by a direct line of sight (LOS) between the relay node and the destination node.

[4]In this approach, an AF protocol is adopted at the relay node where the demodulation that takes place at the destination can also be illustrated.

manipulations provided in Appendix A, the instantaneous SINR denoted by γ_2 can be obtained as

$$\gamma_2 = \frac{a_2 \gamma_D \gamma_R^{(2)}}{a_1 \gamma_D \gamma_R^{(1)} + \gamma_D + \Lambda}, \tag{3.5}$$

where $\Lambda = \frac{1}{\mu^2 \mathcal{G}^2 \sigma_R^2}$, $\gamma_D = \frac{|h_{RD}|^2}{\sigma_D^2}$ and the instantaneous SINRs for the composite received signal at the relay denoted by $\gamma_R^{(1)}$ and $\gamma_R^{(2)}$ are expressed respectively as[5]

$$\gamma_R^{(2)} = \frac{X_{U_2 R}}{1 + X_{U_1 R}}, \tag{3.6}$$

$$\gamma_R^{(1)} = \frac{X_{U_1 R}}{1 + X_{U_2 R}}, \tag{3.7}$$

where $X_{U_1 R}$ and $X_{U_2 R}$ are the instantaneous SNRs for each user given by

$$X_{U_1 R} = \frac{a_1 L_1 P_t |h_{U_1^{(b_1^*)} R}|^2}{\sigma_R^2}. \tag{3.8}$$

$$X_{U_2 R} = \frac{a_2 L_2 P_t |h_{U_2^{(b_2^*)} R}|^2}{\sigma_R^2}. \tag{3.9}$$

Subsequently, the instantaneous SNR for the weak user denoted by γ_1 is given by

$$\gamma_1 = \frac{a_1 \gamma_D \gamma_R^{(1)}}{\gamma_D + \Lambda}. \tag{3.10}$$

Due to the nature of the RF transmissions, the communications between the users and the relay node are subjected to security attacks through eavesdropping as depicted in Figure 3.1. Thus, the received signal at the j-th antenna at the eavesdropper is given by

$$y_{E_j} = \left(\sum_{i=1}^{2} x_{U_i} h_{U_i^{(b_i^*)} E_j} \sqrt{a_i L_i P_t} \right) + n_{E_j}. \tag{3.11}$$

It is assumed that the eavesdropper is equipped with multiple antennas and exploits this configuration to improve its ability to extract useful information from the intercepted signals through the EGC scheme. This assumption signifies the inherent security vulnerabilities in the proposed system model. Similar to (3.3),

[5]It is important to note that the relay node does not perform SIC; instead, SIC is applied at the destination node.

the received signal at the eavesdropper is given by

$$y_E = \sqrt{a_1 L_1 P_t} x_{U_1} h_{U_1^{(b_1^*)}E} + \sqrt{a_2 L_2 P_t} x_{U_2} h_{U_2^{(b_2^*)}E} + n_E, \tag{3.12}$$

where $y_E = \sum_{j=1}^{N_E} y_{E_j}$, $h_{U_i^{(b_i^*)}E} = \sum_{j=1}^{N_E} h_{U_i^{(b_i^*)}E_j}$ modeled according to the Nakagami-m distribution, $n_E = \sum_{j=1}^{N_E} n_{E_j}$, and n_{E_j} are assumed to be i.i.d. complex Gaussian random variables with zero mean and variance $\sigma_{E_j}^2$, i.e., $n_{E_j} \sim \mathcal{CN}(0, \sigma_{E_j}^2)$. Although, the best antenna for both users is illustrated in (3.12), it is worth emphasizing that the eavesdropper has no knowledge of this selection, and therefore treats this transmission as one emanating from a random antenna at any of the two users. From (3.12), the instantaneous SINRs at the eavesdropper are given respectively by

$$\gamma_E^{(1)} = \frac{X_{U_1E}}{1 + X_{U_2E}}, \tag{3.13}$$

$$\gamma_E^{(2)} = \frac{X_{U_2E}}{1 + X_{U_1E}}, \tag{3.14}$$

where X_{U_1E} and X_{U_2E} are the instantaneous SNRs for each user given respectively as

$$X_{U_1E} = \frac{a_1 L_1 P_t |h_{U_1^{(b_1^*)}E}|^2}{\sigma_E^2}, \tag{3.15}$$

$$X_{U_2E} = \frac{a_2 L_2 P_t |h_{U_2^{(b_2^*)}E}|^2}{\sigma_E^2}. \tag{3.16}$$

3.3 Channel Statistics

In this section, we present the statistics of both the RF and FSO links to subsequently obtain the analytical expressions of the SOP, the probability of the SPSC, ASC and asymptotic ASC for the mixed system.

3.3.1 RF Links

It is assumed that the RF system experiences the Nakagami- m fading, thus, the CDF of the instantaneous SNR γ_R at the relay node with TAS can be expressed as [13]

$$F_{\gamma_R}(\gamma_R) = \sum_{n=0}^{N_{U_i}} (-1)^n \begin{pmatrix} N_{U_i} \\ n \end{pmatrix} e^{-n\lambda_R \gamma_R} \sum_{k=0}^{n(N_R-1)} C_{k,n} (\lambda_R \gamma_R)^k, \tag{3.17}$$

where $\lambda_R = \frac{m_R}{\bar{\gamma}_R}$ with $m_{_R}$ and $\bar{\gamma}_R = \sum_{j=1}^{N_R} \gamma_R^{(i)}$ being the Nakagami fading parameter and the average SNR, respectively. From (3.17), the PDF of the random variable (RV) γ_R can be obtained as

$$f_{\gamma_R}(\gamma_R) = \sum_{n=0}^{N_{U_i}} \left(\begin{array}{c} N_{U_i} \\ n \end{array} \right) (-1)^n \sum_{k=1}^{n(N_R-1)} C_{k,n} (\lambda_R \gamma_R)^{k-1} e^{(n\lambda_R\gamma_R)\left(k-n(\lambda_R\gamma_R)\right)}. \quad (3.18)$$

Subsequently, the channels statistics associated with the eavesdropper are presented in terms of the PDF and CDF. It is worth recalling that the eavesdropper does not see the antenna selection process at both users, but only a transmission from a single antenna from each user. Hence, the PDF and CDF of the RV γ_E are given, respectively by

$$f_{\gamma_E}(\gamma_E) = \frac{\lambda_E^{N_E}}{\Gamma(N_E)} \gamma_E^{N_E - 1} e^{-\lambda_E \gamma_E}, \quad (3.19)$$

$$F_{\gamma_E}(\gamma_E) = \frac{1}{\Gamma(N_E)} \Upsilon(N_E, \lambda_E \gamma_E), \quad (3.20)$$

where $\lambda_E = \frac{m_E}{\bar{\gamma}_E}$ with $m_{_E}$ and $\bar{\gamma}_E = \sum_{j=1}^{N_E} \gamma_E^{(i)}$ being the Nakagami fading parameter and the average SNR, respectively. Moreover, $\Gamma(\bullet)$ and $\Upsilon(\bullet, \bullet)$ are the Gamma function [128, Eq. 8.339.1] and the lower incomplete gamma function [128, Eq. 8.350.1], respectively.

3.3.2 FSO Link

In the underlying system model, it is assumed that the link between the relay and destination follows the gamma-gamma distribution. This choice is made because the Gamma-gamma distribution exhibits notable flexibility for modeling FSO links, offering an accurate representation of atmospheric turbulence while accommodating varying turbulence strengths. Hence, the PDF of the RV γ_D is given by [109]

$$f_{\gamma_D}(\gamma_D) = \frac{\xi^2}{r\Gamma(\alpha)\Gamma(\beta)\gamma_D} G_{1,3}^{3,0}\left(\frac{d\alpha\beta}{\mu_r^{1/r}} \gamma_D^{\frac{1}{r}} \middle|_{\xi^2, \alpha, \beta}^{\xi^2} \right), \quad (3.21)$$

where the parameters α and β represent the severity of fading/scintillation due to the atmospheric turbulence conditions, $d = \frac{\xi^2}{\xi^2+1}$, μ_r denotes the average electrical

SNR of the FSO link under the HD or IM/DD detection[6], and $G_{p,q}^{m,n}\left(\bullet \mid \begin{matrix}\bullet\\ \bullet\end{matrix}\right)$ denotes the Meijer G-function [128, Eq. 9.343]. From (3.21), the corresponding CDF is given by

$$F_{\gamma_D}(\gamma_D) = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)} G_{r+1,3r+1}^{3r,1}\left(\frac{(d\alpha\beta)^r}{\mu_r r^{2r}}\gamma_D \middle|_{\Delta(r,\xi^2),\Delta(r,\alpha),\Delta(r,\beta),0}^{1,\Delta(r,\xi^2+1)}\right). \quad (3.22)$$

In what follows, we utilize the fixed-gain relaying scheme to keep the difference in power levels among distinct NOMA users, enabling SIC detection at the destination. Using the equivalent end-to-end SNR associated with U_1 in (3.10), the resulting CDF can be expressed as

$$F_{\gamma_{eq}^{(1)}}(x) = \int_0^\infty F_{\gamma_R}\left(\frac{x(\gamma_D+\Lambda)}{a_1\gamma_D}\right) f_{\gamma_D}(\gamma_D)d\gamma_D. \quad (3.23)$$

After substituting (3.21) and (3.17) in (3.23), making use of [129, eq.(21)] and some mathematical manipulations provided in Appendix B, we obtain

$$F_{\gamma_{eq}^{(1)}}(x) = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)} \underbrace{\sum_{n=0}^{N_{U_i}} \binom{N_{U_i}}{n} (-1)^n \sum_{k=0}^{n(N_R-1)} C_{k,n} \sum_{j=0}^{k} \frac{\lambda_R^{k-j}}{n^j} \binom{k}{j}}_{\triangleq \sum_{nkj}}$$

$$\times\, x^{k-j} e^{\frac{-n\lambda_R}{a_1}x} G_{r,3r+1}^{3r+1,0}\left(\frac{(d\alpha\beta)^r n\lambda_R\Lambda}{\mu_r a_1 r^{2r}}x \middle| \begin{matrix} C_1 \\ C_3 \end{matrix}\right), \quad (3.24)$$

where $C_{k,n} = \sum_{p=k-N_R+1}^{k} \frac{C_{p,(n-1)}}{(k-p)!}\delta_{[0,(n-1)(N_R-1)]}(n)$ ($C_{00} = C_{0n} = 1, C_{k,1} = \frac{1}{k!}, C_{1,n} = n$, $C_1 = \Delta(r,\xi^2+1)$, and $C_3 = [\Delta(r,\xi^2), \Delta(r,\alpha), \Delta(r,\beta), j]$. We can further rewrite (3.24) in a compact form as

$$F_{\gamma_{eq}^{(1)}}(x) = 1 + \Psi \sum_{(nkj)} x^{k-j} e^{\frac{-n\lambda_R}{a_1}x} G_{r,3r+1}^{3r+1,0}\left(q_{nU_1}x \middle| \begin{matrix} C_1 \\ C_3 \end{matrix}\right), \quad (3.25)$$

[6] For HD detection, $\mu_1 = \mathbb{E}[\gamma_D] = \bar{\gamma}_D$, and for IM/DD detection, $\mu_2 = \frac{\bar{\gamma}_D\alpha\beta\xi^2(\xi^2+2)}{(\alpha+1)(\beta+1)(\xi^2+1)^2}$ with $\mathbb{E}(\bullet)$ denoting the expectation operator.

where $\Psi = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)}$, and $q_{nU_1} = \frac{(d\alpha\beta)^r n\lambda_R\Lambda}{\mu_r a_1 r^{2r}}$.
Using a similar approach, we can obtain an expression for the equivalent end-to-end SINR associated to U_2 in (3.5) as

$$F_{\gamma_{eq}^{(2)}}(x) = 1 + \Psi \sum_{(nkj)} x^{k-j} exp\left[\frac{-a_1 n\lambda_R}{a_2} x\right] G_{r,3r+1}^{3r+1,0}\left(q_{nU_2} x \middle| \begin{matrix} C_1 \\ C_3 \end{matrix}\right), \tag{3.26}$$

where $q_{nU_2} = \frac{(d\alpha\beta)^r n a_1 \lambda_R\Lambda}{\mu_r a_2 r^{2r}}$.

3.4 Secrecy Performance Analysis

3.4.1 Secrecy Outage Probability

The SOP is a useful performance metric when considering passive eavesdropping. It is defined as the probability that the instantaneous secrecy capacity falls below a predetermined secrecy rate [3,109]. In our proposed model, two signals are received by the destination from the NOMA users with the help of a relay. Therefore, secrecy outage event happens when either $C_{s_{U_1}}$ or $C_{s_{U_2}}$ falls below a secrecy rate R_s. This can be expressed mathematically as

$$\begin{aligned} \mathcal{P}_{\text{out}} &= \mathbb{P}\left(C_{s_{U_1}} \leq R_s \text{ or } C_{s_{U_2}} \leq R_s\right) \\ &= 1 - \left(1 - \mathcal{P}_{\text{out}}^{(1)}\right)\left(1 - \mathcal{P}_{\text{out}}^{(2)}\right), \end{aligned} \tag{3.27}$$

where $C_{s_{U_1}} = log_2(1+\gamma_R^{(1)}) - log_2(1+\gamma_E^{(1)})$, $C_{s_{U_2}} = log_2(1+\gamma_R^{(2)}) - log_2(1+\gamma_E^{(2)})$, $\mathbb{P}(\bullet)$ is the probability operator and $\mathcal{P}_{\text{out}}^{(i)}$ is the SOP associated with user U_i given by

$$\mathcal{P}_{\text{out}}^{(i)} = \int_0^\infty F_{\gamma_{eq}^{(i)}}((1+\gamma_E)\Theta - 1) f_{\gamma_E}(\gamma_E) \mathrm{d}\gamma_E, \tag{3.28}$$

with $\Theta = exp(R_s) \geq 1$. However, deriving a closed-form expression for the exact SOP in (3.28) is rather intricate due to the shift in Meijer's G-function. To address this issue, we propose to derive a lower bound expression which can be given by

$$\mathcal{P}_{\text{out,lb}}^{(i)} = \int_0^\infty F_{\gamma_{eq}^{(i)}}(\Theta\gamma_E) f_{\gamma_E}(\gamma_E) \mathrm{d}\gamma_E. \tag{3.29}$$

In what follows, we derive the expressions of the lower bound on the SOP associated with U_1 and U_2. To obtain the lower bound on the SOP expression associated with U_1, (3.25) and (3.19) can be substituted in (3.29), to yield

$$\mathcal{P}_{\text{out,lb}}^{(1)} = 1 + \frac{\lambda_E^{N_E}\Psi}{\Gamma(N_E)} \sum_{(nkj)} \Theta^{k-j} \int_0^\infty \gamma_E^{N_E+k-j-1} e^{-\left(\lambda_E + \frac{n\lambda_R\Theta}{a_1}\right)\gamma_E} \times G_{r,3r+1}^{3r+1,0}\left(q_{nU_1} \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \right) \mathrm{d}\gamma_E. \quad (3.30)$$

To solve the integral in (3.30), we further utilize the antiderivative [128, eqn. 7.813], thus, the lower bound of the SOP associated with U_1 can be expressed as

$$\mathcal{P}_{\text{out,lb}}^{(1)} = 1 + \frac{\lambda_E^{N_E}\Psi}{\Gamma(N_E)} \sum_{(nkj)} \Theta^{k-j} \left(\frac{n\Theta\lambda_R}{a_1} + \lambda_E \right)^{\iota_{jk}} \times G_{r+1,3r+1}^{3r+1,1}\left(\frac{q_{nU_1}}{(\frac{n\Theta\lambda_R}{a_1} + \lambda_E)} \middle| \begin{matrix} 1-\iota_{jk}, C_1 \\ C_3 \end{matrix} \right). \quad (3.31)$$

To derive an analytical expression for the lower bound of the SOP associated with U_2, we can adopt a similar approach to the one used to obtain (3.31). Hence, the lower bound for the SOP associated with U_2 is given by

$$\mathcal{P}_{\text{out,lb}}^{(2)} = 1 + \frac{\lambda_E^{N_E}\Psi}{\Gamma(N_E)} \sum_{(nkj)} \sum_{nkj} \Theta^{k-j} \left[\frac{n\Theta\lambda_R a_1}{a_2} + \lambda_E \right]^{\iota_{jk}} \times G_{r+1,3r+1}^{3r+1,1}\left(\frac{q_{nU_2}}{(\frac{n\Theta\lambda_R a_1}{a_2} + \lambda_E)} \middle| \begin{matrix} 1-\iota_{jk}, C_1 \\ C_3 \end{matrix} \right), \quad (3.32)$$

where $\iota_{jk} = j - N_E - k$. Plugging (3.31) and (3.32) into (3.27) yields the analytical expression of the lower bound on the SOP.

3.4.2 Probability of the Strictly Positive Secrecy Capacity

The probability of the SPSC is another fundamental metric used to evaluate the secrecy performance in passive eavesdropping scenarios. It is defined as the probability of the existence of the secrecy capacity namely the probability of positive secrecy capacity. In our proposed model, SPSC can be formulated mathematically as

$$\begin{aligned}\mathcal{P}_{\text{SPSC}} &= \mathbb{P}\left(C_{s_{U_1}} > 0, C_{s_{U_2}} > 0\right)\\ &= 1 - \left[1 - \left(1 - \mathcal{P}_{\text{out}}^{(1)}(0)\right)\left(1 - \mathcal{P}_{\text{out}}^{(2)}(0)\right)\right]\\ \mathcal{P}_{\text{SPSC}}^{(i)} &= 1 - \int_0^\infty F_{\gamma_{eq}^{(i)}}(\Theta\gamma_E) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E.\end{aligned} \tag{3.33}$$

To solve the integral in (3.33), we can further use a similar analysis developed in (3.29) by substituting $R_S = 0$, and the $\mathcal{P}_{\text{SPSC}}$ expressions for U_1 and U_2 can be directly given by.

$$\mathcal{P}_{\text{SPSC}}^{(1)} = \frac{\lambda_E^{N_E}\Psi}{\Gamma(N_E)}\sum_{(nkj)}\left(\frac{n\lambda_R}{a_1} + \lambda_E\right)^{\iota_{jk}} G_{r+1,3r+1}^{3r+1,1}\left(\frac{q_{nU_1}}{(\frac{n\lambda_R}{a_1} + \lambda_E)}\middle|\begin{matrix}1-\iota_{jk}, C_1\\ C_3\end{matrix}\right), \tag{3.34}$$

$$\mathcal{P}_{\text{SPSC}}^{(2)} = \frac{\lambda_E^{N_E}\Psi}{\Gamma(N_E)}\sum_{(nkj)}\left[\frac{n\lambda_R a_1}{a_2} + \lambda_E\right]^{\iota_{jk}} G_{r+1,3r+1}^{3r+1,1}\left(\frac{q_{nU_2}}{(\frac{n\lambda_R a_1}{a_2} + \lambda_E)}\middle|\begin{matrix}1-\iota_{jk}, C_1\\ C_3\end{matrix}\right). \tag{3.35}$$

Substituting (3.34) and (3.35) into (3.33) results the analytical expression of the SPSC.

3.4.3 Average Secrecy Capacity

In this section, an active eavesdropping scenario is assumed wherein the CSI of the eavesdropper channel is known at either user. Hence, a fundamental performance metric used to evaluate the secrecy performance is the ASC. It can be formulated mathematically as

$$\bar{C}_S = \int_0^\infty \frac{F_{\gamma_E}^{(i)}(\gamma)}{1+\gamma}[1 - F_{\gamma_{eq}^{(i)}}(\gamma)]d\gamma. \tag{3.36}$$

Considering the two-user NOMA, the ASC is given by

$$\bar{C}_S = \sum_{i=1}^{2} \bar{C}_{S_{U_i}}, \tag{3.37}$$

where $\bar{C}_{S_{U_i}} = \max[\ln(1+\gamma_{eq}^{(i)}) - \ln(1+\gamma_E), 0]$. After plugging (3.20) and (3.25) into (3.36), the ASC associated with U_1 is given by

$$\bar{C}_{S_{U_1}} = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)} \sum_{(nkj)} \left[\epsilon_1^{(1)} - \epsilon_2^{(1)}\right]. \tag{3.38}$$

$$\epsilon_1^{(1)} = \int_0^\infty \frac{\gamma^{k-j}\exp[-\omega_1\gamma]}{1+\gamma} G_{r,3r+1}^{3r+1,0}\left(q_{nU_1} n\lambda_R \Lambda\gamma \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \right) d\gamma, \tag{3.39}$$

$$\epsilon_2^{(1)} = \sum_{p=0}^{N_E-1} \frac{\lambda_E^p}{p!} \int_0^\infty \frac{\gamma^{p+k-j}\exp[-(\omega_1+\lambda_E)\gamma]}{1+\gamma} G_{r,3r+1}^{3r+1,0}\left(q_{nU_1} n\lambda_R \Lambda\gamma \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \right) d\gamma. \tag{3.40}$$

With the aid of $\frac{x^a}{1+x} = G_{1,1}^{1,1}\left(x\middle|_a^a\right), \exp(-bx) = G_{0,1}^{1,0}\left(bx\middle|_0^-\right)$ [128, 130], we can evaluate (3.39) in a closed-form expression given by

$$\epsilon_1^{(1)} = \frac{1}{\omega_1} G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} k-j \\ k-j \end{matrix} \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \middle| \frac{1}{\lambda_R}, q_{nU_1}\Lambda \right], \tag{3.41}$$

where $\omega_1 = \frac{n\lambda_R}{a_1}$. Similarly, the expression of ϵ_{U_2} can be obtained as

$$\epsilon_2^{(1)} = \frac{G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left(\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} p+k-j \\ p+k-j \end{matrix} \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \middle| \frac{1}{\omega_1+\lambda_E}, \frac{q_{nU_1} n\Lambda}{\omega_1+\lambda_E} \right)}{\omega_1+\lambda_E}. \tag{3.42}$$

After substituting (3.41) and (3.42) into (3.38), a closed-form expression of the ASC associated with U_1 can be obtained. Similarly, the ASC associated with U_2 can be expressed by

$$\begin{aligned}\bar{C}_{S_{U_2}} = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)} \sum_{(nkj)} \Bigg[&\frac{1}{\omega_2} G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} k-j \\ k-j \end{matrix} \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \middle| \frac{1}{\lambda_R}, q_{nU_2}\Lambda \right] \\ &- \frac{1}{\omega_2+\lambda_E} G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left(\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} p+k-j \\ p+k-j \end{matrix} \middle| \begin{matrix} C_1 \\ C_3 \end{matrix} \middle| \frac{1}{\omega_1+\lambda_E}, \frac{q_{nU_2} n\Lambda}{\omega_2+\lambda_E} \right)\Bigg],\end{aligned} \tag{3.43}$$

where $\omega_2 = \frac{na_1}{a_2}\lambda_R$. Consequently, the ASC of the fixed-gain relaying scheme can be obtained using (3.37).

3.5 Asymptotic Analysis

Here, the asymptotic analysis of the ASC is provided to approximate the exact performance in the high SNR regime. First, we approximate (3.26) as $\mu_r \to \infty$ which yields [131]

$$F^{\infty}_{\gamma^{(2)}_{eq}}(x) = 1 + \Psi \sum_{(nkj)} \sum_{s=1}^{3r+1} B_{s_{U_2}} x^{k-j+C_{3,s}} e^{\frac{-a_1 n \lambda_R}{a_2} x}, \tag{3.44}$$

where $B_{s_{U_2}} = (q_{nU_2})^{C_{3,s}} \frac{\prod_{M=1,M\neq s}^{3r+1} \Gamma\left(C_{3,M}-C_{3,s}\right)}{\prod_{m=1}^{r} \Gamma(C_{1,m}-C_{3,s})}$ and is dominated by $\min\{C_3\}$ with $C_{3,s}$ being the s-th term within the sequence C_3. For $\mu_r \to \infty$, the CDF in (3.25) can be approximated in a simpler form as

$$F^{\infty}_{\gamma^{(1)}_{eq}}(x) = 1 + \Psi \sum_{(nkj)} \sum_{s=1}^{3r+1} B_{s_{U_1}} x^{k-j+C_{3,s}} e^{\frac{-n \lambda_R}{a_1} x}, \tag{3.45}$$

where $B_{s_{U_1}} = (q_{nU_1})^{C_{3,s}} \frac{\prod_{M=1,M\neq s}^{3r+1} \Gamma\left(C_{3,M}-C_{3,s}\right)}{\prod_{m=1}^{r} \Gamma(C_{1,m}-C_{3,s})}$. After substituting (3.20) and (3.45) into (3.36), and with the help of [130], the asymptotic ASC associated with U_1 can given by

$$\begin{aligned}\bar{C}^{\infty}_{S_{U_1}} = \sum_{nkj} \sum_{s=1}^{3r+1} B_{s_{U_1}} \Bigg[\omega_1 G^{2,2}_{1,2}\left(\omega_1 \middle| \begin{matrix} \digamma \\ \digamma \end{matrix}\right) \\ - (\omega_1 + \lambda_E) \sum_{p=0}^{N_E-1} \frac{\lambda_E^p}{p!} G^{2,2}_{1,2}\left(\omega_1 + \lambda_E \middle| \begin{matrix} \digamma + n \\ \digamma + n \end{matrix}\right) \Bigg],\end{aligned} \tag{3.46}$$

where $\digamma = p - q + C_{3,s} + 1$. Similarly, the asymptotic ASC of U_2 can be obtained by plugging (3.20) and (3.44) into (3.36).

3.6 Numerical Results

In this section, we present the numerical results of the proposed system. The following parameters are used for the FSO link: (a) for weak turbulence conditions, α=2.902 and β= 2.510; (b) for moderate turbulence conditions, α=2.296 and β= 1.822; (c) for strong turbulence conditions, α=2.064 and β=1.342 [17]. Moreover, we set $m_R = m_E = 2$, $a_1 = 0.35$, $a_2 = 0.65$, and $\Lambda = 1$ without loss of generality. It is evident from all the results presented in this section that the analytical results for the SOP, probability of the SPSC, and ASC are in good agreement with the Monte Carlo simulations. This validates the correctness of our proposed mathematical framework. Moreover, it is noteworthy that the derived asymptotic results for the ASC are a good approximation of the exact ones for high SNR values. Figure 3.2 shows the lower bound of the SOP versus the average SNR at the

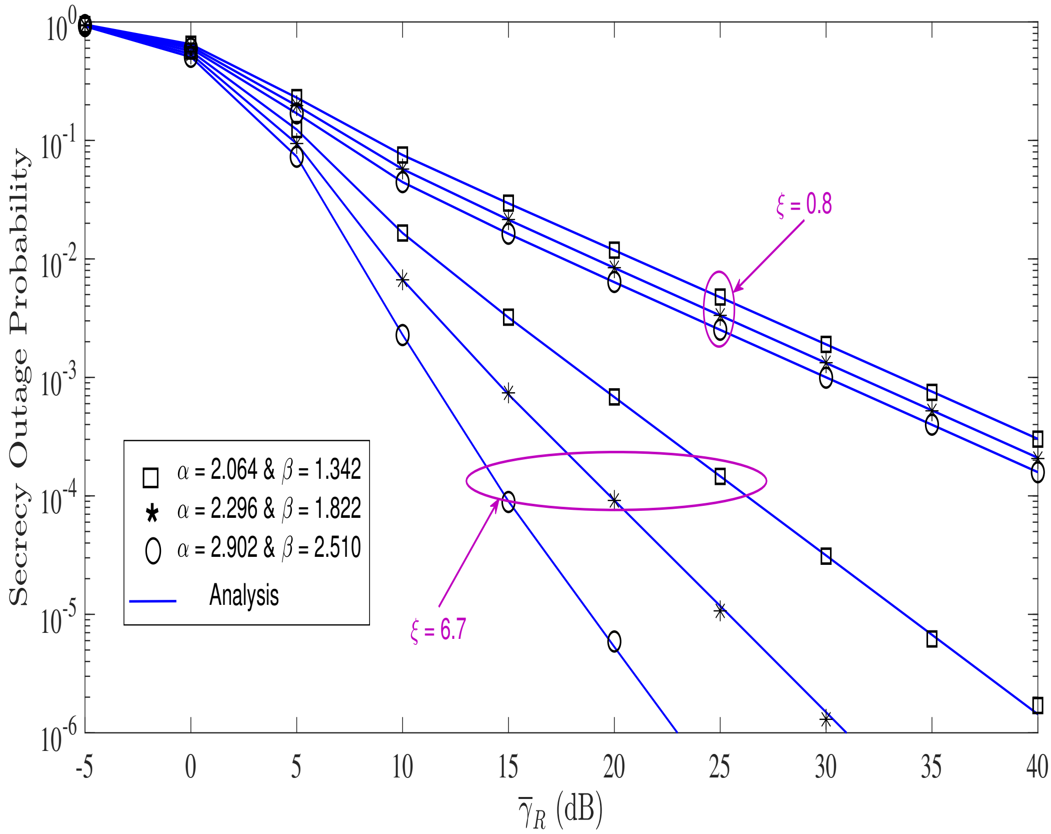

FIGURE 3.2: SOP versus $\bar{\gamma}_R$ for different values of ξ and turbulence conditions, $\bar{\gamma}_E$ = 1 dB, μ_r = 10 dB, N_U = 2, N_R = 4, N_E = 2, r =1, and R_s = 0.01.

relay for different values of ξ and turbulence conditions. As expected, the performance under weak turbulence conditions outperforms the one under moderate and strong turbulence conditions. This is because the weak turbulence typically results in less severe atmospheric effects, leading to reduced signal attenuation compared to moderate or strong turbulence conditions. As a result, the signal experiences less fading and distortion, leading to better secrecy performance. Moreover, it can be seen that the SOP performance varies with the various levels of the pointing error; for low-level pointing error (i.e., a large value of ξ), a better secrecy performance can be achieved in comparison to a high-level pointing error. This arises from the condition wherein low-level pointing errors occur, there is less unintended signal leakage outside the desired transmission direction. Therefore, the risk of interception by unintended receivers, such as eavesdroppers, is minimized, leading to better secrecy performance. Figure 3.3 illustrates the lower bound of

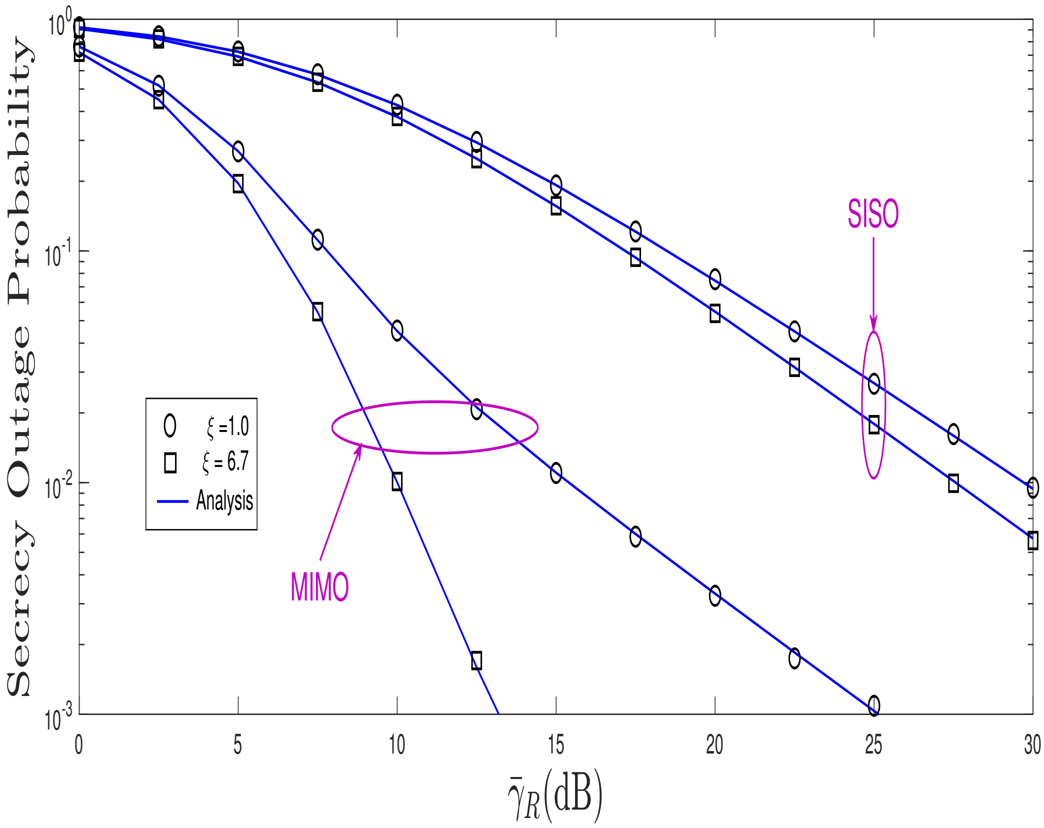

FIGURE 3.3: SOP versus $\bar{\gamma}_R$ for different values of ξ, $\bar{\gamma}_E = 1$ dB, $\mu_r = 10$ dB, $N_U = 2$, $N_R = 4$, $N_E = 2$, r =1, and $R_s = 0.01$.

the SOP versus the average SNR at the relay $\bar{\gamma}_R$. It is shown that MIMO-NOMA outperforms single-input-single-output (SISO)-NOMA in terms of the secrecy performance. This is due to the fact that MIMO NOMA systems generally exhibit superior performance due to their inherent spatial diversity, which allows them to effectively mitigate fading and interference. Additionally, MIMO systems offer higher channel capacities by exploiting multiple antennas to transmit multiple data streams simultaneously. This advantage not only increases data throughput but also enhances potential secrecy capacity.

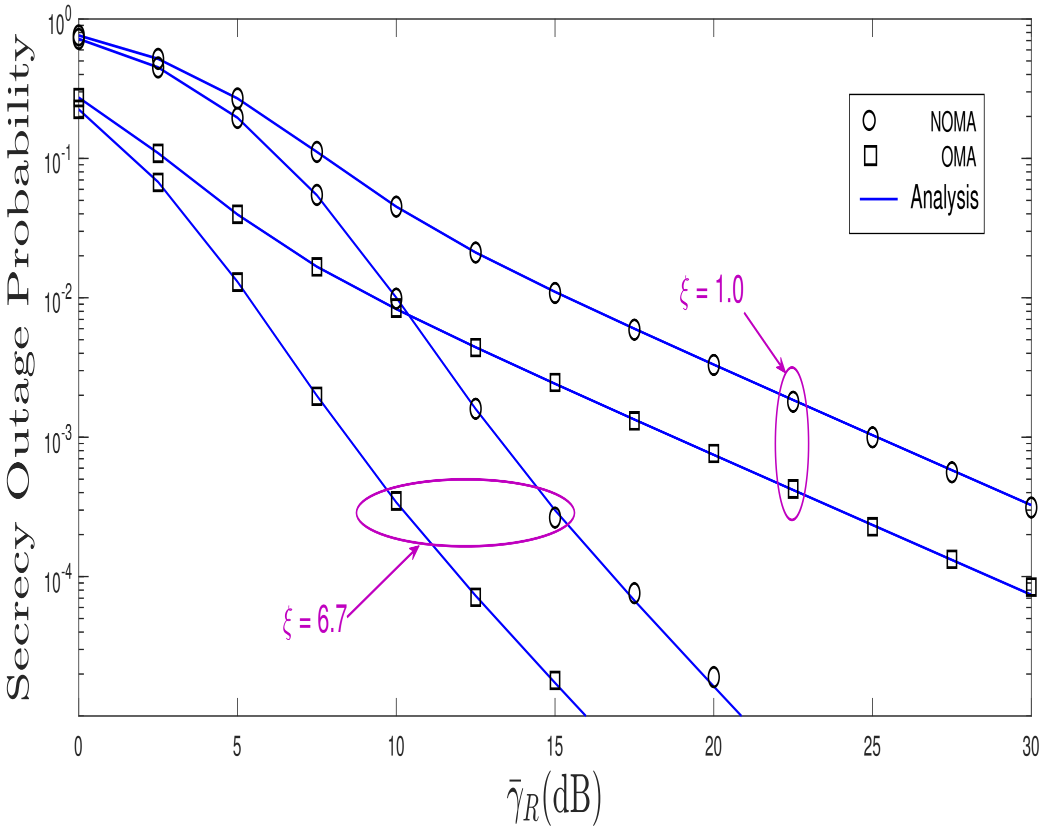

FIGURE 3.4: SOP versus $\bar{\gamma}_R$ for different values of ξ, $\bar{\gamma}_E$ = -1 dB, N_U = 2, N_R = 4, N_E = 2, r =1, and R_s = 0.01.

In Figure 3.4, the lower bound of the SOP versus $\bar{\gamma}_R$ is illustrated for both a single-user system (OMA) and the proposed AF-based NOMA scheme in this thesis. The analysis considers two levels of pointing error to demonstrate their impact on the secrecy performance. The AF-based NOMA scheme generally exhibits worse secrecy performance compared to the single-user system. This difference arises because in the single-user-based system, all power is allocated to a single link, thereby maximizing its secure performance. In contrast, NOMA distributes power among multiple users, which often results in reduced individual SNRs and diminished secure performance. Although this power-sharing strategy can enhance overall system capacity, it highlights the necessity of careful planning and optimization of power allocation in practical NOMA designs to achieve optimal secure performance.

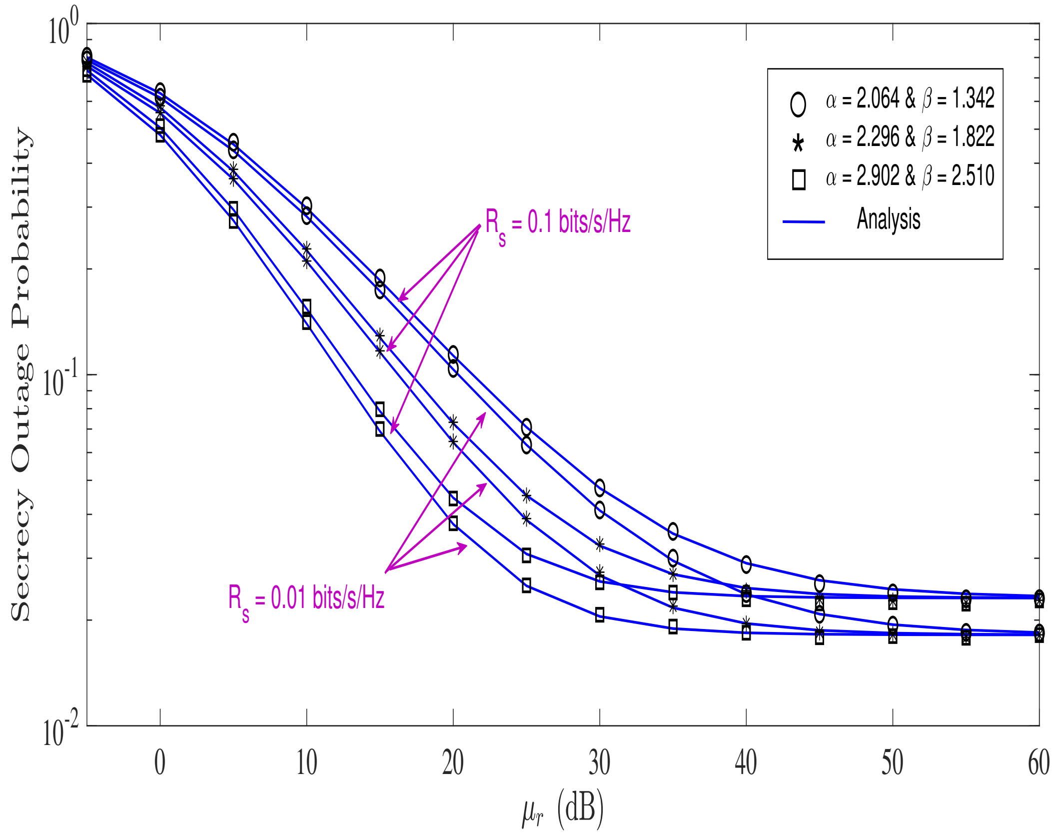

FIGURE 3.5: SOP versus μ_r with different R_s and turbulence conditions, $\bar{\gamma}_E$ = -1 dB, $\bar{\gamma}_R$ = 10 dB, N_U = 2, N_R = 2, N_E = 2 and r =2.

In Figure 3.5, the lower bound of the SOP against μ_r is presented under different values of α, β and the target secrecy rate R_s. It is evident that as R_s increases, the secrecy of the underlying system worsens implying worse SOP performance. This degradation is attributed to the fact that higher R_s rates necessitate tighter secrecy constraints, thereby making it more challenging to maintain secure communication in the presence of eavesdroppers. Also, this deterioration can result from the trade-off between achieving higher data rates and ensuring secure communication. Additionally, the saturation of the curves can be attributed to the increasing values of the target secrecy rate; with increasing R_s, more resources are allocated to achieve higher data rates which may potentially compromise the secrecy protection mechanisms. Consequently, the system becomes more susceptible to eavesdropping attacks. Moreover, as it is mentioned, the system performance in weak FSO turbulence conditions is better than the ones under strong turbulence conditions.

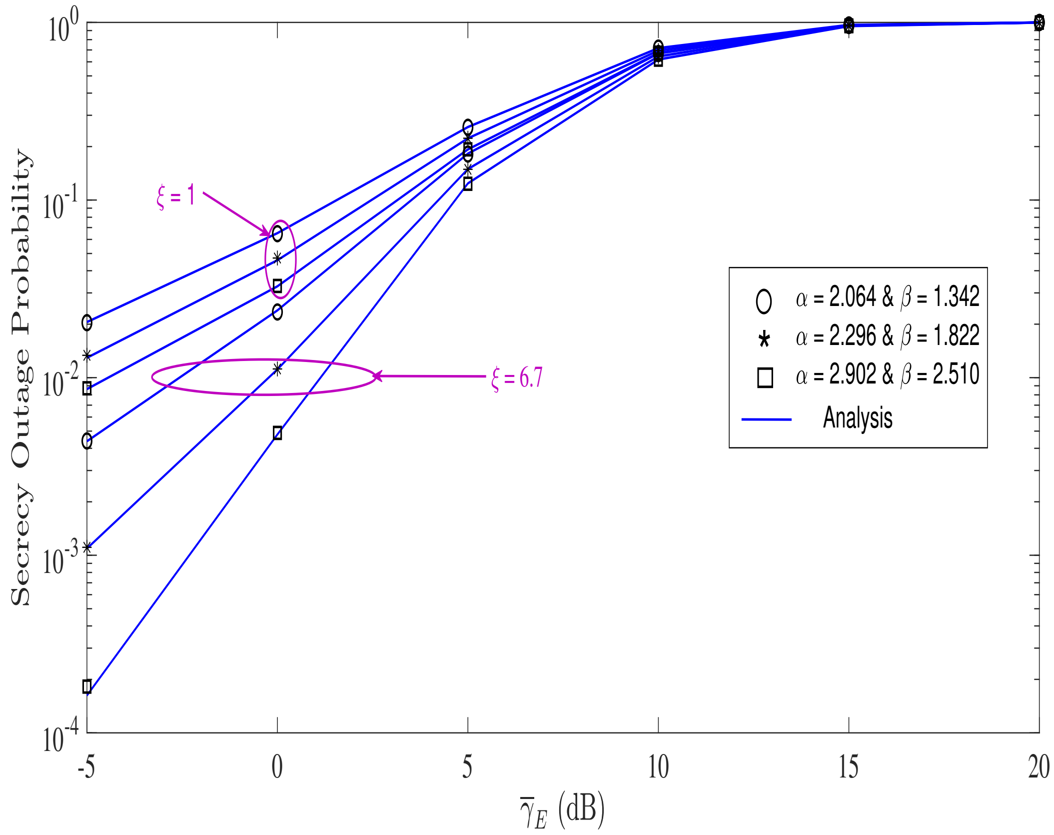

FIGURE 3.6: SOP versus $\bar{\gamma}_E$ with different ξ and turbulence conditions, $\bar{\gamma}_R$ = 10 dB, μ_r = 10 dB, N_U = 2, N_R = 4, N_E = 2 and r =1.

Figure 3.6 depicts the secrecy performance against the average SNR at the eavesdropper $\bar{\gamma}_E$. As the signal quality of the eavesdropper increases, the SOP also increases under the various FSO turbulence conditions and different pointing error levels, until it reaches a saturation level (approximately one) in the high-SNR regime (good signal quality of the eavesdropper link). This can be explained intuitively by the fact that for a strong eavesdropper's signal quality, the system secrecy is guaranteed to be compromised.

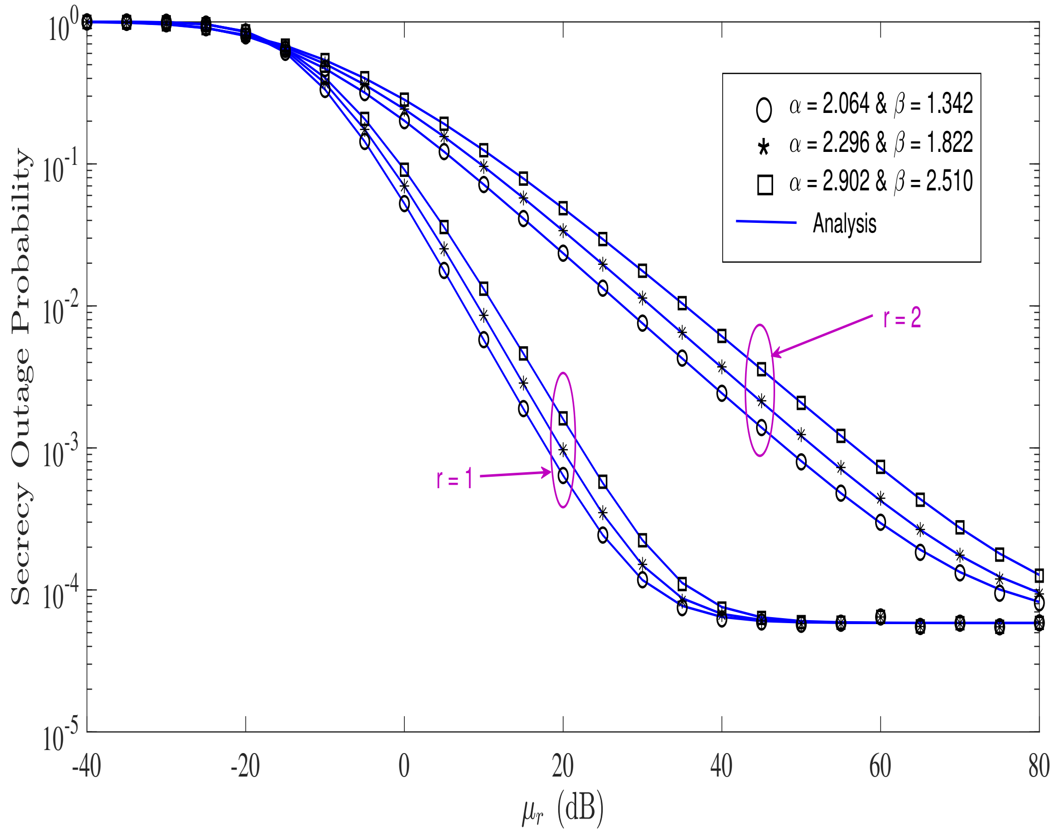

FIGURE 3.7: SOP versus μ_r for different turbulence conditions and detection techniques, $\bar{\gamma}_R = 20$ dB, $\bar{\gamma}_E = 0$ dB, $N_U = 2$, $N_R = 2$, $N_E = 2$, and $R_s = 0.01$.

In Figure 3.7, the impact of the detection technique on the system performance in terms of secrecy is investigated. It can be seen that the system performs better when HD ($r = 1$) is employed than its IM/DD ($r = 2$) counterpart over the entire SNR regime, and for the various FSO turbulence conditions. This emphasizes the fact that intrinsic benefits of HD detection facilitate more effective utilization of the FSO channel by enabling simultaneous transmission and reception of signals. Consequently, this improves the SNR and thereby enhances the system secrecy performance.

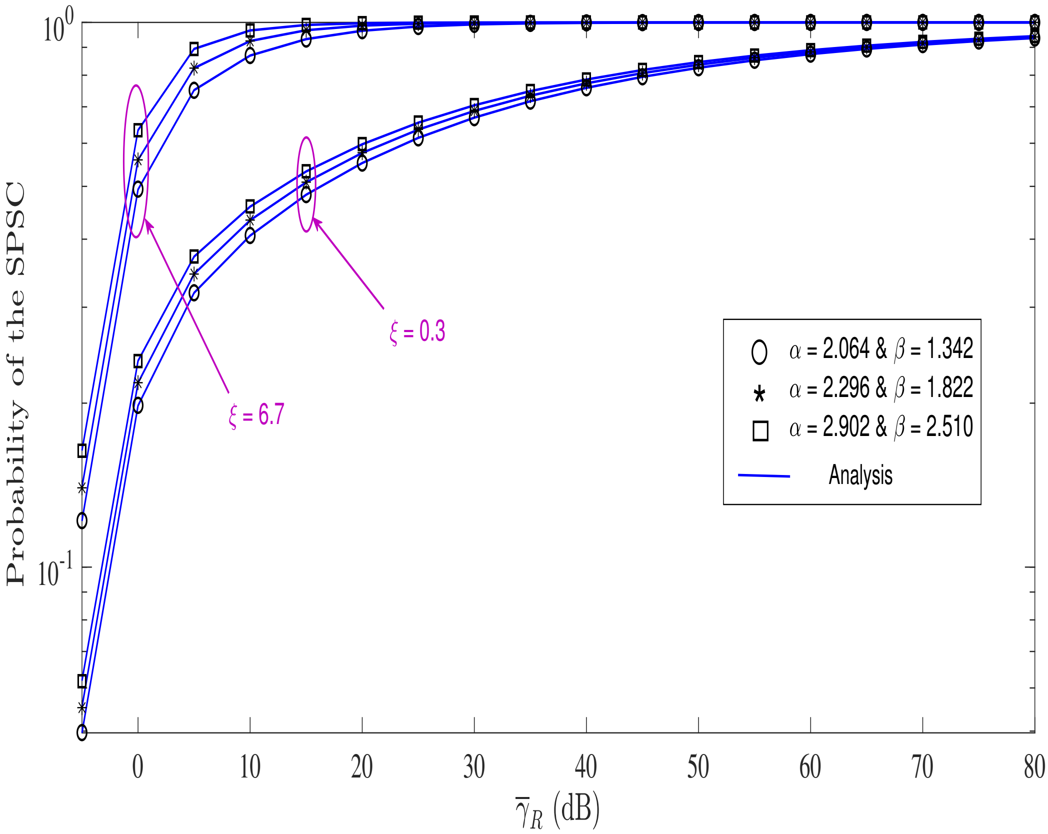

FIGURE 3.8: Probability of the SPSC versus $\bar{\gamma}_R$ for different values of α, β, and ξ, $\bar{\gamma}_E = -10$ dB, $N_R = 4$, $N_E = 4$, $\mu_r = 10$ dB, and $r = 1$.

Figure 3.8 shows the probability of the SPSC versus μ_r for various pointing error levels. It can be observed that as μ_r increases, the probability of the SPSC also increases which is tantamount to an improvement of the secrecy performance. Although the FSO is generally immune to security threats, it is noted that a deviation in the alignment between the transmitter and receiver in the FSO link will have a negative impact on the overall secrecy performance.

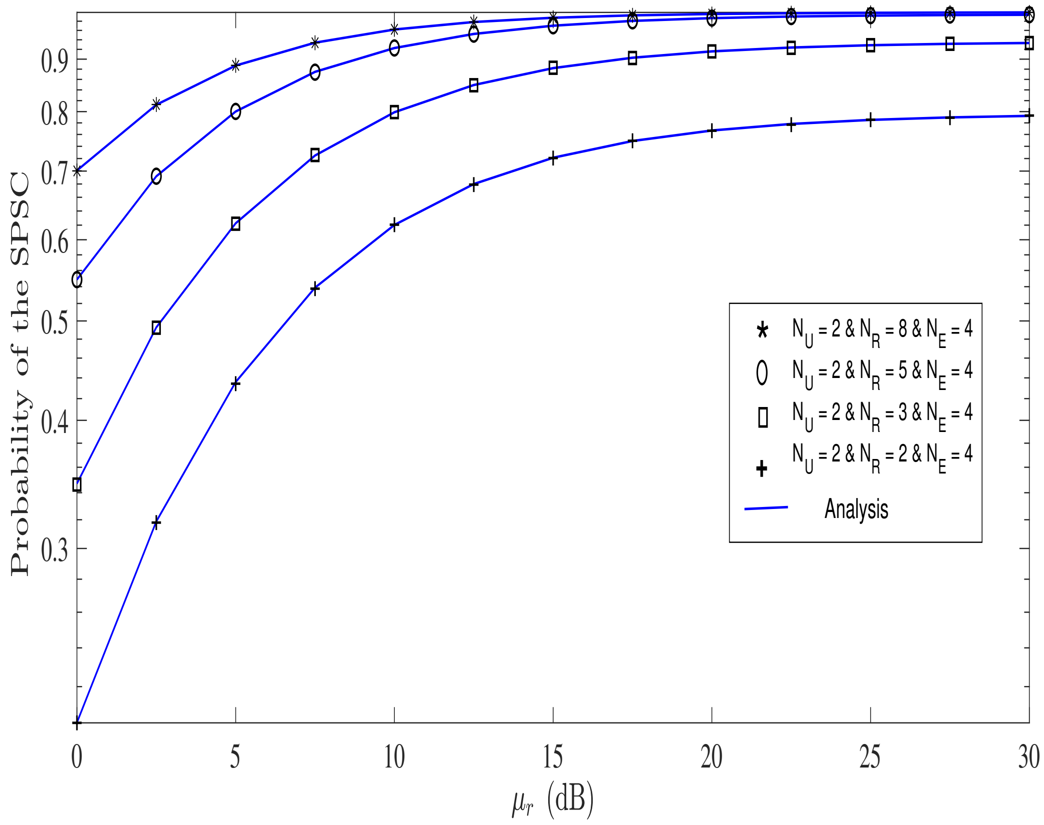

FIGURE 3.9: Probability of the SPSC versus μ_r with different N_R conditions, $\bar{\gamma}_E = 1$ dB, $\bar{\gamma}_R = 10$ dB, $\xi = 1$, $r = 1$, $\alpha = 2.902$, $\beta = 2.510$ and $R_s = 0.01$.

In Figure 3.9, the probability of the SPSC versus μ_r is plotted for various system parameters. It is noted that an increase in the number of antenna at the relay node for a fixed number of antennas at NOMA users and the eavesdropper yields a better system performance. This enhancement can be attributed to the increased spatial diversity provided by additional antennas at the relay which enables better signal reception and processing. Consequently, the system becomes more robust against channel impairments and interference, resulting in a higher probability of successful secure communication.

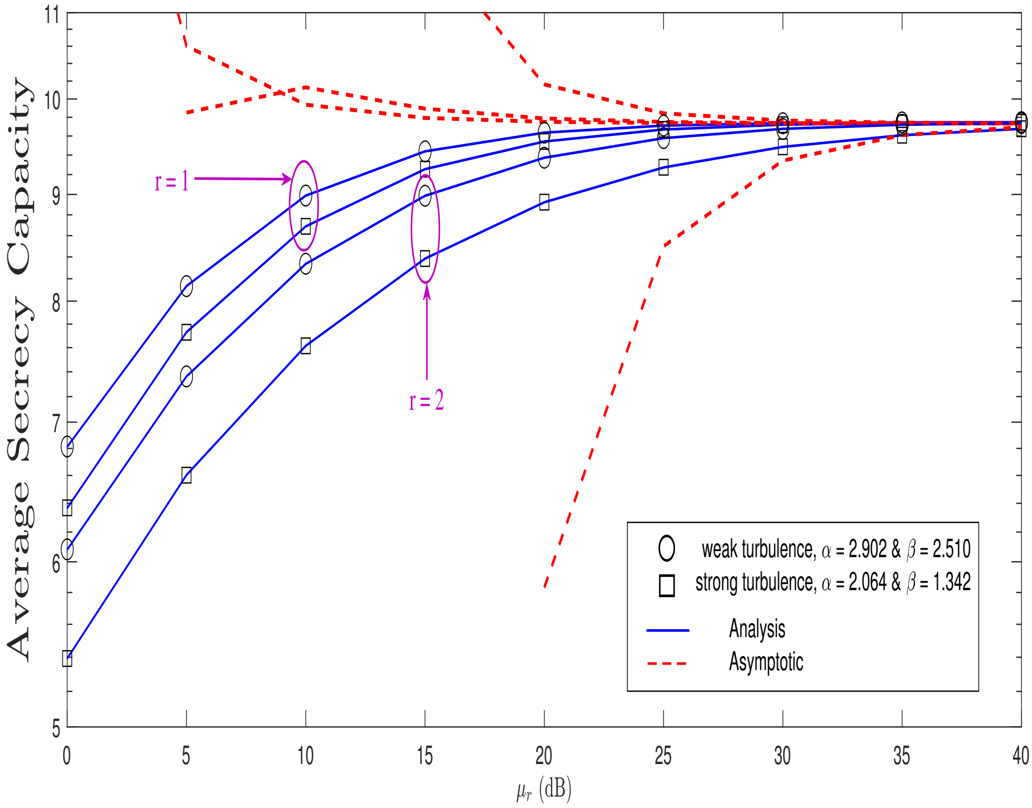

FIGURE 3.10: ASC vs μ_r for $\bar{\gamma}_E$=-10 dB, $\bar{\gamma}_R$ =20 dB, N_U=2, N_R=3, N_E=4, ξ=6.7.

Fig. 3.10 depicts the influence of the detection technique on the secrecy performance. It is observed that the secrecy performance with HD ($r = 1$) performs better than its counterpart IM/DD ($r = 2$), which corroborates with the fact that the SNR achieved with the HD technique surpasses that of the IM/DD technique. Additionally, it is evident that atmospheric turbulence levels affect the secrecy performance as attested by the performance difference between the weak and strong FSO turbulence conditions.

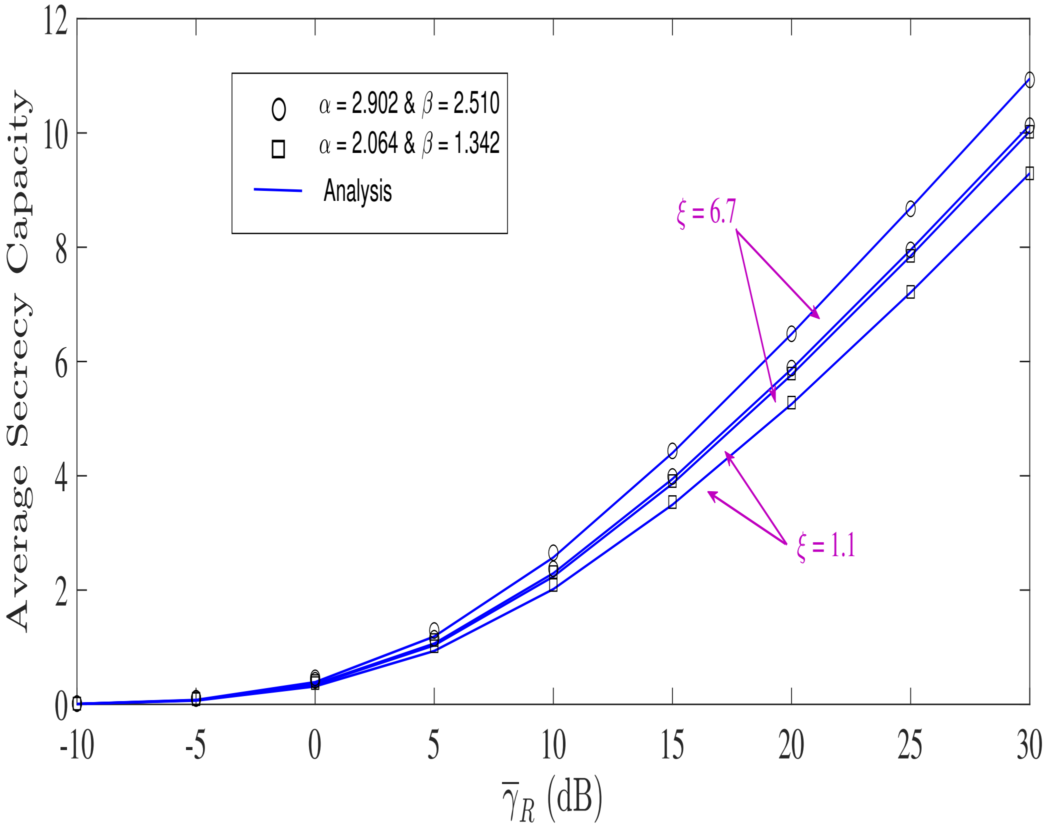

FIGURE 3.11: ASC versus $\bar{\gamma}_R$ for different ξ levels and turbulence conditions, $\bar{\gamma}_E$=-5 dB, μ_r=5 dB, N_U=2, N_R=4, N_E=2, and ξ=1.

Figure 3.11 shows the ASC versus the average SNR $\bar{\gamma}_R$ considering different values of ξ and the turbulence conditions. First, the secrecy performance improves under weak turbulence conditions, exhibiting a direct correlation with the SNR at the relay. Additionally, weak turbulence conditions are detrimental to the eavesdropper and can therefore yield an improvement in the secrecy performance. Also, the ASC performance is dependent of the pointing error levels, i.e., low pointing errors (higher ξ values) yield an improved secrecy performance compared to high values of the pointing errors. This is due to the fact that low pointing errors reduce the unintended signal leakage.

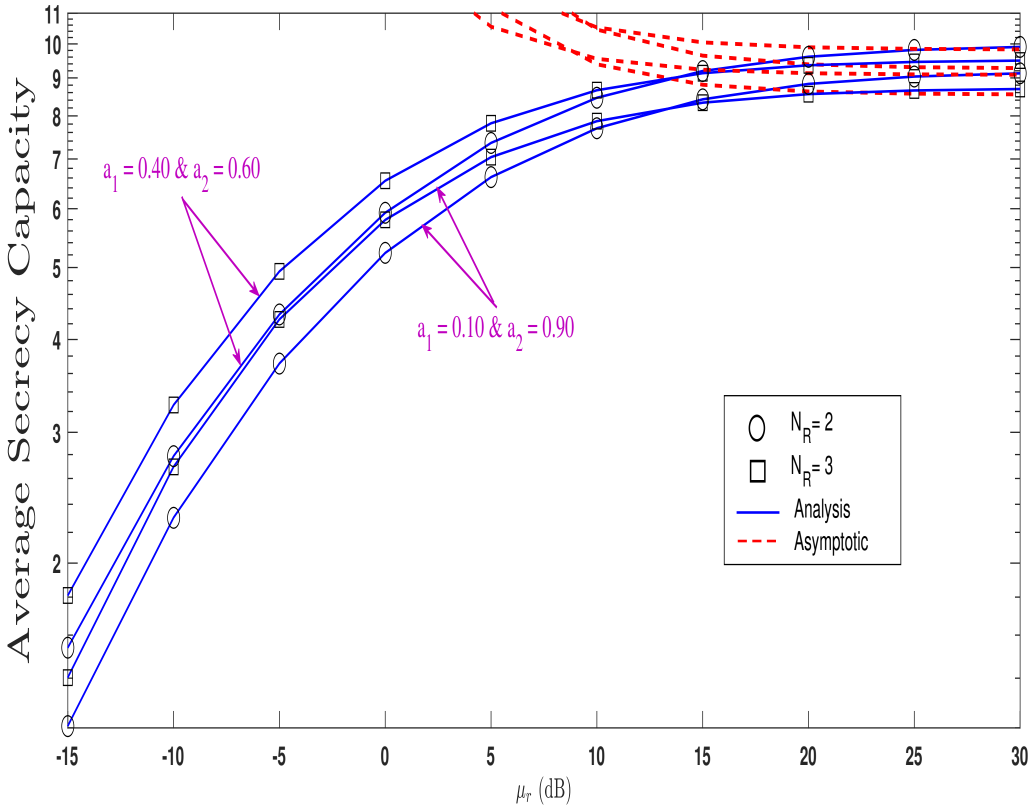

FIGURE 3.12: ASC vs μ_r for $\bar{\gamma}_E$=-10 dB, $\bar{\gamma}_R$=20 dB, N_U=2, N_E=4, α=2.902, β=2.510, r=1, and ξ=1.1.

Fig. 3.12 shows the ASC performance under weak turbulence conditions for various power allocation values, a_1, a_2 and number of antennas at the relay node, N_R. It can be shown that increasing N_R enhances the secrecy performance due to antenna diversity at the relay. In addition, allocating more power a_1 to the weak user U_1 through NOMA yields an improvement of the secrecy performance.

3.7 Conclusions

In this chapter, we have analyzed the secrecy performance of a MIMO-NOMA system using TAS in a mixed RF-FSO. The channel statistics for the underlying system were obtained and further used to derive closed-form expressions for the lower bound of the SOP, the probability of the SPSC and the ASC. Furthermore, the corresponding asymptotic has been derived to approximate the exact ASC at high SNR. The impact of the FSO link on the system performance has been investigated. Numerical results indicate that an increase in the number of antennas at the relay can enhance the system's secrecy performance in terms of the SOP SPSC and ASC. For example, doubling the number of antennas can lead to a corresponding improvement in the secrecy capacity. Conversely, it is observed that pointing errors in the FSO link negatively impact overall secrecy performance. When the SNR is 20 dB in strong turbulence conditions, a higher pointing error angle (i.e., $\xi = 0.8$) can reduce the achievable secrecy performance by up to approximately 50%. Furthermore, the corresponding asymptotic analysis has been derived to approximate the exact ASC at high SNR. To validate our theoretical results, Monte Carlo simulations were conducted across various system scenarios, confirming the efficacy of our mathematical derivations and providing practical insights into system design considerations. These specific examples illustrate how system parameters directly influence secrecy performance, offering practical implications for the deployment and optimization of MIMO-NOMA systems in mixed RF-FSO networks.

CHAPTER 4

Secrecy Performance Analysis of Uplink MIMO-NOMA in a Mixed RF-FSO System

4.1 Introduction

In modern mobile communication systems, the integration of the radio frequency (RF) spectrum with the free-space optical (FSO) spectrum stands out as a prospective security solution as highlighted in Chapter 3. For instance, the choice between mixed RF-FSO and hybrid RF-FSO systems is crucial for achieving robust security and reliable performance [132]. The mixed RF-FSO system enhances network resilience and efficiency by strategically deploying RF and FSO technologies tailored to turbulence conditions and security requirements, effectively balancing cost-effectiveness with optimized performance. This approach ensures that the system can adapt to varying turbulence conditions while maintaining high levels of security. In contrast, the hybrid RF-FSO system integrates RF and FSO technologies to leverage FSO's high data rates alongside RF's reliability in challenging conditions, ensuring uninterrupted and high-performance transmission despite potentially higher initial costs. In addition, detection complexity at relays and destinations involves managing signals from both RF and FSO channels, necessitating advanced signal processing and interference management techniques [79,85]. However, with the recent advancements in communication systems and its applications, there has been a concurrent enhancement in the methods employed to compromise the confidentiality of communication. Several studies have indicated that positive secrecy capacity is attainable when the legitimate receiver experiences a superior channel condition compared to the eavesdropper (see [21, 79, 85, 133] and the references therein). In scenarios where the legitimate receiver encounters a less favorable channel condition compared to the eavesdropper, physical layer security (PLS) presents a novel approach to ensuring secure communication by the utilization of interference, specifically artificial noise (AN) [101, 134]. This approach represents a strategic advancement in wireless communication systems, introducing an unconventional method to ensure the security of the legitimate nodes. Unlike traditional encryption methods operating at higher communication layers, AN operates at the physical layer capitalizing on the inherent characteristics of the communication channel to introduce intentional interference. The main objective of this technique is to add a layer of uncertainty for unauthorized nodes [10], rendering it challenging for eavesdroppers to accurately decipher the original signal. This method can enhance the security performance by introducing controlled interference at the foundational level of communication. Recently, several research endeavors have explored the security of mixed RF and FSO spectrum bands in diverse contexts, aiming to harness the advantages offered by both technologies [3, 19, 20, 124]. These investigations have encompassed a comprehensive examination of various RF-FSO link conditions, considering factors such as channel characteristics, atmospheric conditions, and system parameters. However, It is observed that none of the aforementioned investigations has presupposed an eavesdropper channel superior to the main channel. In such scenarios, the eavesdropper may possess favorable conditions that facilitate successful eavesdropping, which could reflect more advanced and realistic scenario. Therefore, emphasizing the necessity of adopting AN due to the absence of such assumptions. To this end, this part of work aims to incorporate the AN with non-orthogonal multiple access (NOMA)-aided multiple-input-multiple-output (MIMO) in a mixed RF-FSO system. The incorporation of AN on such mixed systems remains unexplored in the existing literature; and the present work aims to partially fill this knowledge gap. The main contributions of this chapter are as follows:

(a) We propose a two-user multi-antenna NOMA capable of generating AN in a mixed RF-FSO system with equal gain combining (EGC) scheme.

(b) Different from [3], we consider variable gain scheme at the relay node and further develop closed-form expressions of the associated statistical features, encompassing the probability density function (PDF) and the cumulative distribution function (CDF).

(c) Subsequently, we derive analytical expressions for the secrecy outage probability (SOP), the probability of the strictly positive secrecy capacity (SPSC) and the average secrecy capacity (ASC).

(d) Using the asymptotic expansion of the Meijer's G function at the high signal-to-noise ratio (SNR) conditions, we derive the asymptotic results for the SOP.

(e) Finally, Monte Carlo simulations are provided to validate the accuracy of the proposed analytical findings.

The remainder of the chapter is organized as follows. Section 4.2 delineates the proposed system model, followed by an exposition on channel statistics in Section 4.3. In Section 4.4, the secrecy performance of the underlying system is evaluated based on SOP, probability of the SPSC, and the ASC. Moreover, the corresponding asymptotic analytical framework for SOP is presented in Section 4.5 followed by the discussion of the results is detailed in 4.6. Finally, insights and observations are articulated in Section 4.7.

4.2 System Model

As shown in Figure 4.1, we consider an uplink AN-aided MIMO-NOMA communication in a dual-hop mixed RF-FSO system. This scenario considers the presence of an eavesdropper equipped with N_E antennas, aiming to attack the legitimate RF links. The legitimate RF transmissions occur between two multi-antenna users denoted as U_i with $i = \{1, 2\}$, and a legitimate receiver (relay) mounted with N_R antennas. Particularly, each user employs transmit antenna selection (TAS) to

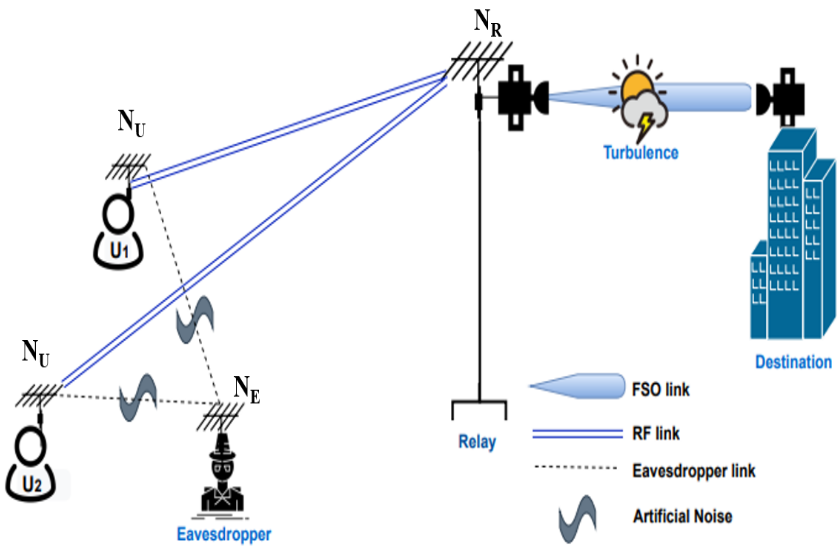

FIGURE 4.1: Illustration of an uplink two-user MIMO-NOMA configuration in a Mixed RF-FSO system.

transmit the confidential information to the destination with the help of the intermediate amplify-and-forward (AF) relay in a NOMA fashion. The selection of the best antenna at each user is given as [3]

$$b_i^* = \arg\max_k \sum_{j=1}^{N_R} |h_{U_i^{(k)}R_j}|^2, \tag{4.1}$$

where $h_{U_i^{(k)}R_j}$ corresponds the fading coefficient between the k^{th} antenna at U_i and j^{th} at the relay with $k \in \{1, \ldots, N_U\}$ follows the Nakagami-m distribution. To ensure secure transmission, each user transmits the information signal x_{U_i} with AN signal x_{AN_i} in the same time slot, intentionally causing interference with the eavesdropper's channel. Therefore, the transmitted signal from U_i is given as [90]

$$\mathcal{X}_{U_i} = x_{U_i} + x_{AN_i}, \tag{4.2}$$

where $E\left[|\mathcal{X}_{U_i}|^2\right] = 1$ and x_{AN_i} is designed to lie in the null space of the main channels. Subsequently, the received signal at the j-th antenna of the relay node is given by

$$y_{R_j} = \left(\sum_{i=1}^{2} \mathcal{X}_{U_i} h_{U_i^{(b_i^*)}R_j} \sqrt{a_i L_i P_t}\right) + n_{R_j}, \tag{4.3}$$

with $a_1 P_t$ being the signal power transmitted by U_1 and $a_2 P_t$ being the signal power transmitted by U_2, P_t stands for the total transmitted power by U_i, a_i is the power allocation coefficient with $\sum_{i=1}^{2}(a_i + a_{AN_i}) = 1$ encompasses the power of the AN signal and $\sum_{i=1}^{2} a_{AN_i} = a_{AN}$, $n_R = \sum_{j=1}^{N_R} n_{R_j}$, n_{R_j} is a Gaussian random variable at the j-th antenna of the relay with mean zero and variance $\sigma_{R_j}^2$, i.e., $n_{R_j} \sim \mathcal{CN}(0, \sigma_{R_j}^2)$, and L_i is the attenuation due to propagation loss [125]. Consequently, the EGC is employed to improve the SNR at the relay. Thus, the received signal at the relay node after the combiner is given by [135]

$$y_R = \sqrt{a_1 L_1 P_t} x_{U_1} h_{U_1^{(b_1^*)}R} + \sqrt{a_2 L_2 P_t} x_{U_2} h_{U_2^{(b_2^*)}R} + n_R, \tag{4.4}$$

where $y_R = \sum_{j=1}^{N_R} y_{R_j}$, $h_{U_i^{(b_i^*)}R} = \sum_{j=1}^{N_R} h_{U_i^{(b_i^*)}R_j}$ and $n_R = \sum_{j=1}^{N_R} n_{R_j}$.

In the FSO link, where a line of sight (LOS) exists between the relay and destination, the relay converts the composite signal in (4.4) to an optical signal[1]. As a result, the optical signal transmitted to the destination is formulated as $S_R = \mathcal{G}(1 + \mu y_R)$, where μ denotes the electrical-to-optical conversion coefficient

[1] The electrical signal is converted to an optical signal utilizing either intensity–modulation direct detection (IM/DD) or heterodyne detection (HD). It is worth mentioning that the HD offers better performance in terms of sensitivity and noise rejection compared to IM/DD. However, this comes at the cost of increased complexity due to the additional components and synchronization requirements. IM/DD, on the other hand, is a simpler and cheaper solution, but it might be less suitable for applications demanding high sensitivity or operation in noisy environments.

and $\mathcal{G}$ is the amplification factor [127]. Subsequently, the received optical signal $h_{RD}S_R$ at the destination undergoes a filtering process to eliminate the direct current (DC) component, effectively enhancing signal quality by eliminating undesired signals. Therefore, the received signal is given by

$$y_D = h_{RD}\mathcal{G}\mu y_R + n_D, \tag{4.5}$$

where the composite channel gain coefficient $h_{RD} = h_l h_a h_p$ represents the combined impact of atmospheric loss (h_l), atmospheric turbulence (h_a), pointing errors caused by the misalignment (h_p), and n_D represents zero mean Gaussian noise at the destination with variance σ_D^2.

Following the principles of the power domain NOMA, we delve into the instantaneous SNR at the relay and the signal-to-interference-plus-noise ratio (SINR) at the destination. Initially, the strongest user's signal x_{U_2} is decoded at the destination, and U_1's signal will be treated as noise, and subsequently apply the successive interference cancellation (SIC) to decode x_{U_1}. By substituting (4.4) in (4.5) and conducting some algebraic operations provided in Appendix C, the instantaneous SINR denoted by γ_2 can be obtained as

$$\gamma_2 = \frac{a_2\gamma_D\gamma_R^{(2)}}{a_1\gamma_D\gamma_R^{(1)} + \gamma_R^{(1)} + \gamma_D + 1}, \tag{4.6}$$

where $\gamma_D = \frac{|h_{RD}|^2}{\sigma_D^2}$ and the instantaneous SINRs for the composite received signal at the relay denoted by $\gamma_R^{(1)}$ and $\gamma_R^{(2)}$ defined in (3.5) respectively as

$$\gamma_R^{(2)} = \frac{X_{U_2R}}{1 + X_{U_1R}}, \tag{4.7}$$

$$\gamma_R^{(1)} = \frac{X_{U_1R}}{1 + X_{U_2R}}, \tag{4.8}$$

where X_{U_1R} and X_{U_2R} are the instantaneous SNRs for each user expressed as

$$X_{U_1R} = \frac{a_1L_1P_t|h_{U_1^{(b_1^*)}R}|^2}{\sigma_R^2}, \tag{4.9}$$

$$X_{U_2R} = \frac{a_2L_2P_t|h_{U_2^{(b_2^*)}R}|^2}{\sigma_R^2}. \tag{4.10}$$

The expression in (4.6) is mathematically intractable. To circumvent this, we focus on the analysis at high SNR values and adopt the following upper bound

$$\gamma_2 \cong \min(\gamma_D, \gamma_R^{(2)}). \tag{4.11}$$

Subsequently, the instantaneous SNR for the weak user denoted by γ_1 is given by

$$\gamma_1 = \frac{a_1 \gamma_D \gamma_R^{(1)}}{\gamma_R^{(1)} + \gamma_D + \Lambda} \cong \min(\gamma_D, \gamma_R^{(1)}). \tag{4.12}$$

As aforementioned, the legitimate RF transmissions can be compromised by security attacks due to eavesdropping efforts. It is assumed that the eavesdropper leverages its multiple antennas and adopts the EGC to improve the probability of successful eavesdropping. Similar to (4.4), the received EGC signal at the eavesdropper is given by[2]

$$\begin{aligned} y_E = {} & \sqrt{a_1 L_1 P_t} x_{U_1} h_{U_1^{(b_1^*)} E} + \sqrt{a_2 L_2 P_t} x_{U_2} h_{U_2^{(b_2^*)} E} \\ & + \sqrt{a_{AN_1} L_1 P_t} x_{U_1} h_{U_1^{(b_1^*)} E} + \sqrt{a_{AN_2} L_1 P_t} x_{U_1} h_{U_1^{(b_1^*)} E} + n_E, \end{aligned} \tag{4.13}$$

where $y_E = \sum_{j=1}^{N_E} y_{E_j}$, $h_{U_i^{(b_i^*)} E} = \sum_{j=1}^{N_E} h_{U_i^{(b_i^*)} E_j}$ modeled according to the Nakagami-m distribution, and $n_E = \sum_{j=1}^{N_E} n_{E_j}$, n_{E_j} are assumed to be i.i.d. complex Gaussian random variables with zero mean and variance $\sigma_{E_j}^2$, i.e., $n_{E_j} \sim \mathcal{CN}(0, \sigma_{E_j}^2)$. Hence, the instantaneous SNRs obtained from (4.13) are given by[3]

$$\gamma_E^{(1)} = \frac{(X_{U_1E}/\sigma_{AN_1}^2)}{1 + (X_{U_2E}/\sigma_{AN_2}^2)}, \tag{4.14}$$

$$\gamma_E^{(2)} = \frac{(X_{U_2E}/\sigma_{AN_2}^2)}{1 + (X_{U_1E}/\sigma_{AN_1}^2)}, \tag{4.15}$$

where X_{U_1E} and X_{U_2E} instantaneous SNRs for each user defined in (3.12) as

$$X_{U_1E} = \frac{a_1 L_1 P_t |h_{U_1^{(b_1^*)} E}|^2}{\sigma_E^2}, \tag{4.16}$$

[2]Significant emphasis should be placed on the deliberate design of the AN signal to reside within the null space of the legitimate channel, with the eavesdropper being the intentional recipient of this AN signal.

[3]Here, we assume that the eavesdropper faces difficulty distinguishing between multiple user signals due to interference resulting from NOMA technology.

$$X_{U_2E} = \frac{a_2 L_2 P_t |h_{U_2^{(b_2^*)}E}|^2}{\sigma_E^2}. \tag{4.17}$$

It is assumed that the antenna selection relies on the $U_i -\ R$ link, presuming the eavesdropper is unaware of this selection and perceives the transmission as originating randomly from each user.

4.3 Channel Model

The channel statistics of both the RF and FSO links are presented in terms of PDF and CDF in this section.

4.3.1 RF Links

Considering TAS at each user where the best antenna is selected, the CDF of the instantaneous SNR of the random variable (RV) γ_R at the relay can be expressed as [13]

$$F_{\gamma_R}(\gamma_R) = \sum_{n=0}^{N_{U_i}} (-1)^n \begin{pmatrix} N_{U_i} \\ n \end{pmatrix} e^{-n\lambda_R \gamma_R} \sum_{k=0}^{n(N_R-1)} C_{k,n} (\lambda_R \gamma_R)^k, \tag{4.18}$$

where $\lambda_R = \frac{m_R}{\bar{\gamma}_R}$. The PDF obtained from (4.18) is given by

$$f_{\gamma_R}(\gamma_R) = \sum_{n=0}^{N_{U_i}} \begin{pmatrix} N_{U_i} \\ n \end{pmatrix} (-1)^n \sum_{k=1}^{n(N_R-1)} C_{k,n} (\lambda_R \gamma_R)^{k-1} e^{(n\lambda_R \gamma_R)} \Big(k - n(\lambda_R \gamma_R)\Big). \tag{4.19}$$

Next, we present the statistical analysis of the eavesdropper's channel in terms of the PDF and CDF as

$$f_{\gamma_E}(\gamma_E) = \frac{(\lambda_E a_{AN})^{N_E}}{\Gamma(N_E)} \gamma_E^{N_E - 1} e^{-a_{AN} \lambda_E \gamma_E}, \tag{4.20}$$

$$F_{\gamma_E}(\gamma_E) = \frac{1}{\Gamma(N_E)} \Upsilon(N_E, a_{AN} \lambda_E \gamma_E). \tag{4.21}$$

4.3.2 FSO Link

Similar to Chapter 3, we utilize a unified gamma-gamma distribution on the FSO link due to its accurate representation of atmospheric turbulence with diverse turbulence severity. To this end, the PDF of the gamma-gamma RV γ_D is given as (3.21)

$$F_{\gamma_D}(\gamma_D) = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)} G^{3r,1}_{r+1,3r+1}\left(\frac{(d\alpha\beta)^r}{\mu_r r^{2r}}\gamma_D \middle|^{1,\Delta(r,\xi^2+1)}_{\Delta(r,\xi^2),\Delta(r,\alpha),\Delta(r,\beta),0}\right). \quad (4.22)$$

In this chapter, we assume the variable-gain relaying scheme since the use of variable gain has several advantages over fixed-gain relaying schemes, such as improved spectral efficiency, reduced power consumption, and enhanced reliability[4]. Making use of the equivalent end-to-end SNR associated with U_1 in (4.12), the resulting CDF can be expressed as

$$\begin{aligned} F_{\gamma^{(V)}_{eq_1}}(x) &= \Pr\left(\min\left(\gamma_R^{(1)}, \gamma_D\right) < x\right) \\ &= F_{\gamma_R}(\gamma_R) + F_{\gamma_D}(\gamma_D) - F_{\gamma_R}(\gamma_R)F_{\gamma_D}(\gamma_D), \end{aligned} \quad (4.23)$$

where (V) indicates the variable gain relaying scheme utilized at the relay. After substituting (4.18) and (4.22) in (4.23), and adopting some mathematical manipulations, we obtain

$$F_{\gamma^{(V)}_{eq_1}}(x) = 1 + \sum_{(nk)} x^k e^{\frac{-n\lambda_R}{a_1}x}\left[1 - \Psi G^{3r+1,0}_{r,3r+1}\left(q_{nU_1}x \middle| \begin{matrix} C_1 \\ C_3 \end{matrix}\right)\right]. \quad (4.24)$$

Using a similar methodology adopted in (4.24), we derive an expression for the equivalent end-to-end SINR linked to U_2 in (4.6) as

$$F_{\gamma^{(V)}_{eq_2}}(x) = 1 + \sum_{(nk)} x^k exp\left[\frac{-a_1 n\lambda_R}{a_2}x\right]\left[1 - \Psi G^{3r+1,0}_{r,3r+1}\left(q_{nU_2}x \middle| \begin{matrix} C_1 \\ C_3 \end{matrix}\right)\right]. \quad (4.25)$$

[4]It is important to note that the variable-gain relaying requires a full knowledge of channel state information (CSI) [127].

4.4 Secrecy Performance Analysis

4.4.1 Secrecy Outage Probability

In the underlying system model, the destination receives signals from two users simultaneously. Thus, the occurrence of a secrecy outage event is defined by the event where either $C_{s_{U_1}}$ or $C_{s_{U_2}}$ falls below a predefined secrecy rate R_s. Mathematically, this can be formulated as (3.27). Thus, the SOP corresponding to user U_i can be given by

$$\mathcal{P}_{\text{out,lb}}^{(i)} = \int_0^\infty F_{\gamma_{eq_i}^{(V)}}(\Theta\gamma_E) f_{\gamma_E}(\gamma_E) \mathrm{d}\gamma_E. \tag{4.26}$$

Then, we substitute (4.24) and (4.20) in (4.26) to derive the expression for the lower bound of the SOP associated with U_1 as

$$\begin{aligned}\mathcal{P}_{\text{out,lb}}^{(1)} = 1 + \frac{(a_{\text{AN}_1}\lambda_E)^{N_E}}{\Gamma(N_E)} \sum_{(nk)} \frac{\Theta^k}{k!} \int_0^\infty \gamma_E^{N_E+k-1} e^{-\left(a_{\text{AN}_1}\lambda_E + \frac{n\lambda_R\Theta}{a_1}\right)\gamma_E} d\gamma_E \\ - \Psi \int_0^\infty \gamma_E^{N_E+k-1} e^{-\left(a_{\text{AN}_1}\lambda_E + \frac{n\lambda_R\Theta}{a_1}\right)\gamma_E} G_{r+1,3r+1}^{3r,1}\left[\Theta q_{n_1}\gamma_E \mid \begin{array}{c} 1, C_1 \\ C_2, 0 \end{array}\right] d\gamma_E.\end{aligned} \tag{4.27}$$

To solve the integrals in (4.27), we leverage the antiderivative [128], (see Eqn. 7.813 and Eqn.3.326.2). Thus, the resulting lower bound of the SOP corresponding to U_1 can be expressed as

$$\mathcal{P}_{\text{out,lb}}^{(1)} = 1 + \frac{(a_{\text{AN}_1}\lambda_E)^{N_E}}{\Gamma(N_E)} \sum_{(nk)} \frac{(\Theta)^k}{k!} (K_1 - K_2), \tag{4.28}$$

where $K_1 = \Psi \left(\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E\right)^{-N_E-k} G_{r+2,3r+1}^{3r,2}\left[\frac{\Theta q_{n_1}}{\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E}\middle|\begin{array}{c} 1, 1-N_E-k, C_1 \\ C_2, 0 \end{array}\right]$, and $K_2 = \frac{\Gamma(N_E+k)}{\left(\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E\right)^{N_E+k}}$.

To develop the lower bound of the SOP associated with U_2 in a closed-form, we utilize a similar methodology to the one used to obtain (4.28). Hence, the lower bound on the SOP linked to U_2 is expressed as

$$\mathcal{P}_{\text{out,lb}}^{(2)} = 1 + \frac{(a_{\text{AN}_2}\lambda_E)^{N_E}}{\Gamma(N_E)} \sum_{(nk)} \frac{\Theta^k}{k!} (K_3 - K_4), \tag{4.29}$$

where $K_3 = \Psi\left(\frac{n\lambda_R\Theta a_1}{a_2} + a_{\text{AN}_2}\lambda_E\right)^{-N_E-k} G^{3r,2}_{r+2,3r+1}\left[\frac{\Theta q_{n_1}}{\frac{n\lambda_R\Theta a_1}{a_2}+a_{\text{AN}_2}\lambda_E}\middle|^{1,1-N_E-k,C_1}_{C_2,0}\right]$ and $K_4 = \frac{\Gamma(N_E+k)}{\left(\frac{n\lambda_R\Theta a_1}{a_2}+a_{\text{AN}_2}\lambda_E\right)^{N_E+k}}$.

Plugging (4.28) and (4.29) into (3.27) results in the closed-form expression of the overall SOP associated with the proposed NOMA system.

4.4.2 Probability of the Strictly Positive Secrecy Capacity

In the underlying system model, SPSC is mathematically is formulated as

$$\begin{aligned}\mathcal{P}_{\text{SPSC}} &= 1 - \left[1 - \left(1 - \mathcal{P}^{(1)}_{\text{out}}(0)\right)\left(1 - \mathcal{P}^{(2)}_{\text{out}}(0)\right)\right]\\ \mathcal{P}^{(i)}_{\text{SPSC}} &= 1 - \int_0^\infty F_{\gamma^{(V)}_{eq_i}}(\Theta\gamma_E) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E.\end{aligned} \tag{4.30}$$

To solve the integral in (4.30), we can further use a similar analysis developed in (4.26) by substituting $R_s = 0$, and the expressions for $\mathcal{P}_{\text{SPSC}}$ related to U_1 can be directly obtained as

$$\mathcal{P}^{(1)}_{\text{SPSC}} = \frac{(a_{\text{AN}_1}\lambda_E)^{N_E}}{\Gamma(N_E)}\sum_{(nk)}\frac{(I_1 - I_2)}{k!}, \tag{4.31}$$

where $I_1 = \Psi\left(\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E\right)^{-N_E-k} G^{3r,2}_{r+2,3r+1}\left[\frac{q_{n_1}}{\frac{n\lambda_R}{a_1}+a_{\text{AN}_1}\lambda_E}\middle|^{1,1-N_E-k,C_1}_{C_2,0}\right]$, and $I_2 = \frac{\Gamma(N_E+k)}{\left(\frac{n\lambda_R}{a_1}+a_{\text{AN}_1}\lambda_E\right)^{N_E+k}}$.

Similarly, the lower bound on the SOP linked to U_2 is expressed as

$$\mathcal{P}^{(2)}_{\text{SPSC}} = \frac{(a_{\text{AN}_2}\lambda_E)^{N_E}}{\Gamma(N_E)}\sum_{(nk)}\frac{(I_3 - I_4)}{k!}, \tag{4.32}$$

where $I_3 = \Psi\left(\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E\right)^{-N_E-k} G^{3r,2}_{r+2,3r+1}\left[\frac{q_{n_1}}{\frac{n\lambda_R a_1}{a_2}+a_{\text{AN}_2}\lambda_E}\middle|^{1,1-N_E-k,C_1}_{C_2,0}\right]$, and $I_4 = \frac{\Gamma(N_E+k)}{\left(\frac{n\lambda_R a_1}{a_2}+a_{\text{AN}_2}\lambda_E\right)^{N_E+k}}$.

Substituting (4.31) and (4.32) into (4.30) results the analytical expression of the SPSC.

4.4.3 Average Secrecy Capacity

Assuming active eavesdropping scenario, the ASC of the underlying system can be mathematically formulated as

$$\mathcal{ASC}^{(i)} = \sum_{i=1}^{2} \int_{0}^{\infty} \frac{F_{\gamma_E}(\gamma)}{1+\gamma} \left[1 - F_{\gamma_{eq_i}^{(V)}}(\gamma)\right] d\gamma. \tag{4.33}$$

After substituting (4.21) and (4.24) into (4.33) and adopting some mathematical manipulations provided in Appendix D, we obtain

$$\begin{aligned}
\mathcal{ASC}^{(1)} = \sum_{(nk)} \left(\frac{n\lambda_R}{a_1}\right)^k \Bigg\{ \Bigg[G_{2,2}^{1,2}\left[\frac{n\lambda_R}{a_1}\middle|^{0,-(k+1)}_{-,-(k+1)}\right] - \frac{a_1 \Psi}{n\lambda_R} \\
\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k & 1, C_1 & \frac{a_1}{n\lambda_R}, \frac{q_{nU_1} a_1}{n\lambda_R} \\ - & k & C_2, 0 & \end{array}\right] + \sum_{j=0}^{N_E-1} \binom{N_E-1}{j} (-1)^j \\
\times \frac{(a_{\mathrm{AN}_1}\lambda_E)^j}{j!} \Bigg(G_{2,2}^{1,2}\left[\frac{n\lambda_R}{a_1} + a_{\mathrm{AN}_1}\lambda_E \middle|^{0,-(k+j+1)}_{-,-(k+j+1)}\right] - \frac{\Psi}{\frac{n\lambda_R}{a_1} + a_{\mathrm{AN}_1}\lambda_E} \\
\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k+g & 1, C_1 & \frac{1}{\frac{n\lambda_R}{a_1} + a_{\mathrm{AN}_1}\lambda_E}, \frac{q_{nU_1}}{\frac{n\lambda_R}{a_1} + a_{\mathrm{AN}_1}\lambda_E} \\ - & k+g & C_2, 0 & \end{array}\right] \Bigg) \Bigg] \Bigg\}.
\end{aligned} \tag{4.34}$$

Similarly, we can obtain the closed-form expression of the exact ASC for U_2 as

$$\begin{aligned}
\mathcal{ASC}^{(2)} = \sum_{(nk)} (\frac{n\lambda_R a_1}{a_2})^k \Bigg\{ \Bigg[G_{2,2}^{1,2}\left[(\frac{n\lambda_R a_1}{a_2})\middle|^{0,-(k+1)}_{-,-(k+1)}\right] - \frac{a_2 \Psi}{n\lambda_R a_1} \\
\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k & 1, C_1 & \frac{a_2}{n\lambda_R a_1}, \frac{a_2 q_{nU_1}}{n\lambda_R a_1} \\ - & k & C_2, 0 & \end{array}\right] + \sum_{j=0}^{N_E-1} \binom{N_E-1}{j} (-1)^j \\
\times \frac{(a_{\mathrm{AN}_2}\lambda_E)^j}{j!} \Bigg(G_{2,2}^{1,2}\left[(\frac{n\lambda_R a_1}{a_2}) + a_{\mathrm{AN}_2}\lambda_E \middle|^{0,-(k+g+1)}_{-,-(k+g+1)}\right] - \frac{\Psi}{(\frac{n\lambda_R a_1}{a_2}) + a_{\mathrm{AN}_2}\lambda_E} \\
\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k+g & 1, C_1 & \frac{1}{(\frac{n\lambda_R a_1}{a_2}) + a_{\mathrm{AN}_2}\lambda_E}, \frac{q_{nU_1}}{(\frac{n\lambda_R a_1}{a_2}) + a_{\mathrm{AN}_2}\lambda_E} \\ - & k+g & C_2, 0 & \end{array}\right] \Bigg) \Bigg] \Bigg\}.
\end{aligned} \tag{4.35}$$

Consequently, the ASC of the variable-gain relaying scheme can be obtained using (4.33).

4.5 Asymptotic SOP Analysis

In this section, we provide the asymptotic analysis of the SOP at high SNR values. First, we obtain the CDF of the equivalent SNR to U_1. As $\mu_r \to \infty$, (4.24) can be approximated as

$$F^{\infty}_{\gamma^{(1)}_{\text{eq}}}(x) = 1 + \sum_{(nk)} x^k e^{-\frac{n\lambda_R}{a_1}x}\left(1 - \Psi \sum_{i=1}^{3r} \varphi_i x^{C_{2,i}}\right), \tag{4.36}$$

where

$$\varphi_i = \left(\frac{(d\alpha\beta)^r n\lambda_R}{a_1\mu_r r^{2r}}\right)^{C_{2,i}} \frac{\prod_{l=1,l\neq i}^{3r}\Gamma\left(C_{2,l} - C_{2,i}\right)}{C_{2,i}\prod_{m=1}^{r}\Gamma\left(C_{1,m} - C_{2,i}\right)}.$$

The expression in (4.36) can be represented via the dominant term $(min(\xi, \alpha, \beta))$ where ξ stands for the 1-st term in $C_{2,i}$, α represents the $(r+1)$-th term and β represents $(2r+1)$-th term, respectively. To obtain the CDF of the equivalent SINR for U_2, we utilize the same approach used to obtain (4.36). To derive the asymptotic SOP for U_1, we substitute (4.36) and (4.20) into (4.26) as

$$\mathcal{P}^{\infty(1)}_{\text{out,lb}} \approx 1 - \frac{(a_{\text{AN}_1}\lambda_E)^{N_E}}{\Gamma(N_E)} \sum_{(nk)} \left(\frac{\lambda_R\Theta}{a_1}\right)^k \left[\Psi \sum_{i=1}^{3r} \frac{\varphi_i \Theta^{C_{2,i}}\Gamma(Q_i)}{\kappa_1^{Q_i}} + \left(\frac{\Gamma(\omega)}{\kappa_1^{\omega}}\right)\right], \tag{4.37}$$

where $\omega = N_E L + k$ and $Q_i = C_{2,i} + k + N_E$. A similar approach can be used to obtain the lower bound of the asymptotic SOP for U_2 given by

$$\mathcal{P}^{\infty(2)}_{\text{out,lb}} \approx 1 - \frac{(a_{\text{AN}_2}\lambda_E)^{N_E}}{\Gamma(N_E)} \sum_{(nk)} \left(\frac{a_1\lambda_R\Theta}{a_2}\right)^k \left[\Psi \sum_{i=1}^{3r} \frac{\varphi_i \Theta^{C_{2,i}}\Gamma(Q_i)}{\kappa_2^{Q_i}} + \left(\frac{\Gamma(\omega)}{\kappa_2^{\omega}}\right)\right]. \tag{4.38}$$

After plugging (4.37) and (4.38) into (3.27) yields the asymptotic SOP for the mixed RF-FSO system.

4.6 Numerical Results

In this section, representative numerical results are plotted along with Monte Carlo simulations to assess the accuracy of our proposed mathematical analysis. Without loss of generality, we use various atmospheric turbulence associated with the FSO link: weak turbulence– α=2.902 and β= 2.510; moderate turbulence– α=2.296 and β= 1.822; strong turbulence–, α=2.064 and β=1.342 [3]. Moreover, it is assumed that $R_S = 0.01$ and $m_R = m_E = 2$ throughout this section. It can be observed that all the derived analytical results pertaining to the SOP, probability of the SPSC, ASC, and the asymptotic SOP are matching with the Monte Carlo simulations. This validates the accuracy of the proposed mathematical framework. Furthermore, it is noteworthy that the derived asymptotic SOP curves are a good approximation of the exact ones for high SNR values. The lower bound on the

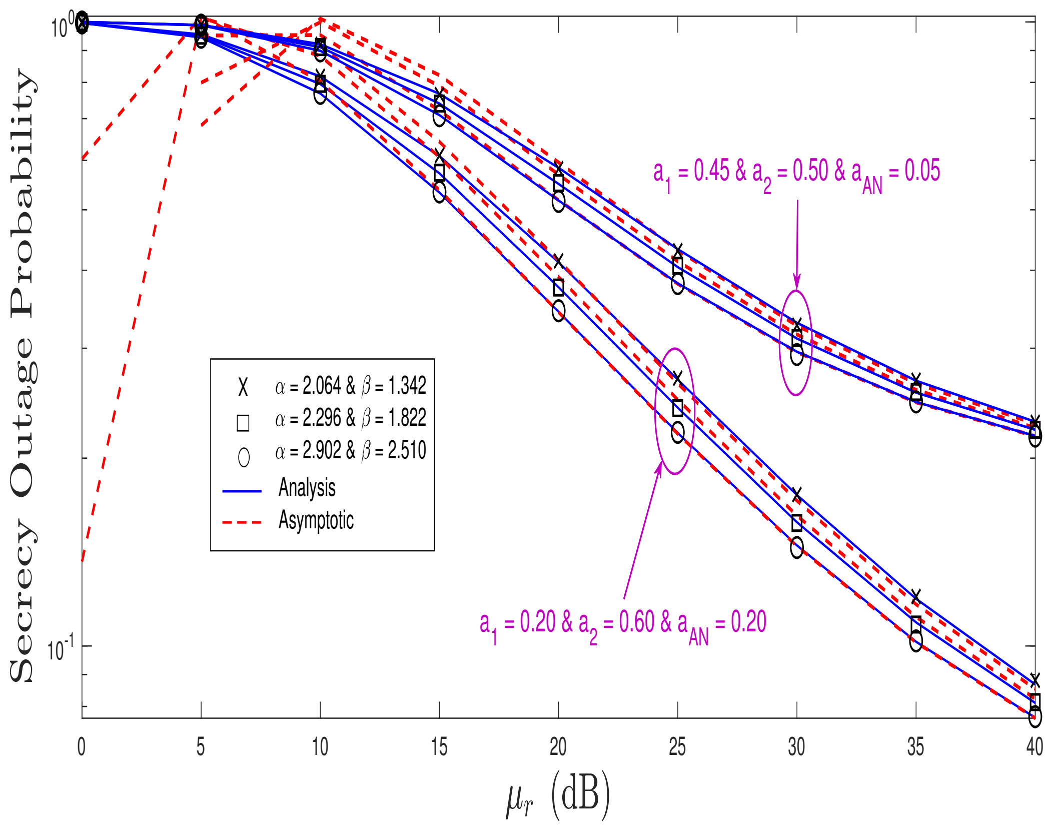

FIGURE 4.2: SOP vs μ_r with different values of a_{AN}, α and β, $\bar{\gamma}_R = 10$ dB, $\bar{\gamma}_E$ = -10 dB, r =1, $\xi = 1$, $N_U = 2$, $N_R = 4$, $N_E = 2$ and $R_s = 0.01$.

SOP versus μ_r is shown in Figure 4.2 with different values of a_{AN} and turbulence conditions. The system demonstrates superior performance under weak turbulence conditions when contrasted with scenarios involving moderate and strong turbulence. Additionally, it is evident that the SOP performance exhibits variability across different levels of a_{AN}; with the established fact that increasing AN power degrades the quality of the eavesdropper channel.

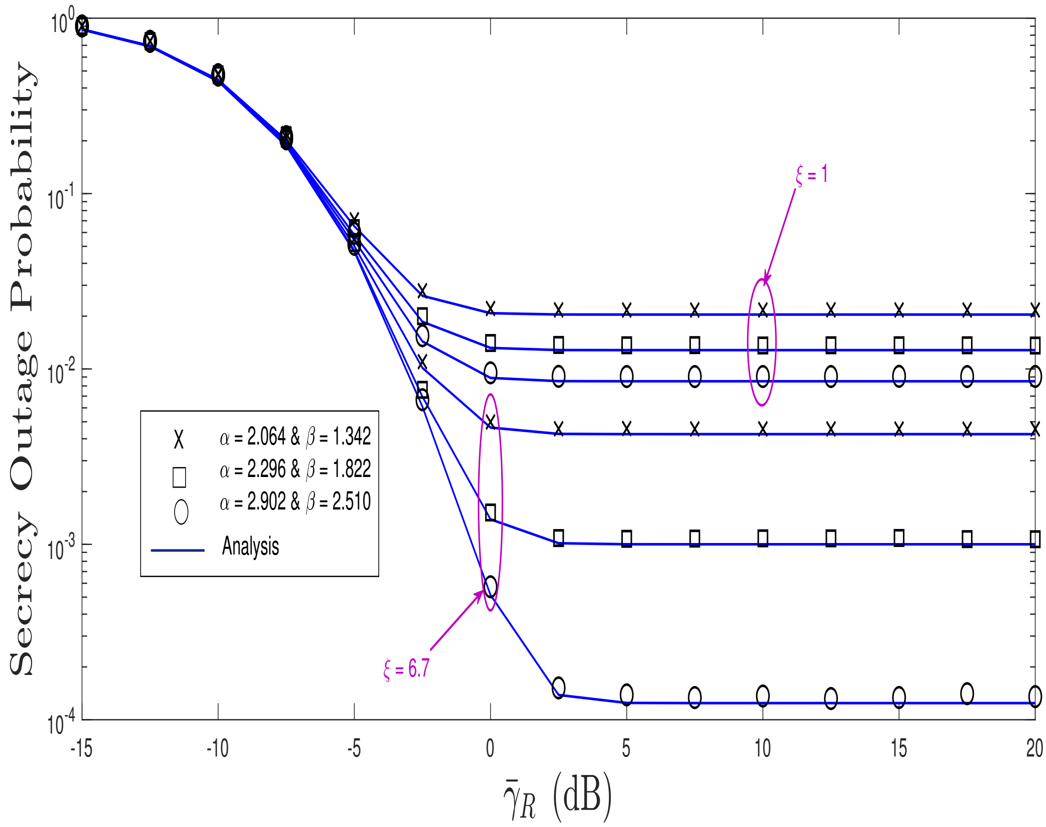

FIGURE 4.3: SOP vs $\bar{\gamma}_R$ with different ξ and α, β, $\bar{\gamma}_E$ = -1 dB, μ_r = 10 dB, r =2, a_1 = 0.20, a_2 = 0.60, a_{AN} = 0.20 and $N_U = N_R = N_E = 2$.

Figure 4.3 illustrates the lower bound of the SOP vs $\bar{\gamma}_R$ considering different turbulence conditions and ξ. First, the SOP curves initially decrease slightly until $\bar{\gamma}_R$ = 10 dB. Then, the secrecy performance of the mixed RF-FSO system shows minimal sensitivity to further increases in the average SNR at the relay. This is because the equivalent end-to-end SNR with variable gain relaying remains equal to the average SNR at the destination, even when the average SNR at the relay node becomes significantly large. Second, it is clear that the SOP performance displays variability with distinct levels of ξ. Specifically, the secrecy performance of the mixed system deteriorates with strong pointing errors ($\xi = 1$). This is due to the misalignment between the transmitter and receiver aperture in the FSO link. As a result, the eavesdropper may have an increased chance of eavesdropping the transmitted signal and thereby deteriorating the secrecy performance of the mixed system. Conversely, when the pointing error is negligible ($\xi = 6.7$), the secrecy performance is primarily influenced by atmospheric turbulence and RF link conditions.

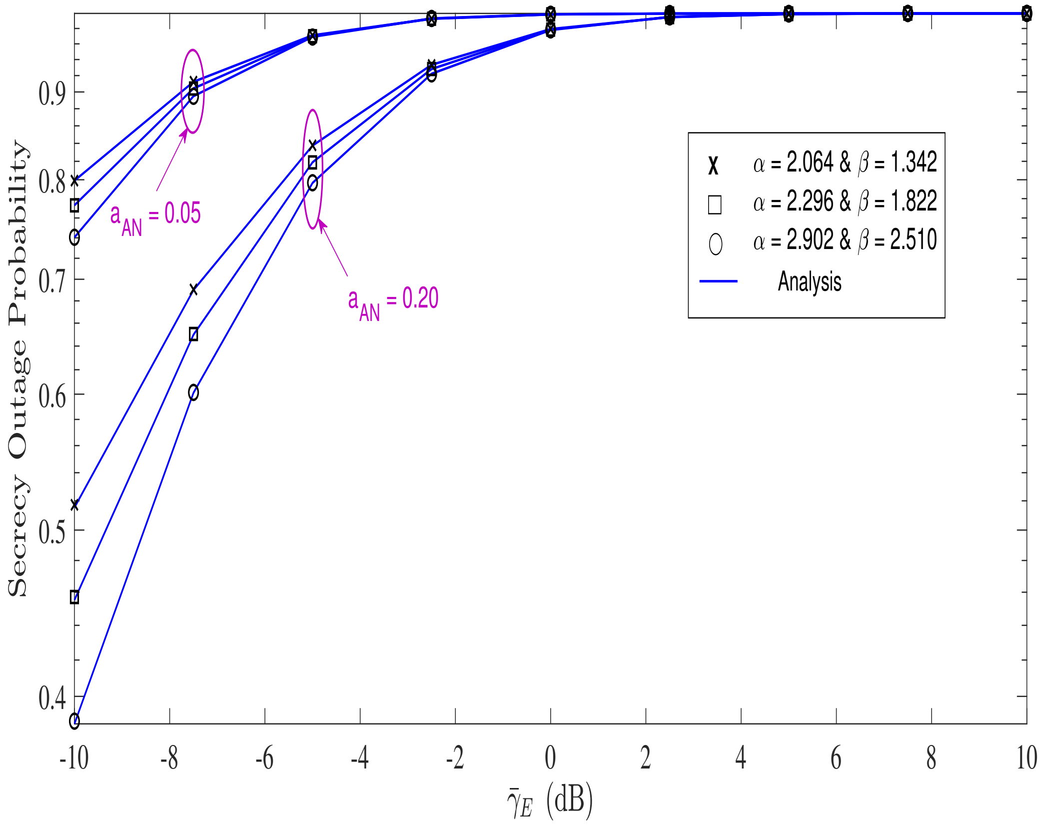

FIGURE 4.4: SOP vs $\bar{\gamma}_E$ with different a_{AN}, α and β, $\bar{\gamma}_R = 10$ dB, $\mu_r = 10$ dB, $N_U = 2$, $N_R = 4$, $N_E = 2$ and r =1.

Figure 4.4 depicts the secrecy performance against the average SNR at the eavesdropper $\bar{\gamma}_E$. As the signal quality of the eavesdropper increases, the SOP also increases under the various FSO turbulence conditions and different pointing error levels, until it reaches a saturation level (approximately one) in the high-SNR regime (good signal quality of the eavesdropper link). This can be explained intuitively by the fact that for a strong eavesdropper's signal quality, the system secrecy is guaranteed to be compromised. This behavior lies in the inherent vulnerability of the system's security performance to strong eavesdropper channels. When the eavesdropper's channel experiences high signal quality, it becomes more adept at intercepting and decoding the transmitted information, thereby compromising the secrecy of the communication link.

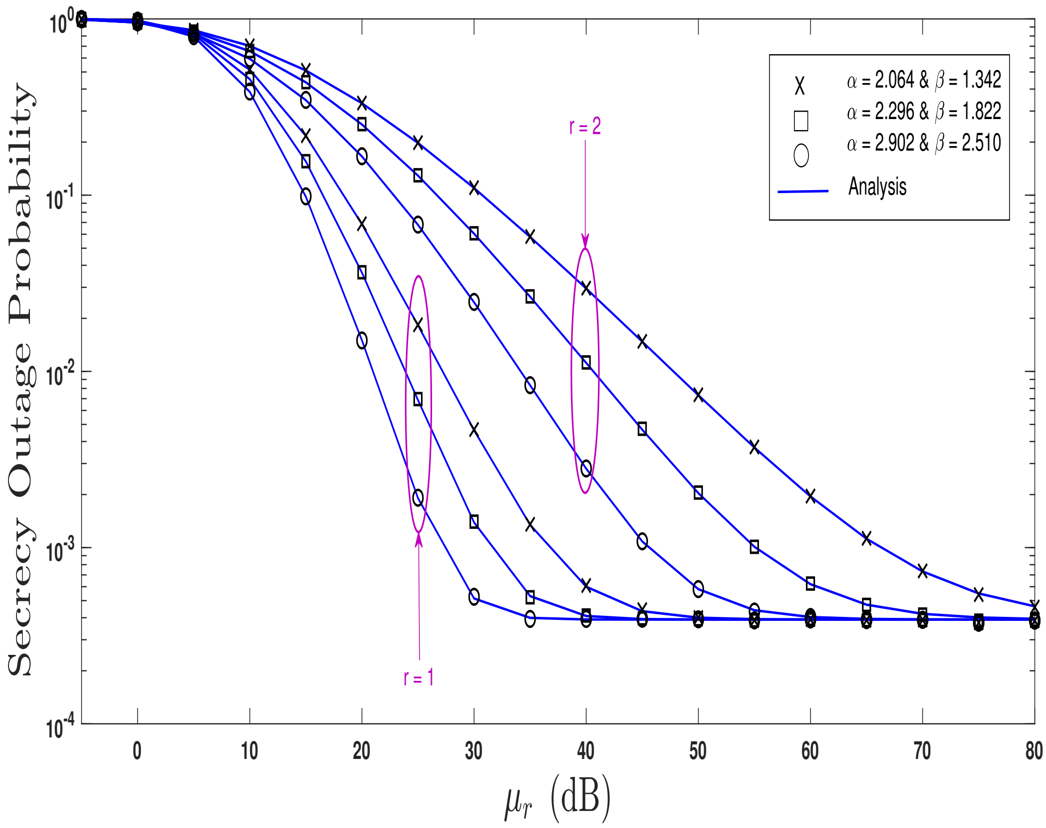

FIGURE 4.5: SOP vs μ_r for different α, β and r, $\bar{\gamma}_R = 10$ dB, $\bar{\gamma}_E = 0$ dB, $N_U = 2$, $N_R = 4$, $N_E = 2$, and $R_s = 0.01$.

The impact of the detection technique on the secrecy performance in terms of secrecy is investigated in Figure 4.5. It can be seen that HD with $r = 1$ results in superior performance compared to IM/DD with $r = 2$ counterpart over the entire SNR regime, and for the various FSO turbulence conditions. This superiority can be attributed to the enhanced sensitivity and selectivity of HD techniques which allow for more accurate and reliable detection of the received signal, thereby mitigating the effects of turbulence and improving overall secrecy performance.

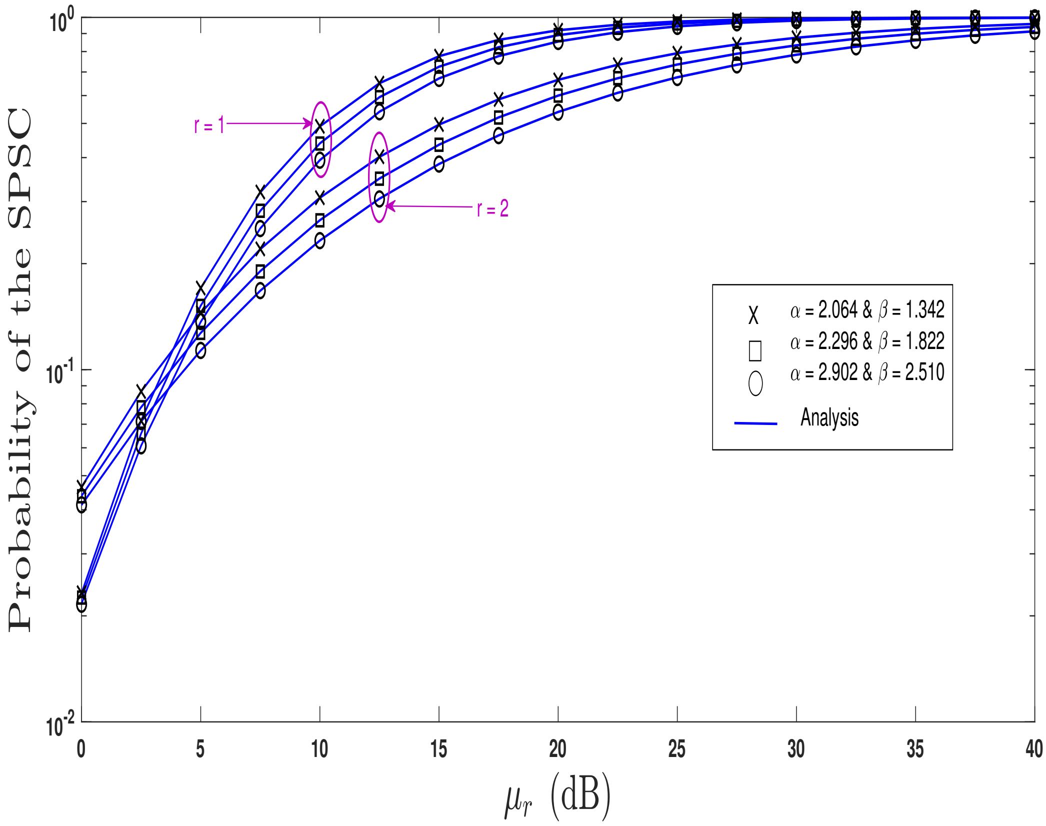

FIGURE 4.6: Probability of the SPSC vs μ_r with different values of α, β, and r, $\bar{\gamma}_E = -10$ dB, $\bar{\gamma}_R = 10$ dB, $\xi = 1$, $N_R = 4$, $N_E = 2$ and $r = 1$.

Figure 4.6 illustrates the probability of the SPSC vs μ_r considering different detection techniques. It can be observed that as μ_r increases, the probability of the SPSC also increases, indicative of an enhancement in secrecy performance. As previously highlighted, the HD ($r = 1$) exhibits superior performance compared to IM/DD ($r = 2$). This superiority is attributed to the HD's better SNR performance.

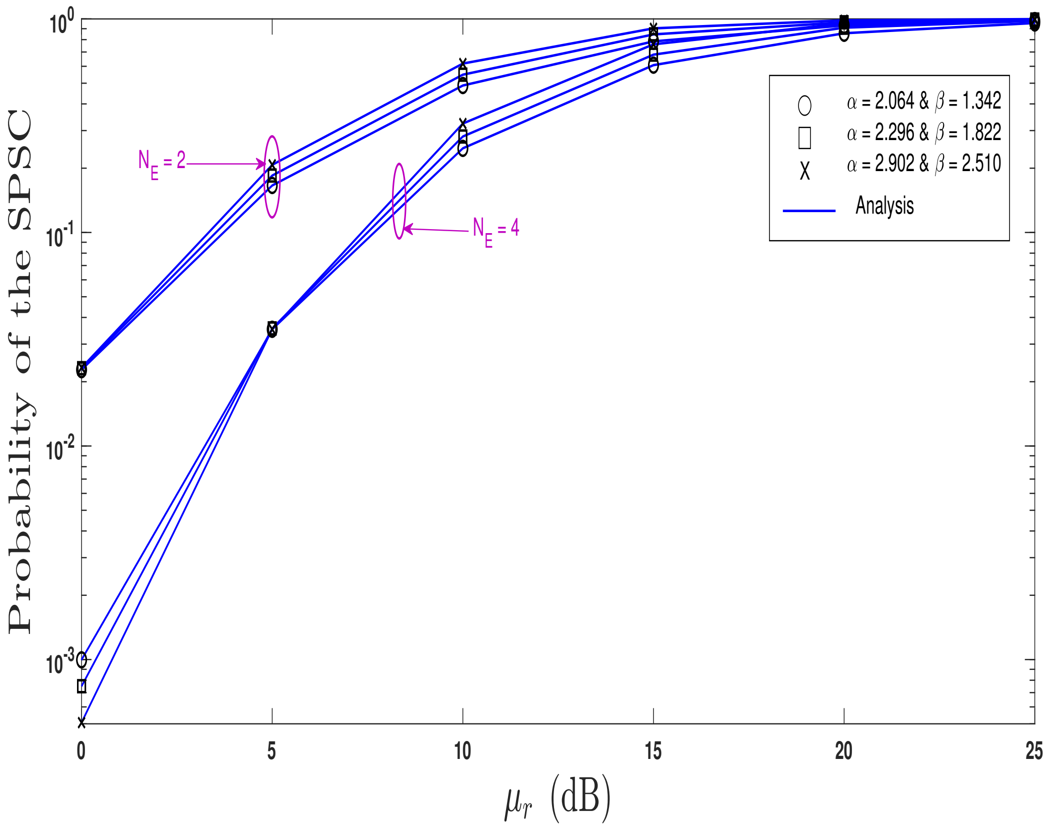

FIGURE 4.7: Probability of the SPSC vs μ_r with different N_E, $N_R = 4$, $\bar{\gamma}_E = -1$ dB, $\bar{\gamma}_R = 10$ dB, $\xi = 6.7$.

In Figure 4.7, the probability of the SPSC vs μ_r is displayed with different antenna configuration. It is noted that an augmentation in the number of antenna at the eavesdropper remarkably deteriorates the system secrecy performance. This degradation can be attributed to the increased eavesdropping capabilities resulting from its multiple antennas. Specifically, the eavesdropper can leverage its antenna diversity to maximize the likelihood of successful eavesdropping by utilizing EGC.

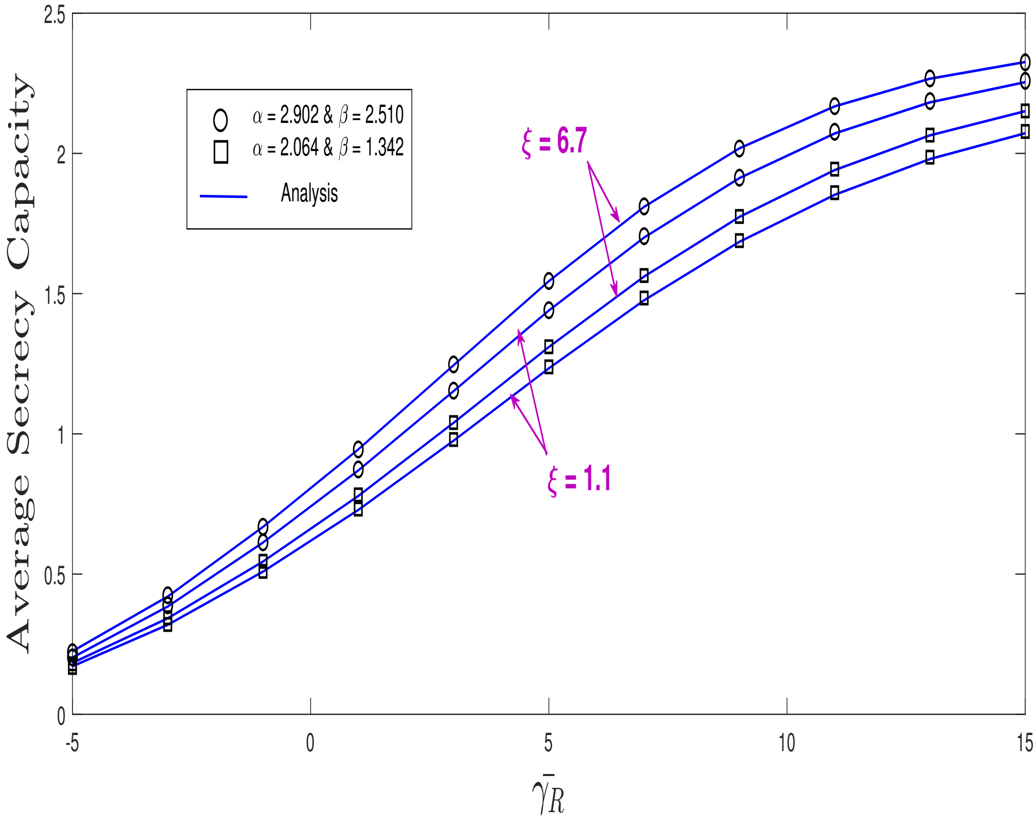

FIGURE 4.8: ASC vs $\bar{\gamma}_R$ with different $\xi = 6.7$ and turbulence conditions $N_E = 4$, $N_R = 4$, $\bar{\gamma}_E = -10$ dB, $m_R = m_E = 2$.

.

In Figure 4.8, it can be observed that an increase in pointing error levels deteriorates the ASC performance. As previously stated, the misalignment between the transmitter and receiver apertures results in unintended signal leakage and consequently reducing the ASC of the proposed system model.

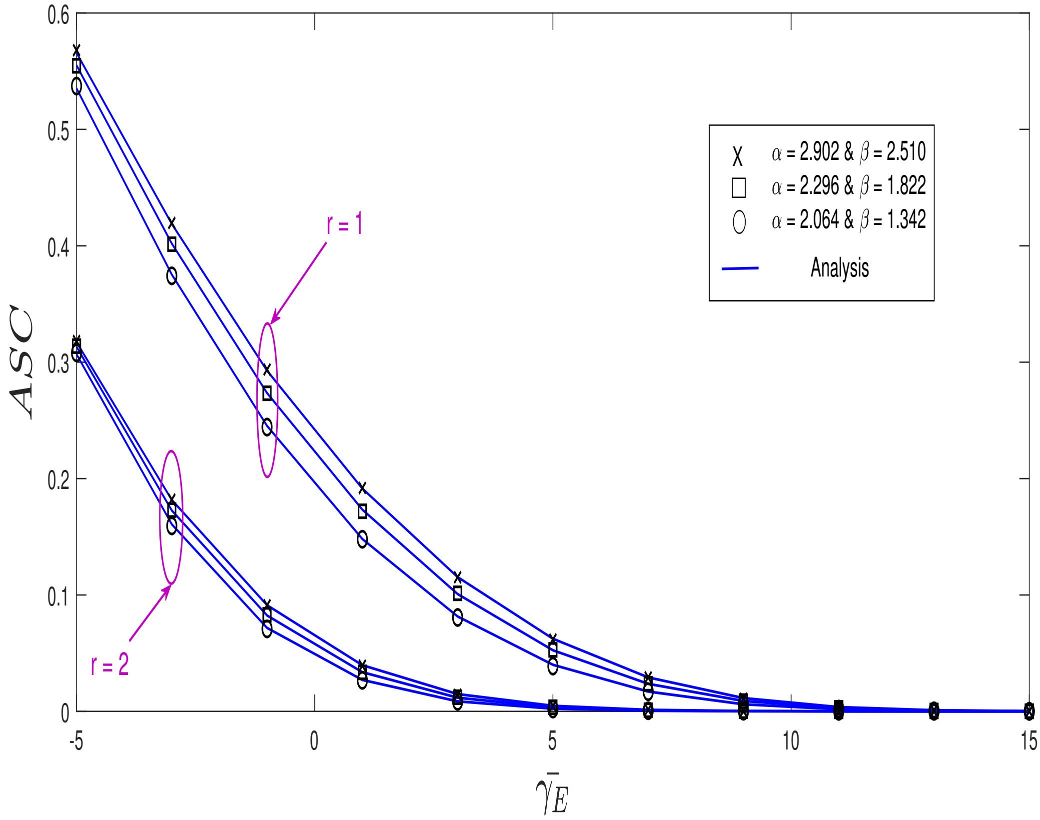

FIGURE 4.9: ASC vs $\bar{\gamma}_E$ with different r and turbulence conditions $N_E = 4$, $N_R = 4$, $\bar{\gamma}_R = 2$ dB, $m_R = m_E = 2$.

.

The ASC vs the average SNR at the eavesdropper is illustrated in Fig.4.9 with different detection techniques and turbulence conditions. First, the secrecy performance deteriorates as the average SNR at the eavesdropper increases. This is because the security is compromised when the eavesdropper's channel condition is favorable, resulting in a high probability of eavesdropping and consequently reducing the ASC. Second, it can be seen that the performance with HD performs better than its counterpart IM/DD, which corroborates with the fact that the SNR achieved with the HD technique surpasses that of the IM/DD technique.

4.7 Conclusion

In this chapter, we investigate the secrecy performance of a a two-user multi-antenna NOMA in a mixed RF-FSO system by injecting artificial noise to counter eavesdropping. The channel statistics for the underlying system were acquired and subsequently employed to formulate closed-form expressions for the lower bound of the SOP, the probability of the SPSC and the ASC. In addition, the asymptotic analysis of the SOP derived earlier is obtained using the expansion of the Meijer's G function at the high SNR regime. Numerical results demonstrate that the secrecy performance of the mixed RF-FSO system exhibits minimal sensitivity to the increase in the average SNR at the relay. This is attributed to the fact that the equivalent end-to-end SNR with variable gain relaying remains equal to the average SNR at the destination, even when the average SNR at the relay node becomes large. Moreover, the presence of AN significantly enhances the system's ability to mitigate eavesdropping, thereby improving secrecy rates across various operational scenarios. For instance, when the AN power used to confuse the eavesdropper link increases from 0.05 to 0.20 in moderated turbulence conditions, the SOP decreases from $(1 * 10^{-2})$ to $(3 * 10^{-3})$, highlighting the effectiveness of the AN in enhancing system security. Additionally, the secrecy performance in weak atmospheric turbulence conditions outperforms that of strong conditions, this is due to the fact that atmospheric turbulence primarily affects the SNR at the destination. Furthermore, the corresponding asymptotic analysis has been derived to approximate the exact SOP at high SNR. Finally, Monte Carlo simulations for various system scenarios have been conducted to corroborate the proposed analytical framework.

CHAPTER 5

On Secure Mixed RF-FSO MIMO-NOMA Systems with Colluding and Non-Colluding Eavesdroppers

5.1 Introduction

In light of the recent advancements in wireless communication systems, mixed radio frequency (RF)-free-space optical (FSO) systems stand as promising potentials that address different communication challenges. The mixed nature of these systems allows for improved reliability and performance, particularly in scenarios where one technology may face limitations [2]. Despite these advantages, the mixed RF-FSO systems are vulnerable to eavesdropping attacks due to the inherent broadcast nature of the RF transmissions. To this end, several studies have investigated the secrecy performance of mixed FSO-RF systems [3, 109, 136, 137]. For the sake of practicality, some recent studies have considered multiple eavesdroppers wherein collaborative efforts (colluding eavesdropping) and independent efforts (non-colluding eavesdropping) may render the system more susceptible to security threats [88, 138]. The performance of both non-colluding and colluding eavesdroppers is investigated in [139], with a focus on evaluating the average secrecy throughput. In this scenario, the information signal is transmitted to a multiple legitimate receivers in the presence of multiple colluding and non-colluding eavesdroppers. Their findings unveil that the influence of colluding eavesdroppers on average secrecy throughput results in more degradation of the security performance compared to a non-colluding scenario, particularly as the number of eavesdroppers increases. To get more insights, the authors in [85] have derived the exact and asymptotic closed-form expressions for the secrecy outage probability (SOP), the probability of strictly positive secrecy capacity (SPSC), and average secrecy capacity (ASC) considering both eavesdropper modes. Moreover, the impact of the fading severity of the RF links, atmospheric turbulence, misalignment, the quality of eavesdropping link, is evaluated. In addressing the aforementioned security threats, one strategic approach is to incorporate artificial noise (AN) into the transmitted signal. This technique aims to enable the intended receiver to successfully decode the information-bearing signal, while concurrently elevating the interference level experienced by potential eavesdroppers. Although the physical layer security (PLS) of mixed RF-FSO systems has recently garnered considerable interest (e.g., [3, 19, 20, 124] and the references therein), the impact of AN on such mixed systems in the presence of multiple colluding and non-colluding eavesdroppers has not been addressed. As such, the present research work focuses on data interception in mixed RF-FSO links where a multiple-input-multiple-output (MIMO)-non-orthogonal multiple access (NOMA) technology is employed. Hence, the proposed system aims to improve spectral efficiency and secrecy while providing large bandwidths and license-free spectrum through the FSO links. Motivated by the above discussion, the proposed work contributes to the current state-of-the-art in the following way.

(a) The analytical expressions of the statistical properties of the proposed system which include the probability density function (PDF) and cumulative distribution function (CDF) are obtained.

(b) Capitalizing on these statistical formulations, the analytical expressions of the SOP, the probability of the SPSC and the ASC are derived in closed form.

(c) To approximate the SOP in the high signal-to-noise ratio (SNR) regime, the corresponding asymptotic analysis is presented for both the colluding and non-colluding scenarios.

(d) Monte Carlo simulations are provided to verify the correctness of the proposed mathematical derivations.

The subsequent sections of this chapter are structured as follows. Section 5.2 presents the proposed system model, while the channel statistics are detailed in Section 5.3. In Section 5.4, the secrecy performance of the underlying system is evaluated based on SOP, probability of the SPSC, and the ASC for both colluding and non-colluding scenarios followed by the corresponding asymptotic analytical framework for SOP in Section 5.5. The discussion of the obtained results is provided in 5.6. Finally, insights and observations are encapsulated in Section 5.7.

5.2 System Model

We consider a two-user MIMO-NOMA in a mixed RF-FSO system in the presence of multiple eavesdroppers as shown in Figure 5.1. On one hand, the RF links

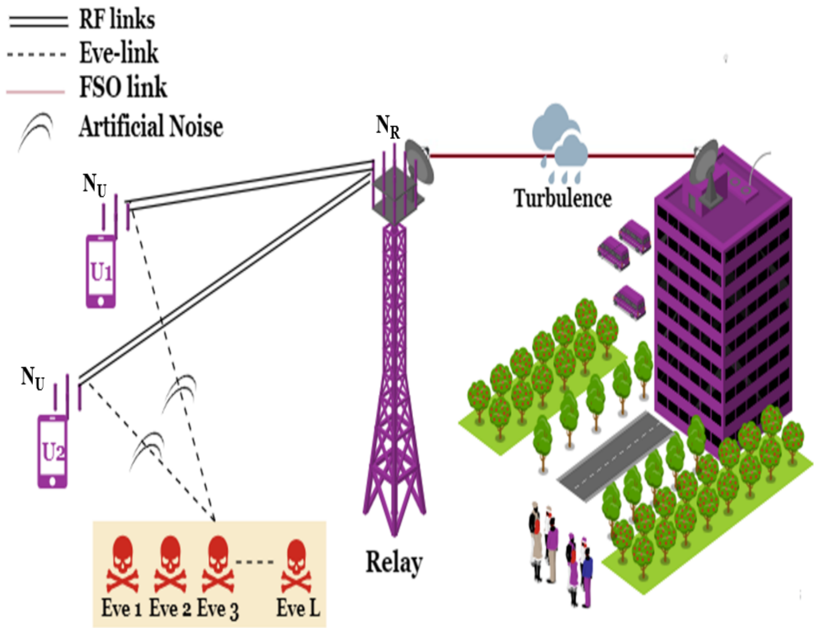

FIGURE 5.1: Uplink MIMO-NOMA in a Mixed RF-FSO system with multiple eavesdroppers.

consist of two users U_1 and U_2 each mounted with N_U antennas, an N_R-antenna amplify-and-forward (AF) relay node, and L single-antenna eavesdroppers strategically positioned to overhear the RF transmissions. In this context, a single antenna is selected at each user to transmit confidential messages in a NOMA fashion to the destination (via the relay node) with an AN signal injected to increase the interference level at the eavesdropper[1]. To this end, the transmitted signal from U_i is given as [90]

$$\mathcal{X}_{U_i} = x_{U_i} + x_{\mathrm{AN}_i}, \tag{5.1}$$

where $E\left[|\mathcal{X}_{U_i}|^2\right] = 1$ with x_{U_i} and x_{AN_i} being the information-bearing and AN signals, respectively, with $i \in \{1, 2\}$. In what follows, the received signal at the output of the combiner (equal gain combining (EGC) scheme) at the relay node

[1]It is noteworthy that the channel estimation of the legitimate link is assumed to be perfect. Hence, the AN signal is designed to lie in the null space of the legitimate link, so that the relay only receives the information-bearing signal.

can be expressed as [42]

$$y_R = \sum_{j=1}^{N_R} \left(\sum_{i=1}^{2} \left(\mathcal{X}_{U_i} h_{U_i^{(b_i^*)} R_j} \sqrt{a_i L_i P_t} \right) + n_{R_j} \right), \tag{5.2}$$

where $h_{U_i^{(b_i^*)} R_j}$ corresponds the fading coefficient of the link between the best antenna of U_i and the j-th antenna of the relay node follows the Nakagami-m distribution, P_t is the average power transmitted by U_i, a_i is the power allocated at U_i with $\sum_{i=1}^{2}(a_i + a_{\mathrm{AN}_i}) = 1$ which includes the power of the AN signal with $a_{\mathrm{AN}} = \sum_{i=1}^{2} a_{\mathrm{AN}_i}$ and $a_2 > a_1$, $n_R = \sum_{j=1}^{N_R} n_{R_j}$, and n_{R_j} modeled as a complex Gaussian random variable at the j-th antenna of the relay with mean zero and variance $\sigma_{R_j}^2$, i.e., $n_{R_j} \sim \mathcal{CN}(0, \sigma_{R_j}^2)$, L_i is the path loss gain, and the subscript b_i^* represents the best antenna of U_i selected defined as $b_i^* = \arg\max_k \sum_{j=1}^{N_R} |h_{U_i^{(k)} R_j}|^2$. On the other hand, the FSO link consists of the relay and the destination nodes. The composite signal in (5.2) is converted to an optical signal before being forwarded to the destination and further filtered out to eliminate undesirable components. Consequently, the resulting signal received at the destination can be given by

$$y_D = h_{RD} \mathcal{G} \mu y_R + n_D, \tag{5.3}$$

where $h_{RD} = h_l h_a h_p$ represents the overall FSO channel gain coefficient between the relay and the destination nodes with h_l, h_a and h_p being the overall fading impact of deterministic path loss, the atmospheric turbulence-induced fading, and the pointing errors-induced fading on the optical FSO link, respectively, and n_D is the additive white Gaussian noise (AWGN) variable at the destination with mean zero and variance σ_D^2. To this end, the instantaneous signal-to-interference-plus-noise ratio (SINR) at the destination can be obtained by substituting (5.2) into the expression of y_D and doing some mathematical manipulations, the instantaneous SINR can be obtained as

$$\gamma_2 = \frac{a_2 \gamma_D \gamma_R^{(2)}}{a_1 \gamma_D \gamma_R^{(1)} + \gamma_R^{(1)} + \gamma_D + 1}. \tag{5.4}$$

The expression in (5.4) is mathematically intractable. To address this issue, we adopt the following upper bound as $\gamma_2 \cong \min(\gamma_D, \gamma_R^{(2)})$ [19]. Subsequently, the instantaneous SNR for the weak user denoted by

$$\gamma_1 \cong \min(\gamma_D, \gamma_R^{(1)}). \tag{5.5}$$

Similar to (5.2), the signal received by k-th eavesdropper is expressed as

$$y_{E_k} = \sum_{i=1}^{2} \sqrt{a_i L_i P_t} x_{U_i} h_{U_i^{(b_i^*)} E_k} + \sum_{i=1}^{2} \sqrt{a_{\mathrm{AN}_i} L_i P_t} x_{U_i} h_{U_i^{(b_i^*)} E_k} + n_{E_k}, \quad (5.6)$$

where n_{E_k} is the AWGN variable at the k-th eavesdropper with zero mean and variance σ_E^2. It is assumed that the eavesdroppers have no knowledge of the antenna selection at the users, and thus, do not see the transmission from a best antenna viewpoint. From (5.6), the instantaneous SNRs at the k-th eavesdropper are respectively given by

$$\gamma_{E_k}^{(1)} = \frac{(X_{U_1 E_k}/\sigma_{\mathrm{AN}_1}^2)}{1 + (X_{U_2 E_k}/\sigma_{\mathrm{AN}_2}^2)}, \quad (5.7)$$

$$\gamma_{E_k}^{(2)} = \frac{(X_{U_2 E_k}/\sigma_{\mathrm{AN}_2}^2)}{1 + (X_{U_1 E_k}/\sigma_{\mathrm{AN}_1}^2)}, \quad (5.8)$$

where $\sigma_{\mathrm{AN}_i}^2$ being the variance of the AN signal, $X_{U_1 E_k}$ and $X_{U_2 E_k}$ represent the SNRs of the received signal from each user respectively expressed as

$$X_{U_1 E_k} = \frac{a_1 L_1 P_t |h_{U_1^{(b_1^*)} E}|^2}{\sigma_{E_k}^2}, \quad (5.9)$$

$$X_{U_2 E_k} = \frac{a_2 L_2 P_t |h_{U_2^{(b_2^*)} E_k}|^2}{\sigma_{E_k}^2}. \quad (5.10)$$

5.3 Channel Statistics

5.3.1 Main RF-FSO Links

It is assumed that the RF system experiences the Nakagami-m fading, while the FSO system is subjected to the gamma-gamma fading[2]. To this end, the CDF of the equivalent SNR of U_1 is given by

$$\begin{aligned} F_{\gamma_{eq_1}^{(V)}}(x) &= \mathbb{P}\left(\min\left(\gamma_R^{(1)}, \gamma_D\right) < x\right) \\ &= F_{\gamma_R}(\gamma_R) + F_{\gamma_D}(\gamma_D) - F_{\gamma_R}(\gamma_R) F_{\gamma_D}(\gamma_D), \end{aligned} \quad (5.11)$$

[2] The gamma-gamma model accurately describes the impairments introduced by atmospheric turbulence and pointing errors in the FSO link.

where $\mathbb{P}(\bullet)$ denotes the probability operator. After substituting [13, eqn. (10)] and [85, eqn. (6)] in (5.11), and performing some mathematical manipulations, we obtain

$$F_{\gamma_{eq_1}^{(V)}}(x) = 1 + \sum_{(nk)} \frac{x^k}{e^{\zeta x}} \left[1 - \Psi G_{r,a}^{a,0} \left(q_{n_1} x \middle| \begin{array}{c} C_1 \\ C_3 \end{array} \right) \right], \tag{5.12}$$

where $\sum_{(nk)} = \sum_{n=0}^{N_U} \binom{N_U}{n} (-1)^n \sum_{k=0}^{n(N_R-1)} C_{k,n}$, $C_1 = \Delta(r, \xi^2 + 1)$, $C_2 = [\Delta(r, \xi^2), \Delta(r, \alpha), \Delta(r, \beta)]$, $\Psi = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)}$, $q_{n_1} = \frac{(d\alpha\beta)^r n \lambda_R \Lambda}{\mu_r a_1 r^{2r}}$, $\lambda_R = \frac{m_R}{\bar{\gamma}_R}$, and $C_{k,n} = \sum_{p=k-N_R+1}^{k} \frac{C_{p,(n-1)}}{(k-p)!} \delta_{[0,(n-1)(N_R-1)]}(n) (C_{00} = C_{0n} = 1, C_{k,1} = 1/k!, C_{1,n} = n)$, $a = 3r + 1$ with α and β representing parameters of the atmospheric turbulence effect, and $\zeta = \frac{n\lambda_R}{a_1}$. Similarly, the CDF of the equivalent SINR linked with U_2 is given by

$$F_{\gamma_{eq_2}^{(V)}}(x) = 1 + \sum_{(nk)} x^k e^{-\frac{a_1 n \lambda_R}{a_2} x} \left[1 - \Psi G_{r,3r+1}^{3r+1,0} \left(\frac{(d\alpha\beta)^r n \lambda_R}{\mu_r a_2 r^{2r}} x \middle| \begin{array}{c} C_1 \\ C_2 \end{array} \right) \right]. \tag{5.13}$$

5.3.2 Eavesdropper RF Links

5.3.2.1 Non-Colluding Eavesdropping

In this scenario, only a single eavesdropper among the L ones is selected to overhear the RF transmissions, defined as

$$\gamma_{\mathrm{E}}^{\mathrm{nc}} = \max_{1 \le k \le L} \{\gamma_{E_k}\}. \tag{5.14}$$

To this end, the CDF and PDF of the random variable (RV) $\gamma_{\mathrm{E}}^{\mathrm{nc}}$ are given respectively by [139, Eqns. 23–24]

$$F_{\gamma_E^{\mathrm{nc}}}(\gamma_E) = \sum_{g=0}^{L-1} \binom{L}{g} (-1)^g e^{-\lambda_E g \gamma_{\mathrm{E}}^{\mathrm{nc}}} \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} (\lambda_E \gamma_{\mathrm{E}}^{\mathrm{nc}})^\tau, \tag{5.15}$$

$$f_{\gamma_E^{\mathrm{nc}}}(\gamma_{\mathrm{E}}^{\mathrm{nc}}) = \frac{L}{\Gamma(m_E)} \sum_{g=0}^{L-1} \binom{L-1}{g} (-1)^g e^{-(g+1)\lambda_E \gamma_{\mathrm{E}}^{\mathrm{nc}}} \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} \lambda_E^{m_E+\tau} (\gamma_{\mathrm{E}}^{\mathrm{nc}})^{m_E+\tau-1}, \tag{5.16}$$

where $\beta_{\tau,g} = \sum_{z=\tau-m_E+1}^{\tau} \frac{\beta_{z,(g-1)}}{(\tau-z)!}\delta_{[0,(g-1)(m_E-1)]}(g)(\beta_{00} = \beta_{0g} = 1, \beta_{\tau,1} = 1/\tau!, \beta_{1,g} = g)$.

5.3.2.2 Colluding Eavesdropping

In this scenario, all the eavesdroppers collaboratively join their effort in a central data processing, to overhear the RF transmissions, and the output SNR is given by

$$\gamma_{\mathrm{E}}^{\mathrm{c}} = \sum_{k=1}^{L} \gamma_{E_k}. \tag{5.17}$$

The corresponding CDF and PDF are respectively given by [85, Eqns. 9–10]

$$F_{\gamma_E^{\mathrm{c}}}(\gamma_E) = \frac{\Upsilon(LN_E, \lambda_E \gamma_E)}{\Gamma(LN_E)}, \tag{5.18}$$

$$f_{\gamma_E^{\mathrm{c}}}(\gamma_{\mathrm{E}}^{\mathrm{c}}) = \frac{(\lambda_E a_{\mathrm{AN}})^{m_E L}}{\Gamma(m_E L)} (\gamma_{\mathrm{E}}^{\mathrm{c}})^{m_E L - 1} e^{-a_{\mathrm{AN}} \lambda_E \gamma_{\mathrm{E}}^{\mathrm{nc}}}, \tag{5.19}$$

where $\Gamma(\bullet)$ is the Gamma function.

5.4 Secrecy Performance Analysis

5.4.1 Secrecy Outage Probability

Here, the outage event occurs when either $C_{s_{U_1}}$ or $C_{s_{U_2}}$ falls below the predefined secrecy rate R_s. This can be mathematically defined as

$$\begin{aligned} \mathcal{P}_{\mathrm{out}} &= \mathbb{P}\left(C_{s_{U_1}} \leq R_s \text{ or } C_{s_{U_2}} \leq R_s\right) \\ &= 1 - \left(1 - \mathcal{P}_{\mathrm{out}}^{(1,j)}\right)\left(1 - \mathcal{P}_{\mathrm{out}}^{(2,j)}\right), \end{aligned} \tag{5.20}$$

where $j \in \{\mathrm{nc}, \mathrm{c}\}$ with nc and c standing for *non-colluding* and *colluding*, respectively, $C_{s_{U_1}} = \log_2(1 + \gamma_{\mathrm{eq}}^{(1)}) - \log_2(1 + \gamma_E^{(1)})$, $C_{s_{U_2}} = \log_2(1 + \gamma_{\mathrm{eq}}^{(2)}) - \log_2(1 + \gamma_E^{(2)})$ and $\mathcal{P}_{\mathrm{out}}^{(i)}$ is the SOP related to U_i. However, obtaining a closed-form expression of the exact SOP is not straightforward. For this reason, we revert to the expression of the lower bound which can be given by

$$\mathcal{P}_{\mathrm{out,lb}}^{(i)} = \int_0^{\infty} F_{\gamma_{eq_i}^{(V)}}(\Theta \gamma_E) f_{\gamma_E}(\gamma_E) \mathrm{d}\gamma_E, \tag{5.21}$$

where $\Theta = e^{R_s} \geq 1$. Next, we derive the SOP expressions for both the colluding and non-colluding scenarios.

5.4.1.1 Secrecy Outage Probability of the Non-Colluding Eavesdropping

After substituting (5.12) and (5.16) into (5.21), and performing some mathematical manipulations with the help of [128, eqn. (7.813)] and [128, eqn.(3.326.2)], the lower bound of the SOP for U_1 is given by

$$\mathcal{P}_{\text{out,lb}}^{(1,\text{nc})} = 1 + \frac{a_{\text{AN}_1} L \lambda_E}{\Gamma(m_E)} \sum_{g=0}^{L-1} \begin{pmatrix} L-1 \\ g \end{pmatrix} (-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} \lambda_E^{\tau} \sum_{(nkj)} \frac{\Theta^k}{k!} \Bigg\{ \Psi \\ \times \left(\frac{n\lambda_R \Theta}{a_1} + a_{\text{AN}_1} \lambda_E \right)^{-N_E-\tau-k} G_{r+2,3r+1}^{3r,2} \left[\frac{\Theta q_{n_1}}{\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E} \Bigg|_{C_2,0}^{1,1-N_E-\tau-k,C_1} \right] \\ - \left(\frac{\Gamma(N_E+\tau+k)}{\left(\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E \right)^{N_E+\tau+k}} \right) \Bigg\}. \quad (5.22)$$

To derive the SOP for U_2, we adopt a similar approach to the one for U_1 by substituting (5.13) and (5.16) into (5.21), to obtain

$$\mathcal{P}_{\text{out,lb}}^{(2,\text{nc})} = 1 + \frac{a_{\text{AN}_2} L \lambda_E}{\Gamma(m_E)} \sum_{g=0}^{L-1} \begin{pmatrix} L-1 \\ g \end{pmatrix} (-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} \lambda_E^{\tau} \sum_{(nkj)} \frac{\Theta^k}{k!} \Bigg\{ \Psi \\ \times \left(\frac{n\lambda_R \Theta a_1}{a_2} + a_{\text{AN}_2} \lambda_E \right)^{-N_E-\tau-k} G_{r+2,3r+1}^{3r,2} \left[\frac{\Theta q_{n_1}}{\frac{n\lambda_R\Theta a_1}{a_2} + a_{\text{AN}_2}\lambda_E} \Bigg|_{C_2,0}^{1,1-N_E-\tau-k,C_1} \right] \\ - \left(\frac{\Gamma(N_E+\tau+k)}{\left(\frac{n\lambda_R\Theta a_1}{a_2} + a_{\text{AN}_2}\lambda_E \right)^{N_E+\tau+k}} \right) \Bigg\}. \quad (5.23)$$

Plugging (5.22) and (5.23) into (5.20), the lower bound of the SOP for the proposed system for the non-colluding eavesdropping can be obtained.

5.4.1.2 Secrecy Outage Probability of the Colluding Eavesdropping

The substitution of (5.12) and (5.19) into (5.21) yields the lower bound of the SOP for U_1 given by

$$\mathcal{P}_{\text{out,lb}}^{(1,\text{c})} = 1 + \frac{(a_{\text{AN}_1}\lambda_E)^{m_E L}}{\Gamma(m_E L)} \sum_{(nkj)} \frac{\Theta^k}{k!} \left\{ \Psi \left(\frac{n\lambda_R \Theta}{a_1} + a_{\text{AN}_1}\lambda_E \right)^{-m_E L - k} \right.$$
$$\left. \times\, G_{r+2,3r+1}^{3r,2} \left[\frac{\Theta q_{n_1}}{\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E} \middle|_{C_2,0}^{1,1-m_E L-k,C_1} \right] - \left(\frac{\Gamma(m_E L + k)}{\left(\frac{n\lambda_R\Theta}{a_1} + a_{\text{AN}_1}\lambda_E\right)^{m_E L + k}} \right) \right\}. \tag{5.24}$$

A similar approach can be used to obtain the lower bound of the SOP for U_2 given by

$$\mathcal{P}_{\text{out,lb}}^{(2,\text{c})} = 1 + \frac{(a_{\text{AN}_2}\lambda_E)^{m_E L}}{\Gamma(m_E L)} \sum_{(nkj)} \frac{\Theta^k}{k!} \left\{ \Psi \left(\frac{n\lambda_R \Theta a_1}{a_2} + a_{\text{AN}_2}\lambda_E \right)^{-m_E L - k} \right.$$
$$\left. \times G_{r+2,3r+1}^{3r,2} \left[\frac{\Theta q_{n_1}}{\frac{n\lambda_R\Theta a_1}{a_2} + a_{\text{AN}_2}\lambda_E} \middle|_{C_2,0}^{1,1-m_E L-k,C_1} \right] - \left(\frac{\Gamma(m_E L + k)}{\left(\frac{n\lambda_R\Theta a_1}{a_2} + a_{\text{AN}_2}\lambda_E\right)^{m_E L + k}} \right) \right\}. \tag{5.25}$$

Finally, using the derived expressions of (5.24) and (5.25) into (5.20) yields a closed-form expression of the lower bound of the SOP for the colluding eavesdropping scenario.

5.4.2 Probability of the Strictly Positive Secrecy Capacity

The probability of the SPSC indicates the probability of secure transmission. Here, it is mathematically defined as

$$\begin{aligned} \mathcal{P}_{\text{SPSC}} &= \mathbb{P}\left(C_{s_{U_1}} > R_S, C_{s_{U_2}} > R_S\right) \\ &= \left[1 - \left(\mathcal{P}_{\text{SPSC}}^{1,j}\right)\left(\mathcal{P}_{\text{SPSC}}^{2,j}\right)\right], \end{aligned} \tag{5.26}$$

where $\mathcal{P}_{\text{SPSC}}^{i,j}$ is given by

$$\mathcal{P}_{\text{SPSC}}^{(i,j)} = 1 - \int_0^\infty F_{\gamma_{eq_i}^{(V)}}(\Theta\gamma_E) f_{\gamma_E}(\gamma_E) \text{d}\gamma_E. \tag{5.27}$$

To derive the integral in (5.27), similar analysis as the one adopted in (5.21) can be employed. Therefore, the closed form expressions of $\mathcal{P}_{\text{SPSC}}$ for non-colluding and colluding eavesdropping scenario can be expressed as follows.

5.4.2.1 Probability of the Strictly Positive Secrecy Capacity for Non-Colluding Eavesdropping

From (5.27), the probability of the SPSC can be obtained by leveraging (5.22) and substituting $R_s = 0$. Thus, the analytical expression of SPSC for U_1 is given by

$$\mathcal{P}_{\text{SPSC}}^{(1,\text{nc})} = \frac{a_{\text{AN}_1} L\lambda_E}{\Gamma(m_E)} \sum_{g=0}^{L-1} \binom{L-1}{g} (-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} \lambda_E^{\tau} \sum_{(nkj)} \frac{1}{k!} \Bigg\{ \Psi \times \left(\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E \right)^{-N_E-\tau-k} G_{r+2,3r+1}^{3r,2} \left[\frac{q_{n_1}}{\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E} \middle|_{C_2,0}^{1,1-N_E-\tau-k,C_1} \right] - \left(\frac{\Gamma\left(N_E+\tau+k\right)}{\left(\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E\right)^{N_E+\tau+k}} \right) \Bigg\}. \tag{5.28}$$

To derive the probability of SPSC for U_2, we adopt a similar approach to the one used for U_1 by capitalizing on (5.23), to obtain

$$\mathcal{P}_{\text{SPSC}}^{(2,\text{nc})} = \frac{a_{\text{AN}_2} L\lambda_E}{\Gamma(m_E)} \sum_{g=0}^{L-1} \binom{L-1}{g} (-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} \lambda_E^{\tau} \sum_{(nkj)} \frac{1}{k!} \Bigg\{ \Psi \times \left(\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E \right)^{-N_E-\tau-k} G_{r+2,3r+1}^{3r,2} \left[\frac{q_{n_1}}{\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E} \middle|_{C_2,0}^{1,1-N_E-\tau-k,C_1} \right] - \left(\frac{\Gamma\left(N_E+\tau+k\right)}{\left(\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E\right)^{N_E+\tau+k}} \right) \Bigg\}. \tag{5.29}$$

By substituting (5.28) and (5.29) into (5.27), the probability of the SPSC for the non-colluding eavesdropping can be obtained.

5.4.2.2 Probability of the Strictly Positive Secrecy Capacity for the Colluding Eavesdropping

To start with, the probability of the SPSC associated with U_1 can be directly obtained by substituting $R_s = 0$ and leveraging (5.24), to derive

$$\mathcal{P}_{\text{SPSC}}^{(1,\text{c})} = \frac{(a_{\text{AN}_1}\lambda_E)^{m_E L}}{\Gamma(m_E L)} \sum_{(nkj)} \frac{1}{k!} \Bigg\{ \Psi \left(\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E \right)^{-m_E L - k} \\ \times G_{r+2,3r+1}^{3r,2} \left[\frac{q_{n_1}}{\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E} \middle|_{C_2,0}^{1,1-m_E L-k,C_1} \right] - \left(\frac{\Gamma(m_E L + k)}{\left(\frac{n\lambda_R}{a_1} + a_{\text{AN}_1}\lambda_E \right)^{m_E L + k}} \right) \Bigg\}. \tag{5.30}$$

Similarly, substituting $R_s = 0$ and utilizing (5.25) yields a closed-form expression for the probability of the SPSC associated with U_2 as

$$\mathcal{P}_{\text{SPSC}}^{(2,\text{c})} = \frac{(a_{\text{AN}_2}\lambda_E)^{m_E L}}{\Gamma(m_E L)} \sum_{(nkj)} \frac{1}{k!} \Bigg\{ \Psi \left(\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E \right)^{-m_E L - k} \\ \times G_{r+2,3r+1}^{3r,2} \left[\frac{q_{n_1}}{\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E} \middle|_{C_2,0}^{1,1-m_E L-k,C_1} \right] - \left(\frac{\Gamma(m_E L + k)}{\left(\frac{n\lambda_R a_1}{a_2} + a_{\text{AN}_2}\lambda_E \right)^{m_E L + k}} \right) \Bigg\}. \tag{5.31}$$

Substituting the derived expressions of (5.30) and (5.31) into (5.27) yields a closed-form expression of the lower bound of the SPSC for the colluding eavesdropping scenario.

5.4.3 Average Secrecy Capacity

The ASC of the underlying system can be mathematically formulated as $\mathcal{ASC}^{(j)} = \sum_{i=1}^{2} \mathcal{ASC}^{(i,j)}$ with $\mathcal{ASC}^{(i,j)}$ being given by

$$\mathcal{ASC}^{(i,j)} = \int_0^\infty \frac{F_{\gamma_E^j}(\gamma)}{1+\gamma} \left[1 - F_{\gamma_{eq_i}^{(V)}}(\gamma) \right] d\gamma, \tag{5.32}$$

where $j \in \{\text{c}, \text{nc}\}$. In what follows, we evaluate the ASC in (5.32).

5.4.3.1 Average Secrecy Capacity of the Non-Colluding Eavesdropping

The analytical expressions of the ASC associated with U_1 and U_2 can be obtained by substituting (5.12) and (5.15) in (5.32) for the former and (5.13) and (5.15) in (5.32) for the latter. Next, with the aid of $\frac{x^a}{1+x} = G_{1,1}^{1,1}\left(x\middle|_{a}^{a}\right), \exp(-bx) = G_{0,1}^{1,0}\left(bx\middle|_{0}^{-}\right)$, [128, eqn.(7.813)], [128, eqn.(3.326.2)] and [140, eqn.(2.3.6.9)], and after some mathematical manipulations, we can obtain the closed-form expression of the exact ASC for U_1 and U_2 as given respectively by

$$\begin{aligned}\mathcal{ASC}^{(1,\text{nc})} &= \sum_{(nk)} \left(\frac{n\lambda_R}{a_1}\right)^k \Bigg\{ \Bigg[G_{2,2}^{1,2}\left[\frac{n\lambda_R}{a_1}\middle|_{-,-(k+1)}^{0,-(k+1)}\right] - \frac{a_1\Psi}{n\lambda_R} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k & 1, C_1 & \frac{a_1}{n\lambda_R}, \frac{q_{nU_1}a_1}{n\lambda_R} \\ - & k & C_2, 0 & \end{array}\right] + \sum_{g=0}^{L}\binom{L}{g}(-1)^g \\ &\times \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g}(a_{\text{AN}_1}\lambda_E)^\tau \Bigg(G_{2,2}^{1,2}\left[\frac{n\lambda_R}{a_1} + g a_{\text{AN}_1}\lambda_E \middle|_{-,-(k+\tau+1)}^{0,-(k+\tau+1)}\right] - \frac{\Psi}{\frac{n\lambda_R}{a_1} + g a_{\text{AN}_1}\lambda_E} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k+\tau & 1, C_1 & \frac{1}{\frac{n\lambda_R}{a_1} + g a_{\text{AN}_1}\lambda_E}, \frac{q_{nU_1}}{\frac{n\lambda_R}{a_1} + g a_{\text{AN}_1}\lambda_E} \\ - & k+\tau & C_2, 0 & \end{array}\right]\Bigg)\Bigg]\Bigg\}, \end{aligned} \tag{5.33}$$

$$\begin{aligned}\mathcal{ASC}^{(2,\text{nc})} &= \sum_{(nk)} \left(\frac{na_1\lambda_R}{a_2}\right)^k \Bigg\{ \Bigg[G_{2,2}^{1,2}\left[\frac{na_1\lambda_R}{a_2}\middle|_{-,-(k+1)}^{0,-(k+1)}\right] - \frac{a_2\Psi}{na_1\lambda_R} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k & 1, C_1 & \frac{a_2}{na_1\lambda_R}, \frac{q_{nU_1}a_2}{na_1\lambda_R} \\ - & k & C_2, 0 & \end{array}\right] + \sum_{g=0}^{L}\binom{L}{g}(-1)^g \\ &\times \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g}(a_{\text{AN}_2}\lambda_E)^\tau \Bigg(G_{2,2}^{1,2}\left[\frac{na_1\lambda_R}{a_2} + g a_{\text{AN}_2}\lambda_E \middle|_{-,-(k+\tau+1)}^{0,-(k+\tau+1)}\right] - \frac{\Psi}{\frac{na_1\lambda_R}{a_2} + g a_{\text{AN}_2}\lambda_E} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{array}{c|c|c|c} 1 & k+\tau & 1, C_1 & \frac{1}{\frac{na_1\lambda_R}{a_2} + g a_{\text{AN}_2}\lambda_E}, \frac{q_{nU_1}}{\frac{na_1\lambda_R}{a_2} + g a_{\text{AN}_2}\lambda_E} \\ - & k+\tau & C_2, 0 & \end{array}\right]\Bigg)\Bigg]\Bigg\}, \end{aligned} \tag{5.34}$$

where $G_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}\left[\begin{array}{c|c|c|c} a_{m_1}, b_{n_1} & c_{m_2}, c_{p_2} & e_{m_3}, e_{p_3} & \frac{x}{z}, \frac{y}{z} \\ a_{p_1}, b_{q_1} & d_{n_2}, d_{q_2} & f_{n_3}, f_{q_3} & \end{array}\right]$ is the extended generalized bivariate Meijer's G-function [19]. The derived expressions in (5.33) and (5.34) can then be plugged into the equation of the ASC preceding (5.32) to yield the analytical expression of the ASC for the non-colluding eavesdropping case.

5.4.3.2 Average Secrecy Capacity of the Colluding Eavesdropping

Using the same approach adopted in the case of the non-colluding eavesdropping scenario, we can obtain the analytical expressions of the ASC associated with U_1 and U_2. After plugging respectively (5.12) and (5.18) in (5.32), and (5.13) and (5.18) in (5.32) and performing some mathematical manipulations, we obtain

$$\begin{aligned}\mathcal{ASC}^{(1,\mathrm{c})} &= \sum_{(nk)} \left(\frac{n\lambda_R}{a_1}\right)^k \Bigg\{ \Bigg[G_{2,2}^{1,2}\left[\frac{n\lambda_R}{a_1}\middle|\begin{matrix}0,-(k+1)\\ -,-(k+1)\end{matrix}\right] - \frac{a_1\Psi}{n\lambda_R} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix}1\\ -\end{matrix}\middle|\begin{matrix}k\\ k\end{matrix}\middle|\begin{matrix}1,C_1\\ C_2,0\end{matrix}\middle|\frac{a_1}{n\lambda_R},\frac{q_{nU_1}a_1}{n\lambda_R}\right] + \sum_{g=0}^{L-1}\binom{L-1}{g}(-1)^g\frac{(a_{\mathrm{AN}_1}\lambda_E)^g}{g!} \\ &\times \Bigg(G_{2,2}^{1,2}\left[\frac{n\lambda_R}{a_1}+a_{\mathrm{AN}_1}\lambda_E\middle|\begin{matrix}0,-(k+g+1)\\ -,-(k+g+1)\end{matrix}\right] - \frac{\Psi}{\frac{n\lambda_R}{a_1}+a_{\mathrm{AN}_1}\lambda_E} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix}1\\ -\end{matrix}\middle|\begin{matrix}k+g\\ k+g\end{matrix}\middle|\begin{matrix}1,C_1\\ C_2,0\end{matrix}\middle|\frac{1}{\frac{n\lambda_R}{a_1}+a_{\mathrm{AN}_1}\lambda_E},\frac{q_{nU_1}}{\frac{n\lambda_R}{a_1}+a_{\mathrm{AN}_1}\lambda_E}\right]\Bigg)\Bigg]\Bigg\}, \end{aligned} \tag{5.35}$$

$$\begin{aligned}\mathcal{ASC}^{(2,\mathrm{c})} &= \sum_{(nk)} \left(\frac{na_1\lambda_R}{a_2}\right)^k \Bigg\{ \Bigg[G_{2,2}^{1,2}\left[\frac{na_1\lambda_R}{a_2}\middle|\begin{matrix}0,-(k+1)\\ -,-(k+1)\end{matrix}\right] - \frac{a_2\Psi}{na_1\lambda_R} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix}1\\ -\end{matrix}\middle|\begin{matrix}k\\ k\end{matrix}\middle|\begin{matrix}1,C_1\\ C_2,0\end{matrix}\middle|\frac{a_2}{na_1\lambda_R},\frac{q_{nU_1}a_2}{na_1\lambda_R}\right] + \sum_{g=0}^{L-1}\binom{L-1}{g}(-1)^g\frac{(a_{\mathrm{AN}_2}\lambda_E)^g}{g!} \\ &\times \Bigg(G_{2,2}^{1,2}\left[\frac{na_1\lambda_R}{a_2}+a_{\mathrm{AN}_2}\lambda_E\middle|\begin{matrix}0,-(k+g+1)\\ -,-(k+g+1)\end{matrix}\right] - \frac{\Psi}{\frac{na_1\lambda_R}{a_2}+a_{\mathrm{AN}_2}\lambda_E} \\ &\times G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix}1\\ -\end{matrix}\middle|\begin{matrix}k+g\\ k+g\end{matrix}\middle|\begin{matrix}1,C_1\\ C_2,0\end{matrix}\middle|\frac{1}{\frac{na_1\lambda_R}{a_2}+a_{\mathrm{AN}_2}\lambda_E},\frac{q_{nU_1}}{\frac{na_1\lambda_R}{a_2}+a_{\mathrm{AN}_2}\lambda_E}\right]\Bigg)\Bigg]\Bigg\}. \end{aligned} \tag{5.36}$$

Both (5.35) and (5.36) can be substituted in the equation preceding (5.32) to yield the ASC for the colluding eavesdropping scenario.

5.5 Asymptotic SOP Analysis

In this section, we provide the asymptotic analysis of the SOP at high SNR values. First, we obtain the CDF of the equivalent SINR to U_1. As $\mu_r \to \infty$, (5.12) can be approximated as

$$F^{\infty}_{\gamma^{(1)}_{\text{eq}}}(x) = 1 + \sum_{(nk)} x^k e^{-\frac{n\lambda_R}{a_1}x}\left(1 - \Psi \sum_{i=1}^{3r} \varphi_i x^{C_{2,i}}\right), \tag{5.37}$$

where

$$\varphi_i = \left(\frac{(d\alpha\beta)^r n\lambda_R}{a_1\mu_r r^{2r}}\right)^{C_{2,i}} \frac{\prod_{l=1,l\neq i}^{3r}\Gamma\left(C_{2,l} - C_{2,i}\right)}{C_{2,i}\prod_{m=1}^{r}\Gamma\left(C_{1,m} - C_{2,i}\right)}.$$

The expression in (5.37) can be represented via the dominant term ($min(\xi, \alpha, \beta)$) where ξ stands for the 1-st term in $C_{2,i}$, α represents the $(r+1)$-th term and β represents $(2r+1)$-th term, respectively. To obtain the CDF of the equivalent SINR for U_2, we utilize the same approach used to obtain (5.37).

5.5.1 Non-Colluding Eavesdropping Case

After substituting (5.37) and (5.16) into (5.21) and performing some mathematical manipulations with the help of [128, eqn.3.326.2], the approximate of the SOP for U_1 at high SNR can be obtained as

$$\mathcal{P}^{\infty(1,\text{nc})}_{\text{out,lb}} \approx 1 - \frac{a_{\text{AN}_1} L\lambda_E}{\Gamma(m_E)} \sum_{g=0}^{L-1}\binom{L-1}{g}(-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} M_1^{-Q_\tau}\lambda_E^{\tau} \sum_{(nk)}\left(\frac{\lambda_R\Theta}{a_1}\right)^k \times\left[\Psi\sum_{i=1}^{3r}\frac{\varphi_i\Theta^{C_{2,i}}\Gamma\left(Q_i\right)}{M_1^{Q_i}} + \left(\frac{\Gamma\left(Q_\tau\right)}{M_1^{Q_\tau}}\right)\right], \tag{5.38}$$

where $Q_i = C_{2,i}+k+m_E$, $M_1 = \left(\frac{n\lambda_R\Theta}{a_1} + (g+1)a_{\text{AN}_1}\lambda_E\right)$ and $Q_\tau = m_E+k$. Using a similar approach to get (5.38), the asymptotic SOP for U_2 can be obtained as

$$\mathcal{P}^{\infty(2,\text{nc})}_{\text{out,lb}} \approx 1 - \frac{a_{\text{AN}_2} L\lambda_E}{\Gamma(m_E)} \sum_{g=0}^{L-1}\binom{L-1}{g}(-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} M_2^{-Q_\tau}\lambda_E^{\tau} \sum_{(nk)}\left(\frac{\lambda_R\Theta a_1}{a_2}\right)^k \times\left[\Psi\sum_{i=1}^{3r}\frac{\varphi_i\Theta^{C_{2,i}}\Gamma\left(Q_i\right)}{M_2^{Q_i}} + \left(\frac{\Gamma\left(Q_\tau\right)}{M_2^{Q_\tau}}\right)\right], \tag{5.39}$$

with $M_2 = \left(\frac{n\lambda_R\Theta a_1}{a_2} + (g+1)a_{\mathrm{AN}_2}\lambda_E\right)$. After plugging (5.38) and (5.39) into (5.20), the asymptotic SOP for the non-colluding yields

$$\mathcal{P}^{\infty(\mathrm{nc})}_{\mathrm{out,lb}} \approx 1 - \frac{a_{\mathrm{AN}}L^2\lambda_E^2}{\Gamma(m_E)^2}\left\{\sum_{g=0}^{L-1}\binom{L-1}{g}(-1)^g \sum_{\tau=0}^{g(m_E-1)} \beta_{\tau,g} M_1^{-Q_\tau}\lambda_E^{\tau}\sum_{(nk)}\left(\frac{\lambda_R\Theta}{a_1}\right)^k \right.$$
$$\times\left[\Psi\sum_{i=1}^{3r}\frac{\varphi_i\Theta^{C_{2,i}}\Gamma(Q_i)}{M_1^{Q_i}} + \left(\frac{\Gamma(Q_\tau)}{M_1^{Q_\tau}}\right)\right]\Bigg\}\Bigg\{\sum_{g=0}^{L-1}\binom{L-1}{g}(-1)^g$$
$$\left.\times\sum_{\tau=0}^{g(m_E-1)}\beta_{\tau,g}M_2^{-Q_\tau}\lambda_E^{\tau}\sum_{(nk)}\left(\frac{\lambda_R\Theta a_1}{a_2}\right)^k\left[\Psi\sum_{i=1}^{3r}\frac{\varphi_i\Theta^{C_{2,i}}\Gamma(Q_i)}{M_2^{Q_i}} + \left(\frac{\Gamma(Q_\tau)}{M_2^{Q_\tau}}\right)\right]\right\}. \tag{5.40}$$

5.5.2 Colluding Eavesdropping Case

After substituting (5.37) and (5.19) into (5.21), the asymptotic SOP for U_1 is given by

$$\mathcal{P}^{\infty(1,\mathrm{c})}_{\mathrm{out,lb}} \approx 1 - \frac{(a_{\mathrm{AN}_1}\lambda_E)^{m_E L}}{\Gamma(m_E L)}\sum_{(nk)}\left(\frac{\lambda_R\Theta}{a_1}\right)^k\left[\Psi\sum_{i=1}^{3r}\frac{\varphi_i\Theta^{C_{2,i}}\Gamma(Q_i)}{\kappa_1^{Q_i}} + \left(\frac{\Gamma(\omega)}{\kappa_1^{\omega}}\right)\right], \tag{5.41}$$

where $\omega = m_E L + k$. A similar approach can be used to obtain the lower bound of the asymptotic SOP for U_2 given by

$$\mathcal{P}^{\infty(2,\mathrm{c})}_{\mathrm{out,lb}} \approx 1 - \frac{(a_{\mathrm{AN}_2}\lambda_E)^{m_E L}}{\Gamma(m_E L)}\sum_{(nk)}\left(\frac{a_1\lambda_R\Theta}{a_2}\right)^k\left[\Psi\sum_{i=1}^{3r}\frac{\varphi_i\Theta^{C_{2,i}}\Gamma(Q_i)}{\kappa_2^{Q_i}} + \left(\frac{\Gamma(\omega)}{\kappa_2^{\omega}}\right)\right]. \tag{5.42}$$

After plugging (5.41) and (5.42) into (5.20) yields the asymptotic SOP for the colluding eavesdropping case.

5.6 Numerical Results

In this section, representative numerical results are presented. Without loss of generality, we use the following parameters: $a_{\mathrm{AN}} = a_{\mathrm{AN}_i}$, $R_s = 0.01$ bits/s/Hz and the various levels of atmospheric turbulence strength categorized as (a) weak: α=2.902 and β= 2.510; (b) moderate: α=2.296 and β= 1.822; (c) strong: α=2.064 and β=1.342. It can be seen from all the set of results that both the analytical and simulated results are in good agreement, which validates the correctness of the proposed mathematical framework. In Figure 5.2, the asymptotic SOP expressions

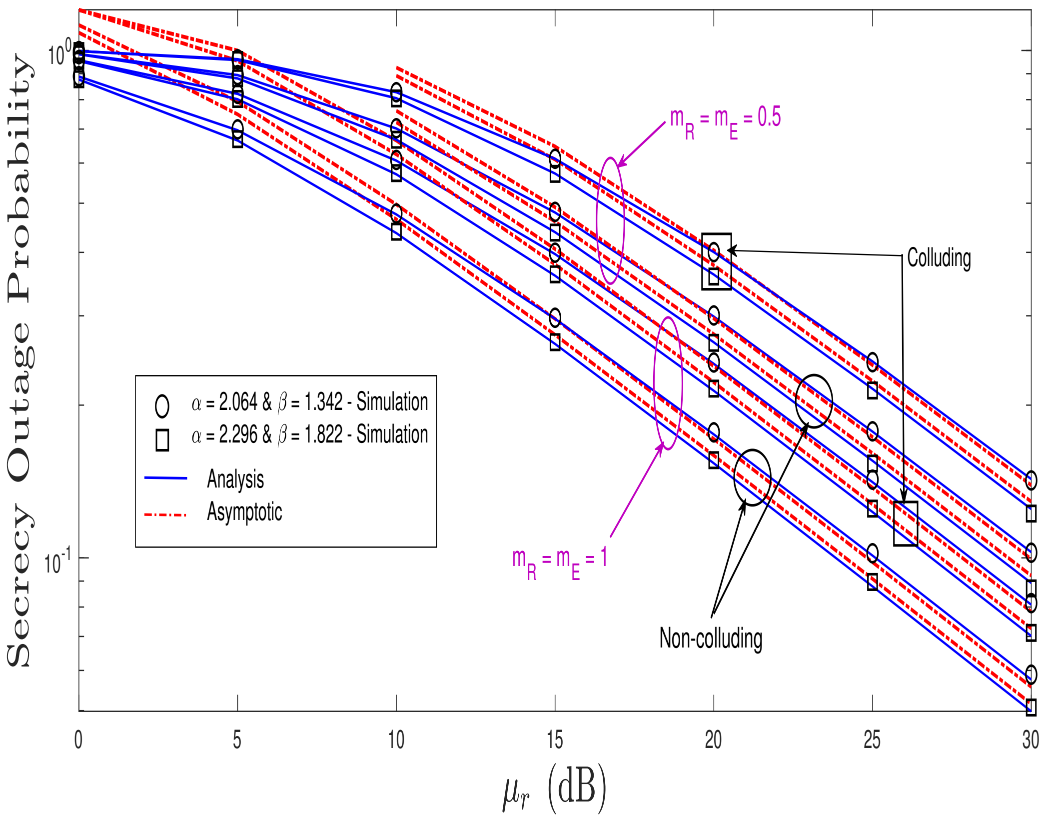

FIGURE 5.2: SOP vs μ_r with N_U= 2, N_R=4, L=4, ξ=0.5, r=1, $\bar{\gamma}_R$=10 dB, $\bar{\gamma}_E$=-10 dB, a_1=0.25, a_2=0.60, and a_{AN}=0.15.

are plotted and compared with both the exact and simulated SOP for scenarios involving both colluding and non-colluding eavesdroppers. It can be observed that the overall secrecy performance degrades as the atmospheric turbulence increases from weak to strong. This is due to the fact that strong turbulence conditions induce severe fluctuations leading to an increase in the signal attenuation. Furthermore, the secrecy performance deteriorates even further under the colluding eavesdropping mode compared to the non-colluding one, as the eavesdroppers' collaboration in the colluding mode enhances their ability to extract meaningful information from the transmitted signal. In the context of Nakagami-m fading, ($m_R = m_E = 0.5$) represents severe fading, where the main RF channels experience significant signal degradation and deep fades, potentially degrading secrecy performance. Conversely, ($m_R = m_E = 1$) indicates moderate fading, also modeled by Rayleigh fading, with less severe signal fluctuations. This results in a more stable signal for the main RF channels, thereby improving overall secrecy performance due to a more reliable connection.

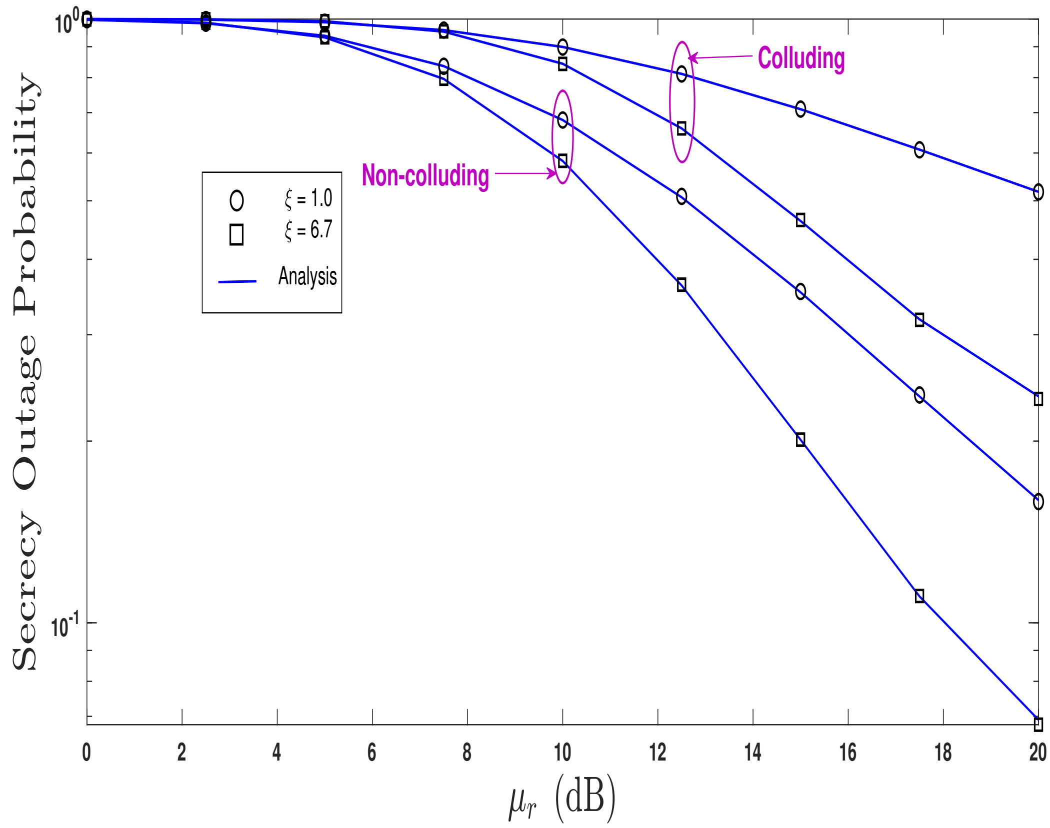

FIGURE 5.3: SOP vs μ_r with different ξ levels, $N_U = N_R = 2$, $L = 4$, $R_s = 0.01$, $\alpha = 2.902$, $\beta = 2.510$, $r = 1$, $\bar{\gamma}_R = 10$ $\bar{\gamma}_E =$ -10, $a_1 = 0.30$, $a_2 = 0.60$ and $a_{\text{AN}} = 0.10$.

In Figure 5.3, the lower bound of SOP vs μ_r is plotted for two levels of ξ. It can be seen that the SOP performance exhibits variations with different levels of ξ; In the low-level pointing error (large ξ), an improved secrecy performance is attainable in contract to a high-level pointing error. This is because low-level pointing errors correspond to better alignment between the transmitter and receiver apertures in the FSO link. This alignment ensures that the transmitted signal is accurately directed towards the intended receiver, resulting in improved reception quality and higher secrecy performance.

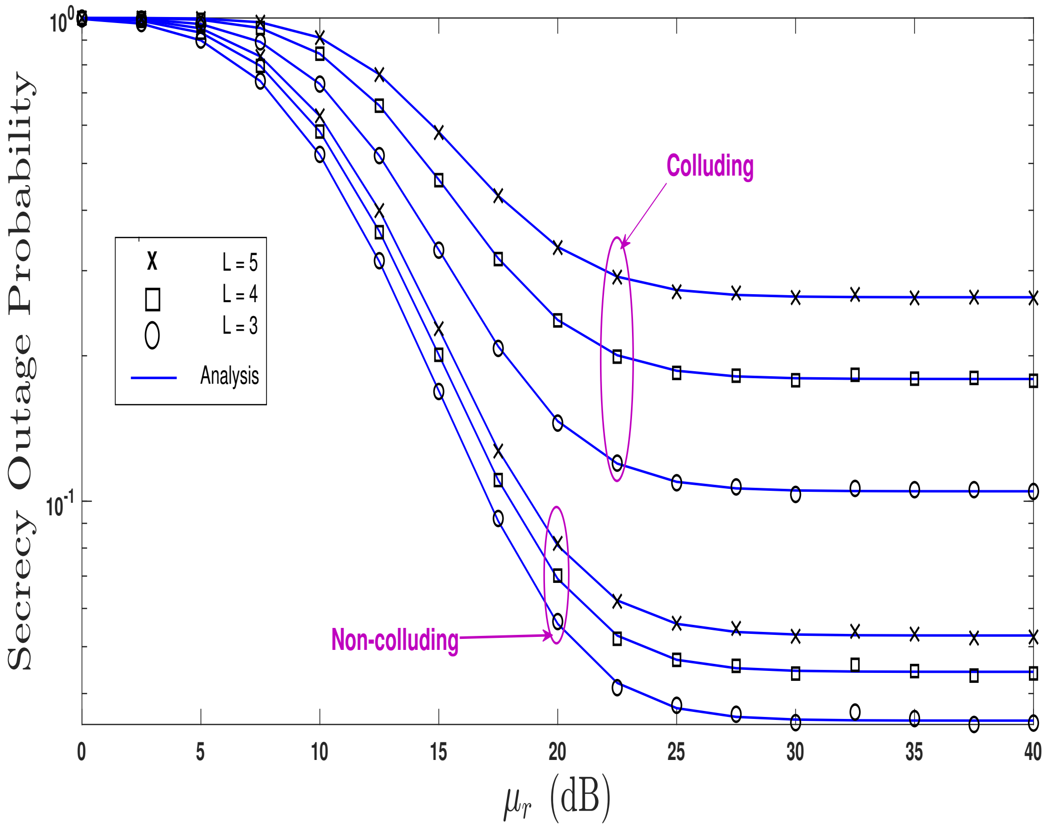

FIGURE 5.4: SOP vs μ_r with different L, $N_U = N_R = 2$, $R_s = 0.01$, $\alpha = 2.902$, $\beta = 2.510$, $r = 1$, $\bar{\gamma}_R = 10$ dB, $\bar{\gamma}_E =$ -10 dB, $a_1 = 0.30$, $a_2 = 0.60$ and $a_{\text{AN}} = 0.10$, $\xi = 6.7$.

The secrecy performance against μ_r is depicted in Figure 5.4 considering different numbers of the eavesdropper in both colluding and non-colluding scenarios. Initially, as μ_r increases, the system's secrecy performance improves due to enhanced signal decoding by the destination. However, as μ_r continues to rise, this improvement degrades and eventually saturates, this is because the destination's decoding capability reaches its maximum, and further SNR increases do not significantly enhance secrecy performance. Moreover, It is clear that the system's secrecy performance experiences a significant decline with an increase in the number of eavesdroppers. This decline can be attributed to the increased likelihood of eavesdropping attacks as more eavesdroppers are present, posing more opportunities for unauthorized threat to compromise the security of the proposed system model. Moreover, the deterioration in secrecy performance in colluding scenarios is notably significant due to the collaborative efforts of multiple eavesdroppers to intercept the transmitted information. This collaborative effort enables them to maximize the SNR of the received signal and thereby increase the probability of successful eavesdropping.

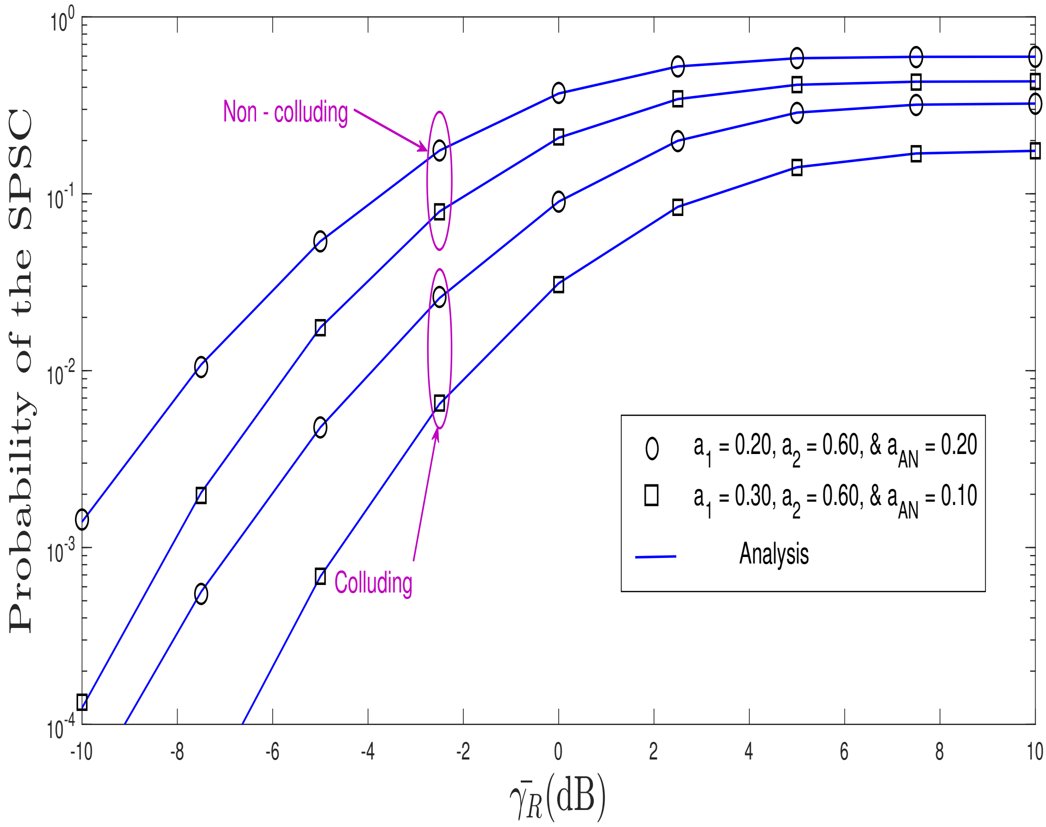

FIGURE 5.5: SPSC vs $\bar{\gamma}_R$ with different power allocation factors, $N_U = 2$, $N_R = 4$, $R_s = 0.01$, $\alpha = 2.902$, $\beta = 2.510$, $L = 4$, $\mu_r = 10$ dB, $\bar{\gamma}_E =$ -10, and $\xi =$ 6.7.

In Figure 5.5, the impact of the interference caused by the AN signal on the eavesdropping modes is investigated. It can be seen that the system performs better when more AN power is received at the Eve-link as illustrated in Figure 5.1. This emphasizes the fact that the more interfering signal by AN, the more noise at the Eve-link; which yields to degrade the quality of the Eve-link and therefore mitigates the ability of the eavesdroppers to attack the legitimate RF links.

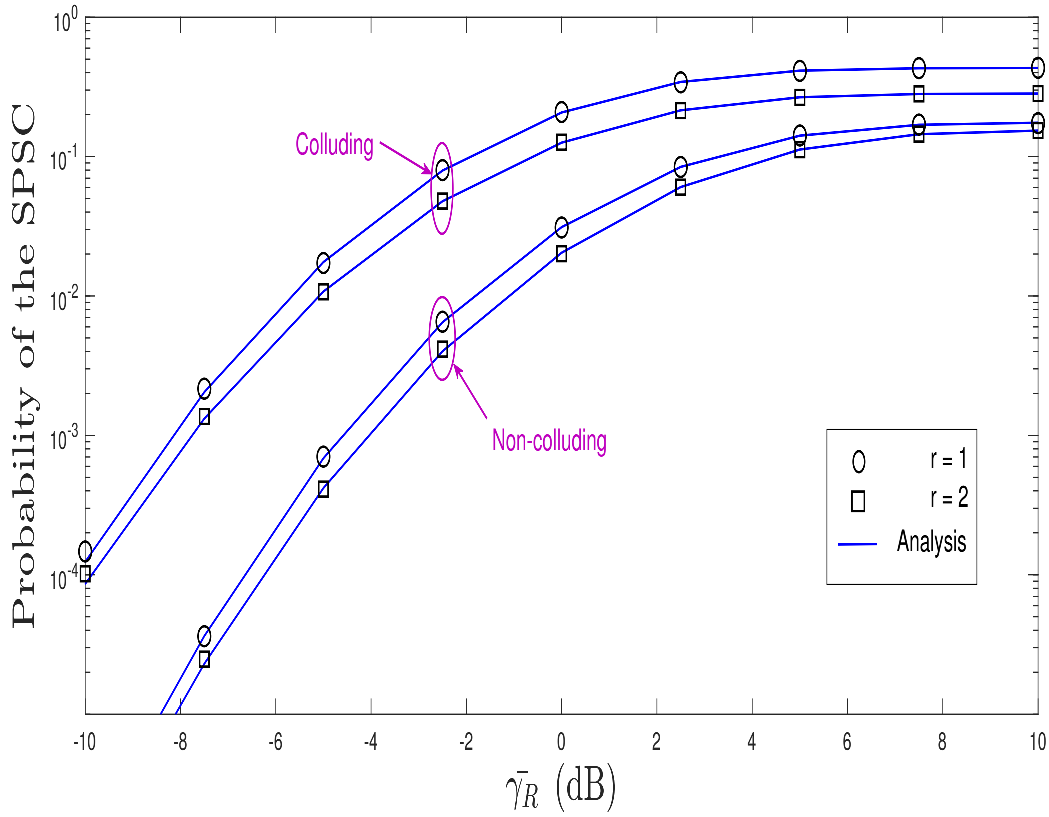

FIGURE 5.6: SPSC vs $\bar{\gamma}_R$ with different r, $N_U = 2$, $N_R = 4$, $R_s = 0.01$, $\alpha = 2.902$, $\beta = 2.510$, $L = 4$, $\mu_r = 10$ $\bar{\gamma}_E$ = -10, $a_1 = 0.30$, $a_2 = 0.60$ and $a_{\text{AN}} = 0.10$, $\xi = 6.7$.
.

In Figure 5.6, the probability of the SPSC vs $\bar{\gamma}_R$ is represented with various system parameters. It is evident that with the increase of $\bar{\gamma}_R$ (within the low SNR regime), the likelihood of the SPSC also rises, indicating an enhancement in the secrecy performance. As expected, the heterodyne detection (HD) ($r = 1$) outperforms the intensity–modulation direct detection (IM/DD) ($r = 2$). This can be explained by the fact that the HD offers better performance in terms of sensitivity and noise rejection compared to IM/DD. However, this comes at the cost of increased complexity due to the additional components and synchronization requirements.

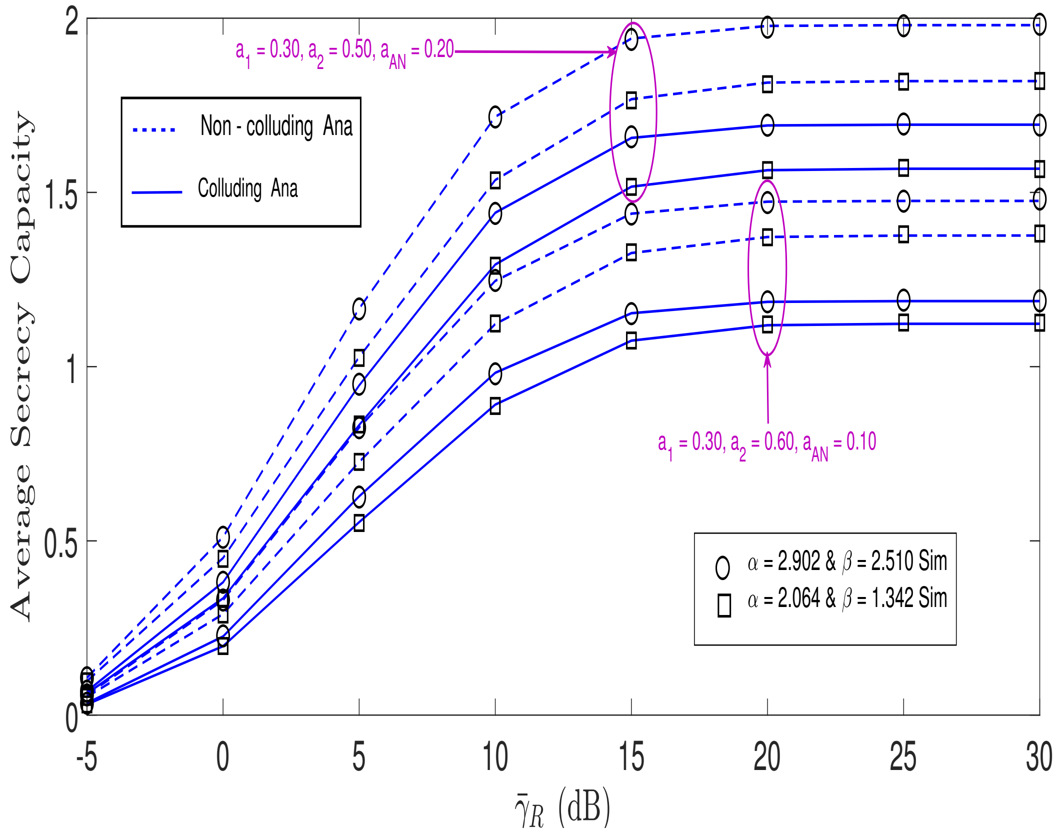

FIGURE 5.7: ASC vs $\bar{\gamma}_R$ for various values of a_{AN} with N_U=2, N_R=2, L=2, $\mu_r = 10$ dB, $\bar{\gamma}_E = -5$ dB, ξ=1.1, $m_R = m_E = 2$.

Figure 5.7 shows the ASC performance under various atmospheric conditions and AN power levels. It can be observed that the best ASC performance is achieved in weak turbulence scenarios for both eavesdropping cases. Moreover, an increase in the AN power level yields a better security performance. This is due to the degradation of the Eve-link by the injection of the AN to confound the malicious nodes.

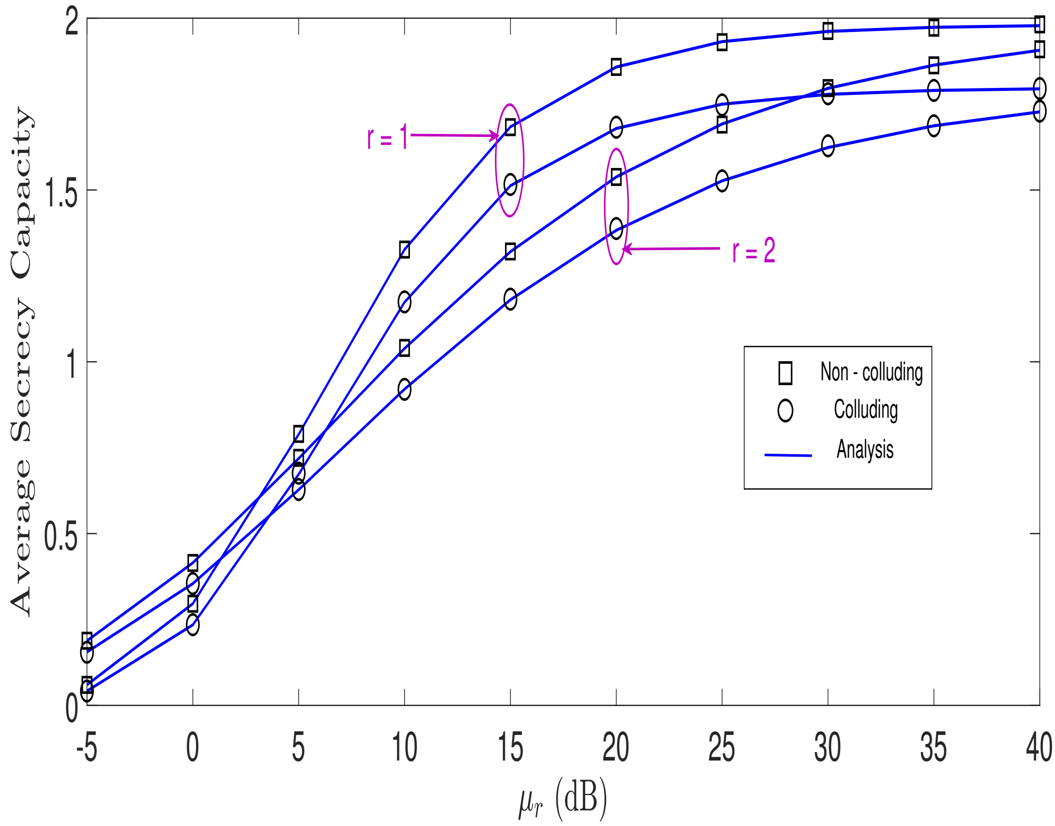

FIGURE 5.8: ASC vs μ_r with different r, $N_U = 2$, $N_R = 2$, $L = 2$, $\bar{\gamma}_R = 2$ dB, $\bar{\gamma}_E =$ -10 dB, $\alpha = 2.902$, $\beta = 2.510$, $a_1 = 0.30$, $a_2 = 0.50$, $a_{\text{AN}} = 0.20$, $\xi = 0.8$.
.

Figure 5.8 depicts the secrecy performance, as represented by the ASC, in both colluding and non-colluding eavesdropping scenarios. It is evident that the secrecy performance is superior under the HD compared to IM/DD. This observation is consistently supported throughout this thesis, as the HD technique consistently demonstrates better performance in terms of SNR due to its reduced susceptibility to signal attenuation and distortion caused by atmospheric turbulence. This attribute further contributes to the superior performance of HD systems compared to IM/DD systems.

5.7 Conclusions

In this chapter, we investigate PLS of two MIMO-NOMA aided by AN in a mixed RF-FSO system. To analyze the system secrecy performance, we consider colluding and non-colluding eavesdropping scenarios. The corresponding asymptotic analysis has been derived to approximate the exact SOP at high SNR. The channel statistics for the underlying system were obtained for each eavesdropping scenario in closed forms. Utilizing these forms, closed-form expressions for the lower bound of the SOP, the probability of the SPSC and the ASC are obtained and verified by Monte Carlo simulation. Numerical results illustrated the presence of colluding eavesdroppers significantly influences the system's secrecy performance, particularly when compared to non-colluding eavesdroppers. Nevertheless, an increase in the number of eavesdroppers, under both eavesdropping modes, markedly degrades the system's secrecy performance. For instance, increasing the probability that at least one eavesdropper will successfully intercept transmissions and compromise communication confidentiality.

CHAPTER 6

Conclusion and Future Work

6.1 Conclusion

This chapter provides a comprehensive overview of the key findings and remarks derived from the work presented in this thesis. Additionally, it outlines potential avenues for further investigation and suggests directions for future research. Specifically, the main motivation and novel contributions to the work presented in this thesis have been outlined in Chapter 1. In Chapter 2, the fundamental thesis concepts are initially introduced, followed by relevant studies in the existing literature. Subsequently, Chapter 3 investigates the PLS of the uplink MIMO-NOMA over the mixed RF and FSO spectrum bands with a fixed gain relaying scheme. Furthermore, TAS is adopted at each user to reduce the complexity associated with the number of the RF chains. The numerical findings have shown significant effects of pointing errors and atmospheric turbulence on secrecy performance. For instance, When the signal-to-noise ratio (SNR) is 20 dB in strong turbulence conditions, a higher pointing error angle (i.e., $\xi = 0.8$) can reduce the achievable secrecy performance by up to approximately 50%.

In Chapter 4, we investigated the establishment of secure communication through the utilization of AN signal as a countermeasure against eavesdropping while considering variable gain relaying scheme. Numerical results have shown that the secrecy performance exhibits minimal sensitivity to increases in the average SNR at the relay. This is because the end-to-end SNR with variable gain relaying remains equal to the average SNR at the destination, even when the SNR at the relay node is high. In addition, the HD technique exhibits superior secrecy performance compared to the IM/DD technique under typical channel conditions. Furthermore, as artificial noise (AN) power used to confuse the eavesdropper link increases from 0.05 to 0.20 in moderated turbulence conditions, the secrecy outage probability (SOP) decreases from $(1 * 10^{-2})$ to $(3 * 10^{-3})$, highlighting the effectiveness of the AN in enhancing system security. Chapter 5 provides a comprehensive analysis of

the proposed system model considering multiple colluding and non-colluding eavesdropping scenarios. The numerical results depicted a substantial impact on the system's secrecy performance when colluding eavesdroppers are present, compared to non-colluding eavesdroppers. Moreover, the system's secrecy performance experiences a pronounced degradation with an increase in the number of eavesdroppers, observed under both colluding and non-colluding eavesdropping scenarios. This increase elevates the probability that at least one eavesdropper will successfully intercept transmission, thereby compromising communication confidentiality.
To analyze the secrecy performance related to each assumption in this thesis, we obtained the statistical properties of the proposed system consisting of the PDF and CDF. Utilizing these obtained expressions, analytical expressions of the SOP, the probability of SPSC, and the ASC are derived in closed forms. Moreover, the asymptotic analysis is presented utilizing the basic elementary of the of Meijer's G-function. Finally, Monte Carlo simulations are provided to verify the accuracy of the proposed analytical framework.

6.2 Future Work

Building on the insights gained from the current investigation, several directions for future research are highlighted in the following:

- **Downlink Transmission Investigation with Non-Trustful NOMA Users:** This study can be Extended to explore the downlink transmission. Particularly, applying MIMO-NOMA on the FSO link. In this case, scenarios where NOMA users in the FSO link may not be trustworthy to each other will be considered. This introduces an additional layer of complexity, addressing the security challenges that arise when users within the NOMA framework are potential eavesdroppers. Furthermore, different scenarios whereby eavesdroppers can simultaneously target both the RF and FSO links can also be studied in the future. Investigating the interplay of MIMO-NOMA in the downlink scenario under these enhanced security considerations could provide valuable insights not only into enhancing spectral efficiency but also into fortifying the security aspects of FSO communication systems against more sophisticated attacks.
- **Mitigation Strategies for Colluding Eavesdroppers:** The observed significant influence of colluding eavesdroppers on the system's secrecy performance highlights the need for robust mitigation strategies. Besides adopting

AN signal to interfere with the eavesdropper's channel, future research could focus on developing advanced cryptographic techniques or dynamic resource allocation schemes to counteract collusion attempts effectively.

- **Integration of Machine Learning (ML):** Leveraging machine learning algorithms to predict and adapt to evolving eavesdropping patterns could be a promising direction. Developing intelligent systems that can dynamically adjust security parameters based on real-time threat assessments may contribute to more robust and adaptive wireless communication security.

- **Integration of Reconfigurable Intelligent Surface (RIS):** Investigating the potential of RIS to enhance the security of MIMO-NOMA technologies in the mixed RF-FSO systems presents a promising avenue for future direction. RIS can dynamically adjust the propagation environment, leading to improved secrecy performance and better resistance against eavesdropping attacks. Future research in this area may focus on developing novel RIS-based security mechanisms, optimizing RIS deployment strategies, and evaluating the practical feasibility and scalability of RIS-enabled mixed MIMO-NOMA/RF-FSO systems navigating the intricacies posed by imperfect CSI.

- **Mitigation the Interference:** An essential avenue for future research involves developing robust interference mitigation strategies tailored to suppress interference from overlapping signals in MIMO-NOMA systems with multiple concurrent transmissions especially in mixed RF-FSO systems. This requires innovative approaches that effectively manage the interference sources by utilizing advanced signal processing algorithms and resource allocation schemes. In addition, addressing interference mitigation comprehensively while enhancing the secrecy performance can present a security-reliability trade-off challenge in multi-antenna NOMA-enabled users in a mixed RF-FSO systems.

- **Cross-Layer Security Optimization in Mixed RF-FSO MIMO-NOMA Networks:** Investigating cross-layer security optimization techniques that integrate PLS mechanisms with higher-layer security protocols is crucial for comprehensive security in mixed RF-FSO MIMO-NOMA networks. Future research can explore novel cross-layer security designs that investigate PLS approaches to enhance higher-layer security mechanisms such as authentication, key management, and intrusion detection. In such scenarios, the ability to detect, prevent, and mitigate various security threats can be enhanced and thereby improving the overall secrecy performance of the mixed RF-FSO MIMO-NOMA network.

Appendix A

The Equivalent SINR at the Destination-Fixed Gain Relaying Scheme

The received signal at the relay node and the destination can be expressed respectively as

$$y_R = \sqrt{a_1 P_t L_1} x_{U_1} h_{U_1^{(b_1^*)} R_j} + \sqrt{a_2 P_t L_2} x_{U_2} h_{U_2^{(b_2^*)} R_j} + n_R \tag{A.1}$$

$$y_D = h_{RD} \mu \mathcal{G} y_R + n_D \tag{A.2}$$

Substitute (A.1) in (A.2), the received signal at the destination is given by

$$y_D = h_{RD} \mu \mathcal{G} \left[\sqrt{a_1 P_t L_1} x_{U_1} h_{U_1^{(b_1^*)} R_j} + \sqrt{a_2 P_t L_2} x_{U_2} h_{U_2^{(b_2^*)} R_j} + n_R \right] + n_D, \tag{A.3}$$

where the signal power transmitted by U_1 is $a_1 P_t$ and the signal power transmitted by U_2 is $a_2 P_t$. From (A.3), the signal-to-interference-plus-noise ratio (SINR) γ_2 associated with U_2 can be expressed as

$$\gamma_2 = \frac{(h_{RD} \mu \mathcal{G})^2 a_2 P_t L_2 \left| h_{U_2^{(b_2^*)} R_j} \right|^2}{(h_{RD} \mu \mathcal{G})^2 a_1 P_t L_1 \left| h_{U_1^{(b_1^*)} R_j} \right|^2 + h_{RD}^2 \mu^2 \mathcal{G}^2 \sigma_R^2 + \sigma_D^2}. \tag{A.4}$$

By dividing each term by $(\mu^2 \mathcal{G}^2 \sigma_R^2 \sigma_D^2)$ and performing some mathematical manipulations, (A.4) can be rewritten in a compact form as

$$\gamma_2 = \frac{\gamma_D \gamma_R^{(2)} a_2}{\gamma_D \gamma_R^{(1)} a_1 + \gamma_D + \Lambda}, \tag{A.5}$$

where $\Lambda = \frac{1}{\mu^2 \mathcal{G}^2 \sigma_R^2}$, $\mathcal{G}^2 = \frac{1}{\sigma_{U_2}^2 + \sigma_R^2}$ with $\sigma_{U_2}^2$ being the power noise of U_2 signal (variance), $\gamma_D = \frac{|h_{RD}|^2}{\sigma_D^2}$ is the instantaneous SNR for the received signal at the destination and $\gamma_R^{(i)}$ the instantaneous SINRs for the composite received signal at the relay denoted by $\gamma_R^{(1)}$ and $\gamma_R^{(2)}$ are expressed respectively as

$$\gamma_R^{(2)} = \frac{X_{U_2R}}{1 + X_{U_1R}}, \tag{A.6}$$

$$\gamma_R^{(1)} = \frac{X_{U_1R}}{1 + X_{U_2R}}, \tag{A.7}$$

where X_{U_1R} and X_{U_2R} are the instantaneous SNRs for each user given by

$$X_{U_1R} = \frac{a_1 L_1 P_t |h_{U_1^{(b_1^*)}R}|^2}{\sigma_R^2}, \tag{A.8}$$

$$X_{U_2R} = \frac{a_2 L_2 P_t |h_{U_2^{(b_2^*)}R}|^2}{\sigma_R^2}. \tag{A.9}$$

.

Appendix B

The CDF of the Equivalent SNR associated with U_1

To obtain the equivalent end-to-end SNR in (3.10), we first substitute (3.21) and (3.17) in (3.23).

$$F_{\gamma_{eq}^{(1)}}(x) = \frac{\xi^2}{r\Gamma(\alpha)\Gamma(\beta)\gamma_D} \underbrace{\sum_{n=0}^{N_{U_i}} \begin{pmatrix} N_{U_i} \\ n \end{pmatrix} (-1)^n \sum_{k=0}^{n(N_R-1)} C_{k,n}}_{\triangleq \sum_{nk}}$$
$$\times \int_0^\infty \left[\frac{x(\gamma_D+\Lambda)}{a_1\gamma_D}\right]^k exp\left[\frac{-n\lambda_R x(\gamma_D+\Lambda)}{\gamma_D a_1}\right] G_{r,3r+1}^{3r+1,0}\left(\frac{(d\alpha\beta)^r}{\mu_r^{\frac{1}{r}}}\gamma_D^{\frac{1}{r}} \middle| \begin{matrix} \xi^2+1 \\ \xi^2\alpha\beta \end{matrix}\right) d\gamma_D, \tag{B.1}$$

Next, by rewriting the expression $\left[\frac{x(\gamma_D+\Lambda)}{a_1\gamma_D}\right]^k$ as a series using the binomial expansion, and making use of the transformation $e^{-\frac{a}{z}} = G_{0,1}^{1,0}\left(\frac{z}{a} \middle| \begin{matrix} 1 \\ - \end{matrix}\right)$, the integral in (B.1) can be expressed as

$$F_{\gamma_{eq}^{(1)}}(x) = \frac{\xi^2}{r\Gamma(\alpha)\Gamma(\beta)} \underbrace{\sum_{n=0}^{N_{U_i}} \begin{pmatrix} N_{U_i} \\ n \end{pmatrix} (-1)^n \sum_{k=0}^{n(N_R-1)} C_{k,n} \sum_{j=0}^{k} \lambda_R^k \begin{pmatrix} k \\ j \end{pmatrix} \Lambda^j}_{\triangleq \sum_{nkj}}$$
$$\times\, x^k e^{\frac{-n\lambda_R}{a_1}x} \int_0^\infty \frac{1}{\gamma_D^{j+1}} G_{0,1}^{1,0}\left(\frac{a_1}{nx\lambda_R\Lambda}\gamma_D \middle| \begin{matrix} 1 \\ - \end{matrix}\right) G_{r,3r+1}^{3r+1,0}\left(\frac{(d\alpha\beta)^r}{\mu_r^{\frac{1}{r}}}\gamma_D^{\frac{1}{r}} \middle| \begin{matrix} \xi^2+1 \\ \xi^2\alpha\beta \end{matrix}\right) d\gamma_D, \tag{B.2}$$

Finally, we solve the integral in (B.2) using [130].

Appendix C

The Equivalent SINR at the Destination-Variable Gain Relaying Scheme

To derive the SINR of the γ_2 related to U_2 while considering variable gain at the relay node, we firstly divide (A.3) by $\sigma_R^2\sigma_D^2$ and perform some algebraic manipulations as

$$\gamma_2 = \frac{\gamma_D\gamma_R a_2}{\gamma_D\gamma_R a_1 + \gamma_D + \frac{1}{\mu^2\mathcal{G}^2\sigma_R^2\sigma_D^2}}, \tag{C.1}$$

Then, we substitute the value of the variable gain factor as $\mathcal{G}^2 = \frac{1}{\left|h_{U_2^{(b^*)}R_j}\right|^2 + \sigma_R^2}$ [141]. Thus, the SINR can be expressed as:

$$\gamma_2 = \frac{a_2\gamma_D\gamma_R^{(2)}}{a_1\gamma_D\gamma_R^{(1)} + \gamma_R^{(1)} + \gamma_D + 1}, \tag{C.2}$$

Appendix D

The ASC with Variable Gain at the Relay

After substituting (4.21) and (4.24) into (4.33), the average secrecy capacity (ASC) associated to U_1 can be derived as

$$
\begin{aligned}
\mathcal{ASC}^{(1)} &= \sum_{(nk)} \left(\frac{n\lambda_R}{a_1}\right)^k \\
&\times \int_0^\infty \left[\frac{1}{1+\gamma} exp\left(-\frac{n\lambda_R}{a_1}\gamma\right) - \frac{\Psi\gamma^k}{1+\gamma} exp\left(-\frac{n\lambda_R}{a_1}\right) G^{3r,1}_{r+1,3r+1}\left[q_{nU_1}\gamma|^{1,C_1}_{C_2,0}\right]\right. \\
&+ \sum_{j=0}^{N_E-1} \begin{pmatrix} N_E-1 \\ j \end{pmatrix} \frac{(a_{AN_1}\lambda_E)^j(-1)^j}{j!} \left(\frac{\gamma^{k+j}}{1+\gamma} exp\left[-\left(\frac{n\lambda_R}{a_1} + a_{\mathrm{AN}_1}\lambda_E\right)\gamma\right]\right. \\
&\left.\left. - \frac{\Psi\gamma^{k+j}}{1+\gamma} exp\left[-\left(\frac{n\lambda_R}{a_1} + a_{\mathrm{AN}_1}\lambda_E\right)\gamma\right] G^{3r,1}_{r+1,3r+1}\left[q_{nU_1}\gamma|^{1,C_1}_{C_2,0}\right]\right)\right] d\gamma. \quad \text{(D.1)}
\end{aligned}
$$

To solve the integral in (D.1), we make use of $\frac{x^a}{1+x} = G^{1,1}_{1,1}\left(x|^a_a\right), \exp(-bx) = G^{1,0}_{0,1}\left(bx|^-_0\right)$, [128, eqn. (7.813)], [128, eqn. (3.326.2)] and [140, eqn. (2.3.6.9)], and after some mathematical manipulations, we can obtain the closed-form expression of the exact ASC associated with U_1.

References

[1] M. Wu, K. Guo, Z. Lin, X. Li, K. An, and Y. Huang, "Joint optimization design of ris-assisted hybrid fso sagins using deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, 2023.

[2] S. A. H. Mohsan, M. A. Khan, and H. Amjad, "Hybrid fso/rf networks: A review of practical constraints, applications and challenges," *Optical Switching and Networking*, vol. 47, p. 100697, 2023.

[3] A. A. Osman, J. M. Moualeu, and F. Takawira, "Secrecy performance of uplink mimo-noma with antenna selection in a mixed rf-fso system," in *2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 2023, pp. 1–6.

[4] N. Nandan, S. Majhi, and H.-C. Wu, "Secure beamforming for MIMO-NOMA-based cognitive radio network," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1708–1711, Aug. 2018.

[5] Y. Qi and M. Vaezi, "Secure transmission in mimo-noma networks," *IEEE Communications Letters*, vol. 24, no. 12, pp. 2696–2700, Dec. 2020.

[6] K. Jadhav and A. Vidyarthi, "Optimal transmit antenna selection for non-orthogonal multiple access with improved lion algorithm," *International Journal of Communication Systems*, vol. 35, no. 18, p. e5327, 2022.

[7] S. I. Adam, "Performance enhancement of 5g networks: Remodeling power domain scheme through noma-mimo technologies integration," *International Journal of Advanced Engineering, Management and Science*, vol. 9, p. 11, 2023.

[8] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative noma systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.

[9] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, 1988.

[10] F. Irram, M. Ali, M. Naeem, and S. Mumtaz, "Physical layer security for beyond 5g/6g networks: Emerging technologies and future directions," *Journal of Network and Computer Applications*, vol. 206, p. 103431, 2022.

[11] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part ii: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[13] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. Nkouatchah, and U. S. Dias, "Transmit antenna selection in secure mimo systems over α-μ fading channels," *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6483–6498, 2019.

[14] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[15] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[16] M. Sadeghzadeh and M. Salehi, "Physical layer security in multi-user wireless networks: Interference effect on large scale analysis," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE, 2020, pp. 1–6.

[17] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed rf-fso systems," *IEEE Photonics Journal*, vol. 9, no. 4, pp. 1–14, 2017.

[18] J. Liu, J. Wang, B. Zhang, and Q. Wang, "Secrecy performance analysis of hybrid rf/vlc dual-hop relaying systems," *Frontiers in Physics*, p. 390, 2021.

[19] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed rf-fso systems," *IEEE Photonics Journal*, vol. 9, no. 4, pp. 1–14, Aug. 2017.

[20] H. Lei, Z. Dai, K.-H. Park, W. Lei, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6384–6395, Dec. 2018.

[21] D. R. Pattanayak, V. K. Dwivedi, V. Karwal, I. S. Ansari, H. Lei, and M.-S. Alouini, "On the physical layer security of a decode and forward based mixed fso/rf co-operative system," *IEEE Wireless Communications Letters*, vol. 9, no. 7, pp. 1031–1035, 2020.

[22] S. Islam, M. Zeng, and O. A. Dobre, "Noma in 5g systems: Exciting possibilities for enhancing spectral efficiency," *arXiv preprint arXiv:1706.08215*, 2017.

[23] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5g and beyond," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2347–2381, 2017.

[24] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, 2013, pp. 1–5.

[25] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Non-orthogonal multiple access for 5g: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, pp. 74–81, 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:206455590

[26] A. Akbar, S. Jangsher, and F. A. Bhatti, "Noma and 5g emerging technologies: A survey on issues and solution techniques," *Computer Networks*, vol. 190, p. 107950, 2021.

[27] M. Zeng, A. Yadav, O. A. Dobre, G. I. Tsiropoulos, and H. V. Poor, "On the sum rate of mimo-noma and mimo-oma systems," *IEEE Wireless communications letters*, vol. 6, no. 4, pp. 534–537, 2017.

[28] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (noma) for cellular future radio access," in *2013 IEEE 77th vehicular technology conference (VTC Spring)*. IEEE, 2013, pp. 1–5.

[29] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5g systems with randomly deployed users," *IEEE signal processing letters*, vol. 21, no. 12, pp. 1501–1505, 2014.

[30] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5g networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017.

[31] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin, and Z. Wang, "Non-orthogonal multiple access for 5g: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74–81, 2015.

[32] D. A. Bashar, "Artificial intelligence based lte mimo antenna for 5th generation mobile networks," *Journal of Artificial Intelligence and Capsule Networks*, vol. 2, no. 3, pp. 155–162, 2020.

[33] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive mimo: Benefits and challenges," *IEEE journal of selected topics in signal processing*, vol. 8, no. 5, pp. 742–758, 2014.

[34] N. H. M. Adnan, I. M. Rafiqul, and A. Z. Alam, "Massive mimo for fifth generation (5g): Opportunities and challenges," in *2016 International Conference on Computer and Communication Engineering (ICCCE)*. IEEE, 2016, pp. 47–52.

[35] A. Khuntia, R. Divya Dharshini, R. Mythri, K. Aditya, and D. Pradhan, "Energy-efficiency for 5g networks with mimo system," *Journal of Network Security Computer Networks*, vol. 9, no. 3, pp. 26–38, 2023.

[36] J. Frigon, B. Daneshrad, J. Putnam, E. Berg, R. Kim, T. Sun, and H. Samueli, "Field trial results for high-speed wireless indoor data communications," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 297–309, 2000.

[37] X. Jin, J.-S. No, and D.-J. Shin, "Source transmit antenna selection for mimo decode-and-forward relay networks," *IEEE transactions on signal processing*, vol. 61, no. 7, pp. 1657–1662, 2013.

[38] S. Sanayei and A. Nosratinia, "Antenna selection in mimo systems," *IEEE Communications magazine*, vol. 42, no. 10, pp. 68–73, 2004.

[39] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Müller, and R. F. Schaefer, "Optimal transmit antenna selection for massive mimo wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 817–828, 2018.

[40] A. F. Molisch and M. Z. Win, "Mimo systems with antenna selection," *IEEE microwave magazine*, vol. 5, no. 1, pp. 46–56, 2004.

[41] A. Gorokhov, D. A. Gore, and A. J. Paulraj, "Receive antenna selection for mimo spatial multiplexing: theory and algorithms," *IEEE Transactions on signal processing*, vol. 51, no. 11, pp. 2796–2807, 2003.

[42] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in rayleigh fading channels," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 4, pp. 1312–1321, 2005.

[43] W. C. Jakes and D. C. Cox, *Microwave mobile communications.* Wiley-IEEE press, 1994.

[44] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in rayleigh fading channels," *IEEE transactions on wireless communications*, vol. 3, no. 6, pp. 1980–1983, 2004.

[45] B. Q. Vo-Nguyen, T. Q. Duong, and N. N. Tran, "Ergodic capacity of cooperative networks using adaptive transmission and selection combining," in *2009 3rd International Conference on Signal Processing and Communication Systems.* IEEE, 2009, pp. 1–6.

[46] D. Brennan, "Linear diversity combining techniques," *Proceedings of the IEEE*, vol. 91, no. 2, pp. 331–356, 2003.

[47] D. G. Brennan, "Linear diversity combining techniques," *Proceedings of the IRE*, vol. 47, no. 6, pp. 1075–1102, 1959.

[48] T. Maseng, "Digital communication over fading channels: a unified approach to performance analysis [book review]," *IEEE Communications Magazine*, vol. 39, no. 7, pp. 36–36, 2001.

[49] W. Li and L. Kundu, "Study of multiple antenna systems: Capacity, diversity gain and spatial multiplexing."

[50] S. M. Ivari, M. R. Soleymani, and Y. R. Shayan, “Rs-based mimo-noma systems in multicast framework,” in *MIMO Communications-Fundamental Theory, Propagation Channels, and Antenna Systems.* IntechOpen, 2023.

[51] Z. Ding, F. Adachi, and H. V. Poor, “The application of mimo to non-orthogonal multiple access,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 537–552, 2015.

[52] Q. Sun, S. Han, I. Chin-Lin, and Z. Pan, “On the ergodic capacity of mimo noma systems,” *IEEE Wireless Communications Letters*, vol. 4, no. 4, pp. 405–408, 2015.

[53] Y. Liu, G. Pan, H. Zhang, and M. Song, “On the capacity comparison between mimo-noma and mimo-oma,” *IEEE Access*, vol. 4, pp. 2123–2129, 2016.

[54] M. Zeng, A. Yadav, O. A. Dobre, G. I. Tsiropoulos, and H. V. Poor, “Capacity comparison between mimo-noma and mimo-oma with multiple users in a cluster,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2413–2424, 2017.

[55] A. Benjebbour, K. Saito, A. Li, Y. Kishiyama, and T. Nakamura, “Non-orthogonal multiple access (noma): Concept, performance evaluation and experimental trials,” in *2015 International conference on wireless networks and mobile communications (WINCOM).* IEEE, 2015, pp. 1–6.

[56] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, “Application of non-orthogonal multiple access in lte and 5g networks,” *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, 2017.

[57] J. Choi, “Minimum power multicast beamforming with superposition coding for multiresolution broadcast and application to noma systems,” *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 791–800, 2015.

[58] Y. Liu, H. Xing, C. Pan, A. Nallanathan, M. Elkashlan, and L. Hanzo, “Multiple-antenna-assisted non-orthogonal multiple access,” *IEEE Wireless Communications*, vol. 25, no. 2, pp. 17–23, 2018.

[59] Z. Q. Al-Abbasi and D. K. C. So, “User-pairing based non-orthogonal multiple access (noma) system,” in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1–5.

[60] N. Nandan, S. Majhi, and H.-C. Wu, "Beamforming and power optimization for physical layer security of mimo-noma based crn over imperfect csi," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5990–6001, June 2021.

[61] J. A. Oviedo and H. R. Sadjadpour, "A new noma approach for fair power allocation," in *2016 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. IEEE, 2016, pp. 843–847.

[62] S. Jo, C. Jong, C. Pak, and H. Ri, "Multi-agent deep reinforcement learning-based energy efficient power allocation in downlink mimo-noma systems," *IET Communications*, vol. 15, no. 12, pp. 1642–1654, 2021.

[63] W. Shin, M. Vaezi, B. Lee, D. J. Love, J. Lee, and H. V. Poor, "Coordinated beamforming for multi-cell mimo-noma," *IEEE Communications Letters*, vol. 21, no. 1, pp. 84–87, 2016.

[64] R. Ge, D. Bian, J. Cheng, K. An, J. Hu, and G. Li, "Joint user pairing and power allocation for noma-based geo and leo satellite network," *IEEE Access*, vol. 9, pp. 93 255–93 266, 2021.

[65] S. Chinnadurai, P. Selvaprabhu, Y. Jeong, A. L. Sarker, H. Hai, W. Duan, and M. H. Lee, "User clustering and robust beamforming design in multicell mimo-noma system for 5g communications," *AEU-International Journal of Electronics and Communications*, vol. 78, pp. 181–191, 2017.

[66] J.-M. Kang, I.-M. Kim, and C.-J. Chun, "Deep learning-based mimo-noma with imperfect sic decoding," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3414–3417, 2019.

[67] C. Lin, Q. Chang, and X. Li, "A deep learning approach for mimo-noma downlink signal detection," *Sensors*, vol. 19, no. 11, p. 2526, 2019.

[68] M. K. Hasan, M. Shahjalal, M. M. Islam, M. M. Alam, M. F. Ahmed, and Y. M. Jang, "The role of deep learning in noma for 5g and beyond communications," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2020, pp. 303–307.

[69] I. Kumar, V. Sachan, R. Shankar, and R. K. Mishra, "Performance analysis of multi-user massive mimo systems with perfect and imperfect csi," *Procedia Computer Science*, vol. 167, pp. 1452–1461, 2020.

[70] R. Alberto and F. A. Monteiro, "Downlink mimo-noma with and without csi: A short survey and comparison," in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*. IEEE, 2020, pp. 1–6.

[71] X. Chen, Z. Zhang, C. Zhong, and D. W. K. Ng, "Exploiting multiple-antenna techniques for non-orthogonal multiple access," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2207–2220, 2017.

[72] E. C. Vilas Boas, J. D. e Silva, F. A. de Figueiredo, L. L. Mendes, and R. A. de Souza, "Artificial intelligence for channel estimation in multicarrier systems for b5g/6g communications: a survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 116, 2022.

[73] V. P. Rekkas, S. Sotiroudis, P. Sarigiannidis, S. Wan, G. K. Karagiannidis, and S. K. Goudos, "Machine learning in beyond 5g/6g networks—state-of-the-art and future trends," *Electronics*, vol. 10, no. 22, p. 2786, 2021.

[74] A. I. Salameh and M. El Tarhuni, "From 5g to 6g—challenges, technologies, and applications," *Future Internet*, vol. 14, no. 4, p. 117, 2022.

[75] Z. Liu, L. Zhang, and Z. Ding, "Overcoming the channel estimation barrier in massive mimo communication via deep learning," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 104–111, 2020.

[76] K. Hassan, M. Masarra, M. Zwingelstein, and I. Dayoub, "Channel estimation techniques for millimeter-wave communication systems: Achievements and challenges," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1336–1363, 2020.

[77] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies," *IEEE access*, vol. 9, pp. 67 512–67 547, 2020.

[78] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6g wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020.

[79] W. Shakir and R. Abdulkareem, "A survey on physical layer security for fso communication systems," in *Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey*, 2022.

[80] M. Bloch, *Physical-layer security.* Georgia Institute of Technology, 2008.

[81] D. R. Pattanayak, V. K. Dwivedi, and V. Karwal, "On the physical layer security of hybrid rf-fso system in presence of multiple eavesdroppers and receiver diversity," *Optics Communications*, 2020.

[82] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1470–1482, 2017.

[83] C. Gong, X. Yue, Z. Zhang, X. Wang, and X. Dai, "Enhancing physical layer security with artificial noise in large-scale noma networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2349–2361, 2021.

[84] V. N. Nayak and K. K. Gurrala, "Enhanced physical layer security for cooperative noma network with hybrid-decode-amplify-forward relaying via power allocation assisted control jamming," *Wireless Personal Communications*, vol. 120, no. 3, pp. 2473–2490, 2021.

[85] W. M. R. Shakir, "Physical layer security performance analysis of hybrid fso/rf communication system," *IEEE Access*, vol. 9, pp. 18 948–18 961, 2020.

[86] D.-D. Tran, H.-V. Tran, D.-B. Ha, and G. Kaddoum, "Secure transmit antenna selection protocol for mimo noma networks over nakagami-m channels," *IEEE Systems Journal*, vol. 14, no. 1, pp. 253–264, 2019.

[87] X. Liu, L. Zhang, W. Xie, Y. Cao, and C. Fan, "Physical layer security of the mimo-noma systems under near-field scenario," *Electronics*, vol. 13, no. 4, p. 670, 2024.

[88] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink noma multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70 422–70 435, 2019.

[89] Y. Dursun, K. Wang, and Z. Ding, "Secrecy sum rate maximization for a mimo-noma uplink transmission in 6g networks," *Physical Communication*, vol. 53, p. 101675, 2022.

[90] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *2009 3rd International Conference on Signal Processing and Communication Systems.* IEEE, 2009, pp. 1–5.

[91] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2016.

[92] H. M. Furqan, J. Hamamreh, H. Arslan *et al.*, "Physical layer security for noma: Requirements, merits, challenges, and recommendations," *arXiv preprint arXiv:1905.05064*, 2019.

[93] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.

[94] A. Abushattal, S. Althunibat, M. Qaraqe, and H. Arslan, "A secure downlink noma scheme against unknown internal eavesdroppers," *IEEE Wireless Communications Letters*, 2021.

[95] M. Abolpour, M. Mirmohseni, and M. R. Aref, "On the secrecy performance of noma systems with both external and internal eavesdroppers," *arXiv preprint arXiv:1906.03929*, 2019.

[96] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, "Optimal relay selection for secure noma systems under untrusted users," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 1942–1955, 2019.

[97] D. Mihaylova, V. Stoynov, A. Ivanov, and Z. Valkova-Jarvis, "An overview of methods to combat eavesdropping in noma-based networks through physical layer security," in *IOP Conference Series: Materials Science and Engineering*, vol. 1032, no. 1. IOP Publishing, 2021, p. 012011.

[98] E. Bayaki, R. Schober, and R. K. Mallik, "Performance analysis of free-space optical systems in gamma-gamma fading," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference.* IEEE, 2008, pp. 1–6.

[99] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 2231–2258, Fourthquarter 2014.

[100] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, no. 2, pp. 1–14, Apr. 2015.

[101] A. Sikri, A. Mathur, M. Bhatnagar, G. Kaddoum, P. Saxena, and J. Nebhen, "Artificial noise injection–based secrecy improvement for fso systems," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–12, 2021.

[102] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of fso communications over málaga channels," *IEEE Photonics Journal*, vol. 12, no. 6, pp. 1–17, 2020.

[103] J. Anguita, I. Djordjevic, M. Neifeld, and B. Vasic, "Shannon capacities and error-correction codes for optical atmospheric turbulent channels," *Journal of Optical Networking*, vol. 4, no. 9, pp. 586–601, 2005.

[104] E. Bayaki, R. Schober, and R. K. Mallik, "Performance analysis of mimo free-space optical systems in gamma-gamma fading," *IEEE Transactions on Communications*, vol. 57, no. 11, pp. 3415–3424, 2009.

[105] Y. Wu, M. Jiang, G. Li, and D. Kong, "Systematic performance analysis of hybrid fso/rf system over generalized fading channels with pointing errors," in *Photonics*, vol. 9, no. 11. MDPI, 2022, p. 873.

[106] K. O. Odeyemi and P. A. Owolawi, "Selection combining hybrid fso/rf systems over generalized induced-fading channels," *Optics Communications*, vol. 433, pp. 159–167, 2019.

[107] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE communications surveys and tutorials*, vol. 16, no. 4, pp. 2231–2258, 2014.

[108] L. Yang, T. Liu, J. Chen, and M.-S. Alouini, "Physical-layer security for mixed η - μ and m -distribution dual-hop rf/fso systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12 427–12 431, 2018.

[109] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar, and H. Lei, "Physical layer security of hybrid satellite-fso cooperative systems," *IEEE Photonics Journal*, vol. 11, no. 1, pp. 1–14, 2019.

[110] N. Mensi and D. B. Rawat, "Security analysis of noma-fso/rf network over double shadowed k- μ and Mlaga channels," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 1691–1696.

[111] V. Bankey, V. Singh, and P. K. Upadhyay, "Physical layer secrecy of noma-based hybrid satellite-terrestrial relay networks," in *2020 IEEE Wireless*

Communications and Networking Conference (WCNC). IEEE, 2020, pp. 1–6.

[112] N. Varshney, A. K. Jagannatham, and P. K. Varshney, "Cognitive mimo-rf/fso cooperative relay communication with mobile nodes and imperfect channel state information," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 3, pp. 544–555, 2018.

[113] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, and M.-S. Alouini, "On secure mixed rf-fso systems with tas and imperfect csi," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4461–4475, 2020.

[114] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[115] A. K. Shukla, K. Yadav, P. K. Upadhyay, and J. M. Moualeu, "Exploiting deep learning in the performance evaluation of EH-based coordinated direct and relay transmission system with cognitive noma," *IEEE Communications Letters*, vol. 27, no. 6, pp. 1501–1505, June 2023.

[116] Z. Ding, F. Adachi, and H. V. Poor, "The application of MIMO to non-orthogonal multiple access," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 537–552, Jan. 2016.

[117] S. V. Kartalopoulos, "A primer on cryptography in communications," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 146–151, Apr. 2006.

[118] Y. Qi and M. Vaezi, "IRS-assisted physical layer security in MIMO-NOMA networks," *IEEE Communications Letters*, vol. 27, no. 3, pp. 792–796, Mar. 2023.

[119] D.-D. Tran, H.-V. Tran, D.-B. Ha, and G. Kaddoum, "Secure transmit antenna selection protocol for mimo noma networks over nakagami-m channels," *IEEE Systems Journal*, vol. 14, no. 1, pp. 253–264, Mar. 2020.

[120] L. Han, Y. Wang, X. Liu, and B. Li, "Secrecy performance of fso using hd and im/dd detection technique over f-distribution turbulence channel with pointing error," *IEEE Wireless Communications Letters*, 2021.

[121] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, no. 2, pp. 1–14, 2015.

[122] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, “Survey on physical layer security in optical wireless communication systems,” in *2018 Seventh International Conference on Communications and Networking (ComNet)*. IEEE, 2018, pp. 1–5.

[123] G. D. Verma, A. Mathur, Y. Ai, and M. Cheffena, “Secrecy performance of fso communication systems with non-zero boresight pointing errors,” *IET Communications*, 2021.

[124] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, and M.-S. Alouini, “On secure mixed RF-FSO systems with TAS and imperfect CSI,” *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020.

[125] M. V. Jamali and H. Mahdavifar, “Uplink non-orthogonal multiple access over mixed rf-fso systems,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3558–3574, 2020.

[126] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martínez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, “Information-theoretic security of mimo networks under kappa-mu shadowed fading channels,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 6302–6318, 2021.

[127] C. S. Patel, G. L. Stuber, and T. G. Pratt, “Statistical properties of amplify and forward relay fading channels,” *IEEE Transactions on Vehicular Technology*, vol. 55, no. 1, pp. 1–9, 2006.

[128] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products.* Academic press, 2014.

[129] V. S. Adamchik and O. Marichev, “The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system,” in *Proceedings of the international symposium on Symbolic and algebraic computation*, 1990, pp. 212–224.

[130] W. Alpha. (01.06.2023) Meijer g-function. [Online]. Available: https://functions.wolfram.com/HypergeometricFunctions/MeijerG/21/02/04/0001/MainEq1.L.gif

[131] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, “Performance analysis of fso links over unified gamma-gamma turbulence channels,” in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–5.

[132] M. A. Amirabadi and V. T. Vakili, "Performance of a relay-assisted hybrid fso/rf communication system," *Physical communication*, vol. 35, p. 100729, 2019.

[133] J.-Y. Wang, C. Liu, J.-B. Wang, J. Dai, M. Lin, and M. Chen, "Secrecy outage probability analysis over Malaga-Malaga fading channels," in *2018 IEEE International Conference on Communications (ICC).* IEEE, 2018, pp. 1–6.

[134] D. Jiang, Y. Gao, G. Li, N. Sha, X. Bian, and X. Wang, "Enhancing physical layer security of cooperative nonorthogonal multiple access networks via artificial noise," *Electronics*, vol. 12, no. 10, p. 2224, 2023.

[135] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias, and R. A. de Souza, "Physical layer security over α κ -μ and α -\$*eta*-μ fading channels," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 1025–1029, 2018.

[136] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "Secrecy performance of cognitive underlay hybrid rf/fso system under pointing errors and link blockage impairments," *Optical and Quantum Electronics*, vol. 52, no. 3, pp. 1–16, 2020.

[137] A. A. F. Osman, J. M. Moualeu, F. Takawira, K. Yadav, and P. K. Upadhyay, "On secure hybrid RF-FSO MIMO-NOMA systems with colluding and non-colluding eavesdroppers," *IEEE Wireless Commun. Lett.*, pp. 1–1, 2024.

[138] D. R. Pattanayak, V. K. Dwivedi, V. Karwal, A. Upadhya, H. Lei, and G. Singh, "Secure transmission for energy efficient parallel mixed fso/rf system in presence of independent eavesdroppers," *IEEE Photonics Journal*, vol. 14, no. 1, pp. 1–14, 2021.

[139] N. Arı, N. Thomos, and L. Musavian, "Secrecy performance of short packet communications: Wiretap channel with multiple receivers and eavesdroppers," in *2022 International Wireless Communications and Mobile Computing (IWCMC).* IEEE, 2022, pp. 395–400.

[140] A. Prudnikov, *Integrals and series: direct laplace transforms.*

[141] F. S. Tabataba, P. Sadeghi, T. Lamahewa, and M. R. Pakravan, "Statistical properties of amplify and forward relay links with channel estimation errors," in *2009 Australian Communications Theory Workshop.* IEEE, 2009, pp. 44–49.