Physical Layer Security in Emerging Wireless Transmission Systems

by

Tingnan Bao
B.Sc., Liaoning Technical University, 2007
M.Sc., KTH Royal Institute of Technology, 2015
M.Sc., University of Trento, 2015

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Electrical & Computer Engineering

Physical Layer Security in Emerging Wireless Transmission Systems

by

Tingnan Bao
B.Sc., Liaoning Technical University, 2007
M.Sc., KTH Royal Institute of Technology, 2015
M.Sc., University of Trento, 2015

Supervisory Committee

Dr. Hong-Chuan Yang, Supervisor
(Department of Electrical & Computer Engineering)

Dr. Mazen O. Hasna, Co-Supervisor
(Department of Electrical Engineering)

Dr. Julie Zhou, Outside Member
(Department of Mathematics and Statistics)

Supervisory Committee

Dr. Hong-Chuan Yang, Supervisor
(Department of Electrical & Computer Engineering)

Dr. Mazen O. Hasna, Co-Supervisor
(Department of Electrical Engineering)

Dr. Julie Zhou, Outside Member
(Department of Mathematics and Statistics)

ABSTRACT

Traditional cryptographic encryption techniques at higher layers require a certain form of information sharing between the transmitter and the legitimate user to achieve security. Besides, it also assumes that the eavesdropper has an insufficient computational capability to decrypt the ciphertext without the shared information. However, traditional cryptographic encryption techniques may be insufficient or even not suitable in wireless communication systems. Physical layer security (PLS) can enhance the security of wireless communications by leveraging the physical nature of wireless transmission. Thus, in this thesis, we study the PLS performance in emerging wireless transmission systems. The thesis consists of two main parts.

We first consider the PLS design and analysis for ground-based networks employing random unitary beamforming (RUB) scheme at the transmitter. With RUB technique, the transmitter serves multiple users with pre-designed beamforming vectors, selected using limited channel state information (CSI). We study multiple-input single-output single-eavesdropper (MISOSE) transmission system, multi-user multiple-input multiple-output single-eavesdropper (MU-MIMOSE) transmission system, and massive multiple-input multiple-output multiple-eavesdropper (massive MIMOME) transmission system. The closed-form expressions of ergodic secrecy rate

and the secrecy outage probability (SOP) for these transmission scenarios are derived. Besides, the effect of artificial noise (AN) on secrecy performance of RUB-based transmission is also investigated. Numerical results are presented to illustrate the trade-off between performance and complexity of the resulting PLS design.

We then investigate the PLS design and analysis for unmanned aerial vehicle (UAV)-based networks. We first study the secrecy performance of UAV-assisted relaying transmission systems in the presence of a single ground eavesdropper. We derive the closed-form expressions of ergodic secrecy rate and intercept probability. When multiple aerial and ground eavesdroppers are located in the UAV-assisted relaying transmission system, directional beamforming technique is applied to enhance the secrecy performance. Assuming the most general κ-μ shadowed fading channel, the SOP performance is obtained in the closed-form expression. Exploiting the derived expressions, we investigate the impact of different parameters on secrecy performance. Besides, we utilize a deep learning approach in UAV-based network analysis. Numerical results show that our proposed deep learning approach can predict secrecy performance with high accuracy and short running time.

Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

I would like to thank:

My parents for giving me the moral and finical support throughout my life.

Dr. Hong-Chuan Yang for helping me as supervisor all the time in my research work. I could not have imagined having a better advisor and mentor for my graduate studies.

Dr. Mazen O. Hasna for the continuous support of my graduate studies as co-supervisor, for his inspiration, patience, dedicated attention and immense knowledge.

Dr. Julie Zhou for serving as an outside member in my thesis supervisory committee.

DEDICATION

Just hoping this is useful!

Chapter 1

Introduction

Information security is a critical issue for wireless communication systems. Booming data traffic of wireless communication systems has prompted demand for growing level of information security. Nowadays, high-layer encryption techniques are widely adopted to achieve information security [1]. However, traditional cryptographic techniques may be insufficient or even not suitable, partly because an additional channel is required for secret key exchanges between the transmitter and the legitimate user [2], and partly because it is unreliable to assume that the eavesdropper has an insufficient computational capability to decrypt the ciphertext without the secret key [3]. Fortunately, physical layer security (PLS) can enhance communication securing by leveraging the physical nature of wireless transmission.

This chapter provides an overview of the fundamentals of this thesis, including PLS, multiple antennas transmission, massive multiple-input multiple-output (MIMO), and unmanned aerial vehicle (UAV) techniques. The chapter is organized as follows. In Section 1.1, we briefly review these techniques as backgrounds. In Section 1.2, literature survey of these techniques related to PLS is carried out. Lastly, the thesis outline is provided in Section 1.3.

1.1 Backgrounds

1.1.1 Physical Layer Security

Security plays a significant role in terms of wireless network design due to the broadcast nature of the wireless medium. Traditional cryptographic encryption techniques at higher layers require a certain form of shared information (e.g., secret key) be-

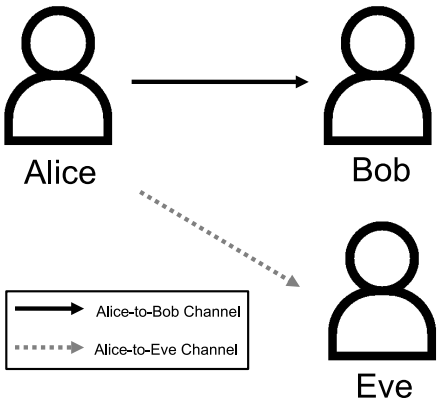

Figure 1.1: The Wiretap channel.

tween the transmitter and the legitimate user to achieve security [2]. This approach assumes that the communication of the secret key is error-free. However, error-free communication cannot be always guaranteed in non-deterministic wireless channels [4]. More importantly, all cryptographic measures assume that it is computationally infeasible for the eavesdropper to break the cipher without the secret key. Due to the increase of computational power, unbreakable ciphers in the past can be defeated now. Thus, PLS, as a novel approach for wireless security, is proposed to take advantage of the wireless channel characteristics. Wyner firstly developed a secure communication model as the wiretap channel, which consists of three members including a transmitter (Alice), a legitimate user (Bob) and an eavesdropper (Eve) [5], as shown in Fig. 1.1. In such a scenario, Alice sends a confidential message to Bob, while Eve receives the signal and intends to decode it. The key implementation of PLS is that Alice sends a confidential message to Bob with a maximum transmission rate, at which Eve cannot to decode any information. We assume the maximum achievable secrecy transmission rate as secrecy capacity, which is a principal metric to measure secrecy performance over wireless communication systems. Generally speaking, secrecy capacity is determined by the qualities of Alice-to-Bob channel and Alice-to-Eve channel. Wyner's result shows that a confidential message can be exchanged between Alice and Bob with a positive secrecy capacity if the channel conditions of Alice-to-Bob is better than that of Alice-to-Eve over a discrete memoryless wiretap channel [5]. As an extension of Wyner's work, [6] calculates the secrecy capacity of a Gaussian wiretap channel as the difference between the capacities of Alice-to-Bob

channel and Alice-to-Eve channel, given by

$$C_s = C_m - C_w, \tag{1.1}$$

where $C_m = \log_2(1 + P/N_m)$ is the Shannon capacity of Alice-to-Bob channel, $C_w = \log_2(1+P/N_w)$ is the Shannon capacity of Alice-to-Eve channel, P denotes the transmit power, and N_m and N_w are the noise power of Alice-to-Bob channel and Alice-to-Eve channel, respectively. Note that Gaussian channel is time-invariant. In such a scenario, the channel gain is constant during the whole transmission. Thus, non-zero secrecy capacity exists only when the received signal-to-noise ratio (SNR) at Bob is greater than that at Eve (i.e., $P/N_m > P/N_w$) [6]. Moreover, in a quasi-static flat fading scenario, the gains of Alice-to-Bob channel and Alice-to-Eve channel change randomly over different time slots but remain constant in each slot. Thus, the secrecy capacity for one realization of the quasi-static flat fading wiretap-channel is given by [7]

$$C_s = \begin{cases} \log_2(1 + |h_m|^2 \frac{P}{N_m}) - \log_2(1 + |h_w|^2 \frac{P}{N_w}), & \text{if} \quad \gamma_B > \gamma_E; \\ 0, & \text{if} \quad \gamma_B \leq \gamma_E, \end{cases} \tag{1.2}$$

where $|h_m|^2$ and $|h_w|^2$ denote the complex channel coefficients of Alice-to-Bob channel and Alice-to-Eve channel, respectively. However, the instantaneous secrecy capacity is different for different fading scenarios. Ergodic secrecy rate is proposed as a performance metric to investigate the security in a long-term sense [8]. In [9], the capacity-secrecy tradeoff is characterized in extending wiretap channel to the broadcast channel. Afterwards, information theoretical results for secure communications are derived for several wireless networks [10, 11, 12]. The secrecy rate of single-input single-output (SISO) fading channels [13], [14], Gaussian multiple access channels [15], [16], interference channels [17, 18, 19] and relay channels [20], [21] have been studied.

1.1.2 Multiple Antennas Transmission

Multiple-antenna wireless communication systems are conceived to increase transmission reliability with spatial diversity techniques and support high data rates through spatial multiplexing techniques [22]. In general, an multiple-antenna transmission system consists of M transmit and N receive antennas. There are several special

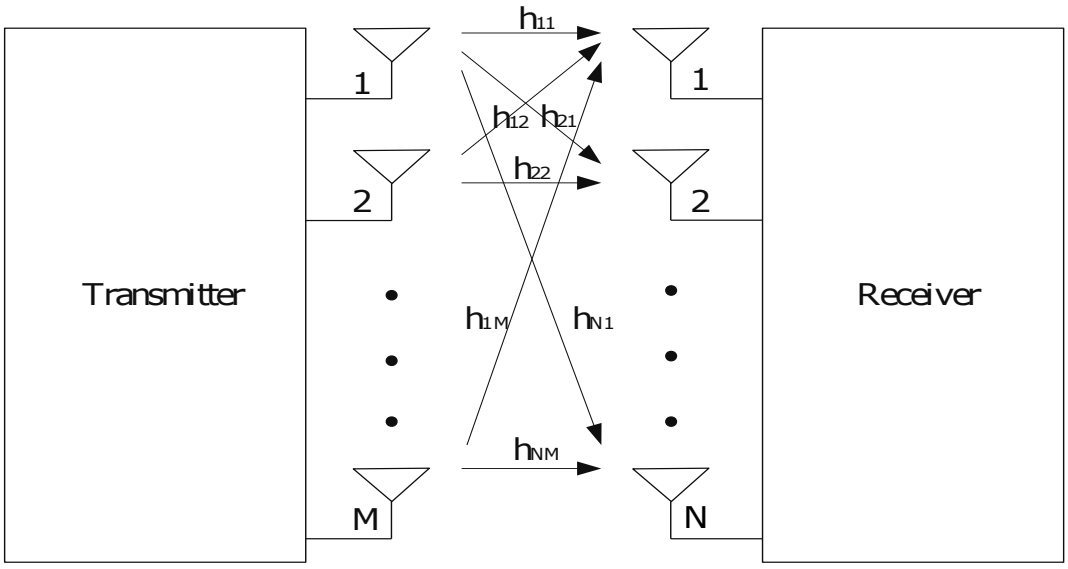

Figure 1.2: A generic model of MIMO systems.

cases of multiple antennas transmission system. If $M \geq 2$ and $N \geq 2$, we call the system as multiple-input multiple-output (MIMO) system. If $M = 1$ and $N \geq 2$, we term the system as single-input multiple-output (SIMO) system, vice versa. If $M = 1$ and $N = 1$, we name the system as SISO system, which is a conventional wireless system [23]. A generic model of MIMO systems can be shown in Fig. 1.2. Considering a narrowband MIMO channel, the received symbol vectors over a symbol period can be expressed as

$$\begin{bmatrix} y_1 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} h_{11} & \cdots & h_{1M} \\ \vdots & \ddots & \vdots \\ h_{N1} & \cdots & h_{NM} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_M \end{bmatrix} + \begin{bmatrix} n_1 \\ \vdots \\ n_N \end{bmatrix}, \tag{1.3}$$

or equivalently:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1.4}$$

where $\mathbf{x}$ is the transmitted symbol vector, $\mathbf{y}$ is the received vector, $\mathbf{H}$ is the channel matrix and $\mathbf{n}$ is the noise vector. Note that all the transmitted symbols from $\mathbf{x}$ are superposed, leading to interchannel interference (ICI). Linear zero-forcing (ZF) detection, as one of spatial multiplexing technique, can completely remove spatial

interference [24]. However, variance of the resulting noise samples may be enhanced. Linear minimizing mean squared error (MMSE) detection is proposed to provide a better trade-off between spatial interference mitigation and noise enhancement [25]. Both techniques assume that the channel state information (CSI) is only known at the receiver. Moreover, when the CSI is known to both the transmitter and receiver, the singular value decomposition (SVD) of the channel matrix $\mathbf{H}$ is possible, resulting a better system performance [26].

While MIMO techniques can achieve high data rates, it is impossible to deploy the same number of antennas at the mobile terminals as the base stations (BSs). Considering the hardware size and cost constraints, most mobile receivers in wireless systems still have a single antenna. We can still explore spatial multiplexing gain to improve data rate in such a scenario through the simultaneous transmission to multiple single-antenna receivers [27, 28, 29]. Thus, attention has shifted to the resulting multiuser MIMO (MU-MIMO) transmission. Particularly, dirty-paper coding (DPC) [30] can achieve the maximum sum rate and provide the maximum diversity order for an MU-MIMO transmission. However, the DPC technique requires very high computational complexity and complete CSI at the transmitter, which makes it hard to implement in practice. Suboptimal beamforming-based schemes, such as ZF beamforming (ZFBF) [31, 32] and random unitary beamforming (RUB) [33, 34, 35], can offer a practical solution for MU-MIMO transmission.

Zeroforcing Beamforming

ZFBF technique is a beamforming scheme for MU-MIMO transmission. With ZFBF, one user's beamforming vector is designed to be orthogonal to other selected users' channel vectors. As such, multiuser interference can be completely eliminated. In particular, when we consider a downlink MU-MIMO transmission where the BS with M antennas serves N single-antenna users, the transmitted signal vector from M antennas of the BS over a symbol period can be written as

$$\mathbf{x} = \sum_{m=1}^{M} \mathbf{u}_m s_m, \tag{1.5}$$

where $\mathbf{u}_m$ is the beamforming vector and s_m is the information symbol for the mth selected user. Thus, the received symbol at user i can be expressed as

$$y_i = \mathbf{h}_i^T \mathbf{x} + n_i = \mathbf{h}_i^T \mathbf{u}_i s_i + \sum_{m=1, m\neq i}^{M} \mathbf{h}_i^T \mathbf{u}_m s_m + n_i, \tag{1.6}$$

where $\mathbf{h}_i$ and n_i are channel vector and additive noise, respectively and the superscript $(\cdot)^T$ is the transpose.

If we design beamforming vector $\mathbf{u}_m$ is orthogonal to other selected users' channel vectors (i.e. $\mathbf{h}_i^T \mathbf{u}_m = 0$), then the multiuser interference is eliminated. As such, the received symbol at user i becomes

$$y_i = \mathbf{h}_i^T \mathbf{u}_i s_i + n_i. \tag{1.7}$$

As such, the BS needs to calculate the beamforming vectors for downlink transmission. Generally, a common solution of beamforming matrix design is the pseudo inverse of the channel matrix $\mathbf{H}$. Note that the computational complexity of the beamforming matrix is higher with the increase of the number of antennas at the BS or the number of users, leading to the larger channel matrix. Thus, full CSI at the BS is required for the ZFBF scheme, which leads to high computational complexity.

Random Unitary Beamforming

RUB is a low-complexity transmission scheme for MU-MIMO transmission. Different from ZFBF scheme, RUB scheme only requires partial CSI at the BS. In particular, when we consider a downlink MU-MIMO transmission, the BS will serve N target users using one of M random orthonormal beams, generated from an isotropic distribution [36]. The set of these random orthonormal beamforming vectors is denoted by $\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_M]$. It is assumed that the set of beamforming vectors changes in each time slot and is always known to each user. When we consider a downlink MU-MIMO transmission, the transmitted signal vector from M antennas of the BS over a symbol period can be written as

$$\mathbf{x} = \sum_{i=1}^{M} \mathbf{u}_i s_i, \tag{1.8}$$

where $\mathbf{u}_i$ is the beamforming vector selected for user i and s_i is the information symbol for user i. Thus, the received symbol at user i, assigned to the jth beam, can be expressed as

$$y_i = \mathbf{h}_i^T \mathbf{x} + n_i = \mathbf{h}_i^T \mathbf{u}_j s_j + \sum_{m=1, m\neq j}^{M} \mathbf{h}_i^T \mathbf{u}_m s_m + n_i. \tag{1.9}$$

Consequently, the received signal to interference plus noise ratio (SINR) at user i on the jth beam is given by

$$\gamma_{i,j} = \frac{|\mathbf{h}_i^T \mathbf{u}_j|^2}{\sum_{m=1, m\neq j}^{M} |\mathbf{h}_i^T \mathbf{u}_m|^2 + 1/\rho}, j = 1, 2, \cdots, M, \tag{1.10}$$

where ρ is the normalized average received SNR per transmit antenna.

There are two feedback strategies including full SINR feedback and best SINR feedback for the RUB scheme. In the case of a full SINR feedback strategy, each user needs to calculate and feedback on its experienced SINR value on M beams. The feedback load is $M \times N$ real numbers. Based on the feedback information, the BS selects the user experiencing the highest SINR among N users on a particular beam by ranking all the N feedback SINRs, assuming no user is the strongest user on two different beams. Afterwards, the BS similarly assigns other beams. This process continues till M beams have been assigned. In the case of the best SINR feedback strategy, each user feeds back its highest SINR and the corresponding beam index. The feedback load is one real number for the SINR value and one finite integer for the index of the best beam per user. Based on the feedback information, the BS assigns a beam to the user with the highest SINR among N users who feed back the index of that beam by ranking all N feedback best beam SINRs. Afterwards, the BS will rank the feedback SINRs for the remaining beams. This process continues until M beams have been assigned.

Compared with ZFBF technique, RUB scheme has its own characteristics. Firstly, beamforming vectors are pre-determined. Secondly, although multiuser interference exists, it can be controlled through user selection strategy. For example, each user feeds back its SINR information on different beamforming directions. Thus, it is noted that only partial CSI at the BS is required for RUB scheme, resulting in lower computational complexity.

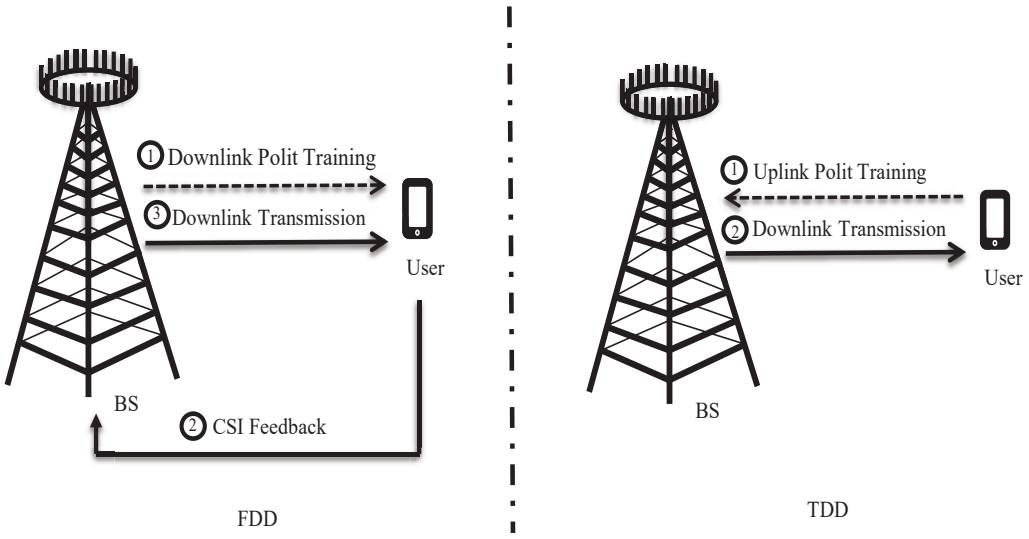

Figure 1.3: FDD versus TDD.

1.1.3 Massive MIMO Systems

Massive MIMO is a critical wireless technology in the evolution of 4G towards 5G networks [37]. In massive MIMO, a BS is equipped with a large number of antenna elements and serves several users simultaneously. Massive MIMO can enhance network capacity, spectral and energy efficiency of wireless transmission [38, 39]. Particularly, linear precoding techniques such as simple matched filter (MF) and beamforming are employed at the BS to alleviate the effect of noise and interference in massive MIMO systems [39]. These beamforming techniques assume that the accurate full CSI of users is available at the BS to improve the network performance. It is, generally, very challenging to provide accurate full CSI at the BS in practice. Typically, most massive MIMO systems adopt time-division-duplex (TDD) implementation and exploit channel reciprocity for CSI acquisition at the BS, shown in Fig. 1.3. [40, 41, 42]. Particularly, users send pilots on the uplink channel. Then, the BS estimates the downlink channel by using uplink pilots from users. Thus, the overhead of the pilot transmission is proportional to the number of users. However, the estimated uplink CSI may not match the actual downlink CSI when the BS performs transmission due to, for example, channel decorrelation, calibration error, and hardware impairment in uplink/downlink radio frequency (RF) chain [43]. When the CSI needs to be fed back from the users, these full CSI based beamforming schemes will incur large feedback

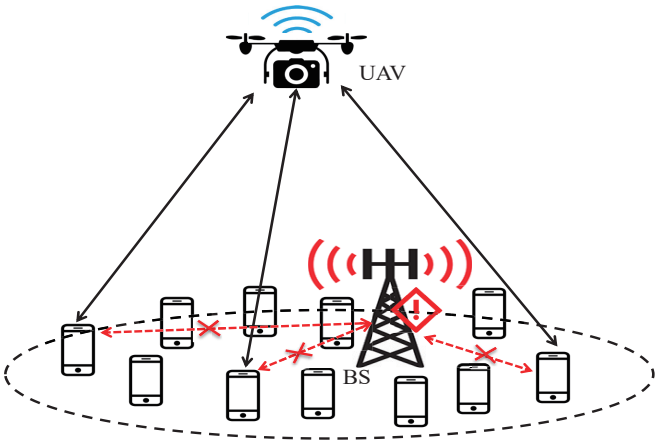

Figure 1.4: UAV-assisted Communication System.

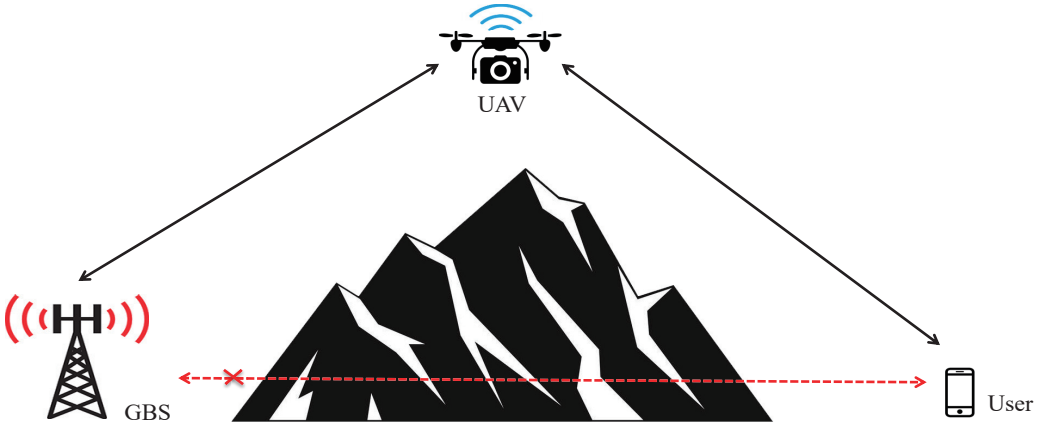

Figure 1.5: UAV relaying Communication System.

load in frequency-division-duplex (FDD) implementation, shown in Fig. 1.3 [44]. This is because the number of downlink resources needed for pilots will be proportional to the number of BS antennas and the required bandwidth of CSI feedback becomes large. As such, it is of great practical importance to study transmission schemes requiring partial CSI for massive MIMO systems.

1.1.4 Unmanned Aerial Vehicle based Networks

UAV or drone, which is an aircraft without a human pilot aboard, has found a wide range of applications with high mobility and low cost over the last decades [45]. UAVs are primarily used for excessive risky military missions, such as providing battlefield

intelligence or attack capability. With the cost reduction, UAVs can be used in commercial or scientific domains including weather monitoring, cargo transport, traffic control and others [46]. Thus, the implementation of UAVs can be seen as an alternative solution for wireless communications. In particular, UAVs can be deployed to extend the coverage area and enhance the capacity over wireless communications [47, 48, 49]. For example, the deployment of UAVs can assist the existing cellular networks to enhance the reliability in some emergency environments, such as natural disasters or temporary crowded events, shown in Fig. 1.4 [49]. In this scenario, some mobile users in this extremely crowded area can access the cellular networks by the assistant of UAV rather than the overloaded BS. Besides, UAVs can be implemented as a relay to provide coverage extension between the ground base station (GBS) and distant users without direct communication links, shown in Fig. 1.5 [50]. Apart from the benefit of providing reliable and cost-effective deployment for unexpected situations, UAV-assisted wireless communication can establish light-of-sight (LoS) communication links between UAV and the ground users to improve network performance.

Although UAV-assisted wireless communications have several advantages, they are still faced with many challenges. First, UAV-assisted wireless communications may transmit potentially sensitive information such as patient health information in natural disasters or military information in military operations. Due to the broadcast nature of wireless channels, security issues are playing an increasingly important role in UAV-assisted wireless communications. Thus, it is necessary to design security mechanisms for UAV-assisted wireless communications. Besides, the high mobility of UAV-assisted wireless communications can result in dynamic network topologies. As such, for guaranteeing reliable connectivity, UAV swarm communication and control architectures need to be designed [51]. Furthermore, due to the size, weight, flight time duration constraints of UAVs, energy-efficient UAV mechanisms are needed to maximize the time of the communication coverage with minimizing energy consumption. Lastly, interference coordination from the neighbouring cells over multiple-cell wireless communication with UAV is more changeling because of the mobility of UAVs and the lack of centralized control. These results in effective interference managements need to be designed for UAV-assisted multiple-cell wireless communication.

1.2 Literature Survey

1.2.1 Physical Layer Security in Multiple Antennas Transmission

Multiple antennas transmission can significantly enhance the secrecy rate performance of wireless systems [52, 53, 54, 55]. In [56, 57, 58, 59, 60], the beamforming technique is employed to increase the SNR difference between a legitimate user and an eavesdropper over a MISO broadcast channel. Secrecy rate performance of MISO systems can also be improved with artificial noise (AN) [61, 62, 63]. AN injected in the transmitted signals can efficiently reduce eavesdropper's SNR [64]. In general, eavesdroppers are passive so that the transmitter cannot obtain their CSI. Thus, the effect of beamforming technique and AN on multiple antenna transmission has been investigated in [65, 66, 67] to enhance secrecy performance. Moreover, MU-MIMO transmission has been proposed by leveraging multiple users as spatially distributed transmission resources for secrecy performance enhancement [68], [69]. Particularly, the harmful multiuser interference in MU-MIMO transmission can disrupt the reception of the eavesdropper [4]. In [70], the authors investigate secrecy performance over an MU-MIMO transmission scenario when the full CSI of all the legitimate users is available to the transmitter. However, this assumption seems unrealistic since the feedback full of legitimate users' CSI can increase computational complexity and leads to the imperfect CSI. A robust beamforming scheme is proposed for the imperfect CSI case to enhance secrecy performance in [71]. Besides, the secrecy outage probability (SOP) is analyzed over an MU-MIMO transmission, along with the optimal mode selection (i.e. the number of scheduled users) [72]. In multiple antenna transmission, the secrecy performance of RUB scheme and AN enhanced RUB method for multiple antenna transmission have not been fully considered in the literature. Chapter 2 will investigate secrecy performance of RUB over multiple-input single-output single-eavesdropper (MISOSE) and multiuser multiple-input multiple-output single-eavesdropper (MU-MIMOSE) broadcast channels.

1.2.2 Physical Layer Security in Massive MIMO Systems

Compared with multiple antenna transmission, massive MIMO is inherently more secure, as a large antenna element equipped at the BS can accurately serve the narrow and directional information beam on the legitimate user in the presence of passive

eavesdroppers. Thus, many research have focused on the study of secrecy performance over massive MIMO transmission. In [73], the authors investigate a multi-cell massive MIMO system in the presence of a passive eavesdropper in TDD operation at the BS where achievable ergodic secrecy rate and the SOP have been analyzed applied MF precoder and AN generation. As an extension, ZF precoder, polynomial data precoder and AN generation are employed in [74]. Besides, PLS over massive MIMO relay channel and massive MIMO Rician channel have been investigated in [75], and [76], respectively. All of the authors of [73, 77, 74, 75, 76] assumes that full CSI of legitimate users is available at the BS. However, the estimated uplink CSI may not match the actual downlink CSI when the BS performs transmission. When the CSI needs to be fed back from the users, as in FDD implementation, these full CSI based beamforming schemes will incur large feedback load. Thus, a beam domain transmission with statistical CSI of users has been proposed in [78] over single-cell FDD massive MIMO communications. The work in [78] is further extended to the scenario where the required statistical CSI of legitimate users and eavesdroppers is available at the BS over an FDD massive MIMO transmission. However, there are still few works on RUB design with partial CSI at the BS in the literature. Chapter 3 will investigate the secrecy performance of RUB over massive multiple-input multiple-output multiple-eavesdropper (MIMOME) broadcast channels.

1.2.3 Physical Layer Security in UAV based Networks

UAV can enhance communication reliability in the environment by acting as a relay to assist the existing wireless communication systems. Meanwhile, UAV-assisted relaying systems face serious security challenges. Many research works have studied the secrecy performance of UAV-assisted relaying communication systems in the presence of one or more eavesdroppers [79, 80]. The SOP performance analysis is carried out in a UAV-assisted network with multiple UAV transmitters, multiple UAV relays in the presence of multiple UAV eavesdroppers [81]. A ground communication network consisting of a transmitter, a legitimate user, and an eavesdropper with the deployment of a UAV jammer is analyzed [82]. In [83], the authors study a UAV-assisted jamming scheme for improving the secrecy rate of the ground wiretap channel. Besides, the secrecy performance of the UAV-assisted relaying system has also been investigated in [84, 85, 86]. Furthermore, multiple eavesdroppers considered as non-cooperation are often assumed to operate independently, whereas these eavesdroppers may coop-

erative to enhance their eavesdropping capability. In [87], the authors investigate the secrecy performance of a UAV-assisted relaying system with multiple non-cooperative ground eavesdroppers following an independent homogeneous Poisson point process (PPP). In [88], the SOP is derived for a secure communication system in the presence of multiple cooperative UAV eavesdroppers with the help of UAV swarm relay in the three-dimensional space. From chapter 4, we will investigate secrecy performance analysis for UAV-assisted relaying communication systems in the presence of single and/or multiple eavesdroppers.

1.3 Thesis Outline

In this thesis, we study secrecy performance in emerging wireless transmission systems. We first consider PLS design and analysis for ground-based networks employing the RUB scheme at the transmitter. Then, we investigate UAV-based networks with PLS. Each of chapters 2-6 in this thesis is self-contained and included in separate journal or conference papers.

In Chapter 2, we investigate the secrecy performance of RUB transmission over MISOSE and MU-MIMOSE channels. We also propose a novel RUB-based AN method for multiple antennas communication systems. We derive the closed-form expressions of the exact and the asymptotic ergodic secrecy rate and the SOP for these transmission scenarios. Numerical results are presented to illustrate the trade-off between performance and complexity of the resulting physical layer security design. We show that the deployment of RUB and RUB-based AN offers an attractive solution for enhancing the security of wireless transmission systems.

In Chapter 3, we consider the downlink transmission over a massive MIMOME channel employing RUB scheme. We concentrate on the practical scenario where partial CSI of legitimate users and no CSI of eavesdroppers are available at the BS and consider both types of eavesdroppers including the non-colluding and colluding eavesdroppers. We derive the closed-form expressions of ergodic secrecy rate for RUB based massive MIMOME transmission, and its single legitimate user particular case. We also present numerical results to illustrate the performance-complexity tradeoff among different massive MIMO transmission schemes. We show that RUB based scheme can enhance secrecy performance of massive MIMO transmission with lower implementation complexity.

In Chapter 4, we study a UAV-assisted relaying communication system, where a

GBS intends to send information to a legitimate ground user with the help of a UAV relay, in the presence of a passive ground eavesdropper. In particular, assuming an urban operating environment, we analyze and derive the closed-form approximation of the intercept probability and the ergodic secrecy rate. Through analytical and numerical results, we examine the effect of different system parameters on secrecy performance.

In Chapter 5, we study the secrecy performance of a UAV-assisted relay communication system, where a GBS intends to send confidential information to the ground legitimate user with the help of a UAV relay in the presence of multiple aerial and ground eavesdroppers. To enhance the secrecy performance, the GBS and the UAV relay apply directional beamforming transmission while implementing protection zones around their intended receiving destinations. Assuming the general κ-μ shadowed fading model, we derive the exact closed-form expressions of the SOP with/without aerial and ground eavesdroppers cooperation cases. Through selected numerical results, we examine the effect of different system parameters on the overall SOP performance.

In Chapter 6, we study the secure information transmission from a GBS to a legitimate UAV user, in the presence of multiple UAV eavesdroppers. To enhance the secrecy performance, the GBS applies beamforming transmission while enforcing a protection zone around it. Utilizing the general κ-μ shadowed fading distribution to model the ground-to-air channel, we derive the exact closed-form expression of the SOP. To further facilitate performance evaluation, we adopt a data-driven approach and develop a deep learning model that can predict the SOP performance with high accuracy and short computation time. Through selected numerical results, we examine the effect of different system parameters on the SOP performance.

In Chapter 7, we summarize this thesis and outline the future works.

Chapter 2

Secrecy Performance Analysis of Multiple Antenna Transmission with Random Unitary Beamforming

2.1 Introduction

Transmit beamforming can achieve diversity gain as well as array gain for enhancing secrecy performance and most previous research on beamforming transmission assume that the exact and full channel state information (CSI) of the legitimate user, and even that of eavesdroppers are available at the transmitter [89, 90, 91, 92]. In [93], although the statistical CSI of uniformly distributed eavesdroppers is assumed, the full CSI of the legitimate user is still required at the transmitter. Both legitimate user's full CSI and eavesdropper's partial CSI are assumed to be available at the transmitter in [61], [94]. However, providing full CSI of legitimate users at the transmitter can be challenging in practice, due to, for example, the limited feedback channel bandwidth in frequency-division-duplex (FDD) systems [95] and the increasing computational complexity. Furthermore, it will be unrealistic to assume any CSI about the eavesdroppers when the transmitter is unaware of their existence. Thus, it is of considerable interest to extract the array gain and enhance secrecy performance with partial CSI of legitimate users and no CSI of eavesdroppers at the transmitter. In [68], [96], the quantized CSI of the legitimate user is assumed at the transmit-

ter, leading to a limited feedback solution. Meanwhile, the quantization codebook is predetermined based on channel gain, still rendering the very complex design.

Artificial noise (AN) techniques can also enhance secrecy performance over multiple antenna transmission since as the AN is placed in the null space of the legitimate user's channel, and hence affects the eavesdropper channel only [61, 62, 63, 64]. The effect of both conventional beamforming and AN on secure transmission has also been studied in [65, 66, 67]. Such implementation requires that the full CSI of the legitimate user to be known at the transmitter. Thus, either the conventional beamforming or the conventional AN is adopted in the wireless systems with a cost of increasing computational complexity.

Random unitary beamforming (RUB) is a low-complexity scheme for multiple antenna transmission, only requiring partial CSI at the transmitter. With RUB scheme, each user feeds back some quality information of each beam and Alice transmits to the user with particular beam based on the feedback information of this user. Moreover, employing novel RUB-based AN, requiring the feedback information of the beam index from RUB scheme, is also an attractive low-complexity method to enhance secrecy performance. To the best of the authors' knowledge, the secrecy performance of RUB scheme and AN enhanced RUB method for multiple antenna transmission has not been fully investigated in the literature.

In this chapter, we propose to apply RUB scheme over multiple antenna transmission for enhancing the secrecy performance of a legitimate user in a wiretap environment. We examine the practical scenarios that Alice has only partial CSI for Bob and no CSI knowledge about Eve. Both single user transmission and multiple user transmission cases with user scheduling are considered. The effect of RUB-based AN method on single user transmission is also investigated. The major contributions of this chapter can be summarized as follows:

1. We investigate the secrecy performance of RUB scheme over multiple-input single-output single-eavesdropper (MISOSE) broadcast channel. The exact closed-form expressions of ergodic secrecy rate and the secrecy outage probability (SOP) are derived. We also present compact expressions for the asymptotic ergodic secrecy rate and the asymptotic SOP for this scenario.

2. The effect of RUB-based AN method on the MISOSE channel is investigated. The analytical expression of ergodic secrecy rate is obtained and the exact closed-form expression of SOP is derived. We show that RUB-based AN method

can enhance the secrecy performance of transmission over low signal-to-noise ratio (SNR) region.

3. We carry out a thorough secrecy performance analysis of RUB scheme over multiuser multiple-input multiple-output single-eavesdropper (MU-MIMOSE) channel. The exact closed-form expressions of ergodic secrecy rate and the SOP are obtained. We show that RUB scheme over MU-MIMOSE channel can effectively enhance the secrecy performance over low signal to interference plus noise ratio (SINR) region since the harmful multiuser interference can disrupt the reception of the eavesdropper.

The remainder of this chapter is organized as follows. The system and channel models are presented in Section 2.2. The secrecy performance analysis of the proposed RUB design for MISOSE scenario is presented in Section 2.3. The effect of RUB-based AN method is investigated in Section 2.4. The RUB design over MU-MIMOSE channel is presented and studied in Section 2.5. Finally, we draw our conclusions in Section 2.6.

2.2 System Model and Channel Models

We consider the downlink transmission from a transmitter Alice to a legitimate user Bob in the presence of an eavesdropper Eve, shown in Fig. 6.1. Alice is equipped with M antennas and therefore can serve a single or M users simultaneously. Meanwhile, Bob is either the single scheduled user or one of M scheduled users among N legitimate users. Legitimate users and Eve have only a single antenna. We assume Alice adopts RUB scheme to serve the scheduled users. In particular, Alice will serve Bob using one of M random orthonormal beams, generated from an isotropic distribution [36]. The set of beamforming vectors, denoted by $\mathcal{U} = [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_M]$, is assumed to be unknown to Eve.

We assume that the wireless channel introduces path loss and Rayleigh fading effects. In particular, the path loss effect follows the log-distance model. The path loss over the link from Alice to the legitimate user j, $j = 1, 2, \cdots, N$, is characterized by average power gain $Kd_j^{-\alpha}$, where K is the path loss constant, d_j is the distance between Alice and the legitimate user j, and α is the path loss exponent of the environment. Also, the path loss over the link from Alice to Eve is characterized by

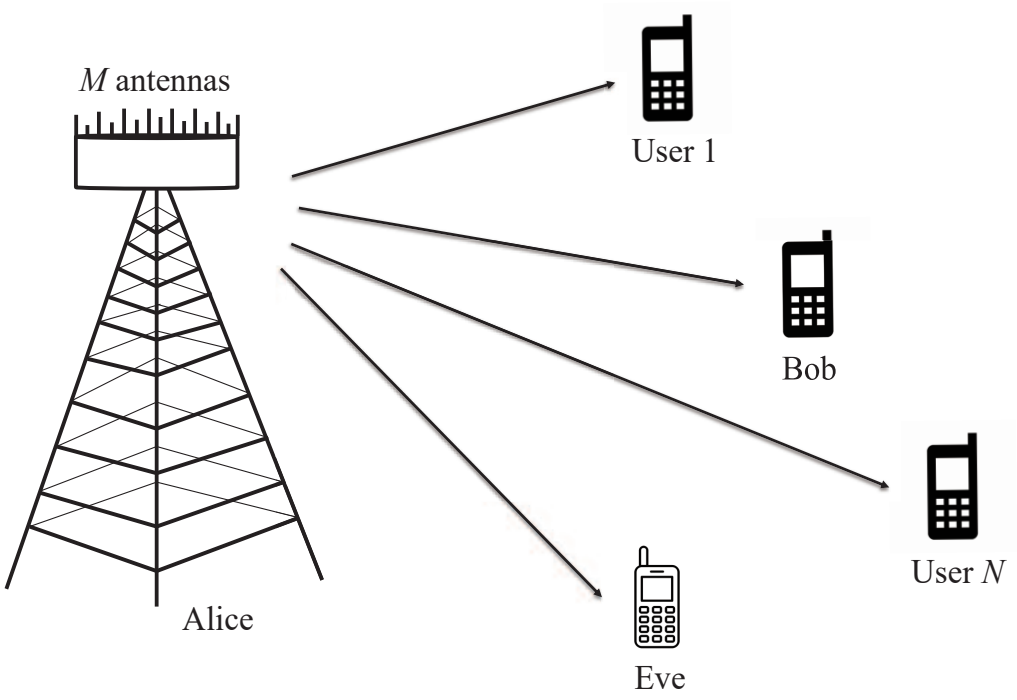

Figure 2.1: Single-cell downlink transmission in the presence of a passive eavesdropper.

average power gain $Kd_E^{-\alpha}$, where d_E is the distance between Alice and Eve. Considering Rayleigh fading model, the channel gains from the ith antenna of Alice to the legitimate user j and Eve, denoted by $h_{j,i}$ and $h_{E,i}$, respectively, are assumed to be independent and identically distributed (i.i.d) complex Gaussian random variable with zero mean and unitary variance, i.e. $h_{j,i} \sim \mathcal{CN}(0,1)$ and $h_{E,i} \sim \mathcal{CN}(0,1)$.

2.3 RUB Transmission over MISOSE Channel

In this section, we assume that Bob is a single scheduled user out of N candidate legitimate users in the presence of Eve. That is, MISOSE transmission is considered. The transmitted signal vector from Alice's M antennas over a single symbol period can be written as:

$$\mathbf{x} = \mathbf{u}_i s, \tag{2.1}$$

where $\mathbf{u}_i$ is the selected beamforming vector and s represents the information symbol. Let P denotes the maximum average power of the transmitted symbol vector $\mathbf{x}$. We

have $\mathbb{E}[|\mathbf{x}^H\mathbf{x}|] \leq P$. Thus, the received symbol at legitimate user j can be expressed as

$$y_j = Kd_j^{-\alpha}\mathbf{h}_j^T\mathbf{u}_i s + n_j, \tag{2.2}$$

where $\mathbf{h}_j = [h_{j,1}, h_{j,2}, \cdots, h_{j,M}]^T$ represents the fading channel vector, and n_j denotes additive Gaussian noise assumed with zero mean and variance N_0. Similarly, the received symbol at Eve can be expressed as

$$y_E = Kd_E^{-\alpha}\mathbf{h}_E^T\mathbf{u}_i s + n_E, \tag{2.3}$$

where $\mathbf{h}_E = [h_{E,1}, h_{E,2}, \cdots, h_{E,M}]^T$ is the vector of fading channel gains for Eve and n_E denotes additive Gaussian noise with zero mean and variance N_0. Consequently, the received SNR at legitimate user j on beam i is given by

$$\gamma_{j,i} = \frac{Kd_j^{-\alpha}\mathbb{E}[|\mathbf{h}_j^T\mathbf{u}_i s|^2]}{N_0} = \rho d_j^{-\alpha}|\mathbf{h}_j^T\mathbf{u}_i|^2, \tag{2.4}$$

where $\rho = \frac{PK}{N_0}$. For long term fairness among legitimate users, we assume that the transmitter adopts power control to mitigate path loss difference among users. As such, all candidate users have the same average SNR of $\overline{\gamma}_B = \rho d_B^{-\alpha}$, where d_B denotes the effective common distance of legitimate users. Likewise, the received SNR at Eve is given by

$$\gamma_E = \frac{Kd_E^{-\alpha}\mathbb{E}[|\mathbf{h}_E^T\mathbf{u}_i s|^2]}{N_0} = \rho d_E^{-\alpha}|\mathbf{h}_E^T\mathbf{u}_i|^2. \tag{2.5}$$

With RUB transmission, we apply best beam selection together with user scheduling to improve the legitimate user channel capacity. In particular, each user finds its best beam based on the instantaneous channel condition. We assume that each legitimate user can estimate its instantaneous channel vector $\mathbf{h}_j$'s based on, for example, the pilot symbols sent by Alice. With the knowledge of beamforming vectors $\mathcal{U}$, the user can evaluate the instantaneous received SNR on various beams using (2.4). Then, each user sends its best beam index and the corresponding SNR value to Alice as feedback information. For instance, if the i^*th beam results in the maximum SNR for legitimate user j, i.e. $\gamma_{j,i^*} = \max\{\gamma_{j,i}\}$, where $i \in \{1, 2, \cdots, M\}$, user j will feed back a finite integer for the beam index i^* and a real number for the SNR value γ_{j,i^*}. Note that the feedback load of this scheme is one finite integer and one real number per user. Based on the feedback information, Alice schedules the user with the largest SNR value among N users and serves it using the corresponding beam. Particularly,

if γ_{j^*,i^*} is the largest one among N feedback SNRs, then Alice transmits to user j^* (Bob) with beam i^*. As such, Alice transmits to the user with highest best beam SNR.

In the following, we analyze the secrecy performance of the proposed design in terms of ergodic secrecy rate and SOP.

2.3.1 Ergodic Secrecy Rate

Non-zero secrecy rate exists when the scheduled user Bob's received SNR γ_B is greater than the eavesdropper Eve's received SNR γ_E. Thus, the instantaneous secrecy rate per unit bandwidth is expressed as the capacity difference between the legitimate user's instantaneous channel and the eavesdropper's instantaneous channel, given by [6]

$$C_s = \begin{cases} \log_2(1+\gamma_B) - \log_2(1+\gamma_E), & \text{if} \quad \gamma_B > \gamma_E; \\ 0, & \text{if} \quad \gamma_B \leq \gamma_E. \end{cases} \tag{2.6}$$

The ergodic secrecy rate can be calculated as

$$\mathbb{E}[C_s] = \int_0^\infty \left[\int_{\gamma_E}^\infty \big(\log_2(1+\gamma_B) - \log_2(1+\gamma_E) \big) p_{\gamma_B}(x) dx \right] p_{\gamma_E}(y) dy, \tag{2.7}$$

where $p_{\gamma_B}(x)$ and $p_{\gamma_E}(y)$ denote the probability density function (PDF) of the received SNR at Bob and Eve, respectively.

Exact Analysis

The projection of the legitimate user j's channel vector onto M beamforming vectors, $|\mathbf{h}_j^T \mathbf{u}_i|$'s are i.i.d since the beamforming vectors are orthonormal, i.e. $\mathbf{u}_i^T \mathbf{u}_j = 1$ when $i = j$, and 0 otherwise. Therefore, the PDF of the jth user's received SNR on the ith beam can be obtained as

$$p_{\gamma_{j,i}}(x) = \frac{1}{\overline{\gamma}_B} \exp\left(-\frac{x}{\overline{\gamma}_B} \right). \tag{2.8}$$

Since Alice schedules the user (Bob) with the largest feedback SNR among N users, the received SNR at Bob on the selected beam is equivalent to the largest one among $M \times N$ i.i.d exponential random variables. As such, the PDF and CDF of the received

SNR at Bob on the selected beam can be obtained as

$$p_{\gamma_B}(x) = \frac{MN}{\overline{\gamma}_B}\left(1 - \exp\left(-\frac{x}{\overline{\gamma}_B}\right)\right)^{MN-1} \exp\left(-\frac{x}{\overline{\gamma}_B}\right), \tag{2.9}$$

and

$$F_{\gamma_B}(x) = \left(1 - \exp\left(-\frac{x}{\overline{\gamma}_B}\right)\right)^{MN}, \tag{2.10}$$

respectively.

Since Alice selects beamforming vector based on the feedback information from the legitimate users, the chosen vector appears arbitrary to Eve. As such, we obtain the PDF and the cumulative distribution function (CDF) of the received SNR at Eve as [65]

$$p_{\gamma_E}(y) = \frac{1}{\overline{\gamma}_E} \exp\left(-\frac{y}{\overline{\gamma}_E}\right), \tag{2.11}$$

and

$$F_{\gamma_E}(y) = 1 - \exp\left(-\frac{y}{\overline{\gamma}_E}\right), \tag{2.12}$$

respectively, where the average SNR $\overline{\gamma}_E = \rho d_E^{-\alpha}$. after substituting (2.9) and (2.11) into (2.7), applying the binomial expansion [97, eq.(1.111)], and performing integration, the closed-form expression of ergodic secrecy rate of the RUB transmission over MISOSE channel can be obtained as

$$\begin{aligned}\mathbb{E}[C_s] = \frac{MN}{\ln 2} \sum_{i=0}^{MN-1} \binom{MN-1}{i} \frac{(-1)^i}{i+1} \Bigg[E_1\left(\frac{i+1}{\rho d_B^{-\alpha}}\right) \\ - E_1\left(\frac{i+1}{\rho d_B^{-\alpha}} + \frac{1}{\rho d_E^{-\alpha}}\right) \exp\left(\frac{1}{\rho d_E^{-\alpha}}\right) \Bigg] \exp\left(\frac{i+1}{\rho d_B^{-\alpha}}\right),\end{aligned} \tag{2.13}$$

where $E_1(x) = \int_1^\infty \frac{e^{-xt}}{t} dt$ denotes the exponential integral function.

Asymptotic Analysis

We now investigate the asymptotic ergodic secrecy rate of RUB transmission in the high SNR region. Specifically, we assume that Bob is located near Alice, which means $\overline{\gamma}_B \to \infty$, and the distance from Alice to Eve is arbitrary.

To facilitate the asymptotic analysis, we calculate the ergodic secrecy rate as

$$\mathbb{E}[C_s] = \frac{1}{\ln 2}\int_0^\infty \left[\int_0^x \frac{F_{\gamma_E}(y)}{1+y}dy\right] p_{\gamma_B}(x)dx. \tag{2.14}$$

Rewriting the CDF of γ_E as $1-[1-F_{\gamma_E}(y)]$, and substituting into (2.14), we obtain

$$\mathbb{E}[C_s] = C_1 - C_2, \tag{2.15}$$

where

$$C_1 = \frac{1}{\ln 2}\int_0^\infty \ln(1+x)p_{\gamma_B}(x)dx, \tag{2.16}$$

and

$$C_2 = \frac{1}{\ln 2}\int_0^\infty \left[\int_0^x \frac{1-F_{\gamma_E}(y)}{1+y}dy\right] p_{\gamma_B}(x)dx. \tag{2.17}$$

When $x \to \infty$, $\ln(1+x) \approx \ln(x)$, then the asymptotic expression of C_1 can be obtained, and employing [97, eq.(1.111) and eq.(4.331.1)], the asymptotic expression of C_1 can be obtained as

$$C_1^\infty = \frac{MN}{\ln 2}\left(\ln(\overline{\gamma}_B) - \sum_{i=0}^{MN-1}\binom{MN-1}{i}\frac{(-1)^i}{i+1}\Big[\ln(i+1)+\mathcal{E}\Big]\right), \tag{2.18}$$

where $\mathcal{E}$ is the Euler's constant [97, eq.(8.367.1)]. We note that C_1^∞ presents the impact of Alice-to-Bob channel on the ergodic secrecy rate. Changing the order of integration and noting $F_{\gamma_B}(y) \approx 0$ as $\overline{\gamma}_B \to \infty$. the asymptotic expression of C_2 can be expressed as

$$C_2^\infty = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_{\gamma_E}(y)}{1+y}dy. \tag{2.19}$$

Substituting (2.12) into (2.19), the asymptotic expression of C_2 is derived as

$$C_2^\infty = \frac{1}{\ln 2}E_1\left(\frac{1}{\overline{\gamma}_E}\right)\exp\left(\frac{1}{\overline{\gamma}_E}\right), \tag{2.20}$$

which characterizes the impact of Alice-to-Eve channel on the ergodic secrecy rate. According to (2.18) and (2.20), the asymptotic ergodic secrecy rate can be determined

as

$$\overline{C}_s^{\infty} = \frac{MN}{\ln 2}\Bigg[\ln(\overline{\gamma}_B) - \sum_{i=0}^{MN-1}\binom{MN-1}{i}\frac{(-1)^i}{i+1}\Big[\ln(i+1)+\mathcal{E}\Big] - \frac{1}{MN}E_1\left(\frac{1}{\overline{\gamma}_E}\right)\exp\left(\frac{1}{\overline{\gamma}_E}\right)\Bigg]. \tag{2.21}$$

2.3.2 Secrecy Outage Probability

Exact Analysis

The SOP is the probability that the instantaneous secrecy rate C_s is less than the target secrecy rate R_s, defined as

$$P_{\text{out}}(R_s) = \Pr[C_s < R_s]. \tag{2.22}$$

Using (6.21) and conditioning on γ_E, the SOP of RUB-based MISOSE transmission can be calculated as

$$P_{\text{out}}(R_s) = \int_0^{\infty} p_{\gamma_E}(y)\left[\int_0^{2^{R_s}(1+y)-1} p_{\gamma_B}(x)dx\right]dy. \tag{2.23}$$

After substituting (2.9) and (2.11) into (2.23), applying the binomial expansion [97, eq.(1.111)], and performing integration, we obtain the closed-form expression of the SOP as

$$P_{\text{out}}(R_s) = 1 - \left(\frac{MN}{MN-1}\right)\sum_{i=0}^{MN-1}\binom{MN-1}{i}\frac{(-1)^{MN-i-1}d_B^{-\alpha}}{d_B^{-\alpha}+2^{R_s}(MN-i)d_E^{-\alpha}} \exp\left(-\frac{(MN-i)2^{R_s}-1}{\rho d_B^{-\alpha}}\right). \tag{2.24}$$

Asymptotic Analysis

We now derive the asymptotic SOP of RUB transmission over MISOSE channel in high SNR region, where Bob is located close to Alice with $\overline{\gamma}_B \to \infty$.

The asymptotic SOP is derived as

$$P_{\text{out}}^{\infty}(R_s) = \int_0^{\infty} p_{\gamma_E}(x)F_{\gamma_B}^{\infty}[2^{Rs}(1+x)-1]dx, \tag{2.25}$$

where $F_{\gamma_B}^{\infty}(x)$ is the asymptotic CDF of the received SNR at Bob in high SNR region. Based on (2.10), the asymptotic CDF of γ_B is given by

$$F_{\gamma_B}^{\infty}(x) = \left(\frac{x}{\overline{\gamma}_B}\right)^{MN}. \tag{2.26}$$

Substituting (2.26) into (2.25) and employing [97, eq.(3.382.4)], we obtain the asymptotic SOP as

$$P_{\text{out}}^{\infty}(R_s) = (G_a\overline{\gamma}_B)^{-G_d} + o\left(\overline{\gamma}_B^{-G_d}\right), \tag{2.27}$$

where the secrecy diversity order is

$$G_d = MN \tag{2.28}$$

and the secrecy array gain is

$$G_a = \left(\frac{\overline{\gamma}_E}{2^{R_s}}\right)\left[\Gamma\left(MN+1, \left(1-\frac{1}{2^{R_s}}\right)\frac{1}{\overline{\gamma}_E}\right)\exp\left(\left(1-\frac{1}{2^{R_s}}\right)\frac{1}{\overline{\gamma}_E}\right)\right]^{-\frac{1}{MN}}, \tag{2.29}$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function. We note that antenna configuration and user scheduling in Alice-to-Bob channel determine the secrecy diversity order. The secrecy array gain is influenced by antenna configuration, user scheduling over Alice-to-Bob channel, target secrecy rate and the average SNR of Alice-to-Eve channel.

2.3.3 Numerical Results

Fig. 2.2 plots the ergodic secrecy rate of ZFBF and RUB schemes over MISOSE transmission versus the distance d_B. We can see that the ergodic secrecy rate of both schemes decline as the distance d_B increases. We also note that the ergodic secrecy rate has a growing trend as the antenna number M increases. The asymptotic curves for RUB scheme well approximate the exact curves in high SNR region. With the same number of antennas, the results show that the performance of ZFBF scheme slightly outperforms that of RUB scheme. However, RUB scheme has lower complexity since legitimate users just feed back the best beam index as the partial CSI information to the transmitter. We can also note that the performance gap between these two methods is not large. Thus, RUB scheme serves as a low complexity solution to

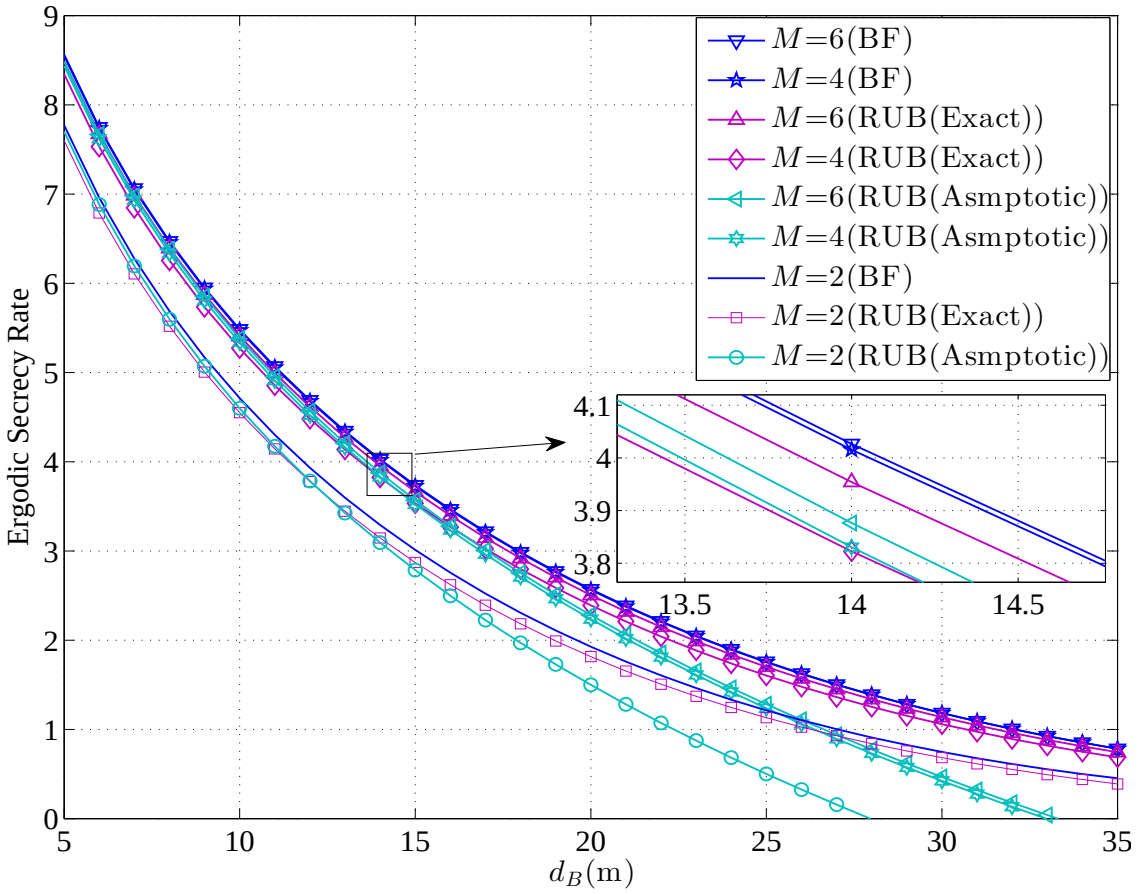

Figure 2.2: Ergodic secrecy rate of ZFBF and RUB (exact and asymptotic) versus d_B with different M ($N = 7$, $d_E = 30$ m, $\rho = 90$ dB, $\alpha = 3.1$).

enhance the secrecy performance of wireless transmission systems.

Fig. 2.3 depicts the SOP performance comparison between ZFBF and RUB (exact and asymptotic) schemes with different number of users N when the distance d_E is fixed to 30 m. The SOP of both schemes increases with the growth of distance d_B since the average SNR of the legitimate user channel decreases with increasing d_B. For RUB scheme, the asymptotic SOP declines with the increasing number of users in high SNR region. The SOP of both schemes decreases as the number of users increases, which shows that user selection plays a positive role in reducing the SOP. With the same number of users, the result indicates that the proposed method underperforms ZFBF scheme. However, with ZFBF, Alice typically obtains the channel knowledge to legitimate users through feedback, which presents an overhead of the system and might be explored by Eve. With our RUB design, Eve hardly gets any information

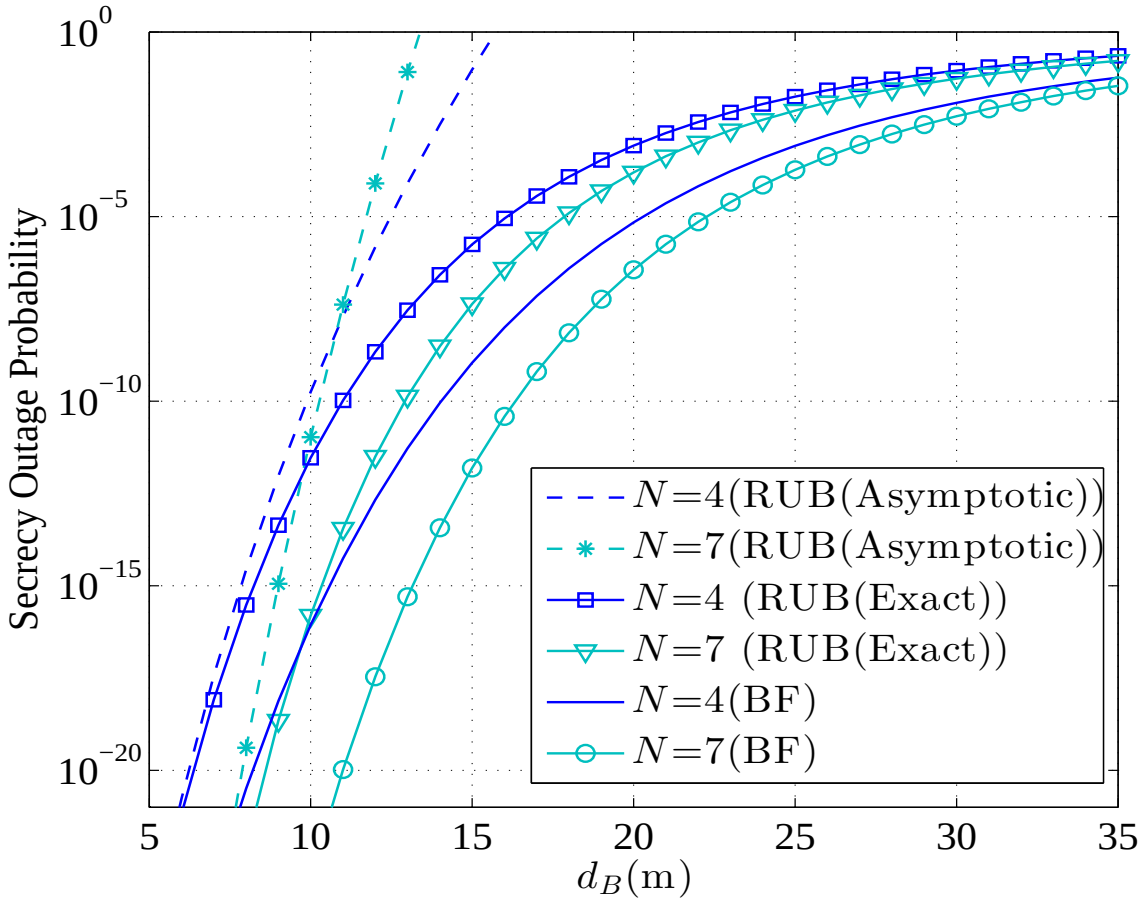

Figure 2.3: Secrecy outage probability comparison between ZFBF and RUB (exact and asymptotic) versus d_B with different N ($M = 4$, $d_E = 30$ m, $\rho = 90$ dB, $\alpha = 3.1$, $R_s = 0.1$ bit/s).

on beamforming design from the feedback beam index. Therefore, the RUB scheme serves as an attractive alternative in achieving PLS.

2.4 Effect of Artificial Noise

In this section, we consider the application of AN in the RUB-based MISOSE transmission. With the conventional beamforming, such as ZFBF, AN is injected to the null space of the legitimate user's channel, which requires full CSI of legitimate user at the transmitter. For RUB-based AN transmission, AN should be injected based on the feedback information of the beam index. Specifically, we propose to transmit AN on the beam that leads to the minimum interference at the scheduled legitimate

user, Bob. As a result, Bob will need to feed back the index of its worst beam to Alice.

The transmitted symbol from Alice can be written as

$$\mathbf{x}^{'} = \sqrt{\lambda P}\mathbf{u}_i s + \sqrt{(1-\lambda)P}\mathbf{u}_j n_a, \tag{2.30}$$

where $\mathbf{u}_i$ is the best beam for Bob, $\mathbf{u}_j$ is the worst beam for Bob, n_a is the injected noise symbol with unit energy, and λ is the power allocation coefficient between the information symbol and noise symbol.

The received symbol at Bob and Eve are given by

$$y_B^{'} = K d_B^{-\alpha} \mathbf{h}_B^T (\sqrt{\lambda P}\mathbf{u}_i s + \sqrt{(1-\lambda)P}\mathbf{u}_j n_a) + n_B, \tag{2.31}$$

and

$$y_E^{'} = K d_E^{-\alpha} \mathbf{h}_E^T (\sqrt{\lambda P}\mathbf{u}_i s + \sqrt{(1-\lambda)P}\mathbf{u}_j n_a) + n_E, \tag{2.32}$$

respectively. Thus, the received SINR at Bob and Eve is given by

$$\gamma_B^{'} = \frac{K d_B^{-\alpha} \lambda P |\mathbf{h}_B^T \mathbf{u}_i|^2}{K d_B^{-\alpha}(1-\lambda)P|\mathbf{h}_B^T \mathbf{u}_j|^2 + N_0} = \frac{|\mathbf{h}_B^T \mathbf{u}_i|^2}{(1/\lambda - 1)|\mathbf{h}_B^T \mathbf{u}_j|^2 + 1/\rho_B}, \tag{2.33}$$

where $\rho_B = \frac{\lambda P K d_B^{-\alpha}}{N_0}$, and

$$\gamma_E^{'} = \frac{|\mathbf{h}_E^T \mathbf{u}_i|^2}{(1/\lambda - 1)|\mathbf{h}_E^T \mathbf{u}_j|^2 + 1/\rho_E}, \tag{2.34}$$

where $\rho_E = \frac{\lambda P K d_E^{-\alpha}}{N_0}$, respectively. Note that AN for RUB scheme can degrade Eve's SNR at the expense of introducing a certain amount of interference at Bob. Since $\mathbf{u}_j$ is the worst beam for Bob and appears arbitrary to Eve, we expect AN degrades Eve's channel capacity more seriously, especially when the number of beams M is large.

2.4.1 Ergodic Secrecy Rate

To facilitate the following analysis, we rewrite (2.7) into

$$\mathbb{E}[C_s^{'}] = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E^{'}}(x)}{1+x}[1 - F_{\gamma_B^{'}}(x)]dx, \tag{2.35}$$

where $F_{\gamma_B^{'}}(x)$ and $F_{\gamma_E^{'}}(x)$ denote the CDF of the received SINR at Bob and Eve, respectively.

The received SINR at the scheduled user Bob can be calculated as

$$\gamma_B^{'} = \frac{z_B}{aw_B + 1/\rho_B}, \tag{2.36}$$

where $a = 1/\lambda - 1$, z_B is the largest one of $M \times N$ independent $\chi^2(2)$ distributed random variables, and w_B is the minimum of M independent $\chi^2(2)$ distributed ones. Conditioning on w_B, the PDF of the received SINR at Bob can be written as

$$\begin{aligned} p_{\gamma_B^{'}}(x) &= \int_0^{\infty} p_{\gamma_B|w_B}(x|w) p_{w_B}(w) dw \\ &= \int_0^{\infty} MN \left(aw + \frac{1}{\rho_B}\right) \exp\left(-\left(aw + \frac{1}{\rho_B}\right)x\right) \\ &\times \left[1 - \exp\left(-\left(aw + \frac{1}{\rho_B}\right)x\right)\right]^{MN-1} M e^{-Mw} dw. \end{aligned} \tag{2.37}$$

After applying the binomial theorem [97, eq.(1.111)] and performing integration, we obtain the following closed-form expression for $p_{\gamma_B^{'}}(x)$ as

$$p_{\gamma_B^{'}}(x) = M^2 N \sum_{i=0}^{MN-1} \binom{MN-1}{i} (-1)^i \frac{M + a[\rho_B + (1+i)x]}{\rho_B [M + a(1+i)x]^2} \exp\left(-\frac{(1+i)x}{\rho_B}\right). \tag{2.38}$$

The CDF of the received SINR at Bob with AN can be calculated as

$$F_{\gamma_B^{'}}(x) = M^2 N \sum_{i=0}^{MN-1} \binom{MN-1}{i} (-1)^i \left(\frac{1}{M(1+i)} - \frac{\exp\left(-\frac{(1+i)x}{\rho_B}\right)}{(1+i)[a(1+i)x + M]}\right). \tag{2.39}$$

Meanwhile, the beamforming vector appears arbitrary to Eve. As such, $|\mathbf{h}_E^T \mathbf{u}_i|^2$ and $|\mathbf{h}_E^T \mathbf{u}_j|^2$ have independent $\chi^2(2)$ distributions. Then, the PDF and the CDF of the received SINR at Eve can be determined as

$$p_{\gamma_E^{'}}(x) = \frac{e^{-x/\rho_E}}{(1+ax)^2} \left(\frac{1}{\rho_E}(1+ax) + a\right), \tag{2.40}$$

and

$$F_{\gamma_E^{'}}(x) = 1 - \frac{e^{-x/\rho_E}}{1+ax}. \tag{2.41}$$

Substituting (2.39) and (2.41) into (2.35), the ergodic secrecy rate of RUB-based AN

transmission over MISOSE channel can be obtained as

$$\mathbb{E}[C_s'] = \frac{1}{\ln 2}\int_0^{\infty} \frac{1-\frac{e^{-x/\rho_E}}{1+ax}}{1+x} \left(1 - M^2N\sum_{i=0}^{MN-1}\binom{MN-1}{i}(-1)^i\left(\frac{1}{M(1+i)} - \frac{e^{-\frac{(1+i)x}{\rho_B}}}{(1+i)[a(1+i)x+M]}\right)\right)dx. \tag{2.42}$$

Unfortunately, a closed-form expression can not be obtained due to the complicated integrand.

2.4.2 Secrecy Outage Probability

The SOP of RUB-based AN transmission can be calculated as [98]

$$P_{\text{out}}(R_s) = \int_0^{\infty} p_{\gamma_E'}(x) F_{\gamma_B'}[2^{R_s}(1+x)-1]dx. \tag{2.43}$$

Substituting (2.40) and (2.39) into (2.43), and after performing integration, the closed-form expression of the SOP for RUB-based AN MISOSE transmission can be obtained as

$$\begin{aligned} P_{\text{out}}(R_s) = &\sum_{i=0}^{MN-1}\binom{MN-1}{i}\frac{(-1)^i M^2 N}{1+i}\left(\frac{1}{M} - \frac{1}{a\rho_B\rho_E[(1+i)(2^{R_s}(1-a)-a)-M]^2}\right. \\ &\left(\rho_B\left(a\rho_E\Big((1+i)[2^{R_s}(a-1)-a+M]\Big) + \Big((1+i)\Big([2^{R_s}((\rho_E-1)a+1)+a]-M\Big)\Big)\right.\right. \\ &E_1\left(\frac{2^{-R_s}\left(\rho_B+2^{R_s}\rho_E(1+i)\right)\left(a(1+i)(2^{R_s}-1)+M\right)}{a\rho_B\rho_E(1+i)}\right) \\ &\left.\left.\exp\left(\frac{2^{-R_s}\left(a(1+i)\left(2^{R_s}-1\right)+M\right)\left(\rho_B+2^{R_s}\rho_E(1+i)\right)}{a\rho_B\rho_E(1+i)}\right)\right) \\ &-\ 2^{R_s}\rho_E(1+i)\Big((1+i)[2^{R_s}(a-1)+a(b-1)]+M\Big) \\ &\left.E_1\left(-\frac{\rho_B+2^{R_s}\rho_E(1+i)}{a\rho_B\rho_E}\right)\exp\left(-\frac{\rho_B+2^{R_s}\rho_E(1+i)}{a\rho_B\rho_E}\right)\right)\exp\left(-\frac{(1+i)(2^{R_s}-1)}{\rho_B}\right)\Big)\Big). \end{aligned} \tag{2.44}$$

2.4.3 Numerical Results

Fig. 2.4 illustrates that the ergodic secrecy rate of the RUB-based MISOSE transmission with/without AN versus the distance d_B for $M = 4$ and $N = 7$ case. We can

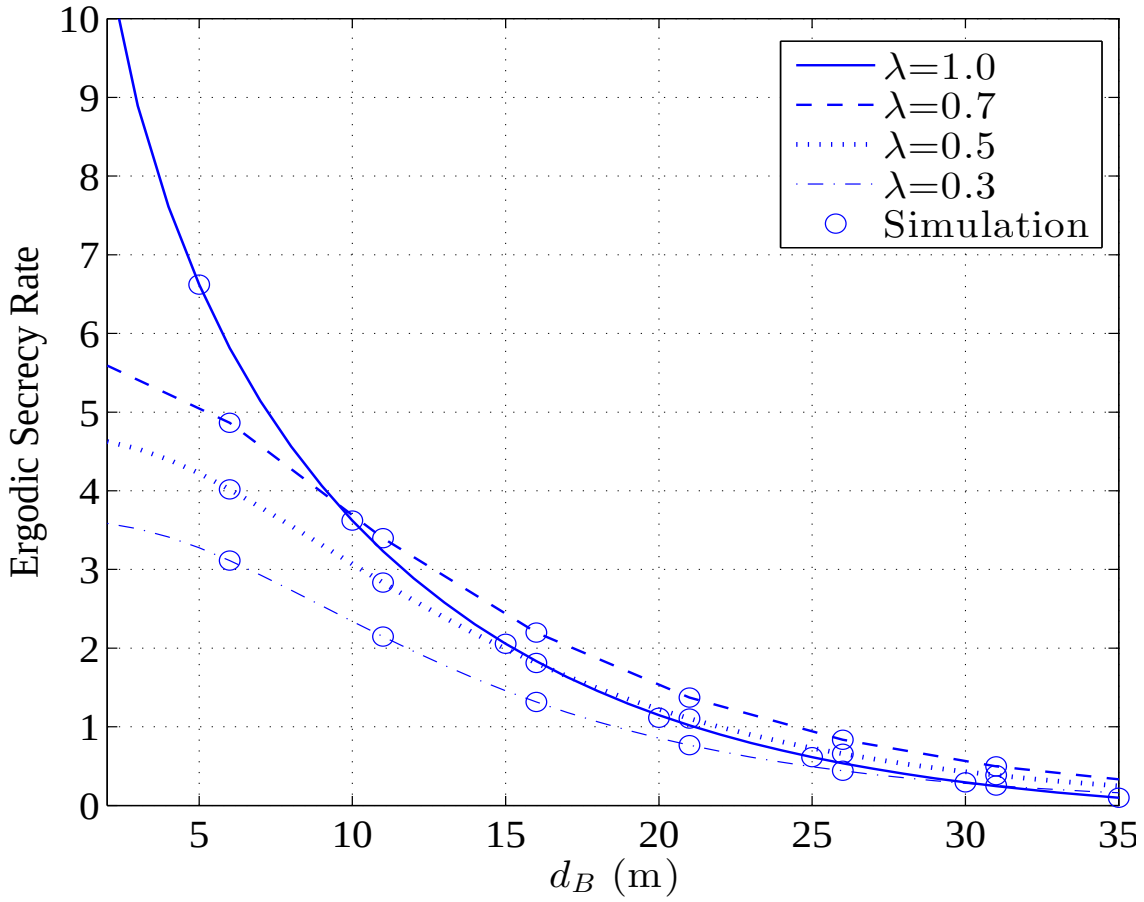

Figure 2.4: Ergodic secrecy rate of RUB-based MISOSE transmission with/without AN for different power allocation coefficient λ ($M = 4$, $N = 7$, $d_E = 30$ m, $\alpha = 3.1$, $R_s = 0.1$ bit/s).

see that AN has a mixed effect on the ergodic secrecy rate of RUB-based transmission over MISOSE channel. When the distance d_B is relatively small compared to d_E, AN degrades the secrecy performance, partly because of the introduction of interference to Bob's reception and partly because the transmit power is partially allocated to transmit noise symbols. Note that the secrecy rate decreases with the decrease of the power allocation factor λ. When the distance d_B is comparable with d_E, AN can considerably improve the secrecy rate of the transmission system if λ is larger than 0.5. In this scenario, the SNR degradation at Eve is more significant than the effect of added interference to Bob. Based on these observations, we can conclude that RUB-based transmission can benefit from AN only for the low SNR region and the power allocated to AN should not be greater than that used for data symbol transmission.

Fig. 2.5 shows that the SOP performance of RUB-based MISOSE transmission

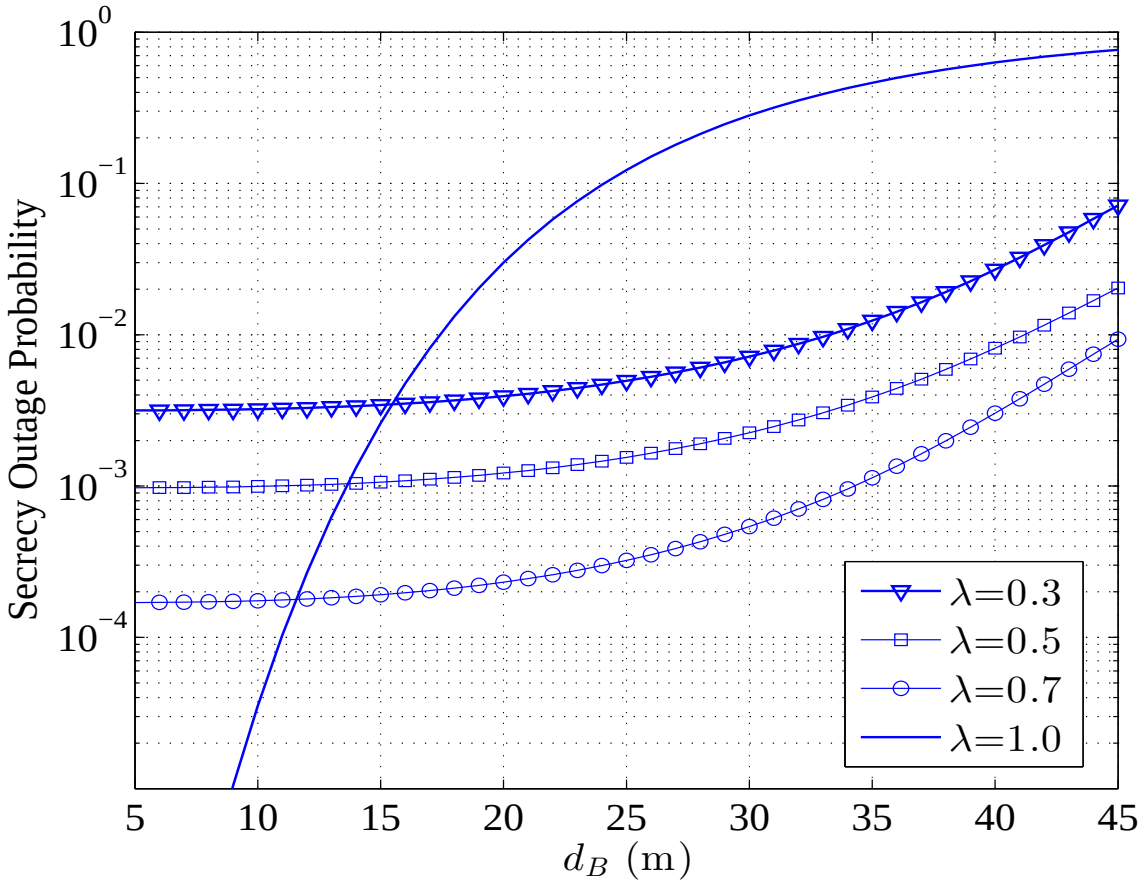

Figure 2.5: Secrecy outage probability of RUB-based MISOSE transmission with/without AN for different power allocation coefficient λ ($M = 4$, $N = 7$, $d_E = 30$ m, $\alpha = 3.1$, $R_s = 0.1$ bit/s).

with/without AN versus the distance d_B for different power allocation coefficient λ. When the distance d_B increases with a fixed d_E, the SOP of RUB-based transmission increases for all cases. Clearly, the proposed AN has mixed effects on the SOP of RUB-based MISOSE transmission. When the distance d_B is small compared with d_E, the SOP of RUB-based without AN ($\lambda = 1$) is lower than that of RUB-based with AN. With increasing d_B, the trend is reversed. We also observe that increasing power allocation factor λ effectively helps to reduce the SOP of RUB-based with AN. Thus, we conclude that RUB-based AN transmission can enhance the secrecy performance of MISOSE channel in low SNR region.

2.5 RUB Transmission over MU-MIMOSE Channel

In this section, we consider an MU-MIMOSE channel where Alice transmits to M scheduled users including Bob from N ($N \geq M$) legitimate users in the presence of an eavesdropper Eve. The transmitted signal vector from M antennas of Alice over a single symbol period can be written as

$$\mathbf{x}^{''} = \sum_{m=1}^{M} \mathbf{u}_m s_m, \tag{2.45}$$

where $\mathbf{u}_m$'s are the selected beamforming vectors and s_m represents the information symbol for the mth selected user. Therefore, the received symbol at legitimate user n, who is interested in the signal on the jth beam, can be expressed as

$$y_n^{''} = \mathbf{h}_n^T \mathbf{x}^{''} + n_n = K d_n^{-\alpha} \left(\mathbf{h}_n^T \mathbf{u}_j s_j + \sum_{m=1, m\neq j}^{M} \mathbf{h}_n^T \mathbf{u}_m s_m \right) + n_n. \tag{2.46}$$

The received symbol at Eve can be expressed as

$$y_E^{''} = \mathbf{h}_E^T \mathbf{x}^{''} + n_E = K d_E^{-\alpha} \left(\mathbf{h}_E^T \mathbf{u}_j s_j + \sum_{m=1, m\neq j}^{M} \mathbf{h}_E^T \mathbf{u}_m s_m \right) + n_E. \tag{2.47}$$

We assume a uniform power allocation to scheduled users. The received SINR at user n is given by

$$\gamma_{n,j}^{''} = \frac{\frac{P}{M} K d_n^{-\alpha} |\mathbf{h}_n^T \mathbf{u}_j|^2}{\frac{P}{M} K d_n^{-\alpha} \sum_{m=1, m\neq j}^{M} |\mathbf{h}_n^T \mathbf{u}_m|^2 + N_0} = \frac{|\mathbf{h}_n^T \mathbf{u}_j|^2}{\sum_{m=1, m\neq j}^{M} |\mathbf{h}_n^T \mathbf{u}_m|^2 + 1/\rho_B^{''}}, \tag{2.48}$$

where $\rho_B^{''} = \frac{P K d_n^{-\alpha}}{N_0 M}$. Again, we assume for long term fairness, the transmitter adopts power control to mitigate path loss difference. As such, all candidate users have the same $\rho_B^{''}$. The received SINR at Eve is obtained as

$$\gamma_{E,j}^{''} = \frac{|\mathbf{h}_E^T \mathbf{u}_j|^2}{\sum_{m=1, m\neq j}^{M} |\mathbf{h}_E^T \mathbf{u}_m|^2 + 1/\rho_E^{''}}, \tag{2.49}$$

where $\rho_E^{''} = \frac{P K d_E^{-\alpha}}{N_0 M}$.

For RUB transmission over MIMO broadcast channel, user scheduling and beam selection are carried out as follows. Each legitimate user calculates and feeds back its experienced SINR value on M different beams. The feedback load is $M \times N$ real numbers. Based on the feedback information, Alice assigns a beam to the user with the largest SINR value among N legitimate users. Particularly, Alice ranks all the N feedback SINRs for one beam and selects the legitimate users with the largest SINR. If Bob's SINR for the jth beam $\gamma_{B,j}$ is the largest SINR among all N feedback SINRs, then Alice assigns Bob with the jth beam. After that, Alice assigns other beams by ranking the feedback SINRs for those beams in a similar fashion. This process continues till M beams have been assigned. We assume that no user has the largest SINR on two different beams.

To better understand the application prospect of the RUB scheme, we compare its complexity with conventional beamforming in terms of feedback load. With conventional beamforming, such as ZFBF and minimizing mean squared error (MMSE), each user needs to feed back its channel vector. Thus, the feedback load is $M \times N$ complex numbers. However, the feedback load of RUB scheme is $M \times N$ real numbers since each user needs to feed back M SINR to Alice. The feedback load of RUB can be further reduced to N real numbers and N integers if each user only feeds back its best beam SINR and index [99], [33]. Therefore, RUB scheme provides a low-complexity solution over an MU-MIMO channel.

2.5.1 Ergodic Secrecy Rate

The ergodic secrecy rate of Bob can be calculated as

$$\mathbb{E}[C_s^{''}] = \frac{1}{\ln 2} \int_0^{\infty} \frac{F_{\gamma_{E,j}^{''}}(x)}{1+x} [1 - F_{\gamma_{B,j}^{''}}(x)] dx, \tag{2.50}$$

where $F_{\gamma_{B,j}^{''}}(x)$ denotes the CDF of the received SINR at Bob on the jth beam and $F_{\gamma_{E,j}^{''}}(x)$ is the CDF of the received SINR at Eve on the jth beam.

As mentioned earlier, $|\mathbf{h}_n^T \mathbf{u}_j|^2$ has $\chi^2(2)$ distribution and $\sum_{m=1, m\neq j}^{M} |\mathbf{h}_n^T \mathbf{u}_m|^2$ has $\chi^2(2M-2)$ distributions. The CDF of the recieved SINR at user n on beam j can be obtained as [33]

$$F_{\gamma_{n,j}^{''}}(x) = \left(1 - \frac{e^{-x/\rho_B^{''}}}{(1+x)^{M-1}}\right). \tag{2.51}$$

The received SINR at Bob $\gamma''_{B,j}$ is the largest one of N i.i.d random variables with the above CDF since different users experience independent channels. Therefore, the CDF of the received SINR at Bob $\gamma''_{B,j}$ can be obtained as

$$F_{\gamma''_{B,j}}(x) = \left(1 - \frac{e^{-x/\rho''_B}}{(1+x)^{M-1}}\right)^N. \tag{2.52}$$

Since beamforming vectors appear arbitrary to Eve, the CDF of the received SINR at Eve on the jth beam can be obtained as

$$F_{\gamma''_{E,j}}(x) = 1 - \frac{e^{-x/\rho''_E}}{(1+x)^{M-1}}. \tag{2.53}$$

Substituting (2.52) and (2.53) into (2.50), applying the binomial expansion [97, eq.(1.111)] and carrying out integration, the closed-form expression of ergodic secrecy rate at (2.54) can be obtained as

$$\begin{aligned}\mathbb{E}[C''_s] = \frac{1}{\ln 2}\sum_{i=1}^{N}\binom{N}{i}(-1)^i\Bigg[E_{[(M-1)i+M]}\left(\frac{1}{\rho''_E}+\frac{i}{\rho''_B}\right)\exp\left(\frac{1}{\rho''_E}\right) \\ - E_{[(M-1)i+1]}\left(\frac{i}{\rho''_B}\right)\Bigg]\exp\left(\frac{i}{\rho''_B}\right),\end{aligned} \tag{2.54}$$

where $E_{[n]}(x) = \int_1^\infty \frac{e^{-xt}}{t^n}dt$ denotes the two-argument exponential integral function [100].

2.5.2 Secrecy Outage Probability

Taking derivative of $F_{\gamma''_{E,j}}(x)$ from (2.53), the PDF of the received SINR at Eve can be obtained as

$$p_{\gamma''_{E,j}}(x) = \frac{[\rho''_E(1+x)+(M-1)]e^{\rho''_E x}}{(1+x)^M}. \tag{2.55}$$

Substituting (2.52) and (2.55) into (2.43) and performing integration, the closed-form expression of the SOP for RUB transmission in MU-MIMOSE channel can be

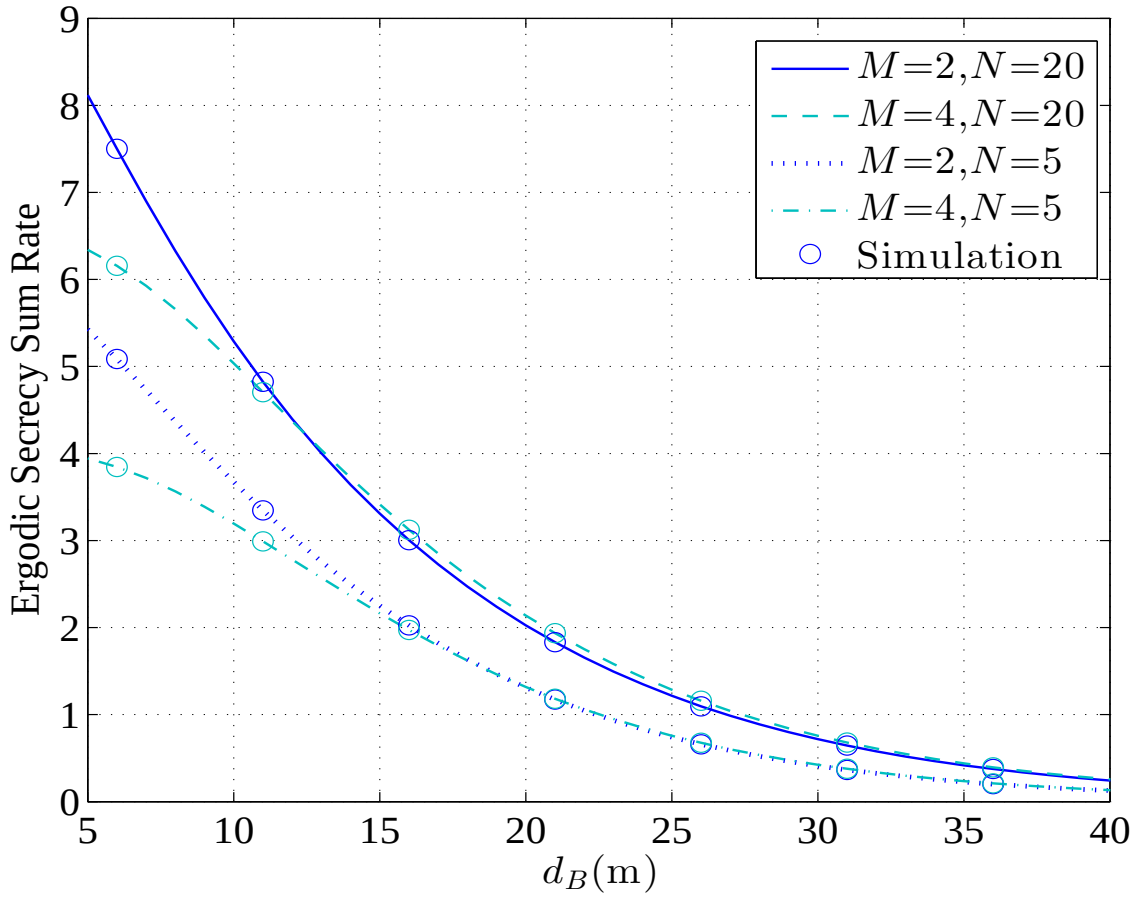

Figure 2.6: Ergodic secrecy rate of RUB-based MU-MIMOSE transmission versus d_B for different antenna numbers M and/or users N ($d_E = 30$ m, $\alpha = 3.1$).

obtained as

$$P_{\text{out}}(R_s) = \sum_{i=0}^{N} \binom{N}{i} \frac{(-1)^i}{2^{R_s(M-1)i}} \left[\frac{1}{\rho_E''} E_{[(M-1)(i+1)]} \left(\frac{2^{R_s} i}{\rho_B''} + \frac{1}{\rho_E''} \right) \right.$$
$$\left. + (M-1) E_{[(M-1)i+M]} \left(\frac{2^{R_s} i}{\rho_B''} + \frac{1}{\rho_E''} \right) \right] \exp\left(-\frac{(2^{R_s}-1)i}{\rho_B''} \right) \exp\left(\frac{2^{R_s} i}{\rho_B''} + \frac{1}{\rho_E''} \right). \tag{2.56}$$

2.5.3 Numerical Results

Fig. 2.6 shows that ergodic secrecy rate of RUB-based MU-MIMOSE transmission versus the distance d_B for different antenna numbers and user numbers when Eve is located in 30 m from Alice. We can see that ergodic secrecy rate declines with the

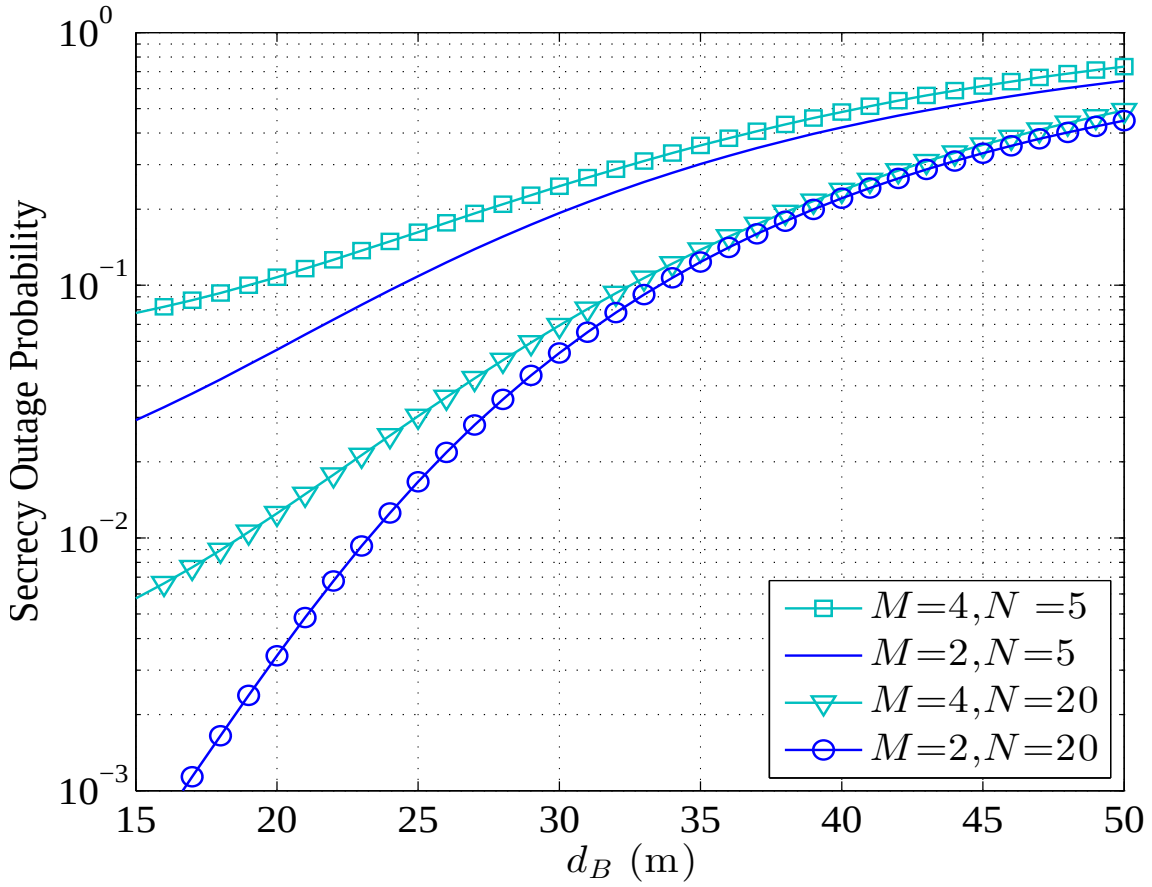

Figure 2.7: Secrecy outage probability of RUB-based MU-MIMOSE transmission versus d_B for different antenna numbers M and/or users N (d_E = 30 m, α = 3.1, $R_s = 0.1$ bit/s).

growth of the distance d_B. For fixed N, as antenna number increases and as such more users are served, ergodic secrecy rate decreases when the distance d_B is small compared to d_E. The reason is that more multiuser interference has been introduced to Bob. However, when the distance d_B is comparable with d_E, ergodic secrecy rate slightly increases with the increase of antenna number. Although more multiuser interference has been introduced to Bob, the SINR at Eve is degraded more seriously. Therefore, over low SINR region, ergodic secrecy rate of RUB scheme increases when Alice serves more users. Therefore, we can conclude that RUB-based MU-MIMOSE transmission can effectively enhance ergodic secrecy rate in low SINR region.

Fig. 2.7 plots the SOP performance of RUB-based MU-MIMOSE transmission versus d_B for different antenna numbers M, and user numbers N when Eve's distance

is fixed to 30 m. We observe that the SOP increases as the distance d_B increases due to more severe path loss. For fixed N, as antenna number M increases, the SOP increases. This is because multiuser interference at Bob plays a dominant role in the SOP performance. We also see that, when M is fixed, the SOP at a given d_B decreases when N becomes larger, as the SOP performance benefits from multiuser scheduling.

2.6 Conclusions

In this chapter, the secrecy performance of multiple antenna transmission with partial CSI of legitimate users has been analyzed. The closed-form expressions of the exact ergodic secrecy rate and the exact SOP for MISOSE channel have been derived. In addition, compact expressions for the asymptotic ergodic secrecy rate and the asymptotic SOP have also been derived. Moreover, the effects of RUB-based AN method and multiuser interference are also investigated. Numerical results have demonstrated that the RUB-based multi-antenna transmission serves as an effective low complexity solution for enhancing secrecy performance. In addition, the proposed RUB-based AN method can improve the ergodic secrecy rate over low SNR region. Meanwhile, RUB-based MU-MIMOSE transmission can effectively enhance the secrecy performance over low SINR region and increasing the number of candidate legitimate users can help improve the secrecy performance by exploring multiuser diversity.

Chapter 3

Secrecy Performance Analysis of Massive MIMO Transmission with Random Unitary Beamforming

3.1 Introduction

Massive multiple-input multiple-output (MIMO) is a critical wireless technology in the evolution towards 5G networks as it can improve system capacity, spectral efficiency, and energy efficiency [38, 39, 37]. In massive MIMO system, a base station (BS), equipped with a large number of antenna elements, serves multiple users simultaneously. As the number of antenna elements grows very large, user channel vectors become pairwise orthogonal [101] and inter-user interference becomes negligible [102]. Thus, linear precoding techniques, such as simple matched filter (MF) and zero-forcing (ZF) beamforming, can apply [39]. The premise of these beamforming techniques requires accurate full channel state information (CSI) of users at the BS. It is, generally, very challenging to provide accurate full CSI at the BS in practice. Most massive MIMO systems adopt time-division-duplex (TDD) implementation, where at BS obtains the required CSI by exploring channel reciprocity [40, 41, 42]. However, the estimated uplink CSI may not match the actual downlink CSI when the BS performs transmission due to, for example, channel decorrelation, calibration error, and hardware impairment in uplink/downlink radio frequency (RF) chains [43]. When the CSI needs to be fed back from the users, as in frequency-division-duplex (FDD) implementation, these full CSI based beamforming schemes will incur large feedback

load, especially for massive MIMO systems [44]. Therefore, it is of great practice importance to study transmission schemes requiring limited CSI for massive MIMO systems. In this chapter, we investigate the secrecy performance of massive MIMO downlink transmission with limited CSI at the transmitter.

Random unitary beamforming (RUB) is a low-complexity transmission scheme for multiuser MIMO systems and requires limited CSI of mobile users at the BS [99]. With RUB, the BS serves multiple users with pre-designed beamforming vectors selected using limited CSI. In FDD implementation, users only need to feed back the index of their preferred beams, and with TDD, BS chooses beamforming vectors based on uplink channel estimation. To the best of the authors' knowledge, the performance of RUB in massive MIMO setting has not been reported yet. In this work, we investigate the secrecy performance of massive MIMO transmission with RUB, where partial CSI of legitimate users and no CSI of eavesdropper is available at the BS.

In this chapter, we investigate a massive MIMO downlink transmission system, consisting of a multiple-antenna BS, multiple single-antenna legitimate users in the presence of multiple single-antenna eavesdroppers. Meanwhile, we consider two types of eavesdroppers, namely non-colluding eavesdroppers and colluding eavesdroppers. We propose to apply RUB-based multiple antenna transmission to enhance the secrecy performance of legitimate users in the wiretap environment. Thus, we summarize the following key contributions:

1. We present an analytical framework to evaluate the secrecy performance of massive MIMO transmission in the presence of two types of eavesdroppers when RUB is employed at the BS.

2. We derive the closed-form expressions of ergodic secrecy rate and secrecy outage probability (SOP) of massive multiple-input multiple-output multiple-eavesdropper (MIMOME) transmission including the interference-limited and single legitimate user special cases in the presence of non-colluding eavesdroppers. We also derive the closed-form of the upper bound of ergodic secrecy rate and the asymptotic SOP of massive MISOME transmission when the number of antenna elements grows very large.

3. We carry out secrecy performance of massive MIMOME transmission in the presence of colluding eavesdroppers. We obtain the expression of ergodic secrecy rate and solve it by numerical approaches.

The remainder of the chapter is organized as follows. The system, channel, and signal models of a massive MIMO downlink transmission scenario are presented in Section 3.2. We analyze the statistics of received signal to interference plus noise ratio (SINR) at the legitimate user and non-colluding eavesdroppers in Section 3.3. We derive the expressions of the ergodic secrecy rate and the SOP with the proposed RUB design for different scenarios and the corresponding numerical results in Section 3.4 and Section 3.5, respectively. The effect of colluding eavesdroppers is investigated in Section 3.6. Finally, we draw our conclusions in Section 3.7.

3.2 System and Channel Models

We consider a single-cell massive MIMO downlink transmission system, consisting of an M-antenna BS (Alice), N ($N \ll M$) single-antenna legitimate users and N_E ($N_E \ll M$) single-antenna eavesdroppers, as shown in Fig. 6.1. We assume that there is a secured area which we are sure that it has no eavesdroppers like a ring and then they try to approach the area at its borders. Eavesdroppers attempt to overhear the signal to one of N scheduled users (a.k.a Bob), and two types of eavesdroppers including non-colluding eavesdroppers and colluding eavesdroppers are considered. We assume Alice has limited CSI of legitimate users and no CSI of passive eavesdroppers. In addition, Alice applies RUB to serve N legitimate users where it serves each legitimate user using one of M random orthonormal beams, generated from an isotropic distribution [19]. We denote the set of beamforming vectors as $\mathcal{U} = [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_M]$, assumed to be unknown to eavesdroppers.

We assume that the wireless channel introduces path loss and Rayleigh fading effects. In particular, the path loss effect follows the log-distance model. The path loss over the link from Alice to legitimate user j, $j = 1, 2, \cdots, N$, is characterized by average power gain $Kd_j^{-\alpha}$, where K is the path loss constant, d_j is the distance between Alice and legitimate user j, and α is the path loss exponent. Also, the path loss over the link from Alice to eavesdropper e is characterized by average power gain $Kd_e^{-\alpha}$, where d_e is the distance between Alice and eavesdropper e. Under Rayleigh fading model, the channel gains from the ith antenna of Alice to legitimate user j and eavesdropper e, denoted by $h_{j,i}$ and $g_{e,i}$, respectively, are assumed to be independent and identically distributed (i.i.d) complex Gaussian random variables with zero mean and unitary variance, i.e. $h_{j,i} \sim \mathcal{CN}(0,1)$ and $g_{e,i} \sim \mathcal{CN}(0,1)$.

The transmitted signal vector from M antennas of Alice over a symbol period can

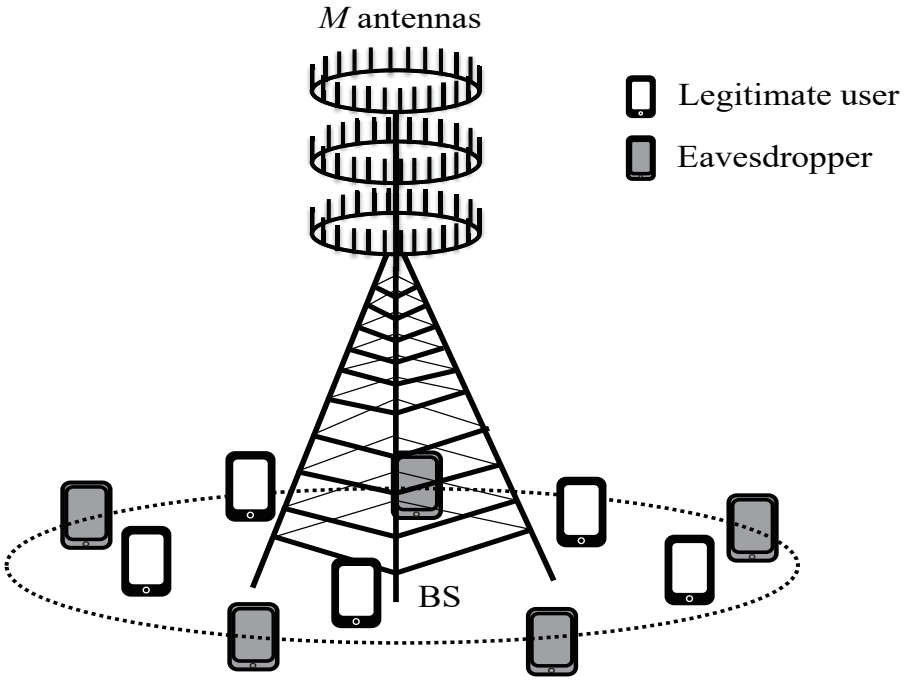

Figure 3.1: Single-cell multiuser massive MIMO system in the presence of multiple eavesdroppers.

be written as

$$\mathbf{x} = \sum_{j=1}^{N} \mathbf{u}_j s_j, \tag{3.1}$$

where $\mathbf{u}_j$ is the beamforming vector selected for user j and s_j represents the information symbol for user j. P denotes the maximum average power of the transmitted signal vector $\mathbf{x}$. The transmitted signal vectors satisfies an average power constraint given as $\mathbb{E}[|\mathbf{x}^H\mathbf{x}|] \leq P$. Therefore, the received symbol at the legitimate user i, who is interested in the signal on the jth beam, can be expressed as

$$y_i = \mathbf{h}_i^T\mathbf{x} + n_i = Kd_i^{-\alpha}\left(\mathbf{h}_i^T\mathbf{u}_j s_j + \sum_{n=1,n\neq j}^{N} \mathbf{h}_n^T\mathbf{u}_n s_n\right) + n_i, \tag{3.2}$$

where $\mathbf{h}_i = [h_{i,1}, h_{i,2}, \cdots, h_{i,N}]^T$ denotes the fading channel vector of legitimate user i, and n_i is the additive Gaussian noise with zero mean and variance N_0. Likewise,

the received symbol at eavesdropper e can be expressed as

$$y_e = \mathbf{g}_e^T \mathbf{x} + n_e = K d_e^{-\alpha} \left(\mathbf{g}_e^T \mathbf{u}_j s_j + \sum_{n=1, n\neq j}^{N} \mathbf{g}_n^T \mathbf{u}_n s_n \right) + n_e, \tag{3.3}$$

where $\mathbf{g}_e = [g_{e,1}, g_{e,2}, \cdots, g_{e,N}]^T$ denotes the fading channel vector of eavesdropper e and n_e is the zero mean white Gaussian noise with variance N_0. Assuming uniform power allocation to different legitimate users, the received SINR at legitimate user i on beam j is given by

$$\gamma_{i,j} = \frac{\frac{P}{N} K d_i^{-\alpha} |\mathbf{h}_i^T \mathbf{u}_j|^2}{\frac{P}{N} K d_i^{-\alpha} \sum_{n=1, n\neq j}^{N} |\mathbf{h}_i^T \mathbf{u}_n|^2 + N_0} = \frac{|\mathbf{h}_i^T \mathbf{u}_j|^2}{\sum_{n=1, n\neq j}^{N} |\mathbf{h}_i^T \mathbf{u}_n|^2 + 1/\rho_i}, \tag{3.4}$$

where $\rho_i = \frac{P K d_i^{-\alpha}}{N_0 N}$. The received SINR at eavesdropper e is given by

$$\gamma_{e,j} = \frac{|\mathbf{g}_e^T \mathbf{u}_j|^2}{\sum_{n=1, n\neq j}^{N} |\mathbf{g}_e^T \mathbf{u}_n|^2 + 1/\rho_e}, \tag{3.5}$$

where $\rho_e = \frac{P K d_e^{-\alpha}}{N_0 N}$.

In order to enhance the legitimate user channel capacity, RUB with beam selection is applied in the massive MIMO system as follows, where we assume FDD implementation. At the beginning of each time slot, each legitimate user estimates its channel vector and determines the best beam that leads to largest SINR given in (3.4). Then the user feeds back the index of its best beam to the BS. For example, if the j^*th beam leads to the largest SINR for legitimate user i, i.e. $\gamma_{i,j^*} = \max\{\gamma_{i,j}\}$, where $j \in \{1, 2, \cdots, M\}$, then user i feeds back beam index j^*. We assume that the best beam index feedback is error free. Note that the feedback load is $\lceil \log_2 M \rceil$ bits per user. Then, the BS assigns beam j^* to legitimate user i. Thereafter, the BS transmits to N legitimate users using the selected beams for the rest of this time slot. We neglect the small probability that two legitimate users select the same beam since the number of beamforming vectors is much larger than the number of users in massive MIMO setting.

3.3 Statistics of Received SINR with non-colluding eavesdroppers

In this section, we analyze the statistics of received SINR at the legitimate user Bob and non-colluding eavesdroppers, while Alice apply RUB to serve N legitimate users and eavesdroppers overhear the messages.

The received SINR at Bob on the selected beam can be written as

$$\gamma_B = \frac{z}{y + 1/\rho_B}, \tag{3.6}$$

where $z = |\mathbf{h}_B^T \mathbf{u}_{j^*}|^2$ is the largest one of M independent $\chi^2(2)$ distributed random variables and $y = \sum_{n=1, n\neq j^*}^{N} |\mathbf{h}_B^T \mathbf{u}_n|^2$ follows $\chi^2(2(N-1))$ distribution. Conditioning on y, the probability density function (PDF) of the received SINR at Bob on the selected beam can be written as

$$p_{\gamma_B}(x) = \int_0^\infty M(1/\rho_B + y) e^{-(1/\rho_B + y)x} \left(1 - e^{-(1/\rho_B + y)x}\right)^{M-1} \frac{y^{N-2} e^{-y}}{(N-2)!} dy. \tag{3.7}$$

Applying the binomial expansion [97, eq.(1.111)], using [97, eq.(3.351.3)] and performing integration, the closed-form expressions of the PDF and cumulative distribution function (CDF) of the received SINR at Bob on the selected beam can be obtained as

$$p_{\gamma_B}(x) = \sum_{i=0}^{M-1} \binom{M-1}{i} \frac{(-1)^i M e^{-(1+i)x/\rho_B}}{[(1+i)x+1]^N} \left(\frac{1}{\rho_B}[(1+i)x+1] + N - 1\right), \tag{3.8}$$

and

$$F_{\gamma_B}(x) = \sum_{i=0}^{M-1} \binom{M-1}{i} \frac{(-1)^i M}{1+i} \left(1 - \frac{e^{-(1+i)x/\rho_B}}{[1+(1+i)x]^{N-1}}\right), \tag{3.9}$$

respectively.

Since the selected beamforming vector appears arbitrary to eavesdropper e, $|\mathbf{g}_e^T \mathbf{u}_j^*|^2$ follows $\chi^2(2)$ and $\sum_{n=1, n\neq j^*}^{N} |\mathbf{g}_e^T \mathbf{u}_n|^2$ follows $\chi^2(2(N-1))$ distributions in (3.5). As such, the CDF of the received SINR at eavesdropper e on the selected beam can be

obtained as [103]

$$F_{\gamma_e}(x) = 1 - \frac{e^{-x/\rho_e}}{(1+x)^{N-1}}. \tag{3.10}$$

In non-colluding eavesdroppers case, the eavesdroppers individually overhear the messages without the central processing unit. Assuming Eve is the strongest one among N_E non-colluding eavesdroppers, the received SINR at Eve on the selected beam can be given by

$$\gamma_E = \max_{e \in N_E} \gamma_{e,j^*}. \tag{3.11}$$

Thus, the CDF of the received SINR at Eve on the selected beam can be calculated by

$$F_{\gamma_E}^{\mathrm{NCE}}(x) = \Pr\left(\max_{e \in N_E} \gamma_{e,j^*} < x\right) = \prod_{e=1}^{N_E} \Pr(\gamma_{e,j^*} < x). \tag{3.12}$$

Substituting (3.10) into (3.12), the closed-form expressions of the CDF and the corresponding PDF of the received SINR at Eve on the selected beam can be obtained as

$$F_{\gamma_E}^{\mathrm{NCE}}(x) = \left(1 - \frac{e^{-x/\rho_e}}{(1+x)^{N-1}}\right)^{N_E}, \tag{3.13}$$

and

$$p_{\gamma_E}^{\mathrm{NCE}}(x) = N_E \left(1 - \frac{e^{-x/\rho_e}}{(1+x)^{N-1}}\right)^{N_E-1} \frac{e^{-x/\rho_e}}{(1+x)^N} \left[\frac{1+x}{\rho_e} + (N-1)\right], \tag{3.14}$$

respectively.

3.4 Ergodic Secrecy Rate

In this section, we characterize the ergodic secrecy rate of massive MIMOME transmission and its interference-limited and single legitimate user special cases. When the number of antenna elements grows very large, the upper bound of ergodic secrecy rate is analyzed.

3.4.1 Massive MIMOME Transmission

The ergodic secrecy rate can be calculated as [98]

$$\mathbb{E}[C_s] = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(x)}{1+x}[1 - F_{\gamma_B}(x)]dx. \tag{3.15}$$

Substituting (3.9) and (3.13) into (4.12), we can obtain the ergodic secrecy rate in the presence of non-colluding eavesdroppers as

$$\mathbb{E}^{\mathrm{NCE}}[C_s] = \frac{1}{\ln 2}\Bigg[\int_0^\infty \frac{\left(1 - \frac{e^{-x/\rho_E}}{(1+x)^{N-1}}\right)^{N_E}}{1+x}dx - \int_0^\infty \frac{\left(1 - \frac{e^{-x/\rho_E}}{(1+x)^{N-1}}\right)^{N_E}}{1+x}\left(\sum_{i=0}^{M-1}\binom{M-1}{i}\right.$$
$$\left.\times\frac{(-1)^i M}{1+i}\left(1 - \frac{e^{-(1+i)x/\rho_B}}{[1+(1+i)x]^{N-1}}\right)\right)\Bigg]dx. \tag{3.16}$$

Applying the binomial expansion [97, eq.(1.111)], using the integration results as shown

$$I_0(a,b,m) = \int_0^\infty \frac{e^{-ax}}{(x+b)^m}dx = a^{m-1}e^{ab}\Gamma(1-m,ab), \tag{3.17}$$

and

$$\begin{aligned} I_1(a,b,m,n) &= \int_0^\infty \frac{e^{-ax}}{(x+b)^m(1+x)^n}dx \\ &= (1-b)^{-n}I_0(a,b,m) + \sum_{i=2}^{m}\frac{(-1)^{i-1}\prod_{j=0}^{i-2}(n+j)}{(i-1)!(1-b)^{n+(i-1)}}I_0(a,b,m-i+1) \\ &+ (b-1)^{-m}I_0(a,1,n) + \sum_{i=2}^{n}\frac{(-1)^{i-1}\prod_{j=0}^{i-2}(m+j)}{(i-1)!(b-1)^{m+(i-1)}}I_0(a,1,n-i+1), \end{aligned} \tag{3.18}$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function and after some mathematical manipulations, we obtain the closed-form expression of the ergodic secrecy rate in the

presence of non-colluding eavesdroppers as

$$\begin{aligned}\mathbb{E}^{\mathrm{NCE}}[C_s] = \frac{1}{\ln 2}\Bigg[&\sum_{i=0}^{N_E} \binom{N_E}{i} (-1)^i I_0\big(\frac{i}{\rho_E}, 1, Ni - i + 1\big) \\ &- \sum_{j=0}^{N_E}\sum_{i=0}^{M-1} \binom{N_E}{j}\binom{M-1}{i} \frac{(-1)^{i+j} M}{1+i} \Big(I_0\big(\frac{i}{\rho_E}, 1, Ni - i + 1\big) \\ &- \frac{I_1\big(\frac{j\rho_B + (1+i)\rho_E}{\rho_B \rho_E}, \frac{1}{1+i}, N-1, Nj - j + 1\big)}{(1+i)^{N-1}} \Big) \Bigg]. \end{aligned} \tag{3.19}$$

Interference-Limited Case

Interference limited systems are expected when the number of antennas and the number of users is large, thus the noise terms in (3.4) and (3.5) can be negligible. Setting $1/\rho_B$ and $1/\rho_e$ equal to zero in (3.9) and (3.13), respectively, then substituting them into (4.12), applying [97, eq.(1.111)], [97, eq.(3.259.3^{11})], [97, eq.(8.384.1)] and performing integration, we obtain the closed-form expression of the ergodic secrecy rate of interference-limited case as

$$\begin{aligned}\mathbb{E}^{\mathrm{IL}}[C_s] = &\frac{\sum_{j=1}^{N_E} \binom{N_E}{j} (-1)^j}{\ln 2 (N-1)} \Bigg\{ \frac{1}{j} \\ &- \Bigg[\sum_{i=0}^{MN-1} \binom{MN-1}{i} \frac{(-1)^i MN}{1+i} \left(\frac{1}{j} - \frac{{}_2F_1(N-1; 1; (N-1)(1+j)+1; -i)}{(1+j)} \right) \Bigg] \Bigg\}, \end{aligned} \tag{3.20}$$

where ${}_2F_1(\cdot;\cdot;\cdot;\cdot)$ is the Gaussian hypergeometric function. Note that the ergodic secrecy rate for interference-limited case is related to the number of antenna M at Alice, the number of legitimate users N and the number of non-colluding eavesdropper N_E over a massive MIMOME transmission.

Single Legitimate User Case

In order to find the insight of the power of RUB, we consider a massive multiple-input single-output multiple-eavesdropper (MISOME) transmission where Alice transmits signal to single legitimate user Bob in the presence of the non-colluding eavesdroppers. Thus, the interference terms in (3.4) and (3.5) disappear. The received SNR at Bob

are given by

$$\gamma_{B1} = \frac{PKd_B^{-\alpha}|\mathbf{h}_B^T\mathbf{u}_{j^*}|^2}{N_0} = \rho_{B1}|\mathbf{h}_B^T\mathbf{u}_{j^*}|^2, \tag{3.21}$$

where $\rho_{B1} = \frac{PKd_B^{-\alpha}}{N_0}$ and $|\mathbf{h}_B^T\mathbf{u}_{j^*}|^2$ is the largest one of M independent $\chi^2(2)$ distributed random variables. Thus, the CDF of the received SNR at Bob can be obtained as

$$F_{\gamma_{B1}}(x) = (1 - e^{-x/\rho_{B1}})^M. \tag{3.22}$$

The received SNR at eavesdropper e is

$$\gamma_{E1,j} = \rho_{E1}|\mathbf{g}_E^T\mathbf{u}_{j^*}|^2, \tag{3.23}$$

where $\rho_{E1} = \frac{PKd_E^{-\alpha}}{N_0}$ and $|\mathbf{g}_E^T\mathbf{u}_{j^*}|^2$ follows $\chi^2(2)$ distribution since the chosen vector for Bob appears arbitrary to eavesdropper e. Thus, the CDF of the received SNR at Eve, considered as the strongest non-colluding eavesdropper, can be obtained as

$$F_{\gamma_{E1}}(x) = (1 - e^{-x/\rho_{E1}})^{N_E}. \tag{3.24}$$

Substituting (3.22) and (3.24) into (4.12), applying [97, eq.(1.111)], using [97, eq.(3.352.4)] and performing integration, the closed-form expression of the ergodic secrecy rate in the presence of non-colluding eavesdroppers can be obtained as

$$\mathbb{E}^{\mathrm{SU}}[C_s] = \sum_{i=0}^{N_E}\sum_{j=1}^{M}\binom{N_E}{i}\binom{M}{j}\frac{(-1)^{i+j+1}}{\ln 2}\exp\left(\frac{i}{\rho_{E1}} + \frac{j}{\rho_{B1}}\right)E_1\left(\frac{i}{\rho_{E1}} + \frac{j}{\rho_{B1}}\right), \tag{3.25}$$

where $E_1(x) = \int_1^\infty \frac{e^{-xt}}{t}dt$ denotes the exponential integral function.

We are interested in the asymptotic analysis where $M \to \infty$ in the massive MISO system. When M approaches infinity, the limiting distribution of $\gamma_{B1,j}$ exists and follows the Gumbel type with the distribution function, given by

$$\lim_{M\to\infty} F_{\gamma_{B1}}(x) = \exp(-e^{-\frac{x-b_K}{a_K}}), \tag{3.26}$$

where $K = M$, a_K and b_K are normalizing factors given by $a_K = \rho_{B1}$ and $b_K = \rho_{B1}\ln M$, respectively. Thus, the upper bound of the ergodic secrecy rate of Bob on

the selected beam is obtained as

$$\mathbb{E}^{\mathrm{AA}}[C_B] \leq \log_2[1 + \mathbb{E}(\gamma_{B1})] = \log_2[1 + (\mathcal{E} + \ln M)\rho_{B1}], \tag{3.27}$$

where $\mathcal{E}$ is the Euler−Mascheroni constant. Meanwhile, the ergodic secrecy rate at Eve on the selected beam can be given by [104]

$$\mathbb{E}^{\mathrm{AA}}[C_E] = \frac{1}{\ln 2}\int_0^{\infty} \frac{1 - F_{\gamma_{E1}}(x)}{1+x} dx. \tag{3.28}$$

Substituting (3.24) into (3.28), applying [97, eq.(1.111)], [97, eq.(3.352.4)] and performing integration, the closed-form expression of the ergodic secrecy rate at Eve can be obtained as

$$\mathbb{E}^{\mathrm{AA}}[C_E] = \frac{1}{\ln 2}\sum_{i=1}^{N_E} \binom{N_E}{i} (-1)^{i+1} e^{\frac{i}{\rho_{E1}}} E_1\left(\frac{i}{\rho_{E1}}\right). \tag{3.29}$$

Substituting (3.27) and (3.29) into (4.12), the upper bound of the ergodic secrecy rate in massive MIMO system in the presence of non-colluding eavesdroppers can be obtained as

$$\mathbb{E}^{\mathrm{AA}}[C_s] = \log_2[1 + (\mathcal{E} + \ln M)\rho_{B1}] - \frac{1}{\ln 2}\sum_{i=1}^{N_E} \binom{N_E}{i} (-1)^{i+1} e^{\frac{i}{\rho_{E1}}} E_1\left(\frac{i}{\rho_{E1}}\right). \tag{3.30}$$

3.4.2 Numerical Results

In Fig. 3.2, we compare the ergodic secrecy rate performance of three beamforming schemes for massive MIMO system, namely, RUB, ZF and MRT schemes as a function of distance d_B in the presence of non-colluding eavesdroppers. We assume perfect CSI for ZF and MRT schemes. We see that the ergodic secrecy rate decreases as the distance d_B increases due to more severe effect of path loss. We can also observe that the ergodic secrecy rate increases when the number of antenna M increases as spatial diversity plays a positive role in the ergodic secrecy rate performance. It is noted that the secrecy rate performance of RUB scheme is lower than other schemes since RUB scheme requires limited CSI at the BS whereas ZF and MRT need full CSI.

Fig. 3.3 plots the ergodic secrecy rate performance of RUB with ZF and MRT schemes while assuming the CSI is imperfect. Specifically, we assume the estimated CSI and actual CSI have a correlation coefficient $\lambda < 1$. As we can see, the ergodic

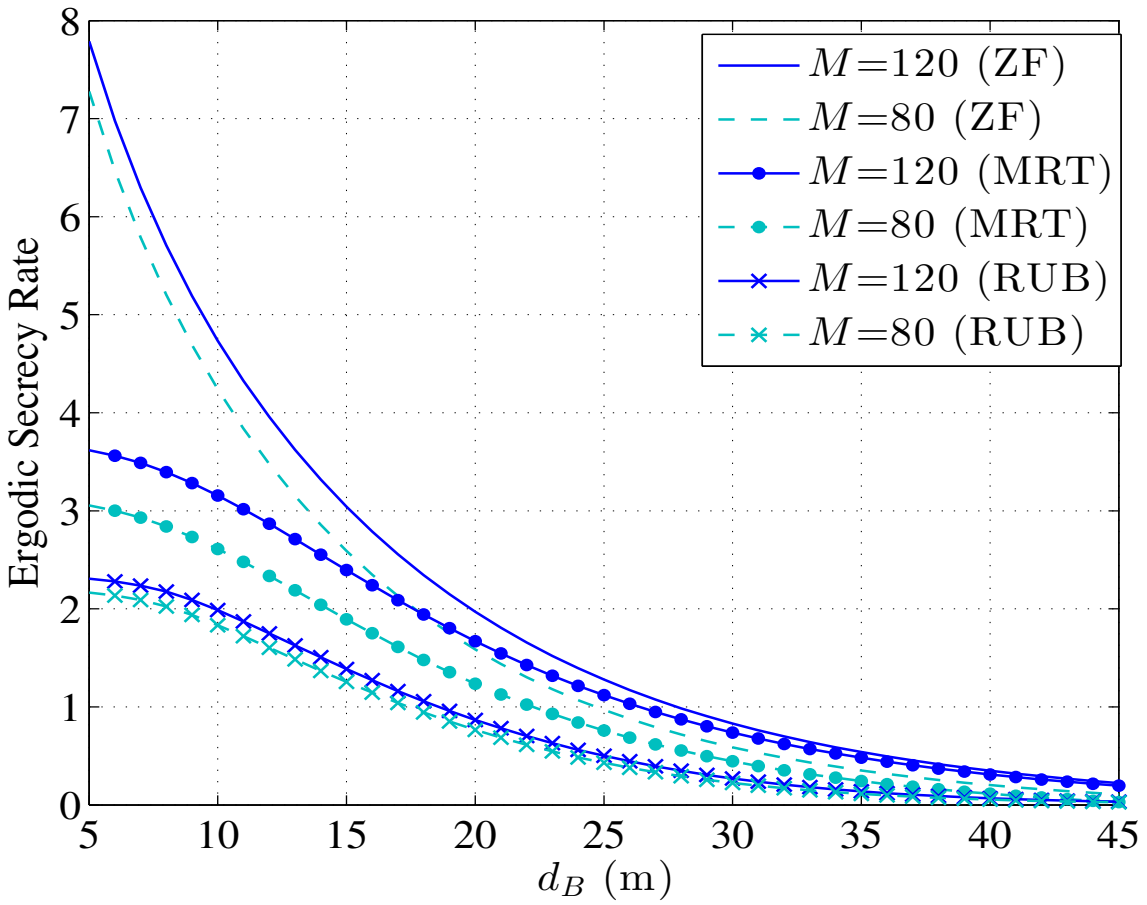

Figure 3.2: Ergodic secrecy rate performance of three different beamforming schemes, RUB, ZF and maximum ratio transmission (MRT) (with perfect CSI), over a massive MIMOME transmission for different antenna numbers M ($N = 20$, $N_E = 20$, $d_e = 30$ m, $\alpha = 3.1$ and $\rho = 90$ dB).

secrecy rate of ZF and MRT decreases as the correlation coefficient λ decreases. Since a channel estimation error becomes larger with the decrease of correlation coefficient λ, the secrecy performance gets worse, leading to lower secrecy rate. We also notice that ZF and MRT better performance than RUB scheme with $\lambda = 0.7$. However, the trend changes when $\lambda = 0.5$. In particular, the ergodic secrecy rate of RUB is higher than that of MRT, and even higher than that of ZF when the distance d_B is small compared with d_e. Moreover, the RUB scheme starts to superceeds the other schemes at $\lambda = 0.3$ as it is robust to imperfect CSI. Therefore, the secrecy performance of RUB scheme with limited CSI can be better than ZF and MRT schemes with imperfect CSI when λ becomes smaller.

Fig. 3.4 shows that the exact and asymptotic upper bound of ergodic secrecy rate

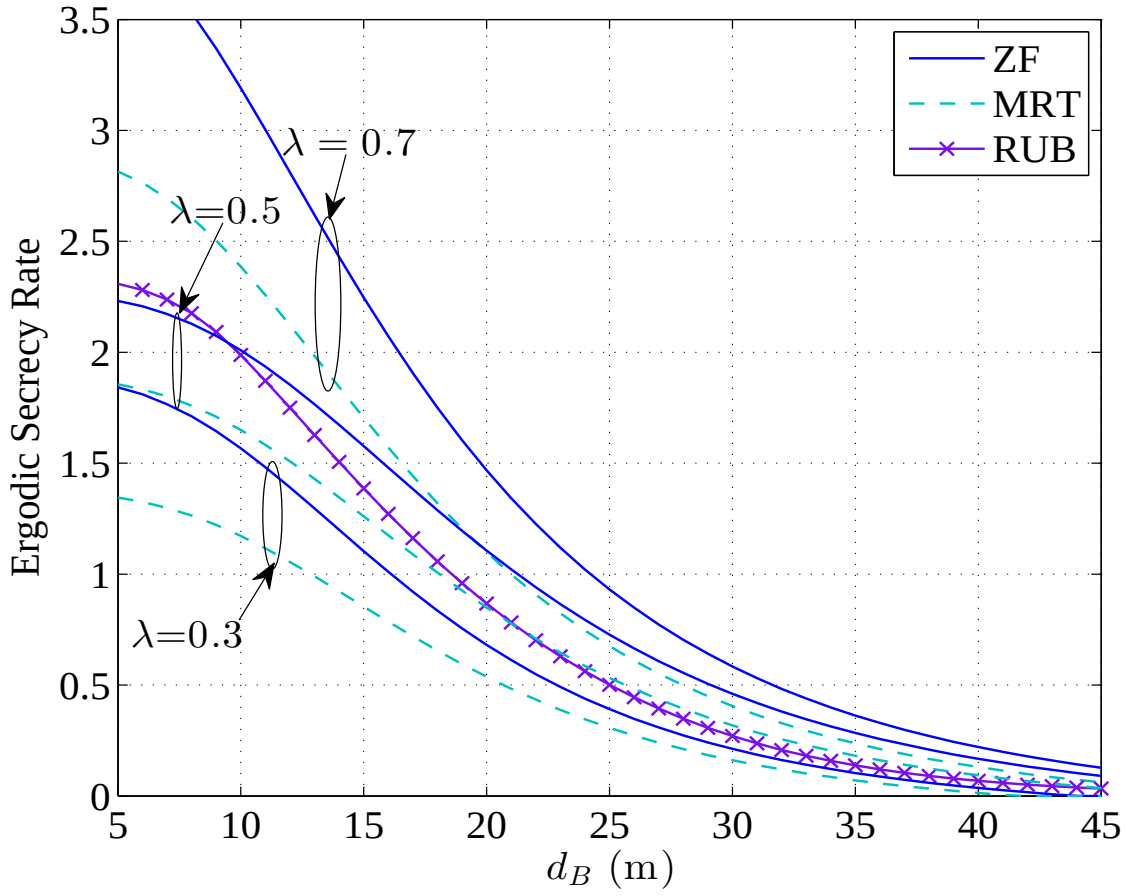

Figure 3.3: Ergodic secrecy rate performance of three different beamforming schemes, RUB, ZF and MRT schemes (with imperfect CSI), over a massive MIMOME transmission ($M = 120$, $N = 20$, $N_E = 20$, $d_e = 30$ m, $\alpha = 3.1$ and $\rho = 90$ dB).

with RUB scheme over a massive MISOME transmission versus the distance d_B for the number of non-colluding eavesdroppers N_E. We can see that the ergodic secrecy rate decreases as the distance d_B increases. Moreover, as we expected, the ergodic secrecy rate deceases when N_E increases. This is because eavesdropping ability of eavesdropper increases with N_E.

3.5 Secrecy Outage Probability

In this section, we characterize the SOP of massive MIMOME transmission and its existence probability of secrecy rate, interference-limited and single legitimate user special cases. When the number of antenna elements grows very large, the asymptotic

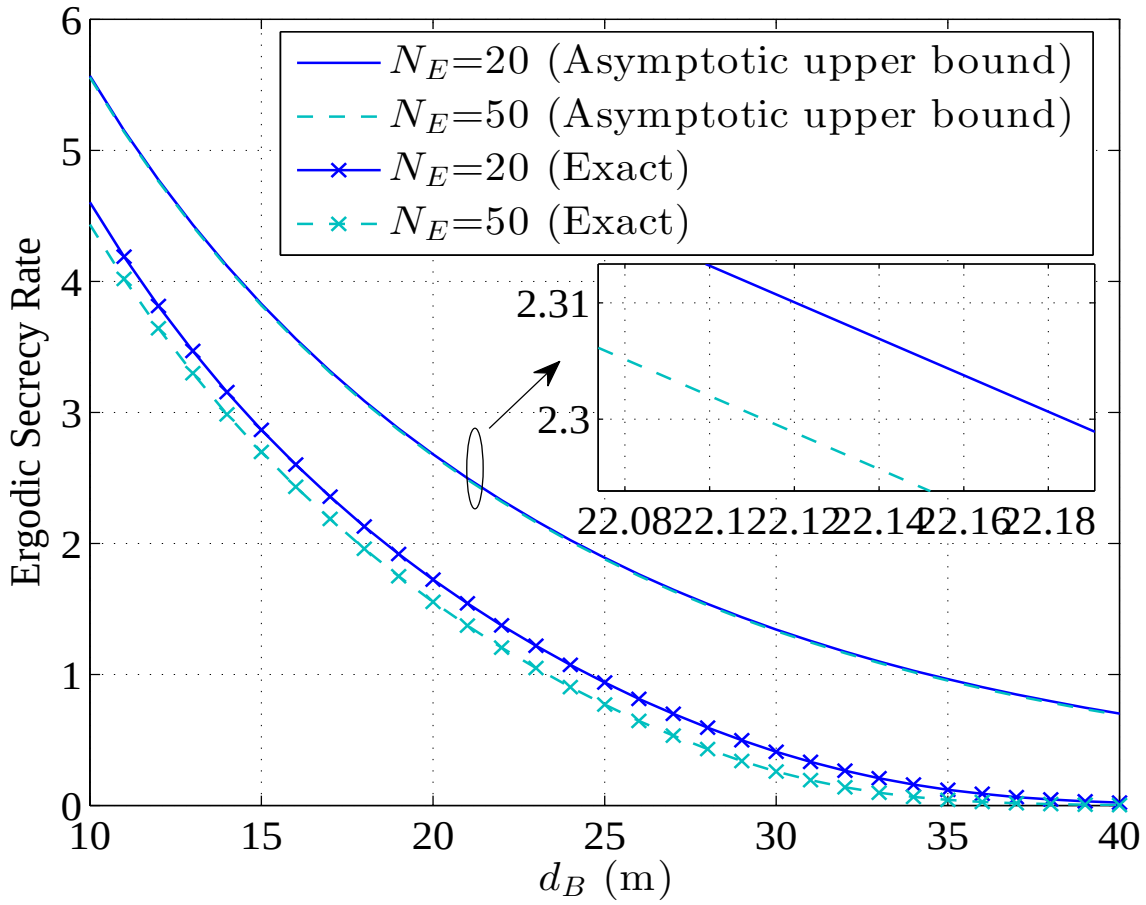

Figure 3.4: Exact and asymptotic upper bound of ergodic secrecy rate with RUB scheme over a massive MISOME transmission for the number of non-colluding eavesdroppers N_E ($M = 200$, $d_e = 30$ m, $\alpha = 3.1$ and $\rho = 90$ dB).

SOP is analyzed.

3.5.1 Massive MIMOME Transmission

The SOP can be calculated as

$$P_{\text{out}}(R_s) = \int_0^\infty p_{\gamma_E}(x) F_{\gamma_B}[2^{Rs}(1+x) - 1] dx. \tag{3.31}$$

Substituting (3.9) and (3.14) into (3.31), applying [97, eq.(1.111)], we can obtain

$$P_{\text{out}}^{\text{NCE}}(R_s) = \sum_{j=0}^{N_E-1}\sum_{i=0}^{M-1}\binom{N_E-1}{j}\binom{M-1}{i}\frac{(-1)^{i+j}MN_E}{1+i} \times \int_0^{\infty}\frac{e^{-x(1+j)/\rho_e}}{(1+x)^{(N-1)j+N}}\left[\frac{1+x}{\rho_e}+(N-1)\right] \times\left(1-\frac{e^{-(1+i)(2^{Rs}-1)/\rho_B}e^{-(1+i)2^{Rs}x/\rho_B}}{[1+(1+i)(2^{Rs}-1)+(1+i)2^{Rs}x]^{N-1}}\right)dx. \tag{3.32}$$

After some mathematical manipulations, we obtain the closed-form expression of the SOP in the presence of non-colluding eavesdroppers as

$$P_{\text{out}}^{\text{NCE}}(R_s) = \sum_{j=0}^{N_E-1}\sum_{i=0}^{M-1}\binom{N_E-1}{j}\binom{M-1}{i}\frac{(-1)^{i+j}MN_E}{1+i} \left[\frac{e^{(1+j)/\rho_E}}{\rho_E}I_0\left(\frac{1+j}{\rho_E},1,(N-1)(1+j)\right)-\frac{e^{-(1+i)(2^{Rs}-1)/\rho_B}}{\rho_E}\right. I_1\left(\frac{\rho_B(1+j)+\rho_e(1+i)2^{Rs}}{\rho_B\rho_e},\frac{1+(1+i)(2^{Rs}-1)}{(1+i)2^{Rs}},N-1,(N-1)(1+j)\right) +(N-1)I_0\left(\frac{1+j}{\rho_e},1,(N-1)j+N\right)-(N-1)e^{-(1+i)(2^{Rs}-1)/\rho_B} \left.I_1\left(\frac{\rho_B(1+j)+\rho_e(1+i)2^{Rs}}{\rho_B\rho_e},\frac{1+(1+i)(2^{Rs}-1)}{(1+i)2^{Rs}},N-1,(N-1)j+N\right)\right]. \tag{3.33}$$

Existence Probability of Secrecy Rate

The existence probability of secrecy rate is the probability that the instantaneous secrecy rate C_s is greater than zero, we can calculate the existence probability of secrecy rate as

$$\Pr\left[C_s>0\right]=\int_0^{\infty}p_{\gamma_B}(x)F_{\gamma_E}(x)dx. \tag{3.34}$$

Substituting (3.8) and (3.13) into (3.34), applying [97, eq.(1.111)], and after performing integration, we can obtain the closed-form expression of the existence probability

of secrecy rate in the presence of non-colluding eavesdroppers as

$$\Pr^{\mathrm{NCE}}[C_s > 0] = \sum_{j=0}^{N_E} \sum_{i=0}^{M-1} \binom{N_E}{j} \binom{M-1}{i} \frac{(-1)^{i+j} M}{(1+i)^N}$$
$$\times \left[\frac{1+i}{\rho_B} I_1 \left(\frac{(1+i)\rho_e + j\rho_B}{\rho_B \rho_e}, \frac{1}{1+i}, N-1, (N-1)j \right) \right.$$
$$\left. + (N-1) I_1 \left(\frac{(1+i)\rho_e + j\rho_B}{\rho_B \rho_e}, \frac{1}{1+i}, N, (N-1)j \right) \right]. \tag{3.35}$$

Interference-Limited Case

Setting $1/\rho_B$ and $1/\rho_e$ are equal to zero in (3.9) and (3.14), substituting them into (3.31), applying [97, eq.(1.111)], using [97, eq.(3.259.3^{11}), eq.(8.384.1)], and performing integration, we obtain the closed-form expression of SOP of interference-limited case in the presence of non-colluding eavesdroppers as

$$P_{\mathrm{out}}^{\mathrm{IL}}(R_s) = \sum_{j=0}^{N_E-1} \sum_{i=0}^{M-1} \binom{N_E-1}{j} \binom{M-1}{i} \frac{(-1)^{i+j} M N_E}{(1+i)(1+j)}$$
$$\left[1 - \frac{{}_2F_1 \left(N-1; 1; (N-1)(1+j)+1; 1 - \frac{2^{R_s}(1+i)}{2^{R_s}(1+i)-i} \right)}{\left[2^{R_s}(1+i) - i \right]^{N-1}} \right]. \tag{3.36}$$

Single Legitimate User Case

Considering massive MISOME transmission scenario, the closed-form expression of the SOP in the presence of non-colluding eavesdroppers can be obtained as

$$P_{\mathrm{out}}^{\mathrm{SU}}(R_s) = \sum_{i=0}^{N_E-1} \sum_{j=0}^{M} \binom{N_E-1}{i} \binom{M}{j} \frac{(-1)^{i+j} N_E e^{-(2^{R_s}-1)j/\rho_{B1}}}{(1+i) + 2^{R_s} j \rho_{E1}}. \tag{3.37}$$

If the number of antennas M at Alice is large enough, the legitimate channel capacity approaches a constant $\log_2(1 + \rho_{B1} \ln M)$ [105]. Conditioning on γ_{E1}, the SOP can be calculated as

$$P_{\mathrm{out}}^{\mathrm{AA}}(R_s) = \Pr\{\gamma_{E1} > [(1 + \rho_{B1} \ln M) - 2^{R_s}]/2^{R_s}\}. \tag{3.38}$$

Substituting (3.24) into (3.38), we obtain the closed-form of the SOP in the presence

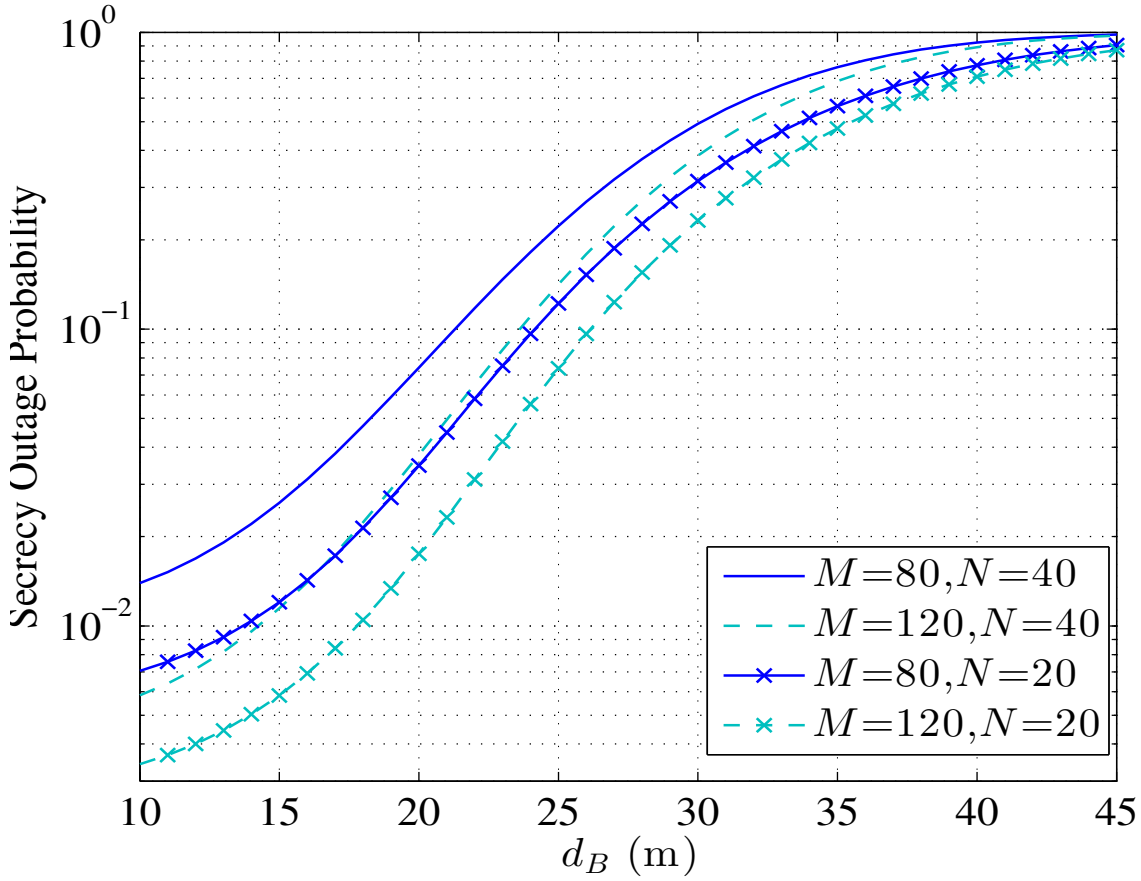

Figure 3.5: Secrecy outage probability of RUB scheme over a massive MIMOME transmission for different antenna numbers M and/or legitimate users N ($N_E = 20$, $d_e = 30$ m, $\alpha = 3.1$, $R_s = 0.1$ bit/s and $\rho = 90$ dB).

of non-colluding eavesdroppers as

$$P_{\text{out}}^{\text{AA}}(R_s) = 1 - \left(1 - e^{-[(1+\rho_{B1}\ln M)-2^{R_s}]/2^{R_s}\rho_{E1}}\right)^{N_E}. \tag{3.39}$$

3.5.2 Numerical Results

Fig. 3.5 shows the SOP performance of RUB transmission over massive MIMO channels as a function of distance d_B for different antenna number M and legitimate user number N. We consider the scenario where all non-colluding eavesdroppers are located on the ring with the distance 30 m from Alice. We can see that the SOP increases to 1 as the distance d_B increases due to severe path loss. Besides, multiuser interference plays an important role in the SOP performance, resulting in higher SOP

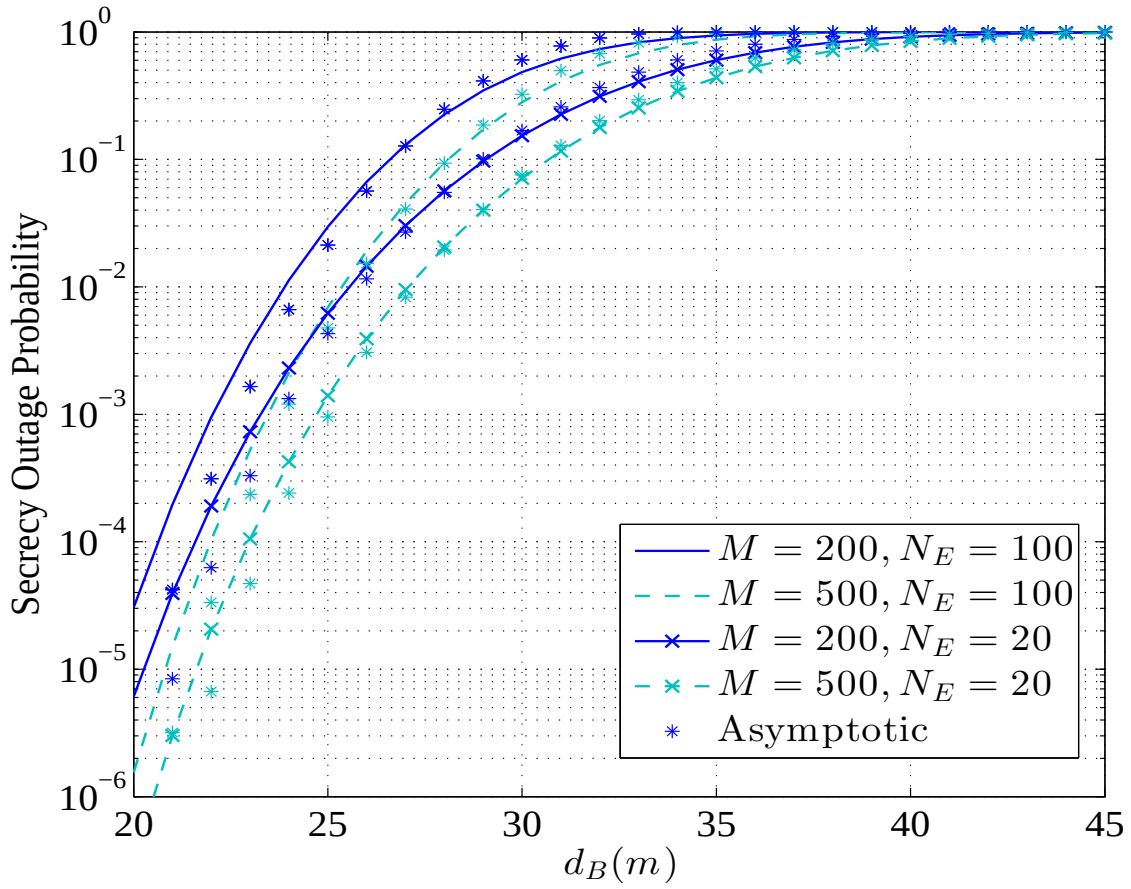

Figure 3.6: Exact and asymptotic of secrecy outage probability with RUB scheme over a massive MISOME transmission for different antenna numbers M and/or eavesdroppers N_E ($d_e = 30$ m, $\alpha = 3.1$, $R_s = 0.1$ bit/s and $\rho = 90$ dB).

with the increasing of legitimate user number N for fixed M. We also observe that, the SOP decreases when M increases, as the SOP performance benefits from spatial diversity.

Fig. 3.6 plots the exact and asymptotic SOP versus distance d_B for different antenna number M and different number of non-colluding eavesdroppers N_E, while assuming Eve is the strongest one. We can observe that these two groups of curves are approximately matched with each other, especially when the distance d_B is comparable to d_e. Thus, the asymptotic SOP can used as the secrecy performance indicator instead of the exact SOP, avoiding the complex expression of the exact SOP. Meanwhile, in both groups, the SOP increases when the distance d_B increases. For fixed N_E, the SOP decreases as antenna number M increases. The SOP increases when more non-colluding eavesdroppers exist in the system.

3.6 Effect of Colluding Eavesdroppers

In this section, we first analyze the statistics of received SINR in the presence of colluding eavesdroppers. Then, we derive an expression of ergodic secrecy rate of massive MIMO transmission. Numerical results are presented to compare the secrecy performance of the system with two types of eavesdroppers.

When we consider the colluding eavesdroppers in the system, all eavesdroppers cooperate together, and thus can be seen as a single multiple-antenna eavesdropper. Thus, as an optimal technique, maximum-ratio combing (MRC) is employed at the colluding eavesdroppers [106, 107]. As such, the received SINR at Eve, denoted as the total received SINR at the colluding eavesdroppers, on the selected beam can be given by

$$\gamma_{\mathrm{E,CE}} = \sum_{e=1}^{N_e} \gamma_e. \tag{3.40}$$

As all links between Alice and each of colluding eavesdroppers experience i.i.d fading, we apply the moment generating function (MGF) to obtain the distribution of $\gamma_{\mathrm{E,CE}}$. As such, the MGF of $\gamma_{\mathrm{E,CE}}$ can be obtained as

$$\begin{aligned}&\mathcal{M}\gamma_{\mathrm{E,CE}}(s)\\ &= \left[1 + \frac{s\rho_e}{1-s\rho_e} - \frac{s\rho_e(N-1)e^{\left(\frac{1}{\rho_e}-s\right)}\left(\frac{1}{\rho_e}-s\right)^{N-1}\Gamma\left(1-N,\frac{1}{\rho_e}-s\right)}{1-s\rho_e}\right]^{N_E}.\end{aligned} \tag{3.41}$$

We can obtain the corresponding PDF of $\gamma_{\mathrm{E,CE}}$ as $p_{\gamma_{\mathrm{E,CE}}}(x) = \mathcal{L}^{-1}[\mathcal{M}\gamma_{\mathrm{E,CE}}(s)]$ The CDF of $\gamma_{\mathrm{E,CE}}$ can be calculated as $F_{\gamma_{\mathrm{E,CE}}}(x) = \int_0^x p_{\gamma_{\mathrm{E,CE}}}(t)dt$.

Substituting (3.9) and $F_{\gamma_{\mathrm{E,MRC}}}(x)$ into (4.12), the ergodic secrecy rate in the presence of colluding eavesdroppers is given by

$$\begin{aligned}&\mathbb{E}^{\mathrm{CE}}[C_s]\\ &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_{\mathrm{E,CE}}}(x)}{1+x}\left[1 - \sum_{i=0}^{M-1}\binom{M-1}{i}\frac{(-1)^i M}{1+i}\left(1 - \frac{e^{-(1+i)x/\rho_B}}{[1+(1+i)x]^{N-1}}\right)\right]dx.\end{aligned} \tag{3.42}$$

The integration can be solved numerically. The corresponding SOP and existence probability of secrecy rate can be also evaluated.

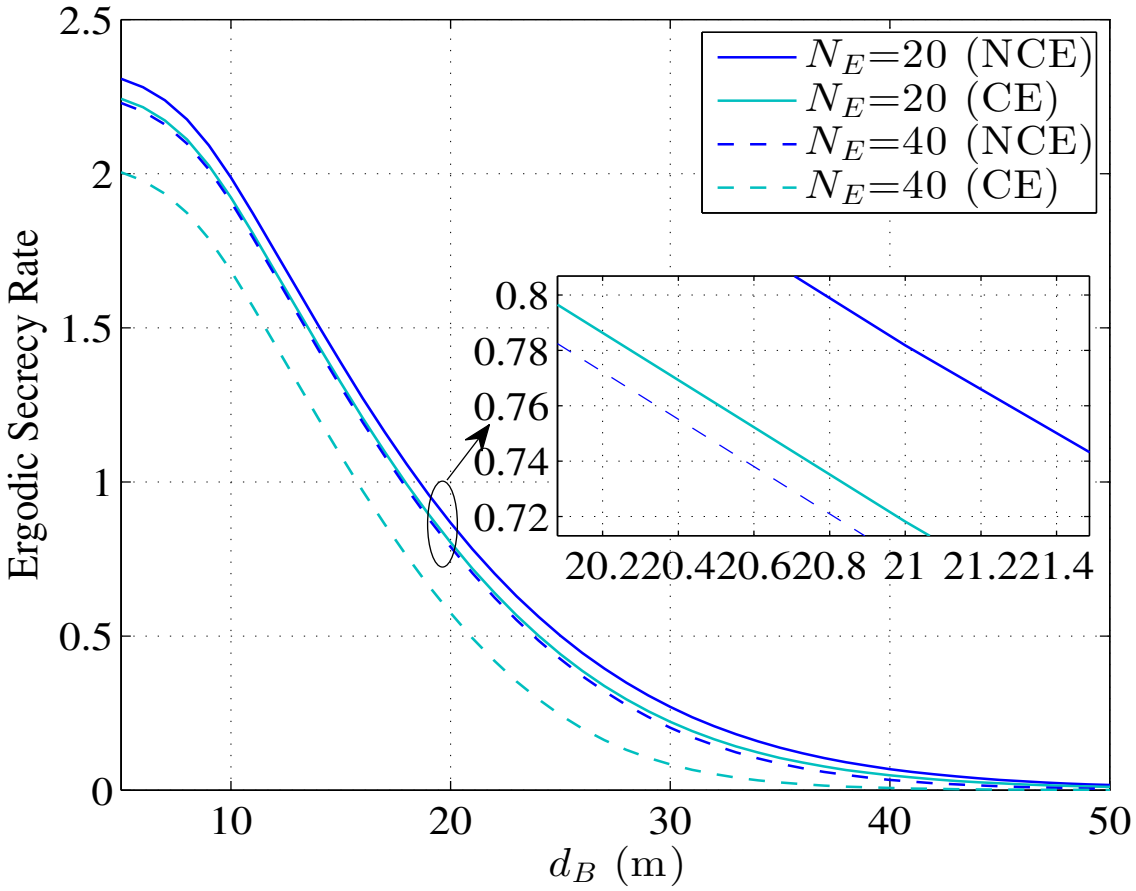

Figure 3.7: Ergodic secrecy rate of RUB scheme over a massive MIMOME transmission in the presence of non-colluding eavesdroppers and colluding eavesdroppers (M=120, $N = 20$, $d_e = 30$ m, $\alpha = 3.1$ and $\rho = 90$ dB).

Fig. 3.7 shows the ergodic secrecy rate as a function of d_B with two types of eavesdroppers over a massive MIMOME transmission. We can see that the ergodic secrecy rate deceases as the distance d_B increases. We can also observe that the ergodic secrecy rate deceases for both non-colluding eavesdroppers and colluding eavesdroppers cases, as the number of eavesdroppers N_E increases. For fixed N_E, the ergodic secrecy rate in the presence of non-colluding eavesdroppers is higher than in the presence of colluding eavesdroppers as expected.

3.7 Conclusions

In this chapter, the secrecy performance of the RUB-based massive MIMOME transmission has been analyzed. We propose to apply RUB-based multiple antenna transmission to enhance the secrecy performance of legitimate users in a wiretap environment. We derived the closed-form expressions of ergodic secrecy rate and SOP of massive MIMOSE transmission and its interference-limited and single legitimate user special cases in the presence of two types of eavesdroppers. Numerical results have illustrated the performance-complexity tradeoff among different massive MIMO transmission schemes. Furthermore, RUB scheme can be considered to enhance secrecy performance where only partial CSI of legitimate users is available at the BS as compared with ZF based and MRT based schemes, where the full CSI of legitimate users is required.

Chapter 4

Secrecy Performance Analysis of UAV-Assisted Relaying Communication Systems with Single ground Eavesdroppers

4.1 Introduction

Wireless communication in an urban environment is challenging due to frequent obstructions and occlusions by buildings and other man-made obstacles. Unmanned aerial vehicle (UAV) or drone can enhance communication reliability in such environment by acting as relays to assist the existing communication systems. Unlike traditional fixed ground relay, UAV relaying can adjust its location to cope with the change of communication environment. Such development motivates many research works on UAV-assisted relaying system in an urban scenario. More specifically, [108] derives the optimal altitude for maximum coverage of the ground nodes in an urban communication environment. The outage probability and optimal altitude for a multiple-hop UAV-assisted relaying system are studied in [109]. The authors in [110] investigate the outage performance of a UAV-assisted relaying system with energy harvesting under various parameters settings. In [111], the authors study the optimal UAV relay position to enhance end-to-end throughput. The authors in [112] investigate a UAV relay trajectory planning in an urban environment based on air-to-ground signal strength.

Meanwhile, UAV-assisted relaying systems face serious security challenges, especially in urban environment. First of all, the UAV-to-user channel can be easily eavesdropped. Since urban environment is densely populated, it is very difficult to identify and avoid eavesdroppers. Physical layer security (PLS) can enhance the security of wireless transmission by leveraging the wireless channel characteristics [113]. We note that the study of the secrecy performance of UAV-assisted relaying system, especially in the urban environment, is very limited. The authors in [81] analyze the secrecy outage probability (SOP) for a UAV-assisted network with multiple UAV transmitters, multiple UAV relays, and multiple collaborative UAV eavesdroppers. The authors in [82] analyze a ground communication network consisting of a transmitter, a legitimate user, and an eavesdropper with the deployment of a UAV jammer. In [83], the authors study a UAV-assisted jamming scheme for improving the secrecy rate of ground wiretap channel. Besides, the secrecy performance of UAV-assisted relaying system has also been investigated in [84, 85, 86]. The main challenge of secrecy performance analysis of UAV-assisted relay system in urban environment is the consideration of shadowing effect caused by the high density of man-made structures.

In this chapter, we study the secrecy performance of a UAV-assisted relaying communication system including a ground base station (GBS), a UAV relay, a legitimate ground user (Bob), and a ground eavesdropper (Eve) in urban environments. We assume the direct GBS-to-Bob channel is blocked and Eve tries to eavesdrop UAV-to-Bob channel, which is subject to random shadowing effect. We derive the closed-form approximation of the intercept probability and the ergodic secrecy rate of the system considering both line-of-sight (LoS) and non-LoS (NLoS) propagation groups. We present numerical results which provide useful insight into the secrecy performance of UAV-assisted communication systems in urban environment, including the effect of the altitude of UAV, the types of the urban environment, and the UAV transmit power.

The remainder of this chapter is organized as follows. The system and channel models are presented in Section 4.2. We derive the expressions of the ergodic secrecy rate and intercept probability in Section 4.3 and Section 4.4, respectively. Numerical results are shown in Section 4.5. Finally, we draw our conclusions in Section 4.6.

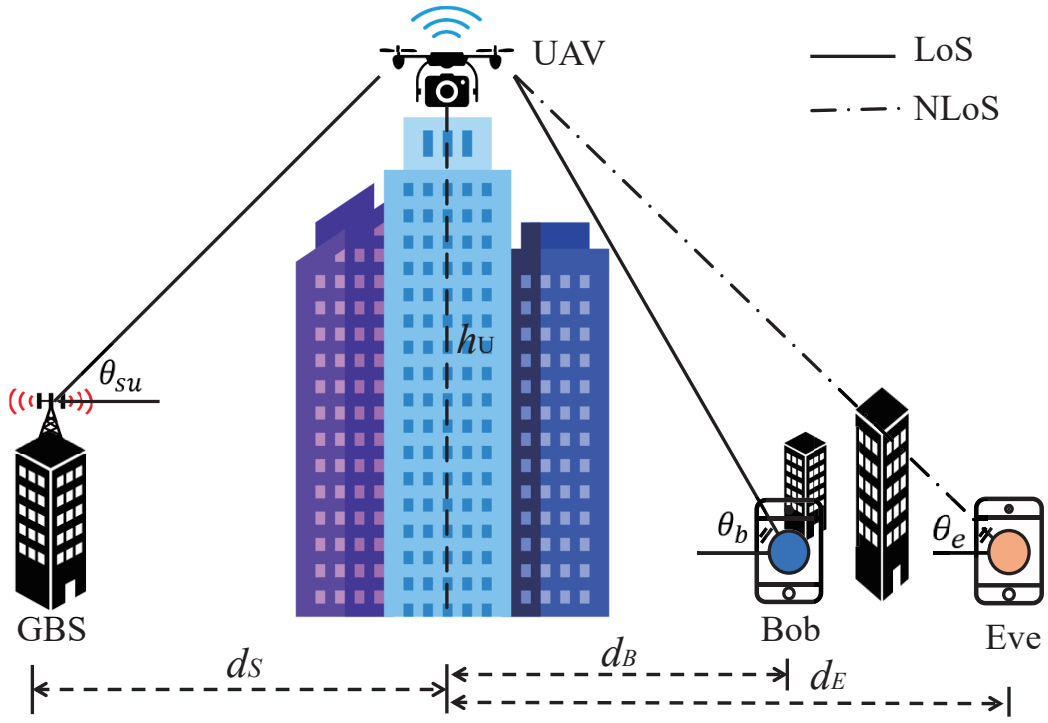

Figure 4.1: UAV relay-assisted relaying communication system in the presence of a single passive eavesdropper.

4.2 System and Channel Models

We consider a UAV-assisted relaying communication system, as shown in Fig. 6.1, in which a GBS intends to send information to Bob with the help of a decode-and-forward (DF) UAV relay in the presence of Eve. We assume that the direct link from GBS to Bob/Eve is blocked due to large obstructions, such as skyscrapers or large buildings in the urban environment. We also ignore the effect of small scale fading. We further assume that the UAV is hovering over a small area, the dimension of which is much smaller than the distance from UAV to users. As such, the effect of UAV movement is captured by shadowing effect. The altitude of the UAV relay is h_U, and the horizontal distances between the GBS and the UAV relay, between the UAV relay and Bob and between the UAV relay and Eve are d_S, d_B and d_E, respectively.

In the first hop, the GBS transmits its signal to the UAV relay, while in the second hop, the UAV relay forwards its decoded signal to Bob. Eve eavesdrops the transmitted message from the UAV relay. The received symbol at the UAV relay can

be expressed as

$$y_{su} = \sqrt{P_s}\sqrt{L_{su}}x_s + n_{su}, \tag{4.1}$$

where P_s is the ground base station power, L_{su} is the power attenuation due to path loss and shadowing effects, x_s denotes the transmit symbol with unit power, and n_{su} is the additive white Gaussian noise with zero mean and variance N_0. The instantaneous received signal to noise ratio (SNR) at the UAV relay can be expressed as

$$\gamma_{su} = \frac{P_s|g_{su}|^2}{L_0 N_0}, \tag{4.2}$$

where L_0 is the free space path loss (FSPL) between GBS and UAV, depending on the distance between GBS and UAV given by $\sqrt{h_U^2 + d_S^2}$, and $|g_{su}|^2$ is the log-normal shadowing gain, which can be expressed as [114]

$$|g_{su}|^2 = \exp\left(-\frac{\sigma_{su}^2}{2} + \sigma_{su}X\right), \tag{4.3}$$

where $\sigma_{su} = \frac{\ln(10)}{10}a_{su}e^{-b_{su}\theta_{su}}$ with elevation angle θ_{su} and frequency and environment dependent parameters, a_{su} and b_{su} and X is a normal variable with zero mean and unit variance. As such, the cumulative distribution function (CDF) of the received SNR at the UAV can be obtained as

$$F_{\gamma_{su}}(x) = 1 - \frac{1}{2}\,\mathrm{erfc}\left(\frac{\ln x - \mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right), \tag{4.4}$$

where $\mu_{\gamma_{su}} = -\frac{\sigma_{su}^2}{2} + \ln\left(\frac{P_s}{L_0 N_0}\right)$ and $\mathrm{erfc}(\cdot)$ is the complementary error function, defined as $\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt$.

In the second hop, the UAV relay transmits the re-encoded symbol x_u with power P_u. As UAV communicates with user j, $j \in \{b : \text{Bob}, e : \text{Eve}\}$ over an urban environment, we consider two main propagation groups based on the definition in [114] over UAV-to-user links. The first group corresponds to the LoS condition with $\xi_j = 1$, while the second group corresponds to NLoS with $\xi_j = 2$. Let p_{ξ_j} denote the probability of these two propagation groups for target user j. Thus, the probability

of LoS group can be expressed as [115]

$$p_1 = 1 - p_2 = \frac{1}{1 + a_j \exp(-b_j \theta_j)}, \tag{4.5}$$

where θ_j denotes elevation angle in radian between UAV and user j, and a_j and b_j are constant values determined by the environment characteristics and the transmission frequency. As such, the received symbol at user j can be expressed as

$$y_{uj} = \sqrt{P_u}\sqrt{L_{\xi_j}} x_u + n_{uj}, \tag{4.6}$$

where L_{ξ_j} is the power loss attenuation for propagation group ξ_j, and n_{uj} is the additive white Gaussian noise with zero mean and the variance N_0 at user j. The instantaneous received SNR at user j under the propagation group ξ_j can be expressed as

$$\gamma_{uj} = \frac{P_u |g_{\xi_j}|^2}{L_{0\xi_j} N_0}, \tag{4.7}$$

where $L_{0\xi_j}$ is the FSPL between UAV and user j and $|g_{\xi_j}|^2$ is the log-normal shadowing gain for propagation group ξ_j. After some mathematical manipulations, the CDF of the received SNR at user j can be obtained as

$$F_{\gamma_{uj}}(x) = 1 - \sum_{\xi_j=1}^{2} \frac{p_{\xi_j}}{2} \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{uj}}}{\sqrt{2\sigma_{\xi_j}^2}}\right), \tag{4.8}$$

where $\mu_{\gamma_{uj}} = -\frac{\sigma_{\xi_j}^2}{2} + \ln\left(\frac{P_u}{L_{0\xi_j} N_0}\right)$ and $\sigma_{\xi_j} = \frac{\ln(10)}{10} a_{\xi_j} e^{-b_{\xi_j}\theta_j}$.

With DF UAV relay, the instantaneous effective end-to-end SNR γ_{sj} at user j can be written as $\gamma_{sj} = \min(\gamma_{su}, \gamma_{uj})$. The CDF of the received SNR at user j can be obtained as

$$F_{sj}(x) = 1 - [1 - F_{su}(x)][1 - F_{uj}(x)]. \tag{4.9}$$

Substituting (4.4) and (4.8) into (4.9), we obtain the CDF of the end-to-end SNR γ_{sj}

at user j as

$$F_{sj}(x) = 1 - \sum_{\xi_j=1}^{2} \frac{p_{\xi_j}}{4} \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right) \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{uj}}}{\sqrt{2\sigma_{\xi_j}^2}}\right). \tag{4.10}$$

4.3 Ergodic Secrecy Rate

Non-zero instantaneous secrecy rate exists when legitimate user's instantaneous channel capacity is larger than the eavesdropper's instantaneous channel capacity, given by [6]

$$C_s = \begin{cases} \log_2(1+\gamma_{sb}) - \log_2(1+\gamma_{se}), & \text{if} \quad \gamma_{sb} > \gamma_{se}; \\ 0, & \text{if} \quad \gamma_{sb} \leq \gamma_{se}. \end{cases} \tag{4.11}$$

As such, the ergodic secrecy rate can be calculated as [98]

$$\mathbb{E}[C_s] = \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_{se}}(x)}{1+x} [1 - F_{\gamma_{sb}}(x)] dx. \tag{4.12}$$

Substituting the CDF of SNR at Bob and Eve in (4.10) into (4.12), we can calculate the ergodic secrecy rate as

$$\begin{aligned} \mathbb{E}[C_s] = \sum_{\xi_b=1}^{2} \sum_{\xi_e=1}^{2} \frac{p_{\xi_b} p_{\xi_e}}{4 \ln 2} \int_0^\infty \frac{1}{1+x} \left[1 - \frac{1}{4} \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right) \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{ue}}}{\sqrt{2\sigma_{\xi_e}^2}}\right)\right] \\ \times \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right) \operatorname{erfc}\left(\frac{\ln x - \mu_{\gamma_{ub}}}{\sqrt{2\sigma_{\xi_b}^2}}\right) dx. \end{aligned} \tag{4.13}$$

Applying Gauss-Hermite Quadrature integration result [116], the closed-form approximation of the ergodic secrecy rate can be obtained as

$$\mathbb{E}[C_s] \simeq \frac{p_{\xi_b} p_{\xi_e}}{4 \ln 2} \sum_{\xi_b=1}^{2} \sum_{\xi_e=1}^{2} \sum_{j=1}^{n} w_j \left(g_{I_1}(x_j) - \frac{1}{4} g_{I_2}(x_j) \right), \tag{4.14}$$

where n is the number of sample points used, x_j, $j = 1, 2, \cdots, n$, is the roots of the physicists' version of the Hermite polynomial $H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$ [117], the associated weights w_j are given by

$$w_j = \frac{2^{n-1} n! \sqrt{\pi}}{n^2 [H_{n-1}(x_j)]^2} [116], \tag{4.15}$$

$$g_{I_1}(t) = \frac{e^{t^2+t}}{1+e^t} \operatorname{erfc}\left(\frac{t-\mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right) \operatorname{erfc}\left(\frac{t-\mu_{\gamma_{ub}}}{\sqrt{2\sigma_{\xi_b}^2}}\right) \tag{4.16}$$

and

$$g_{I_2}(t) = \frac{e^{t^2+t}}{1+e^t} \operatorname{erfc}^2\left(\frac{t-\mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right) \operatorname{erfc}\left(\frac{t-\mu_{\gamma_{ue}}}{\sqrt{2\sigma_{\xi_e}^2}}\right) \operatorname{erfc}\left(\frac{t-\mu_{\gamma_{ub}}}{\sqrt{2\sigma_{\xi_b}^2}}\right). \tag{4.17}$$

4.4 Intercept Probability

The intercept probability is the probability that the instantaneous end-to-end SNR at Bob is less than that at. Eve (i.e. $\gamma_{sb} \leq \gamma_{se}$). Conditioning on γ_{se}, the intercept probability can be calculated as

$$P_{\text{int}} = \int_0^\infty p_{\gamma_{se}}(x) F_{\gamma_{sb}}(x) dx, \tag{4.18}$$

where $p_{\gamma_{se}}(x)$ and $F_{\gamma_{sb}}(x)$ denote the probability density function (PDF) of end-to-end SNR at Eve and the CDF of end-to-end SNR at Bob, respectively.

Substituting the corresponding PDF of SNR at Eve and the CDF of SNR at Bob

in (4.10) into (4.18), we can rewrite P_{int} as

$$P_{\text{int}} = \sum_{\xi_b=1}^{2}\sum_{\xi_e=1}^{2}\int_0^{\infty}\frac{p_{\xi_b}p_{\xi_e}}{2x\sqrt{2\pi}}\Bigg[\frac{\exp\left(-\left(\frac{\ln x-\mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right)^2\right)}{\sqrt{\sigma_{su}^2}}\operatorname{erfc}\left(\frac{\ln x-\mu_{\gamma_{ue}}}{\sqrt{2\sigma_{\xi_e}^2}}\right)$$
$$+\frac{\exp\left(-\left(\frac{\ln x-\mu_{\gamma_{ue}}}{\sqrt{2\sigma_{\xi_e}^2}}\right)^2\right)}{\sqrt{\sigma_{\xi_e}^2}}\operatorname{erfc}\left(\frac{\ln x-\mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right)\Bigg]\Bigg[1-\frac{1}{4}\operatorname{erfc}\left(\frac{\ln x-\mu_{\gamma_{su}}}{\sqrt{2\sigma_{su}^2}}\right)$$
$$\times\operatorname{erfc}\left(\frac{\ln x-\mu_{\gamma_{ub}}}{\sqrt{2\sigma_{\xi_b}^2}}\right)\Bigg]dx. \tag{4.19}$$

Using the approximation of error function [118] and carrying out integration and manipulations, the closed-form approximation of the intercept probability can be obtained as

$$P_{\text{int}} = \frac{p_{\xi_b}p_{\xi_e}}{2\sqrt{2}}\sum_{\xi_b=1}^{2}\sum_{\xi_e=1}^{2}\left[\sum_{m=1}^{2}\sigma_m\left(\frac{1}{3}I_1+\sqrt{3}I_{2,m}\right)-\sum_{m=1}^{10}I_{3,m}\right], \tag{4.20}$$

where

$$I_1 = \frac{\exp\left(-\frac{(\mu_1-\mu_2)^2}{\sqrt{\sum_{i=1}^{2}\sigma_i}}\right)}{\sqrt{\sum_{i=1}^{2}\sigma_i}}, \tag{4.21}$$

$I_{2,1} = I_2(3,4)$, $I_{2,2} = I_2(4,3)$, $I_{3,1} = I_3(7,4,4,\frac{\sqrt{3}}{8})$, $I_{3,2} = I_3(7,3,4,\frac{3}{8\sqrt{3}})$, $I_{3,3} = I_3(6,3,4,\frac{1}{12\sqrt{3}})$, $I_{3,4} = I_3(2,1,1,\frac{1}{108})$, $I_{3,5} = I_3(7,3,3,\frac{1}{8\sqrt{3}})$, $I_{3,6} = I_3(7,4,3,\frac{1}{8\sqrt{3}})$, $I_{3,7} = I_3(6,4,3,\frac{1}{24\sqrt{3}})$, $I_{3,8} = I_3(3,2,2,\frac{1}{256\sqrt{6}})$, $I_{3,9} = I_3(8,3,4,\frac{\sqrt{3}}{8})$ and $I_{3,10} = I_3(8,3,3,\frac{1}{\sqrt{3}})$. Here

$$I_2(a_1,a_2) = \frac{\exp\left(-\frac{4(\mu_1-\mu_2)^2}{\sqrt{\sum_{i=1}^{2}a_i\sigma_i}}\right)}{\sqrt{\sum_{i=1}^{2}a_i\sigma_i}}, \tag{4.22}$$

and

$$I_3(a_1,a_2,a_3,a_4)=\frac{a_4\exp\left(\frac{(\sum\limits_{i=1}^{3}\prod\limits_{\substack{j=1\\j\neq i}}^{3}a_j\frac{\mu_i}{\sigma_i})^2}{3\sum\limits_{i=1}^{3}\prod\limits_{\substack{j=1\\j\neq i}}^{3}\frac{a_j}{\sigma_i}}\right)}{\sqrt{\sum\limits_{i=1}^{3}\prod\limits_{\substack{j=1\\j\neq i}}^{3}\frac{a_j}{\sigma_i}}\exp\left(\frac{1}{3}\sum\limits_{i=1}^{3}\prod\limits_{\substack{j=1\\j\neq i}}^{3}a_j\frac{\mu_i^2}{\sigma_i}\right)}, \tag{4.23}$$

μ_i, $i=1,2,3$, denote $\mu_{\gamma_{su}}$, $\mu_{\gamma_{ue}}$, $\mu_{\gamma_{ub}}$, respectively, and σ_i, $i=1,2,3$, denote $2\sigma_{su}^2$, $2\sigma_{\xi_e}^2$, $2\sigma_{\xi_b}^2$, respectively.

4.5 Numerical Results

In this section, we present selected numerical results to investigate the security performance of a UAV-assisted relaying system. The adopted urban environments parameters with the carrier frequency $f_c = 2000$ MHz follow those used in [114], [119].

Fig. 4.2 presents the intercept probability as a function of eavesdropper distance d_E in an urban environment. We can see that the intercept probability decreases as d_E increases. Without loss of generality, we assume that the random small scale fading factor follows Rician distribution with shape parameter $K = 1/2$. As such, we can also observe that the small scale fading has a negligible effect on intercept probability. This is because path loss and shadowing effects play the dominant role in aerial communication systems.

Fig. 4.3 presents the intercept probability of UAV-assisted relaying system vs. UAV height h_U for different d_E values in different urban environments. We can see that the approximate results match well with the exact results from numerical integration. We can also see that when $d_E > d_B$ the intercept probability first decreases and then increases, and finally approaches $1/2$ with increasing h_U. The reason is that initial increase of h_U can increase the probability of the LoS transmission for Bob more than Eve. Further increasing h_U results in a higher path-loss for both UAV-to-Bob and UAV-to-Eve channels, causing the quality of both channels very similar. For the same reason, the trend reverses when $d_E < d_B$. Moreover, we can also observe that the intercept probability for urban environment is larger than that for dense urban environment when $d_E < d_B$, and the trend reverses when $d_E > d_B$. We note that the probability of LoS decreases and shadowing variance increases when moving from

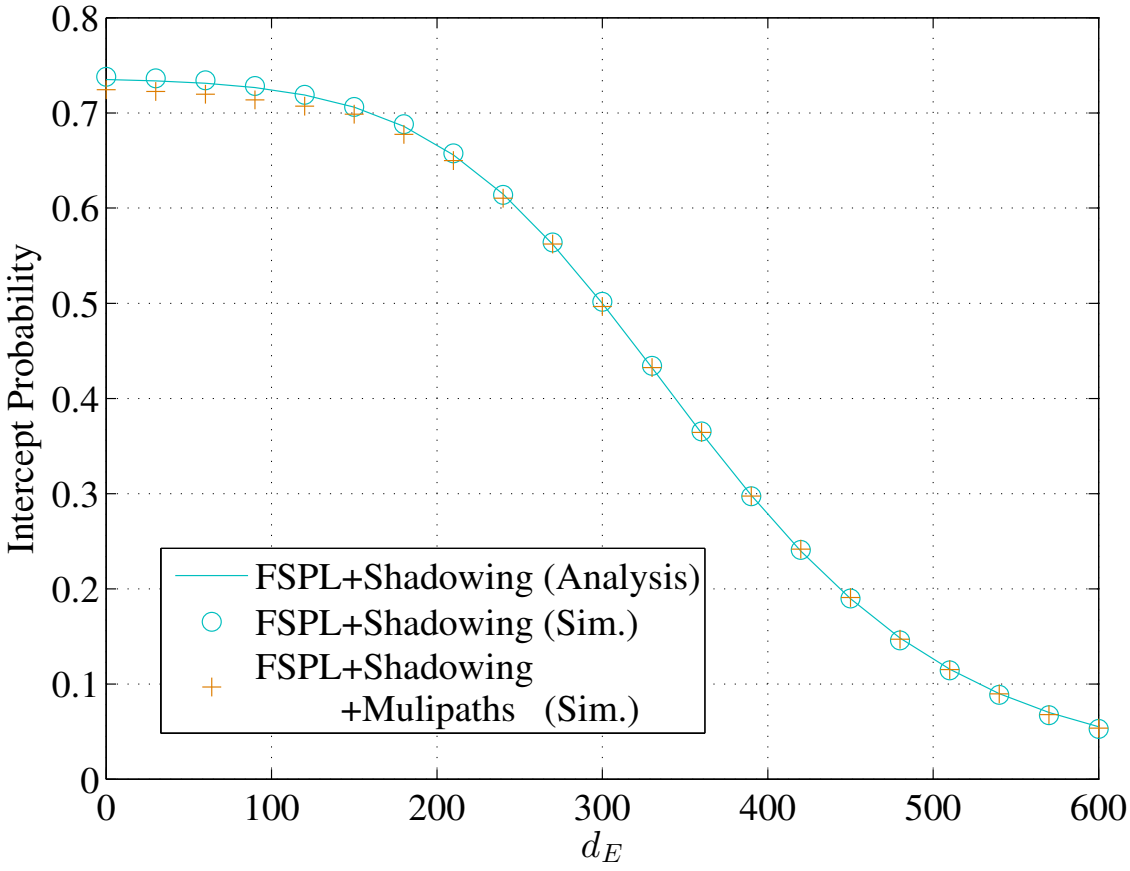

Figure 4.2: Intercept probability versus d_E in an urban environment ($d_S = 250$ m, $h_U = 1000$ m, $d_B = 300$ m, $P_s = P_u = 10$ dBm).

urban environment to dense urban environment. When $d_E < d_B$, Eve experiences less path loss but larger shadowing variance in the dense urban environment, which helps reduce the intercept probability. When d_E is larger than d_B, the shadowing variation benefits Eve more, leading to a higher intercept probability in the dense urban environment.

Fig. 4.4 shows the ergodic secrecy rate as a function of UAV height h_U for different d_E values in different urban environments. We can see that the approximate results match well with the exact results from numerical integration. Besides, we can also observe that the ergodic secrecy rate decreases as h_U increases, due to an increasing path loss for UAV-to-Bob channel, which reduces the amount of data that can be securely transmitted. The ergodic secrecy rate in both urban and dense urban environments is higher when $d_B < d_E$, as expected. Meanwhile, the ergodic secrecy performance

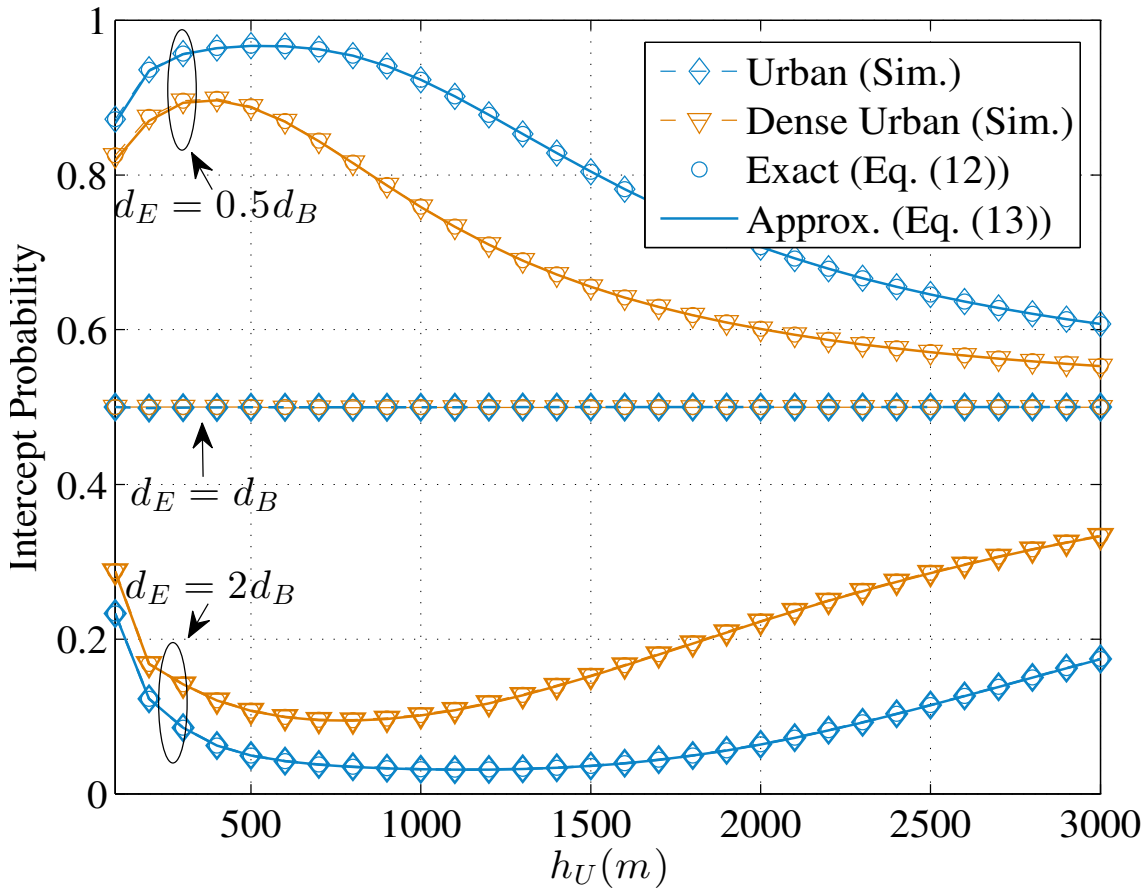

Figure 4.3: Intercept probability versus h_U for different values of d_E in different urban environments ($d_S = 150$ m, $d_B = 300$ m, $P_s = P_u = 10$ dBm).

benefits from larger shadowing variance of dense urban environment when $d_E < d_B$, but suffers from it when $d_E > d_B$.

Fig. 4.5 shows the ergodic secrecy rate as a function of the UAV relay transmit power P_u for different GBS transmit power P_s in different urban environments. We observe that the ergodic secrecy rate first increases, then decreases with increasing P_u, and finally converges to a constant value. We can explain the behaviour as follows. The end-to-end SNR γ_{sj} is limited by the second hop SNR γ_{uj} when P_u is much lower than P_s. The increasing P_u leads to an increase of γ_{sj}, resulting in the growth of the ergodic secrecy rate. When P_u is slightly larger than P_s, γ_{sb} is largely determined by the first hop SNR γ_{su} while the end-to-end SNR for Eve γ_{se} is still determined by the second hop SNR γ_{ue}, since the distance of UAV-to-Eve channel is larger than the distance of UAV-to-Bob channel. In this situation, the enhancement

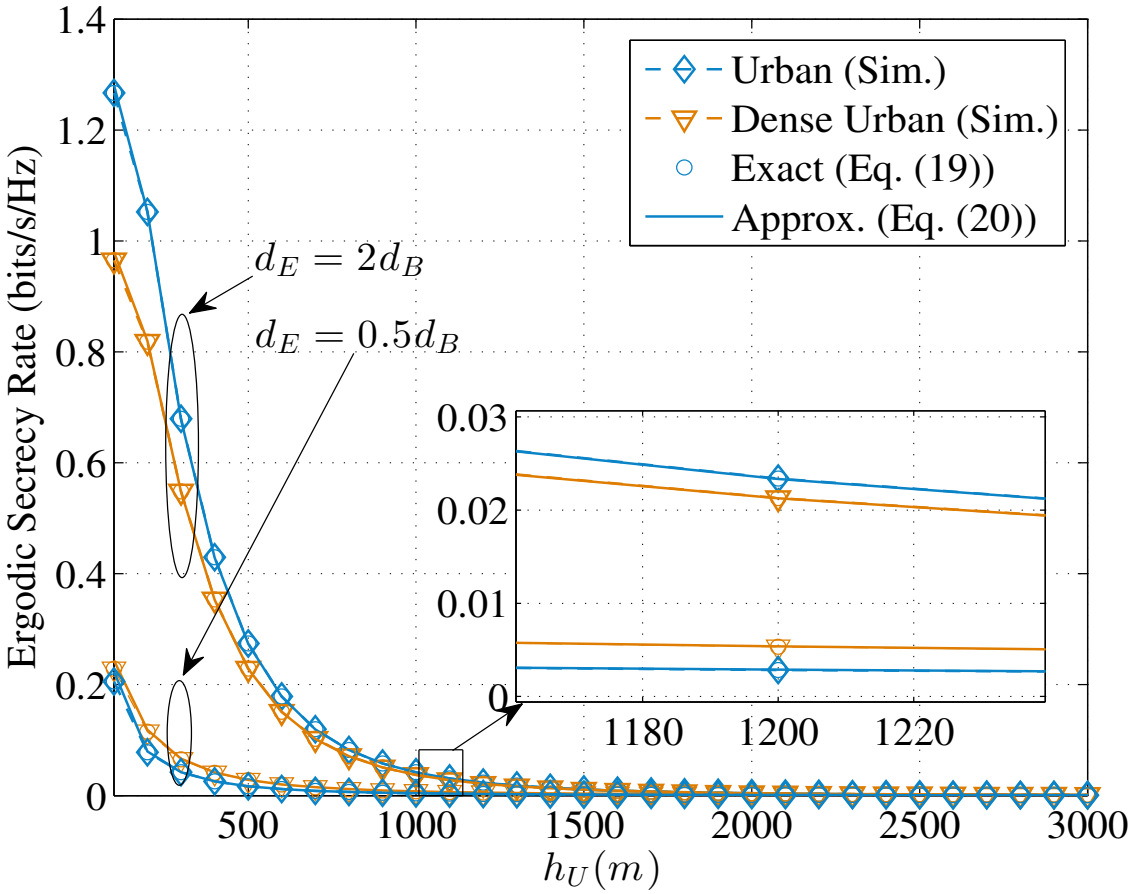

Figure 4.4: Ergodic secrecy rate versus h_U for different values of d_E in different urban environments ($d_S = 150$ m, $d_B = 300$ m, $P_s = P_u = 10$ dBm, $n = 20$).

of the instantaneous capacity at Eve is higher than the enhancement at Bob with the increasing P_u, which results in the decrease of the ergodic secrecy rate. However, when P_u is much larger than P_s, the first hop SNR γ_{su} limits both γ_{sb} and γ_{se}, resulting in a constant secrecy rate value.

4.6 Conclusions

In this chapter, we analyze the secrecy performance of a UAV-assisted relaying system with a single eavesdropper in urban environments. We derive the closed-form approximation of the intercept probability and the ergodic secrecy rate. The numerical results show that increasing UAV height has different effect on intercept probability depending on whether Bob or Eve is closer to UAV. We also show that shadowing

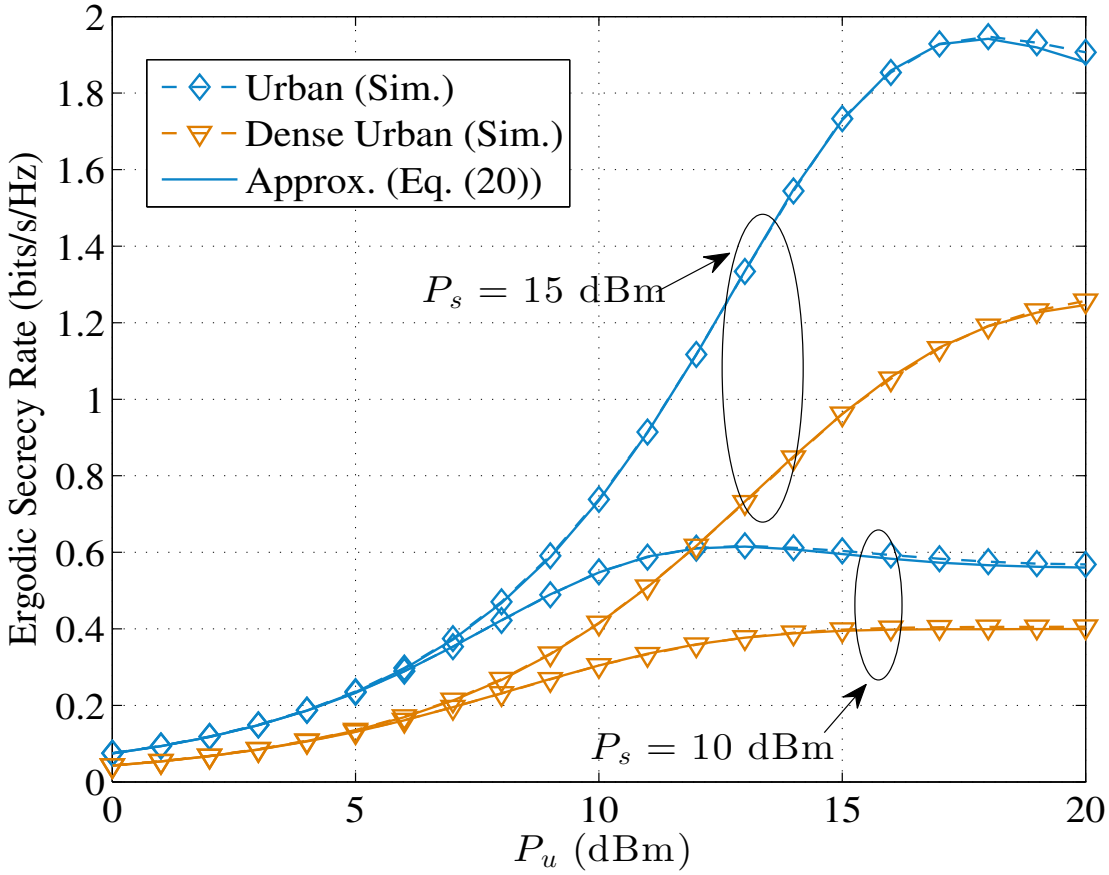

Figure 4.5: Ergodic secrecy rate versus P_u for different transmit power P_s in different urban environments ($h_U = 200$ m, $d_S = 250$ m, $d_B = 300$ m and $d_E = 2d_B = 600$ m).

effect can benefit the ergodic secrecy performance when Eve is closer to UAV than Bob. Finally, we find that increasing UAV transmit power may not always increase ergodic secrecy rate.

Chapter 5

Secrecy Outage Performance Analysis of UAV-assisted Relaying Communication Systems with Multiple Aerial and Ground Eavesdroppers

5.1 Introduction

Unmanned aerial vehicles (UAVs), deployed as relays, can enhance the coverage and connectivity of traditional wireless communication systems, due to their inherent properties, such as high mobility and flexible deployment [120]. Meanwhile, security is a significant challenge in UAV-assisted relaying communication systems since UAVs are mostly unattended, and as such highly subject to eavesdropping. Physical layer security has been proposed to improve the communication security by exploiting wireless channel characteristics [121].

Many research works have studied the secrecy performance of UAV-assisted relaying communication systems in the presence of one or more eavesdroppers [79, 80]. The authors in [122] derive the closed-form approximation of the ergodic secrecy rate and intercept probability while a ground base station (GBS) sends information to a legitimate ground user with the help of a UAV relay in the presence of a ground eavesdropper. Furthermore, multiple eavesdroppers considered as non-cooperation

are often assumed to operate independently, whereas these eavesdroppers may cooperative to enhance their eavesdropping capability. In [87], the authors investigate the secrecy performance of a UAV-assisted relaying system with multiple non-cooperative ground eavesdroppers following an independent homogeneous Poisson point process (PPP) in the two-dimensional (2D) space. The authors assume selection combining (SC) scheme to combine the direct and relay branches at eavesdroppers. In [88], the secrecy outage probability (SOP) is derived for a secure communication system in the presence of multiple cooperative UAV eavesdroppers with the help of UAV swarm relay in the three-dimensional (3D) space. Maximum-ratio combining (MRC) is applied across multiple UAV eavesdroppers for overhearing the legitimate transmissions from both the selected UAV transmitter and the UAV relay. Meanwhile, most works on secrecy performance analysis under traditional relay networks have focused on relay selection rather than cooperative strategies among multiple eavesdroppers [123, 124, 125]. As such, it is necessary to investigate the cooperative strategy for both multiple aerial and ground eavesdroppers under a UAV-assisted relaying communication system. Note that while having multiple eavesdroppers can degrade the secrecy performance, directional beamforming transmission can be employed in UAV networks together with maintaining protection zones around the destinations to enhance secrecy performance [126]. Moreover, random shadowing can impact channel quality for UAV-based communications [122]. Yet, the existing works have not considered such an important effect.

Motivated by the above, this paper aims to analyze the SOP of a UAV-assisted relay communication system taking into account the shadowing effect, directional beamforming, and cooperation between ground and aerial eavesdroppers. In the considered system, the UAV acts as a decode-and-forward (DF) relay to re-transmit the signal from a GBS to the legitimate user in the presence of multiple UAV and ground eavesdroppers. Particularly, we assume that multiple UAV and ground eavesdroppers are randomly located outside of the protection zones in 3D and 2D space, following a homogeneous PPP distribution, respectively. Herein, we study both the non-cooperative and cooperative scenarios between the UAV and ground eavesdroppers. By assuming the most general κ-μ shadowed fading channel [127], we derive the exact closed-form expression of SOP for both scenarios of cooperation. Through selected numerical results, we examine the effect of different parameters on the SOP performance.

The remainder of this chapter is organized as follows. The system and channel

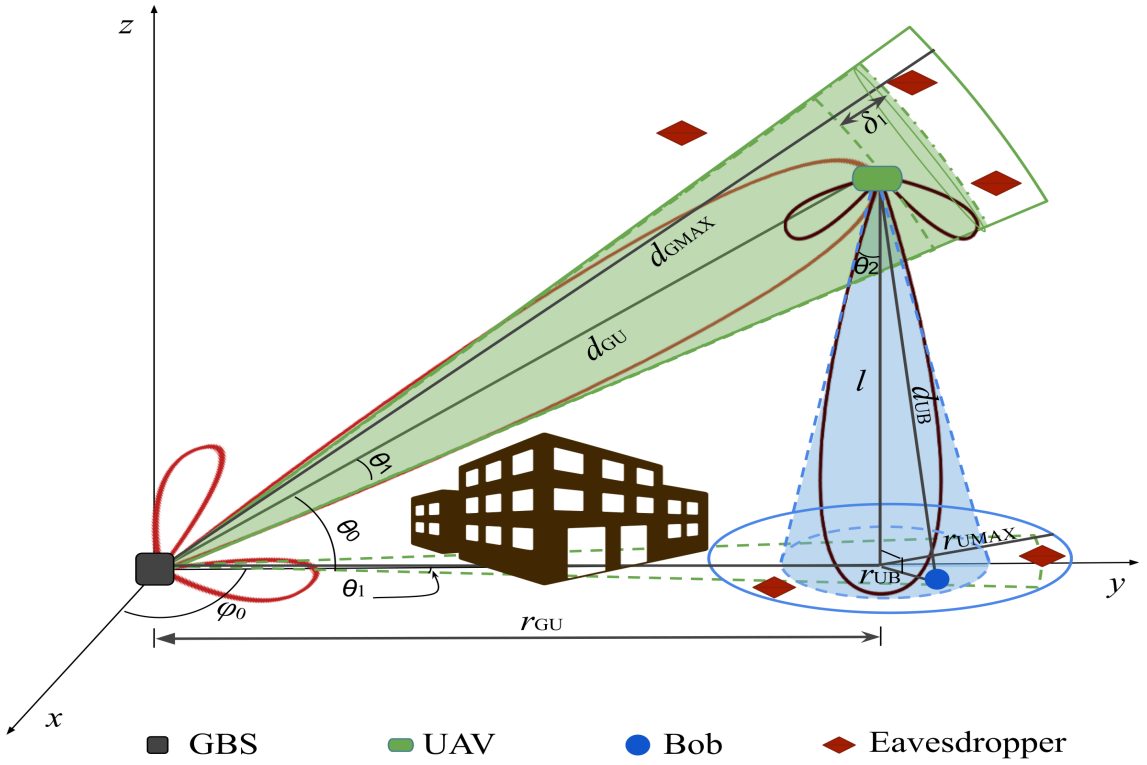

Figure 5.1: Illustration of 3D geometric model of UAV-assisted relaying communication system in the presence of multiple colluding UAV eavesdroppers.

models are presented in Section 5.2. The moment generating function (MGF) of eavesdropping SNR in the first hop and the second hop is derived in Section 5.3. We derive the SOP analysis for non-cooperative and cooperative aerial and ground eavesdroppers in Section 5.4. Numerical results are shown in Section 5.5. Finally, we draw our conclusions in Section 5.6.

5.2 System and Channel Models

We consider a UAV-assisted relay communication system, as shown in Fig. 6.1, where a GBS transmits confidential information to the legitimate ground user Bob. Since the direct link from the GBS to Bob is blocked by large obstructions, e.g. mountains and/or skyscrapers, the system employs a UAV relay to forward the information in a DF fashion. Multiple aerial and ground eavesdroppers are assumed to try to eavesdrop the information at different locations of the system.

5.2.1 GBS-to-UAV Transmission

We assume the GBS, with a maximum coverage area radius of d_{GMAX}, is located at the origin of the 3D space and the UAV relay is spatially located at a distance d_{GU} ($d_{\mathrm{GU}} < d_{\mathrm{GMAX}}$), with an elevation angle θ_0, and azimuth angle φ_0, from the GBS. As such, the altitude of the UAV relay is $l = d_{\mathrm{GU}} \sin(\theta_0)$. The GBS employs directional beamforming transmission towards the UAV relay. For the sake of analytical tractability, we assume an ideal beam pattern with half beamwidth θ_1 and constant gains inside and outside of beamforming direction. Specifically, the GBS antenna gain is approximately given by

$$G_{\mathrm{GBS}} = \begin{cases} G_1, & \text{inside beamforming direction;} \\ \eta G_1, & \text{outside beamforming direction,} \end{cases} \tag{5.1}$$

where $\eta < 1$ is an attenuating factor. Assuming a log-distance path-loss and shadowed fading model, the received symbol at the UAV relay can be expressed as

$$y_{\mathrm{GU}} = \sqrt{P_t G_1} \sqrt{K d_{\mathrm{GU}}^{-\alpha}} h_{\mathrm{GU}} x_t + n_{\mathrm{GU}}, \tag{5.2}$$

where P_t is the transmit power of the GBS, K is the path-loss constant, α denotes the path-loss exponent, h_{GU} denotes the complex fading channel gain, x_t is the transmit symbol with unit power, and n_{GU} is the additive white Gaussian noise with zero mean and variance N_0. Accordingly, the instantaneous received singal to noise ratio (SNR) at the UAV relay is given by

$$\gamma_{\mathrm{GU}} = \frac{P_t G_1 K d_{\mathrm{GU}}^{-\alpha} |h_{\mathrm{GU}}|^2}{N_0} = \rho_1 d_{\mathrm{GU}}^{-\alpha} |h_{\mathrm{GU}}|^2, \tag{5.3}$$

where $\rho_1 = P_t G_1 K / N_0$ and $|h_{\mathrm{GU}}|^2$ is the fading channel power gain for the UAV relay with $\mathbb{E}[|h_{\mathrm{GU}}|^2] = 1$.

To enhance the secrecy performance, the GBS implements a protection zone along the beamforming direction, with the help of a radar system. The range of the radar system is $d_{\mathrm{GU}} + \delta_1$. As such, aerial eavesdroppers can only hover outside the protection zone, i.e. at distances greater than $d_{\mathrm{GU}} + \delta_1$ from the GBS along the beamforming direction and at arbitrarily distances outside it. The received symbol at a particular

aerial eavesdropper can be expressed as

$$y_{\mathrm{Ge}} = \sqrt{P_t G_{\mathrm{GBS}}}\sqrt{K d_{\mathrm{Ge}}^{-\alpha}} h_{\mathrm{Ge}} x_t + n_{\mathrm{Ge}}, \tag{5.4}$$

where d_{Ge} is the distance between the GBS and eavesdropper and n_{Ge} is the additive white Gaussian noise with zero mean and variance N_0. As such, the instantaneous SNR at the eavesdropper is given by

$$\gamma_{\mathrm{Ge}} = \rho d_{\mathrm{Ge}}^{-\alpha} |h_{\mathrm{Ge}}|^2, \tag{5.5}$$

where $\rho = P_t G_{\mathrm{GBS}} K / N_0$ is the transmit SNR and $|h_{\mathrm{Ge}}|^2$ is the fading channel power gain with $\mathbb{E}[|h_{\mathrm{Ge}}|^2] = 1$.

We assume that the aerial eavesdroppers cooperate with each other. Particularly, the signals received at the different eavesdroppers are combined together using MRC before detection [106]. As such, the effective eavesdropping SNR over the first hop is given by

$$\gamma_{\mathrm{GE}} = \sum_{e \in \Phi_{\mathrm{GE}}} \rho d_{\mathrm{Ge}}^{-\alpha} |h_{\mathrm{Ge}}|^2, \tag{5.6}$$

where Φ_{GE} denotes the set of aerial eavesdroppers.

5.2.2 UAV-to-Bob Transmission

The UAV relay first decodes the information symbol and then forwards it to Bob over the second hop with power P_u. We assume that the UAV relay also adopts beamforming transmission with half mainlobe beamwidth θ_2 and antenna gain approximated as:

$$G_{\mathrm{UAV}} = \begin{cases} G_2, & \text{inside beamforming direction;} \\ \eta G_2, & \text{outside beamforming direction.} \end{cases} \tag{5.7}$$

As shown in Fig. 6.1, the coverage of the second hop is a circular area centered at the UAV relay's ground projection with a radius of $l \tan(\theta_2)$, and there exist a protection zone around it with radius r_{UMAX}. We assume that Bob lies inside the coverage area with distance $d_{\mathrm{UB}} < l/\cos(\theta_2)$ from the UAV relay and no UAV eavesdropper is in the protected area to eavesdrop on the second hop. As such, the instantaneous received

SNR at Bob is given by

$$\gamma_{\mathrm{UB}} = \rho_2 d_{\mathrm{UB}}^{-\alpha} |h_{\mathrm{UB}}|^2, \tag{5.8}$$

where $\rho_2 = P_u G_2 K / N_0$ and $|h_{\mathrm{UB}}|^2$ is the normalized fading channel power gains.

With the help of the UAV relay, Bob can ensure that no eavesdropper is located inside the coverage area of the beamforming direction, yet, multiple ground eavesdroppers are randomly located outside of the mainlobe area, following a PPP of density λ_{UE}. The instantaneous SNR at a ground eavesdropper is given by

$$\gamma_{\mathrm{Ue}} = \eta \rho_2 d_{\mathrm{Ue}}^{-\alpha} |h_{\mathrm{Ue}}|^2, \tag{5.9}$$

where $|h_{\mathrm{Ue}}|^2$ is the fading channel power gains with $\mathbb{E}[|h_{\mathrm{Ue}}|^2] = 1$ and distance $d_{\mathrm{Ue}} > l/\cos(\theta_2)$. Following the colluding eavesdropper assumption, the effective eavesdropping SNR over the second hop is given by

$$\gamma_{\mathrm{UE}} = \sum_{e \in \Phi_{\mathrm{UE}}} \eta \rho_2 d_{\mathrm{Ue}}^{-\alpha} |h_{\mathrm{Ue}}|^2, \tag{5.10}$$

where Φ_{UE} denotes the set of ground eavesdroppers.

Throughout the analysis, the general κ-μ shadowed fading model that takes into account the existence of the Line of Sight (LOS) component and local obstacles is assumed. As such, the cumulative distribution function (CDF) of the received SNRs at legitimate destinations and eavesdroppers are generally given by [127]

$$F_{\gamma_M}(x) = 1 - \sum_{i=0}^{m-\mu} C_i \exp\left(-\frac{x}{\rho_N d_M^{-\alpha} a_1}\right) \sum_{j=0}^{m-i-1} \frac{1}{j!} \left(\frac{x}{\rho_N d_M^{-\alpha} a_1}\right)^j, \tag{5.11}$$

where $M \in \{\mathrm{GU}, \mathrm{Ge}, \mathrm{UB}, \mathrm{Ue}\}$, $N = 1$ or 2 depending up the hop under consideration, C_i and a_1 are expressed in terms of the κ-μ shadowed fading parameters (κ, μ and m) as $C_i = \binom{m-\mu}{i} \left(\frac{m}{\kappa+m}\right)^i \left(\frac{\kappa}{\kappa+m}\right)^{m-\mu-i}$, and $a_1 = \frac{\kappa+m}{m\mu(1+\kappa)}$. Here, κ is the strength of LOS component, μ is the number of clusters and m is the parameter of the Nakagami-m fading.

5.3 MGF of Eavesdropping SNR

In this section, we derive the MGF of eavesdropping SNR.

5.3.1 First Hop

Applying the probability generating functional (PGFL) for the PPP Φ_{GE}, the MGF of γ_{GE} can be calculated as

$$\begin{aligned}\mathcal{M}_{\gamma_{\mathrm{GE}}}(s) &= \mathbb{E}\left[\exp\left(s\sum_{e\in\Phi_{\mathrm{GE}}}\rho d_{\mathrm{Ge}}^{-\alpha}|h_{\mathrm{Ge}}|^2\right)\right] \\ &= \exp\left\{-\lambda_{\mathrm{GE}}\int_V\left[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}\left(\exp\left(s\rho r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\right)\right)\right]d\gamma_e\right\},\end{aligned} \tag{5.12}$$

where V is the spacial area that UAV eavesdroppers are located.

Considering eavesdroppers inside and outside mainlobe separately, the MGF of γ_{GE} can be rewritten by

$$\mathcal{M}_{\gamma_{\mathrm{GE}}}(s) = \mathcal{M}_{\gamma_{\mathrm{GE1}}}(s)\times\mathcal{M}_{\gamma_{\mathrm{GE2}}}(s), \tag{5.13}$$

where

$$\begin{aligned}\mathcal{M}_{\gamma_{\mathrm{GE1}}}(s) \approx \exp\Bigg\{-\lambda_{\mathrm{GE}}\int_{\frac{\pi}{2}-(\theta_0-\theta_1)}^{\frac{\pi}{2}-(\theta_0+\theta_1)}\int_{\varphi_0-\theta_1}^{\varphi_0+\theta_1}\int_{d_{\mathrm{GU}}+\delta_1}^{d_{\mathrm{GMAX}}} r_e^2\sin\theta \\ \left[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}(\exp\left(s\rho_1 r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\right))\right]dr_e d\theta d\varphi\Bigg\},\end{aligned} \tag{5.14}$$

and

$$\mathcal{M}_{\gamma_{\mathrm{GE2}}}(s) \approx \exp\Bigg\{ -\lambda_{\mathrm{GE}}\Bigg[\int_0^{\frac{\pi}{2}-(\theta_0+\theta_1)} \int_0^{2\pi} \int_0^{d_{\mathrm{GMAX}}} r_e^2 \sin\theta \Big[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}\big(\exp\big(s\eta\rho_1 r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\big)\big)\Big] dr_e d\theta d\varphi \Bigg] + \Bigg[\int_{\frac{\pi}{2}-(\theta_0-\theta_1)}^{\frac{\pi}{2}} \int_0^{2\pi} \int_0^{d_{\mathrm{GMAX}}} r_e^2 \sin\theta \Big[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}\big(\exp\big(s\eta\rho_1 r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\big)\big)\Big] dr_e d\theta d\varphi \Bigg] + \Bigg[\int_{\frac{\pi}{2}-(\theta_0+\theta_1)}^{\frac{\pi}{2}-(\theta_0-\theta_1)} \int_0^{\varphi_0-\theta_1} \int_0^{d_{\mathrm{GMAX}}} r_e^2 \sin\theta \Big[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}\big(\exp\big(s\eta\rho_1 r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\big)\big)\Big] dr_e d\theta d\varphi \Bigg] + \Bigg[\int_{\frac{\pi}{2}-(\theta_0+\theta_1)}^{\frac{\pi}{2}-(\theta_0-\theta_1)} \int_{\varphi_0+\theta_1}^{2\pi} \int_0^{d_{\mathrm{GMAX}}} r_e^2 \sin\theta \Big[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}\big(\exp\big(s\eta\rho_1 r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\big)\big)\Big] dr_e d\theta d\varphi \Bigg] - \Bigg[\int_0^{d_{\mathrm{GU}}\sin(\theta_0)+\frac{d_{\mathrm{GU}}^2\sin(\theta_0)\cos(\theta_0)}{r_{\mathrm{UMAX}}}-\frac{d_{\mathrm{GU}}\sin(\theta_0)r_e}{r_{\mathrm{UMAX}}}} \int_{d_{\mathrm{GU}}\cos(\theta_0)}^{d_{\mathrm{GU}}\cos(\theta_0)+r_{\mathrm{UMAX}}} \int_0^{2\pi} r_e \Big[1-\mathbb{E}_{|h_{\mathrm{Ge}}|^2}\big(\exp\big(s\eta\rho_1 r_e^{-\alpha}|h_{\mathrm{Ge}}|^2\big)\big)\Big] \mathrm{d}r_e \mathrm{d}z \mathrm{d}\varphi \Bigg] \Bigg] \Bigg\}. \tag{5.15}$$

Note that we approximate the round spherical sector with rectangle one for a tractable analysis, the accuracy of which is checked using simulation results.

Substituting the MGF of received SNR over κ-μ shadowed fading [127] into (5.14) and after some mathematical manipulation, the closed-form expression of $\mathcal{M}_{\gamma_{\mathrm{GE1}}}(s)$ can be obtained as

$$\mathcal{M}_{\gamma_{\mathrm{GE1}}}(s) = \exp\Bigg\{ -\frac{2}{3}\theta_1\lambda_{\mathrm{GE}}[\sin(\theta_0+\theta_1)-\sin(\theta_0-\theta_1)] \Bigg(d_{\mathrm{GMAX}}^3 \Big[1-F_1\Big(-\frac{3}{\alpha};\mu-m,m;1-\frac{3}{\alpha};s\rho_1 d_{\mathrm{GMAX}}^{-\alpha}a_1, s\rho_1 d_{\mathrm{GMAX}}^{-\alpha}a_2\Big)\Big] - (d_{\mathrm{GU}}+\delta_1)^3 \times \Big[1-F_1\Big(-\frac{3}{\alpha};\mu-m,m;1-\frac{3}{\alpha};s\rho_1(d_{\mathrm{GU}}+\delta_1)^{-\alpha}a_1, s\rho_1(d_{\mathrm{GU}}+\delta_1)^{-\alpha}a_2\Big)\Big] \Bigg) \Bigg\}, \tag{5.16}$$

where $a_2 = \frac{1}{\mu(1+\kappa)}$ and $F_1(a;b_1,b_2;c;x,y) = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{(a)_{m+n}(b_1)_m(b_2)_n}{m!n!(c)_{m+n}} x^m y^n$ with the Pochhammer symbol $(q)_n$ is the Appell hypergeometric function of two variables [128]. Furthermore, the closed-form expression of $\mathcal{M}_{\gamma_{\mathrm{GE2}}}(s)$ can be also obtained following the similar steps. By combining $\mathcal{M}_{\gamma_{\mathrm{GE1}}}(s)$ and $\mathcal{M}_{\gamma_{\mathrm{GE2}}}(s)$, the closed-form

expression of the MGF of γ_{GE} for a κ-μ shadowed fading channel can be obtained as

$$\mathcal{M}_{\gamma_{\mathrm{GE}}}(s) = \exp\Bigg\{ -\frac{2}{3}\theta_1\lambda_{\mathrm{GE}}[\sin(\theta_0+\theta_1)-\sin(\theta_0-\theta_1)]$$
$$\Bigg(d_{\mathrm{GMAX}}^3\Bigg[1-F_1\left(-\frac{3}{\alpha};\mu-m,m;1-\frac{3}{\alpha};s\rho_1 d_{\mathrm{GMAX}}^{-\alpha}a_1, s\rho_1 d_{\mathrm{GMAX}}^{-\alpha}a_2\right)\Bigg] - (d_{\mathrm{GU}}+\delta_1)^3$$
$$\times\Bigg[1-F_1\left(-\frac{3}{\alpha};\mu-m,m;1-\frac{3}{\alpha};s\rho_1(d_{\mathrm{GU}}+\delta_1)^{-\alpha}a_1, s\rho_1(d_{\mathrm{GU}}+\delta_1)^{-\alpha}a_2\right)\Bigg]\Bigg)$$
$$-\frac{2}{3}\lambda_{\mathrm{GE}}\Bigg[\pi-\theta_1[\sin(\theta_0+\theta_1)-\sin(\theta_0-\theta_1)]\Bigg]\Bigg(d_{\mathrm{GMAX}}^3\Bigg[1-F_1\left(-\frac{3}{\alpha};\mu-m,m;1-\frac{3}{\alpha};$$
$$s\eta\rho_1 d_{\mathrm{GMAX}}^{-\alpha}a_1, s\eta\rho_1 d_{\mathrm{GMAX}}^{-\alpha}a_2\right)\Bigg]\Bigg) + \pi\lambda_{\mathrm{GE}}\Bigg[d_{\mathrm{GU}}\sin(\theta_0)+\frac{d_{\mathrm{GU}}^2\sin(\theta_0)\cos(\theta_0)}{r_{\mathrm{UMAX}}}\Bigg]\Bigg((d_{\mathrm{GU}}\cos(\theta_0)$$
$$+r_{\mathrm{UMAX}})^2\Bigg[1-F_1\Bigg(-\frac{2}{\alpha};\mu-m;m;1-\frac{2}{\alpha};s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0)+r_{\mathrm{UMAX}})^{-\alpha}a_1,$$
$$s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0)+r_{\mathrm{UMAX}})^{-\alpha}a_2\Bigg)\Bigg] - d_{\mathrm{GU}}^2\cos^2(\theta_0)\Bigg[1-F_1\Bigg(-\frac{2}{\alpha};\mu-m;m;1-\frac{2}{\alpha};$$
$$s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0))^{-\alpha}a_1, s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0))^{-\alpha}a_2\Bigg)\Bigg]\Bigg) - \frac{2d_{\mathrm{GU}}\sin(\theta_0)\pi\lambda_{\mathrm{GE}}}{3r_{\mathrm{UMAX}}}\Bigg((d_{\mathrm{GU}}\cos(\theta_0)$$
$$+r_{\mathrm{UMAX}})^3\Bigg[1-F_1\Bigg(-\frac{3}{\alpha};\mu-m;m;1-\frac{3}{\alpha};s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0)+r_{\mathrm{UMAX}})^{-\alpha}a_1,$$
$$s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0)+r_{\mathrm{UMAX}})^{-\alpha}a_2\Bigg)\Bigg] - d_{\mathrm{GU}}^3\cos^3(\theta_0)\Bigg[1-F_1\Bigg(-\frac{3}{\alpha};\mu-m;m;1-\frac{3}{\alpha};$$
$$s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0))^{-\alpha}a_1, s\eta\rho_1(d_{\mathrm{GU}}\cos(\theta_0))^{-\alpha}a_2\Bigg)\Bigg]\Bigg)\Bigg\}. \quad (5.17)$$

5.3.2 Second Hop

Applying the PGFL for the PPP Φ_{UE}, we arrive at

$$\mathcal{M}_{\gamma_{\mathrm{UE}}}(s) = \exp\Bigg\{ -2\pi\lambda_{\mathrm{UE}}\int_{r_{\mathrm{UMAX}}-\delta_2}^{r_{\mathrm{UMAX}}} r_e\Big[1-\mathcal{M}_{|h_{\mathrm{Ue}}|^2}(s\eta\rho_2(h^2+r_e^2)^{-\frac{\alpha}{2}})\Big]dr_e\Bigg\}, \quad (5.18)$$

where $\mathcal{M}_{|h_{\mathrm{Ue}}|^2}(\cdot)$ is the MGF of $|h_{\mathrm{Ue}}|^2$. Changing $h^2+r_e^2=u$ and $du=2r_e dr_e$ and after some mathematical manipulation, the closed-form expression of the MGF of γ_{UE}

can be obtained as

$$\mathcal{M}_{\gamma_{\mathrm{UE}}}(s) = \exp\Bigg\{ -\pi\lambda_{\mathrm{UE}}\Bigg(\Big[r_{\mathrm{UMAX}}^2 + d_{\mathrm{GU}}^2\sin^2(\theta_0)\Big]\Big[1 - F_1\left(-\frac{2}{\alpha}; \mu-m, m; 1-\frac{2}{\alpha};\right.$$
$$\left. s\eta\rho_2(r_{\mathrm{UMAX}}^2 + d_{\mathrm{GU}}^2\sin^2(\theta_0))^{-\alpha}a_1, s\eta\rho_2(r_{\mathrm{UMAX}}^2 + d_{\mathrm{GU}}^2\sin^2(\theta_0))^{-\alpha}a_2\right)\Big]$$
$$-\Big[d_{\mathrm{GU}}^2\sin^2(\theta_0)(1+\sin^2(\theta_2))\Big]\Big[1 - F_1\left(-\frac{2}{\alpha}; \mu-m, m; 1-\frac{2}{\alpha};\right.$$
$$\left. s\eta\rho_2 d_{\mathrm{GU}}^{-\alpha}\sin^{-\alpha}(\theta_0)(1+\sin^2(\theta_2))^{-\frac{\alpha}{2}}a_1,\ s\eta\rho_2 d_{\mathrm{GU}}^{-\alpha}\sin^{-\alpha}(\theta_0)(1+\sin^2(\theta_2))^{-\frac{\alpha}{2}}a_2\right)\Big]\Bigg)\Bigg\}. \tag{5.19}$$

5.4 Secrecy Outage Probability Analysis

The instantaneous secrecy rate C_s exists when instantaneous capacity of GBS-to-Bob channel C_B is better than that of GBS-to-Eve channel C_E, i.e.

$$C_s = \begin{cases} C_B - C_E, & C_B \geq C_E; \\ 0, & C_B < C_E, \end{cases} \tag{5.20}$$

where $C_B = \log_2(1+\gamma_{\mathrm{B}})$ and $C_E = \log_2(1+\gamma_{\mathrm{E}})$. As such, the SOP is the probability that the instantaneous secrecy rate C_s is below the target secrecy rate R_s, given by

$$P_{\mathrm{o}}(R_s) = \Pr(C_s < R_s). \tag{5.21}$$

5.4.1 Non-Cooperative Aerial and Ground Eavesdroppers

In this case, secrecy outage occurs when either the first or the second hops (or both) experience security outage. Consequently, the overall SOP at a target secrecy rate R_s can be calculated as

$$P_{\mathrm{o1}}(R_s) = 1 - (1 - \mathrm{SOP}_1)(1 - \mathrm{SOP}_2), \tag{5.22}$$

where SOP_1 is the SOP of the first hop and SOP_2 is that of the second hop. Note that the SOP of the first hop at the target secrecy rate R_s is mathematically defined

as

$$\mathrm{SOP}_1 = \Pr[\log_2(1+\gamma_{\mathrm{GU}}) - \log_2(1+\gamma_{\mathrm{GE}}) < R_s], \tag{5.23}$$

and that of the second hope as

$$\mathrm{SOP}_2 = \Pr[\log_2(1+\gamma_{\mathrm{UB}}) - \log_2(1+\gamma_{\mathrm{UE}}) < R_s]. \tag{5.24}$$

Conditioning on the eavesdropping SNR, the SOP can be calculated as

$$\begin{aligned} P_{\mathrm{o1}}(R_s) = 1 - &\left(1 - \mathbb{E}_{\gamma_{\mathrm{GE}}}\left[F_{\gamma_{\mathrm{GU}}}\left((2^{R_s}-1) + 2^{R_s}\gamma_{\mathrm{GE}}\right)\right]\right) \\ &\times \left(1 - \mathbb{E}_{\gamma_{\mathrm{UE}}}\left[F_{\gamma_{\mathrm{UB}}}\left((2^{R_s}-1) + 2^{R_s}\gamma_{\mathrm{UE}}\right)\right]\right), \end{aligned} \tag{5.25}$$

where $F_{\gamma_{\mathrm{GU}}}(\cdot)$ and $F_{\gamma_{\mathrm{UB}}}(\cdot)$ are the CDFs of the received SNR at UAV and Bob, respectively. Substituting (5.11) into (6.17), we can rewrite the expression of SOP, while noting that $\mathbb{E}[Z^k e^{sZ}] = \frac{d^k}{ds^k}\mathbb{E}[e^{sZ}] = \mathcal{M}_Z^{(k)}(s)$, as

$$\begin{aligned} P_{\mathrm{o1}}(R_s) = 1 - &\sum_{i_1=0}^{m-\mu}\sum_{i_2=0}^{m-\mu}\sum_{j_1=0}^{m-i_1-1}\sum_{j_2=0}^{m-i_2-1}\sum_{k_1=0}^{j_1}\sum_{k_2=0}^{j_2}\binom{j_1}{k_1}\binom{j_2}{k_2} \\ &\times \Xi 2^{R_s(k_1+k_2)}(2^{R_s}-1)^{(j_1+j_2)-(k_1+k_2)}e^{-(2^{R_s}-1)(A+B)} \\ &\times \mathcal{M}_{\gamma_{\mathrm{GE}}}^{(k)}(-2^{R_s}A)\mathcal{M}_{\gamma_{\mathrm{UE}}}^{(k)}(-2^{R_s}B), \end{aligned} \tag{5.26}$$

where $\Xi = \frac{C_{i_1}C_{i_2}}{(j_1)!(j_2)!(\rho_1 d_{\mathrm{GU}}^{-\alpha}a_1)^{j_1}(\rho_2 d_{\mathrm{UB}}^{-\alpha}a_1)^{j_2}}$, $A = \frac{1}{\rho_1 d_{\mathrm{GU}}^{-\alpha}a_1}$ and $B = \frac{1}{\rho_2 d_{\mathrm{UB}}^{-\alpha}a_1}$. Thus, the closed-form expression of the effective end-to-end SOP can be obtained by substituting (5.17) and (5.19) into (5.26).

5.4.2 Cooperative Aerial and Ground Eavesdroppers

When the aerial and ground eavesdroppers can cooperate with each other, the effective eavesdropping SNR γ_{Ecop} can be written as

$$\gamma_{\mathrm{Ecop}} = \gamma_{\mathrm{GE}} + \gamma_{\mathrm{UE}}. \tag{5.27}$$

We can obtain the closed-form expression of the MGF of γ_{Ecop} by multiplying (5.17) and (5.19). The SOP of the relay transmission system at target secrecy rate R_s can

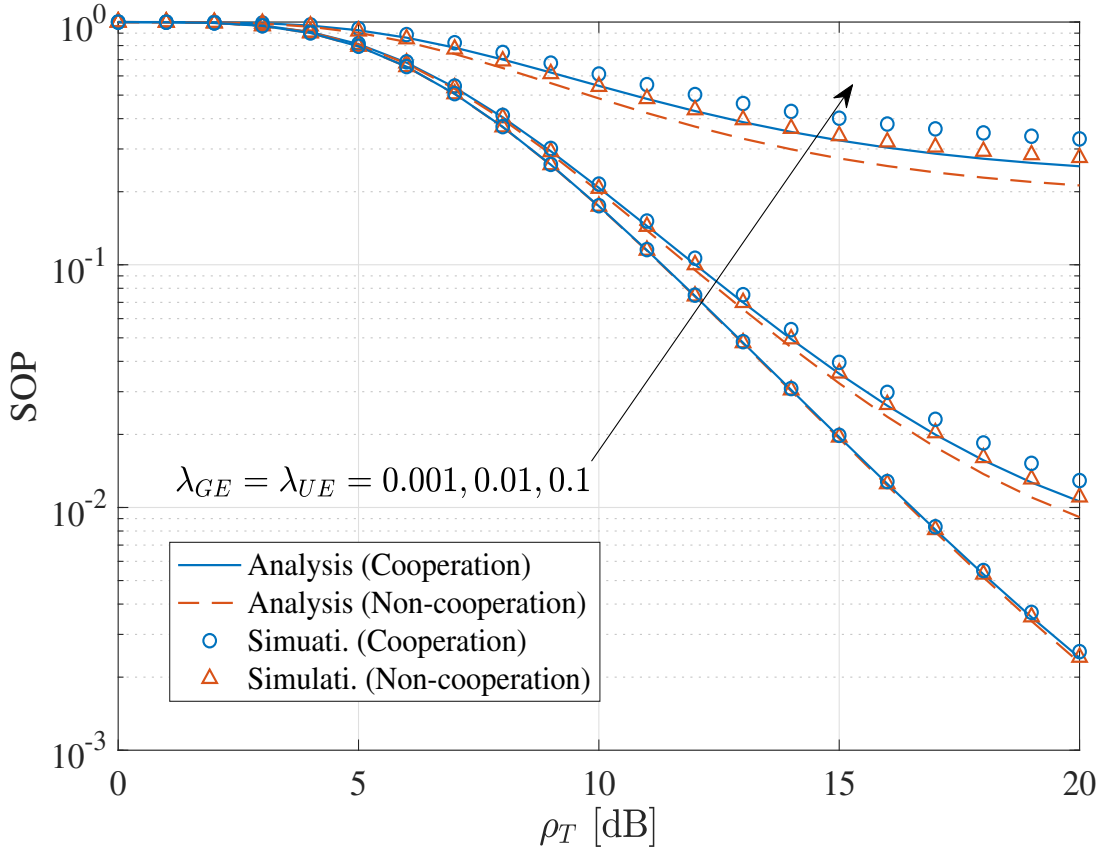

Figure 5.2: SOP as a function of transmit SNR ρ_{T} for non-cooperative/cooperative UAV and ground eavesdroppers with different densities λ_{GU}, λ_{UE} ($\eta = 0.1$ and $R_s = 5$).

be calculated as

$$P_{\mathrm{o2}}(R_s) = \Pr[\log_2(1+\gamma_{\mathrm{Bend}}) - \log_2(1+\gamma_{\mathrm{Ecop}}) < R_s], \tag{5.28}$$

where γ_{Bend} is the effective instantaneous end-to-end SNR, i.e. $\gamma_{\mathrm{Bend}} = \min\{\gamma_{\mathrm{GU}}, \gamma_{\mathrm{UB}}\}$, whose CDF can be obtained as

$$F_{\gamma_{\mathrm{Bend}}}(x) = 1 - [1 - F_{\gamma_{\mathrm{GU}}}(x)][1 - F_{\gamma_{\mathrm{UB}}}(x)] = 1 - \sum_{i_1=0}^{m-\mu} \sum_{i_2=0}^{m-\mu} \sum_{j_1=0}^{m-i_1-1} \sum_{j_2=0}^{m-i_2-1} \Xi x^{j_1+j_2} e^{-\mathrm{D}x}, \tag{5.29}$$

where $\mathrm{D} = \frac{(\rho_1 d_{\mathrm{GU}}^{-\alpha} + \rho_2 d_{\mathrm{UB}}^{-\alpha})}{\rho_1 \rho_2 d_{\mathrm{GU}}^{-\alpha} d_{\mathrm{UB}}^{-\alpha} a_1}$. Conditioning on γ_{Ecop}, the SOP can be calculated as

$$\begin{aligned} P_{\mathrm{o2}}(R_s) &= \mathbb{E}_{\gamma_{\mathrm{Ecop}}}\left[F_{\gamma_{\mathrm{Bend}}}\left((2^{R_s}-1)+2^{R_s}\gamma_{\mathrm{Ecop}}\right)\right] \\ &= 1 - \sum_{i_1=0}^{m-\mu}\sum_{i_2=0}^{m-\mu}\sum_{j_1=0}^{m-i_1-1}\sum_{j_2=0}^{m-i_2-1}\sum_{k=0}^{j_1+j_2}\binom{j_1+j_2}{k} \\ &\times \Xi 2^{R_s k}(2^{R_s}-1)^{j_1+j_2-k}e^{-(2^{R_s}-1)\mathrm{D}} \\ &\times \mathcal{M}_{\gamma_{\mathrm{GE}}}^{(k)}(-2^{R_s}\mathrm{D})\mathcal{M}_{\gamma_{\mathrm{UE}}}^{(k)}(-2^{R_s}\mathrm{D}). \end{aligned} \tag{5.30}$$

5.5 Numerical Results

In this section, we provide simulation results to verify the presented analysis, and to show the effect of different system parameters. The simulation parameters are set as follows: $\theta_0 = 50°$, $\theta_1 = 10°$, $\varphi_0 = 85°$, $\theta_2 = 15°$, $d_{\mathrm{GU}} = 0.5$ km, $d_{\mathrm{GMAX}} = 1$ km, $r_{\mathrm{UB}} = 0.1$ km, $\delta_1 = 0.1$ km, $\alpha = 3$, $\kappa = 5$, $m = 3$, and $\mu = 2$.

Fig. 5.2 plots the SOP versus transmit SNR ρ_{T} for non-cooperative/cooperative UAV and ground eavesdroppers, and different densities λ_{GE} and λ_{UE} by assuming $\rho_{\mathrm{T}} = \rho_1 = \rho_2$. We can see that the analytical SOP values are slightly smaller than the simulated ones. This is because the size of the protected area increases with the approximation in the MGF calculation, leading to a slight increase of the secrecy performance in the analysis. The figure shows that the SOP is a decreasing function in ρ_{T}, which implies that increasing the transmit power can enhance the secrecy performance, as expected. On the other hand, the SOP increases as the density of eavesdroppers increases. Moreover, the gap between cooperative and non-cooperative schemes is larger as the density of eavesdroppers increases.

Fig. 5.3 shows the SOP as a function of the ratio of the eavesdroppers density $\lambda_{\mathrm{GE}}/\lambda_{\mathrm{UE}}$ for non-cooperative/cooperative UAV and ground eavesdroppers with different attenuating factor η. We can see that the SOP generally increases as λ_{GE} increases or η increases for a fixed λ_{UE}. This is because larger λ_{GE} and/or η imply more eavesdroppers with possible better received signals. Again, the cooperative UAV and ground eavesdroppers scheme provides better performance as compared to non-cooperative case.

Fig. 5.4 plots the SOP as a function of the target rate R_s for non-cooperative UAV and ground eavesdroppers with different density λ_{UE}. We consider highly unbalanced hops with $\rho_1 = 20$ dB and $\rho_2 = 1$ dB, leading to a much weaker second hop. We

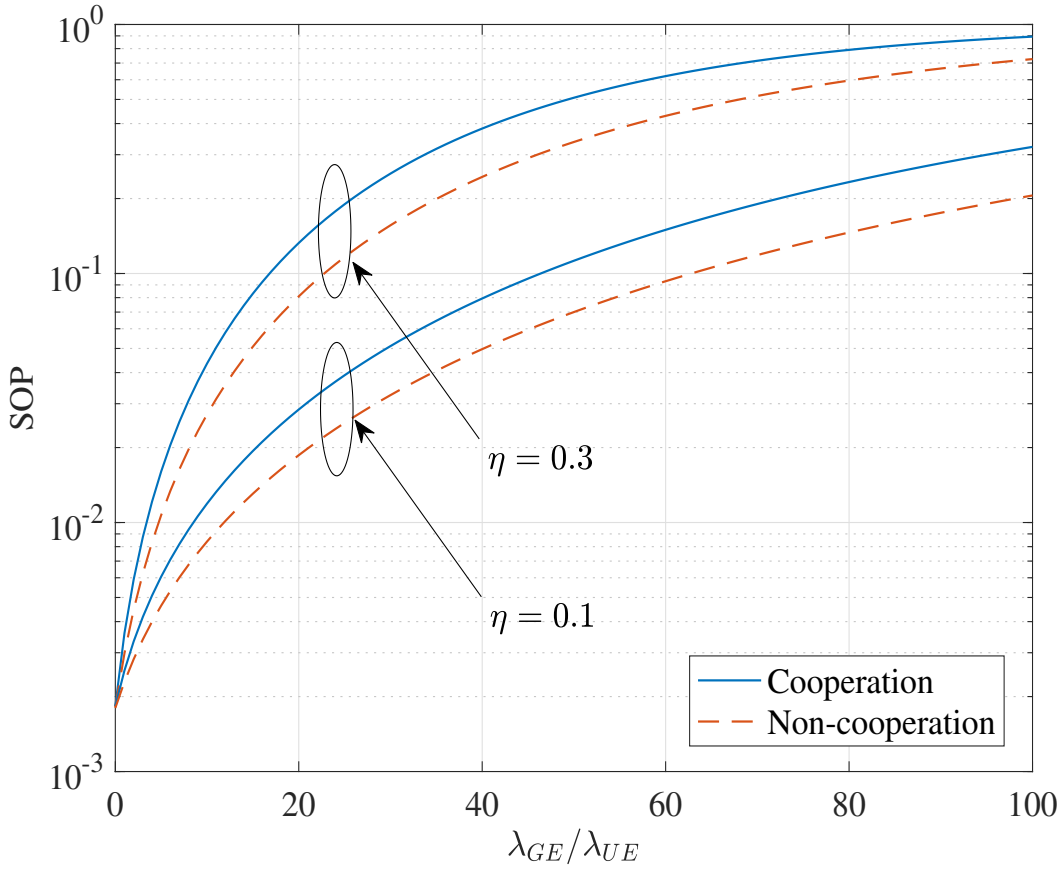

Figure 5.3: SOP as a function of the ratio of the eavesdroppers density $\lambda_{\mathrm{GE}}/\lambda_{\mathrm{UE}}$ for non-cooperative/cooperative UAV and ground eavesdroppers with different attenuating factor η ($\lambda_{\mathrm{UE}} = 0.001$, $\eta = 0.1$, $R_s = 5$ and $\rho_1 = \rho_2 = 20$ dB).

observe that the SOP and SOP_2 increase as R_s increases as expected. We can also see that the gap between SOP and SOP_2 becomes smaller as λ_{UE} is increased over the second hop. This implies that the weaker hop has a major effect on the SOP performance for non-cooperative schemes.

5.6 Conclusion

In this chapter, we analyzed the secrecy performance of a UAV-assisted relaying communication system in the presence of multiple UAV and ground eavesdroppers. Directional beamforming transmission is employed at the GBS and UAV relay to enhance secrecy performance. We derived the closed-form expression of the SOP for

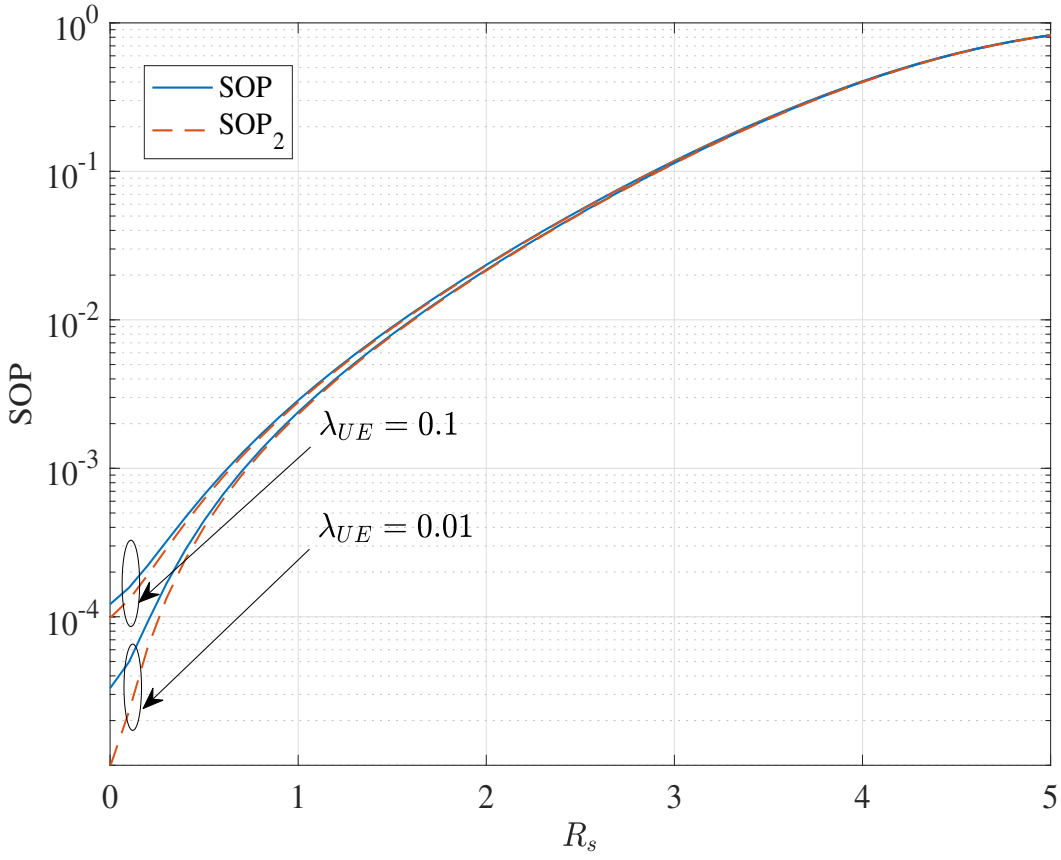

Figure 5.4: SOP as a function of target rate R_s for non-cooperative UAV and ground eavesdroppers with different density λ_{UE} ($\lambda_{\mathrm{GE}} = 0.01$, $\eta = 0.1$, $\rho_1 = 20$ dB and $\rho_2 = 1$ dB).

both non-cooperative and cooperative UAV and ground eavesdroppers schemes while all the channels experienced κ-μ shadowed fading. Selected numerical results showed the advantage of cooperative schemes over non-cooperative ones from eavesdropping point of view.

Chapter 6

Secrecy Performance Analysis of Ground-to-Air Communications with Multiple Aerial Eavesdroppers and its Deep Learning Evaluation

6.1 Introduction

Unmanned aerial vehicles (UAVs), also known as drones, can enhance the performance of wireless communication systems, especially in some emergency environments, such as natural disasters and military operations [120]. Meanwhile, the broadcast nature of wireless channels makes the exchange of secure information challenging. Physical layer security can exploit wireless channel characteristics and serve as an additional security mechanism [129].

There is a continuing interest in the secrecy performance improvement for UAV-based communications [130, 79, 80, 131, 132, 133]. Meanwhile, few work consider the case of UAV eavesdropping. Note that all UAV-based communication systems involve the ground-to-air transmission link, which may be subject to eavesdropping by enemy UAVs. [134] studies the secure connection probability in the presence of multiple non-colluding UAV eavesdroppers, where the eavesdroppers are assumed to be deployed in an aerial two-dimensional (2D) plane. In general, UAV eavesdroppers may randomly

distributed in three-dimensional (3D) space [135, 136]. In this paper, we study the secrecy performance of information transmission from a ground base station (GBS) to a legitimate UAV user in the presence of multiple UAV eavesdroppers. GBS applies the directional beamforming for transmission while maintaining a protection zone to enhance secrecy performance[126]. UAV eavesdroppers are randomly located outside of the exclusion zone in 3D space, following a homogeneous Poisson point process (PPP) distribution [137]. Due to obstacles in the local environment, random shadowing can impact channel quality for UAV-based communications. Assuming the most general κ-μ shadowed fading model[138], we derive an exact closed-form expression of secrecy outage probability (SOP) for the ground-to-air transmission scenario under consideration.

As a subset of machine learning, deep learning technique has been wildly applied to wireless system and network design [139, 140, 141]. Unlike theoretical tools provided by the complexity analysis, deep learning techniques can easily handle the wireless network by mapping the input network parameters with the output network performance. In [142], the authors use a parametrized sigmoid-like function to predict the coverage probability in a random wireless network. In [143], the UAV positioning for throughput maximization is analyzed by applying multi-layer perceptron and long short-term memory approaches. Besides, the unsupervised learning clustering technology is employed to the air-to-ground channel for UAV based communication networks [144]. Nevertheless, few work has adopted deep learning in system performance analysis. To our best knowledge, the only previous work along this direction is [142], which use a parametrized sigmoid-like function to predict the coverage probability in a random wireless network. In this paper, to further reduce the computation time for evaluating the resulting SOP, we derive a deep learning model to accurately predict SOP. In particular, we build a deep neural network (DNN) to capture the relationship between system parameters and the corresponding SOP, which can efficiently predict the SOP performance for various practical scenarios of interest.

The remainder of this chapter is organized as follows. The system and channel models are presented in Section 6.2. The secrecy performance analysis is presented in Section 6.3. We propose a deep learning approach and corresponding numerical results in Section 6.4. Finally, we draw our conclusions in Section 6.5.

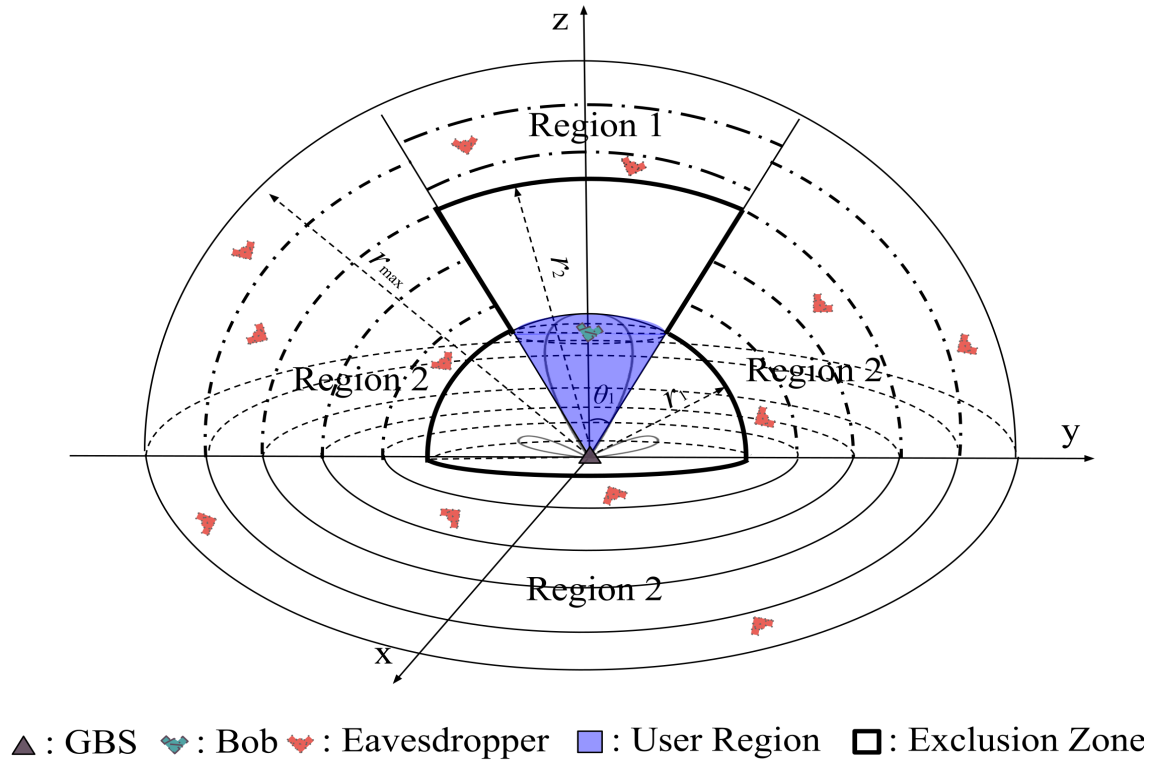

Figure 6.1: Illustration of 3D geometric model of UAV-based communications in the presence of multiple UAV eavesdroppers.

6.2 System and Channel Models

We consider the transmission from a GBS to a legitimate UAV user (Bob) in the presence of multiple UAV eavesdroppers. Without a lack of generality, we assume the GBS is located at the origin of the 3D space and its coverage area is a hemisphere centred at the GBS with radius $r_{\max}$, as shown in Fig. 6.1. We assume the GBS applies the directional beamforming transmission with half mainlobe width θ_1. The antenna gain can be approximately modeled as :

$$G = \begin{cases} G_0, & \text{inside mainlobe;} \\ \eta G_0, & \text{outside mainlobe,} \end{cases} \tag{6.1}$$

where $\eta < 1$ is the attenuating factor for the sidelobe gain. We assume Bob lies at the center of the mainlobe with distance r_B. The GBS maintains a protection zone to enhance secrecy performance. The protection zone X has a radius of r_1 for sidelobes and a radius of r_2 for mainlobe, $r_2 \geqslant r_1$. We assume the spatial distribution of UAV

eavesdroppers follows a homogeneous 3D PPP Φ_e/X of density λ_e.

The received symbol at Bob can be expressed as

$$y_B = \sqrt{P_t G_0}\sqrt{K r_B^{-\alpha}} h_B x_t + n_B, \tag{6.2}$$

where P_t is the transmit power of GBS, K is the path-loss constant, α is the path-loss exponent, h_B is the complex fading channel coefficient, x_t is the transmit symbol with unit power, and n_B is the additive white Gaussian noise with zero mean and variance N_0. Accordingly, the instantaneous received signal to noise ratio (SNR) at Bob is given by

$$\gamma_B = \frac{P_t G_0 K r_B^{-\alpha} |h_B|^2}{N_0} = \rho_{\mathrm{M}} r_B^{-\alpha} |h_B|^2, \tag{6.3}$$

where $\rho_{\mathrm{M}} = P_t G_0 K / N_0$ and $|h_B|^2$ is the fading channel power gain with $\mathbb{E}[|h_B|^2] = 1$. Due to the existence of the Light of Sight (LOS) component and obstacles in the local environment for the open air scenario, we assume that the GBS-to-Bob channel follows κ-μ shadowed fading. As such, the cumulative distribution function (CDF) of the received SNR at Bob γ_B is given by [127]

$$F_{\gamma_B}(x) = 1 - \sum_{i=0}^{m-\mu} C_i \exp\left(-\frac{x}{\rho_{\mathrm{M}} r_B^{-\alpha} a_1}\right) \sum_{j=0}^{m-i-1} \frac{1}{j!} \left(\frac{x}{\rho_{\mathrm{M}} r_B^{-\alpha} a_1}\right)^j, \tag{6.4}$$

where the parameters C_i and a_1 are expressed in terms of κ-μ shadowed fading parameters, namely κ, μ and m, as $C_i = \binom{m-\mu}{i} \left(\frac{m}{\kappa+m}\right)^i \left(\frac{\kappa}{\kappa+m}\right)^{m-\mu-i}$, and $a_1 = \frac{k+m}{m\mu(k+1)}$. Here, κ is the strength of LOS component, μ is the number of clusters and m is the parameter of Nakagami-m fading.

Similarly, the received symbol at UAV eavesdropper e can be expressed as

$$y_e = \sqrt{P_t G}\sqrt{K r_e^{-\alpha}} h_e x_t + n_e, \tag{6.5}$$

where r_e is the distance between GBS and UAV eavesdropper e and n_e is the additive white Gaussian noise with zero mean and variance N_0. As such, the instantaneous SNR at UAV eavesdropper e is given by

$$\gamma_e = \rho r_e^{-\alpha} |h_e|^2, \tag{6.6}$$

where $\rho = P_t GK/N_0$ is the transmit SNR and $|h_e|^2$ is the fading channel power gain with $\mathbb{E}[|h_e|^2] = 1$. We also assume GBS-to-UAV eavesdropper channel follows κ-μ shadowed fading. Since all UAV eavesdroppers cooperate together, the optimal technique is to apply maximum-ratio combining (MRC) to the signal received at the eavesdroppers before detection [106]. As such, the effective eavesdropping SNR is the sum of received SNR at the colluding UAV eavesdroppers, given by

$$\gamma_{\mathrm{E/X}} = \sum_{e \in \Phi_e/X} \rho r_e^{-\alpha} |h_e|^2. \tag{6.7}$$

As such, the moment-generating function (MGF) of $\gamma_{\mathrm{E/X}}$ can be calculated as

$$\mathcal{M}_{\gamma_{\mathrm{E/X}}}(s) = \mathbb{E}\left[\exp\left(s \sum_{e \in \Phi_e/X} \rho r_e^{-\alpha} |h_e|^2\right)\right], \tag{6.8}$$

where s is a complex number frequency parameter.

Applying the probability generating functional (PGFL) for the PPP Φ_e/X [137], we arrive at

$$\mathcal{M}_{\gamma_{\mathrm{E/X}}}(s) = \exp\left\{ -\lambda_e \int_V \left[1 - \mathbb{E}_{|h_e|^2}\left(\exp\left(s\rho r_e^{-\alpha}|h_e|^2\right)\right)\right] \mathrm{d}r_e \right\}, \tag{6.9}$$

where V is the spacial area that UAV eavesdroppers are located. Considering eavesdroppers inside and outside mainlobe seperately, the MGF of $\gamma_{\mathrm{E/X}}$ can be rewritten by

$$\mathcal{M}_{\gamma_{\mathrm{E/X}}}(s) = \mathcal{M}_{\gamma_{\mathrm{E1}}}(s) \times \mathcal{M}_{\gamma_{\mathrm{E2}}}(s), \tag{6.10}$$

where

$$\mathcal{M}_{\gamma_{\mathrm{E1}}}(s) = \exp\left\{ -\lambda_e \int_0^{2\pi} \int_{\theta_1}^{\frac{\pi}{2}} \int_{r_1}^{r_{\max}} r_e^2 \sin\theta \left[1 - \mathbb{E}_{|h_e|^2}(\exp\left(s\eta\rho_{\mathrm{M}} r_e^{-\alpha}|h_e|^2\right))\right] \mathrm{d}\theta \mathrm{d}\varphi \mathrm{d}r_e \right\}, \tag{6.11}$$

and

$$\mathcal{M}_{\gamma_{\mathrm{E2}}}(s) = \exp\left\{ -\lambda_e \int_0^{2\pi} \int_0^{\theta_1} \int_{r_2}^{r_{\max}} r_e^2 \sin\theta \Big[1 - \mathbb{E}_{|h_e|^2}(\exp\left(s\rho_{\mathrm{M}} r_e^{-\alpha}|h_e|^2\right))\Big] \mathrm{d}\theta \mathrm{d}\varphi \mathrm{d}r_e \right\}. \tag{6.12}$$

As such, $\mathcal{M}_{\gamma_{\mathrm{E1}}}(s)$ can be rewirtten as

$$\mathcal{M}_{\gamma_{\mathrm{E1}}}(s) = \exp\left\{ -2\pi\lambda_e \cos(\theta_1) \int_{r_1}^{r_{\max}} \Big[1 - \mathcal{M}_{|h_e|^2}(s\eta\rho_{\mathrm{M}} r_e^{-\alpha})\Big] r_e^2 \mathrm{d}r_e \right\}, \tag{6.13}$$

where $\mathcal{M}_{|h_e|^2}(\cdot)$ is the MGF of $|h_e|^2$. Substituting the MGF of $|h_e|^2$ for κ-μ fading [127] into (6.13), the closed-form expression of $\mathcal{M}_{\gamma_{\mathrm{E1}}}(s)$ can be obtained as

$$\begin{aligned} \mathcal{M}_{\gamma_{\mathrm{E1}}}(s) = \exp\Bigg\{ & -2\pi\lambda_e \cos(\theta_1) \Bigg[\frac{r_{\max}^3}{3} \\ & \times \left(1 - F_1\left(-\frac{3}{\alpha}; \mu - m, m; 1 - \frac{3}{\alpha}; \frac{s\eta\rho_{\mathrm{M}} a_1}{r_{\max}^{\alpha}}, \frac{s\eta\rho_{\mathrm{M}} a_2}{r_{\max}^{\alpha}}\right)\right) - \frac{r_1^3}{3} \\ & \times \left(1 - F_1\left(-\frac{3}{\alpha}; \mu - m, m; 1 - \frac{3}{\alpha}; \frac{s\eta\rho_{\mathrm{M}} a_1}{r_1^{\alpha}}, \frac{s\eta\rho_{\mathrm{M}} a_2}{r_1^{\alpha}}\right)\right) \Bigg] \Bigg\}, \end{aligned} \tag{6.14}$$

where $a_2 = \frac{1}{\mu(k+1)}$ and $F_1(a; b_1, b_2; c; x, y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \frac{(a)_{m+n}(b_1)_m(b_2)_n}{m!n!(c)_{m+n}} x^m y^n$ with the Pochhammer symbol $(q)_n$ is the Appell hypergeometric function of two variables [128]. The closed-form expression of $\mathcal{M}_{\gamma_{\mathrm{E2}}}(s)$ can be also obtained following the similar steps. After combining $\mathcal{M}_{\gamma_{\mathrm{E1}}}(s)$ and $\mathcal{M}_{\gamma_{\mathrm{E2}}}(s)$, we obtain the closed-form

expression of the MGF of $\gamma_{\mathrm{E/X}}$ for a κ-μ shadowed fading channel as

$$\begin{aligned}\mathcal{M}_{\gamma_{\mathrm{E/X}}}(s) = \exp\Bigg\{ \frac{-2\pi\lambda_e}{3}\Bigg(\cos(\theta_1)\Bigg[r_{\max}^3 \\ \times \left(1 - F_1\left(-\frac{3}{\alpha}; \mu - m, m; 1 - \frac{3}{\alpha}; \frac{s\eta\rho_{\mathrm{M}} a_1}{r_{\max}^{\alpha}}, \frac{s\eta\rho_{\mathrm{M}} a_2}{r_{\max}^{\alpha}}\right)\right) - r_1^3 \\ \times \left(1 - F_1\left(-\frac{3}{\alpha}; \mu - m, m; 1 - \frac{3}{\alpha}; \frac{s\eta\rho_{\mathrm{M}} a_1}{r_1^{\alpha}}, \frac{s\eta\rho_{\mathrm{M}} a_2}{r_1^{\alpha}}\right)\right)\Bigg]\Bigg) \\ + \Bigg([1 - \cos(\theta_1)]\Bigg[r_{\max}^3 \\ \times \left(1 - F_1\left(-\frac{3}{\alpha}; \mu - m, m; 1 - \frac{3}{\alpha}; \frac{s\rho_{\mathrm{M}} a_1}{r_{\max}^{\alpha}}, \frac{s\rho_{\mathrm{M}} a_2}{r_{\max}^{\alpha}}\right)\right) - r_2^3 \\ \times \left(1 - F_1\left(-\frac{3}{\alpha}; \mu - m, m; 1 - \frac{3}{\alpha}; \frac{s\rho_{\mathrm{M}} a_1}{r_2^{\alpha}}, \frac{s\rho_{\mathrm{M}} a_2}{r_2^{\alpha}}\right)\right)\Bigg]\Bigg)\Bigg\}. \end{aligned} \tag{6.15}$$

6.3 Secrecy Performance Analysis

The instantaneous secrecy rate C_s exists when instantaneous capacity of GBS-to-Bob channel C_B is better than that of eavesdropping channel C_E, i.e.

$$C_s = \begin{cases} C_B - C_E & \text{if} \quad C_B \geq C_E; \\ 0 & \text{else} \quad C_B < C_E, \end{cases} \tag{6.16}$$

where $C_B = \log_2(1 + \gamma_B)$ and $C_E = \log_2(1 + \gamma_{\mathrm{E/X}})$. The SOP is the probability that the instantaneous secrecy rate C_s is below the target threshold secrecy rate R_s ($R_s > 0$). Accordingly, the SOP can be calcuated as

$$P_{\mathrm{out}}(R_s) = \mathbb{E}_{\gamma_{\mathrm{E/X}}}\left[F_{\gamma_B}\left((2^{R_s} - 1) + 2^{R_s}\gamma_{\mathrm{E/X}}\right)\right]. \tag{6.17}$$

Substituting the CDF of the received SNR at Bob in (6.4) into (6.17), we can calculate of the SOP as

$$\begin{aligned} P_{\mathrm{out}}(R_s) = 1 - \sum_{i=0}^{m-\mu} C_i \exp\left(-\frac{2^{R_s} - 1}{\rho_{\mathrm{M}} r_B^{-\alpha} a_1}\right) \sum_{j=0}^{m-i-1} \sum_{k=0}^{j} \binom{j}{k} \frac{(2^{R_s} - 1)^{j-k} 2^{R_s k}}{j! (\rho_{\mathrm{M}} r_B^{-\alpha} a_1)^j} \\ \times \mathbb{E}_{\gamma_{\mathrm{E/X}}}\left[{\gamma_{\mathrm{E/X}}}^k \exp\left(-\frac{2^{R_s}\gamma_{\mathrm{E/X}}}{\rho_{\mathrm{M}} r_B^{-\alpha} a_1}\right)\right]. \end{aligned} \tag{6.18}$$

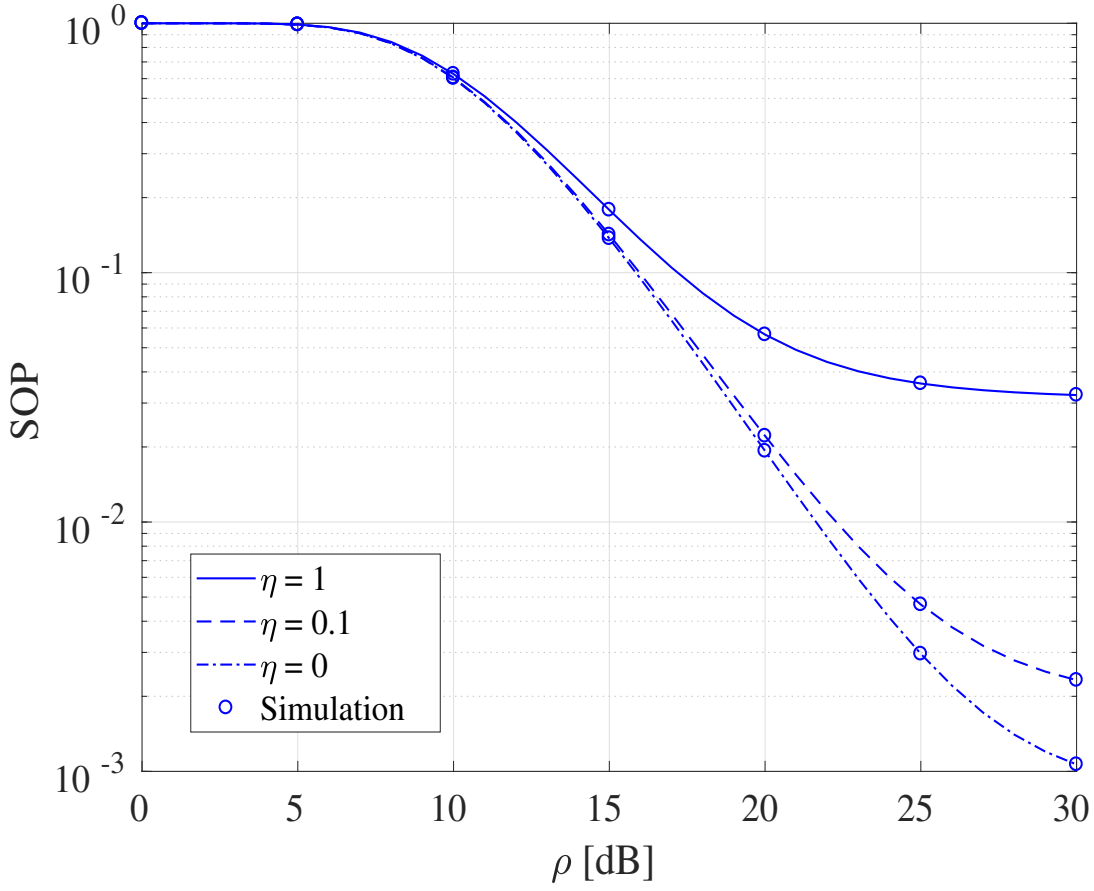

Figure 6.2: Secrecy outage probability of GBS to UAV transmission versus various transmit SNR ρ for different attenuating factor η ($\lambda_e = 10^{-3}$, $\alpha = 3$, $\theta_1 = 30°$, $r_B = 1.5$ km, $r_1 = 2$ km, $r_2 = 4$ km and $r_{\max} = 5$ km).

Noting that $\mathbb{E}[Z^k e^{sZ}] = \frac{d^k}{ds^k}\mathbb{E}[e^{sZ}] = \mathcal{M}_Z^{(k)}(s)$, the closed-form expression of SOP can be obtained as

$$P_{\text{out}}(R_s) = 1 - \sum_{i=0}^{m-\mu} C_i \exp\left(-\frac{2^{R_s}-1}{\rho_{\text{M}} r_B^{-\alpha} a_1}\right) \sum_{j=0}^{m-i-1} \sum_{k=0}^{j} \binom{j}{k} \frac{(2^{R_s}-1)^{j-k} 2^{R_s k}}{j!(\rho_{\text{M}} r_B^{-\alpha} a_1)^j} \times \mathcal{M}_{\gamma_{\text{E/X}}}^{(k)}\left(-\frac{2^{R_s}}{\rho_{\text{M}} r_B^{-\alpha} a_1}\right), \tag{6.19}$$

where $\mathcal{M}_{\gamma_{\text{E/X}}}(s)$ is given in (6.15).

Fig. 6.2 plots the SOP as the function of transmit SNR ρ for different sidelobe attenuating factor η. The parameters for fading channel are set as: $\kappa = 5$, $\mu =$

2, and $m = 3$. The perfect match with simulation result verifies our analysis. We first find that the SOP is a decreasing function in ρ, which implies that increasing transmit power can enhance secrecy performance. Another non-trivial observation is that the SOP increases with the increase of η. This implies a larger protection zone radius for sidelobe is needed to maintain the same SOP performance when η increases. Although the closed-form result saves the running time to evaluate SOP compared to simulation, it is still quite complex, requiring long computation time. In the following section, we develop a deep learning approach to predict SOP efficiently.

6.4 Deep Learning Evaluation

In this section, we build a DNN to evaluate the SOP performance. In particular, the system parameters, including $R_s, \alpha, \lambda_e, \theta_1, r_1, r_2, r_B$, and $r_{\max}$, denoted collectively as $\mathbf{\Phi}$, are used as the input to the network. The corresponding SOP $P_{\text{out}}(R_s)$ is the output of the network, shown in Figure 6.3. Each hidden layer consists of many neurons, which apply nonlinear activation function to the weighted sum of the outputs of the preceding layer. The commonly used activation functions for such nonlinear regression problems include the sigmoid function and the rectified linear unit (ReLU) function. We use ReLU function, given by [145] $\delta(x) = \max(0, x)$, as our activation function due to its high computational efficiency and good convergence performance [146], which will be illustrated in the following numerical examples.

To train the DNN and determine the optimal weights $\mathbf{w}$, we use the analytical SOP expression derived in previous subsection to generate a data set, denoted by

$$Z = \left\{ \left(\mathbf{\Phi}^{(i)}, P_{\text{out}}(R_s)^{(i)} \right), i = 1, 2, \cdots, N \right\}, \tag{6.20}$$

where $\mathbf{\Phi}^{(i)}$ is the ith input, $P_{\text{out}}(R_s)^{(i)}$ is the corresponding SOP, and N is the size of the dataset. The values of the input parameters are randomly drawn over the value range shown in Table 6.1. During the training process, we apply the mini-batch algorithm [147] to minimize the Huber loss function, defined as

$$L_{\delta_L}(\mathbf{w}) = \sum_{j \in N_T} \begin{cases} \frac{1}{2} |P_{\text{out}}(R_s)^{(j)} - f(\mathbf{\Phi}^{(j)}; \mathbf{w})|^2, & \text{for } L^{(j)} \leq \delta_L; \\ \delta_L |P_{\text{out}}(R_s)^{(j)} - f(\mathbf{\Phi}^{(j)}; \mathbf{w})| - \frac{1}{2}\delta_L^2, & \text{otherwise,} \end{cases} \tag{6.21}$$

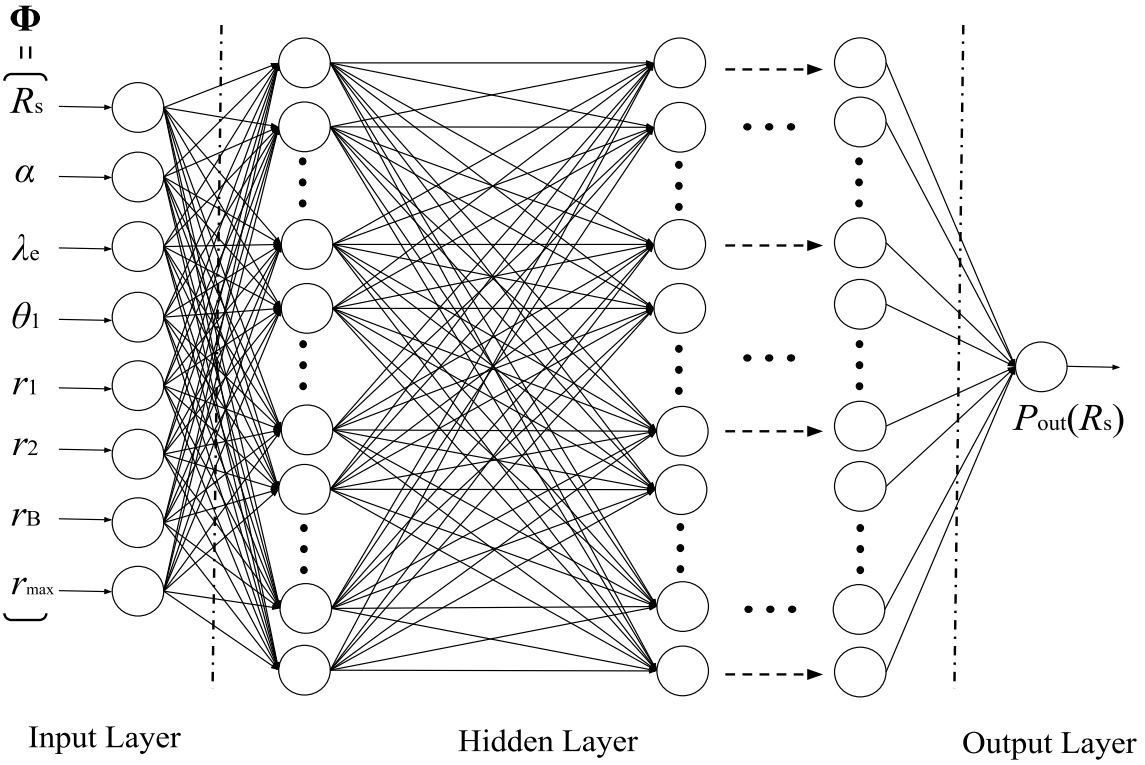

Figure 6.3: Structure and components of our DNN model.

Table 6.1: Input Parameters and Values for DNN Model

R_s	α	λ_e	θ_1
$[0, 7]$ bits/Hz/s	$[2, 4]$	$[1, 5]\times 10^{-3}$	$[30°, 60°]$
r_1	r_2	r_B	$r_{\max}$
$[2, 3]$ km	$[3, 4]$ km	$[0.5, 1.5]$ km	$[5, 6]$ km

where δ_L is a hyperparameter, $f(\mathbf{\Phi}^{(j)}; \mathbf{w})$ is the output of DNN for input $\mathbf{\Phi}^{(j)}$, and $N_T < N$ is the size of training dataset. Huber loss function has the property of mean square error (MSE) when the error is small, but more robustness to outliers [148]. Note that the remaining $N - N_T$ data samples are used for validation purpose.

Fig. 6.4 compares the accuracy and loss with different activation and loss functions for both training and validation datasets. We use 3 hidden layers and 64 neurons/layer in the DNN model with $\delta_L = 10^{-8}$ for Huber function. From the loss subfigure, we observe that the loss of Huber function is smaller than that of MSE for both Sigmoid and ReLU activation functions. For each loss function, ReLU performs better than Sigmoid. Meanwhile, from the accuracy subfigure, although MSE loss with ReLU can provide the accuracy as well as the convergence speed, Huber loss with ReLU can

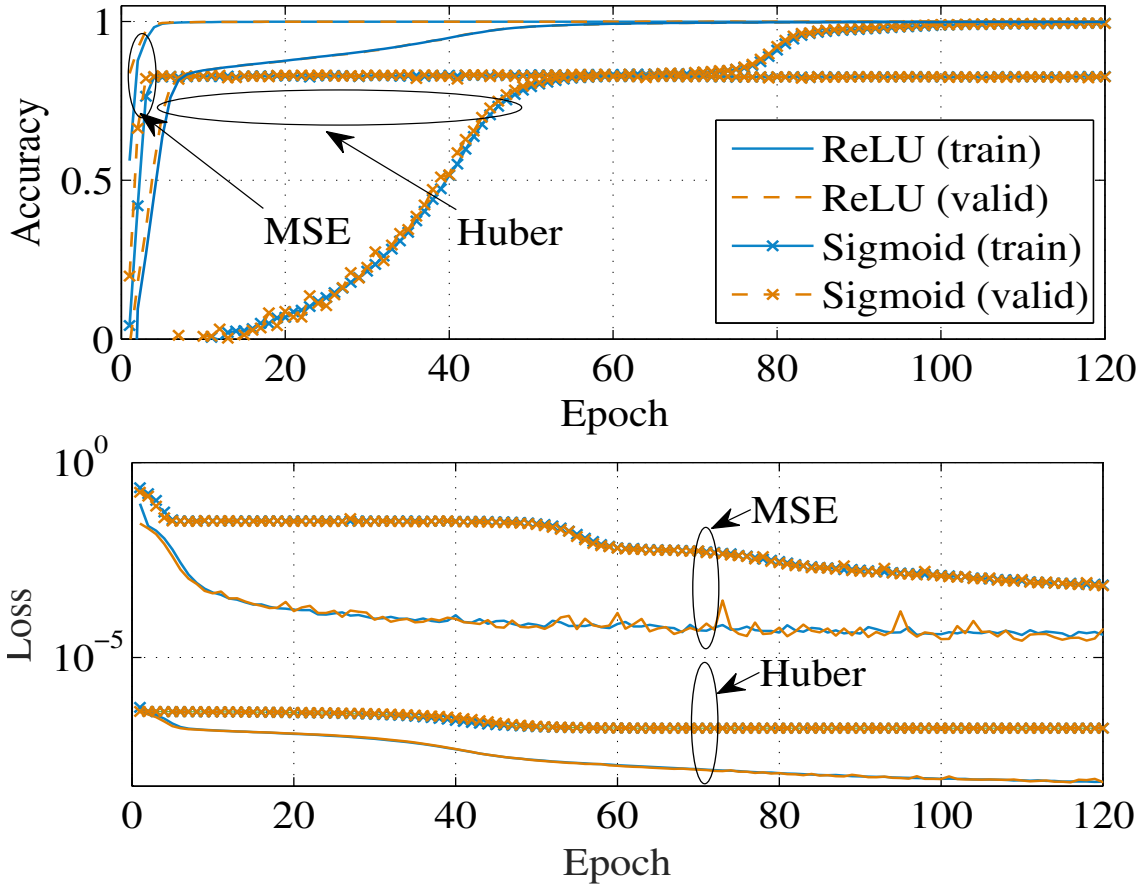

Figure 6.4: Accuracy and loss versus epoch for different activation and loss functions.

also increase to one after 50 epochs. Considering the property of Huber loss function and its accuracy, we use the Huber loss together with ReLU activation to predict the SOP performance in our DNN model.

Fig. 6.5 presents the SOP as a function of R_s for different λ_e and α. we can find that our DNN model provides a very accurate prediction of the SOP. Besides, we can observe that the SOP improves when α increases performance and/or λ_e decreases.

Fig. 6.6 plots the SOP as a function of r_1/r_2 for different θ_1 and ρ. We can see that the SOP decreases as r_1/r_2 increases. This is because fewer eavesdroppers outside the main lobe area eavesdrop the transmitted signal. For fixed ρ, we can also observe that the SOP with larger θ_1 provides lower value. This is implied that increasing the protection zone can improve secrecy performance. Particularly, when r_1/r_2 is equal to one, the value of SOP from different θ_1 is the same. This is because all the eavesdroppers are located in a half-spherical ring area. Furthermore, the SOP

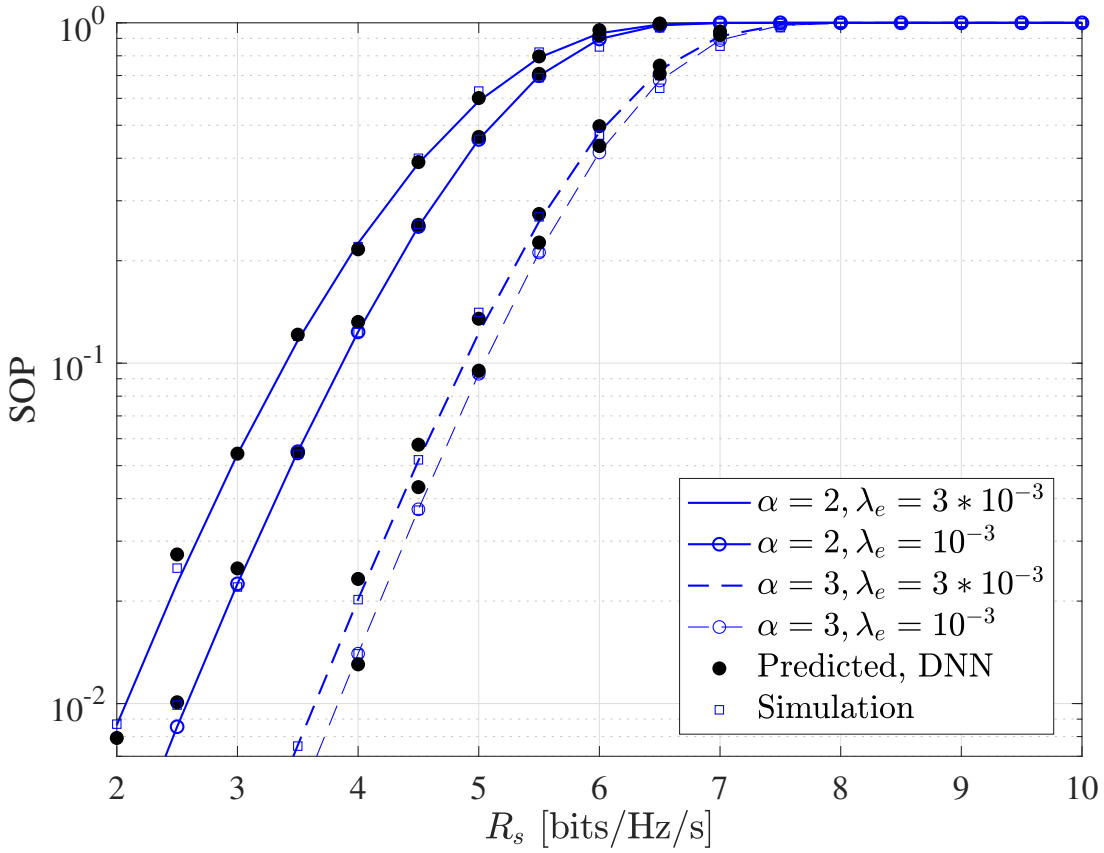

Figure 6.5: Secrecy outage probability of GBS to UAV transmission versus different target rate R_s for different λ_e and α ($\rho = 10$, $\theta_1 = 30°$, $r_B = 0.5$ km, $r_1 = 2$ km, $r_2 = 3$ km, $r_{\max} = 5$ km).

decreases as ρ increases for both θ_1 as expected.

We also compare the running time of Monte-Carlo simulation, closed-form analysis, and DNN prediction. The results show DNN analysis takes the shortest running time, only requiring 162.6535 microseconds to obtain a target SOP value. Closed-form analysis follows with 0.4851 seconds/value. In order to get stable results, we select 100,000 samples through Monte-Carlo model, which takes 221.8186 seconds/value. DNN approach can greatly facilitate SOP analysis.

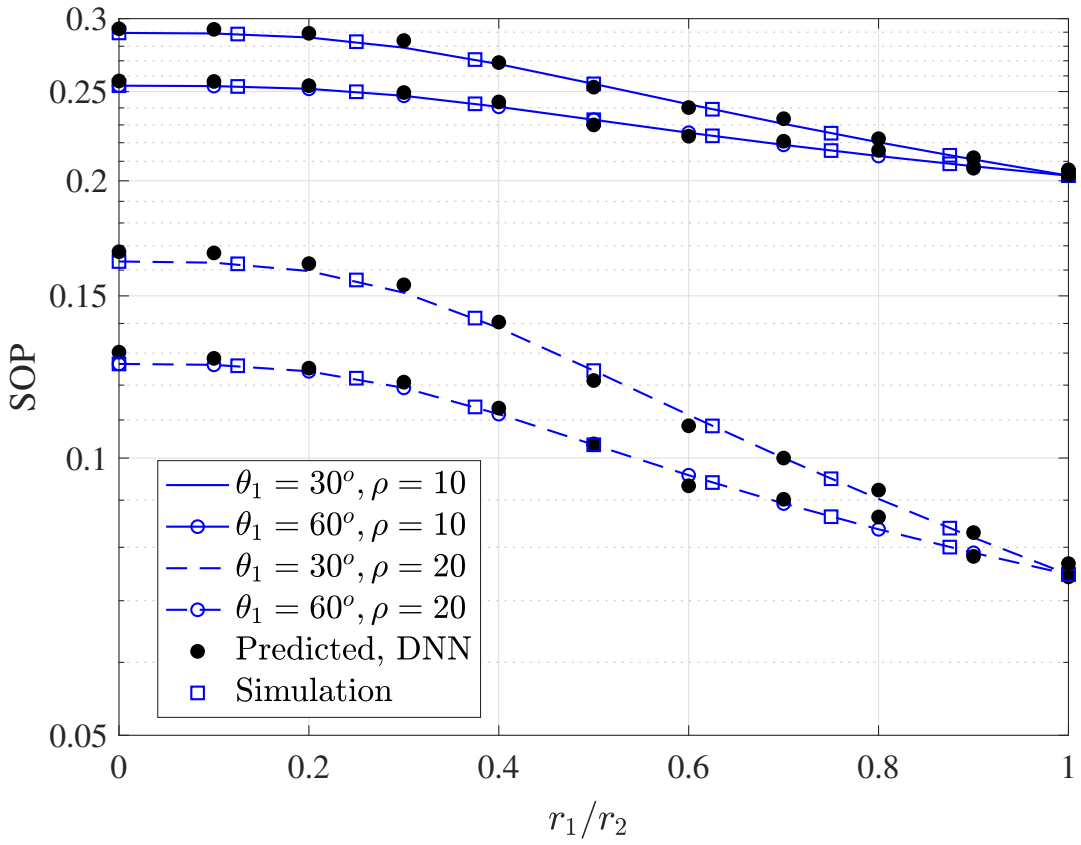

Figure 6.6: Secrecy outage probability of GBS to UAV transmission versus different ratio r_1/r_2 for different θ_1 and ρ ($\lambda_e = 3 * 10^{-3}$, $R_s = 5$ bits/Hz/s, $r_B = 0.5$ km, $r_2 = 4$ km, $r_{\max} = 5$ km, $\eta = 1$).

6.5 Conclusion

In this chapter, we analyzed the secrecy performance of GBS to UAV transmission in the presence of multiple UAV eavesdroppers. We derived the closed-form expression of the SOP while all the ground-to-air channels experience κ-μ shadowed fading when a general exclusion zone is implemented. Moreover, we proposed a DNN model with ReLU as activation function and Huber loss as loss function to predict the SOP. Numerical results have verified that our proposed DNN model can predict SOP performance with high accuracy and short running time.

Chapter 7

Conclusions and Future Works

In this chapter, we first highlight the contributions of this thesis. Then, we propose some research topics as future works.

7.1 Conclusions

In this thesis, we focus on the secrecy performance analysis for ground-based networks and UAV-based networks. In the following, we summarise the major contributions of each chapter as follows:

In Chapter 2, we investigated the secrecy performance of RUB transmission over MISOSE channel. We derived the closed-form expressions of the exact and the asymptotic ergodic secrecy rate and the SOP. Moreover, we investigated the effect of the RUB-based AN transmission on the MISOSE channel and obtained the corresponding expressions of the ergodic secrecy rate and the asymptotic ergodic secrecy rate. Besides, the closed-form expressions of the exact and the asymptotic SOP are also derived. Meanwhile, we carried out a thorough secrecy performance analysis of RUB transmission over MU-MIMOSE channel. We showed that RUB-based MU-MIMOSE transmission can effectively enhance the secrecy performance over low-SINR regions, and increasing the number of legitimate users can help enhance the secrecy performance by exploring multiuser diversity. Thus, the deployment of RUB and RUB-based AN offers an attractive solution for enhancing the security of wireless transmission systems.

In Chapter 3, we considered the secrecy performance of RUB transmission over massive MIMO channel in the presence of non-colluding and colluding eavesdrop-

pers. For non-colluding eavesdroppers, we derived the closed-form expressions of ergodic secrecy rate and the SOP of massive MIMOME transmission including the interference-limited and single legitimate user cases. When the number of antenna elements grows very large, we also derived the closed-form expressions of the upper bound of ergodic secrecy rate and the asymptotic SOP of massive MISOME transmission. For colluding eavesdroppers, we obtained the expression of ergodic secrecy rate and solved it by numerical approaches. Numerical results reveal that RUB scheme can be considered as an alternative method to enhance secrecy performance with only partial CSI of legitimate users is available at the BS.

In Chapter 4, we studied the secrecy performance of UAV-assisted relaying transmission where GBS intends to transmit signal to the ground legitimate user in the presence of a ground eavesdropper with the help of UAV relay. We derived the closed-form approximation of ergodic secrecy rate and intercept probability under an urban operating environment. Through analytical and numerical results, we examined the effect of different system parameters on secrecy performance. Particularly, the growth of UAV height can impact the different effects on intercept probability depending on whether Bob or Eve is closer to UAV. Under urban environment, shadowing effect can benefit the ergodic secrecy performance when Eve is closer to UAV than Bob, and increasing UAV transmit power may not always increase ergodic secrecy rate.

In Chapter 5, we investigated the secrecy performance of UAV-assisted relaying transmission in the presence of non-cooperative and cooperative multiple aerial and ground eavesdroppers. To enhance the secrecy performance, the GBS and the UAV relay apply directional beamforming transmission while implementing a protection zone around their intended receiver. Assuming the general κ-μ shadowed fading model, we derived the closed-form expressions of the SOP for both non-cooperation and cooperation cases. Numerical results show cooperative eavesdroppers can degrade the secrecy performance. Besides, the eavesdroppers' density, the angle of directional beamforming transmission and the attenuating factor of sidelobe gain can also affect the SOP performance.

In Chapter 6, we studied the secrecy performance of ground-to-air communication in the presence of multiple aerial eavesdroppers. We first derived the closed-form expression of the SOP by utilizing the general κ-μ shadowed fading distribution to model the ground-to-air channel. To further, facilitate performance evaluation, we adopted a data-driven approach and develop a deep learning model that can predict the SOP performance with high accuracy and short computation time. Particularly,

we proposed a DNN model with ReLU as an activation function and Huber loss as loss function to predict the SOP. Numerical results show the deep learning method can efficiently predict the SOP performance for various practical scenarios of interest.

7.2 Future works

7.2.1 Secrecy Performance for Ultra-Reliable Low-Latency Communications over Fading Channels

Ultra-reliable low-latency communications (URLLC) is one of the services to be provided in the future wireless communication systems. Many new mission-critical applications, such as autonomous networked vehicles and next-generation factory automation, require URLLC [149]. To satisfy the quality-of-service (QoS) requirements of these mission-critical applications, effective wireless transmission schemes are also investigated. In [150], the authors propose a data-oriented approach to analyze and design wireless transmission technologies from an individual transmission session perspective. However, the performance of individual transmission sessions varies with the transient behaviour of the channel, as an extension work, [151] develops transient performance limits for data transmission sessions that last multiple coherence intervals.

Although the data-oriented approach has been proposed to better stratify the QoS requirements of mission-critical applications, security issues are the major challenge in such mission-critical applications. PLS can improve secrecy due to the intrinsic randomness of the wireless medium. As such, it is necessary to investigate the secrecy performance for URLLC over fading channels. To the best of our knowledge, there is no work considering about secrecy rate over a certain period in URLLC. As such, one promising research direction is to investigate how much information can be securely transmitted during a fixed time duration over fading channels. We first derive the statistics of received SNR at the legitimate user and eavesdroppers over a certain period. Then, the transmitted secure information can be calculated as the capacity of difference between a transmitter and the legitimate user and between a transmitter and eavesdroppers. As such, the secrecy performance can be evaluated. One foreseeable challenge is that the exact distribution of the SNR ratio between transmitter-to-legitimate user channel and the transmitter-to-eavesdropper channel is hardly obtained since the statistics of received SNR at target user over a fixed time

duration is already complex [151]. Machine learning approach is a possible option to solve such complex analysis.

7.2.2 Secrecy Performance for Reconfigurable Intelligent Surface Aided UAV Communications

Reconfigurable intelligent surfaces (RISs), which are man-made surfaces of electromagnetic material, have been proposed to improve signal quality and coverage by artificially reconfiguring the propagation environment of electromagnetic waves [152]. Applications of RIS-based transmission have been wildly studies in SNR maximisation [153], signal coverage enhancement [154], beamforming optimisation [155]. Utilizing RIS makes signal transmission from a UAV to a remote user feasible, which is originally blocked by buildings in an urban area. This is because a RIS-relay can communicate with the UAV mainly via the LoS path. In [156], the authors investigate to maximize the average achievable rate in RIS-aided UAV communications.

However, the problem of secrecy performance analysis for RIS-aided UAV communications has not been studied before. Assume that a UAV transmits the signal to a ground legitimate user with the help of a RIS-relay in the presence of a ground eavesdropper. Meanwhile, RIS-induced phases can be controlled to maximize the received SNR through phase cancellations and proper alignment of reflected signals from the intelligent surface [153]. To analyze secrecy performance, we should derive the statistics of received SNR at the legitimate user and eavesdroppers. It is hard to directly obtain the closed-form expressions of the PDF distribution of the legitimate user and eavesdroppers since the received SNR contains multiple reflectors of the RIS in the general κ-μ shadowed fading. We may need to apply approach to obtain the MGF distribution of the received SNR. As such, ongoing effort is carried out to derive the statistics of received SNR of both legitimate user and eavesdroppers in RIS-aided UAV communications. Machine learning approach is also a solution by setting the CSI of the legitimate user and eavesdroppers as input and secrecy performance metric in terms of SOP as output via a DNN model.

List of Publications

[J1]. T. Bao, H.-C. Yang, and M. O. Hasna. "Secrecy Performance Analysis of UAV-Assisted Relaying Communication Systems." *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1122-1126, Nov. 2019.

[J2]. T. Bao, H.-C. Yang, and M. O. Hasna. "Physical layer secrecy performance of multiple antennas transmission with partial legitimate user CSI." *IET Commun.*, vol. 13, no. 15, pp. 2285-2295, Aug. 2019.

[J3]. T. Bao, J. Zhu, H.-C. Yang, and M. O. Hasna. "Secrecy Performance and Deep Learning Analysis of UAV Based Transmissions." submitted to *IEEE Wireless Commun. Lett.*, accepted, Apr. 2020.

[J4]. H.-C. Yang, T. Bao, and S. Alouini, "Transient Performance Limits for Wireless Transmissions over Fading Channels." *IEEE Trans. Veh. Technol.*, accepted, Mar. 2020.

[J5]. T. Bao, H.-C. Yang, and M. O. Hasna. "Secrecy Outage Analysis over Random Beamforming Transmission with User Scheduling: Collusion vs. Exclusion." submitted to *IEEE Signal Process. Lett.*, 2020.

[J6]. T. Bao, H.-C. Yang, and M. O. Hasna. "Secrecy Outage Performance Analysis of UAV-assisted Relay Communication Systems with Multiple Aerial and Ground Eavesdroppers." submitted to *IEEE Trans. Veh. Technol.*, 2020.

[C1]. T. Bao, H.-C. Yang, and M. O. Hasna. "On the Ergodic Secrecy Rate of Massive MIMO Transmission with Partial Legitimate User CSI." *IEEE PacRim*, pp. 1-5, Victoria, BC, Aug., 2019.

[C2]. T. Bao, H.-C. Yang, and M. O. Hasna. "Secrecy Outage Performance Analysis of Massive MIMO Transmission with Multiple Non-Colluding Eavesdroppers and Partial Legitimate User CSI." *IEEE VTC-Fall*, pp. 1-5, Honolulu, HI, Sep., 2019.

[C3]. T. Bao, H.-C. Yang, and M. O. Hasna. "Security Performance Analysis of MISOSE Transmission with Random Unitary Beamforming." *IEEE VTC-Fall*, pp. 1-5, Chicago, IL, Aug., 2018.

Bibliography

[1] William Stallings. Cryptography and network security: principles and practice. *Practice (6th Edition)*, 9:09685, 1998.

[2] James L Massey. An introduction to contemporary cryptology. *P. IEEE*, 76(5):533–549, May 1988.

[3] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proc. ACM TC*, pages 427–437, Atlanta, Georgia, 1990.

[4] Amitav Mukherjee, S Ali A Fakoorian, Jing Huang, and A Lee Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tut.*, 16(3):1550–1573, Feb. 2014.

[5] Aaron D Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, Oct. 1975.

[6] S Leung-Yan-Cheong and M Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul, 1978.

[7] Matthieu Bloch, João Barros, Miguel RD Rodrigues, and Steven W McLaughlin. Wireless information-theoretic security. *IEEE Trans. Inf. Theory*, 54(6):2515–2534, May 2008.

[8] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In *Proc. IEEE ISIT*, pages 356–360, Seattle, WA, Dec. 2006.

[9] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[10] Aylin Yener and Sennur Ulukus. Wireless physical-layer security: lessons learned from information theory. *Proc. IEEE Inst. Electr. Electron. Eng.*, 103(10):1814–1825, Sep. 2015.

[11] Patricio Parada and Richard Blahut. Secrecy capacity of SIMO and slow fading channels. In *Proc. IEEE ISIT*, pages 2152–2155, Adelaide, Australia, Oct. 2005.

[12] Shih-Chun Lin. On ergodic secrecy capacity of fast fading MIMOME wiretap channel with statistical CSIT. In *Proc. IEEE APSIPA*, pages 1–4, Kaohsiung, Taiwan, Jan. 2013.

[13] Yingbin Liang, H Vincent Poor, and Shlomo Shamai. Secure communication over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2470–2492, May 2008.

[14] Zang Li, Roy Yates, and Wade Trappe. Secret communication with a fading eavesdropper channel. In *Proc. IEEE ISIT*, pages 1296–1300, Nice, France, Jul. 2007.

[15] Ender Tekin and Aylin Yener. The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming. In *Proc. IEEE ITAW*, pages 1–5, La Jolla, CA, Feb. 2007.

[16] Yingbin Liang and H Vincent Poor. Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, Feb. 2008.

[17] O Ozan Koyluoglu, Hesham El Gamal, Lifeng Lai, and H Vincent Poor. Interference alignment for secrecy. *IEEE Trans. Inf. Theory*, 57(6):3323–3332, May 2011.

[18] Ruoheng Liu, Ivana Maric, Predrag Spasojevic, and Roy D Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, May 2008.

[19] Yingbin Liang, Anelia Somekh-Baruch, H Vincent Poor, Shlomo Shamai, and Sergio Verdú. Capacity of cognitive interference channels with and without secrecy. *IEEE Trans. Inf. Theory*, 55(2):604–619, Feb 2009.

[20] Yasutada Oohama. Capacity theorems for relay channels with confidential messages. In *Proc. IEEE ISIT*, pages 926–930, Nice, France, Jul. 2007.

[21] Lifeng Lai and Hesham El Gamal. The relay–eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, Aug. 2008.

[22] Abbas Mohammadi and Fadhel M Ghannouchi. Single RF front-end MIMO transceivers. In *RF Transceiver Design for MIMO Wireless Communications*, pages 265–288. Springer, 2012.

[23] Edward A Lee and David G Messerschmitt. *Digital communication*. Springer Science & Business Media, Berlin,Germany, 2012.

[24] Peter W Wolniansky, Gerard J Foschini, GD Golden, and Reinaldo A Valenzuela. V-BLAST: An architecture for realizing very high data rates over the rich-scattering wireless channel. In *Proc. IEEE URSI*, pages 295–300, Pisa, Italy, Oct. 1998.

[25] Sergio Verdu et al. *Multiuser detection*. Cambridge university press, Cambridge, 1998.

[26] John G Proakis, Masoud Salehi, Ning Zhou, and Xiaofeng Li. *Communication systems engineering*, volume 2. Prentice Hall New Jersey, Upper Saddle River, New Jersey, 1994.

[27] Christian B Peel, Quentin H Spencer, A Lee Swindlehurst, and Martin Haardt. An introduction to the multi-user MIMO downlink. *IEEE Commun. Mag.*, 61, Oct. 2004.

[28] Lai-U Choi and Ross D Murch. A transmit preprocessing technique for multiuser MIMO systems using a decomposition approach. *IEEE Trans. Wireless Commun.*, 3(1):20–24, Jan. 2004.

[29] Quentin H Spencer, A Lee Swindlehurst, and Martin Haardt. Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels. *IEEE Trans. Signal Process.*, 52(2):461–471, Jan. 2004.

[30] Max Costa. Writing on dirty paper (corresp.). *IEEE Trans. Inf. Theory*, 29(3):439–441, May 1983.

[31] Wonjong Rhee, Wei Yu, and John M Cioffi. The optimality of beamforming in uplink multiuser wireless systems. *IEEE Trans. Wirel. Commun.*, 3(1):86–96, Jan. 2004.

[32] Taesang Yoo and Andrea Goldsmith. On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming. *IEEE J. Sel. Area Comm.*, 24(3):528–541, Mar. 2006.

[33] Masoud Sharif and Babak Hassibi. On the capacity of MIMO broadcast channels with partial side information. *IEEE Trans. Inf. Theory*, 51(2):506–522, Jan. 2005.

[34] Hong-Chuan Yang, Peng Lu, Hyung-Ki Sung, and Young-Chai Ko. Exact sum-rate analysis of MIMO broadcast channels with random unitary beamforming. *IEEE Trans. Commun.*, 59(11):2982–2986, Jun. 2011.

[35] Jae-Hong Kwon, Young-Chai Ko, and Hong-Chuan Yang. Optimizing random unitary beamforming for energy efficiency in MIMO broadcast channels. In *Proc. IEEE VTC-Fall*, pages 1–5, Montreal, QC, Mar. 2016.

[36] Babak Hassibi and Thomas L Marzetta. Multiple-antennas and isotropically random unitary inputs: The received signal density in closed form. *IEEE Trans. Inf. Theory*, 48(6):1473–1484, Aug. 2002.

[37] Erik G Larsson, Ove Edfors, Fredrik Tufvesson, and Thomas L Marzetta. Massive MIMO for next generation wireless systems. *IEEE Commun. Mag.*, 52(2):186–195, Feb. 2014.

[38] Hien Quoc Ngo, Erik G Larsson, and Thomas L Marzetta. Energy and spectral efficiency of very large multiuser MIMO systems. *IEEE Trans. Commun.*, 61(4):1436–1449, Feb. 2013.

[39] Lu Lu, Geoffrey Ye Li, A Lee Swindlehurst, Alexei Ashikhmin, and Rui Zhang. An overview of massive MIMO: Benefits and challenges. *IEEE J. Sel. Top. Signal Process.*, 8(5):742–758, Apr. 2014.

[40] Thomas L Marzetta. Noncooperative cellular wireless with unlimited numbers of base station antennas. *IEEE Trans. Wireless Commun.*, 9(11):3590–3600, Oct. 2010.

[41] Jakob Hoydis, Stephan Ten Brink, and Mérouane Debbah. Massive MIMO in the UL/DL of cellular networks: How many antennas do we need? *IEEE J. Sel. Areas Commun.*, 31(2):160–171, Jan. 2013.

[42] Thomas L Marzetta. How much training is required for multiuser MIMO? In *Proc. IEEE ACSSC*, pages 359–363, Pacific Grove, CA, Oct. 2006.

[43] Junil Choi, David J Love, and Patrick Bidigare. Downlink training techniques for FDD massive MIMO systems: Open-loop and closed-loop training with memory. *IEEE J. Sel. Top. Signal Process.*, 8(5):802–814, Mar. 2014.

[44] Nihar Jindal. MIMO broadcast channels with finite rate feedback. *IEEE Trans. Inf. Theory*, 52(11):5045–5060, Oct. 2006.

[45] Kimon P Valavanis and George J Vachtsevanos. *Handbook of unmanned aerial vehicles*. Springer, Switzerland, 2015.

[46] Chris A Wargo, Gary C Church, Jason Glaneueski, and Mark Strout. Unmanned aircraft systems (uas) research and future analysis. In *Proc. IEEE AERO*, pages 1–16, Big Sky, MT, Mar. 2014.

[47] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Mérouane Debbah. Mobile unmanned aerial vehicles (UAVs) for energy-efficient internet of things communications. *IEEE Trans. Wireless Commun.*, 16(11):7574–7589, Sep. 2017.

[48] Elham Kalantari, Halim Yanikomeroglu, and Abbas Yongacoglu. On the number and 3D placement of drone base stations in wireless cellular networks. In *Proc. IEEE VTC-Fall*, pages 1–6, Sep. 2016.

[49] Yong Zeng, Rui Zhang, and Teng Joon Lim. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Commun. Mag.*, 54(5):36–42, May 2016.

[50] Chen-Mou Cheng, Pai-Hsiang Hsiao, HT Kung, and Dario Vlah. Maximizing throughput of UAV-relaying networks with the load-carry-and-deliver paradigm. In *Proc. IEEE WCNC*, pages 4417–4424, Kowloon, China, Mar. 2007.

[51] Mitch Campion, Prakash Ranganathan, and Saleh Faruque. UAV swarm communication and control architectures: a review. *J. Unmanned Vehicle Systems*, 7(2):93–106, Nov. 2018.

[52] Y-W Peter Hong, Pang-Chang Lan, and C-C Jay Kuo. Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches. *IEEE Signal Process. Mag.*, 30(5):29–40, Aug. 2013.

[53] Tie Liu and Shlomo Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Inf. Theory*, 55(6):2547–2553, May 2009.

[54] Frédérique Oggier and Babak Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, Jul. 2011.

[55] Chia-Hua Lin, Shang-Ho Tsai, and Yuan-Pei Lin. Secure transmission using MIMO precoding. *IEEE Trans. Inf. Forensics Security*, 9(5):801–813, Feb. 2014.

[56] Liyun Zhang, Haixia Zhang, Dalei Wu, and Dongfeng Yuan. Improving physical layer security for MISO systems via using artificial noise. In *Proc. IEEE GLOBECOM*, pages 1–6, San Diego, CA, Dec. 2015.

[57] Sungjun Ahn, Seungjae Jung, Wonju Lee, Tae-Kyung Sung, Joon-Goo Park, Kwang Eog Lee, and Joonhyuk Kang. Enhancing physical-layer security in MISO wiretap channel with pilot-assisted channel estimation: Beamforming design for pilot jamming. In *Proc. IEEE ICSPCS*, pages 1–5, Queensland, Australia, Feb. 2016.

[58] Ashish Khisti, Gregory Wornell, Ami Wiesel, and Yonina Eldar. On the gaussian MIMO wiretap channel. In *Proc. IEEE ISIT*, pages 2471–2475, Nice, France, Jul. 2007.

[59] Minyan Pei, Lei Wang, and Dongtang Ma. Linear MMSE transceiver optimization for general MIMO wiretap channels with QoS constraints. In *Proc. IEEE/CIC ICCC*, pages 259–263, Xi'an, China, Aug. 2013.

[60] Zouheir Rezki and Mohamed-Slim Alouini. On the finite-SNR diversity-multiplexing tradeoff of zero-forcing transmit scheme under secrecy constraint. In *Proc. IEEE ICC*, pages 1–5, Kyoto, Japan, Jun. 2011.

[61] Nabil Romero-Zurita, Mounir Ghogho, and Des McLernon. Outage probability based power distribution between data and artificial noise for physical layer security. *IEEE Signal Process. Lett.*, 19(2):71–74, Dec. 2012.

[62] Qiang Li and Wing-Kin Ma. Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization. *IEEE Trans. Signal Process.*, 61(10):2704–2717, Mar. 2013.

[63] Shuiyin Liu, Yi Hong, and Emanuele Viterbo. Practical secrecy using artificial noise. *IEEE Commun. Lett.*, 17(7):1483–1486, May 2013.

[64] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.*, 7(6), Jun. 2008.

[65] Hao Wang, Li Chen, and Weidong Wang. Enhancing physical layer security through beamforming and noise injection. In *Proc. IEEE WCSP*, pages 1–6, Hefei, China, Dec. 2014.

[66] Van-Dinh Nguyen, Trung Q Duong, Octavia A Dobre, and Oh-Soon Shin. Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks. *IEEE Trans. Inf. Forensics Security*, 11(11):2609–2623, Jul. 2016.

[67] Qiang Li, Ye Yang, Wing-Kin Ma, Meilu Lin, Jianhua Ge, and Jingran Lin. Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks. *EEE Trans. Signal Process.*, 63(1):206–220, Nov. 2015.

[68] Na Li, Xiaofeng Tao, and Jin Xu. Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback. *IEEE Commun. Lett.*, 18(6):969–972, Apr. 2014.

[69] Xiaoming Chen, Derrick Wing Kwan Ng, Wolfgang H Gerstacker, and Hsiao-Hwa Chen. A survey on multiple-antenna techniques for physical layer security. *IEEE Commun. Surv. Tut.*, 19(2):1027–1053, Nov. 2017.

[70] Ye Fan, Xuewen Liao, and Athanasios V Vasilakos. Physical layer security based on interference alignment in K-user MIMO Y wiretap channels. *IEEE Access*, 5:5747–5759, Apr. 2017.

[71] Amitav Mukherjee and A Lee Swindlehurst. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Trans. Signal Process.*, 59(1):351–361, Sep. 2011.

[72] Xiaoming Chen and Yu Zhang. Mode selection in MU-MIMO downlink networks: A physical-layer security perspective. *IEEE Syst. J.*, 11(2):1128–1136, May 2017.

[73] Jun Zhu, Robert Schober, and Vijay K Bhargava. Secure transmission in multicell massive MIMO systems. *IEEE Trans. Wireless Commun.*, 13(9):4766–4781, Jul. 2014.

[74] Jun Zhu, Robert Schober, and Vijay K Bhargava. Linear precoding of data and artificial noise in secure massive MIMO systems. *IEEE Trans. Wireless Commun.*, 15(3):2245–2261, Nov. 2016.

[75] Xiaoming Chen, Lei Lei, Huazi Zhang, and Chau Yuen. Large-scale MIMO relaying techniques for physical layer security: AF or DF? *IEEE Trans. Wireless Commun.*, 14(9):5135–5146, May 2015.

[76] Jue Wang, Jemin Lee, Fanggang Wang, and Tony QS Quek. Jamming-aided secure communication in massive MIMO rician channels. *IEEE Trans. Wireless Commun.*, 14(12):6854–6868, Jul. 2015.

[77] Yongpeng Wu, Robert Schober, Derrick Wing Kwan Ng, Chengshan Xiao, and Giuseppe Caire. Secure massive MIMO transmission with an active eavesdropper. *IEEE Trans. Inf. Theory*, 62(7):3880–3900, May 2016.

[78] Chen Sun, Xiqi Gao, Shi Jin, Michail Matthaiou, Zhi Ding, and Chengshan Xiao. Beam division multiple access transmission for massive MIMO communications. *IEEE Trans. Communi.*, 63(6):2170–2184, Apr. 2015.

[79] Xiaofang Sun, Derrick Wing Kwan Ng, Zhiguo Ding, Yanqing Xu, and Zhangdui Zhong. Physical layer security in UAV systems: Challenges and opportunities. *IEEE Wireless Commun.*, 26(5):40–47, Oct. 2019.

[80] Qingqing Wu, Weidong Mei, and Rui Zhang. Safeguarding wireless network with UAVs: A physical layer security perspective. *IEEE Wireless Commun.*, 26(5):12–18, Oct. 2019.

[81] Hongwu Liu and Kyung Sup Kwak. Secrecy outage probability of UAV-aided selective relaying networks. In *Proc. IEEE ICUFN*, pages 24–29, Milan, Italy, Jul. 2017.

[82] Yi Zhou, Phee Lep Yeoh, He Chen, Yonghui Li, Wibowo Hardjawana, and Branka Vucetic. Secrecy outage probability and jamming coverage of UAV-enabled friendly jammer. In *Proc. IEEE ICSPCS*, pages 1–6, Surfers Paradise, QLD, Dec. 2017.

[83] An Li, Qingqing Wu, and Rui Zhang. UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel. *IEEE Wireless Commun. Lett.*, 8(1):181–184, 2018.

[84] Meng Hua, Yi Wang, Min Lin, Chunguo Li, Yongming Huang, and Luxi Yang. Joint CoMP transmission for UAV-aided cognitive satellite terrestrial networks. *IEEE Access*, 7:14959–14968, Jan. 2019.

[85] Yu Pan, Xinyu Da, Hang Hu, Zhengyu Zhu, Ruiyang Xu, and Lei Ni. Energy-efficiency optimization of UAV-based cognitive radio system. *IEEE Access*, 7:155381–155391, Sep. 2019.

[86] Meng Hua, Yi Wang, Chunguo Li, Yongming Huang, and Luxi Yang. UAV-aided mobile edge computing systems with one by one access scheme. *IEEE Trans. Green Commun. and Networking*, Apr. 2019.

[87] Xiaoli Sun, Weiwei Yang, Yueming Cai, Ruiqian Ma, and Liwei Tao. Physical layer security in millimeter wave SWIPT UAV-based relay networks. *IEEE Access*, 7:35851–35862, Mar. 2019.

[88] Hongwu Liu, Sang-Jo Yoo, and Kyung Sup Kwak. Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers. *J. Commun. Networks*, 20(5):496–508, Nov. 2018.

[89] Zouheir Rezki and Mohamed-Slim Alouini. Secure diversity-multiplexing trade-off of zero-forcing transmit scheme at finite-SNR. *IEEE Trans. Commun.*, 60(4):1138–1147, Feb. 2012.

[90] Kanapathippillai Cumanan, Zhiguo Ding, Bayan Sharif, Gui Yun Tian, and Kin K Leung. Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper. *IEEE Trans. Veh. Technol.*, 63(4):1678–1690, Oct. 2014.

[91] S Ali A Fakoorian and A Lee Swindlehurst. Full rank solutions for the MIMO gaussian wiretap channel with an average power constraint. *IEEE Trans. Signal Process.*, 61(10):2620–2631, Mar. 2013.

[92] Ashish Khisti and Gregory W Wornell. Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Trans. Inf. Theory*, 56(7):3088–3104, Oct. 2010.

[93] Dimitrios S Karas, Alexandros-Apostolos A Boulogeorgos, and George K Karagiannidis. Physical layer security with uncertainty on the location of the eavesdropper. *IEEE Wireless Commun. Lett.*, 5(5):540–543, Aug. 2016.

[94] Sabrina Gerbracht, Christian Scheunert, and Eduard A Jorswieck. Secrecy outage in MISO systems with partial channel information. *IEEE Trans. Inf. Forensics Security*, 7(2):704–716, Dec. 2012.

[95] David J Love, Robert W Heath, Vincent KN Lau, David Gesbert, Bhaskar D Rao, and Matthew Andrews. An overview of limited feedback in wireless communication systems. *IEEE J. Sel. Areas Commun.*, 26(8), Oct. 2008.

[96] Shafi Bashar, Zhi Ding, and Geoffrey Ye Li. On secrecy of codebook-based transmission beamforming under receiver limited feedback. *IEEE Trans. Wireless Commun.*, 10(4):1212–1223, Feb. 2011.

[97] Alan Jeffrey and Daniel Zwillinger. *Table of integrals, series, and products*. Academic press, London, United Kingdom, 2007.

[98] Maoqiang Yang, Bangning Zhang, Yuzhen Huang, Daoxing Guo, and Xu Yi. Ergodic secrecy capacity for downlink multiuser networks using switch-and-examine combining with post-selection scheduling scheme. *Electronics Lett.*, 52(9):720–722, Apr. 2016.

[99] Peng Lu, Hong-Chuan Yang, and Young-Chai Ko. Sum-rate analysis of MIMO broadcast channel with random unitary beamforming. In *Proc. IEEE WCNC*, pages 533–537, Las Vegas, NV, Mar. 2008.

[100] Milton Abramowitz and Irene A Stegun. *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, volume 55. Courier Corporation, North Chelmsford, Massachusetts, 1964.

[101] Fredrik Rusek, Daniel Persson, Buon Kiong Lau, Erik G Larsson, Thomas L Marzetta, Ove Edfors, and Fredrik Tufvesson. Scaling up MIMO: Opportunities and challenges with very large arrays. *IEEE Signal Process. Mag.*, 30(1):40–60, Dec. 2013.

[102] Thomas L Marzetta. Massive MIMO: an introduction. *Bell Syst. Tech. J.*, 20:11–22, Mar. 2015.

[103] Tingnan Bao, Hong-Chuan Yang, and Mazen O Hasna. Physical layer secrecy performance of multiple antennas transmission with partial legitimate user CSI. *IET Commun.*, 13(15):2285–2295, Jan. 2019.

[104] J Zhang, RW Heath Jr, M Kountouris, and JG Andrews. Mode switching for MIMO broadcast channel based on delay and channel quantization. *EURASIP J. Adv. Signal Process.*, page 15, Jun. 2009.

[105] Pramod Viswanath, David N. C. Tse, and Rajiv Laroia. Opportunistic beamforming using dumb antennas. *IEEE Trans. Inf. Theory*, 48(6):1277–1294, Aug. 2002.

[106] Giovanni Geraci, Sarabjot Singh, Jeffrey G Andrews, Jinhong Yuan, and Iain B Collings. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. *IEEE Trans. Wireless Commun.*, 13(5):2931–2943, Apr. 2014.

[107] Andrea Goldsmith. *Wireless communications*. Cambridge university press, Cambridge, 2005.

[108] Akram Al-Hourani, Sithamparanathan Kandeepan, and Simon Lardner. Optimal LAP altitude for maximum coverage. *IEEE Wireless Commun. Lett.*, 3(6):569–572, Jul. 2014.

[109] Liang Yang, Jinhai Yuan, Xinxin Liu, and Mazen O Hasna. On the performance of LAP-based multiple-hop RF/FSO systems. *IEEE Trans. Aerosp. Electron. Syst.*, 55(1):499–505, Jul. 2019.

[110] Liang Yang, Jianchao Chen, Mazen O Hasna, and Hong-Chuan Yang. Outage performance of UAV-assisted relaying systems with rf energy harvesting. *IEEE Commun. Lett.*, 22(12):2471–2474, Oct. 2018.

[111] Junting Chen and David Gesbert. Local map-assisted positioning for flying wireless relays. *arXiv preprint arXiv:1801.03595*, 2018.

[112] Pawel Ladosz, Hyondong Oh, and Wen-Hua Chen. Prediction of air-to-ground communication strength for relay UAV trajectory planner in urban environments. In *Proc. IEEE IROS*, pages 6831–6836, Vancouver, BC, Sept. 2017.

[113] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, Cambridge, 2011.

[114] Akram Al-Hourani, Sithamparanathan Kandeepan, and Abbas Jamalipour. Modeling air-to-ground path loss for low altitude platforms in urban environments. In *Proc. IEEE GLOBECOM*, pages 2898–2904, Austin, TX, Dec. 2014.

[115] Mohammad Mahdi Azari, Fernando Rosas, Kwang-Cheng Chen, and Sofie Pollin. Ultra reliable UAV communication using altitude and cooperation diversity. *IEEE Trans. Commun.*, 66(1):330–344, Aug. 2018.

[116] Milton Abramowitz, Irene A Stegun, et al. *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, volume 55. Dover publications New York, New York, 1972.

[117] Barry Spain and Michael Gambier Smith. *Functions of mathematical physics*. Van Nostrand Reinhold Co., London, 1970.

[118] Marco Chiani, Davide Dardari, and Marvin K Simon. New exponential bounds and approximations for the computation of error probability in fading channels. *IEEE Trans. Wireless Commun.*, 2(4):840–845, Jul. 2003.

[119] Aymen Omri and Mazen O Hasna. Physical layer security analysis of uav based communication networks. In *Proc. IEEE VTC-Fall*, Chicago,IL, Sep. 2018.

[120] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, Young-Han Nam, and Mérouane Debbah. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutor.*, 21(3):2334–2360, Mar. 2019.

[121] Lun Dong, Zhu Han, Athina P Petropulu, and H Vincent Poor. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.*, 58(3):1875–1888, Dec. 2009.

[122] Tingnan Bao, Hong-Chuan Yang, and Mazen O Hasna. Secrecy performance analysis of UAV-assisted relaying communication systems. *IEEE Trans. Veh. Technol.*, 69(1):1122–1126, Jan. 2020.

[123] Xuening Liao, Yuanyu Zhang, Zhenqiang Wu, and Xiaohong Jiang. Buffer-aided relay selection for secure two-hop wireless networks with decode-and-forward relays and a diversity-combining eavesdropper. *Ad Hoc Networks*, 98:102039, Mar. 2020.

[124] Majid Moradikia, Hamed Bastami, Ali Kuhestani, Hamid Behroozi, and Lajos Hanzo. Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments. *IEEE Access*, 7:116942–116964, Aug. 2019.

[125] He Zhou, Dongxuan He, and Hua Wang. Joint relay and jammer selection for secure cooperative networks with a full-duplex active eavesdropper. *IET Commun.*, 14(6):1043–1055, Apr. 2020.

[126] Nadisanka Rupasinghe, Yavuz Yapıcı, Ismail Güvenç, Huaiyu Dai, and Arupjyoti Bhuyan. Enhancing physical layer security for NOMA transmission in mmWave drone networks. In *Proc. IEEE ACSSC*, pages 729–733, Pacific Grove, CA, Feb. 2018.

[127] F Javier Lopez-Martinez, Jose F Paris, and Juan M Romero-Jerez. The κ-μ shadowed fading model with integer fading parameters. *IEEE Trans. Veh. Technol.*, 66(9):7653–7662, Mar. 2017.

[128] Arthur Erdélyi et al. Hypergeometric functions of two variables. *Acta mathematica*, 83:131–164, 1950.

[129] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.*, 53(4):20–27, Oct. 2015.

[130] Hui-Ming Wang, Xu Zhang, and Jia-Cheng Jiang. UAV-involved wireless physical-layer secure communications: Overview and research directions. *IEEE Wireless Commun.*, 26(5):32–39, Oct. 2019.

[131] Bin Li, Zesong Fei, Yan Zhang, and Mohsen Guizani. Secure UAV communication networks over 5G. *IEEE Wireless Commun.*, 26(5):114–120, Jul. 2019.

[132] Jianping Yao and Jie Xu. Secrecy transmission in large-scale UAV-enabled wireless networks. *IEEE Trans. Commun.*, 67(11):7656–7671, Aug. 2019.

[133] Xin Yuan, Zhiyong Feng, Wei Ni, Zhiqing Wei, Ren Ping Liu, and J Andrew Zhang. Secrecy rate analysis against aerial eavesdropper. *IEEE Trans. Commun.*, 67(10):7027–7042, Jul. 2019.

[134] Jinchuan Tang, Gaojie Chen, and Justin P Coon. Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers. *IEEE Trans. Inf. Forensics Security*, 14(11):3026–3041, Apr. 2019.

[135] Pankaj K Sharma and Dong In Kim. Random 3D mobile UAV networks: Mobility modeling and coverage probability. *IEEE Trans. Wireless Commun.*, 18(5):2527–2538, Mar. 2019.

[136] Vishnu Vardhan Chetlur and Harpreet S Dhillon. Downlink coverage analysis for a finite 3-D wireless network of unmanned aerial vehicles. *IEEE Trans. Commun.*, 65(10):4543–4558, Jul. 2017.

[137] Sung Nok Chiu, Dietrich Stoyan, Wilfrid S Kendall, and Joseph Mecke. *Stochastic geometry and its applications*. John Wiley & Sons, San Francisco, CA, Aug. 2013.

[138] José F Paris. Statistical characterization of κ-μ shadowed fading. *IEEE Trans. Veh. Technol.*, 63(2):518–526, Sep. 2013.

[139] Chaoyun Zhang, Paul Patras, and Hamed Haddadi. Deep learning in mobile and wireless networking: A survey. *IEEE Commun. Surveys Tuts.*, 21(3):2224–2287, Mar. 2019.

[140] Longbiao Chen, Dingqi Yang, Daqing Zhang, Cheng Wang, Jonathan Li, et al. Deep mobile traffic forecast and complementary base station clustering for C-RAN optimization. *J. Netw. Computer Appl.*, 121:59–69, Nov. 2018.

[141] Hao Ye, Geoffrey Ye Li, and Biing-Hwang Juang. Power of deep learning for channel estimation and signal detection in OFDM systems. *IEEE Wireless Commun. Lett.*, 7(1):114–117, Sep. 2017.

[142] Hajar El Hammouti, Mounir Ghogho, and Syed Ali Raza Zaidi. A machine learning approach to predicting coverage in random wireless networks. In *Proc. IEEE Globecom*, pages 1–6, Abu Dhabi, UAE, Dec. 2018.

[143] Yirga Yayeh Munaye, Hsin-Piao Lin, Abebe Belay Adege, and Getaneh Berie Tarekegn. UAV positioning for throughput maximization using deep learning approaches. *Sensors*, 19(12):2775, Jun. 2019.

[144] Jing-Ling Wang, Yun-Ruei Li, Abebe Belay Adege, Li-Chun Wang, Shiann-Shiun Jeng, and Jen-Yeu Chen. Machine learning based rapid 3D channel modeling for UAV communication networks. In *Proc. IEEE CCNC*, pages 1–5, Las Vegas, NV, Jan. 2019.

[145] Xavier Glorot, Antoine Bordes, and Yoshua Bengio. Deep sparse rectifier neural networks. In *Proc. K4A AISTATS*, pages 315–323, Ft. Lauderdale, FL, Apr. 2011.

[146] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *IEEE Proc. NIPS*, pages 1097–1105, Lake Tahoe, NV, Dec. 2012.

[147] Sebastian Ruder. An overview of gradient descent optimization algorithms. *arXiv preprint arXiv:1609.04747*, 2016.

[148] Trevor Hastie, Robert Tibshirani, and Jerome Friedman. *The elements of statistical learning: data mining, inference, and prediction*. Springer Science & Business Media, Berlin, Germany, 2009.

[149] Siddhartha Kumar Khaitan and James D McCalley. Design techniques and applications of cyberphysical systems: A survey. *IEEE Syst. J.*, 9(2):350–365, June 2014.

[150] Hong-Chuan Yang and Mohamed-Slim Alouini. Data-oriented transmission in future wireless systems: Toward trustworthy support of advanced internet of things. *IEEE Veh. Technol. Mag.*, 14(3):78–83, Sep. 2019.

[151] Hong-Chuan Yang, Tingnan Bao, and Mohamed-Slim Alouini. Transient performance limits for ultra-reliable low-latency communications over fading channels. *IEEE Trans. Veh. Technol.*, Mar. 2020.

[152] Ertugrul Basar, Marco Di Renzo, Julien De Rosny, Merouane Debbah, Mohamed-Slim Alouini, and Rui Zhang. Wireless communications through reconfigurable intelligent surfaces. *IEEE Access*, 7:116753–116773, Aug. 2019.

[153] Ertugrul Basar. Transmission through large intelligent surfaces: A new frontier in wireless communications. In *IEEE Proc. EuCNC*, pages 112–117, Valencia, Spain, Jun. 2019.

[154] Ludek Subrt and Pavel Pechac. Controlling propagation environments using intelligent walls. In *IEEE Proc. EUCAP*, pages 1–5, Prague,Czech, Mar. 2012.

[155] Qingqing Wu and Rui Zhang. Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design. In *IEEE Proc. GLOBECOM*, pages 1–6, Abu Dhabi,United Arab Emirates, Dec. 2018.

[156] Sixian Li, Bin Duo, Xiaojun Yuan, Ying-Chang Liang, and Marco Di Renzo. Reconfigurable intelligent surface assisted uav communication: Joint trajectory design and passive beamforming. *IEEE Wireless Commun. Lett.*, Jan. 2020.