Physical Layer Security in Wireless Networks: Design and Enhancement.

Wang, Lifeng

Physical Layer Security in Wireless Networks: Design and Enhancement

by

Lifeng Wang

Doctor of Philosophy

Department of Electronic Engineering
Queen Mary University of London
United Kingdom

March 2015

Abstract

Security and privacy have become increasingly significant concerns in wireless communication networks, due to the open nature of the wireless medium which makes the wireless transmission vulnerable to eavesdropping and inimical attacking. The emergence and development of decentralized and ad-hoc wireless networks pose great challenges to the implementation of higher-layer key distribution and management in practice. Against this background, physical layer security has emerged as an attractive approach for performing secure transmission in a low complexity manner. This thesis concentrates on physical layer security design and enhancement in wireless networks.

First, this thesis presents a new unifying framework to analyze the average secrecy capacity and secrecy outage probability. Besides the exact average secrecy capacity and secrecy outage probability, a new approach for analyzing the asymptotic behavior is proposed to compute key performance parameters such as high signal-to-noise ratio slope, power offset, secrecy diversity order, and secrecy array gain. Typical fading environments such as two-wave with diffuse power and Nakagami-m are taken into account.

Second, an analytical framework of using antenna selection schemes to achieve secrecy is provided. In particular, transmit antenna selection and generalized selection combining are considered including its special cases of selection combining and maximal-ratio combining.

Third, the fundamental questions surrounding the joint impact of power constraints on the cognitive wiretap channel are addressed. Important design insights are revealed regarding the interplay between two power constraints, namely the maximum transmit at the secondary network and the peak interference power at the primary network.

Fourth, secure single carrier transmission is considered in the two-hop decode-and-

forward relay networks. A two-stage relay and destination selection is proposed to minimize the eavesdropping and maximize the signal power of the link between the relay and the destination. In two-hop amplify-and-forward untrusted relay networks, secrecy may not be guaranteed even in the absence of external eavesdroppers. As such, cooperative jamming with optimal power allocation is proposed to achieve non-zero secrecy rate.

Fifth and last, physical layer security in large-scale wireless sensor networks is introduced. A stochastic geometry approach is adopted to model the positions of sensors, access points, sinks, and eavesdroppers. Two scenarios are considered: i) the active sensors transmit their sensing data to the access points, and ii) the active access points forward the data to the sinks. Important insights are concluded.

Acknowledgments

First of all, I would like to express my great gratitude to my supervisor Dr Maged Elkashlan. Working with Maged for the past three years is a superb experience. I have been fortunate to work on my research under his invaluable guidance and support. He always encourages me to deal with interesting and challenging problems. He is friendly, considerate and knowledgeable. His nice personality and hard-working attitude have a profound effect on my future academic career.

I would like to thank Dr. Nan Yang (Jonas) (ANU), Dr. Trung Q. Duong (QUB), Dr. Kyeong Jin Kim (Mitsubishi), Dr. Marco Di Renzo (Supélec), Prof. G. K. Karagiannidis (AUTh), Prof. Ranjan K. Mallik (IIT), Prof. Jinhong Yuan (UNSW), Prof. Robert Schober (UBC) and Prof. H. Vincent Poor (Princeton) for their helpful suggestions and comments on my research. A special thanks to Prof. Jinhong Yuan for inviting me to visit his lab last summer.

I would also like to thank Prof. Lajos Hanzo (Southampton) and Prof. Mischa Dohler (KCL) for agreeing to serve on my Ph.D examiners.

During the past three years, many friends and colleagues have given me huge support and help. Thanks to their genuine friendship, I have had many good memories in my both Ph.D study and life. I would like to thank Dr. Lexi Xu, Dr. Fei Peng, Dr. Nan Wang, Dr. Yue Liu, Dr. Xiuxian Lao, Dr. Bo Zhong, Xingyu Han, Dan Zhao, Xinyue Wang, Yansha Deng, Dantong Liu, Zhijin Qin, Yuanwei Liu, Jingjing Zhao, Anqi He, Bingyu Xu among others.

Finally, I would like to thank my parents for their invaluable love and support.

Table of Contents

List of Figures

List of Abbreviations

D2D	Device-Device
5G	Fifth Generation
IEEE	Institute of Electrical and Electronics Engineers
WLAN	Wireless Local Area Networks
LTE	Long Term Evolution
SNR	Signal-to-Noise Ratio
SINR	Signal-to-Interference-plus-Noise Ratio
TWDP	Two-wave with Diffuse Power
MIMO	Multiple-input Multiple-output
MISO	Multiple-input Single-output
SIMO	Single-input Multiple-output
CSI	Channel State Information
MRC	Maximal-ratio Combining
GSC	Generalized Selection Combining
TAS	Transmit Antenna Selection
DF	Decode-and-Forward
AF	Amplify-and-Forward
CJ	Cooperative Jamming
CDF	Cumulative Distribution Function
PDF	Probability Density Function

AWGN	Additive White Gaussian Noise
PU	Primary User
SU-Tx	SU Transmitter
PU-Rx	PU Receiver
PAPR	Peak-to-Average Power Ratio
OFDM	Orthogonal Frequency-Division Multiplexing
CP-SC	Cyclic Prefix Single Carrier
ISI	InterSymbol Interference
FDE	Frequency-Domain Equalizer
BPSK	Binary Phase Shift Keying
i.i.d.	independent and identically distributed
OPA	Optimal Power Allocation
EPA	Equal Power Allocation
MRT	Maximal-Ratio Transmission
ESC	Ergodic Secrecy Capacity
PPP	Poisson Point Process
HPPP	Homogeneous Poisson Point Process
HCNs	Heterogeneous Cellular Networks
MGF	Moment Generating Function
TDD	Time Division Duplex
RF	Radio Frequency
BS	Base Station
WSNs	Wireless Sensor Networks
mmWave	Millimeter Wave

Chapter 1

Introduction

Wireless networks have experienced rapid evolutions towards scalability, interoperability, and sustainability. Future networked societies will drive the digital economy to a more holistic community of intelligent infrastructures and connected services for a smarter and more sustainable society. Device-to-device (D2D) communication, dense networks, and security are envisaged as core components of next generation heterogeneous 5G networks. Traditional homogeneous cellular networks are moving towards heterogeneous for seamless transmission in multi-tiered networks with multiple classes of base stations. D2D communication has been developed to support direct single- and multi-user transmissions, in order to decrease delays and enhance spectrum efficiency and energy efficiency. The secondary users are allowed to utilize the same frequency spectrum with the primary users in cognitive radio, to improve the spectrum efficiency. Multi-hop transmissions in wireless sensor and ad-hoc networks expand the coverage. Future 5G network will serve as a key enabler to meet the continuously increasing demand for future wireless applications, including ultra-high data rate, ultra-wide radio coverage, ultra-large number of devices, and ultra-low latency [1, 2]. Given the ubiquitousness and necessity of 5G connections in the near future, an enormous amount of sensitive and confidential information, e.g., financial data, electronic media, medical records, and customer files, will

be transmitted via wireless channels. However, the emergence of these new advanced systems pose great challenges to the implementation of higher-layer key distribution and management. Physical layer security is an appealing alternative to resist various malicious abuses and security attacks. The basic concept behind it is to exploit characteristics of wireless channels for transmitting confidential messages. Its target is to blind the eavesdroppers such that they cannot extract any confidential information from the received signals.

1.1 Research Motivation

Compared with cryptography, physical layer security techniques do not depend on computational complexity, which implies that the achieved level of security will not be compromised even if the unauthorized smart devices in the network have powerful computational capabilities. This is in contrast to the computation-based cryptography which is based upon the premise that the unauthorized devices have insufficient computational capabilities for hard mathematical problems. In the future network, devices are always connected to the nodes with different powers and computation capabilities at the different levels of the hierarchical architecture. Also, devices always join in or leave the network at random time instants, due to the decentralized nature of the network. As a consequence, cryptographic key distribution and management become very challenging. To cope with this, physical layer security can be used to either provide direct secure data communication or facilitate the distribution of cryptographic keys. The potentials of physical layer security in the multiple-antenna techniques and emerging systems need to be exploited. Therefore, this thesis is motivated by the following aspects.

Antenna Selection: Amongst multiple-antenna techniques, the low-complexity antenna selection schemes have been widely adopted and standardized in the IEEE 802.11n for WLAN [3], IEEE 802.16 for WiMAX [4], long term evolution (LTE) and LTE-Advanced [5]. Physical layer security using transmit antenna selection has been

investigated in the literature such as [6, 7]. However, a comprehensive study for generalized antenna selection system has not been provided, some key performance parameters such as high signal-to-noise ratio (SNR) slope and high SNR power offset have not been evaluated in the existing works. Moreover, since physical layer security exploits the properties of wireless fading channel, the use of multi-antenna techniques in some practical and flexible fading wiretap channels such as two-wave with diffuse power has not been examined. In this thesis, new analytical frameworks are developed to tackle these issues.

Cognitive Radio: In cognitive radio networks, the data of the secondary network needs to be protected, since the eavesdroppers or malicious primary users may intercept it. Although existing works [8–14] laid a solid foundation for understanding the role of physical layer security in cognitive radio networks, the impact of multi-antenna wiretap channels in cognitive networks with passive eavesdropping is less well understood. Key performance parameters such as secrecy diversity order and secrecy array gain under interference power constraint in cognitive radio networks have not been addressed in the existing literature.

Single Carrier Systems: Single carrier transmission is now being adopted in several wireless systems such as millimeter wave wireless personal area networks (WPAN) targeting in-flight entertainment distribution and wireless high-definition multimedia interface (HDMI), high-speed backhaul, etc. [15]. In this thesis, physical layer security in single carrier systems is first introduced.

Wireless Sensor Networks: In wireless sensor networks, secure transmission is crucial. Sensors are densely and randomly distributed in practical scenarios, which brings new difficulties for security. In this thesis, a stochastic geometry approach is implemented to model the three-tier sensor network. The impact of network parameters such as density of nodes on the secrecy performance is investigated.

5G Networks: Massive multiple-input multiple-output (MIMO) and millimeter wave are two key technologies in 5G systems, which provide physical layer security

with big opportunities [16]. In this thesis, opportunities and challenges of physical layer security in massive MIMO and mmWave systems are investigated. In particular, some traditional techniques such as artificial noise need to be re-designed in 5G networks.

1.2 Physical Layer Security Related Works

Secure transmission in wireless networks is confronted with increasing problems due to the rapid evolution of wireless network architectures [17–19]. The mobile terminals are more vulnerable to eavesdropping compared to their fixed counterparts, and the implementation of conventional cryptographic protocols to ensure security becomes difficult [20, 21]. In the 1970s, Aaron D. Wyner first introduced physical layer security [22]. Triggered by the rapid evolution of wireless network architectures, the idea of enabling security at physical layer has drawn attention of the wireless community [23, 24].

MIMO Wiretap Channel: Physical layer security has recently been addressed in MIMO wiretap channels where the transmitter, the receiver, and/or the eavesdropper are equipped with multiple antennas, as shown in [25–29] and the references therein.

Growing research interests have been devoted to examine physical layer security from a practical perspective. To design secure transmission schemes in practice, [20] proposed robust beamforming with artificial noise to mitigate the effect of inaccurate channel state information (CSI) in MIMO wiretap channels. An effective power distribution between the information signal and artificial noise was introduced in [30], which considered the use of beamforming with artificial noise over a multiple-input single-output (MISO) system in the presence of multiple single-antenna eavesdroppers. Considering the availability of partial CSI from the eavesdropper at the transmitter, [31] analyzed the secrecy outage probability in MISO wiretap channels. To facilitate low-complexity implementation, transmit antenna selection was utilized to promote security with low feedback overhead and low computational cost [6, 32]. Based on this, [33] examined the impact of antenna correlation at the receiver and the eavesdropper on the secrecy performance. For confi-

dential broadcasting, [34] proposed the regularized channel inversion precoding for the downlink of a multi-user MIMO system, where multiple users act as eavesdroppers. In [34], power allocation to maximize the achievable secrecy sum rate was considered. To provide valuable insights into the secrecy performance in practical fading channels, [35] introduced two secrecy performance metrics, namely the average secrecy rates and the secrecy outage probability, for single antenna wiretap channels. Inspired by this work, [36] took into consideration the single-input multiple-output (SIMO) wiretap channel and analyzed the secrecy outage probability with maximal-ratio combing (MRC) at the receiver and the eavesdropper in Rayleigh fading.

Cognitive Radio Networks: Spectrum-sharing cognitive radio is a promising technique to improve efficient utilization of the scarce radio spectrum, in order to tackle constant growth of numerous bandwidth-consuming wireless network users [37–39]. Security in cognitive radio networks is critical as it is easily exposed to external threats. The robust transmitter design via optimization for secure cognitive radio networks with and without perfect channel state information (CSI) was addressed in [8] and [9], respectively. In [10], cognitive relay beamforming was designed to maximize the secrecy rate, while the interference on the primary receiver was kept below a predefined value. In [11], relay selection was proposed for cognitive radio with a single eavesdropper. The proposed scheme in [11] selected a relay to maximize the achievable secrecy rate of the cognitive radio network subject to interference power constraint at the primary user. In [40], a pair of cognitive relays was opportunistically selected, where the first relay transmits confidential signals and the second relay transmits jamming signals. In [12], secure communications with untrusted secondary users in cognitive radio was examined and the achievable secrecy rate was derived. In [13], secure transmission in primary networks with the help of trusted secondary users was considered in the presence of a malicious eavesdropper attempting to obtain the primary user's messages. The proposed method in [13] modeled the cooperative transmission as a Stackelberg game. In [14], it was shown that non-cooperative jammers can be employed to improve the secrecy rate by

compensating them with a fraction of bandwidth, which implies that secondary users can act as non-cooperative jammers in cognitive radio networks.

Cooperative Relay: Cooperative relay communications has attracted much attention, due to its capabilities to establishing reliable links and increasing capacity [41]. Therefore, several recent works have considered physical layer security in cooperative communications [42–48]. In [42], cooperative decode-and-forward (DF) relays were deployed to perform distributed beamforming, and the secrecy diversity-multiplexing tradeoff was analyzed. In [43], several opportunistic relay selection schemes were proposed to achieve secrecy. In [44], based on the DF, amplify-and-forward (AF) and cooperative jamming (CJ) relay protocols, relay cooperation was investigated to increase the secrecy rate. In [45], optimal CJ using multiple relays for security enhancement was studied and the condition for positive secrecy rate was derived. In [46], CJ and relay chatting schemes for secrecy were proposed in opportunistic relay systems, which showed that the proposed relay chatting scheme can perform better than CJ. Joint relay and jammer selection for security enhancement was examined in one-way DF relay networks [47] and two-way AF relay networks [48].

Untrusted Relay: Standards for relay-assisted transmission have been established, such as the IEEE 802.11s and the IEEE 802.16j. Relay is a low-cost technique to increase the coverage and maintain link reliability in wireless networks [18, 49]. However, if the relay is untrusted or unauthenticated, it becomes an issue to keep the messages confidential between the source and the destination. The reason is that the untrusted relay may belong to public networks that have low security clearance. In this case, the untrusted relay acts as both a helper and an eavesdropper. The optimal secure beamforming design for an AF MIMO untrusted relay system was proposed in [50]. Ergodic secrecy capacity for the untrusted relay selection was derived in [51], where the destination-based jamming was used to achieve positive secrecy rate. The outage performance in two-hop relaying with CJ was analyzed in [52], where all nodes are equipped with a single antenna. In [53], antenna selection at the untrusted relay was

considered, in which the relay selects the strongest source-relay link to receive the signal and the strongest relay-destination link to forward the signal.

Wireless Sensor Networks: In wireless sensor networks (WSNs), the sensed data is usually sensitive, and therefore secure transmission is critical in WSNs. Physical layer security has been recently introduced in WSNs to combat eavesdropping [54–57]. In [54], the downlink secure transmission from the mobile agent to the authorized user was considered and two randomized array transmission schemes were developed. In [55], Distributed detection under secrecy constraint in an energy-constrained WSN was addressed, and the optimal operative solutions were analyzed. In [56], sensor transmissions were observed by the authorized fusion center (FC) and unauthorized (third party) FC. It was shown in [56] that the proposed security scheme at physical layer is highly scalable with low-complexity, compared to the traditional network security protocols such as cryptography and key management at the link and network layer. More recently in [57], AF compressed sensing (CS) was introduced to provide secrecy against eavesdropping in WSNs, and it was confirmed that the eavesdroppers cannot successfully decode the signal when the number of eavesdropper is less than the sparsity level of the signal.

Cellular Networks: In cellular networks, physical layer security is important for adding another level of protection. In [58], secure downlink transmission in cellular networks was investigated, and the secrecy using linear precoding based on regularized channel inversion was examined. In multi-cell environments, cell association and location information of mobile users play an important role in determining the secrecy performance [59]. In [60], the Kuhn-Munkres (KM) algorithm was introduced to solve the radio resource allocation problem, in order to maximize the sum secrecy capacity for both cellular and D2D users. In [61], it was shown that the interference from D2D transmission can enhance the physical layer security of cellular communications. In [62], secure transmission in multi-cell massive MIMO systems was exploited, which showed that random artificial noise (AN) generation can provide a favourable performance/complexity tradeoff compared to conventional AN.

Millimeter Wave: As an innovative solution to meet the 5G's requirement, millimeter wave (mmWave) communication systems use a huge swath of spectrum, from 30 to 300 GHz, to shift wireless transmissions away from the nearly fully occupied spectral band of current wireless networks [63–65]. In [66], antenna subset modulation with large antenna arrays was introduced to provide secure mmWave transmission at the physical layer. In [67], the secrecy throughput using analog beamforming with phase shifters was analyzed. Since secure mmWave transmission is a completely new and promising research frontier, new secure transmission designs are needed by taking advantage of the mmWave channel properties [63, 64].

1.3 Dissertation Organization and Contributions

The remainder of the thesis is organized as follows. Chapter 2 presents some fundamental concepts such as physical layer security, stochastic geometry, and cooperative jamming. Chapter 3 exploits the benefits of MRC in two-wave with diffuse power (TWDP) fading wiretap channel. Chapter 4 provides an analytical framework for antenna selection in Nakagami-m fading wiretap channel. Chapter 5 examines the effect of power constraint on the secrecy in cognitive radio networks. Chapter 6 introduces physical layer security in single carrier systems. Chapter 7 proposes cooperative jamming with optimal power allocation in two-hop untrusted relay networks. Chapter 8 investigates secure transmission in three-tier WSNs with stochastic geometry. The main contributions of this thesis are detailed as follows.

Chapter 3 focuses on physical layer security of MRC in TWDP fading channels. The TWDP fading is of high flexibility as it includes Rayleigh, Rician, and hyper-Rayleigh fading as special cases. In such a channel model, two practical scenarios are considered, namely the active eavesdropping scenario and the passive eavesdropping scenario. Key performance parameters such as high SNR slope, power offset, and secrecy diversity order are introduced and derived. The performance gap for different number of antennas is

quantified.

Chapter 4 focuses on transmit antenna selection and receive generalized selection combining in MIMO Nakagami-m fading wiretap channels. The aim is to construct a unifying approach to evaluate the secrecy performance using practical antenna selection techniques. Two distinct and practical scenarios are considered: 1) the legitimate receiver is located close to the transmitter, and 2) the legitimate receiver and the eavesdropper are located close to the transmitter.

Chapter 5 focuses on secure cognitive transmission in passive eavesdropping. Both the legitimate receiver and eavesdropper use selection combining to receive the signal. An analytical framework is first presented. Under interference power constraint, closed-form expressions for secrecy outage probability are derived. Based on the asymptotic analysis, the secrecy diversity order and secrecy array gain are explicitly obtained.

Chapter 6 focuses on cooperative single carrier systems. A new relay selection criterion is proposed to enhance the security. Closed-form expressions for key performance metrics such as ergodic secrecy rate and secrecy outage probability are derived. It is shown that the multipath diversity and multiuser diversity can be utilized to improve the secrecy.

Chapter 7 focuses on security design in untrusted relay networks, which is different from the relay networks presented in Chapter 6. In untrusted relay networks, the relay is also an eavesdropper and intercepts the information transmitted by the source. Optimal power allocation with cooperative jamming to maximize the ergodic secrecy capacity is examined. The benefits of using large antenna arrays are also shown.

Chapter 8 focuses on physical layer security in three-tier WSNs. The system topology is built based on stochastic geometry. The aim is to evaluate the effect of the densities of sensors, access points, and sinks on the secure transmission. The average secrecy rate of the three-tier WSN is derived.

Chapter 9 consists of conclusions and future work of this thesis. For future work, two extensions of current work are proposed, i.e., imperfect channel state information condition and multi-hop secure transmission with trusted/untrusted relays. In addition, physical layer security can safeguard data confidentiality by exploiting the intrinsic randomness of the communications medium and reaping the benefits offered by the disruptive technologies to 5G. Among various technologies, two most promising ones are discussed, namely, massive MIMO and millimeter wave. On the basis of the key principles of each technology, the rich opportunities and the outstanding challenges that security designers must tackle are identified. Such an identification is expected to decisively advance the understanding of physical layer security of tomorrow.

1.4 Author's Publications

Journal Papers

1. **L. Wang**, Hien Quoc Ngo, Maged Elkashlan, Trung Q. Duong, and Kai-Kit Wong, "Massive MIMO in spectrum sharing networks: Achievable rate and power efficiency," *IEEE Systems Journal*, major revision.

2. Y. Deng, **L. Wang**, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Enhancing security in large scale spectrum sharing networks," *IEEE Transactions on Wireless Communications*, under review.

3. Y. Deng, **L. Wang**, M. Elkashlan, K. J. Kim, and T. Q. Duong, "Generalized selection combining for cognitive relay networks over Nakagami-m fading," *IEEE Transactions on Signal Processing*, accepted to appear.

4. N. Yang, **L. Wang**, G. Geraci, M. Elkashlan, and J. Yuan, "Safeguarding 5G wireless communication systems using physical layer security," *IEEE Communications Magazine*, accepted to appear.

5. **L. Wang**, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, January 2015.

6. **L. Wang**, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, November 2014.

7. M. Elkashlan, **L. Wang**, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Transactions on Vehicular Technology*, accepted to appear.

8. Y. Liu, **L. Wang**, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, February 2015.

9. K. J. Kim, **L. Wang**, T. Q. Duong, M. Elkashlan and H. Poor, "Cognitive single carrier systems: Joint impact of multiple licensed transceivers," *IEEE Transactions on Wireless Communications*, vol. pp, no. 99, December 2014.

10. **L. Wang**, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Communications Letters*, vol. 3, no. 3, June 2014.

11. **L. Wang**, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, February 2014.

Conference Papers

1. Y. Liu, **L. Wang**, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks with wireless power trans-

fer," in Proc. IEEE Int. Communications Conf. (ICC'15), London, June 2015.

2. A. He, **L. Wang**, Y. Chen, D. Liu, and T. Zhang, "Comparison of CoMP and MISO for Energy Efficiency in HetNets," IEEE WCNC workshop on Cooperative and Heterogeneous Cellular Networks, March 2015.

3. **L. Wang**, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "On the security of cooperative single carrier systems," in Proc. IEEE Global Telecommunications Conf. (GLOBECOM'14), Austin TX, USA, December 2014.

4. Y. Liu, **L. Wang**, M. Elkashlan, T. Q. Duong, and A. Nallanathan, "Two-way relaying networks with wireless power transfer: Policies design and throughput analysis," in Proc. IEEE Global Telecommunications Conf. (GLOBECOM'14), Austin TX, USA, December 2014.

5. **L. Wang**, M. Elkashlan, T. Q. Duong, and R. W. Heath Jr., "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in Proc. IEEE Int. Workshop on Signal Processing Advances in Wireless Communications (SPAWC'14), Toronto, Canada, June 2014. (Invited)

6. **L. Wang**, M. Elkashlan, J. Huang, R. Schober and R. K. Mallik, "Secrecy outage of TAS/GSC in Nakagami-m fading channels," in Proc. IEEE Int. Communications Conf. (ICC'14), Sydney, Australia, June 2014.

7. **L. Wang**, Q. Li, S. Li, and J. Chen, "A general algorithm for uplink opportunistic interference alignment in cellular network," in IEEE GLOBECOM Workshop on Multicell Cooperation, Houston, TX USA, Dec. 2011, pp. 436-440.

Chapter 2

Fundamental Concepts

2.1 Introduction

In this chapter, fundamental concepts are clarified: 1) The basic idea of physical layer security is presented; 2) Physical layer security exploits the properties of the wireless fading channel to transmit confidential messages, therefore several practical and realistic fading models are described; 3) Stochastic geometry is presented as a useful tool to model large-scale wireless networks, in which large number of nodes are randomly located; 4) Antenna selection is presented as a practical implementation design for the uplink of 4G long term evolution (LTE) and LTE-Advanced [5]. It is well known that using antenna selection can achieve the full diversity gain with less number of radio frequency (RF) electronics [68]; 5) Relay protocols are discussed. When the relay is untrusted, secure transmission cannot be achieved by using conventional protocols such as amplify-and-forward and decode-and-forward. The implementation of cooperative jamming can help to achieve positive secrecy rate in untrusted relay networks; 6) Cognitive radio is discussed as an effective way to cope with the scarce spectrum and improve the spectrum efficiency [69]; 7) Single carrier systems is presented as an important technology to support high-speed short-range transmission. It is well-known that single carrier

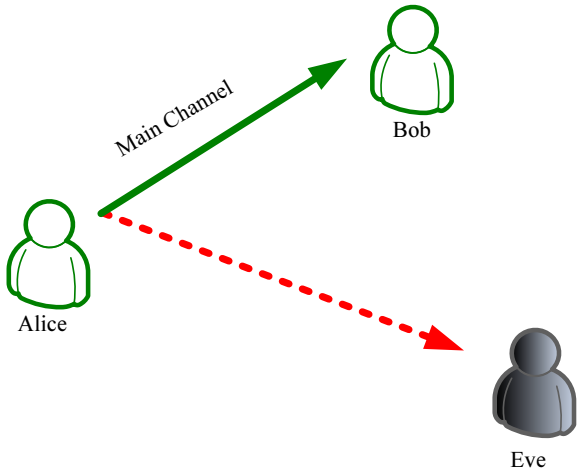

Figure 2.1: A basic wiretap channel.

transmission has a lower peak-to-average power ratio (PAPR) compared to orthogonal frequency-division multiplexing (OFDM); and 8) Wireless sensor networks (WSNs) is discussed, motivated by its widespread use in industrial and scientific applications such as environmental sensing, health monitoring, and military communications [70].

2.2 Physical Layer Security

Physical layer security is not a new paradigm, since it was first proposed by Wyner in the 1970s [22]. Triggered by new transmission techniques such as multiple-input multiple-output (MIMO), cooperative relaying, and emerging decentralized networks such as ad-hoc and sensor networks, physical layer security as a low-complexity approach has regained attention. Under physical layer secrecy constraint, various signal processing techniques have been proposed and analyzed [71]. In [72], artificial noise was designed at the transmitter to confuse the eavesdropper and enhance the secrecy.

A basic wiretap channel is shown in Figure 2.1, where the transmitter (Alice) transmits the secrecy information to the legitimate receiver (Bob), and the eavesdropper (Eve) intends to maliciously obtain this information. In his pioneering work, Wyner has shown that for a degraded eavesdropper's channel, Alice can transmit the confidential

information at a positive secrecy rate, and Eve cannot obtain any bits of information. The secrecy capacity is characterized as [28, 35]

$$C_s = [C_{\mathrm{M}} - C_{\mathrm{E}}]^+ ,$$

where C_{M} is the main channel capacity, and C_{E} is the eavesdropper's channel capacity.

In practice, Alice encodes a message block W^k into a codeword X^n, and Eve receives Y_w^n from the output of its channel. The equivocation rate of Eve is $R_e = H\left(W^k \middle| Y_w^n\right)/n$, which is the amount of ignorance that the eavesdropper has about a message W^k [28]. A secrecy rate R can be achieved when $R \leq R_e$, and C_s is the maximum of the achievable secrecy rate [28].

2.3 Wireless Fading Channels

In this section, some typical fading channels are briefly illustrated. Chapters 3 and 4 consider the two-wave with diffuse power fading channel and Nakagami-m fading channel, respectively, and Chapters 5-8 take into account the Rayleigh fading channel.

2.3.1 Two-wave with Diffuse Power Fading

The two-wave with diffuse power (TWDP) fading was first modeled in [73] to characterize the propagation scenario where the received signal contains two strong, specular multipath waves. This fading model is of high flexibility as it includes Rayleigh, Rician, and hyper-Rayleigh fading as special cases. In particular, it was verified in [74] that the TWDP fading model provides a more accurate way to represent real-world frequency-selective fading data from wireless sensor networks. Moreover, it can be used to describe a link worse than Rayleigh fading [75]. As such, some research attention has been paid to examine the performance of wireless networks under TWDP fading. For example, the

average bit error rate was analyzed in [76] for quadrature amplitude modulation and in [77] for non-coherent multiple frequency-shift keying. More recently, the outage probability was derived in [78] for single decode-and-forward (DF) relay networks. In [79], the symbol error rate was derived for multiple DF relay networks.

In Chapter 3, maximal ratio combining (MRC) is adopted to combine the TWDP fading signals at the receiver. Hence, the PDF for the sum of TWDP fading channel power gains after MRC is expressed as

$$f(\tau) = \frac{1}{2^M} \sum_{l=1}^{\tilde{L}_M} \frac{u_l}{2\sigma^2} e^{-\frac{\tau+\vartheta_l}{2\sigma^2}} \sum_{k=0}^{\infty} \left(\frac{\vartheta_l}{2\sigma^2}\right)^k \frac{1}{k!\,(M+k-1)!} \left(\frac{\tau}{2\sigma^2}\right)^{M+k-1}, \tag{2.1}$$

where M is the number of receive antennas, $\tilde{L}_M = (2L)^M$, L is the order of the PDF, u_l is the lth entry of $\mathbf{u}$ with $\mathbf{u} = \tilde{\mathbf{a}}_1 \otimes \cdots \tilde{\mathbf{a}}_m \otimes \cdots \otimes \tilde{\mathbf{a}}_M$ and $\tilde{\mathbf{a}}_m = [\tilde{a}_1 \cdots \tilde{a}_l \cdots \tilde{a}_{2L}]$, $\tilde{a}_l = a_{\lfloor (l+1)/2 \rfloor}$, where the first five values of $\{a_i\}_{i=1}^{L}$ are given in Table II of [73], $\vartheta_l = \ln(\omega_l)$, ω_l is the lth entry of ω with $\omega = \tilde{\mathbf{b}}_1 \otimes \cdots \tilde{\mathbf{b}}_m \otimes \cdots \otimes \tilde{\mathbf{b}}_M$ and $\tilde{\mathbf{b}}_m = [\exp(\kappa_{m,1}) \cdots \exp(\kappa_{m,l}) \cdots \exp(\kappa_{m,2L})]$, $\kappa_{m,l} = K_m \left(1 + (-1)^l \Delta_m \cos \frac{\lfloor (l-1)/2 \rfloor \pi}{2L-1}\right) 2\sigma^2$, K_m is the ratio of the total specular power to diffuse waves, Δ_m is the relative strength of the two specular components for the mth TWDP branch channel, and $2\sigma^2$ is the average power of the diffuse waves. When $K_m = 0$, TWDP fading reduces to Rayleigh fading, and when $K_m \neq 0$ and $\Delta_m = 0$, TWDP fading reduces to Rician fading.

2.3.2 Nakagami-m Fading

Nakagami-m distribution has versatility in providing a good match to various empirically obtained measurement data [80]. Moreover, it includes Rayleigh as a special case [81]. The PDF of the Nakagami-m channel power gain τ is given by

$$f(\tau) = \frac{m^m \tau^{m-1}}{(m-1)!\bar{\tau}^m} e^{-m\frac{\tau}{\bar{\tau}}}, \tag{2.2}$$

where m is the fading severity parameter and $\bar{\tau} = \mathbb{E}\{\tau\}$ is the mean value.

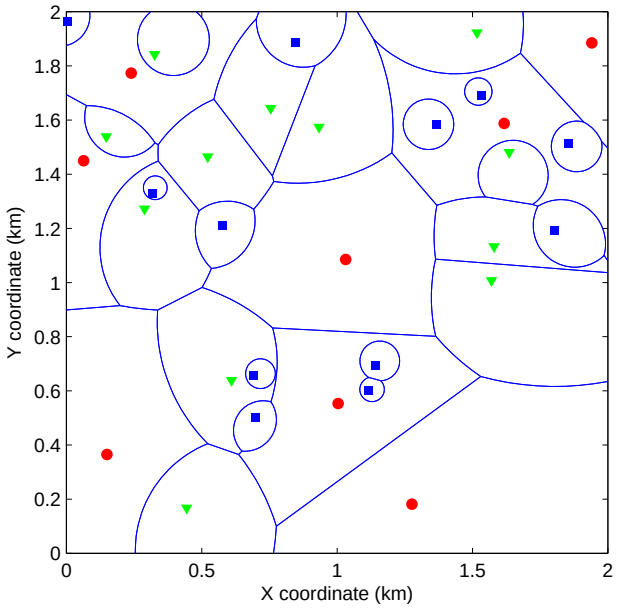

Figure 2.2: A three-tier HCNs with stochastic geometry, where macrocell base stations (red circle) are overlaid with picocell bases stations (green triangle) and femtocell base stations (blue square).

2.3.3 Rayleigh Fading

Rayleigh fading channel is commonly considered in the literature. When the multiple reflective paths are large in number and there is no line-of-sight signal component, the envelope of the received signal τ is statistically described by a Rayleigh probability density function (PDF) [82], which can be expressed as

$$f(\tau) = \frac{2\tau}{\sigma} e^{-\tau^2/\sigma}, \tag{2.3}$$

where $\sigma = \mathbb{E}\{\tau^2\}$.

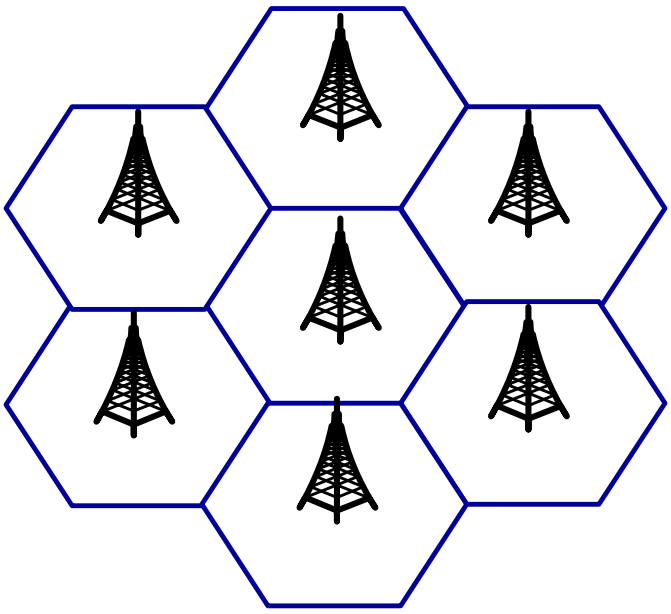

Figure 2.3: Hexagonal Cellular Networks.

2.4 Stochastic Geometry

In conventional system model, density of nodes, node mobility, and triangle inequalities are usually ignored. Stochastic geometry is a useful tool to analyze the average behavior over many spatial realizations of a network whose nodes are located according to some distributions [83]. Recent studies such as [84–87] have shown that stochastic geometry can well model the heterogeneous cellular networks (HCNs). As shown in Figure 2.2, a Poisson point process (PPP) model is used for modeling the three-tier downlink HCNs. The traditional hexagonal model with fixed geometry (See Figure 2.3) cannot model the unplanned networks such as femtocells [86]. Therefore, stochastic geometry is very useful for modeling practical random and distributed networks such as wireless sensor networks and ad-hoc networks.

In stochastic geometry theory, PPP is commonly-used in the literature such as [85, 88], which is defined as follows [83]:

Poisson Point Process (PPP) Definition: Let Λ be a locally finite measure on some metric space $\mathcal{E}$. A point process Φ is Poisson on $\mathcal{E}$ if

- For all disjoint subsets $\mathcal{A}_1,\ldots,\mathcal{A}_n$ of $\mathcal{E}$, the random variables $\Phi(\mathcal{A}_i)$ are independent;
- For all sets $\mathcal{A}$ of $\mathcal{E}$, the random variables $\Phi(\mathcal{A})$ are Poisson;

A PPP can be either homogeneous or heterogeneous. In homogeneous PPP, the density of the points is constant. A fundamental property of PPP is the Slivnyak's theorem, which is as follows [89]:

Slivnyak's Theorem: Let Φ denote a PPP with intensity measure Λ. For Λ almost all $x \in \mathbb{R}^d$,

$$P_x^!(\cdot) = P(\Phi \in \cdot);$$

that is, the reduced Palm distribution $P_x^!(\cdot)$ of the PPP is equal to its original distribution.

Slivnyak's theorem shows that for a PPP including an arbitrary point x, it is identical to the law of the original PPP if point x is ignored. Another useful property that calculates the products over PPP is the probability generating functional (PGFL), which is as follows [90]:

$$\mathbb{E}\left[\prod_{x\in\Phi} f(x)\right] = \exp\left(-\int_{\mathbb{R}^n} (1 - f(x))\,\Lambda(dx)\right).$$

In Chapter 8, a stochastic geometry approach is proposed to model a three-tier wireless sensor network, where the positions of the sensors, access points, sinks, and eavesdroppers are modeled following the independent homogeneous PPPs.

2.5 Antenna Selection

2.5.1 Transmit Antenna Selection and Selection Combining

Transmit antenna selection (TAS) is a low-complexity transmission design, which demands small feedback information. The core idea behind TAS is to select a single antenna that maximizes the receive signal power. TAS achieves the full diversity gain with a single RF chain and has been implemented in LTE systems.

Selection combining adopts the best receive antenna with the largest receive signal power to receive the signal and save the RF chains compared to MRC with multiple RF chains. It has been standardized in the IEEE 802.11n for WLAN [3] and the IEEE 802.16 for WiMAX [4]. In Chapter 5, selection combining at the legitimate receiver and the eavesdropper is considered.

2.5.2 Generalized Selection Combining

Generalized selection combining (GSC), or the so-called hybrid-selection/MRC (HS/MRC), selects a subset of diversity branches with largest signal-to-noise ratio (SNR) and combines them using MRC. This diversity combining method offers a tradeoff between the performance advantage of MRC and the implementation advantage of SC [91]. With the help of the moment generating function (MGF), the performance of GSC was examined over Rayleigh fading [92] and Nakagami fading [93]. The impact of correlated Nakagami fading on GSC was considered in [94, 95]. In [96, 97], the high SNR performance of GSC was analyzed in various environments. In [98], approximations were presented for the high SNR performance of GSC in relay networks over Nakagami-m fading channels. Motivated by these prior works, new analytical results for secure communications with GSC are provided in this thesis.

2.6 Relay

Relay transmission has been widely studied [41, 99], since it can expand the coverage and enhance the system performance. Many relay protocols have been proposed such as amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF) etc. In this thesis, AF and DF are considered.

2.6.1 Amplify-and-Forward

In AF protocol, the source first transmits the signal to the relay, then the relay amplifies the signal and forwards the signal to the destination [99, 100]. In two-hop AF relay networks, based on the end-to-end (e2e) SNR, the achievable rate is expressed as [100]

$$R_{e2e} = \log_2 \left(1+\frac{\gamma_{s,r}\gamma_{r,d}}{1+\gamma_{s,r}+\gamma_{r,d}}\right), \tag{2.4}$$

where $\gamma_{s,r}$ is the receive SNR at the relay and $\gamma_{r,d}$ is the receive SNR at the destination. When the relay is untrusted as an eavesdropper, the secrecy rate is given by [51]

$$R_s = \left[R_{e2e} - \log_2 \left(1 + \gamma_{s,r}\right)\right]^+. \tag{2.5}$$

Note that

$$\frac{\gamma_{s,r}\gamma_{r,d}}{1+\gamma_{s,r}+\gamma_{r,d}} < \min\left\{\gamma_{s,r},\gamma_{r,d}\right\} \leq \gamma_{s,r}.$$

The secrecy rate R_s in (2.5) is zero. Therefore, in two-hop untrusted relay networks, secrecy cannot be achieved for AF transmission. Cooperative jamming is an appealing scheme to achieve positive secrecy rate in two-hop untrusted relay networks [101], and more details are discussed in the following Section 2.7.

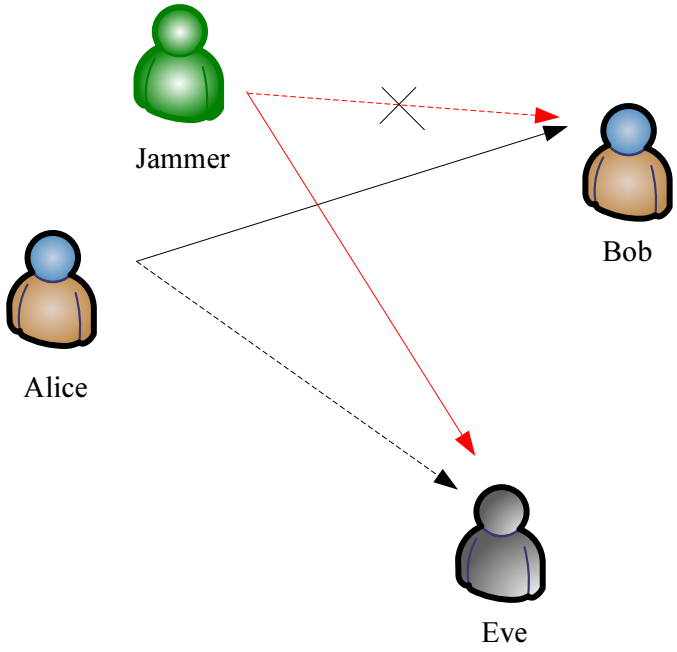

Figure 2.4: A basic wiretap channel with an external cooperative jammer.

2.6.2 Decode-and-Forward

In DF protocol, relay first decodes the signal from the source, then re-encodes it and forwards it to the destination [99]. Therefore, the untrusted DF relay cannot be employed to help forward confidential signals.

2.7 Cooperative Jamming

Cooperative jamming is a security enhancement approach, which can be used to confuse the external eavesdroppers [14, 102–104] or the untrusted relays [101, 105].

As shown in Figure 2.4, Alice transmits the confidential signal to Bob, and Eve intercepts the signal. The external cooperative jammer transmits the jamming signal to confound Eve. In such a scenario, interference from the jamming signal should be mitigated at Bob. If the interfering signal from the cooperative jammer can be shared by Bob with specific method (e.g., use the seed of the random noise generator in a secure

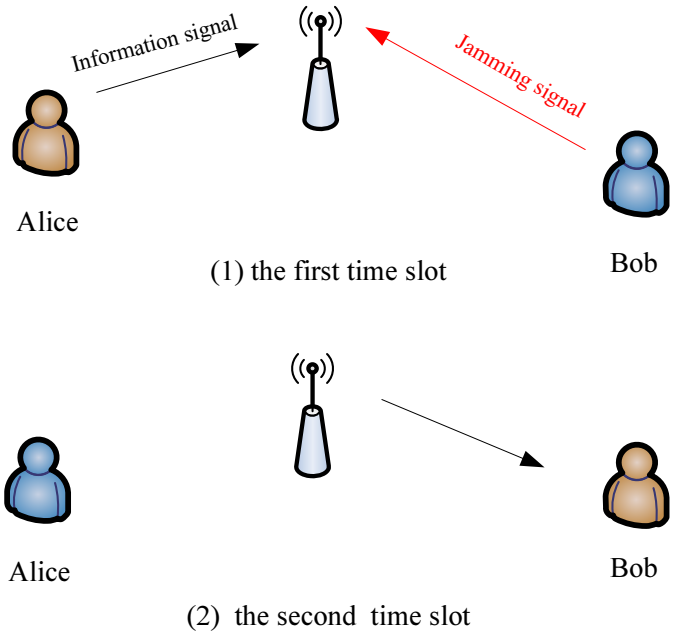

Figure 2.5: A two-hop untrusted relay networks with destination-based cooperative jamming.

fashion [106]), Bob can cancel the jamming signal. Another promising way is for the jammer to use null-steering beamforming [104], i.e., the jamming signal is transmitted using the null space of the channel between jammer and Bob. As such, Bob will not receive the jamming signal.

In untrusted relay networks, destination-based cooperative jamming was proposed to achieve positive secrecy rate [101]. As shown in Figure 2.5, there are two time slots for each information transmission. In the first time slot, while Alice transmits the information signal, Bob transmits the jamming signal. In the second time slot, the relay forwards the signals to Bob. Since Bob knows the jamming signal, it can easily cancel the jamming signal. In Chapter 7, optimal power allocation with cooperative jamming is proposed in two-hop untrusted relay networks.

2.8 Cognitive Radio Networks

Frequency spectrum is an increasingly scarce and expensive wireless resource due to the upsurge in demand for multimedia services in current and future generation wireless networks. Unfortunately, recent measurement campaigns have found that the radio frequency spectrum is not being efficiently utilized [107–113]. Cognitive radio, proposed by Mitola in [114], has the potential to mitigate such inefficiency. Particularly, by allowing a secondary user (SU) to reuse the radio spectrum that is licensed to a primary user (PU), the scarcity of frequency spectrum can be alleviated. Several approaches to cognitive radio such as overlay, interweave, and underlay have been considered [115]. Among them, the most promising approach is underlay spectrum sharing in which the SU simultaneously transmits in the same radio spectrum as the PU, provided that the secondary transmission does not exceed the maximum interference constraint set by the primary network [116]. One of the drawbacks of underlay spectrum sharing is the need to limit the transmit power of the SU transmitter (SU-Tx) to avoid any deleterious effect on the PU receiver (PU-Rx). In some practical scenarios, the cognitive radio network may not be feasible due to heavy pathloss and severe shadowing [117]. As such, several advanced transmission technologies have been introduced to enhance the performance of underlay spectrum sharing such as cognitive relaying [118] and cognitive multiuser diversity [119]. In Chapter 5, secrecy outage for passive eavesdropping is first examined in cognitive radio network.

2.9 Single Carrier Transmission

In practice, multipath components frequently exist in wireless communication systems due to multiple reflectors, in which reflectors cause a time dispersion and frequency selective fading. If the signal bandwidth is larger than the frequency coherence bandwidth or the delay spread is larger than the symbol duration, the signal is distorted due to intersymbol interference (ISI). To avoid the use of equalizers in dealing with ISI, single carrier

(SC) transmission is an alternative attractive solution which uses an increased symbol duration by forming a transmission block symbol [120, 121], with additional cyclic prefix (CP) symbols in front of the transmission block symbol. Thus, compared to OFDM transmission, a block-wise processing is necessary for CP-SC transmission. There are several existing works and on-going activities in the context of CP-SC transmission in several different domains, including non-cooperative systems, cooperative relaying systems, and spectrum sharing systems, as follows.

- *Non-cooperative systems:* Opportunistic scheduling was proposed in [122] to achieve multiuser diversity. In [123], cyclic delay diversity (CDD) was employed for the frequency-domain equalizer (FDE), whereas distributed space-frequency block coding was employed in CP-SC systems [124] to achieve transmit diversity gain. Several channel estimators for CP-SC systems were investigated in [125–127].

- *Cooperative relaying systems:* For several relaying protocols such as DF and AF, as well as project and forward relaying [128], optimal power allocation [129], new receiver design [130], optimal training sequences for channel estimation [131], and best terminal selection [132] were proposed to enhance the performance.

- *Spectrum sharing systems:* For cooperative spectrum sharing [133, 134], and non-cooperative spectrum sharing [135], CP-SC transmission was proposed to examine the impact of multipath diversity on the system performance, by taking into account several performance indicators such as outage probability, symbol error rate, and ergodic capacity.

In Chapter 6, physical layer security is first introduced in single carrier system. An analytical framework is presented and key performance parameters such as multiplexing gain and secrecy diversity gain are explicitly demonstrated.

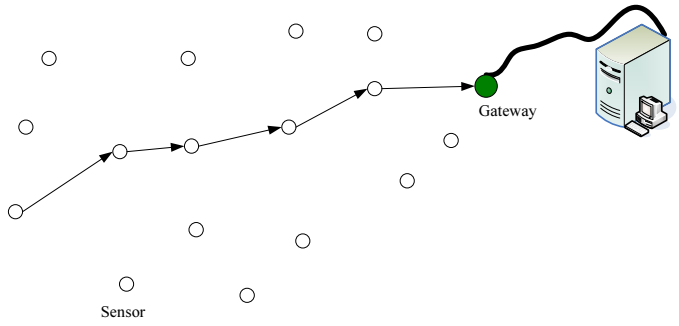

Figure 2.6: Multihop architecture in wireless sensor networks.

2.10 Wireless Sensor Networks

Wireless sensor networks (WSNs) have attracted considerable attention from industry and academia, due to its civilian and military applications [70]. In WSNs, the low-power low-cost sensors are densely deployed. As shown in Figure 2.6, sensors are randomly located, and sensed data are routed back to the gateway through multihop transmission.

Since the sensors are battery-powered devices, it is important to save the sensors'energy, in order to prolong the lifetime of the network. In [136], the delay-aware data collection network structure in WSNs was investigated, in which the delays in the data collection process can be shortened. In [137], an energy-efficient hybrid data collection scheme was proposed and it is shown that substantial energy saving is achieved. In practice, sensors are located in the remote areas, and mobile sinks or data collectors are employed to collect the sensed data [138, 139]. In [138], the impact of density of data collectors on the the successful connectivity probability was examined based on stochastic geometry model. In [139], the use of pairwise key predistribution scheme was developed to provide authentication and pairwise key establishment between the sensors and mobile sinks. In Chapter 8, physical layer security in three-tier wireless sensor networks is proposed, where the sensors communicate with sinks with the help of access points in the presence of eavesdropping.

Chapter 3

Physical Layer Security Enhancement in Two-Wave with Diffuse Power Fading Channels

3.1 Introduction

In this chapter, physical layer security enhancement in the single-input multiple-output (SIMO) wiretap channel with two-wave with diffuse power (TWDP) fading is examined. In this wiretap channel, a single antenna transmitter sends confidential information to an M-antenna receiver, while an N-antenna eavesdropper overhears the transmission. To leverage the benefits of multiple antennas, we assume that maximal-rational combining (MRC) is applied at the receiver and the eavesdropper. We address two practical eavesdropping scenarios. In the first scenario, we consider that the *eavesdropper's channel state information (CSI) is available at the transmitter*. In the second scenario, we consider that the *eavesdropper's CSI is not available at the transmitter*. For the first scenario, we characterize the average secrecy capacity as the principal security performance metric. Since the CSI of the eavesdropper is available at the transmitter, the transmitter adapts its transmission rate in order to achieve perfect secrecy. For the second scenario, we characterize the secrecy outage probability as the principal security metric. Since the CSI of the eavesdropper is not available at the transmitter, the transmitter selects a

constant secrecy rate and perfect secrecy is not always guaranteed.

Notation: $(\cdot)^T$ denotes the transpose operator, $(\cdot)^H$ denotes the conjugate transpose operator, $\|\cdot\|$ denotes the Euclidean norm, $\mathbf{I}_M$ denotes the $M \times M$ identity matrix, $\mathbf{0}_{M\times N}$ denotes the $M \times N$ zero matrix, $\mathrm{E}[\cdot]$ denotes the expectation operator, $\otimes$ denotes the kronecker product operator, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x, and $o(\cdot)$ denotes the higher order terms.

3.2 System Model and Channel Statistical Properties

3.2.1 System Model

Figure 3.1 depicts a SIMO wiretap channel where the transmitter (Alice) encodes her messages and transmits the codewords to the legitimate receiver (Bob), while the malicious eavesdropper (Eve) overhears the transmission. We denote the channel between Alice and Bob as the main channel, and the channel between Alice and Eve as the eavesdropper's channel. We assume that Alice is equipped with a single antenna, Bob is equipped with M antennas, and Eve is equipped with N antennas. In this wiretap channel, the secrecy capacity C_S is defined as [35]

$$C_S = [C_M - C_N]^+, \tag{3.1}$$

where $C_M = \log_2(1+\gamma_M)$ is the capacity of the main channel and $C_N = \log_2(1+\gamma_N)$ is the capacity of the eavesdropper's channel. Here, we denote γ_M as the instantaneous received SNR of the main channel and γ_N as the instantaneous received SNR of the eavesdropper's channel. It is evident from (3.1) that C_S increases with C_M and diminishes with C_N. Motivated by this, Bob applies MRC to combine the received signals and maximize the received SNR. This allows Bob to exploit the M-antenna diversity and maximize the probability of secure transmission. On the other hand, Eve applies MRC to exploit the N-antenna diversity and maximize the probability of successful

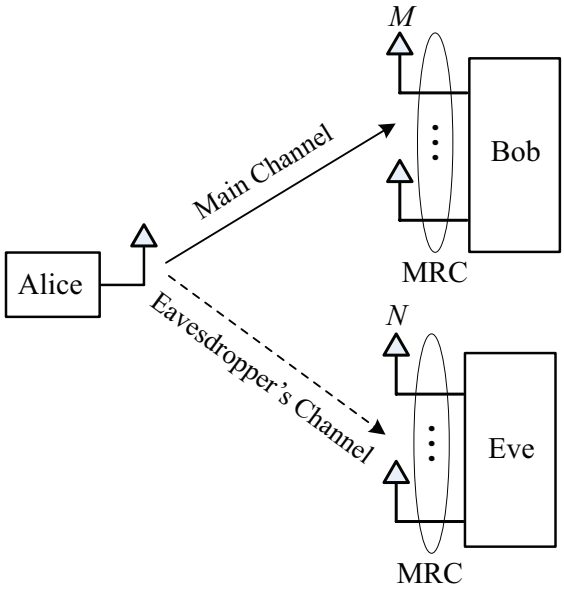

Figure 3.1: Illustration of a SIMO wiretap channel, where an N-antenna eavesdropper (Eve) overhears the transmission from a single antenna transmitter (Alice) to an M-antenna legitimate receiver (Bob).

eavesdropping.

For this wiretap channel, we take into account two distinct scenarios: 1) active eavesdropping and 2) passive eavesdropping. In active eavesdropping, the CSI of the main channel and the eavesdropper's channel are available at Alice. Based on the CSI of these two channels, Alice calculates C_M and C_N and then determine C_S according to (3.1). After this, Alice transmits its messages at a secrecy rate no higher than C_S. In this scenario, perfect secrecy is always guaranteed. In passive eavesdropping, the CSI of the main channel is available at Alice but the CSI of the eavesdropper's channel is not known at Alice. As such, Alice selects a constant secrecy rate R_S to transmit its messages. In this scenario, perfect secrecy is achieved when $R_S < C_S$, and is compromised otherwise.

To perform secure transmission, Alice encodes the message block $\mathbf{w}$ into the codeword $\mathbf{x} = [x(1), \cdots, x(l), \cdots, x(L)]$,where L is the length of $\mathbf{x}$. This codeword is subject to the average power constraint $\frac{1}{L}\sum_{l=1}^{L} E\left[|x(l)|^2\right] \leq P$. We assume that both the main channel and the eavesdropper's channel are quasi-static fading channels where the channel coefficients are constant for each transmission block but vary independently

between different blocks. At the lth time slot, the MRC-combined signal vector at Bob is written as

$$\mathbf{y}_M(l) = \mathbf{h}_M^H \mathbf{h}_M x(l) + \mathbf{h}_M^H \mathbf{n}_M, \tag{3.2}$$

where $\mathbf{h}_M$ is the $M \times 1$ main channel vector and $\mathbf{n}_M \sim \mathcal{CN}_{M\times 1}\left(\mathbf{0}_{M\times 1}, \delta_M^2 \mathbf{I}_M\right)$ is the additive white Gaussian noise (AWGN) vector at Bob. Based on (3.2), the instantaneous SNR of the main channel is given by $\gamma_M = \|\mathbf{h}_M\|^2 P/\delta_M^2$. Correspondingly, the average SNR of the main channel is given by $\overline{\gamma}_M = E\left[\|\mathbf{h}_M\|^2\right] P/\delta_M^2$. In the eavesdropper's channel, the MRC-combined signal vector at Eve is written as

$$\mathbf{y}_N(l) = \mathbf{h}_N^H \mathbf{h}_N x(l) + \mathbf{h}_N^H \mathbf{n}_N, \tag{3.3}$$

where $\mathbf{h}_N$ is the $N \times 1$ eavesdropper's channel vector and $\mathbf{n}_N \sim \mathcal{CN}_{N\times 1}\left(\mathbf{0}_{N\times 1}, \delta_N^2 \mathbf{I}_N\right)$ is the AWGN vector at Eve. Based on (3.3), the instantaneous SNR of the eavesdropper's channel is given by $\gamma_N = \|\mathbf{h}_N\|^2 P/\delta_N^2$. Correspondingly, the average SNR of the eavesdropper's channel is given by $\overline{\gamma}_N = E\left[\|\mathbf{h}_N\|^2\right] P/\delta_N^2$.

3.2.2 Channel Statistical Properties

In the wiretap channel, we assume that the main channel and eavesdropper's channel are subject to independent and non-identically distributed (i.n.i.d.) TWDP fading. According to [78], the probability density function (PDF) of γ_M is given by

$$\begin{aligned} f_{\gamma_M}(\gamma) =& \frac{1}{2^M \overline{\gamma}_M} \sum_{l=1}^{\tilde{L}_M} \frac{u_{M,l}}{2\sigma_M^2} e^{-\frac{\left(\frac{\gamma}{\overline{\gamma}_M}\right)+\vartheta_{\gamma_{M,l}}}{2\sigma_M^2}} \sum_{k=0}^{\infty} \left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma_M^2}\right)^k \\ & \times \frac{1}{k!\,(M+k-1)!} \left(\frac{\gamma}{2\sigma_M^2 \overline{\gamma}_M}\right)^{M+k-1}, \end{aligned} \tag{3.4}$$

where $\tilde{L}_M = (2L)^M$, L is the order of the PDF, $u_{M,l}$ is the lth entry of $\mathbf{u}_M$ with $\mathbf{u}_M = \tilde{\mathbf{a}}_1 \otimes \cdots \tilde{\mathbf{a}}_m \otimes \cdots \otimes \tilde{\mathbf{a}}_M$ and $\tilde{\mathbf{a}}_m = [\tilde{a}_1 \cdots \tilde{a}_l \cdots \tilde{a}_{2L}]$, $\tilde{a}_l = a_{\lfloor (l+1)/2 \rfloor}$, where the first five

values of $\{a_i\}_{i=1}^{L}$ are given in Table II of [73], $\vartheta_{\gamma_{M,l}} = \ln(\omega_{\gamma_{M,l}})$, $\omega_{\gamma_{M,l}}$ is the lth entry of ω_{γ_M} with $\omega_{\gamma_M} = \tilde{\mathbf{b}}_1 \otimes \cdots \tilde{\mathbf{b}}_m \otimes \cdots \otimes \tilde{\mathbf{b}}_M$ and $\tilde{\mathbf{b}}_m = [\exp(\kappa_{m,1}) \cdots \exp(\kappa_{m,l}) \cdots \exp(\kappa_{m,2L})]$, $\kappa_{m,l} = K_m \left(1 + (-1)^l \Delta_m \cos \frac{\lfloor (l-1)/2 \rfloor \pi}{2L-1}\right) 2\sigma_M^2$, K_m is the ratio of the total specular power to diffuse waves, and Δ_m is the relative strength of the two specular components for the mth TWDP branch channel at Bob. Based on (3.4), the cumulative distribution function (CDF) of γ_M is derived using [140, eq. (3.351.1)] as

$$\begin{aligned} F_{\gamma_M}(\gamma) &= \int_0^{\gamma} f_{\gamma_M}(x)dx \\ &= 1 - \frac{1}{2^M} e^{-\frac{\gamma}{2\sigma_M^2 \overline{\gamma}_M}} \sum_{l=1}^{\tilde{L}_M} u_{M,l} e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma_M^2}} \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma_M^2}\right)^k \sum_{i=0}^{M+k-1} \frac{1}{i!} \left(\frac{\gamma}{2\sigma_M^2 \overline{\gamma}_M}\right)^i. \end{aligned} \tag{3.5}$$

Similarly, the PDF and CDF of γ_N are given by

$$f_{\gamma_N}(\gamma) = \frac{1}{2^N \overline{\gamma}_N} \sum_{l=1}^{\tilde{L}_N} \frac{u_{N,l}}{2\sigma_N^2} e^{-\frac{\left(\frac{\gamma}{\overline{\gamma}_N}\right) + \vartheta_{\gamma_{N,l}}}{2\sigma_N^2}} \sum_{k=0}^{\infty} \left(\frac{\vartheta_{\gamma_{N,l}}}{2\sigma_N^2}\right)^k \frac{1}{k!\,(N+k-1)!} \left(\frac{\gamma}{2\sigma_N^2 \overline{\gamma}_N}\right)^{N+k-1} \tag{3.6}$$

and

$$F_{\gamma_N}(\gamma) = 1 - \frac{1}{2^N} e^{-\frac{\gamma}{2\sigma_N^2 \overline{\gamma}_N}} \sum_{l=1}^{\tilde{L}_N} u_{N,l} e^{-\frac{\vartheta_{\gamma_{N,l}}}{2\sigma_N^2}} \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{\vartheta_{\gamma_{N,l}}}{2\sigma_N^2}\right)^k \sum_{i=0}^{N+k-1} \frac{1}{i!} \left(\frac{\gamma}{2\sigma_N^2 \overline{\gamma}_N}\right)^i. \tag{3.7}$$

respectively, where $\tilde{L}_N = (2L)^N$, $u_{N,l}$ is the lth entry of $\mathbf{u}_N$ with $\mathbf{u}_N = \tilde{\mathbf{a}}_1 \otimes \cdots \tilde{\mathbf{a}}_n \otimes \cdots \otimes \tilde{\mathbf{a}}_N$ and $\tilde{\mathbf{a}}_n = [\tilde{a}_1 \cdots \tilde{a}_l \cdots \tilde{a}_{2L}]$, $\tilde{a}_l = a_{\lfloor (l+1)/2 \rfloor}$, $\omega_{\gamma_{N,l}}$ is the lth entry of ω_{γ_N} with $\omega_{\gamma_N} = \tilde{\mathbf{b}}_1 \otimes \cdots \tilde{\mathbf{b}}_n \otimes \cdots \otimes \tilde{\mathbf{b}}_N$ and $\tilde{\mathbf{b}}_n = [\exp(\kappa_{n,1}) \cdots \exp(\kappa_{n,l}) \cdots \exp(\kappa_{n,2L})]$, $\kappa_{n,l} = K_n \left(1 + (-1)^l \Delta_n \cos \frac{\lfloor (l-1)/2 \rfloor \pi}{2L-1}\right) 2\sigma_N^2$, K_n is the ratio of the total specular power to diffuse waves, and Δ_n is the relative strength of the two specular components for the nth TWDP branch channel at Eve.

3.3 Ergodic Secrecy Capacity in Active Eavesdropping Scenario

In this section, we concentrate on active eavesdropping where Alice adapts its transmission rate based on C_M and C_N and thus guarantees perfect secrecy. In such a scenario, ergodic secrecy capacity is a pivotal and practical performance metric to quantify the maximum average achievable secrecy rate [35]. Therefore, we derive new exact and asymptotic closed-form expressions for the ergodic secrecy capacity. Based on the asymptotic result, we characterize the high SNR slope and the high SNR power offset which explicitly capture the impact of the channel parameters on the ergodic secrecy capacity at high SNRs [141]. These new closed-form results encompass Rayleigh fading and Rician fading as special cases. To the best of my knowledge, the analytical framework and the results presented in this section are new.

3.3.1 Exact Ergodic Secrecy Capacity

The ergodic secrecy capacity is the average of the instantaneous secrecy capacity C_S over γ_M and γ_N. We formulate the ergodic secrecy capacity as

$$\begin{aligned}\overline{C}_S &= \int_0^\infty \int_0^\infty C_S f_{\gamma_M}(\gamma_1)\, f_{\gamma_N}(\gamma_2) d\gamma_1 d\gamma_2 \\ &= \int_0^\infty \underbrace{\left[\int_0^\infty C_S f_{\gamma_N}(\gamma_2)\, d\gamma_2\right]}_{\hbar_1} f_{\gamma_M}(\gamma_1)\, d\gamma_1. \end{aligned} \tag{3.8}$$

According to (3.1), we first express $\hbar_1$ in (4.10) as

$$\hbar_1 = \int_0^{\gamma_1} \left(\log_2(1+\gamma_1) - \log_2(1+\gamma_2)\right) f_{\gamma_N}(\gamma_2)\, d\gamma_2. \tag{3.9}$$

Utilizing integration by parts and applying some algebraic manipulations, we derive (4.11) as

$$\begin{aligned}\hbar_1 =&\log_2\left(1+\gamma_1\right)F_{\gamma_N}\left(\gamma_1\right)-\int_0^{\gamma_1}\log_2\left(1+\gamma_2\right)f_{\gamma_N}\left(\gamma_2\right)d\gamma_2\\ =&\frac{1}{\ln 2}\int_0^{\gamma_1}\frac{F_{\gamma_N}\left(\gamma_2\right)}{1+\gamma_2}d\gamma_2.\end{aligned} \tag{3.10}$$

Substituting (4.12) into (4.10), we rewrite the ergodic secrecy capacity as

$$\overline{C}_S=\frac{1}{\ln 2}\int_0^{\infty}\left[\int_0^{\gamma_1}\frac{F_{\gamma_N}\left(\gamma_2\right)}{1+\gamma_2}d\gamma_2\right]f_{\gamma_M}\left(\gamma_1\right)d\gamma_1. \tag{3.11}$$

Changing the order of integration in (A.3.1) with the help of [140, eq. (4.611.1)], we obtain

$$\overline{C}_S=\frac{1}{\ln 2}\int_0^{\infty}\frac{F_{\gamma_N}\left(\gamma_2\right)}{1+\gamma_2}\left[1-F_{\gamma_M}\left(\gamma_2\right)\right]d\gamma_2. \tag{3.12}$$

It is shown in (3.12) that $\overline{C}_S$ depends on the statistics of the main channel and the eavesdropper's channel. Substituting (3.5) and (3.7) into (3.12) and applying [140, eq. (1.111)] and [140, eq. (3.351.2)] to solve the resultant integrals, we derive the exact ergodic secrecy capacity as (3.13), where $E_i\left(\alpha\right)$ is the exponential integral function given by $E_i\left(\alpha\right)=e^{\frac{\alpha}{2\sigma^2}}\int_{\frac{\alpha}{2\sigma^2}}^{\infty}\frac{e^{-x}}{x}dx$.

3.3.2 Asymptotic Ergodic Secrecy Capacity

We proceed to derive the asymptotic ergodic secrecy capacity to examine the maximum average achievable secrecy rate in the high SNR regime. To do so, we consider that the average SNR of the main channel is sufficiently high, i.e., $\overline{\gamma}_M\to\infty$[1]. We maintain the consideration of arbitrary values of the average SNR of the eavesdropper's channel.

We commence the asymptotic analysis by presenting the first order expansion of

[1]We note that as $\overline{\gamma}_N\to\infty$, the probability of successful eavesdropping approaches one. As such, we do not consider $\overline{\gamma}_N\to\infty$.

$$\overline{C}_S = \frac{1}{2^M \ln 2} \sum_{l=1}^{\tilde{L}_M} \sum_{k=0}^{\infty} \frac{u_{M,l}}{k!} e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}} \left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}\right)^k \sum_{i=0}^{M+k-1} \frac{1}{i!} \Bigg[E_i\left(\frac{1}{\bar{\gamma}_M}\right)\left(-\frac{1}{2\sigma^2\bar{\gamma}_M}\right)^i + \sum_{q=1}^{i} \binom{i}{q} \left(-\frac{1}{2\sigma^2\bar{\gamma}_M}\right)^{i-q} \sum_{t=0}^{q-1} \frac{(q-1)!}{t!} \left(\frac{1}{2\sigma^2\bar{\gamma}_M}\right)^t - \frac{1}{2^N(\bar{\gamma}_M)^i} \sum_{l_1=1}^{\tilde{L}_N} \sum_{k_1=0}^{\infty} \frac{u_{N,l_1}}{k_1!} e^{-\frac{\vartheta_{\gamma_{N,l_1}}}{2\sigma^2}} \left(\frac{\vartheta_{\gamma_{N,l_1}}}{2\sigma^2}\right)^{k_1} \sum_{j=0}^{N+k_1-1} \frac{1}{j!(\bar{\gamma}_N)^j} \times \Bigg(E_i\left(\frac{1}{\bar{\gamma}_M} + \frac{1}{\bar{\gamma}_N}\right)\left(-\frac{1}{2\sigma^2}\right)^{i+j} + \sum_{\eta=1}^{i+j} \binom{i+j}{\eta} \left(-\frac{1}{2\sigma^2}\right)^{i+j-\eta} \times \sum_{\phi=0}^{\eta-1} \frac{(\eta-1)!}{\phi!} \left(\frac{1}{\overline{\gamma}_M} + \frac{1}{\overline{\gamma}_N}\right)^{\phi-\eta} \left(\frac{1}{2\sigma^2}\right)^{\phi} \Bigg) \Bigg] \tag{3.13}$$

$F_{\gamma_M}(\gamma)$ in the high SNR regime. Applying the Taylor series expansion truncated to the kth order given by $e^x = \sum_{j=0}^{k} x^j/j! + o\left(x^k\right)$ [142] in (3.5), we derive the first order expansion of $F_{\gamma_M}(\gamma)$ as

$$\begin{aligned} F_{\gamma_M}(\gamma) &= 1 - \frac{1}{2^M} \sum_{l=1}^{\tilde{L}_M} u_{M,l} e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}} \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}\right)^k \\ &\quad \times e^{-\frac{\gamma}{2\sigma^2\overline{\gamma}_M}} \left[e^{\frac{\gamma}{2\sigma^2\overline{\gamma}_M}} - \frac{1}{(M+k)!} \left(\frac{\gamma}{2\sigma^2\overline{\gamma}_M}\right)^{M+k} - o\left(\left(\frac{\gamma}{2\sigma^2\overline{\gamma}_M}\right)^{M+k}\right) \right] \\ &= \frac{1}{2^M M!} \sum_{l=1}^{\tilde{L}_M} u_{M,l} e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}} \left(\frac{\gamma}{2\sigma^2\overline{\gamma}_M}\right)^M + o\left(\overline{\gamma}_M^{-M}\right). \end{aligned} \tag{3.14}$$

To facilitate our asymptotic analysis, we rewrite (3.7) as $F_{\gamma_N}(\gamma) = 1 - \chi_{\gamma_N}(\gamma)$, where

$$\chi_{\gamma_N}(\gamma) = \frac{1}{2^N} e^{-\frac{\gamma}{2\sigma_N^2\overline{\gamma}_N}} \sum_{l=1}^{\tilde{L}_N} u_{N,l} e^{-\frac{\vartheta_{\gamma_{N,l}}}{2\sigma_N^2}} \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{\vartheta_{\gamma_{N,l}}}{2\sigma_N^2}\right)^k \sum_{i=0}^{N+k-1} \frac{1}{i!} \left(\frac{\gamma}{2\sigma_N^2\overline{\gamma}_N}\right)^i.$$

It follows that (A.3.1) is re-expressed as

$$\begin{aligned}\overline{C}_S &= \frac{1}{\ln 2}\int_0^{\infty}\left(\int_0^{\gamma_1}\frac{1-\chi_{\gamma_N}(\gamma_2)}{1+\gamma_2}d\gamma_2\right)f_{\gamma_M}(\gamma_1)d\gamma_1 \\ &= \kappa_1 - \kappa_2, \end{aligned} \tag{3.15}$$

where

$$\kappa_1 = \frac{1}{\ln 2}\int_0^{\infty}\ln(1+\gamma_1)\,f_{\gamma_M}(\gamma_1)d\gamma_1 \tag{3.16}$$

and

$$\kappa_2 = \frac{1}{\ln 2}\int_0^{\infty}\int_0^{\gamma_1}\frac{\chi_{\gamma_N}(\gamma_2)}{1+\gamma_2}f_{\gamma_M}(\gamma_1)d\gamma_2 d\gamma_1. \tag{3.17}$$

We next derive the asymptotic expressions for κ_1 and κ_2. In the high SNR regime with $\overline{\gamma}_M \to \infty$, we have $\ln(1+\gamma_1) \approx \ln(\gamma_1)$. As such, we apply [140, eq. (4.352.1)] and perform some algebraic manipulations to derive the asymptotic expression for κ_1 as

$$\begin{aligned}\kappa_1^{\infty} =& \frac{1}{\ln 2}\int_0^{\infty}\ln(\gamma_1)\,f_{\gamma_M}(\gamma_1)d\gamma_1 \\ =& \log_2\left(2\sigma^2\overline{\gamma}_M\right) + \frac{1}{2^M\ln 2}\sum_{l=1}^{\tilde{L}_M}u_{M,l}e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}}\sum_{k=0}^{\infty}\frac{\psi(M+k)}{k!}\left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}\right)^k, \end{aligned} \tag{3.18}$$

where $\psi(\cdot)$ is the digamma function [143].

To derive the asymptotic expression for κ_2, we change the order of integration in (3.17) and rewrite κ_2 as

$$\kappa_2 = \frac{1}{\ln 2}\int_0^{\infty}\frac{\chi_{\gamma_N}(\gamma_2)}{1+\gamma_2}\left[1-F_{\gamma_M}(\gamma_2)\right]d\gamma_2. \tag{3.19}$$

From (3.14), we find that $F_{\gamma_M}(\gamma) \approx 0$ when $\overline{\gamma}_M \to \infty$. Applying some algebraic manip-

ulations, we derive the asymptotic expression for κ_2 as

$$\begin{aligned}\kappa_2^{\infty} =&\frac{1}{\ln 2}\int_0^{\infty}\frac{\chi_{\gamma_N}(\gamma_2)}{1+\gamma_2}d\gamma_2\\ =&\frac{1}{2^N\ln 2}\sum_{l=1}^{\tilde{L}_N}u_{N,l}e^{-\frac{\vartheta_{\gamma_{N,l}}}{2\sigma^2}}\sum_{k=0}^{\infty}\frac{\left(\frac{\vartheta_{\gamma_{N,l}}}{2\sigma^2}\right)^k}{k!}\sum_{i=0}^{N+k-1}\frac{\zeta(\overline{\gamma}_N,i)}{i!},\end{aligned}\tag{3.20}$$

where

$$\zeta(\overline{\gamma}_N,i)=E_i\left(\frac{1}{\overline{\gamma}_N}\right)\left(-\frac{1}{2\sigma^2\overline{\gamma}_N}\right)^i+\sum_{q=1}^{i}\binom{i}{q}\left(-\frac{1}{2\sigma^2\overline{\gamma}_N}\right)^{i-q}\sum_{t=0}^{q-1}\frac{(q-1)!}{t!}\left(\frac{1}{2\sigma^2\overline{\gamma}_N}\right)^t.\tag{3.21}$$

Finally, by substituting κ_1^{∞} in (3.18) and κ_2^{∞} in (3.20) into (3.15), the asymptotic ergodic secrecy capacity $\overline{C}_S^{\infty}$ is derived as

$$\begin{aligned}\overline{C}_S^{\infty} =&\log_2\left(2\sigma^2\overline{\gamma}_M\right)+\frac{1}{2^M\ln 2}\sum_{l=1}^{\tilde{L}_M}u_{M,l}e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}}\sum_{k=0}^{\infty}\frac{\psi(M+k)}{k!}\left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}\right)^k\\ &-\frac{1}{2^N\ln 2}\sum_{l=1}^{\tilde{L}_N}u_{N,l}e^{-\frac{\vartheta_{\gamma_{N,l}}}{2\sigma^2}}\sum_{k=0}^{\infty}\frac{\left(\frac{\vartheta_{\gamma_{N,l}}}{2\sigma^2}\right)^k}{k!}\sum_{i=0}^{N+k-1}\frac{1}{i!}\zeta(\overline{\gamma}_N,i).\end{aligned}\tag{3.22}$$

Based on (3.22), we evaluate the high SNR slope and the high SNR power offset, as two key parameters determining the ergodic secrecy capacity in the high SNR regime [141, 144]. Conveniently, we rewrite the asymptotic ergodic secrecy capacity in (3.22) in a general form as

$$\overline{C}_S^{\infty}=S_{\infty}\left(\log_2(\overline{\gamma}_M)-\mathcal{L}_{\infty}\right),\tag{3.23}$$

where S_{∞} is the high SNR slope in bits/s/Hz/(3 dB) and $\mathcal{L}_{\infty}$ is the high SNR power offset in 3 dB units.

We first express the high SNR slope as

$$S_\infty = \lim_{\overline{\gamma}_M \to \infty} \frac{\overline{C}_S^\infty}{\log_2\left(\overline{\gamma}_M\right)}. \tag{3.24}$$

Substituting (3.22) into (4.24), we obtain

$$S_\infty = 1. \tag{3.25}$$

From (4.25), we conclude that the number of antennas at Bob and Eve have no impact on the high SNR slope.

We next express the high SNR power offset $\mathcal{L}_\infty$ as

$$\mathcal{L}_\infty = \lim_{\overline{\gamma}_M \to \infty} \left(\log_2\left(\overline{\gamma}_M\right) - \frac{\overline{C}_S^\infty}{S_\infty} \right). \tag{3.26}$$

It is clear from (4.26) that the effects of the main channel and the eavesdropper's channel on the asymptotic ergodic secrecy capacity reside in $\mathcal{L}_\infty$. Substituting (3.22) and (4.25) into (4.26), we derive $\mathcal{L}_\infty$ as

$$\mathcal{L}_\infty = \mathcal{L}_\infty^M + \mathcal{L}_\infty^N, \tag{3.27}$$

where

$$\mathcal{L}_\infty^M = -\log_2\left(2\sigma^2\right) - \frac{1}{2^M \ln 2} \sum_{l=1}^{\tilde{L}_M} u_{M,l} e^{-\frac{\vartheta \gamma_{M,l}}{2\sigma^2}} \sum_{k=0}^{\infty} \frac{\psi\left(M+k\right)}{k!} \left(\frac{\vartheta \gamma_{M,l}}{2\sigma^2} \right)^k \tag{3.28}$$

and

$$\mathcal{L}_\infty^N = \kappa_2^\infty. \tag{3.29}$$

Based on (4.27), (3.28), and (3.29), we conclude that the contribution of the main channel to $\mathcal{L}_\infty$ is characterized by $\mathcal{L}_\infty^M$ and the contribution of the eavesdropper's channel to $\mathcal{L}_\infty$ is characterized by $\mathcal{L}_\infty^N$. We highlight that $\mathcal{L}_\infty^M$ assesses the benefits of M on the ergodic

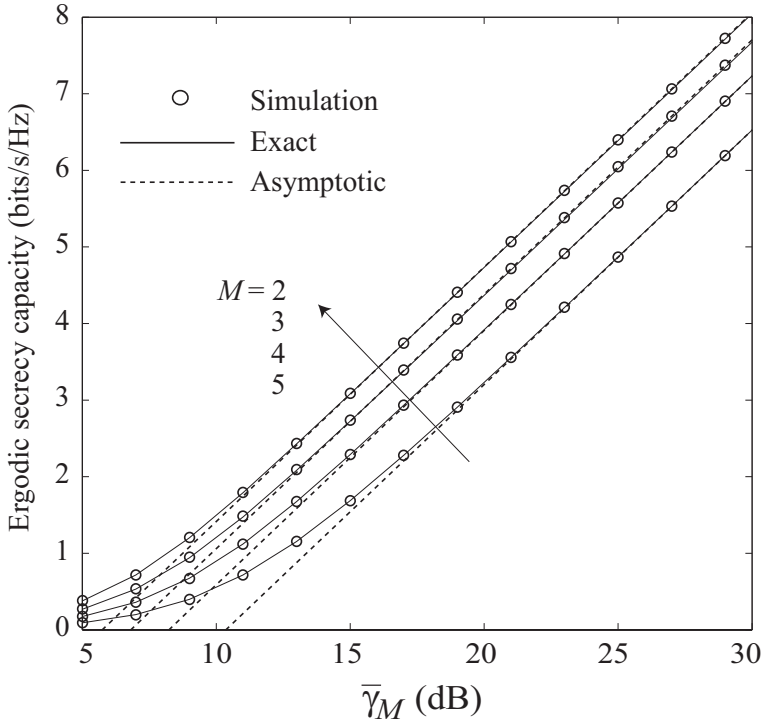

Figure 3.2: Ergodic secrecy capacity versus $\overline{\gamma}_M$ with $\overline{\gamma}_N = 10$ dB and $N = 2$.

secrecy capacity. Specifically, $\mathcal{L}_\infty^M$ decreases as M increases, and as such the ergodic secrecy capacity increases. On the other hand, $\mathcal{L}_\infty^N$ quantifies the loss of ergodic secrecy capacity due to eavesdropping. Specifically, $\mathcal{L}_\infty^N$ increases with N, and as such the ergodic secrecy capacity decreases.

3.3.3 Numerical Examples

Figure 3.2 depicts the ergodic secrecy capacity versus $\overline{\gamma}_M$ for different M in TWDP fading channels. We set $K = 3$ dB and $\Delta = 1$. The exact and asymptotic ergodic capacity results are obtained from (3.13) and (3.22), respectively. Evidently, the exact curves match precisely with Monte Carlo simulations and the asymptotic curves well approximate the exact ones in the high SNR regime. We first see that the curves for different M have the same secrecy capacity slope, which is indicated by (4.25). We also see that the ergodic secrecy capacity increases with increasing M. This can be explained

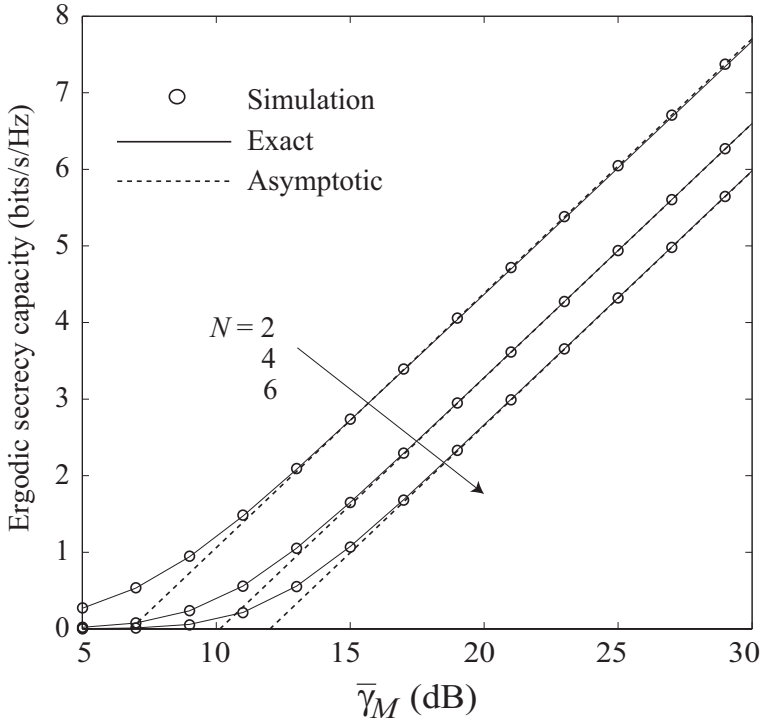

Figure 3.3: Ergodic secrecy capacity versus $\overline{\gamma}_M$ with $\overline{\gamma}_N = 10$ dB and $M = 4$.

by the fact that increasing M brings about additional power gains via MRC. It follows that $\mathcal{L}_\infty^M$ in (3.28) decreases with increasing M and accordingly the high SNR power offset $\mathcal{L}_\infty$ decreases.

Figure 3.3 depicts the ergodic secrecy capacity versus $\overline{\gamma}_M$ for different N in TWDP fading channels. We set $K = 3$ dB and $\Delta = 1$. We see that the ergodic secrecy capacity decreases with increasing N. This is due to the fact that $\mathcal{L}_\infty^N$ in (3.29) increases with increasing N and accordingly the high SNR power offset $\mathcal{L}_\infty$ increases.

Figure 3.4 depicts the high SNR power offset for different M and N in TWDP fading channels. We set $K = 3$ dB and $\Delta = 1$. We first see that for fixed $N = 2$, increasing M decreases $\mathcal{L}_\infty$, which increases the ergodic secrecy capacity. We also see that for fixed $M = 2$, increasing N increases $\mathcal{L}_\infty$, which decreases the ergodic secrecy capacity.

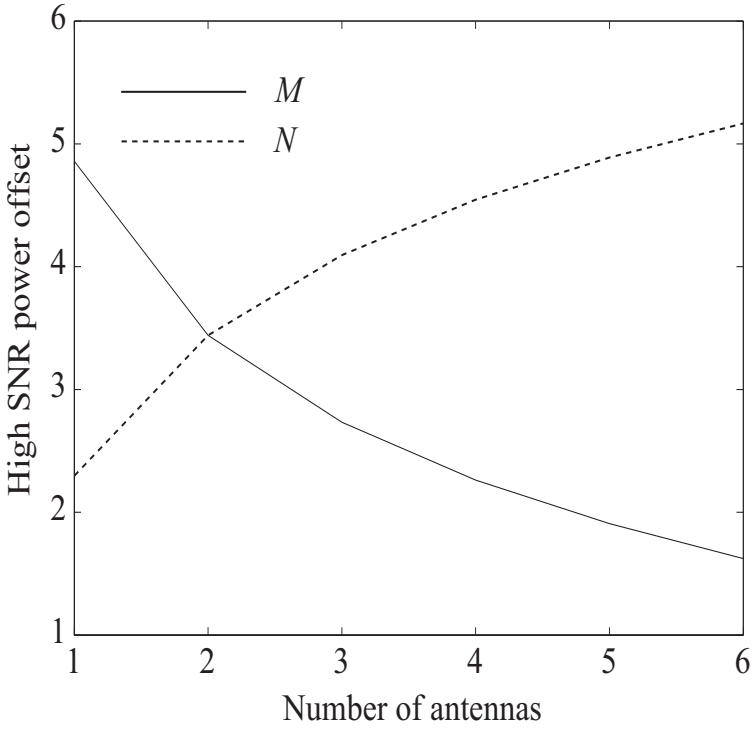

Figure 3.4: Solid line shows the high SNR power offset versus M with $\overline{\gamma}_N = 10$ dB and $N = 2$. Dash line shows the high SNR power offset versus N with $\overline{\gamma}_N = 10$ dB and $M = 2$.

3.3.4 Special Cases

We next present results for the special cases of Rayleigh fading and Rician fading. Observing (4.24), we confirm that the high SNR slope, S_∞, is constant unity for Rayleigh and Rician fading. As such, we provide simplified expressions for $\mathcal{L}_\infty^M$ and $\mathcal{L}_\infty^N$ in the following two remarks.

Remark 1: For Rayleigh fading, $\mathcal{L}_\infty^M$ in (3.28) reduces to

$$\mathcal{L}_\infty^M = -\psi\left(M\right)\log_2 e \tag{3.30}$$

and $\mathcal{L}_{\infty}^{N}$ in (3.29) reduces to

$$\mathcal{L}_{\infty}^{N} = \frac{1}{\ln 2} \sum_{i=0}^{N-1} \frac{1}{i!} \zeta\left(\overline{\gamma}_N, i\right). \tag{3.31}$$

In (3.30), $\psi(M)$ can be expressed as $\psi(M) = -C + \sum_{k=1}^{M-1} \frac{1}{k}$ [140, eq. (8.365.4)], where C is the Euler's constant [140, eq. (8.367.1)]. We confirm that $\psi(M)$ is an increasing function of M. As such, an increase in M decreases $\mathcal{L}_{\infty}^{M}$ and thus improves the ergodic secrecy capacity. We also confirm that an increase in N increases $\mathcal{L}_{\infty}^{N}$ and thus degrades the ergodic secrecy capacity. Furthermore, we note that when the eavesdropper is in absence, we have $\mathcal{L}_{\infty}^{N} = 0$ and $\mathcal{L}_{\infty} = \mathcal{L}_{\infty}^{M}$. In this case, $\mathcal{L}_{\infty}^{M}$ in (3.30) reduces to the high SNR power offset of the SIMO Rayleigh fading channel, equivalent to [141, eq. (15)] with a single transmit antenna.

Remark 2: For Rician fading, K is the Rician K-factor and $2\sigma^2 = \frac{1}{K+1}$. In this case, $\mathcal{L}_{\infty}^{M}$ in (3.28) reduces to

$$\mathcal{L}_{\infty}^{M} = -\log_2\left(\frac{1}{1+K}\right) - \frac{e^{-MK}}{\ln 2} \sum_{k=0}^{\infty} \frac{(MK)^k}{k!} \psi(M+k) \tag{3.32}$$

and $\mathcal{L}_{\infty}^{N}$ in (3.29) reduces to

$$\mathcal{L}_{\infty}^{N} = \frac{1}{\ln 2} e^{-NK} \sum_{k=0}^{\infty} \frac{(NK)^k}{k!} \sum_{i=0}^{N+k-1} \frac{1}{i!} \zeta\left(\overline{\gamma}_N, i\right). \tag{3.33}$$

Taking the derivative of $\mathcal{L}_{\infty}^{N}$ with respect to K, we confirm that $\frac{d\mathcal{L}_{\infty}^{N}}{dK} \geq 0$. This indicates that $\mathcal{L}_{\infty}^{N}$ is an increasing function of K. As such, when the Rician K-factor of the eavesdropper's channel increases, the high SNR power offset increases and the ergodic secrecy capacity decreases.

3.4 Secrecy Outage Probability in Passive Eavesdropping Scenario

In this section, we focus on passive eavesdropping where Alice transmits confidential information at a constant secrecy rate. Perfect secrecy is only guaranteed when the secrecy rate is lower than the instantaneous secrecy capacity, otherwise, perfect secrecy is compromised. In such a scenario, secrecy outage probability is a useful security metric to characterize the probability that perfect secrecy is compromised [35]. Motivated by this, we derive new exact and asymptotic closed-form expressions for secrecy outage probability. Based on the asymptotic expression, we examine two key performance parameters governing secrecy outage probability in the high SNR regime, namely *secrecy diversity order* and *secrecy array gain*. We further derive the probability of non-zero secrecy capacity. This essentially represents the probability of existence of positive secrecy. These new closed-form results encompass Rayleigh fading and Rician fading as special cases.

3.4.1 Exact Secrecy Outage Probability

We first concentrate on the secrecy outage probability. Given the expected secrecy rate R_S, secrecy outage is declared when the instantaneous secrecy capacity C_S drops below R_S. As such, the secrecy outage probability is given by

$$\begin{aligned} P_{out}\left(R_S\right) &= \Pr\left(C_S < R_S\right) \\ &= \int_0^\infty f_{\gamma_N}\left(\gamma_2\right) F_{\gamma_M}\left(2^{R_S}\left(1+\gamma_2\right)-1\right) d\gamma_2. \end{aligned} \tag{3.34}$$

$$
\begin{aligned}
P_{out}\left(R_S\right) =& 1-\frac{e^{-\frac{2^{R_S}-1}{2\sigma^2\overline{\gamma}_M}}}{2^{M+N}}\sum_{l=1}^{\tilde{L}_M}\sum_{k=0}^{\infty}\left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}\right)^k\frac{u_{M,l}e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}}}{k!}\sum_{i=0}^{M+k-1}\frac{1}{i!}\\
&\times\sum_{l_1=1}^{\tilde{L}_N}\sum_{k_1=0}^{\infty}\left(\frac{\vartheta_{\gamma_{N,l_1}}}{2\sigma^2}\right)^{k_1}\frac{u_{N,l_1}e^{-\frac{\vartheta_{\gamma_{N,l_1}}}{2\sigma^2}}}{k_1!\left(N+k_1-1\right)!}\times\sum_{j=0}^{i}\binom{i}{j}\left(\frac{2^{R_S}-1}{2\sigma^2}\right)^{i-j}\\
&\times\frac{2^{R_S j}\overline{\gamma}_M^{N+k_1+j-i}\overline{\gamma}_N^{j}\left(N+k_1+j-1\right)!}{\left(2^{R_S}\overline{\gamma}_N+\overline{\gamma}_M\right)^{N+k_1+j}}.
\end{aligned}
\tag{3.36}
$$

Substituting (3.5) and (3.6) into (3.34), we re-express the secrecy outage probability as

$$
\begin{aligned}
P_{out}\left(R_S\right) =& 1-\frac{1}{2^{M+N}\overline{\gamma}_N}\sum_{l=1}^{\tilde{L}_M}\sum_{k=0}^{\infty}\left(\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}\right)^k\frac{u_{M,l}e^{-\frac{\vartheta_{\gamma_{M,l}}}{2\sigma^2}}}{k!}\\
&\times\sum_{i=0}^{M+k-1}\frac{1}{i!}\sum_{l_1=1}^{\tilde{L}_N}\frac{1}{2\sigma^2}\sum_{k_1=0}^{\infty}\left(\frac{\vartheta_{\gamma_{N,l_1}}}{2\sigma^2}\right)^{k_1}\frac{u_{N,l_1}e^{-\frac{\vartheta_{\gamma_{N,l_1}}}{2\sigma^2}}}{k_1!\left(N+k_1-1\right)!}\\
&\times\int_0^{\infty}e^{-\frac{\gamma_2}{2\sigma^2\overline{\gamma}_N}}\left(\frac{\gamma_2}{2\sigma^2\overline{\gamma}_N}\right)^{N+k_1-1}e^{-\frac{2^{R_S}\left(1+\gamma_2\right)-1}{2\sigma^2\overline{\gamma}_M}}\left(\frac{2^{R_S}\left(1+\gamma_2\right)-1}{2\sigma^2\overline{\gamma}_M}\right)^{i}d\gamma_2.
\end{aligned}
\tag{3.35}
$$

Applying the binomial expansion [140, eq. (1.111)] and [140, eq. (3.351.3)] to solve the integral in (3.35), we derive the exact secrecy outage probability as (3.36). This exact expression is derived in closed-form. It consists of finite summations of exponential functions and power functions.

3.4.2 Asymptotic Secrecy Outage Probability

We now derive the asymptotic secrecy outage probability as $\overline{\gamma}_M \to \infty$. This expression allows us to examine the secrecy performance in the high SNR regime via two parameters, namely the secrecy diversity order and the secrecy array gain. Substituting (3.14) into (3.34) and performing algebraic manipulations, the asymptotic secrecy outage probability is derived as

$$
P_{out}^{\infty}\left(R_S\right) = \left(G_a\overline{\gamma}_M\right)^{-G_d} + o\left(\overline{\gamma}_M^{-G_d}\right),
\tag{3.37}
$$

where the secrecy diversity order is given by

$$G_d = M \tag{3.38}$$

and the secrecy array gain is given by

$$\begin{aligned} G_a = \Bigg[& \frac{1}{2^{M+N} M!} \sum_{l=1}^{\tilde{L}_M} u_{M,l} e^{-\frac{\vartheta \gamma_{M,l}}{2\sigma^2}} \sum_{l_1=1}^{\tilde{L}_N} u_{N,l_1} e^{-\frac{\vartheta \gamma_{N,l_1}}{2\sigma^2}} \\ & \times \sum_{k=0}^{\infty} \left(\frac{\vartheta \gamma_{N,l_1}}{2\sigma^2} \right)^k \frac{1}{k!\,(N+k-1)!} \sum_{i=0}^{M} \binom{M}{i} \left(2^{R_S} \overline{\gamma}_N\right)^i \\ & \times \left(\frac{2^{R_S}-1}{2\sigma^2} \right)^{M-i} (N+k-1+i)! \Bigg]^{-\frac{1}{M}}. \end{aligned} \tag{3.39}$$

It is evident from (3.38) that the secrecy diversity order is solely dependent on M and is independent of N. Hence, the secrecy diversity order increases with the number of antennas at Bob. It is also evident from (3.39) that the eavesdropper's channel exerts a negative effect on the secrecy array gain. As such, increasing the number of antennas at Eve decreases the secrecy array gain and thus degrades the secrecy outage probability.

3.4.3 Probability of Non-Zero Secrecy Capacity

According to (3.1), the non-zero secrecy capacity is achieved when $\gamma_M > \gamma_N$. As such, the probability of non-zero secrecy capacity is given by

$$\begin{aligned} \Pr\left(C_S > 0\right) &= \Pr\left(\gamma_M > \gamma_N\right) \\ &= \int_0^{\infty} f_{\gamma_M}\left(\gamma_1\right) F_{\gamma_N}\left(\gamma_1\right) d\gamma_1. \end{aligned} \tag{3.40}$$

Substituting (3.4) and (3.7) into (3.40) yields

$$\Pr\left(C_S>0\right)=1-\frac{1}{2^{M+N}\overline{\gamma}_M}\sum_{l=1}^{\tilde{L}_N}u_{N,l}e^{-\frac{\vartheta\gamma_{N,l}}{2\sigma^2}}\sum_{k=0}^{\infty}\frac{\left(\frac{\vartheta\gamma_{N,l}}{2\sigma^2}\right)^k}{k!}$$
$$\times\sum_{i=0}^{N+k-1}\sum_{l_1=1}^{\tilde{L}_M}u_{M,l_1}e^{-\frac{\vartheta\gamma_{M,l_1}}{2\sigma^2}}\sum_{k_1=0}^{\infty}\frac{\left(\frac{\vartheta\gamma_{M,l_1}}{2\sigma^2}\right)^{k_1}}{k_1!2\sigma^2\left(M+k_1-1\right)!i!}$$
$$\times\int_0^{\infty}\left(\frac{\gamma_M}{2\sigma^2\overline{\gamma}_M}\right)^{M+k_1-1}\left(\frac{\gamma_M}{2\sigma^2\overline{\gamma}_N}\right)^{i}e^{-\frac{\gamma_M}{2\sigma^2}\left(\frac{1}{\overline{\gamma}_M}+\frac{1}{\overline{\gamma}_N}\right)}d\gamma_M. \tag{3.41}$$

Employing [140, eq. (3.351.3)] to solve the integral in (3.41), we derive the probability of non-zero secrecy capacity as

$$\Pr\left(C_S>0\right)=1-\frac{1}{2^{M+N}}\sum_{l=1}^{\tilde{L}_N}\sum_{k=0}^{\infty}\left(\frac{\vartheta_{\gamma_{N,l}}}{2\sigma^2}\right)^k\frac{u_{N,l}e^{-\frac{\vartheta\gamma_{N,l}}{2\sigma^2}}}{k!}\sum_{l_1=1}^{\tilde{L}_M}\sum_{k_1=0}^{\infty}\sum_{i=0}^{N+k-1}\binom{M+k_1-1+i}{i}$$
$$\times\left(\frac{\vartheta_{\gamma_{M,l_1}}}{2\sigma^2}\right)^{k_1}\frac{u_{M,l_1}e^{-\frac{\vartheta\gamma_{M,l_1}}{2\sigma^2}}\overline{\gamma}_M{}^i\overline{\gamma}_N{}^{M+k_1}}{k_1!(\overline{\gamma}_M+\overline{\gamma}_N)^{M+k_1+i}}. \tag{3.42}$$

For the special case of Rayleigh fading where no specular waves exist in the main channel and eavesdropper's channel, (3.42) reduces to [36, eq. (3)]. This highlights the validity and generality of our result.

3.4.4 Numerical Examples

Figure 3.5 depicts the secrecy outage probability versus $\overline{\gamma}_M$ for different M in TWDP fading channels. We set $R_S = 1$ bit/s/Hz and $K = 3$ dB. The exact and asymptotic secrecy outage probability results are obtained from (3.36) and (3.37), respectively. Precise agreement can be seen between the exact curves and the Monte Carlo simulations. We also see that the asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. We observe that the secrecy outage probability decreases dramatically with increasing M. This can be explained by the fact that M increases the secrecy diversity order.

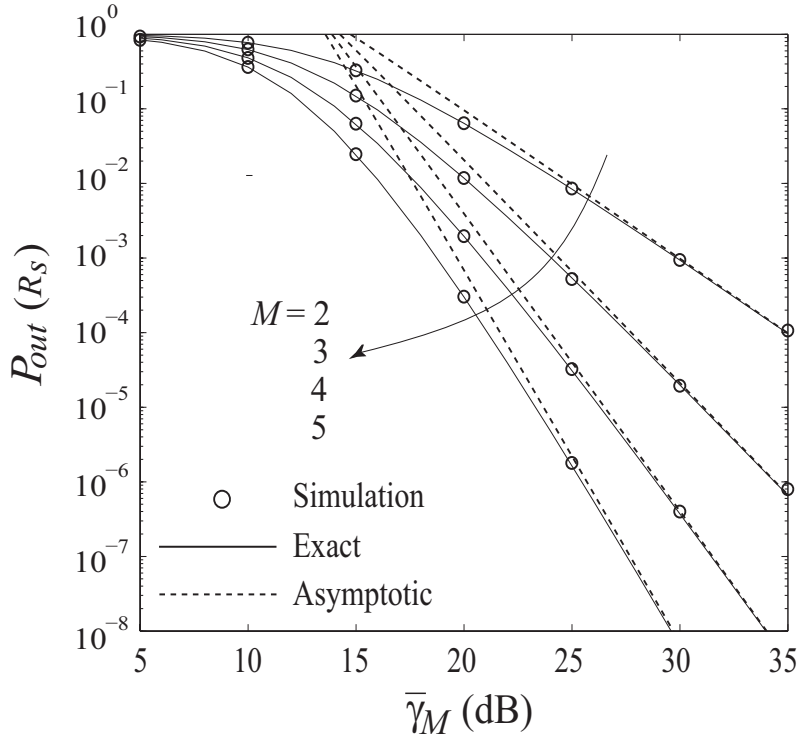

Figure 3.5: Secrecy outage probability versus $\overline{\gamma}_M$ with $\overline{\gamma}_N = 10$ dB, $N = 2$, and $\Delta = 1$.

Figure 3.6 depicts the secrecy outage probability versus $\overline{\gamma}_M$ for different N in TWDP fading channels. We set $R_S = 1$ bit/s/Hz and $K = 3$ dB. We see that the secrecy outage probability curves are parallel in the high SNR regime. This is due to the fact that the secrecy diversity order is independent of N as indicated by (3.38). We also see that the secrecy outage probability increases with N. This is explained by the fact that the secrecy array gain decreases with increasing N as indicated by (3.39).

3.4.5 Special Cases

We next examine results for the special cases of Rayleigh fading and Rician fading. Based on (3.38), we confirm that the secrecy diversity order is maintained at M for Rayleigh and Rician fading. We then offer the following two remarks to present simplified expressions for the exact secrecy outage probability and the secrecy array gain.

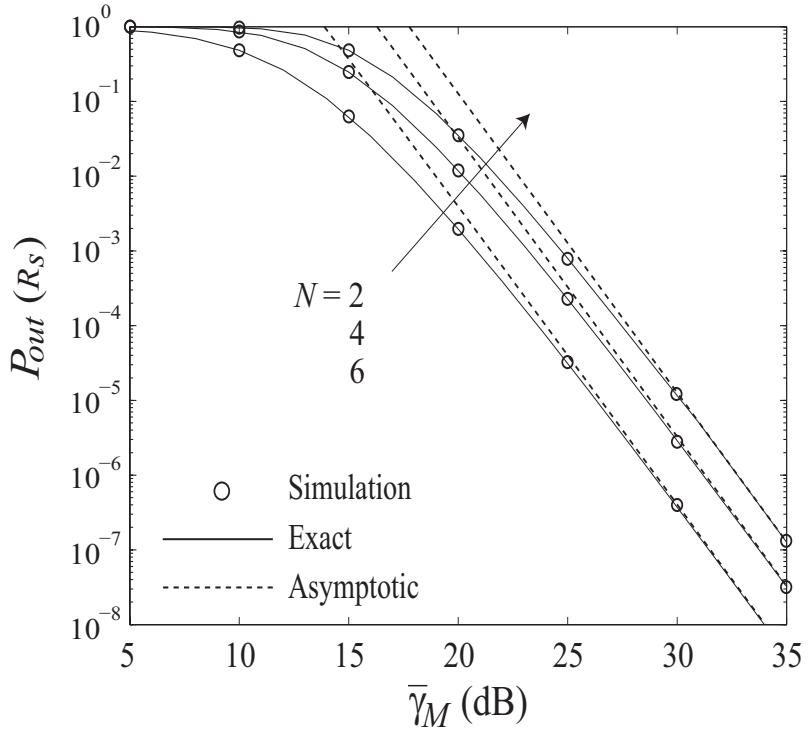

Figure 3.6: Secrecy outage probability versus $\overline{\gamma}_M$ with $\overline{\gamma}_N = 10$ dB, $M = 4$, and $\Delta = 1$.

Remark 1: For Rayleigh fading, the exact secrecy outage probability in (3.36) reduces to

$$P_{out}(R_S) = 1 - \frac{e^{-\frac{2^{R_S}-1}{\overline{\gamma}_M}}}{(N-1)!} \sum_{i=0}^{M-1} \sum_{j=0}^{i} \binom{i}{j} \left(2^{R_S}-1\right)^{i-j} \frac{2^{R_S j} \overline{\gamma}_M^{N+j-i} \overline{\gamma}_N^{j} (N+j-1)!}{i! (2^{R_S}\overline{\gamma}_N + \overline{\gamma}_M)^{N+j}}. \quad (3.43)$$

The secrecy array gain in (3.35) reduces to

$$G_a = \left[\sum_{i=0}^{M} \binom{M}{i} \frac{2^{R_S i} \left(2^{R_S}-1\right)^{M-i} \overline{\gamma}_N^{i} \Gamma(N+i)}{M! \Gamma(N)} \right]^{-\frac{1}{M}}. \quad (3.44)$$

Combining the first two terms of [36, eq. (6)], we find that the exact secrecy outage probability in [36] can be simplified as (3.43). From (3.44), we see that the secrecy array gain decreases with increasing N and $\overline{\gamma}_N$.

Remark 2: For Rician fading, the exact secrecy outage probability in (3.36) reduces

to

$$\begin{aligned} P_{out}\left(R_S\right) =& 1-e^{-\frac{2^{R_S}-1}{2\sigma^2\overline{\gamma}_M}-NK}\sum_{k=0}^{\infty}\frac{(MK)^k e^{-MK}}{k!}\sum_{i=0}^{M+k-1} \\ &\times\sum_{k_1=0}^{\infty}\frac{(NK)^{k_1}}{i!k_1!\left(N+k_1-1\right)!}\sum_{j=0}^{i}\binom{i}{j}\left(\frac{2^{R_S}-1}{2\sigma^2}\right)^{i-j} \\ &\times\frac{2^{R_S j}\overline{\gamma}_M^{N+k_1+j-i}\overline{\gamma}_N^{j}\left(N+k_1+j-1\right)!}{\left(2^{R_S}\overline{\gamma}_N+\overline{\gamma}_M\right)^{N+k_1+j}}. \end{aligned} \tag{3.45}$$

The secrecy array gain in (3.35) reduces to

$$\begin{aligned} G_a =& \left[\frac{e^{-(M+N)K}}{M!}\sum_{k=0}^{\infty}\frac{(NK)^k}{k!\left(N+k-1\right)!}\sum_{i=0}^{M}\binom{M}{i}2^{R_S i}\right. \\ &\left.\times\left(\left(2^{R_S}-1\right)(K+1)\right)^{M-i}\Gamma\left(N+k+i\right)\overline{\gamma}_N^{i}\right]^{-\frac{1}{M}}. \end{aligned} \tag{3.46}$$

Taking the derivative of G_a with respect to K, we confirm that $\frac{dG_a}{dK} > 0$, which indicates that G_a is an increasing function of the Rician K-factor. Thus, we confirm that the secrecy array gain increases with K.

3.4.6 Performance Gap

In this subsection, we evaluate the performance loss when the number of antennas at Eve increases from N to $N+1$. As indicated by (3.38) and (3.39), increasing the number of antennas at Eve only impacts the secrecy array gain. As such, we derive the SNR gap between N and $N+1$ antennas as a simple ratio of their respective secrecy array gains.

Motivated by this, we define the SNR gap between N and $N+1$ antennas as

$$\left.\frac{G_a\left(N+1\right)}{G_a\left(N\right)}\right|_{\mathrm{dB}} = 10\log_{10}\left(\frac{G_a\left(N+1\right)}{G_a\left(N\right)}\right). \tag{3.47}$$

For TWDP fading channels, the SNR gap between N and $N+1$ antennas is calculated using (3.39) together with (3.47). For the special cases of Rayleigh fading and Rician fading, we proceed to provide some useful insights in the following remarks.

Remark 3: For Rayleigh fading, based on (3.44) and (3.47), the SNR gap between N and $N+1$ antennas is characterized as

$$\left.\frac{G_a\left(N+1\right)}{G_a\left(N\right)}\right|_{\mathrm{dB}} = -\frac{10}{M}\log_{10}\left(1+\varpi\right), \tag{3.48}$$

where ϖ is given by

$$\varpi = \frac{\sum_{i=0}^{M}\binom{M}{i} i\left(2^{R_S}-1\right)^{M-i} 2^{R_S i}\Gamma\left(N+i\right)\overline{\gamma}_N^i}{N\sum_{i=0}^{M}\binom{M}{i}\left(2^{R_S}-1\right)^{M-i} 2^{R_S i}\Gamma\left(N+i\right)\overline{\gamma}_N^i}. \tag{3.49}$$

From (3.48), increasing N to $N+1$ antennas results in an SNR loss of $\frac{10}{M}\log_{10}\left(1+\varpi\right)$ dB.

Remark 4: For Rician fading, based on (3.46) and (3.47), the SNR gap between N and $N+1$ antennas is characterized as

$$\left.\frac{G_a\left(N+1\right)}{G_a\left(N\right)}\right|_{\mathrm{dB}} = \frac{10K}{M}\log_{10}e - \frac{10}{M}\log_{10}\left(1+\frac{\varpi_1}{\varpi_2}\right), \tag{3.50}$$

where

$$\begin{aligned}\varpi_1 = &\sum_{k=0}^{\infty}\sum_{j=0}^{k-1}\binom{k}{j}\frac{N^j K^k}{k!\left(N+k\right)!}\sum_{i=0}^{M}\binom{M}{i}\left(2^{R_S}-1\right)^{M-i}\left(K+1\right)^{M-i}2^{R_S i}\left(N+k+i\right)!\overline{\gamma}_N^i \\ &+\sum_{k=0}^{\infty}\frac{\left(NK\right)^k}{k!\left(N+k\right)!}\sum_{i=0}^{M}\binom{M}{i} i\left(2^{R_S}-1\right)^{M-i}\left(K+1\right)^{M-i}2^{R_S i}\left(N+k-1+i\right)!\overline{\gamma}_N^i\end{aligned} \tag{3.51}$$

and

$$\varpi_2 = \sum_{k=0}^{\infty}\frac{\left(NK\right)^k}{k!\left(N+k-1\right)!}\sum_{i=0}^{M}\binom{M}{i}\left(2^{R_S}-1\right)^{M-i}\left(K+1\right)^{M-i}2^{R_S i}\left(N+k-1+i\right)!\overline{\gamma}_N^i. \tag{3.52}$$

From (3.50), increasing N to $N+1$ antennas results in an SNR loss of $\frac{10}{M}\log_{10}\left(1+\frac{\varpi_1}{\varpi_2}\right)-\frac{10K}{M}\log_{10}e$ dB. For the special case of non-line-of-sight with $K=0$, (3.50) reduces to (3.48).

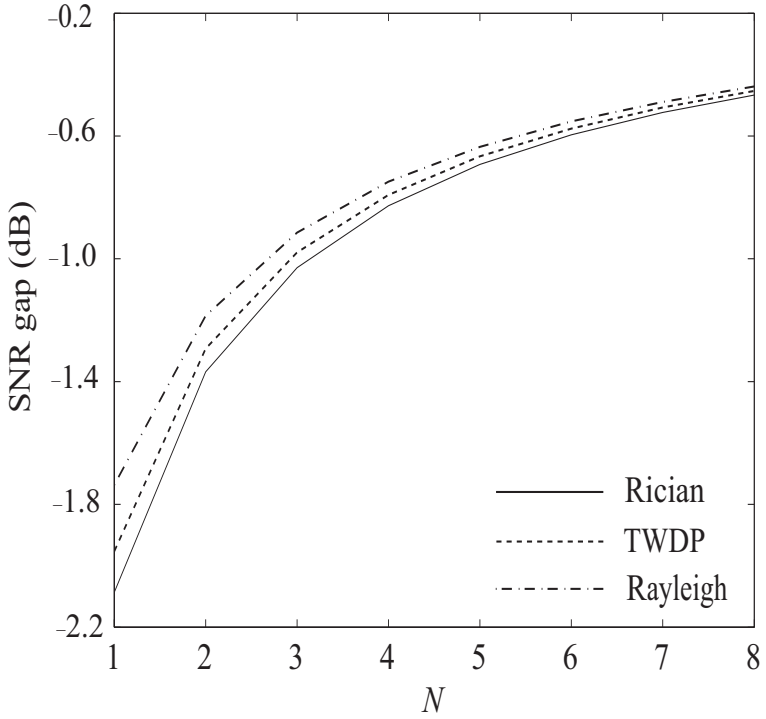

Figure 3.7: SNR gap versus N with $\overline{\gamma}_N = 10$ dB and $M = 4$ in three different fading scenarios.

Figure 3.7 depicts the SNR gap between N and $N + 1$ antennas for three different fading scenarios: 1) TWDP fading with $K = 3$ dB and $\Delta = 1$, 2) Rician fading with $K = 3$ dB and $\Delta = 0$, and 3) Rayleigh fading. We set $R_S = 1$ bit/s/Hz. We see that the SNR gap diminishes with increasing N. We also see that the SNR gap for all three fading scenarios approach each other for large N.

3.5 Conclusions

Physical layer security of MRC systems in TWDP fading channels was analyzed. Two practical scenarios were taken into account, depending on whether or not the CSI of the eavesdropper is known at the transmitter. For the first scenario where Eve's CSI is not known, new expressions for the exact and asymptotic average secrecy capacity were derived. Based on these, it has been demonstrated that the high SNR slope is one. The

joint impacts of the main channel and the eavesdropper's channel on the average secrecy capacity via the high SNR power offset were characterized. For the second scenario where Eve's CSI is known, new expressions for the exact and asymptotic secrecy outage probability were derived. Based on these, it is shown that the secrecy diversity order is solely dependent on the number of receive antennas at the legitimate receiver and independent of the number of antennas at the eavesdropper. We further examined the performance loss by presenting the SNR gap between N and $N+1$ antennas. Based on the SNR gap, the loss of secrecy array gain with increasing number of antennas at the eavesdropper is accurately quantified.

Chapter 4

Secure Transmission with Antenna Selection in MIMO Nakagami-m Fading Channels

4.1 Introduction

In this chapter, transmit antenna selection (TAS) with GSC (TAS/GSC) for secure transmissions in MIMO wiretap channels is proposed. The proposed protocol combines the advantages of TAS and GSC in multiple antenna transmissions. Two eavesdropping scenarios are addressed: 1) Passive eavesdropping and 2) active eavesdropping. For passive eavesdropping, the secrecy outage probability is characterized as the fundamental security metric. For active eavesdropping, the average secrecy rate is characterized as the fundamental security metric. New asymptotic expressions for the average secrecy rate and secrecy outage probability in the high SNR regime are derived for two important cases: 1) The legitimate receiver is located close to the transmitter, and 2) the legitimate receiver and the eavesdropper are located close to the transmitter.

Notation: In this chapter, $(\cdot)^T$ denotes the transpose operator, $\mathbf{I}_M$ denotes the $M \times M$ identity matrix, $\mathbf{0}_{M\times N}$ denotes the $M \times N$ zero matrix, $\mathbb{E}[\cdot]$ denotes the expectation operator, $F_\varphi(\cdot)$ denotes the CDF of random variable (RV) φ, $f_\varphi(\cdot)$ denotes the PDF of φ, $\mathrm{sgn}(\cdot)$ denotes the signum function, $o(\cdot)$ denotes the higher order terms, and $[x]^+ = \max\{x, 0\}$.

4.2 System Model

A MIMO wiretap channel model which consists of a transmitter (Alice) with N_A antennas, a legitimate receiver (Bob) with N_B antennas, and an eavesdropper (Eve) with N_E antennas is considered. The main channel (Alice-Bob) and the eavesdropper's channel (Alice-Eve) are assumed to undergo quasi-static Nakagami-m fading with fading parameters m_B and m_E, respectively. In the main channel, Alice selects a single transmit antenna among N_A antennas that maximizes the GSC output SNR at Bob, while Bob combines the L_B ($1 \le L_B \le N_B$) strongest receive antennas. In the eavesdropper's channel, Eve combines the L_E ($1 \le L_E \le N_E$) strongest receive antennas. The channel power gain from the pth transmit antenna to the l_Bth receive antenna at Bob is denoted as $|h_{p,l_B}|^2$ with $\mathbb{E}\left[|h_{p,l_B}|^2\right] = \Omega_1$, $p = 1,\cdots,N_A$, $l_B = 1,\cdots,N_B$. The channel power gain from the pth transmit antenna to the l_Eth receive antenna at Eve is denoted as $|g_{p,l_E}|^2$ with $\mathbb{E}\left[|g_{p,l_E}|^2\right] = \Omega_2$, $l_E = 1,\cdots,N_E$. Based on GSC, we arrange $\left\{|h_{p,(l_B)}|^2, 1 \le l_B \le N_B\right\}$ in descending order as $|h_{p,(1)}|^2 \ge |h_{p,(2)}|^2 \ge \cdots \ge |h_{p,(N_B)}|^2$, and $\left\{|g_{p,(l_E)}|^2, 1 \le l_E \le N_E\right\}$ in descending order as $|g_{p,(1)}|^2 \ge |g_{p,(2)}|^2 \ge \cdots \ge |g_{p,(N_E)}|^2$. The index of the optimal transmit antenna is determined as

$$p^* = \underset{1\le p\le N_A}{\arg\max} \left\{ \sum_{l_B=1}^{L_B} |h_{p,(l_B)}|^2 \right\}. \tag{4.1}$$

Secure transmission is achieved by encoding the confidential message block W into a codeword $\mathbf{x} = [x(1), \cdots, x(l), \cdots, x(L)]$, where L is the length of $\mathbf{x}$. The codeword

is subject to an average power constraint $\frac{1}{L}\sum_{l=1}^{L}\mathbb{E}\left[\left|x\left(l\right)\right|^2\right] \leq P$. In the main channel, at time slot l, the received signal vector is given by $\mathbf{y}_B\left(l\right) = \mathbf{h}x\left(l\right) + \mathbf{n}_B\left(l\right)$, where $\mathbf{h} = \left[h_{p^*,1}, h_{p^*,2}, \cdots, h_{p^*,N_B}\right]^T \in \mathcal{C}^{N_B \times 1}$ is the main channel vector between transmit antenna p^* at Alice and the N_B receive antennas at Bob, and $\mathbf{n}_B\left(l\right) \sim \mathcal{CN}_{N_B \times 1}\left(\mathbf{0}_{N_B \times 1}, \delta_B^2 \mathbf{I}_{N_B}\right)$ is the additive white Gaussian noise (AWGN) vector at Bob. We denote $\bar{\gamma}_B = \Omega_1 \frac{P}{\delta_B^2}$ as the average SNR per antenna at Bob. Combining the subset of receive antennas with the largest SNRs at Bob results in the instantaneous SNR in the main channel as

$$\gamma_B = \sum_{l_B=1}^{L_B} \gamma_{(l_B)}^B, \tag{4.2}$$

where $\gamma_{(l_B)}^B = \left|h_{p^*,(l_B)}\right|^2 \frac{P}{\delta_B^2}$. In the eavesdropper's channel, at time slot l, the received signal vector is given by $\mathbf{y}_E\left(l\right) = \mathbf{g}x\left(l\right) + \mathbf{n}_E\left(l\right)$, where $\mathbf{g} = \left[g_{p^*,1}, g_{p^*,2}, \cdots, g_{p^*,N_E}\right]^T \in \mathcal{C}^{N_E \times 1}$ is the eavesdropper's channel vector between transmit antenna p^* at Alice and the N_E receive antennas at Eve, and $\mathbf{n}_E\left(l\right) \sim \mathcal{CN}_{N_E \times 1}\left(\mathbf{0}_{N_E \times 1}, \delta_E^2 \mathbf{I}_{N_E}\right)$ is the additive white Gaussian noise (AWGN) vector at Eve. We denote $\bar{\gamma}_E = \Omega_2 \frac{P}{\delta_E^2}$ as the average SNR per antenna at Eve. Combining the subset of receive antennas with the largest SNRs at Eve results in the instantaneous SNR in the eavesdropper's channel as

$$\gamma_E = \sum_{l_E=1}^{L_E} \gamma_{(l_E)}, \tag{4.3}$$

where $\gamma_{(l_E)} = \left|g_{p^*,(l_E)}\right|^2 \frac{P}{\delta_E^2}$.

4.3 New Statistical Properties

In this section, we derive new closed-form expressions for the probability density function (PDF) and the cumulative distribution function (CDF) of γ_B in the main channel, and the PDF and the CDF of γ_E in the eavesdropper's channel, which lay the foundation for extracting several key secrecy performance indicators, namely the high SNR slope, the

high SNR power offset, the secrecy diversity order, and the secrecy array gain. These statistics are general in nature and as such are useful for determining the performance of other wireless systems with GSC.

4.3.1 CDF and PDF of the SNR in the Main Channel

Theorem 1: The expressions for the CDF and the PDF of γ_B are derived as

$$F_{\gamma_B}(x) = \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \widetilde{\sum} \hbar_\rho x^{\theta_\rho} e^{-\eta_\rho x}, \tag{4.4}$$

$$f_{\gamma_B}(x) = \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \widetilde{\sum} \hbar_\rho x^{\theta_\rho - 1} e^{-\eta_\rho x}\left(\theta_\rho - \eta_\rho x\right), \tag{4.5}$$

where $\widetilde{\sum} \triangleq \sum_{\mathcal{S}_B}\sum_{\mathcal{S}_B^1}\cdots\sum_{\mathcal{S}_B^k}\cdots\sum_{\mathcal{S}_B^{|\mathcal{S}|}}$, $\mathcal{S}_B = \left\{ \left(n_{\tau,1},\cdots,n_{\tau,|\mathcal{S}|}\right) \middle| \sum_{k=1}^{|S|} n_{\tau,k} = N_A \right\}$, $|\mathcal{S}|$ is the cardinality of set $\mathcal{S}$, and $\mathcal{S}$ denotes a set of $(2m_B+1)$-tuples satisfying the condition

$$\mathcal{S} = \left\{ \left(n_{k,0}^{\Phi}\cdots,n_{k,m_B-1}^{\Phi},n_{k,0}^{F},\cdots,n_{k,m_B}^{F}\right) \middle| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi} = L_B - 1, \sum_{j=0}^{m_B} n_{k,j}^{F} = N_B - L_B \right\},$$

thereby $|\mathcal{S}| = \binom{m_B+L_B-2}{m_B-1}\binom{m_B+N_B-L_B}{m_B}$, $\mathcal{S}_B^k = \left\{ \left(n_{\rho_k,0},\cdots,n_{\rho_k,m_BL_B+b_k^F}\right) \middle| \sum_{n=0}^{m_BL_B+b_k^F} n_{\rho_k,n} = n_{\tau,k} \right\}$, $k = 1,\cdots,|\mathcal{S}|$, and $\hbar_\rho$, θ_ρ, and η_ρ are respectively given by

$$\hbar_\rho = \prod_{k=1}^{|\mathcal{S}|}\left(\left(a_k^{\Phi}a_k^{F}\frac{(n_1-1)!}{(L_B)^{n_1}}\right)^{n_{\tau,k}}\frac{\prod_{n=0}^{m_BL_B+b_k^F}\ell_n^{n_{\rho_k,n}}}{\prod_{n=0}^{m_BL_B+b_k^F} n_{\rho_k,n}!}\right),$$

$$\theta_\rho = \sum_{k=1}^{|\mathcal{S}|}\sum_{n=0}^{m_BL_B+b_k^F}\mu_n n_{\rho_k,n}, \quad \eta_\rho = \sum_{k=1}^{|\mathcal{S}|}\sum_{n=0}^{m_BL_B+b_k^F}\nu_n n_{\rho_k,n},$$

where $n_1 = b_k^{\Phi} + b_k^{F} + m_B$, a_k^{Φ}, a_k^{F}, ℓ_n, b_k^{F}, b_k^{Φ}, μ_n, and ν_n are defined in Appendix A.1.

Proof. The proof is given in Appendix A.1. □

Theorem 2: In the high SNR regime with $\gamma_B \to \infty$, the asymptotic CDF of γ_B is given by

$$F_{\gamma_B}(x) = \frac{\left(L_B\binom{N_B}{L_B}\right)^{N_A}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B N_A} x^{m_B N_B N_A}}{\left((m_B-1)!(m_B!)^{N_B-L_B}(m_B N_B)!\right)^{N_A}} \left(\sum_{\mathcal{S}_B^{\Phi}} a_k^{\Phi} \frac{\left(b_k^{\Phi}+m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^{\Phi}+m_B(N_B-L_B)+m_B}}\right)^{N_A}, \tag{4.6}$$

where $\mathcal{S}_B^{\Phi} = \left\{ \left(n_{k,0}^{\Phi}, \cdots, n_{k,m_B-1}^{\Phi}\right) \middle| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi} = L_B - 1 \right\}$.

Proof. The proof is given in Appendix A.2. □

4.3.2 CDF and PDF of the SNR in the Eavesdropper's Channel

Alice selects the strongest transmit antenna according to the channel power gains of the main channel, which corresponds to selecting a random transmit antenna for Eve. Hence, similar to (A.1.9) given in Appendix A, the expressions for the CDF and the PDF of γ_E are respectively derived as

$$F_{\gamma_E}(x) = \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=0}^{m_E L_E + b_k^F} a_k^{\Phi} a_k^F \frac{\left(b_k^{\Phi}+b_k^F+m_E-1\right)!}{(L_E)^{b_k^{\Phi}+b_k^F+m_E}} \ell_n x^{\mu_n} e^{-\nu_n x}, \tag{4.7}$$

$$f_{\gamma_E}(x) = \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E + b_k^F} a_k^{\Phi} a_k^F \frac{\left(b_k^{\Phi}+b_k^F+m_E-1\right)!}{(L_E)^{b_k^{\Phi}+b_k^F+m_E}} \ell_n x^{\mu_n-1} e^{-\nu_n x}(\mu_n - \nu_n x), \tag{4.8}$$

where $\mathcal{S}_E$ denotes a set of $(2m_E+1)$-tuples satisfying the condition

$$\mathcal{S}_E = \left\{ \left(n_{k,0}^{\Phi}\cdots, n_{k,m_E-1}^{\Phi}, n_{k,0}^F, \cdots, n_{k,m_E}^F\right) \middle| \sum_{i=0}^{m_E-1} n_{k,i}^{\Phi} = L_E - 1, \sum_{j=0}^{m_E} n_{k,j}^F = N_E - L_E \right\}.$$

All the parameters in (4.7) and (4.8) are identical to those in *Theorem 1* and are calculated accordingly.

4.4 Average Secrecy Rate

In this section, we focus on the active eavesdropping scenario[1], where the CSI of the eavesdropper's channel is also known at Alice. Following the wiretap channel in [28, 35], Alice encodes a message block W^k into a codeword X^n, and Eve receives Y_w^n from the output of its channel. The equivocation rate of Eve is $R_e = H\left(W^k \middle| Y_w^n\right)/n$, which is the amount of ignorance that the eavesdropper has about a message W^k [28]. In the active eavesdropping scenario, Alice can adapt the achievable secrecy rate R such that $R \leq R_e$ [28, 35]. Here, We focus on the maximum achievable secrecy rate $C_s = R_e$ [28, 35], which is characterized as [28, 35, 145, 146]

$$C_s = [C_B - C_E]^+, \tag{4.9}$$

where $C_B = \log_2(1+\gamma_B)$ is the capacity of the main channel and $C_E = \log_2(1+\gamma_E)$ is the capacity of the eavesdropper's channel. Since the CSI of eavesdropper's channel is available to Alice, Alice can transmit confidential messages at a rate C_s, to guarantee perfect secrecy.

In active eavesdropping scenario, the average secrecy rate is essentially a fundamental secrecy performance metric. We derive new exact and asymptotic expressions for the average secrecy rate. Based on the asymptotic expressions, we characterize the average secrecy rate in terms of the high SNR slope and the high SNR power offset, to explicitly capture the impact of arbitrary antennas and channel parameters on the average secrecy rate at high SNR [141].

[1] In this scenario, the eavesdropper is active [35]. Such a scenario is particularly applicable in networks combining multicast and unicast transmissions, where the users play dual roles as legitimate receivers for some signals and eavesdroppers for others [44].

4.4.1 Exact Average Secrecy Rate

The average secrecy rate is the average of the secrecy rate C_s over γ_B and γ_E. As such, the exact average secrecy rate is given by

$$\begin{aligned}\bar{C}_s &= \int_0^\infty \int_0^\infty C_s f_{\gamma_B}(x_1) f_{\gamma_E}(x_2) dx_1 dx_2 \\ &= \int_0^\infty \underbrace{\left[\int_0^\infty C_s f_{\gamma_E}(x_2)\, dx_2\right]}_{\omega_1} f_{\gamma_B}(x_1)\, dx_1. \end{aligned} \tag{4.10}$$

We first calculate ω_1 in (4.10) as

$$\omega_1 = \int_0^{x_1} \left(\log_2(1+x_1) - \log_2(1+x_2)\right) f_{\gamma_E}(x_2)\, dx_2. \tag{4.11}$$

Using integration by parts, and applying some algebra, we derive (4.11) as

$$\begin{aligned}\omega_1 &= \log_2(1+x_1) F_{\gamma_E}(x_1) - \left(\log_2(1+x_1) F_{\gamma_E}(x_1) - \frac{1}{\ln 2}\int_0^{x_1} \frac{1}{1+x_2} F_{\gamma_E}(x_2)\, dx_2\right) \\ &= \frac{1}{\ln 2}\int_0^{x_1} \frac{F_{\gamma_E}(x_2)}{1+x_2} dx_2. \end{aligned} \tag{4.12}$$

Substituting (4.12) into (4.10), and changing the order of integration, we obtain

$$\begin{aligned}\bar{C}_s &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(x_2)}{1+x_2}\left[\int_{x_2}^\infty f_{\gamma_B}(x_1)\, dx_1\right] dx_2 \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(x_2)}{1+x_2}\left(1 - F_{\gamma_B}(x_2)\right) dx_2. \end{aligned} \tag{4.13}$$

Using the new statistical properties in Section III, we calculate (4.13) as

$$\begin{aligned}\bar{C}_s =& \frac{L_E}{\ln 2\,(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=0}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}} \ell_n \Bigg[\mu_n! \Psi(\mu_n+1, \mu_n+1; \nu_n) \\ &- \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \widetilde{\sum} \hbar_\rho (\mu_n+\theta_\rho)! \Psi(\mu_n+\theta_\rho+1, \mu_n+\theta_\rho+1; \nu_n+\eta_\rho)\Bigg], \end{aligned} \tag{4.14}$$

where $\Psi(\cdot,\cdot;\cdot)$ is the confluent hypergeometric function [140, eq. (9.211.4)]. Our new expression for the exact average secrecy rate in (4.14) applies to arbitrary numbers of antennas, arbitrary fading parameters, and arbitrary average SNRs.

4.4.2 Asymptotic Average Secrecy Rate

In order to explicitly examine the performance in the high SNR regime, we proceed to derive the asymptotic average secrecy rate. We take into account two realistic scenarios: 1) Bob is located close to Alice, which can be mathematically described as $\bar{\gamma}_B \to \infty$ for arbitrary $\bar{\gamma}_E$, and 2) Bob and Eve are located close to Alice, which can be mathematically described as $\bar{\gamma}_B \to \infty$ and $\bar{\gamma}_E \to \infty$.

To facilitate the analysis, we rewrite the CDF of γ_E as

$$F_{\gamma_E}(x) = 1 + \chi_{\gamma_E}(x), \tag{4.15}$$

where

$$\chi_{\gamma_E}(x) = \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E + b_k^F} a_k^{\Phi} a_k^{F} \frac{\left(b_k^{\Phi}+b_k^{F}+m_E-1\right)!}{(L_E)^{b_k^{\Phi}+b_k^{F}+m_E}} \ell_n x^{\mu_n} e^{-\nu_n x}.$$

4.4.2.1 $\bar{\gamma}_B \to \infty$

In this case, we introduce a new general form to derive the average secrecy rate in the following theorem.

Theorem 3: The asymptotic average secrecy rate is given by

$$\bar{C}_s^{\infty} = \Delta_1 + \Delta_2, \tag{4.16}$$

where

$$\Delta_1 = \frac{1}{\ln 2}\int_0^\infty \ln\left(x_1\right) f_{\gamma_B}\left(x_1\right) dx_1 \tag{4.17}$$

and

$$\Delta_2 = \frac{1}{\ln 2}\int_0^\infty \frac{\chi_{\gamma_E}\left(x_2\right)}{1+x_2} dx_2. \tag{4.18}$$

Proof. The proof is given in Appendix A.3. □

Based on *Theorem 3*, we calculate the asymptotic average secrecy rate using the new statistical properties in Section III. Specifically, by substituting (4.5) into (4.17), and employing [140, eq. (4.352.1)], Δ_1 is derived as

$$\Delta_1 = \log_2\left(\bar{\gamma}_B\right) - \log_2\left(m_B\right) + \frac{1}{\ln 2}\left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \widetilde{\sum} \tilde{\hbar}_\rho \zeta_1, \tag{4.19}$$

where $\tilde{\hbar}_\rho = \hbar_\rho \left(\frac{m_B}{\bar{\gamma}_B}\right)^{-\theta_\rho}$ and

$$\zeta_1 = \begin{cases} 0, & \theta_\rho = 0, \tilde{\eta}_\rho = 0, \\ \ln(\tilde{\eta}_\rho) + C, & \theta_\rho = 0, \tilde{\eta}_\rho > 0, \\ -\frac{(\theta_\rho - 1)!}{(\tilde{\eta}_\rho)^{\theta_\rho}}, & \theta_\rho > 0, \tilde{\eta}_\rho > 0, \end{cases} \tag{4.20}$$

In (4.20), C is the Euler's constant [140, eq. (8.367.1)] and $\tilde{\eta}_\rho = \left(\frac{m_B}{\bar{\gamma}_B}\right)^{-1} \eta_\rho$. It is worth noting that $\tilde{\hbar}_\rho$ and $\tilde{\eta}_\rho$ are independent of $\bar{\gamma}_B$. We should also note that Δ_1 in (4.19) explicitly quantifies the impact of the main channel on the average secrecy rate.

Substituting χ_{γ_E} given in (4.15) into (4.18), we obtain Δ_2

$$\begin{aligned}\Delta_2 =&\frac{L_E}{\ln 2\,(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E+b_k^F} a_k^{\Phi} a_k^F \\ &\times \frac{\left(b_k^{\Phi}+b_k^F+m_E-1\right)!}{(L_E)^{b_k^{\Phi}+b_k^F+m_E}}\ell_n\mu_n!\Psi\left(\mu_n+1,\mu_n+1,\nu_n\right),\end{aligned} \tag{4.21}$$

which explicitly quantifies the impact of the eavesdropper's channel on the average secrecy rate.

Based on (4.16), (4.19), and (4.21), we derive the asymptotic average secrecy rate as

$$\begin{aligned}\bar{C}_s^{\infty} =&\log_2\left(\bar{\gamma}_B\right)-\log_2\left(m_B\right)+\frac{1}{\ln 2}\left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} \\ &\times N_A!\widetilde{\sum}\tilde{\hbar}_{\rho}\zeta_1+\frac{L_E}{\ln 2\,(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E+b_k^F} a_k^{\Phi} \\ &\times a_k^F\frac{\left(b_k^{\Phi}+b_k^F+m_E-1\right)!}{(L_E)^{b_k^{\Phi}+b_k^F+m_E}}\ell_n\mu_n!\Psi\left(\mu_n+1,\mu_n+1,\nu_r\right).\end{aligned} \tag{4.22}$$

Based on (4.22), we derive two key performance indicators that determine the average secrecy rate at high SNR, namely the high SNR slope and the high SNR power offset [141, 147]. The asymptotic average secrecy rate in (4.22) can be conveniently re-expressed as [141]

$$\bar{C}_s^{\infty}=S_{\infty}\left(\log_2\left(\bar{\gamma}_B\right)-\mathcal{L}_{\infty}\right), \tag{4.23}$$

where S_{∞} is the high SNR slope in bits/s/Hz/(3 dB) and $\mathcal{L}_{\infty}$ is the high SNR power offset in 3 dB units. We note that the high SNR slope is also known as the maximum multiplexing gain or the number of degrees of freedom [148]. The high SNR power offset is a more intricate function which depends on the number of transmit and receive antennas, as well as the channel characteristics [141, 147].

The high SNR slope S_∞ is given by

$$S_\infty = \lim_{\bar{\gamma}_B \to \infty} \frac{\bar{C}_S^\infty}{\log_2(\bar{\gamma}_B)}. \tag{4.24}$$

Substituting (4.22) into (4.24), we obtain

$$S_\infty = 1. \tag{4.25}$$

From (4.25), we see that the eavesdropper's channel and the number of Bob's receive antennas have no impact on the high SNR slope S_∞.

The high SNR power offset $\mathcal{L}_\infty$ is given by

$$\mathcal{L}_\infty = \lim_{\bar{\gamma}_B \to \infty} \left(\log_2(\bar{\gamma}_B) - \frac{\bar{C}_S^\infty}{S_\infty} \right). \tag{4.26}$$

Substituting (4.22) and (4.25) into (4.26), we derive $\mathcal{L}_\infty$ as[2]

$$\mathcal{L}_\infty = \mathcal{L}_\infty^B(m_B, N_B, L_B, N_A) + \mathcal{L}_\infty^E(m_E, N_E, L_E, \bar{\gamma}_E), \tag{4.27}$$

where

$$\mathcal{L}_\infty^B(m_B, N_B, L_B, N_A) = \log_2(m_B) - \frac{1}{\ln 2}\left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B} \right)^{N_A} N_A! \widetilde{\sum} \tilde{\hbar}_\rho \zeta_1 \tag{4.28}$$

and

$$\mathcal{L}_\infty^E(m_E, N_E, L_E, \bar{\gamma}_E) = -\Delta_2. \tag{4.29}$$

In (4.28), $\mathcal{L}_\infty^B$ quantifies the contribution of the main channel to the high SNR power offset. In (4.29), $\mathcal{L}_\infty^E$ quantifies the contribution of the eavesdropper's channel to the high SNR power offset. We next examine special cases of $\mathcal{L}_\infty^B$ and $\mathcal{L}_\infty^E$ in which these

[2]Here, we explicitly reveal the dependence of the high SNR power offset on m_B, N_A, N_B, L_B, m_E, N_E, L_E, $\bar{\gamma}_E$.

expressions reduce to more simple forms.

Corollary 1: For the special case of Rayleigh fading, where $m_B = m_E = 1$, $\mathcal{L}_\infty^B$ in (4.28) reduces to

$$\mathcal{L}_\infty^B\left(1, N_B, L_B, N_A\right) = -\frac{1}{\ln 2}\left(L_B\binom{N_B}{L_B}\right)^{N_A} N_A!\widetilde{\sum}\tilde{\hbar}_\rho\zeta_1 \tag{4.30}$$

and $\mathcal{L}_\infty^E$ in (4.29) reduces to

$$\mathcal{L}_\infty^E\left(1, N_E, L_E, \bar{\gamma}_E\right) = -\frac{1}{\ln 2}\binom{N_E}{L_E}\sum_{\mathcal{S}_E^F}\sum_{n=1}^{L_E} a_k^F \ell_n \mu_n! \Psi\left(\mu_n + 1, \mu_n + 1, \nu_n\right), \tag{4.31}$$

where $\mathcal{S}_E^F = \left\{ \left(n_{k,0}^F, n_{k,1}^F\right) \middle| \sum_{j=0}^{1} n_{k,j}^F = N_E - L_E \right\}$.

Corollary 2: For the special case of Rayleigh fading with TAS/MRC, where $m_B = m_E = 1$, $L_B = N_B$, and $L_E = N_E$, $\mathcal{L}_\infty^B$ in (4.28) reduces to

$$\mathcal{L}_\infty^B\left(1, N_B, N_B, N_A\right) = -\frac{1}{\ln 2} N_A! \sum_{\mathcal{S}_B^1} \frac{\prod_{n=1}^{N_B}\left(\frac{-1}{(n-1)!}\right)^{n_{\rho_1,n}}}{\prod_{n=0}^{N_B} n_{\rho_1,n}!}\beta, \tag{4.32}$$

where $\mathcal{S}_B^1 = \left\{ (n_{\rho_1,0}, \cdots, n_{\rho_1,N_B}) \middle| \sum_{n=0}^{N_B} n_{\rho_1,n} = N_A \right\}$ and

$$\beta = \begin{cases} \ln(N_A) + C, & \theta_\rho = 0, \\ -\frac{(\theta_\rho - 1)!}{(N_A)^{\theta_\rho}}, & \theta_\rho > 0. \end{cases} \tag{4.33}$$

From (4.29), $\mathcal{L}_\infty^E$ reduces to

$$\mathcal{L}_\infty^E\left(1, N_E, N_E, \bar{\gamma}_E\right) = \frac{1}{\ln 2}\sum_{n=1}^{N_E}\left(\frac{1}{\bar{\gamma}_E}\right)^{n-1}\Psi\left(n, n, \frac{1}{\bar{\gamma}_E}\right). \tag{4.34}$$

It is clear from (4.34) that L_∞^E is an increasing function of N_E. As such, when the number of antennas at Eve increases, the high SNR power offset also increases, which in

turn decreases the average secrecy rate.

Corollary 3: For the special case of Rayleigh fading with TAS/SC, where $m_B = m_E = 1$, $L_B = 1$, and $L_E = 1$, $\mathcal{L}_\infty^B$ in (4.28) reduces to

$$\mathcal{L}_\infty^B\left(1, N_B, 1, N_A\right) = -\frac{1}{\ln 2}(N_B)^{N_A} N_A! \widetilde{\sum} \tilde{\hbar}_\rho \mathrm{sgn}(\tilde{\eta}_\rho)(\ln(\tilde{\eta}_\rho) + C). \tag{4.35}$$

By applying [140, eq. (3.352.4)], $\mathcal{L}_\infty^E$ in (4.29) reduces to

$$\mathcal{L}_\infty^E\left(1, N_E, 1, \bar{\gamma}_E\right) = \frac{N_E}{\ln 2} \sum_{S_E^F} \frac{(N_E-1)!}{\prod_{j=0}^{1} n_{k,j}^F!} (-1)^{n_{k,1}^F} \left(\frac{\mathrm{sgn}(n_{k,1}^F)}{n_{k,1}^F + 1} \right.$$
$$\left. + 1 - \mathrm{sgn}(n_{k,1}^F) \right) \left(-e^{\frac{\left(n_{k,1}^F+1\right)}{\bar{\gamma}_E}} \mathrm{Ei}\left(-\frac{\left(n_{k,1}^F+1\right)}{\bar{\gamma}_E} \right) \right), \tag{4.36}$$

where $\mathcal{S}_E^F = \left\{ \left(n_{k,0}^F, n_{k,1}^F\right) \middle| \sum_{j=0}^{1} n_{k,j}^F = N_E - 1 \right\}$ and $\mathrm{Ei}\left(\cdot\right)$ is the exponential integral function defined in [140, eq. (8.211.1)].

4.4.2.2 $\bar{\gamma}_B \to \infty$ and $\bar{\gamma}_E \to \infty$

In this case, the average secrecy rate can be easily obtained based on *Theorem 3*. We only need to further provide the asymptotic Δ_2 with $\bar{\gamma}_E \to \infty$. Observing Δ_1 in (4.19), the asymptotic Δ_2 is derived according to

$$\Delta_2 = -\left(\log_2\left(\bar{\gamma}_E\right) - \log_2\left(m_E\right)\right) - \Xi, \tag{4.37}$$

where

$$\Xi = \frac{1}{\ln 2} \frac{L_E}{(m_E-1)!} \binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{\left(L_E\right)^{b_k^\Phi + b_k^F + m_E}} \tilde{\ell}_n$$
$$\left(\left(1 - \mathrm{sgn}\left(\mu_n\right)\right)\left(C + \ln\left(\tilde{\nu}_n\right)\right) - \mathrm{sgn}\left(\mu_n\right) \frac{(\mu_n - 1)!}{\left(\tilde{\nu}_n\right)^{\mu_n}} \right). \tag{4.38}$$

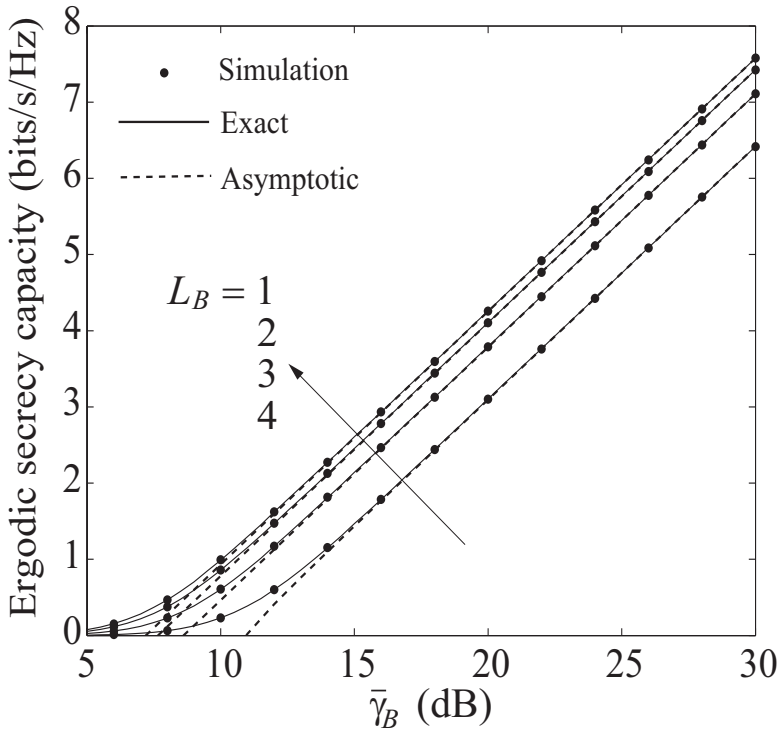

Figure 4.1: The ergodic secrecy capacity for $m_B = m_E = 2$, $N_A = 2$, $N_B = 4$, $N_E = 3$, $L_E = 2$, $\bar{\gamma}_E = 10$ dB.

In (4.38), $\tilde{\ell}_n = \ell_n \left(\frac{m_E}{\bar{\gamma}_E}\right)^{-\mu_n}$ and $\tilde{\nu}_n = \nu_n \left(\frac{m_E}{\bar{\gamma}_E}\right)^{-1}$. We should note that in (4.38), Ξ is independent of $\bar{\gamma}_E$.

Substituting (4.19) and (4.37) into (4.16), we derive the asymptotic average secrecy rate as

$$\bar{C}_s^{\infty} = \log_2\left(\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right) - \log_2\left(\frac{m_B}{m_E}\right) + \frac{1}{\ln 2}\left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \widetilde{\sum} \tilde{h}_\rho \zeta_1 - \Xi. \quad (4.39)$$

From (4.39), we see that for a fixed ratio of $\bar{\gamma}_B$ and $\bar{\gamma}_E$, the average secrecy rate is a constant value at high SNR. According to (4.24), the high SNR slope S_∞ is zero. This new result shows that when the eavesdropper is located close to the transmitter, increasing the transmit power does not have an impact on the average secrecy rate.

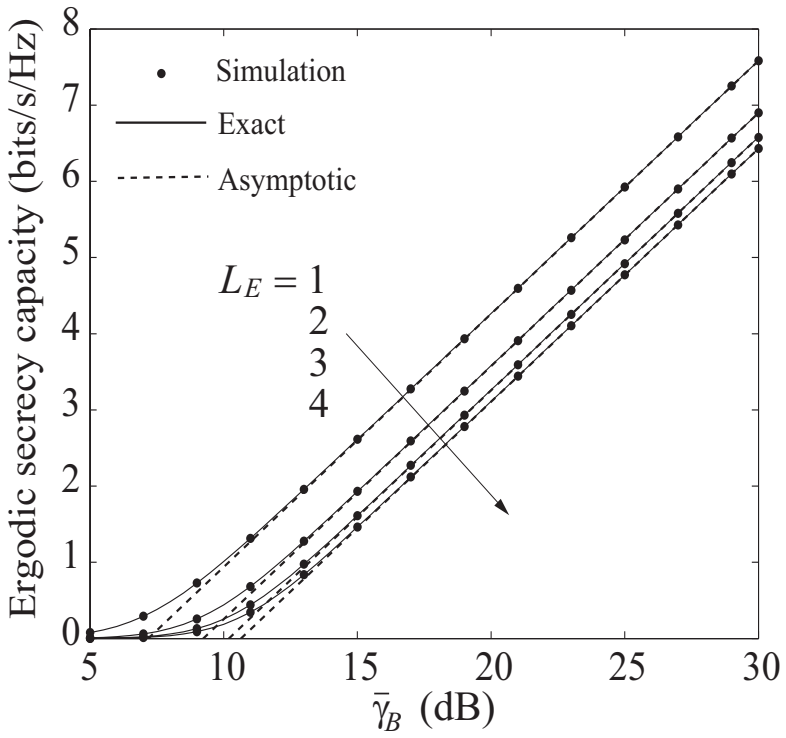

Figure 4.2: The ergodic secrecy capacity for $m_B = m_E = 2$, $N_A = 2$, $N_B = 4$, $N_E = 4$, $L_B = 2$, $\bar{\gamma}_E = 10$ dB.

4.4.3 Numerical Results

Figure 4.1 depicts the ergodic secrecy capacity versus $\bar{\gamma}_B$ for different L_B. The exact and asymptotic ergodic secrecy capacity results are obtained from (4.14) and (4.22), respectively. It is shown that the exact curves match precisely with Monte Carlo simulations and the asymptotic curves well approximate the exact ones in the high SNR regime. The ergodic secrecy capacity increases when more antennas are selected by Bob. However, the improvement diminishes with increasing L_B.

Figure 4.2 depicts the ergodic secrecy capacity versus $\bar{\gamma}_B$ for different L_E. The ergodic secrecy capacity decreases when more antennas are selected by Eve. The loss of ergodic secrecy capacity from selecting one more antenna lessens with increasing L_E.

Figure 4.3 depicts the high SNR power offset for different scenarios. We can see that the power offset increases with increasing N_E and L_E, which decreases the ergodic screcy

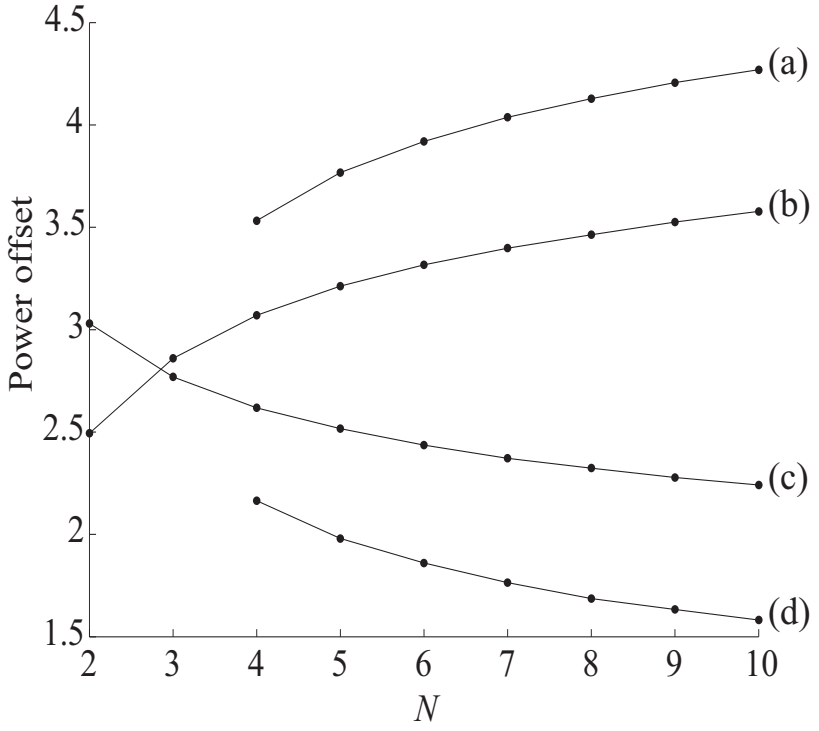

Figure 4.3: The high SNR power offset in decibels, obtaining by either (a) $m_B = m_E = 2$, $N_A = 2$, $N_B = 4$, $N_E = N$, $L_B = 2$, $L_E = 4$, $\bar{\gamma}_E = 10$ dB, (b) $m_B = m_E = 2$, $N_A = 2$, $N_B = 4$, $N_E = N$, $L_B = L_E = 2$, $\bar{\gamma}_E = 10$ dB, (c) $m_B = m_E = 2$, $N_A = 4$, $N_B = N$, $N_E = 3$, $L_B = L_E = 2$, $\bar{\gamma}_E = 10$ dB, (d) $m_B = m_E = 2$, $N_A = 4$, $N_B = N$, $N_E = 3$, $L_B = 4$, $L_E = 2$, $\bar{\gamma}_E = 10$ dB.

capacity. The power offset decreases with increasing N_B and L_B, which increases the ergodic secrecy capacity.

Figure 4.4 depicts the ergodic secrecy capacity versus $\bar{\gamma}_B$ for different L_B. Here we consider the scenario where both Bob and Eve are close to Alice. We set $u = \left.\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right|_{\text{dB}} = 10$ dB[3]. The exact and asymptotic ergodic secrecy capacity are obtained from (4.14) and (4.39), respectively. The ergodic secrecy capacity increases with increasing L_B. In the high SNR regime, the ergodic secrecy capacity becomes a constant value, which has been predicted from (4.39).

Figure 4.5 depicts the ergodic secrecy capacity versus $\bar{\gamma}_B$ for different L_E. We set

[3]Notation: $x|_{\text{dB}} = 10\log_{10}(x)$.

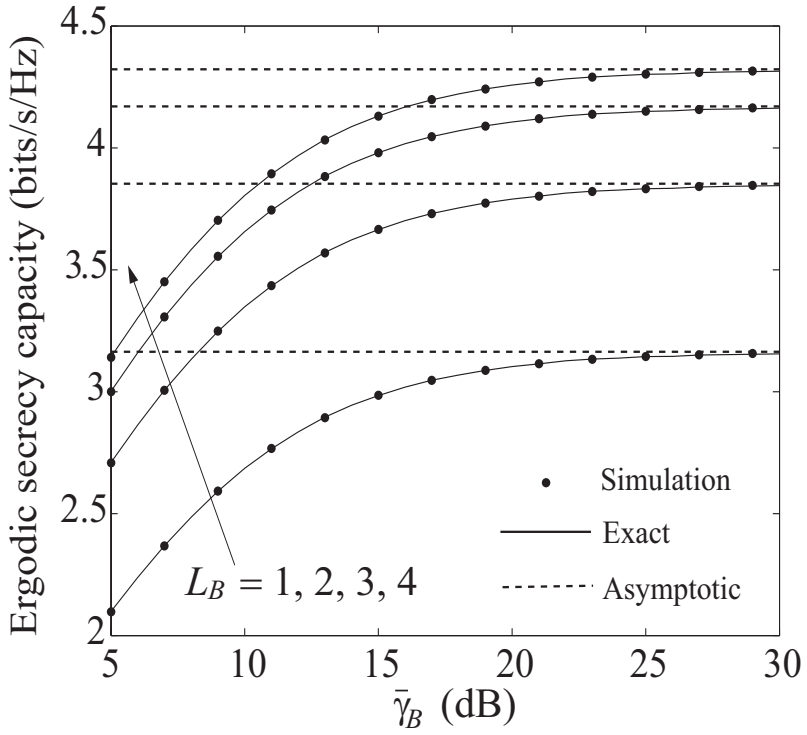

Figure 4.4: The ergodic secrecy capacity for $m_B = m_E = 2$, $N_A = 2$, $N_B = 4$, $N_E = 3$, $L_E = 2$.

$u = 10$ dB. The ergodic secrecy capacity decreases with increasing L_E. As expected, the ergodic secrecy capacity is constant in the high SNR regime.

4.5 Secrecy Outage Probability

In this section, we concentrate on passive eavesdropping scenario, where the CSI of the eavesdropper's channel is not known at Alice. In such a scenario, Alice has no choice but to encode the confidential data into codewords of a constant rate R_s [35], if $R_s \leq C_s$ (C_s has been defined in (4.9)), perfect secrecy can be achieved. Otherwise, if $R_s > C_s$, information-theoretic security is compromised. In other words, unlike the active eavesdropping scenario, perfect secrecy cannot be guaranteed in the passive eavesdropping scenario, since Alice has no information about the eavesdropper's channel. Motivated by this, we adopt the secrecy outage probability as a useful performance measure. We derive

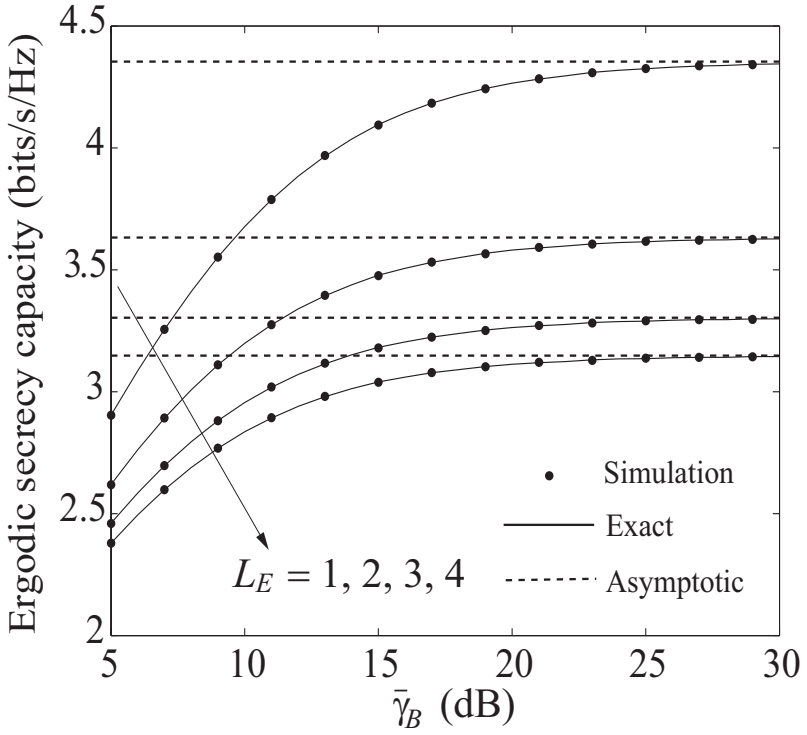

Figure 4.5: The ergodic secrecy capacity for $m_B = m_E = 2$, $N_A = 2$, $N_B = 4$, $N_E = 4$, $L_B = 2$.

new closed-form expressions for the exact and the asymptotic secrecy outage probability. Based on the asymptotic expressions, we present two key performance indicators, namely the secrecy diversity order and the secrecy array gain.

4.5.1 Exact Secrecy Outage Probability

A secrecy outage is declared when the secrecy rate C_s is less than the expected secrecy rate R_s. As such, the secrecy outage probability is derived as

$$P_{out}\left(R_s\right) = \Pr\left(C_s < R_s\right) = \int_0^\infty f_{\gamma_E}\left(x_2\right) F_{\gamma_B}\left(2^{R_s}\left(1+x_2\right)-1\right) dx_2. \tag{4.40}$$

Substituting (4.4) and (4.8) into (4.40), and applying the binomial expansion [140, eq. (1.111)] and [140, eq. (3.351.3)], we obtain

$$\begin{aligned} P_{out}\left(R_s\right) &= \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E+b_k^F} a_k^{\Phi} a_k^F \\ &\times \frac{\left(b_k^{\Phi}+b_k^F+m_E-1\right)!}{\left(L_E\right)^{b_k^{\Phi}+b_k^F+m_E}} \ell_n\left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \\ &\times \widetilde{\sum}\hbar_\rho \sum_{q=0}^{\theta_\rho}\binom{\theta_\rho}{q} 2^{R_s q}\left(2^{R_s}-1\right)^{\theta_\rho-q} e^{-\eta_\rho\left(2^{R_s}-1\right)} \\ &\times \left(\frac{\mu_n \Gamma\left(q+\mu_n\right)}{\left(\eta_\rho 2^{R_s}+\nu_n\right)^{q+\mu_n}} - \frac{\nu_n\left(q+\mu_n\right)!}{\left(\eta_\rho 2^{R_s}+\nu_n\right)^{q+\mu_n+1}}\right). \end{aligned} \tag{4.41}$$

Our new expression for the exact secrecy outage probability in (4.41) applies to arbitrary numbers of antennas at Bob and Eve, arbitrary fading parameters, and arbitrary average SNRs in the main and eavesdropper's channels. As shown in [33], the probability of positive secrecy can be evaluated as $1 - P_{out}\left(0\right)$.

4.5.2 Asymptotic Secrecy Outage Probability

In this subsection, we turn our attention to the asymptotic secrecy outage probability. We consider the following two scenarios.

4.5.2.1 $\bar{\gamma}_B \to \infty$

In this case, Bob is located close to Alice. We substitute (4.6) and (4.8) into (4.40), and derive the asymptotic secrecy outage probability as

$$P_{out}^{\infty}\left(R_s\right) = \left(G_a \bar{\gamma}_B\right)^{-G_d} + o\left(\bar{\gamma}_B^{-G_d}\right), \tag{4.42}$$

where the secrecy diversity order is

$$G_d = m_B N_B N_A \tag{4.43}$$

and the secrecy array gain is

$$\begin{aligned} G_a = & \left[\frac{L_E}{(m_E-1)!} \frac{\left(L_B \binom{N_B}{L_B}\right)^{N_A} (m_B)^{m_B N_B N_A}}{\left(\Gamma(m_B)(m_B!)^{N_B-L_B}(m_B N_B)!\right)^{N_A}} \right. \\ & \times \binom{N_E}{L_E} \left(\sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}} \right)^{N_A} \\ & \times \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}} \ell_n \sum_{q=0}^{m_B N_B N_A} \binom{m_B N_B N_A}{q} \\ & \left. \times \left(\Gamma(q+\mu_n)\mu_n - (q+\mu_n)!\right) \frac{2^{R_s q}\left(2^{R_s}-1\right)^{m_B N_B N_A - q}}{(\nu_n)^{q+\mu_n}} \right]^{-\frac{1}{m_B N_B N_A}}. \end{aligned} \tag{4.44}$$

Based on (4.43) and (4.44), we find that the secrecy diversity order is entirely determined by the antenna configuration and the fading parameters in the main channel. The impact of the eavesdropper's channel is only reflected in the secrecy array gain.

In order to characterize the impact of GSC on the secrecy outage probability, we quantify the secrecy outage tradeoff between $L_B + l$ and L_B, $l = 1, \cdots, N_B - L_B$. From (4.43), we confirm that $L_B + l$ and L_B have the same secrecy diversity order. As such, one can conclude that the SNR gap between $L_B + l$ and L_B is strictly determined by their respective secrecy array gains and is expressed as

$$\frac{G_a(L_B+l)}{G_a(L_B)} = \left[\frac{(m_B!)^l (L_B+l)\binom{N_B}{L_B+l}}{L_B\binom{N_B}{L_B}} \frac{\sum_{S_B^{\Phi^l}} a_k^{\Phi^l} \frac{\left(b_k^{\Phi^l} + m_B(N_B-L_B-l)+m_B-1\right)!}{(L_B+l)^{b_k^{\Phi^l} + m_B(N_B-L_B-l)+m_B}}}{\sum_{S_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}}} \right]^{-\frac{1}{m_B N_B}} \tag{4.45}$$

where $\mathcal{S}_B^{\Phi^l}$ satisfies the condition

$$\mathcal{S}_B^{\Phi^l} = \left\{ \left(n_{k,0}^{\Phi^l}, \cdots, n_{k,m_B-1}^{\Phi^l} \right) \Big| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi^l} = L_B + l - 1 \right\}.$$

Corollary 4: For the special case of Rayleigh fading, the secrecy diversity order in (4.43) reduces to $N_B N_A$ and the secrecy array gain in (4.44) reduces to

$$G_a = \left[\binom{N_E}{L_E} \frac{\left(2^{R_s}-1\right)^{N_B N_A}}{(L_B!)^{N_A} (L_B)^{N_A(N_B-L_B)}} \sum_{\mathcal{S}_E^F} \sum_{n=1}^{L_E} a_k^F \ell_n \right.$$
$$\left. \times \sum_{q=0}^{N_B N_A} \binom{N_B N_A}{q} \left(\frac{2^{R_s}}{2^{R_s}-1} \right)^q \frac{\left(\Gamma\left(q+\mu_n\right)\mu_n - (q+\mu_n)!\right)}{(\nu_n)^{q+\mu_n}} \right]^{-\frac{1}{N_B N_A}}. \tag{4.46}$$

Based on (4.46), we confirm that $\frac{G_a(L_B+1)}{G_a(L_B)} > 1$. This proves that the secrecy array gain is an increasing function of L_B. It follows that the SNR gap between $L_B + l$ and L_B in (4.45) reduces to

$$\frac{G_a\left(L_B+l\right)}{G_a\left(L_B\right)} = \left[\frac{(L_B)^l L_B!}{(L_B+l)! \left(1+\frac{l}{L_B}\right)^{N_B-L_B-l}} \right]^{-\frac{1}{N_B}}. \tag{4.47}$$

Based on (4.47), we confirm that $\left(\frac{G_a(L_B+1+l)}{G_a(L_B+1)}\right) \Big/ \left(\frac{G_a(L_B+l)}{G_a(L_B)}\right) < 1$. This proves that the SNR gap is a decreasing function of L_B.

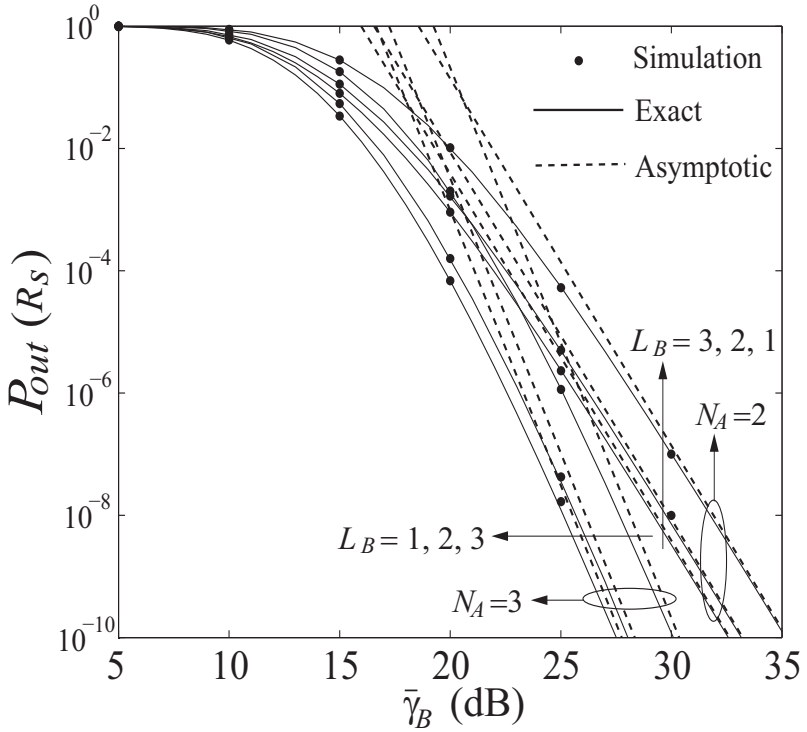

Figure 4.6: The secrecy outage probability for $m_B = 1$, $m_E = 2$, $N_B = 3$, $N_E = 3$, $L_E = 2$, $\bar{\gamma}_E = 10$ dB.

4.5.2.2 $\bar{\gamma}_B \to \infty$, $\bar{\gamma}_E \to \infty$

In this case, both Bob and Eve are located close to Alice. Based on (4.41), the asymptotic secrecy outage probability is derived as

$$\begin{aligned}
P_{out}^{\infty}(R_s) &= \lim_{\bar{\gamma}_B \to \infty,\, \bar{\gamma}_E \to \infty} P_{out}(R_s) \\
&= \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^{\Phi} a_k^F \\
&\times \tilde{\ell}_n \frac{\left(b_k^{\Phi} + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^{\Phi} + b_k^F + m_E}} \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B} \right)^{N_A} N_A! \\
&\times \widetilde{\sum} \tilde{h}_{\rho} \left(\frac{m_B \bar{\gamma}_E}{m_E \bar{\gamma}_B} \right)^{\theta_{\rho}} \frac{2^{R_s \theta_{\rho}}}{\left(\tilde{\eta}_{\rho} 2^{R_s} \frac{m_B \bar{\gamma}_E}{m_E \bar{\gamma}_B} + \tilde{\nu}_n \right)^{\theta_{\rho} + \mu_n}} \\
&\times \left(\mu_n \Gamma(\theta_{\rho} + \mu_n) - \frac{\tilde{\nu}_n (\theta_{\rho} + \mu_n)!}{\tilde{\eta}_{\rho} 2^{R_s} \frac{m_B \bar{\gamma}_E}{m_E \bar{\gamma}_B} + \tilde{\nu}_n} \right).
\end{aligned} \tag{4.48}$$

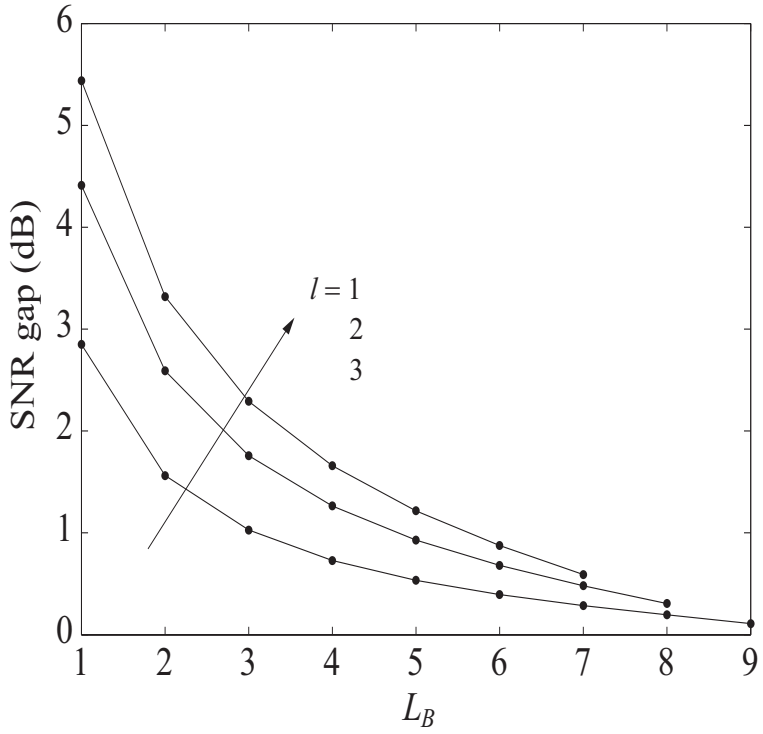

Figure 4.7: The SNR gap for $m_B = 2$, $N_B = 10$.

For a fixed ratio of $\bar{\gamma}_B$ and $\bar{\gamma}_E$, (4.48) confirms that the secrecy outage probability approaches a constant at high SNR, which implies that the secrecy diversity order is zero. Once again, this result shows that increasing the transmit power does not have an impact on the secrecy outage probability.

4.5.3 Numerical Results

In this subsection, we provide some numerical results to confirm the aforementioned analysis. In the simulation, we assume that the expected secrecy rate $R_s = 1$ bit/s/Hz.

Figure 4.6 depicts the secrecy outage probability versus $\bar{\gamma}_B$ for different L_B and N_A. The exact and asymptotic results are obtained from (4.41) and (4.42), respectively. The exact curves are in precise agreement with the Monte Carlo simulations, and the asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. As

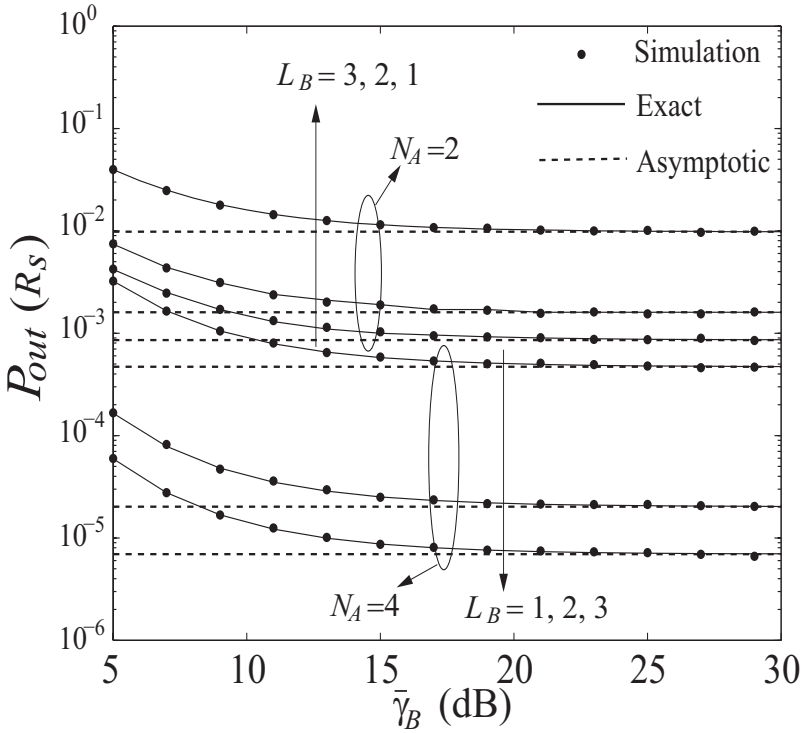

Figure 4.8: The secrecy outage probability for $m_B = 1$, $m_E = 2$, $N_B = 3$, $N_E = 3$, $L_E = 2$.

suggested in (4.43), the secrecy diversity order increases with N_A, which decreases the secrecy outage probability. Increasing L_B decreases the secrecy outage probability, due to the increase of the secrecy array gain.

Figure 4.7 depicts the SNR gap versus L_B for different l, the results are obtained from (4.45). When L_B is low, the SNR gap is sharp and increases with increasing l antenna at Bob. However, increasing L_B can diminish the gap, which indicates that GSC has an advantage of balancing the receive performance and implementation complexity.

Figure 4.8 depicts the secrecy outage probability versus $\bar{\gamma}_B$ for different L_B and N_A. We set $u = \frac{\bar{\gamma}_B}{\bar{\gamma}_E}\Big|_{\text{dB}} = 10$ dB. The exact and asymptotic results are obtained from (4.41) and (4.48). The secrecy outage probability decreases with increasing L_B and N_A. As suggested in (4.48), the secrecy outage probability becomes constant in the high SNR regime.

4.6 Conclusions

Transmit antenna selection with generalized selection (TAS/GSC) combining for physical layer security was examined in MIMO wiretap channels. In doing so, new analytical expressions of the statistical properties on the SNR with TAS/GSC were derived in Nakagami-m fading. With the aid of these results, new closed-form expressions for the exact and the asymptotic average secrecy rate were derived. Using these expressions, the high SNR slope and the high SNR power offset were precisely characterized. New closed-form expressions for the exact and the asymptotic secrecy outage probability were provided, which concisely characterized the secrecy diversity order and the secrecy array gain. Several key observations were drawn based on the locations of the legitimate receiver and the eavesdropper relative to the transmitter. It is shown that a capacity ceiling and an outage floor were created when both the legitimate receiver and the eavesdropper are close to the transmitter.

Chapter 5

Security in Cognitive Radio Networks

5.1 Introduction

Security is an important requirement for future 5G systems, and cognitive radio is no exception. Particularly, security of cognitive radio networks is critical as it is easily exposed to external threats [8–14]. In [10], security for the main channel was guaranteed by performing beamforming from a group of relays. In [12], secure communications with untrusted secondary users in cognitive radio networks was proposed and the achievable secrecy rate was derived. In [13, 14], game theory was utilized to exploit the security aspect of cognitive radio networks.

In this chapter, passive eavesdropping is considered, where the channel state information (CSI) of the eavesdropper's channel is not available at the secondary transmitter. In such a cognitive wiretap channel, the secondary transmitter sends confidential messages to the secondary receiver in the presence of a eavesdropper. In this network, the interference power at the PU from the secondary transmitter must not exceed a peak interference power threshold. The aim is to address fundamental questions surrounding

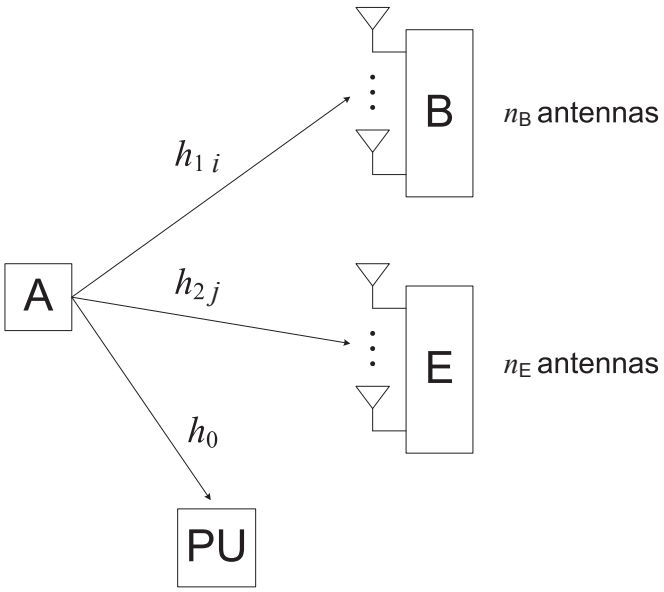

Figure 5.1: A cognitive wiretap radio network.

the joint impact of two power constraints on the cognitive wiretap channel: 1) the maximum transmit power at the secondary transmitter, and 2) the peak interference power at PU. To address these constraints, new closed-form expressions for the exact and asymptotic secrecy outage probability are derived. These analytical results reveal important design insights into the impact of the primary network on the secondary network in cognitive wiretap radio networks.

5.2 System and Channel Models

Consider a cognitive wiretap radio network, where the secondary transmitter Alice (A) communicates with the secondary receiver Bob (B) under the malicious attempt of the eavesdropper Eve (E) as shown in Figure 5.1. We assume a cognitive network with underlay spectrum sharing which allows concurrent transmissions from PU and A in the same spectrum band. For this network, A transmits data to B, where B and E are equipped with multiple antennas n_{B} and n_{E}, respectively, whereas A and PU are equipped with a single antenna.

Both the primary channel and the secondary channel are assumed to undergo independent identically distributed (i.i.d.) Rayleigh fading, where the channel gains $\{h_{1i}\}_{i=1}^{n_{\mathsf{B}}}$, $\{h_{2j}\}_{j=1}^{n_{\mathsf{E}}}$, and h_0 are complex Gaussian random variables (RVs) with zero mean and variances Ω_1, Ω_2, and Ω_0, respectively. We also assume that the main channel from A to B and the eavesdropper's channel from A to E are independent of each other. We consider antenna selection[1] at B and E[2]. Here, B and E select their strongest receive antennas based on perfect CSI estimation via pilot signals transmitted by A. Based on this, the instantaneous signal-to-noise ratio (SNR) in the main and the eavesdropper's channel are given by

$$\gamma_{\mathsf{M}} = \max_{i=1,\ldots,n_{\mathsf{B}}} \frac{\mathsf{P}_{\mathsf{A}}}{N_0}|h_{1i}|^2, \quad \gamma_{\mathsf{E}} = \max_{j=1,\ldots,n_{\mathsf{E}}} \frac{\mathsf{P}_{\mathsf{A}}}{N_0}|h_{2j}|^2, \tag{5.1}$$

respectively, where P_{A} is the transmit power at A and N_0 is the noise variance.

According to underlay cognitive radio transmission, the transmit power at A must be managed under a peak interference power threshold to guarantee reliable communication at PU. With this in mind, A is power-limited such that the maximum transmit power is P_t. As such, the transmit power at A is strictly constrained by the maximum transmit power P_t at A and the peak interference power I_p at PU according to

$$\mathsf{P}_{\mathsf{A}} = \min\left(\frac{\mathsf{I}_p}{|h_0|^2}, \mathsf{P}_t\right), \tag{5.2}$$

from which the instantaneous SNR at Bob and Eve in (5.1) are reexpressed as

$$\gamma_{\mathsf{M}} = \min\left(\frac{\overline{\gamma}_p}{X}, \overline{\gamma}_0\right) Y_M, \quad \gamma_{\mathsf{E}} = \min\left(\frac{\overline{\gamma}_p}{X}, \overline{\gamma}_0\right) Y_E, \tag{5.3}$$

respectively, where $\overline{\gamma}_p = \mathsf{I}_p/N_0$, $\overline{\gamma}_0 = \mathsf{P}_t/N_0$, $X = |h_0|^2$, $Y_M = \max\limits_{i=1,\ldots,n_{\mathsf{B}}} |h_{1i}|^2$, and $Y_E = \max\limits_{j=1,\ldots,n_{\mathsf{E}}} |h_{2j}|^2$.

[1]It is well-known that using antenna selection can achieve the full diversity gain with a less number of RF electronics for each branch compared to maximal ratio combining [68].

[2]In commercial wireless applications, the eavesdropper may be subject to the same resource constraints as the legitimate receiver. Specifically, it may be limited to a single radio frequency (RF) chain due to size and complexity limitations, as was considered in [149] and [7].

5.3 Secrecy Outage Probability

We focus on passive eavesdropping, where knowledge of the eavesdropper's channel is not known at A. In such a scenario, A has no choice but to encode the confidential data into codewords of a constant rate R_s [35]. Following the wiretap channel in [28, 35], A encodes a message block W^k into a codeword X^n, and the eavesdropper receives Y_w^n from the output of its channel. The equivocation rate of Eve is $R_e = H\left(W^k \middle| Y_w^n\right)/n$. We assume slow block fading for the main channel and the eavesdropper's channel, where the fading coefficients are constant during a codeword transmission. Taking this into account, we define the secrecy rate as [35]

$$C_\mathsf{s} = \begin{cases} C_\mathsf{M} - C_\mathsf{E} & \text{if } \gamma_\mathsf{M} > \gamma_\mathsf{E} \\ 0 & \text{if } \gamma_\mathsf{M} \leq \gamma_\mathsf{E} \end{cases}, \tag{5.4}$$

where $C_\mathsf{M} = \log_2(1+\gamma_\mathsf{M})$ is the capacity of the main channel and $C_\mathsf{E} = \log_2(1+\gamma_\mathsf{E})$ is the capacity of the eavesdropper's channel. The secrecy rate C_s in (5.4) is the maximum achievable perfect secrecy rate R such that $R_e = R$ [28, 35]. In passive eavesdropping, if $R_\mathsf{s} \leq C_\mathsf{s}$, perfect secrecy is guaranteed. Otherwise, if $R_\mathsf{s} > C_\mathsf{s}$, information-theoretic security is compromised. As such, the secrecy outage probability is the probability that C_s falls below R_s, which is expressed as

$$P_\mathsf{out} = \Pr(C_\mathsf{s} < R_\mathsf{s}) = \Pr(\gamma_\mathsf{M} \leq \gamma_\mathsf{E}) + \underbrace{\Pr(\gamma_\mathsf{M} > \gamma_\mathsf{E})}_{\mathcal{A}} \underbrace{\Pr(C_\mathsf{s} < R_\mathsf{s} | \gamma_\mathsf{M} > \gamma_\mathsf{E})}_{\mathcal{I}}. \tag{5.5}$$

In order to evaluate the term $\mathcal{I}$, we first rewrite C_s in (5.4) as

$$C_\mathsf{s} = \log_2\left(\frac{1+\gamma_\mathsf{M}}{1+\gamma_\mathsf{E}}\right) < R_\mathsf{s}, \tag{5.6}$$

which is equivalent to

$$\gamma_\mathsf{M} < 2^{R_\mathsf{s}}(1+\gamma_\mathsf{E}) - 1 = \epsilon(\gamma_\mathsf{E}). \tag{5.7}$$

Then $\mathcal{I}$ can be written as

$$\mathcal{I} = \frac{1}{\mathcal{A}} \int_0^\infty \int_0^\infty \int_{\gamma_\mathsf{E}}^{\epsilon(\gamma_\mathsf{E})} f_{\gamma_\mathsf{M}|\{X=x\}}(\gamma_\mathsf{M})\, f_{\gamma_\mathsf{E}|\{X=x\}}(\gamma_\mathsf{E})\, f_X(x)\, d\gamma_\mathsf{M} d\gamma_\mathsf{E} dx. \tag{5.8}$$

where $f_X(x)$ is the PDF of X, $f_{\gamma_\mathsf{A}|\{X=x\}}(\cdot)$ is the PDF of γ_A conditioned on X, $\gamma_\mathsf{A} \in \{\gamma_\mathsf{M}, \gamma_\mathsf{E}\}$. By exchanging the variable in the limits of inner integral $\mathcal{I}$, we obtain

$$\mathcal{I} = \frac{\mathcal{I}_1 - \mathcal{I}_2}{\mathcal{A}}, \tag{5.9}$$

where $\mathcal{I}_1$ and $\mathcal{I}_2$ are respectively given as

$$\mathcal{I}_1 = \int_0^\infty \int_0^\infty \int_0^{\epsilon(\gamma_\mathsf{E})} f_{\gamma_\mathsf{M}|\{X=x\}}(\gamma_\mathsf{M})\, f_{\gamma_\mathsf{E}|\{X=x\}}(\gamma_\mathsf{E})\, f_X(x)\, d\gamma_\mathsf{M} d\gamma_\mathsf{E} dx \tag{5.10}$$

and

$$\mathcal{I}_2 = 1 - \mathcal{A}. \tag{5.11}$$

Putting together (5.5), (5.9), (5.10), and (5.11), we get

$$P_\mathsf{out} = \int_0^\infty \int_0^\infty F_{\gamma_\mathsf{M}|\{X=x\}}(\epsilon(\gamma_\mathsf{E}))\, f_{\gamma_\mathsf{E}|\{X=x\}}(\gamma_\mathsf{E})\, f_X(x)\, d\gamma_\mathsf{E} dx. \tag{5.12}$$

where $F_{\gamma_\mathsf{M}|\{X=x\}}(\cdot)$ is the CDF of γ_M conditioned on X.

For ease of exposition and mathematical tractability, we denote $\overline{\gamma}_1 = \overline{\gamma}_0\Omega_1 = \frac{\overline{\gamma}_p\Omega_1}{\sigma}$ and $\overline{\gamma}_2 = \overline{\gamma}_0\Omega_2 = \frac{\overline{\gamma}_p\Omega_2}{\sigma}$ with $\sigma = \frac{\mathsf{I}_p}{\mathsf{P}_t}$. Here, $\overline{\gamma}_1$ represents the maximum possible average SNR of the channel between A and B, and $\overline{\gamma}_2$ represents the maximum possible average SNR of the channel between A and E.

$$P_{\text{out}} = \left(1 - e^{-\frac{\sigma}{\Omega_0}}\right) \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_2} (-1)^{i+j} e^{-\frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_1}} \left(\frac{i2^{R_{\mathsf{s}}}}{\overline{\gamma}_1} + \frac{j+1}{\overline{\gamma}_2}\right)^{-1}$$
$$+ \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_2 \sigma} (-1)^{i+j} \frac{1}{\Omega_0} \left(\frac{i2^{R_{\mathsf{s}}}}{\overline{\gamma}_1 \sigma} + \frac{j+1}{\overline{\gamma}_2 \sigma}\right)^{-1} \frac{e^{-\frac{\sigma}{\Omega_0} - \frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_1}}}{\frac{1}{\Omega_0} + \frac{i(2^{R_{\mathsf{s}}}-1)}{\overline{\gamma}_1 \sigma}}, \tag{5.13}$$

5.3.1 Exact Secrecy Outage Probability

In this subsection, we present a novel closed-form expression for the exact secrecy outage probability, as given in the following theorem.

Theorem 1. *The exact secrecy outage probability of the proposed cognitive multi-antenna wiretap channel is given by* (5.13)*,*

Proof. See Appendix B.1. □

It is worth noting that (5.13) involves only finite summations of exponentials, powers, and exponential integral functions, thus can be calculated in closed-form. This expression serves as a prerequisite for other secrecy metrics such as the probability of non-zero secrecy capacity, calculated as $\Pr(C_{\mathsf{s}} > 0) = \Pr(\gamma_{\mathsf{M}} > \gamma_{\mathsf{E}}) = 1 - P_{\text{out}}(0)$. In addition, considering the special case of a single antenna transmitter and a single antenna receiver, our secrecy outage probability expression without interference power constraint reduces to [149, eq. (11)]. Our secrecy outage probability expression without interference power constraint also reduces to [7, eq. 34] with a single transit antenna in Rayleigh fading.

5.3.2 Asymptotic Secrecy Outage Probability

We derive a new asymptotic expression for the secrecy outage probability at high SNR operating regions. The main driver is to identify the key players that control network behavior. The aim is to determine the impact of PU on A in the presence of a multi-

antenna wiretap channel. In particular, we are interested in the joint impact of the maximum transmit power P_t at A and the peak interference power I_p at PU on the secrecy outage probability. Other key network players of interest are the number of antennas n_{B} at B and the number of antennas n_{E} at E. With this in mind, we address the interference power constraint of I_p proportional to P_t according to $\mathsf{I}_p = \sigma \mathsf{P}_t$, where σ is a positive constant. Based on Appendix A, we first obtain the first order expansion of $F_{\gamma_{\mathsf{M}}|\{X\}}(\gamma)$ conditioned on X as

$$F_{\gamma_{\mathsf{M}}|\{X\}}(\gamma) = \begin{cases} \left(\frac{\gamma}{\overline{\gamma}_1}\right)^{n_{\mathsf{B}}}, & X \leq \frac{\overline{\gamma}_p}{\overline{\gamma}_0} \\ \left(\frac{X}{\overline{\gamma}_1 \sigma}\gamma\right)^{n_{\mathsf{B}}}, & X > \frac{\overline{\gamma}_p}{\overline{\gamma}_0} \end{cases}. \tag{5.14}$$

Substituting (5.14) and $f_{\gamma_{\mathsf{E}}|\{X=x\}}(\gamma_{\mathsf{E}})$ and $f_X(x)$ into (5.12), and using the binomial expansion, the asymptotic secrecy outage probability is calculated as

$$\begin{aligned} P_{\mathsf{out}}^{\infty} = & \left(1 - e^{-\frac{\overline{\gamma}_p}{\overline{\gamma}_0 \Omega_0}}\right) \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \left(\frac{2^{R_{\mathsf{s}}} - 1}{\overline{\gamma}_1}\right)^{n_{\mathsf{B}}-i} \left(\frac{2^{R_{\mathsf{s}}}}{\overline{\gamma}_1}\right)^{i} \\ & \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_2} (-1)^j \int_0^{\infty} (\gamma_{\mathsf{E}})^i e^{-\frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_2}} d\gamma_{\mathsf{E}} \\ & + \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \left(\frac{2^{R_{\mathsf{s}}} - 1}{\overline{\gamma}_1 \sigma}\right)^{n_{\mathsf{B}}-i} \left(\frac{2^{R_{\mathsf{s}}}}{\overline{\gamma}_1 \sigma}\right)^{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \\ & \frac{n_{\mathsf{E}}}{\overline{\gamma}_2 \sigma} (-1)^j \frac{1}{\Omega_0} \int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} e^{-\frac{x}{\Omega_0}} \int_0^{\infty} x^{n_{\mathsf{B}}+1} (\gamma_{\mathsf{E}})^i e^{-\frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_2 \sigma} x} d\gamma_{\mathsf{E}} dx. \end{aligned} \tag{5.15}$$

Employing [140, eq. (3.351.3)] given by $\int_0^{\infty} x^n e^{-\mu x} dx = \frac{\Gamma(n+1)}{\mu^{n+1}}$, we can evaluate the integrals in (5.15) and derive the secrecy outage probability as

$$P_{\text{out}}^{\infty} = (G_a \overline{\gamma}_1)^{-G_d} + O\left(\overline{\gamma}_1^{-G_d}\right), \tag{5.16}$$

where the secrecy diversity order is

$$G_d = n_{\mathsf{B}} \tag{5.17}$$

and the secrecy array gain is

$$G_a = \Bigg[\left(1-e^{-\frac{\sigma}{\Omega_0}}\right)\sum_{i=0}^{n_{\mathsf{B}}}\binom{n_{\mathsf{B}}}{i}\left(2^{R_{\mathsf{s}}}-1\right)^{n_{\mathsf{B}}-i}2^{R_{\mathsf{s}}i} \sum_{j=0}^{n_{\mathsf{E}}-1}\binom{n_{\mathsf{E}}-1}{j}n_{\mathsf{E}}\overline{\gamma}_2{}^{i}(-1)^j\frac{\Gamma\left(i+1\right)}{\left(j+1\right)^{i+1}} + \sum_{i=0}^{n_{\mathsf{B}}}\binom{n_{\mathsf{B}}}{i} \left(2^{R_{\mathsf{s}}}-1\right)^{n_{\mathsf{B}}-i}\sigma^{-n_{\mathsf{B}}}2^{R_{\mathsf{s}}i}\sum_{j=0}^{n_{\mathsf{E}}-1}\binom{n_{\mathsf{E}}-1}{j}n_{\mathsf{E}}\left(\overline{\gamma}_2\sigma\right)^i (-1)^j(\Omega_0)^{n_{\mathsf{B}}-i}\frac{\Gamma\left(i+1\right)}{\left(j+1\right)^{i+1}}\Gamma\left(n_{\mathsf{B}}-i+1,\frac{\sigma}{\Omega_0}\right)\Bigg]^{-\frac{1}{n_{\mathsf{B}}}}, \tag{5.18}$$

where $\Gamma\left(\cdot,\cdot\right)$ is the incomplete gamma function [140, eq. (8.350.2)].

5.4 Numerical Results

Numerical examples are provided to highlight the impact of the primary network on the secondary network in the presence of a multi-antenna wiretap channel. The exact and asymptotic curves are obtained from (5.13) and (5.16), respectively. The exact curves are in precise agreement with the Monte Carlo simulations. We also see that the asymptotic curves well approximate the exact curves at high SNR. The asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. Throughout this section, we assume unity variance $\Omega_0 = 1$ and expected secrecy rate $R_s = 0.1$ bit/s/Hz.

Figure 5.2 plots the secrecy outage probability versus $\overline{\gamma}_1$ for different σ and different n_{B}. According to (5.17), we see that the secrecy diversity order increases with n_{B}, which in turn decreases the secrecy outage probability. We also see that the secrecy outage probability decreases with increasing σ. This is due to relaxing the peak interference power constraint $\mathsf{I}_p = \sigma\mathsf{P}_t$, which in turn increases transmit power P_{A}, as indicated by (5.2). This can also be explained by the fact that the secrecy array gain in (5.18) increases with increasing σ.

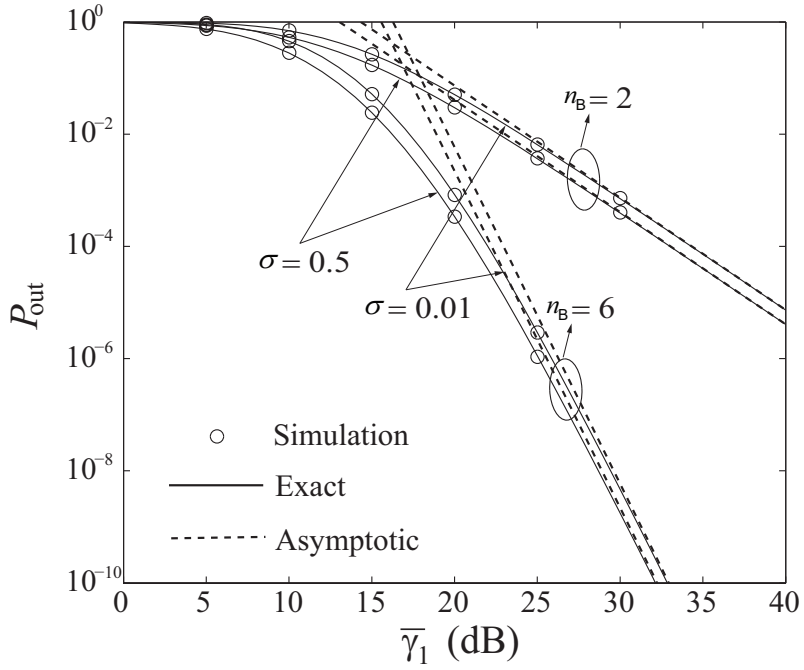

Figure 5.2: Secrecy outage probability with $\overline{\gamma}_2 = 10$ dB and $n_{\mathsf{E}} = 2$.

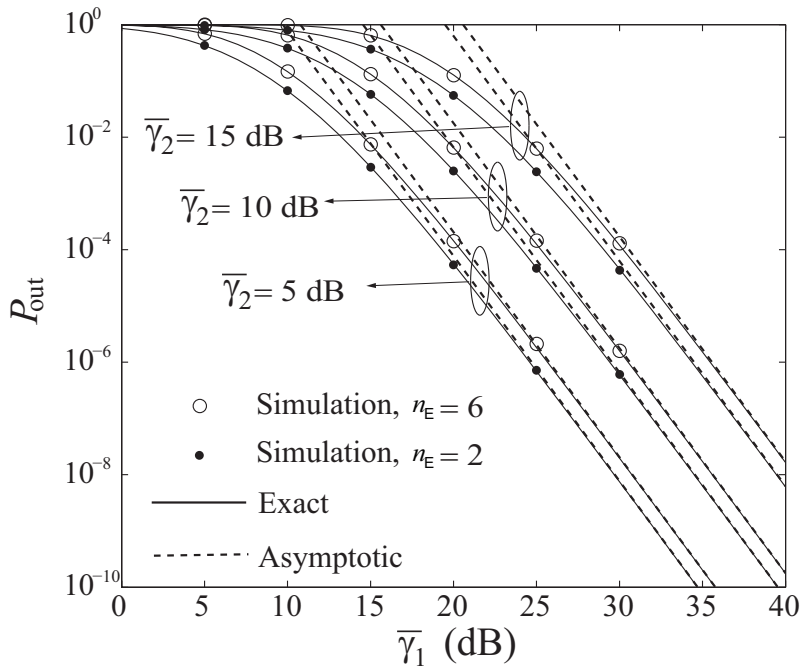

Figure 5.3: Secrecy outage probability with $\sigma = 0.1$ and $n_{\mathsf{B}} = 4$.

Figure 5.3 plots the secrecy outage probability versus $\overline{\gamma}_1$ for different $\overline{\gamma}_2$ and different n_{E}. The parallel slopes of the asymptotes confirm that the secrecy diversity order is independent of $\overline{\gamma}_2$ and n_{E}, as indicated in (5.17). Note the secrecy outage probability increases with increasing $\overline{\gamma}_2$ and n_{E}. This confirms that the secrecy array gain in (5.18) is a decreasing function of $\overline{\gamma}_2$ and n_{E}.

5.5 Conclusions

Physical layer security enhancement in cognitive multi-antenna wiretap channels was analyzed. In an effort to assess the secrecy performance in passive eavesdropping, the secrecy outage probability as a useful performance measure was adopted. New closed-form expressions for the exact and asymptotic secrecy outage probability was derived. Based on these, important design insights into the interplay between two power constraints, namely the maximum transmit power at the secondary network and the peak interference power at the primary network were concluded. The impact of these constraints on the cognitive wiretap channel was showcased.

Chapter 6

Security Enhancement of Cooperative Single Carrier Systems

6.1 Introduction

The physical (PHY) layer security issues with secrecy constraints in cyclic prefix (CP) single-carrier (SC) transmission remain unknown. To harness the aforementioned characteristics of multipath components in practice within the framework of PHY layer security, secure CP-SC transmission in decode-and-forward (DF) relay networks is considered. A two-stage relay and destination selection is proposed to minimize the eavesdropping and maximize the signal power of the link between the relay and the destination. Analytical results for the secrecy outage probability, the probability of non-zero achievable secrecy rate, and the ergodic secrecy rate are derived in closed-form. The secrecy diversity gain and the secrecy array gain are calculated based on simplified expressions for the secrecy outage probability in the high signal-to-noise ratio (SNR) regime. Likewise, the multiplexing gain and the power cost are calculated based on simplified expressions for the

ergodic secrecy rate in the high SNR regime.

Notation: The superscript $(\cdot)^H$ denotes complex conjugate transposition; $\boldsymbol{I}_N$ is an $N \times N$ identity matrix; $\mathbf{0}$ denotes an all-zeros matrix of appropriate dimensions; $\mathcal{CN}\left(\mu, \sigma^2\right)$ denotes the complex Gaussian distribution with the mean μ and the variance σ^2; $\mathbb{C}^{m \times n}$ denotes the vector space of all $m \times n$ complex matrices; $F_{\varphi}(\cdot)$ denotes the cumulative distribution function (CDF) of the random variable (RV) φ; and $E_a\{\cdot\}$ denotes expectation with respect to a. The probability density function (PDF) of φ is denoted by $f_{\varphi}(\cdot)$; $[x]^+ = \max(x, 0)$ and $\sum_{l_1,\ldots,l_a}^{i}$ denotes a set of nonnegative integers $\{l_1, \ldots, l_a\}$ satisfying $\sum_{t=1}^{a} l_t = i$.

6.2 System and Channel Model

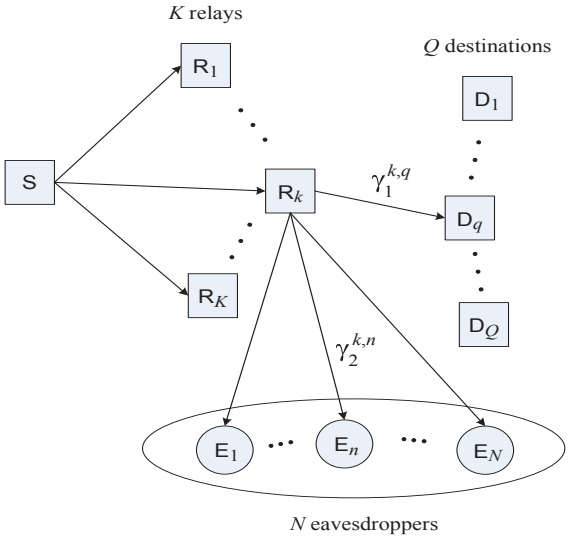

Figure 6.1: PHY layer security for cooperative single carrier systems.

In the considered system, which is shown in Figure 6.1, we assume the following set of instantaneous impulse channel responses.

- A set of channels $\{\boldsymbol{g}^{k,q}, \forall k, q\}$ between a particular kth relay and the qth destination undergo a frequency selective fading. They are assumed to have the same

N_1 multipath components, i.e., $\boldsymbol{g}^{k,q} \triangleq [g_1^{k,q}, \ldots, g_{N_1}^{k,q}]^T \in \mathbb{C}^{N_1 \times 1}$, each of which is distributed by the complex white Gaussian distribution with the zero mean and the unit variance. The path losses over these channels are denoted by $\{\alpha_1^{k,q}, \forall k, q\}$.

- A set of channels $\{\boldsymbol{h}^{k,1}, \ldots, \boldsymbol{h}^{k,n}, \ldots, \boldsymbol{h}^{k,N}\}$ between the kth relay and the N eavesdroppers undergo a frequency selective fading. They are assumed to have the same N_2 multipath components, i.e., $\boldsymbol{h}^{k,n} \triangleq [h_1^{k,n}, \ldots, h_{N_2}^{k,n}]^T \in \mathbb{C}^{N_2 \times 1}$, each of which is distributed by the complex white Gaussian distribution with the zero mean and the unit variance. The path losses over these channels are denoted by $\{\alpha_2^{k,n}, \forall k, n\}$.

- The maximum channel length in the considered system is assumed to be $N_g = \max(N_1, N_2, N_3)$, where N_3 denotes the multipath channel length between the source and relays.

For single-carrier cooperative transmission, we assume that

- Binary phase shift keying (BPSK) modulation is applied such that P modulated data symbols transmitted by the source form a transmit symbol block $\boldsymbol{x} \in \mathbb{C}^{P \times 1} \in \{-1, 1\}^P$ satisfying $E_{\boldsymbol{x}}\{\boldsymbol{x}\} = \boldsymbol{0}$ and $E_{\boldsymbol{x}}\{\boldsymbol{x}\boldsymbol{x}^H\} = \boldsymbol{I}_P$.

- To prevent inter-block symbol interference (IBSI) [120, 129, 131], the CP comprising of P_g symbols is appended to the front of $\boldsymbol{x}$. It is also assume that $P_g \geq N_g$.

- We employ the selective-DF relaying protocol, which selects one relay and destination among their groups. This selection is accomplished via the proposed two-step selection scheme.

- We assume perfect decoding at each relay, so that error propagation does not exist in the considered system [1].

[1] Practically, the source and the relays are located in the same cluster yielding high received SNRs at the DF relays to successfully decode the messages.

The signal received at the nth eavesdropper from the kth relay is given by

$$\boldsymbol{r}^{k,n} = \sqrt{P_s \alpha_2^{k,n}} \boldsymbol{H}^{k,n} \boldsymbol{x} + \boldsymbol{n}_2^{k,n} \tag{6.1}$$

where P_s is the transmit power and $\boldsymbol{H}^{k,n}$ is the right circulant matrix [129, 150] defined by $\boldsymbol{h}^{k,n}$. Also, we assume that $\boldsymbol{n}_2^{k,n} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2 \boldsymbol{I}_P)$. Since we assume perfect decoding at all the relays and perfect knowledge of channel state information (CSI)[2], channels between the source and the relays are not taken into account in (6.1) [43, 151].

Applying the properties of the right circulant channel matrix [129, 150], the instantaneous SNR between the kth relay and the nth eavesdropper is defined as

$$\gamma_2^{k,n} = \frac{P_s \alpha_2^{k,n} \|\boldsymbol{h}^{k,n}\|^2}{\sigma_n^2} = \tilde{\alpha}_2^{k,n} \|\boldsymbol{h}^{k,n}\|^2 \ \sim \chi^2(2N_2, \tilde{\alpha}_2^{k,n}) \tag{6.2}$$

where $\tilde{\alpha}_2^{k,n} \triangleq \frac{P_s \alpha_2^{k,n}}{\sigma_n^2}$, and the CDF and PDF of $\gamma_2^{k,n}$ are, respectively, given by

$$\begin{aligned} F_{\gamma_2^{k,n}}(x) &= 1 - e^{-x/\tilde{\alpha}_2^{k,n}} \sum_{l=0}^{N_2-1} \frac{1}{l!} \left(\frac{x}{\tilde{\alpha}_2^{k,n}} \right)^l \mathrm{U}(x) \text{ and} \\ f_{\gamma_2^{k,n}}(x) &= \frac{1}{(\tilde{\alpha}_2^{k,n})^{N_2} (N_2 - 1)!} x^{N_2 - 1} e^{-x/\tilde{\alpha}_2^{k,n}} \mathrm{U}(x) \end{aligned} \tag{6.3}$$

where $\mathrm{U}(x)$ denotes the discrete unit function.

Now the received signal at the qth destination from the kth relay is given by

$$\boldsymbol{z}^{k,q} = \sqrt{P_s \alpha_1^{k,q}} \boldsymbol{G}^{k,q} \boldsymbol{x} + \boldsymbol{n}_1^{k,q} \tag{6.4}$$

where $\boldsymbol{G}^{k,q}$ is the right circulant matrix defined by $\boldsymbol{g}^{k,q}$. Also, we assume that $\boldsymbol{n}_1^{k,q} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2 \boldsymbol{I}_Q)$. According to Definition 1, the instantaneous SNR of the link between the kth relay and the qth destination is given by $\gamma_1^{k,q} = \frac{P_s \alpha_1^{k,q} \|\boldsymbol{g}^{k,q}\|^2}{\sigma_n^2} = \tilde{\alpha}_1^{k,q} \|\boldsymbol{g}^{k,q}\|^2 \ \sim$

[2]This assumption is commonly seen in the prior literature [43, 44]. The CSI of the eavesdropper channels can be obtained in the scenario where eavesdroppers are active.

$\chi^2(2N_1, \tilde{\alpha}_1^{k,q})$, so that the CDF of $\gamma_1^{k,q}$ is given by

$$F_{\gamma_1^{k,q}}(x) = 1 - e^{-x/\tilde{\alpha}_1^{k,q}} \sum_{l=0}^{N_1-1} \frac{1}{l!} \left(\frac{x}{\tilde{\alpha}_1^{k,q}} \right)^l \mathrm{U}(x). \tag{6.5}$$

In the sequel, we assume that pathloss components $\alpha_2^{k,n}$ and $\alpha_1^{k,q}$ are independent of the indices of the relay, eavesdropper, and destination, so that we have $\alpha_2 = \{\alpha_2^{k,n}, \forall k, n\}$ and $\alpha_1 = \{\alpha_1^{k,q}, \forall k, q\}$.

6.3 Relay and Destination Selection under a group of Eavesdroppers

In this section, we shall first propose the two-stage relay and destination selection procedure, in which a relay is selected to minimize the worst-case eavesdropping in the eavesdropper group, to decrease the amount of information that eavesdroppers wiretap. And then, the desired destination is selected from the chosen relay to have the maximum instantaneous SNR between them. That is, the relay and destination are chosen according to the following selection criterion:

$$\begin{aligned} \text{stage1} \quad &: \; k^* = \min \arg_{k \in [1,K]} (\gamma_2^{k,\max}) \text{ and} \\ \text{stage2} \quad &: \; q^* = \max \arg_{q \in [1,Q]} (\gamma_1^{k^*,q}) \end{aligned} \tag{6.6}$$

where $\gamma_2^{k,\max}$ denotes the maximum instantaneous SNR among those of between the kth relay and N eavesdroppers. In addition, $\gamma_1^{k^*,q}$ denotes the maximum instantaneous SNR between the selected relay and the qth destination. When $Q = 1$, the proposed relay and destination selection scheme becomes somewhat similar to that of [43] (Note that the relay selection based on maximal secrecy rate was analyzed in the prior literature such as [10], which brings large system overhead compared with our proposed scheme.). However, due to an achievable multiuser diversity, the proposed selection scheme will result

$$f_{\gamma_2^{\min,\max}}(x) = \frac{KN}{(\tilde{\alpha}_2)^{N_2}(N_2-1)!}\sum_{k=0}^{K-1}\sum_{m=0}^{Nk}\sum_{j=0}^{N-1}\binom{K-1}{k}\binom{Nk}{m}\binom{N-1}{j}(-1)^{k+m+j}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\sum_{u_1,\ldots,u_{N_2}}^{j}\frac{m!}{v_1!\ldots v_{N_2}!}\frac{j!}{u_1!\ldots u_{N_2}!}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{u_{t+1}}}$$
$$e^{-\frac{x(m+j+1)}{\tilde{\alpha}_2}}x^{N_2+(\sum_{t=0}^{N_2-1}tv_{t+1})+(\sum_{t=0}^{N_2-1}tu_{t+1})-1}$$
$$= C\widetilde{\sum}e^{-\beta_2 x}x^{\tilde{N}_2-1}\mathrm{U}(x) \tag{6.8}$$

where $C\stackrel{\triangle}{=}\frac{KN}{(\tilde{\alpha}_2)^{N_2}(N_2-1)!}$, $\beta_2\stackrel{\triangle}{=}\frac{(m+j+1)}{\tilde{\alpha}_2}$, $\tilde{N}_2\stackrel{\triangle}{=}N_2+(\sum_{t=0}^{N_2-1}tv_{t+1})+(\sum_{t=0}^{N_2-1}tu_{t+1})$, and

$$\widetilde{\sum}\stackrel{\triangle}{=}\sum_{k=0}^{K-1}\sum_{m=0}^{Nk}\sum_{j=0}^{N-1}\binom{K-1}{k}\binom{Nk}{m}\binom{N-1}{j}(-1)^{k+m+j}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\sum_{u_1,\ldots,u_{N_2}}^{j}\frac{m!}{v_1!\ldots v_{N_2}!}\frac{j!}{u_1!\ldots u_{N_2}!}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{u_{t+1}}}. \tag{6.9}$$

---

in better secrecy outage probabilities, non-zero achievable secrecy rates, and ergodic secrecy rates. For this selection, we use a training symbol which has the same statistical properties as $\boldsymbol{x}$, and assume a quasi-stationary channel during its operation.

Next, the corresponding CDF and PDF for a link from a particular relay to a group of eavesdroppers will be derived. We start the derivation for the CDF of $\gamma_2^{k,\max}$, which is given by

$$F_{\gamma_2^{k,\max}}(x) = \left[1-e^{-x/\tilde{\alpha}_2}\sum_{l=0}^{N_2-1}\frac{1}{l!}\left(\frac{x}{\tilde{\alpha}_2}\right)^l\right]^N\mathrm{U}(x) \tag{6.7}$$

where we assume that channels between a particular relay and N eavesdroppers are independent and identically distributed (i.i.d.).

Since $\{\gamma_2^{1,\max},\cdots,\gamma_2^{K,\max}\}$ is a set of i.i.d. continuous random variables, the PDF of $\gamma_2^{\min,\max}\stackrel{\triangle}{=}\gamma_2^{k^*,\max}\stackrel{\triangle}{=}\min(\gamma_2^{1,\max},\cdots,\gamma_2^{K,\max})$ can be derived in the following lemma.

Lemma 1. *For the i.i.d. frequency selective fading channels between a particular relay and a group of eavesdroppers, the PDF of* $\gamma_2^{\min,\max}$ *is given by* (6.8).

Proof. A proof of this lemma is provided in Appendix C.1. □

For the i.i.d. frequency selective fading channels between a particular relay and a group of Q destinations, the CDF of $\gamma_1^{k^*,q^*} \triangleq \max(\gamma_1^{k^*,1}, ..., \gamma_1^{k^*,Q})$ is given by

$$F_{\gamma_1^{k^*,q^*}}(x) = \left[1 - e^{-x/\tilde{\alpha}_1} \sum_{l=0}^{N_1-1} \frac{1}{l!}\left(\frac{x}{\tilde{\alpha}_1}\right)^l\right]^Q \mathrm{U}(x). \tag{6.10}$$

6.4 Performance Analysis of the Physical Secrecy System

The instantaneous secrecy rate is expressed as [28]

$$C_s = \frac{1}{2}[\log_2(1+\gamma_1^{k^*,q^*}) - \log_2(1+\gamma_2^{\min,\max})]^+ \tag{6.11}$$

where $\log_2(1+\gamma_1^{k^*,q^*})$ is the instantaneous capacity of the channel between the chosen relay and the selected destination, whereas $\log_2(1+\gamma_2^{\min,\max})$ is the instantaneous capacity of the wiretap channel between the selected relay and the eavesdropper group. Having obtained PDFs and CDFs of SNRs achieved by the two-stage relay and destination selection scheme, the secrecy outage probability, the probability of non-zero achievable secrecy rate, and the ergodic secrecy rate will be derived. Then, an asymptotic analysis of the secrecy outage probability will be developed to see the asymptotic behavior of the system.

6.4.1 Secrecy Outage Probability

According to [152], the secrecy outage probability for a given secure rate, R, is given by

$$P_{\text{out}} = Pr(C_s < R) = \int_0^\infty F_{\gamma_1^{k^*,q^*}}(2^{2R}(1+\gamma)-1) f_{\gamma_2^{\min,\max}}(\gamma) d\gamma. \tag{6.12}$$

A closed-form expression of (6.12) is provided by the following theorem.

Theorem 1. *The secrecy outage probability of the single carrier system employing the*

proposed relay selection scheme in frequency selective fading is given by

$$P_{\text{out}} = C\widetilde{\sum}\sum_{q=0}^{Q}\binom{Q}{q}(-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}}\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}$$
$$\sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p\left(\frac{qJ_R}{\tilde{\alpha}_1}+\beta_2\right)^{-(p+\tilde{N}_2)}(p+\tilde{N}_2-1)! \tag{6.13}$$

where $J_R \triangleq 2^{2R}$ *and* $\tilde{L}_1 \triangleq \sum_{t=0}^{N_1-1} tw_{t+1}$.

Proof. A detailed derivation is provided in Appendix C.2. □

To explicitly see the secrecy diversity gain, we provide an asymptotic expression for (6.13) in the following theorem.

Theorem 2. *The asymptotic secrecy outage probability at a fixed* $\tilde{\alpha}_2$ *is given by*

$$P_{\text{out}}^{\infty} \triangleq \lim_{\tilde{\alpha}_1\to\infty} P_{\text{out}} = (G_a\tilde{\alpha}_1)^{-QN_1} + O\left((\tilde{\alpha}_1)^{-QN_1}\right) \tag{6.14}$$

where the secrecy array gain is given by

$$G_a = \left[\frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}\sum_{l=0}^{QN_1}\binom{QN_1}{l}(J_R-1)^{QN_1-l}(J_R)^l(\tilde{\alpha}_2)^l\frac{(l+\tilde{N}_2-1)!}{(\hat{\beta})^{l+\tilde{N}_2}}\right]^{-\frac{1}{QN_1}} \tag{6.15}$$

with $\hat{C} \triangleq \frac{KN}{(N_2-1)!}$, $\hat{\beta} \triangleq m+j+1$, *and* $\widehat{\sum}$, *which is given by*

$$\widehat{\sum} \triangleq \sum_{k=0}^{K-1}\sum_{m=0}^{Nk}\sum_{j=0}^{N-1}\binom{K-1}{k}\binom{Nk}{m}\binom{N-1}{j}(-1)^{k+m+j}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\sum_{u_1,\ldots,u_{N_2}}^{j}\frac{m!}{v_1!\ldots v_{N_2}!}\frac{j!}{u_1!\ldots u_{N_2}!}\frac{1}{\prod_{t=0}^{N_2-1}(t!)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_2-1}(t!)^{u_{t+1}}}. \tag{6.16}$$

Proof. A detailed proof of this theorem is provided in Appendix C.3. □

This theorem shows that the secrecy diversity gain is QN_1, which is the product of the multipath diversity gain and the multiuser diversity gain achievable between the

$$Pr(C_s > 0) = 1 - \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{k=0}^{K}\sum_{m=0}^{Nk}\sum_{q=0}^{Q-1}\binom{Q-1}{q}\binom{K}{k}\binom{Nk}{m}(-1)^{q+k+m}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\sum_{w_1,\ldots,w_{N_1}}^{q}\Big(\frac{q!}{w_1!\ldots w_{N_1}!}\Big)\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}$$
$$\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}\Big(\frac{m}{\tilde{\alpha}_2}+\frac{q+1}{\tilde{\alpha}_1}\Big)^{-\tilde{N}_1}(\tilde{N}_1-1)!. \tag{6.18}$$

selected relay and the Q destinations.

Corollary 1. *When $\tilde{\alpha}_1 \to \infty, \tilde{\alpha}_2 \to \infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2} = \kappa$, then the asymptotic secrecy outage probability is given by*

$$P_{\text{out}}^{\infty} = \frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}(\kappa)^{QN_1}(J_R)^{QN_1}\frac{(QN_1+\tilde{N}_2-1)!}{(\hat{\beta})^{QN_1+\tilde{N}_2}} \tag{6.17}$$

which shows that the secrecy diversity gain is not achievable for this particular case.

6.4.2 The Probability of Non-Zero Achievable Secrecy Rate

In the following, we shall derive the probability of non-zero achievable secrecy rate.

Corollary 2. *The probability of non-zero achievable secrecy rate is provided by* (6.18)*. In* (6.18)*, we have defined $\tilde{N}_1 \triangleq N_1 + (\sum_{t=0}^{N_1-1} tw_{t+1}) + (\sum_{t=0}^{N_2-1} tv_{t+1})$.*

Proof. A proof of this corollary is provided in Appendix C.4. □

To investigate the effect of the diversity gain on the convergence behavior of the probability of non-zero achievable secrecy rate to $Pr(C_s > 0) = 1$, we derive an asymptotic probability of non-zero achievable secrecy rate. According to (C.4.3), the probability of non-zero achievable secrecy rate can be rewritten as

$$Pr(C_s > 0) = 1 - \int_0^{\infty} F_{\gamma_1^{k^*,q^*}}(x) f_{\gamma_2^{\min,\max}}(x)dx. \tag{6.19}$$

Substituting (C.3.1) and (6.8) into (6.19), we get the following asymptotic probability of non-zero achievable secrecy rate

$$Pr(C_s^{\infty} > 0) = 1 - \frac{C}{(N_1!)^Q}\left(\frac{1}{\tilde{\alpha}_1}\right)^{N_1 Q} \widetilde{\sum} \frac{(N_1 Q + \tilde{N}_2 - 1)!}{(\beta_2)^{N_1 Q + \tilde{N}_2}} \tag{6.20}$$

which shows that the multipath diversity gain and the multiuser diversity gain simultaneously affect the convergence speed of the non-zero achievable secrecy rate to $Pr(C_s > 0) = 1$. In the following, we shall derive the ergodic secrecy rate for the proposed system.

6.4.3 Ergodic Secrecy Rate

The ergodic secrecy rate is defined as the instantaneous secrecy rate C_s averaged over $\gamma_1^{j^*,q^*}$ and $\gamma_2^{\min,\max}$. As such, we formulate the ergodic secrecy rate as

$$\bar{C}_s = \int_0^{\infty}\int_0^{\infty} C_s f_{\gamma_1^{k^*,q^*}}(x_1)\, f_{\gamma_2^{\min,\max}}(x_2) dx_1 dx_2. \tag{6.21}$$

Substituting (6.11) into (6.21), and applying some algebraic manipulations, we obtain

$$\bar{C}_s = \frac{1}{2\log(2)} \int_0^{\infty} \frac{F_{\gamma_2^{\min,\max}}(x_2)}{1 + x_2} \Big(1 - F_{\gamma_1^{k^*,q^*}}(x_2)\Big) dx_2. \tag{6.22}$$

Based on the PDF of $\gamma_2^{\min,\max}$ given in (6.8), the CDF of $\gamma_2^{\min,\max}$ is given by

$$\begin{aligned} F_{\gamma_2^{\min,\max}}(x) &= \int_0^x f_{\gamma_2^{\min,\max}}(t)\, dt \\ &= C\widetilde{\sum}\left[\frac{(\tilde{N}_2 - 1)!}{(\beta_2)^{\tilde{N}_2}} - e^{-\beta_2 x} \sum_{n_1=0}^{\tilde{N}_2 - 1} \frac{(\tilde{N}_2 - 1)!}{n_1!} \frac{x^{n_1}}{(\beta_2)^{\tilde{N}_2 - n_1}}\right]. \end{aligned} \tag{6.23}$$

$$\bar{C}_s = -\frac{C}{2\log(2)}\widetilde{\sum}\sum_{q=1}^{Q}\binom{Q}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q} \frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}\left(t!(\tilde{\alpha}_1)^t\right)^{w_{t+1}}}$$
$$\Big(\frac{\Gamma(\tilde{N}_2)\Gamma(\tilde{L}_1+1)}{(\beta_2)^{\tilde{N}_2}}\Psi(\tilde{L}_1+1,\tilde{L}_1+1;q/\tilde{\alpha}_1) - \sum_{n_1=0}^{\tilde{N}_2-1}\frac{\Gamma(\tilde{N}_2)\Gamma(\tilde{L}_1+n_1+1)}{n_1!(\beta_2)^{\tilde{N}_2-n_1}}$$
$$\Psi(\tilde{L}_1+n_1+1,\tilde{L}_1+n_1+1;\beta_2+q/\tilde{\alpha}_1)\Big). \tag{6.25}$$

In addition, by employing binomial and multinomial formulas, the CDF of $\gamma_1^{k^*,q^*}$ in (6.10) can be re-expressed as

$$F_{\gamma_1^{k^*,q^*}}(x) = 1 + \sum_{q=1}^{Q}\binom{Q}{q}(-1)^q e^{-qx/\tilde{\alpha}_1}$$
$$\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{x^{\tilde{L}_1}}{\prod_{t=0}^{N_1-1}\left(t!(\tilde{\alpha}_1)^t\right)^{w_{t+1}}}. \tag{6.24}$$

Substituting (6.23) and (6.24) into (6.22), and using the confluent hypergeometric function [140, eq. (9.211.4)] given by $\Psi(\alpha,\gamma;z) = \frac{1}{\Gamma(\alpha)}\int_0^\infty e^{-zt}t^{\alpha-1}(1+t)^{\gamma-\alpha-1}dt$, we obtain the ergodic secrecy rate expressed in (6.25).

In order to gather further insight, we present the asymptotic ergodic secrecy rate. We first consider the case of $\tilde{\alpha}_1 \to \infty$ and a fixed $\tilde{\alpha}_2$, and provide the following corollary.

Corollary 3. *The asymptotic ergodic secrecy rate at $\tilde{\alpha}_1 \to \infty$ and a fixed $\tilde{\alpha}_2$ is given by* (6.26). *In* (6.26), *$\psi(\cdot)$ is the digamma function [153].*

Proof. A proof of this corollary is provided in Appendix C.5. □

With the help of (6.26), we confirm that the multiplexing gain [154] is 1/2 in bits/sec/Hz/(3 dB), which is given by

$$S^\infty = \lim_{\tilde{\alpha}_1\to\infty}\frac{\bar{C}_1^\infty}{\log_2(\tilde{\alpha}_1)} = \frac{1}{2}. \tag{6.27}$$

It is indicated from (6.27) that under these circumstances, secure communication achieves

$$\bar{C}_1^{\infty} = \frac{1}{2}\log_2(\tilde{\alpha}_1) + \frac{1}{2\log(2)}\Big[\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}[\psi(N_1+\tilde{L}_1)-\log(q+1)] + \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}(\frac{m!}{v_1!\ldots v_{N_2}!})\frac{\Gamma(\sum_{t=0}^{N_2-1} tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\Psi(\sum_{t=0}^{N_2-1} tv_{t+1}+1, \sum_{t=0}^{N_2-1} tv_{t+1}+1; m/\tilde{\alpha}_2)\Big]. \tag{6.26}$$

---

the same spectral efficiency as communication without eavesdropping. Moreover, using (6.26), we can easily calculate the additional power cost for different network parameters while maintaining a specified target ergodic secrecy rate. For example, we consider different numbers of relays K_1 and K_2 with $K_1 > K_2$. Compared to the K_1 case, the additional power cost in achieving the specified target ergodic secrecy rate in the K_2 scenario is calculated as

$$\Delta P \ (\text{dB}) = \frac{10}{\log 10}\left[\eta(K_1) - \eta(K_2)\right] \tag{6.28}$$

where

$$\eta(K) = \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}\sum_{v_1,\ldots,v_{N_2}}^{m}(\frac{m!}{v_1!\ldots v_{N_2}!})$$
$$\frac{\Gamma(\sum_{t=0}^{N_2-1} tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\Psi(\sum_{t=0}^{N_2-1} tv_{t+1}+1, \sum_{t=0}^{N_2-1} tv_{t+1}+1; m/\tilde{\alpha}_2).$$

Similarly, the additional power cost in achieving the specified target ergodic secrecy rate under different numbers of destinations or eavesdroppers can be accordingly obtained.

We next consider the case of $\tilde{\alpha}_1 \to \infty$ and $\tilde{\alpha}_2 \to \infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2} = \kappa$, and provide the following corollary.

Corollary 4. *The asymptotic ergodic secrecy rate at $\tilde{\alpha}_1 \to \infty$ and $\tilde{\alpha}_2 \to \infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2} = \kappa$*

$$\bar{C}_2^{\infty} = \frac{1}{2}\log_2(\kappa) + \frac{1}{2\log(2)}\Big[\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}[\psi(N_1+\tilde{L}_1)-\log(q+1)] - \hat{C}\widehat{\sum}\frac{\Gamma(\tilde{N}_2)}{(\hat{\beta})^{\tilde{N}_2}}[\psi(\tilde{N}_2)-\log(\hat{\beta})]\Big]. \quad (6.29)$$

is given by (6.29).

Proof. A proof of this corollary is provided in Appendix C.6. □

It is indicated from (6.29) that a capacity ceiling exists in this case.

6.4.4 The Effects of Multiple Antennas at the Eavesdroppers

We shall investigate the effect of multiple antennas at the eavesdroppers. Using MRC at each eavesdropper, the received signal expressed in (1) becomes

$$\boldsymbol{r}^{k,n} = \sqrt{P_s\alpha_2^{k,n}}\sum_{r=1}^{M}(\tilde{\boldsymbol{H}}_r^{k,n})^H\boldsymbol{H}_r^{k,n}\boldsymbol{x} + \sum_{r=1}^{M}(\tilde{\boldsymbol{H}}_r^{k,n})^H\boldsymbol{n}_1^{k,n} \quad (6.30)$$

where $\boldsymbol{H}_r^{k,n}$ is the right circulant matrix formed for a link from the kth relay to the rth receive antenna branch at the nth eavesdropper. In the formulation of (6.30), we assume M antennas at the each eavesdropper, and $\alpha_2^{k,n}$ is independent of the antenna branches. In addition, $\tilde{\boldsymbol{H}}_r^{k,n}$ is the receive matrix for the rth receive antenna branch at the nth eavesdropper. The maximum instantaneous post-processing SNR due to MRC, which is imposes $\tilde{\boldsymbol{H}}_r^{k,n} = \boldsymbol{H}_r^{k,n}$, becomes [135]

$$\gamma_2^{k,n,\mathrm{eMRC}} = \frac{P_s\alpha_2^{k,n}\sum_{r=1}^{M}\|\boldsymbol{h}_r^{k,n}\|^2}{\sigma_n^2}. \quad (6.31)$$

$$P_{\text{out}}^{\text{eMRC}} = C^{\text{eMRC}}\widetilde{\sum}^{\text{eMRC}} \sum_{q=0}^{Q} \binom{Q}{q}(-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}} \sum_{w_1,\ldots,w_{N_1}}^{q} \frac{q!}{w_1!\ldots w_{N_1}!} \frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}$$

$$\sum_{p=0}^{\tilde{L}_1} \binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p\big(\frac{qJ_R}{\tilde{\alpha}_1}+\beta_2\big)^{-(p+\tilde{N}_2^{\text{eMRC}})}(p+\tilde{N}_2^{\text{eMRC}}-1)!,$$

$$Pr(C_s^{\text{eMRC}}>0) = 1 - \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{k=0}^{K}\sum_{m=0}^{Nk}\sum_{q=0}^{Q-1}\binom{Q-1}{q}\binom{K}{k}\binom{Nk}{m}(-1)^{q+k+m}$$

$$\sum_{v_1,\ldots,v_{MN_2}}^{m}\big(\frac{m!}{v_1!\ldots v_{MN_2}!}\big)\sum_{w_1,\ldots,w_{N_1}}^{q}\big(\frac{q!}{w_1!\ldots w_{N_1}!}\big)\frac{1}{\prod_{t=0}^{MN_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}$$

$$\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}\big(\frac{m}{\tilde{\alpha}_2}+\frac{q+1}{\tilde{\alpha}_1}\big)^{-\tilde{N}_1}(\tilde{N}_1-1)!, \text{ and}$$

$$\bar{C}_s^{\text{eMRC}} = -\frac{1}{2\log(2)}C^{\text{eMRC}}\widetilde{\sum}^{\text{eMRC}}\sum_{q=1}^{Q}\binom{Q}{q}(-1)^q\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}\left(t!(\tilde{\alpha}_1)^t\right)^{w_{t+1}}}$$

$$\Big[\frac{\Gamma(\tilde{N}_2^{\text{eMRC}})\Gamma(\tilde{L}_1+1)}{(\beta_2)^{\tilde{N}_2^{\text{eMRC}}}}\Psi(\tilde{L}_1+1,\tilde{L}_1+1;q/\tilde{\alpha}_1) - \sum_{n_1=0}^{\tilde{N}_2^{\text{eMRC}}-1}\frac{\Gamma(\tilde{N}_2^{\text{eMRC}})\Gamma(\tilde{L}_1+n_1+1)}{n_1!(\beta_2)^{\tilde{N}_2^{\text{eMRC}}-n_1}}$$

$$\Psi(\tilde{L}_1+n_1+1,\tilde{L}_1+n_1+1;\beta_2+q/\tilde{\alpha}_1)\Big]. \tag{6.33}$$

Comparing to the expression in (6.2), we can easily see that

$$\gamma_2^{k,n,\text{eMRC}} = \tilde{\alpha}_2^{k,n}\sum_{r=1}^{M}\|\boldsymbol{h}_r^{k,n}\|^2 \ \sim \chi^2(2N_2M,\tilde{\alpha}_2^{k,n}). \tag{6.32}$$

Using the statistical properties of $\gamma_2^{k,n,\text{eMRC}}$, the performance metrics, such as the secrecy outage probability, the probability of non-zero achievable secrecy rate, and the ergodic secrecy rate can be derived. Their corresponding expressions are given by (6.33) at the bottom of the previous page. In (6.33), we have defined $C^{\text{eMRC}} \triangleq C\Big|_{N_2\to MN_2}$, $\widetilde{\sum}^{\text{eMRC}} \triangleq \widetilde{\sum}\Big|_{N_2\to MN_2}$, and $\tilde{N}_2^{\text{eMRC}} \triangleq MN_2 + (\sum_{t=0}^{MN_2-1} tv_{t+1}) + (\sum_{t=0}^{MN_2-1} tu_{t+1})$.

Corollary 5. *The multiple antennas employed in the form of MRC at each eavesdropper do not influence the secrecy diversity gain. They can only change the secrecy array gain.*

Proof. According to Theorem 2, the asymptotic secrecy outage probability at a fixed $\tilde{\alpha}_2$ is given by

$$P_{\text{out}}^{\infty,\text{eMRC}} = (G_a^{\text{eMRC}}\tilde{\alpha}_1)^{-QN_1} + O((\tilde{\alpha}_1)^{-QN_1}) \tag{6.34}$$

where

$$G_a^{\text{eMRC}} = \left[\frac{\hat{C}^{\text{eMRC}}}{(N_1!)^Q}\widehat{\sum}^{\text{eMRC}} \sum_{l=0}^{QN_1}\binom{QN_1}{l}(J_R-1)^{QN_1-l} (J_R)^l(\tilde{\alpha}_2)^l\frac{(l+\tilde{N}_2^{\text{eMRC}}-1)!}{(\hat{\beta})^{l+\tilde{N}_2^{\text{eMRC}}}}\right]^{-\frac{1}{QN_1}} \tag{6.35}$$

with $\hat{C}^{\text{eMRC}} \triangleq \hat{C}\Big|_{N_2\to MN_2}$ and $\widehat{\sum}^{\text{eMRC}} \triangleq \widehat{\sum}\Big|_{N_2\to MN_2}$, where $\hat{C}$ and $\widehat{\sum}$ are specified in (6.16). From (6.34), we can readily see that MRC at the each eavesdropper does not affect the secrecy diversity gain. □

Corollary 6. *The multiple antennas employed in the form of MRC at the eavesdroppers do not influence the multiplexing gain. They can only change the additional power cost for a specified target ergodic secrecy rate.*

Proof. According to Corollary 3, the asymptotic ergodic secrecy rate at a fixed $\tilde{\alpha}_2$ is given by only interchanging the parameter $N_2 \to MN_2$. From (6.27), we see that the multiplexing gain is still 1/2, and MRC at the eavesdroppers impacts the additional power cost as shown in (6.28). □

6.5 Simulation Results

For the simulations, we use BPSK modulation. The transmission block size is formed by 64 BPSK symbols. The CP length is given by 16 BPSK symbols. Every channel vectors are generated by $\boldsymbol{h}^{k,n} \sim CN(\mathbf{0}, \boldsymbol{I}_{N_2}), \forall k, n$ and $\boldsymbol{g}^{k,q} \sim CN(\mathbf{0}, \boldsymbol{I}_{N_1}), \forall k, q$. The curves obtained via actual link simulations are denoted by **Ex**, whereas analytically derived

curves are denoted by **An**. Asymptotically obtained curves are denoted by **As** in the following figures.

6.5.1 Secrecy Outage Probability

Figures 6.2-6.4 show the secrecy outage probability for various scenarios. Figure 6.2 shows the secrecy outage probability for various values of N_1 at fixed values of $(K = 4, N = 2, N_2 = 3, Q = 1, M = 1, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB. As Theorem 2 proves, a lower secrecy outage probability is achieved by a bigger value of N_1. In this particular scenario, the secrecy diversity gain becomes N_1. We can see exact matches between the analytically derived curves and the simulation obtained curves for the outage probability.

Figure 6.3 shows the secrecy outage probability for various values of Q and M at fixed value of $(K = 4, N = 2, N_1 = 3, N_2 = 2, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB. We can observe the

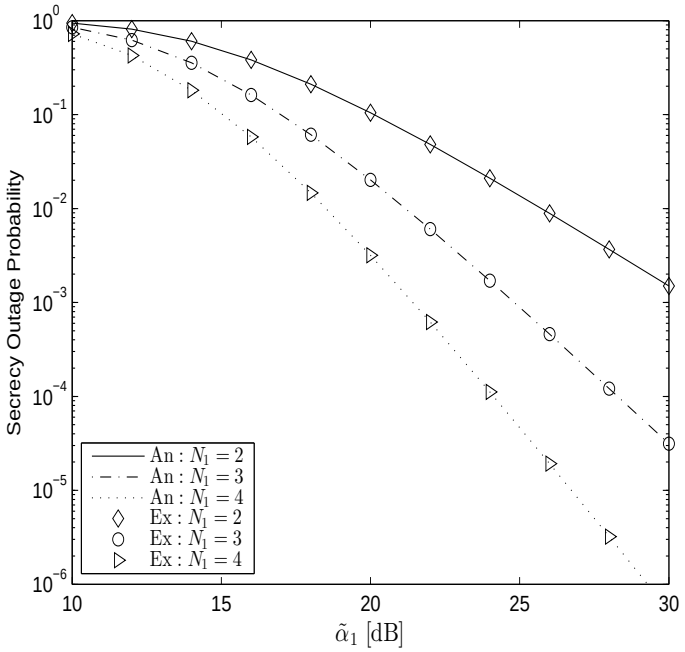

Figure 6.2: Secrecy outage probability for various values of N_1 at fixed values of $(N_2 = 3, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB.

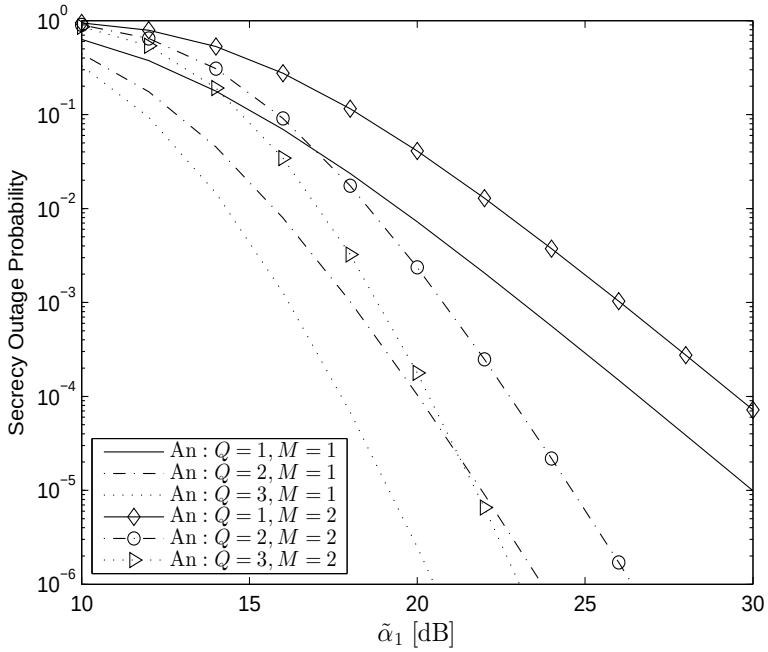

Figure 6.3: Secrecy outage probability for various values of Q and M at fixed values of $(N_1 = 3, N_2 = 2, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB.

effect of the multiuser diversity gain on the secrecy outage probability. As Q increases, a lower secrecy outage probability is obtained due to the multiuser diversity. We can also observe the effect of multiple antennas at the eavesdroppers. For the same channel length and the number of destinations, for example, $(N_1 = 3, N_2 = 2, Q = 1, M = 1)$ has a 3 dB gain over $(N_1 = 3, N_2 = 2, Q = 1, M = 2)$ at 1×10^{-3} outage probability. Similar behavior can be observed as M becomes larger. Moreover, it can be seen that N, the number of eavesdroppers, does not change the secrecy diversity gain.

Figure 6.4 verifies the derived asymptotic secrecy outage probability at a fixed $\tilde{\alpha}_2$. As $\tilde{\alpha}_1$ increases, the asymptotic curves approaches the simulation obtained curves for various values of N_1, Q, and M. From these curves, we can see that the secrecy diversity gain is $N_1 Q$, which is determined by the multipath diversity gain, N_1, and the multiuser diversity gain, Q. It is irrespective of M. A similar overall diversity gain is obtained in [129], which does not consider eavesdroppers.

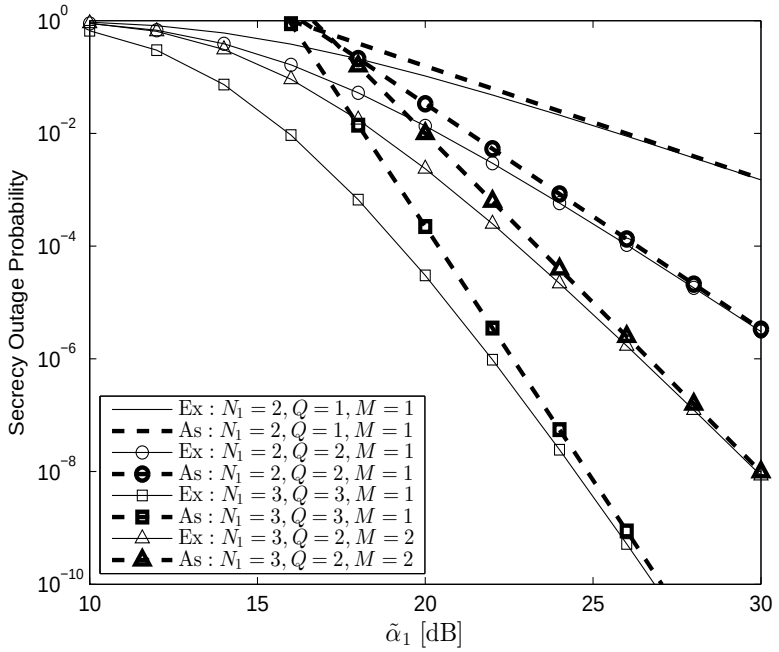

Figure 6.4: Asymptotic secrecy outage probability for various values of N_1, Q, and M at fixed values of $(N_2 = 3, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB.

6.5.2 The Probability of Non-Zero Achievable Secrecy Rate

Figure 6.5 illustrates the probability of non-zero achievable secrecy rate for various values of N_1, M, and Q. At fixed $(K = 4, N = 2)$ and $\tilde{\alpha}_2 = 5$ dB, this figure shows that $(N_1 = 2, M = 2, Q = 1)$ has the slowest convergence speed arriving at $Pr(C_{\min} > 0) = 0.999$ due to the smallest achievable diversity gain and the value of M. Although $(N_1 = 2, M = 2, Q = 1)$ has the same diversity gain as $(N_1 = 2, M = 1, Q = 1)$, its convergence speed is slowest due to greater eavesdropping capability of eavesdroppers. If we compare two particular scenarios, such as $(N_1 = 2, M = 2, Q = 1)$ and $(N_1 = 3, M = 2, Q = 1)$, then the multipath diversity is seen to be one of the key factor in determining the convergence speed, whereas by comparing $(N_1 = 2, M = 2, Q = 1)$ with $(N_1 = 2, M = 2, Q = 2)$, we can see that the multiuser diversity is another key factor in determining the convergence speed of the non-zero achievable secrecy rate.

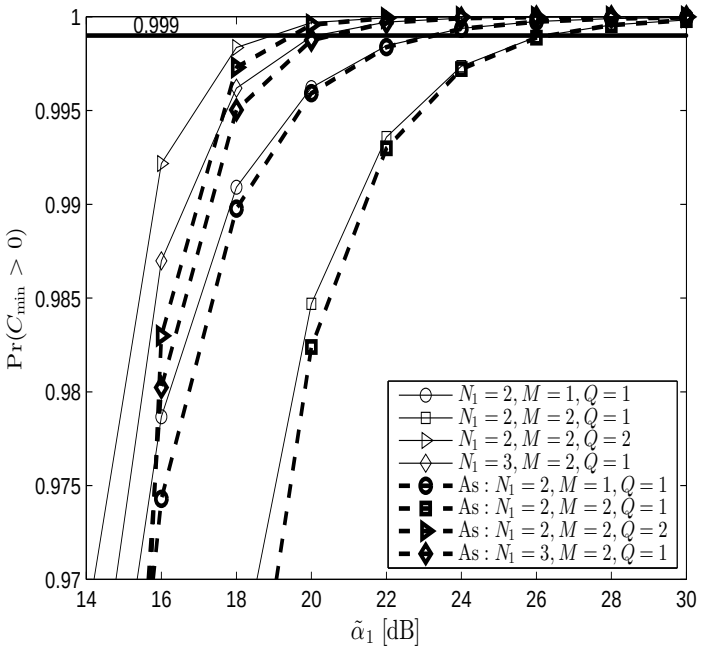

Figure 6.5: The Probability of non-zero achievable secrecy rate for various values of N_1, M, and Q at fixed values of $N_2 = 2$ and $\tilde{\alpha}_2 = 5$ dB.

6.5.3 The Ergodic Secrecy Rate

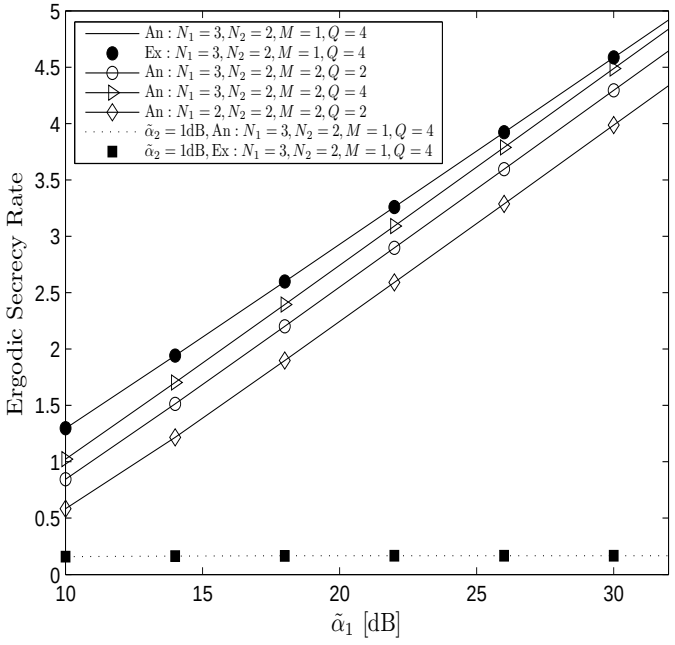

Figure 6.6: Ergodic secrecy rate for various values of (K, N_1, N_2, M, Q).

In Figure 6.6, we first compare the derived ergodic secrecy rate with the simulation obtained ergodic secrecy rate for the case of $(N_1 = 3, N_2 = 2, M = 1, Q = 4)$. We assume a fixed number of eavesdroppers $(N = 3)$ and a single relay $(K = 1)$. Perfect matchings between them can be observed. From this figure, we can compare several scenarios to investigate the effects from the system configurations and channels.

- The effect of eavesdropping: More eavesdropping reduces the ergodic secrecy rate. For example, $(N_1 = 3, N_2 = 2, M = 2, Q = 4)$ vs. $(N_1 = 3, N_2 = 2, M = 1, Q = 4)$.

- The effect of multipath diversity which is achievable between the relay and the destination: Higher multipath diversity gain results in a higher ergodic secrecy rate. For example, $(N_1 = 3, N_2 = 2, M = 2, Q = 2)$ vs. $(N_1 = 2, N_2 = 2, M = 2, Q = 2)$.

- The effect of number of destinations: With more destinations, a higher ergodic secrecy rate can be obtained due to a larger multiuser diversity gain. For example, $(N_1 = 2, N_2 = 2, M = 2, Q = 4)$ vs. $(N_1 = 2, N_2 = 2, M = 2, Q = 2)$.

- The effect of fixed $\tilde{\alpha}_2$: As Corollary 4 verified, capacity ceilings are intrinsic for this case.

In Figure 6.7, we show the asymptotic ergodic secrecy rate for various values of (K, N_1, N_2, M, Q) at a fixed number of eavesdroppers $N = 3$ and $\tilde{\alpha}_2$. This plot shows the corresponding asymptotic ergodic secrecy rate obtained from Corollary 3. As $\tilde{\alpha}_1$ increases, the differences between the analytical ergodic secrecy rates and the asymptotic ergodic secrecy rates are negligible. We can also easily see that the multipath diversity and the multiuser diversity are two key factors in determining the ergodic secrecy rates. According to (6.28), a total of five relays can reduce 0.8 dB power than a single relay in achieving 2.0 secrecy rate.

Figure 6.8 shows the multiplexing gain S^{∞} as a function of (K, N_1, Q), which are the key system and channel parameters in determining the diversity gain. As $\tilde{\alpha}_1$ increases, the multiplexing gain S^{∞} approaches 1/2. Since a larger diversity has a more influence

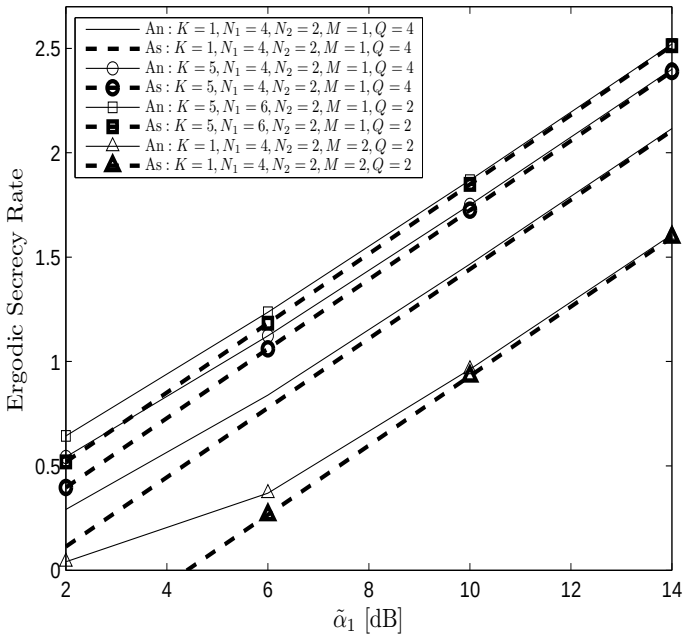

Figure 6.7: Ergodic secrecy rate for various values of N_1 and Q at fixed values of $(K = 4, N = 2)$ and $\tilde{\alpha}_2 = 1$ dB.

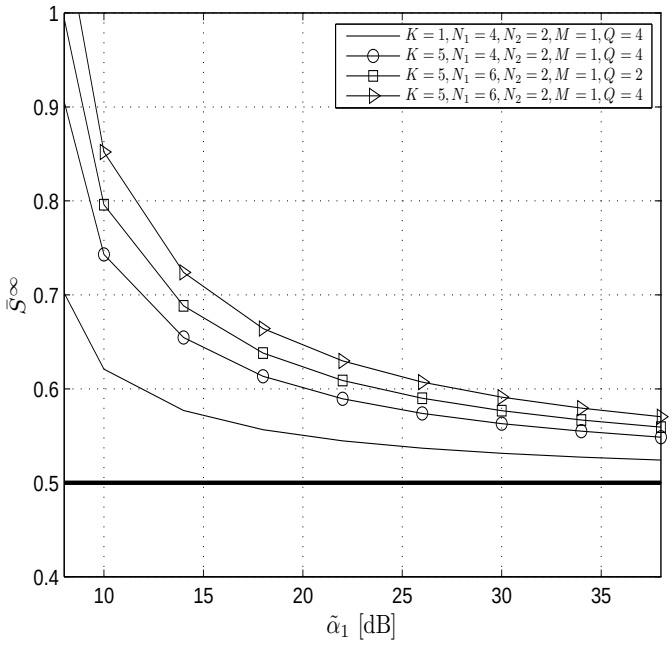

Figure 6.8: Multiplexing gain S^{∞}.

from the second term in the right hand side of (6.26), the convergence speed to 1/2 becomes slower as the diversity gain increases.

6.6 Conclusions

In this chapter, cooperative single carrier systems with multiple relays and destinations was investigated. A coexisting group of eavesdroppers have been assumed to eavesdrop the relays. For this challenging environment, we have proposed a two-stage relay and destination selection scheme: 1) relay is selected to minimize the worst-case eavesdropping, and 2) the desired destination is selected to achieve the multiuser diversity gain. We have derived the secrecy outage probability, the non-zero secrecy rate, and the ergodic secrecy rate. From the derivations and the link simulations, the diversity gain has been shown to be determined by the multipath diversity gain and the multiuser diversity gain. Having derived the asymptotic ergodic secrecy rate, the multiplexing gain has been shown to be equal to the number of hops.

Chapter 7

Secure Transmission with Optimal Power Allocation in Untrusted Relay Networks

7.1 Introduction

Security in untrusted relay networks has been paid considerable attention in the recent literature. For example, cooperative jamming (CJ) was proposed to achieve positive secrecy rate in [101, 105]. Secrecy outage performance for different relaying schemes was examined in [155]. The impact of relay antenna selection on secrecy outage probability was analyzed in [53]. The lower bound of the ergodic secrecy capacity (ESC) without optimal power allocation (OPA) was derived in [51], where single-relay and multiple-relay cases were considered.

Different from the aforementioned works, CJ with OPA is employed for securing the transmission in two-hop amplify-and-forward (AF) untrusted relay networks in this chapter. The asymptotic analysis for large number of antennas is also presented.

7.2 Mathematical Model

The implementation of CJ is considered in a half-duplex two-hop relay network consisting of a source (Alice) and a destination (Bob) communicating via an untrusted AF relay. During the first phase, while Alice transmits the information signal[1], Bob transmits the jamming signal, and the direct link between Alice and Bob is assumed to be non-existent[2]. During the second phase, the relay forwards the signals to Bob. The purpose is to quantify the impact of OPA in securing the transmission for two practical networks: 1) Alice is equipped with N_a antennas, whereas both the relay and Bob are equipped with a single antenna ($N_a{-}1{-}1$), and 2) Bob is equipped with N_b antennas, whereas both the relay and Alice are equipped with a single antenna ($1{-}1{-}N_b$). For the $N_a{-}1{-}1$ network, Alice uses the maximum-ratio transmission (MRT) beamformer to transmit the signal. For the $1{-}1{-}N_b$ network, Bob uses the MRT beamformer to transmit the jamming signal and maximum-ratio combining (MRC) to maximize the received SNR. This transceiver design at Bob can be easily achieved, particularly in reciprocal channels [51, 53]. We note that the MRT beamformer has low implementation complexity compared to other more complex beamforming designs [50]. Let $\mathbf{h}_{a,r}{\sim}\mathcal{CN}_{1\times N_a}\left(\mathbf{0}_{1\times N_a}, \Omega_{a,r}\mathbf{I}_{N_a}\right)$ denote the complex Gaussian channel vector from Alice to relay and $\mathbf{h}_{r,b}{\sim}\mathcal{CN}_{1\times N_b}\left(\mathbf{0}_{1\times N_b}, \Omega_{r,b}\mathbf{I}_{N_b}\right)$ denote the channel vector from relay to Bob. We assume a reciprocal channel between the relay and Bob [51, 53].

The instantaneous received signal-to-interference-plus-noise ratio (SINR) at the relay is given by

$$\gamma_R = \frac{\alpha\gamma_{a,r}}{(1-\alpha)\,\gamma_{r,b} + \lambda} \tag{7.1}$$

[1]Note that Alice knows the channel knowledge of the two hops, in order to determine the length of codeword.

[2]In fact, since the destination operates in half-duplex mode, it cannot receive the transmitted signal from the source while transmitting the jamming signal.

and the instantaneous end-to-end SNR at Bob is given by

$$\gamma_B = \frac{\alpha\gamma_{a,r}\gamma_{r,b}}{\alpha\gamma_{a,r} + (2-\alpha)\,\gamma_{r,b} + \lambda}, \tag{7.2}$$

where α is the power allocation factor, $\alpha \in (0, 1]$. Alice transmits the signal with power αP and Bob transmits the jamming signal with power $(1-\alpha)\,P$, where P is the total power budget in this network for each transmission. Also $\gamma_{a,r} = \|\mathbf{h}_{a,r}\|^2\gamma_0$ and $\gamma_{r,b} = \|\mathbf{h}_{r,b}\|^2\gamma_0$, where $\gamma_0 = \frac{P}{N_0}$ is the transmit SNR of this network. In (7.1) and (7.2), we note that $\lambda = 1$ accounts for the noise variance at the relay and $\lambda = 0$ does not account for the noise variance at the relay.

7.3 Optimal Power Allocation

The instantaneous secrecy rate is expressed as

$$C_s = \frac{1}{2}[\log_2(1+\gamma_B) - \log_2(1+\gamma_R)]^+, \tag{7.3}$$

where $[x]^+ = \max\{0, x\}$.

In order to facilitate analysis and gather deep insights behind this system, we consider $\lambda = 0$, as mentioned in [156]. Note that the $\lambda = 0$ case asymptotically approaches the $\lambda = 1$ case at high SNRs. The $\lambda = 0$ case also takes into account the maximum probability of eavesdropping at the relay, since the received SINR at the relay given in (7.1) becomes the signal-to-interference ratio (SIR)[3]. As such, let $\frac{\gamma_{a,r}}{\gamma_{r,b}} = \mu$, we rewrite (7.1) and (7.2) as

$$\gamma_r = \frac{\alpha\mu}{(1-\alpha)} \text{ and } \gamma_b = \frac{\alpha\mu\gamma_{r,b}}{\alpha\mu + 2 - \alpha}. \tag{7.4}$$

Our aim is to maximize the secrecy rate. Hence, we focus on optimal power allocation

[3]In a practical scenario, the noise power at the untrusted relay may not be available or accurately estimated, in this case the noise power at the relay is ignored.

(OPA). Based on (7.3) and (7.4), the OPA factor is calculated as

$$\alpha^{*}=\arg\max_{\alpha}\left\{\omega\left(\alpha\right)\right\}, \tag{7.5}$$

where $\omega\left(\alpha\right)=\frac{1+\gamma_b}{1+\gamma_r}$. Noting that $\frac{\partial^2\omega(\alpha)}{\partial\alpha^2}<0$, we take the derivative of $\omega\left(\alpha\right)$ w.r.t. α and set it to zero to obtain the OPA factor as

$$\alpha^{*}=\begin{cases}0.5-\frac{1}{\gamma_{r,b}}, \mu=1\\ \frac{2-2\mu-2\gamma_{r,b}+\sqrt{2\gamma_{r,b}}\sqrt{\Delta}}{(\mu-1)^2+(\mu-2)\gamma_{r,b}+\mu^2\gamma_{r,b}}, \mu\neq 1,\end{cases} \tag{7.6}$$

where $\Delta=1-\mu^2+\mu\gamma_{r,b}+\mu^2\gamma_{r,b}$. For large $\gamma_{r,b}$[4], based on (7.6), when $\mu=1$, $\alpha^{*}\approx 1/2$, and when $\mu\neq 1$, α^{*} can be approximated as

$$\begin{aligned}\alpha^{*}=&\frac{\frac{2-2\mu}{\gamma_{r,b}}-2+\sqrt{2}\sqrt{\frac{1-\mu^2}{\gamma_{r,b}}+\mu+\mu^2}}{(\mu-1)^2/\gamma_{r,b}+(\mu-2)+\mu^2}\\ \approx&\frac{-2+\sqrt{2}\sqrt{\mu+\mu^2}}{(\mu-2)+\mu^2}=\frac{-1+\sqrt{(\mu+\mu^2)/2}}{(\mu+\mu^2)/2-1}\\ =&\frac{1}{\sqrt{(\mu+\mu^2)/2}+1}.\end{aligned} \tag{7.7}$$

Since $\mu=1$ case also satisfies $\alpha^{*}=\frac{1}{\sqrt{(\mu+\mu^2)/2}+1}=\frac{1}{2}$, for arbitrary μ, α^{*} is approximated as

$$\alpha^{*}=\frac{1}{\sqrt{(\mu+\mu^2)/2}+1}. \tag{7.8}$$

In an effort to assess the secrecy performance, we proceed to derive the ESC with OPA and present fundamental design insights as the number of antennas grows large.

[4]From (7.4), we note that increasing $\gamma_{r,b}$ increases the end-to-end SNR at Bob and decreases the received SINR at the untrusted relay. Therefore, a larger $\gamma_{r,b}$ will improve the secrecy performance. We also note that $\gamma_{r,b}=\|\mathbf{h}_{r,b}\|^2\gamma_0$, as such $\gamma_{r,b}$ increases with either the transmit power or the number of antennas at Bob.

$$\bar{C}_s = \frac{1}{2\ln 2}\int_0^\infty \int_0^\infty \left[\ln\left(1+\frac{\alpha^*\mu x_2}{\alpha^*\mu+2-\alpha^*}\right) - \ln\left(1+\frac{\alpha^*\mu}{(1-\alpha^*)}\right)\right] \times x_2 f_{\gamma_{a,r}}(\mu x_2)\, f_{\gamma_{r,b}}(x_2)\, d\mu dx_2. \quad (7.11)$$

7.4 Ergodic Secrecy Capacity

The ESC describes the maximum of the average achievable secrecy rate, which is formulated as [35]

$$\bar{C}_s = \mathrm{E}\{C_s\} = \int_0^\infty \int_0^\infty C_s f_{\gamma_{a,r}}(x_1)\, f_{\gamma_{r,b}}(x_2) dx_1 dx_2, \quad (7.9)$$

where $\mathrm{E}\{x\}$ is the expectation of x, $f_{\gamma_{a,r}}(x_1)$ is the probability density function (PDF) of $\gamma_{a,r}$, and $f_{\gamma_{r,b}}(x_2)$ is the PDF of $\gamma_{r,b}$. Using the integration by substitution [140, eq. (4.601.1)], the ESC in (7.9) is re-expressed as

$$\bar{C}_s = \int_0^\infty \int_0^\infty C_s x_2 f_{\gamma_{a,r}}(\mu x_2)\, f_{\gamma_{r,b}}(x_2) d\mu dx_2. \quad (7.10)$$

Substituting (7.3) and (7.4) into (7.10), we obtain the ESC with OPA given in (7.11). Note that (7.11) is the asymptotic ESC expression at high SNRs when the noise variance at the relay is used ($\lambda = 1$). From (7.6) and (7.11), we find that it is intractable to further simplify the ESC expression in (7.11). To gain more insights, we derive new compact expressions for the ESC at high SNRs. We also quantify the impact of large scale antennas on the ESC for the $N_a{-}1{-}1$ and $1{-}1{-}N_b$ networks.

7.4.1 $N_a{-}1{-}1$

In this network, Alice is equipped with N_a antennas and uses the MRT beamformer to transmit the signal.

7.4.1.1 High SNR Analysis

We obtain a simple yet accurate expression for the asymptotic ESC as

$$\bar{C}_s^{asy} = \frac{1}{2\ln 2}\left[\ln \bar{\gamma}_{a,r} + \psi\left(N_a\right) - N_a \frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}} \int_0^{\infty} \varphi\left(\mu\right) \mu^{N_a - 1} \left(\mu + \frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}}\right)^{-(N_a+1)} d\mu\right], \quad (7.12)$$

where $\bar{\gamma}_{a,r} = \Omega_{a,r}\gamma_0$, $\bar{\gamma}_{r,b} = \Omega_{r,b}\gamma_0$, $\psi\left(N_a\right) = -C + \sum_{n=1}^{N_a-1} \frac{1}{n}$ with Euler's constant C [140, eq. (8.365)], and $\varphi\left(\mu\right) = \ln\left(1 + 3\mu + 2\sqrt{2\left(\mu + \mu^2\right)}\right)$. A detailed derivation of (7.12) is provided in Appendix D.1. From (7.12), we find that ESC is an increasing function of the transmit SNR γ_0. Moreover, using (7.12), we can easily calculate and compare the transmit power costs for different network parameters, while maintaining a specified target ESC.

7.4.1.2 Large N_a Analysis

By substituting (7.8) into (7.4), we obtain

$$\gamma_r = \frac{1}{\sqrt{\left(\mu^{-1} + 1\right)/2}}, \quad \gamma_b = \frac{\gamma_{r,b}}{1 + \sqrt{2\left(1 + 1/\mu\right)} + 1/\mu}. \quad (7.13)$$

For large N_a, $\mu = \frac{\gamma_{a,r}}{\gamma_{r,b}} = \frac{\|\mathbf{h}_{a,r}\|^2}{\|h_{r,b}\|^2} \gg 1$, and hence $1/\mu \approx 0$. Therefore, (7.13) reduces to

$$\gamma_r = \sqrt{2} \text{ and } \gamma_b = \frac{\gamma_{r,b}}{1 + \sqrt{2}}. \quad (7.14)$$

Based on (7.14), we have

$$\begin{aligned} \bar{C}_s &= \frac{1}{2}\mathrm{E}\left\{\log_2\left(1 + \frac{\gamma_{r,b}}{1+\sqrt{2}}\right) - \log_2\left(1 + \sqrt{2}\right)\right\} \\ &= \frac{1}{2\ln 2}\int_0^{\infty} \frac{1 - F_{\gamma_{r,b}}\left(x\right)}{1 + \sqrt{2} + x} dx - \frac{1}{2}\log_2\left(1 + \sqrt{2}\right) \\ &= -\frac{e^{\vartheta}}{2\ln 2}\mathrm{Ei}\left(-\vartheta\right) - \frac{1}{2}\log_2\left(1 + \sqrt{2}\right), \end{aligned} \quad (7.15)$$

where $F_{\gamma_{r,b}}(x) = 1 - e^{-x/\bar{\gamma}_{r,b}}$ is the cumulative distribution function (CDF) of $\gamma_{r,b}$, $\vartheta = \left(1+\sqrt{2}\right)/\bar{\gamma}_{r,b} = \left(1+\sqrt{2}\right)/\left(\Omega_{r,b}\gamma_0\right)$, and $\mathrm{Ei}(x)$ is the exponential integral function [140, eq. (8.211.1)]. As indicated by (7.15), the ESC is entirely determined by the average channel gain of the second hop and the transmit SNR of the network. We also find that increasing the number of antennas at Alice has no impact on the ESC when N_a is large.

7.4.2 $1-1-N_b$

In this network, Bob is equipped with N_b antennas and uses the MRT beamformer to transmit the jamming signal to confound the untrusted relay. Upon receiving the signal from the relay, Bob first cancels the jamming signal, then uses MRC to maximize the received SNR.

7.4.2.1 High SNR Analysis

We derive a compact expression for the asymptotic ESC as

$$\bar{C}_s^{asy} = \frac{1}{2\ln 2}\left[\left(\ln\bar{\gamma}_{a,r} - C\right) - \frac{\bar{\gamma}_{r,b}N_b}{\bar{\gamma}_{a,r}}\int_0^\infty \varphi(\mu)\left(\frac{\mu\bar{\gamma}_{r,b}}{\bar{\gamma}_{a,r}}+1\right)^{-(N_b+1)} d\mu\right]. \tag{7.16}$$

7.4.2.2 Large N_b Analysis

Recall that $\mu = \frac{\|h_{a,r}\|^2}{\|\mathbf{h}_{r,b}\|^2}$. For large N_b, $\mu \ll 1$. Based on (7.13) and (**??**), we obtain

$$\gamma_r = \frac{\sqrt{2\mu}}{\sqrt{1+\mu}} \approx \sqrt{2\mu} \text{ and} \tag{7.17}$$

$$\gamma_b = \frac{\mu\gamma_{r,b}}{\mu + \sqrt{2\left(\mu^2+\mu\right)+1}} \approx \mu\gamma_{r,b} = \gamma_{a,r}. \tag{7.18}$$

As such, we have

$$\begin{aligned}\bar{C}_s =&\frac{1}{2}\mathrm{E}\left\{\log_2\left(1+\gamma_{a,r}\right)-\log_2\left(1+\sqrt{2\mu}\right)\right\}\\ =&\frac{1}{2\ln 2}\int_0^\infty \ln\left(1+x\right) f_{\gamma_{a,r}}\left(x\right)dx-\frac{1}{2\ln 2}\times\\ &\int_0^\infty\int_0^\infty x_2\ln\left(1+\sqrt{2\mu}\right) f_{\gamma_{a,r}}\left(\mu x_2\right) f_{\gamma_{r,b}}\left(x_2\right)d\mu dx_2\\ =&-\frac{e^{1/\bar{\gamma}_{a,r}}}{2\ln 2}\mathrm{Ei}\left(-1/\bar{\gamma}_{a,r}\right)-\frac{1}{2\ln 2}\int_0^\infty\left(\frac{\bar{\gamma}_{r,b}t^2}{2\bar{\gamma}_{a,r}}+1\right)^{-N_b}(1+t)^{-1}dt. \end{aligned}\tag{7.19}$$

From (7.19), we see that the ESC increases with increasing number of antennas at Bob. For very large antennas, i.e., $N_b\to\infty$, $\gamma_r\approx 0$, (7.19) reduces to

$$\bar{C}_s=-\frac{e^{1/\bar{\gamma}_{a,r}}}{2\ln 2}\mathrm{Ei}\left(-1/\bar{\gamma}_{a,r}\right). \tag{7.20}$$

It is indicated by (7.20) that ESC only depends on the average channel gain of the first hop and the transmit SNR of the network when N_b is very large.

7.5 Numerical Results

In this section, we present numerical examples for the ESC with OPA to illustrate the N_a-1-1 and $1-1-N_b$ networks. We assume that $\Omega_{a,r}=\Omega_{r,b}=1$. In our examples, 'o' are Monte Carlo simulations with OPA factor given by (7.6) and '+' are Monte Carlo simulations with approximate OPA factor given by (7.8). The solid and dash lines represent the large system analysis and high SNR approximation, respectively. For comparison, we set $\alpha=0.5$ for equal power allocation (EPA).

Figure 7.1 shows ESC versus γ_0 for N_a-1-1. Compared with EPA, OPA can achieve perfect secrecy with some positive secrecy rate, even at low SNRs. The simplified OPA factor in (7.8) can well match those obtained from the exact calculation in (7.6). The asymptotic curves obtained from (7.12) well approximate the Monte Carlo simulations in the high SNR regime. Moreover, our large system analysis in (7.15) well assess the

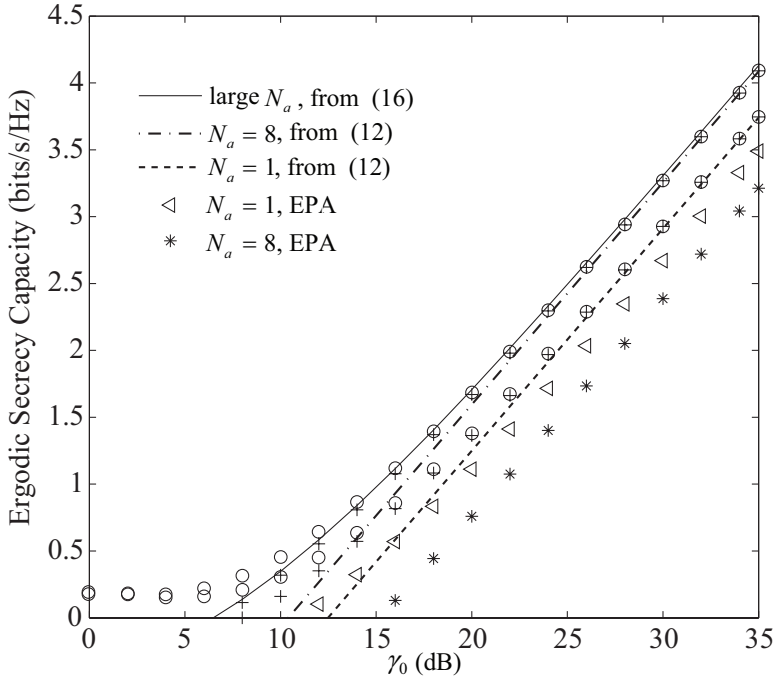

Figure 7.1: Ergodic secrecy capacity versus γ_0 for $N_a - 1 - 1$.

secrecy performance limit with large antennas. It is interesting to note that under OPA, increasing antennas improve the ESC, this however is not the case for EPA. Under EPA, ESC decreases with increasing antennas. This is due to the fact that increasing N_a helps the untrusted relay to increase the probability of successful eavesdropping. In such a scenario, more power should be allocated to the jamming signal.

Figure 7.2 shows ESC versus γ_0 for $1 - 1 - N_b$. The simplified OPA factor in (7.8) well approximates the exact OPA factor in (7.6). The asymptotic curves obtained from (7.16) are in precise agreement with Monte Carlo simulations in the high SNR regime. The theoretical result in (7.19) tightly predicts the ESC with large N_b. As expected from (7.19), the ESC increases with N_b. We also see that the ESC with EPA increases with increasing antennas. The reason is that strengthening the jamming signal reduces the eavesdropping.

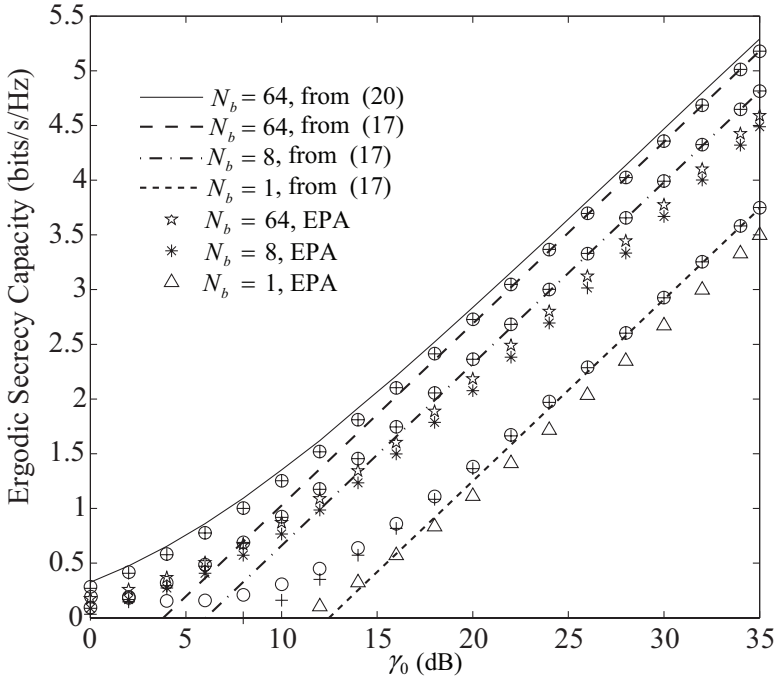

Figure 7.2: Ergodic secrecy capacity versus γ_0 for $1-1-N_b$.

7.6 Conclusions

Cooperative jamming with optimal power allocation was examined in the two-hop untrusted relay network. The ergodic secrecy capacity was derived. Some interesting conclusions are drawn from our large system analysis as $N_a \to \infty$ and $N_b \to \infty$. For large N_a, it is shown that the ergodic secrecy capacity only depends on the average channel gain of the second hop and the transmit SNR. For very large N_b, the ergodic secrecy capacity only depends on the average channel gain of the first hop and the transmit SNR.

Chapter 8

A Stochastic Geometry Approach for Physical Layer Security in Three-Tier Wireless Sensor Networks

8.1 Introduction

The potential of using physical layer security in three-tier wireless sensor networks (WSNs) is investigated in this chapter. In three-tier WSNs, the sensors are located far from the sinks, and the relays are deployed to help the sensors forward their data to the sinks. Confidential information transmissions are intercepted by the eavesdroppers. Considering the fact that sensors are densely deployed and their locations are randomly distributed [70], stochastic geometry is implemented to model the locations of the nodes in WSNs. Such a modeling approach has been applied in heterogeneous networks [85] and cognitive radio networks [88].

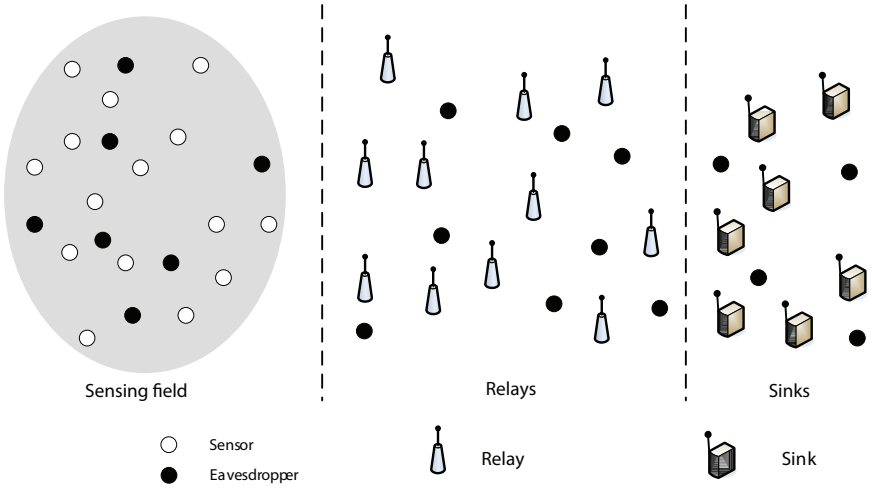

Figure 8.1: The illustration of three-tier wireless sensor networks, where the sensors transmit the sensed data to the sinks via the relays, in the presence of eavesdropping.

8.2 System Description

As shown in Figure 8.1, a three-tier wireless sensor networks is considered, where the geographically remote sensors transmit the sensed data to the sinks with the help of half-duplex decode-and-forward (DF) relays with no direct links between sensors and sinks. The eavesdroppers overhears the data transmission without modifying it. In the sensing field, sensors are randomly located according to a homogeneous Poisson point process (HPPP) $\Phi_{s,a}$ with intensity λ_s. The relays and sinks are randomly located according to independent HPPPs $\Phi_{ap,a}$ and Φ_{sk} with intensities λ_{ap} and λ_{sk}, respectively. Since the sensors may transmit data intermittently, the activity probability of sensor that is triggered to transmit the data is denoted as ρ_s $(0 < \rho_s < 1)$, and the activity probability of relay that forwards the data to the sink is denoted as ρ_{ap} $(0 < \rho_{ap} < 1)$. Non-colluding eavesdroppers are considered and eavesdroppers' locations are modeled as two independent HPPPs $\Phi_{s,e}$ and $\Phi_{ap,e}$ with intensities λ_e^s and λ_e^{ap}, respectively. The eavesdroppers in $\Phi_{s,e}$ intercept the data transmitted by the sensors and the eavesdroppers in $\Phi_{ap,e}$ intercept the data transmitted by the relays. Note that the eavesdroppers in $\Phi_{s,e}$ and in $\Phi_{ap,e}$ are far from each other.

In this three-tier network, the sensor is associated with its nearest relay and the relay is associated with its nearest sink. Each relay is equipped with M antennas, and the sensors and sinks are single-antenna nodes. To enhance the information transmission, the relays use maximal-ratio combining (MRC) to receive the sensors' data signals and maximal-ratio transmission (MRT) beamformer to transmit the signals. The wireless channels are modeled as independent quasi-static Rayleigh fading. For an arbitrary typical sensor o, the receive signal-to-interference-plus-noise ratio (SINR) after MRC at its corresponding typical relay is given by

$$\gamma_{ap} = \frac{\|\mathbf{h}_{s_0,ap_0}\|^2 |X_{s_0,ap_0}|^{-\alpha}}{\underbrace{I_{s,ap} + I_{ap,ap}}_{In_{ap}} + \delta^2/P_s}, \tag{8.1}$$

where $I_{s,ap} = \sum_{i\in\Phi_{s,a}\setminus\{s_0\}} \left| \frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|} \mathbf{h}_{i,ap_0} \right|^2 |X_{i,ap_0}|^{-\alpha}$, $I_{ap,ap} = \mu \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}}$ $\left| \frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|} \mathbf{H}_{j,ap_0} \frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\|\mathbf{h}_{j,sk_j}\|} \right|^2 |X_{j,ap_0}|^{-\alpha}$, $\mu = P_{ap}/P_s$, $\dagger$ is the conjugate transpose. Here, $\Phi_{s,a}$ and $\Phi_{ap,a}$ are the locations of active sensors and active relays, $\mathbf{h}_{s_0,ap_0}$ and $|X_{s_0,ap_0}|$ are the channel fading vector and distance between the typical sensor and its typical relay, respectively, α is the path loss exponent, $\mathbf{h}_{i,ap_0} \in \mathcal{C}^{M\times 1}$ and $|X_{i,ap_0}|$ are the channel fading vector and distance between the sensor i and the typical relay, respectively, $\mathbf{H}_{j,ap_0}$ and $|X_{j,ap_0}|$ are the channel fading matrix and distance between the relay j and the typical relay, respectively, $\mathbf{h}_{j,sk_j} \in \mathcal{C}^{1\times M}$ is the channel fading vector between the relay j and its corresponding sink, P_s is the sensor's transmit power, P_{ap} is the relay's transmit power, and δ^2 is the noise power.

We consider the non-colluding eavesdropping scenario, in which the most detrimental eavesdropper that has the highest receive SINR dominates the secrecy rate [44]. Thus, the received SINR at the most detrimental eavesdropper in Φ_e^s for the sensor and the

relay transmission is given by

$$\gamma_{s,e} = \max_{e_k \in \Phi_{s,e}} \left\{ \frac{|h_{s_0,e_k}|^2 |X_{s_0,e_k}|^{-\alpha}}{\underbrace{I_{s,e} + I_{ap,e}}_{In_{s,e}} + \delta^2 / P_s} \right\}, \tag{8.2}$$

where $I_{s,e} = \sum_{i \in \Phi_{s,a} \setminus \{s_0\}} |h_{i,e_k}|^2 |X_{i,e_k}|^{-\alpha}$ and $I_{ap,e} = \sum_{j \in \Phi_{ap,a} \setminus \{ap_0\}} \mu \left| \mathbf{h}_{j,e_k} \frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\| \mathbf{h}_{j,sk_j} \right\|} \right|^2 |X_{j,e_k}|^{-\alpha}$, h_{s_0,e_k} and $|X_{s_0,e_k}|$ are the channel fading coefficient and distance between the typical sensor and the eavesdropper, respectively, h_{i,e_k} and $|X_{i,e_k}|$ are the channel fading coefficient and distance between sensor i and the eavesdropper, respectively, and $\mathbf{h}_{j,e_k}$ and $|X_{j,e_k}|$ are the channel fading vector and distance between the relay j and the eavesdropper, respectively.

After receiving the sensors' data, relays will forward them to the nearest sinks for data collection. In this scenario, we select an arbitrary relay as a typical node ap_0, and the received SINR at the typical sink sk_0 is given by

$$\gamma_{sk} = \frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 |X_{ap_0,sk_0}|^{-\beta}}{In_{ap,sk} + \delta^2 / P_{ap}}, \tag{8.3}$$

where $In_{ap,sk} = \sum_{j \in \Phi_{ap,a} \setminus \{ap_0\}} \left| \mathbf{g}_{j,sk_0} \frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\| \mathbf{h}_{j,sk_j} \right\|} \right|^2 |X_{j,sk_0}|^{-\beta}$, $\mathbf{g}_{ap_0,sk_0} \in \mathcal{C}^{1 \times M}$ and $|X_{ap_0,sk_0}|$ are the channel fading vector and distance between the typical relay and its typical sink, respectively, β is the path loss exponent, $\mathbf{g}_{j,sk_0} \in \mathcal{C}^{1 \times M}$ and $|X_{j,sk_0}|$ are the channel fading vector and distance between the relay j and the typical sink, and $\mathbf{h}_{j,sk_j} \in \mathcal{C}^{1 \times M}$ is the channel fading vector between the relay j and its associated sink. In this case, the received SINR at the most detrimental eavesdropper for the relay and the sink transmission is given by

$$\gamma_{ap,e} = \max_{e_k \in \Phi_{ap,e}} \left\{ \frac{\left| \mathbf{g}_{ap_0,e_k} \frac{\mathbf{g}_{ap_0,sk_0}{}^{\dagger}}{\left\| \mathbf{g}_{ap_0,sk_0} \right\|} \right|^2 |X_{ap_0,e_k}|^{-\beta}}{In_{ap,e} + \sigma^2 / P_{ap}} \right\}, \tag{8.4}$$

where $In_{ap,e} = \sum_{j \in \Phi_{ap,a} \setminus \{ap_0\}} \left| \mathbf{g}_{j,e_k} \frac{\mathbf{h}_{j,sk_k}{}^{\dagger}}{\|\mathbf{h}_{j,sk_k}\|} \right|^2 |X_{j,e_k}|^{-\beta}$, g_{ap_0,e_k} and $|X_{ap_0,e_k}|$ are the channel fading coefficient and distance between the typical relay and the eavesdropper, respectively, and $\mathbf{g}_{j,e_k}$ and $|X_{j,e_k}|$ are the channel fading vector and distance between the relay j and the eavesdropper, respectively.

8.3 Secrecy Performance Evaluations

In this section, we characterize the secrecy performance in terms of average secrecy rate and secrecy outage probability. Before exhibiting the overall secrecy performance behaviors, we evaluate the secrecy of the two different links, namely the link between the sensor and relay, and the link between the relay and sink, respectively. In doing so, we derive new analytical expressions for the average secrecy rate and secrecy outage probability, and analyze the impact of these two links on the overall secrecy performance.

8.3.1 Average Secrecy Rate between the Sensor and the relay

We evaluate the average secrecy rate based on the worst-case, i.e., the average secrecy rate is dominated by the eavesdropper with the best channel [44]. Hence, for a typical link between a typical sensor and its associated relay, the instantaneous secrecy rate is defined as [146]

$$C_s^{ap} = [C_{ap} - C_{s,e}]^+, \tag{8.5}$$

where $[x]^+ = \max\{x, 0\}$, $C_{ap} = \log_2(1 + \gamma_{ap})$ is the capacity of the channel between the typical sensor and relay, and $C_{s,e} = \log_2(1 + \gamma_{s,e})$ is the capacity of the eavesdropping channel between the typical sensor and the most detrimental eavesdropper.

$$F_{\gamma_{ap}}(\gamma_{th}) = 1 - 2\pi\lambda_{ap}(1-\rho_{ap})\int_0^\infty r\exp\left\{-\left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\right.$$
$$\left.\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)(\gamma_{th})^{\frac{2}{\alpha}}r^2 - \gamma_{th}r^\alpha\delta^2P_s - \pi\lambda_{ap}(1-\rho_{ap})r^2\right\}dr$$
$$-2\pi\lambda_{ap}(1-\rho_{ap})\sum_{m=1}^{M-1}\frac{(r^\alpha)^m}{(-1)^m}\sum\frac{1}{\prod_{l=1}^{m}m_l!l!^{m_l}}\int_0^\infty r\exp\left\{-\left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+\frac{2}{\alpha}\right)\right.$$
$$\left.\Gamma\left(1-\frac{2}{\alpha}\right)(\gamma_{th})^{\frac{2}{\alpha}}r^2 - \gamma_{th}r^\alpha\delta^2/P_s - \pi\lambda_{ap}(1-\rho_{ap})r^2\right\}$$
$$\left[-\frac{2}{\alpha}\left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)(\gamma_{th})^{\frac{2}{\alpha}}r^{(2-\alpha)} - \gamma_{th}\delta^2/P_s\right]^{m_1}$$
$$\prod_{l=2}^{m}\left[-\left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)(\gamma_{th})^{\frac{2}{\alpha}}\prod_{j=0}^{l-1}\left(\frac{2}{\alpha}-j\right)r^{2-l\alpha}\right]^{m_l}dr, \tag{8.6}$$

where $\sum_{l=1}^{m} l\cdot m_l = m.$

8.3.1.1 New Statistics

We first derive the cumulative distribution functions (CDFs) of SINRs at the typical relay and the most detrimental eavesdropper which intercepts the transmission between the typical sensor and the relay in the following **Lemma 1** and **Lemma 2**, respectively.

Lemma 1. *The CDF of SINR at the typical relay is derived as* (8.6).

Proof. See Appendix E.1. □

Lemma 2. *The CDF of SINR at the most detrimental eavesdropper which intercepts the transmission between the typical sensor and the relay is derived as*

$$F_{\gamma_{s,e}}(\gamma_{th}) = \exp\left\{-\pi\lambda_e^s\int_0^\infty\exp\left\{-\left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\pi\right.\right.$$
$$\left.\left.\Gamma(1+2/\alpha)\Gamma(1-2/\alpha)(\gamma_{th})^{\frac{2}{\alpha}}t - \delta^2\gamma_{th}t^{\alpha/2}\Big/P_s\right\}dt. \tag{8.7}$$

Proof. See Appendix E.2. □

8.3.1.2 Average Secrecy Rate

Based on our preliminary work in [152], the average secrecy rate between the sensor and the relay is the average of secrecy rate C_s^{ap} over $\gamma_{s,e}$ and γ_{ap}, which can be written as

$$\bar{C}_s^{ap} = \frac{1}{\ln 2} \int_0^{\infty} \frac{F_{\gamma_{s,e}}(x)}{1+x} (1 - F_{\gamma_{ap}}(x)) dx. \tag{8.8}$$

By substituting the CDF of γ_{ap} in (8.6) and the CDF of $\gamma_{s,e}$ in (8.7) into (8.8), we can obtain the average secrecy rate between the sensor and the relay.

Note that the derived average secrecy rate between the sensor and the relay is not in a simple form, we present the interference-limited case for the average secrecy rate with single antenna at the relay in the following corollary.

Corollary 1. *When the relays are equipped with single antenna in the interference-limited scenario, the average secrecy rate between the sensor and the relay is given by*

$$\bar{C}_s^{ap} = \frac{\pi \lambda_{ap} (1 - \rho_{ap})}{\ln 2} \int_0^{\infty} \frac{\exp\left\{-\pi \lambda_e^s / \left(\Lambda_1 x^{2/\alpha}\right)\right\}}{(1+x)\left(\Lambda_1 x^{2/\alpha} + \pi \lambda_{ap} (1 - \rho_{ap})\right)} dx, \tag{8.9}$$

where $\Lambda_1 = \left(\lambda_s \rho_s + \lambda_{ap} \rho_{ap} \mu^{\frac{2}{\alpha}}\right) \pi \Gamma(1 + 2/\alpha) \Gamma(1 - 2/\alpha)$.

8.3.2 Average Secrecy Rate between the relay and the Sink

Similar to (8.5), for a typical relay and its associated sink, the instantaneous secrecy rate is defined as

$$C_s^{sk} = [C_{sk} - C_{ap,e}]^+, \tag{8.10}$$

where $C_{sk} = \log_2(1 + \gamma_{sk})$ and $C_{ap,e} = \log_2(1 + \gamma_{ap.e})$.

8.3.2.1 New Statistics

We first derive the CDFs of SINRs at the typical sink and the most detrimental eavesdropper which intercepts the transmission between the typical relay and the sink in the following **Lemma 3** and **Lemma 4**, respectively.

Lemma 3. *The CDF of SINR at the typical sink is derived as*

$$
\begin{aligned}
F_{\gamma_{sk}}(x) = 1 - 2\pi\lambda_{sk} \int_0^{\infty} r \exp\Bigg\{ & -\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right) \\
& \Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}} r^2 - \gamma_{th} r^{\beta}\delta^2 \Big/ P_{ap} - \pi\lambda_{sk} r^2 \Bigg\} dr - 2\pi\lambda_{sk} \\
& \sum_{m=1}^{M-1} \frac{1}{(-1)^m} \sum \frac{1}{\prod_{l=1}^{m} m_l! l!^{m_l}} \int_0^{\infty} r^{\beta m+1} \exp\Bigg\{ -\lambda_{ap}\rho_{ap}\pi \\
& \Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}} r^2 - \gamma_{th} r^{\beta}\delta^2 \Big/ P_{ap} - \pi\lambda_{sk} r^2 \Bigg\} \\
& \Bigg[-\lambda_{ap}\rho_{ap}\pi\frac{2}{\beta}\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}} r^{2-\beta} - \gamma_{th} \\
& \delta^2/P_{ap} \Bigg]^{m_1} \prod_{l=2}^{m} \Bigg[-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}} \\
& \prod_{j=0}^{l-1} \left(2/\beta - j\right) r^{2-l\beta} \Bigg]^{m_l} dr. \qquad (8.11)
\end{aligned}
$$

Proof. See Appendix E.3. □

Lemma 4. *The CDF of SINR at the most detrimental eavesdropper which intercepts the transmission between the typical relay and the sensor is derived as*

$$
\begin{aligned}
F_{\gamma_{ap,e}}(x) = \exp\Bigg\{ & -\pi\lambda_e^{ap} \int_0^{\infty} \exp\Bigg\{ -\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right) \\
& \Gamma\left(1-2/\beta\right)\gamma_{th}{}^{\frac{2}{\beta}} t - \sigma^2\gamma_{th} t^{\beta/2} \Big/ P_{ap} \Bigg\} dt \Bigg\}. \qquad (8.12)
\end{aligned}
$$

Proof. See Appendix E.4. □

8.3.2.2 Average Secrecy Rate

The average secrecy rate between the relay and the sink is the average of the secrecy rate C_s^{sk} over γ_{sk} and $\gamma_{ap,e}$, which is given by

$$\bar{C}_s^{sk} = \frac{1}{\ln 2} \int_0^{\infty} \frac{F_{\gamma_{sk}}(x)}{1+x} (1 - F_{\gamma_{ap,e}}(x)) dx. \tag{8.13}$$

By substituting the CDF of γ_{sk} in (8.11) and the CDF of $\gamma_{ap,e}$ in (8.12) into (8.13), we can obtain the average secrecy rate between the relay and the sink.

Note that the derived the average secrecy rate between the relay and the sink is also not in a simple form, we present the interference-limited case for the average secrecy rate with single antenna at the relay in the following corollary.

Corollary 2. *When the relays are equipped with single antenna in the interference-limited scenario, the average secrecy rate between the relay and the sink is given by*

$$\bar{C}_s^{sk} = \frac{\pi \lambda_{sk}}{\ln 2} \int_0^{\infty} \frac{\exp\left\{-\pi \lambda_e^{ap} / \Lambda_2 x^{2/\beta}\right\}}{(1+x)\left(\Lambda_2 x^{2/\beta} + \pi \lambda_{sk}\right)} dx, \tag{8.14}$$

where $\Lambda_2 = \lambda_{ap} \rho_{ap} \pi \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta)$. *Based on* (8.14), *for a specific target average secrecy rate* $\bar{C}_0$ *between the relay and the sink, the number of sinks must satisfy*

$$\lambda_{sk} > \bar{C}_0 \Lambda_2 \frac{\ln 2}{\pi \varepsilon}, \tag{8.15}$$

where $\varepsilon = \int_0^{\infty} \frac{\exp\left\{-\pi \lambda_e^{ap} / \left(\Lambda_2 x^{2/\beta}\right)\right\}}{(1+x) x^{2/\beta}} dx$.

8.3.3 Overall Average Secrecy Rate

In this subsection, we derive the overall average secrecy rate in three-tier WSNs. The instantaneous secrecy rate is defined as $C_s = \min\left(C_s^{ap}, C_s^{sk}\right)$. As such, the overall average

secrecy rate is calculated as

$$\bar{C}_s = \int_0^\infty x f_{C_s}(x)\, dx = \int_0^\infty (1 - F_{C_s}(x)) dx, \tag{8.16}$$

where $f_{C_s}(x)$ and $F_{C_s}(x)$ is the probability density function (PDF) and the CDF of C_s, respectively. The CDF of C_s is calculated as

$$\begin{aligned} F_{C_s}(x) &= \Pr\left(\min\left(C_s^{ap}, C_s^{sk}\right) < x\right) \\ &= 1 - \Pr\left(\min\left(C_s^{ap}, C_s^{sk}\right) > x\right) \\ &= 1 - \Pr\left(C_s^{ap} > x\right) \Pr\left(C_s^{sk} > x\right) \end{aligned} \tag{8.17}$$

Substituting (8.17) into (8.16), we have

$$\bar{C}_s = \int_0^\infty \Pr\left(C_s^{ap} > x\right) \Pr\left(C_s^{sk} > x\right) dx, \tag{8.18}$$

where [152]

$$\Pr\left(C_s^{ap} > x\right) = 1 - \int_0^\infty f_{\gamma_{s,e}}(t)\, F_{\gamma_{ap}}\left(2^x (1+t) - 1\right) dt, \tag{8.19}$$

and

$$\Pr\left(C_s^{sk} > x\right) = 1 - \int_0^\infty f_{\gamma_{ap,e}}(t)\, F_{\gamma_{sk}}\left(2^x (1+t) - 1\right) dt, \tag{8.20}$$

respectively. Here, $f_{\gamma_{s,e}}$ is the derivative of $F_{\gamma_{s,e}}$ given in (8.7), and $f_{\gamma_{ap,e}}$ is the derivative of $F_{\gamma_{ap,e}}$ given in (8.12).

Unfortunately, the derived overall average secrecy rate between the sensor and the sink is not in a simple form, we present the interference-limited case for the overall average secrecy rate with no noise and single antenna at the relay in the following corollary.

Corollary 3. *When the relays are equipped with single antenna in the interference-limited scenario, the overall average secrecy rate between the sensor and the sink is given*

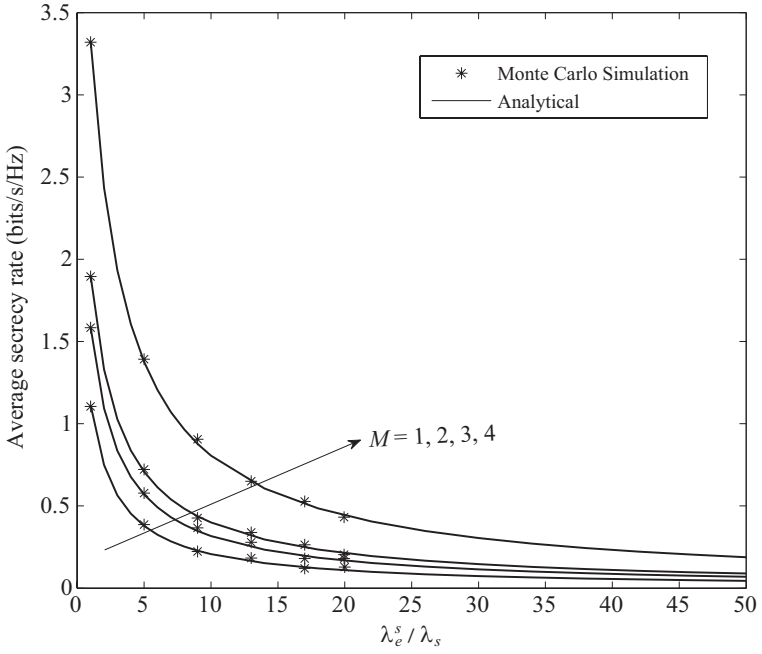

Figure 8.2: The average secrecy rate versus λ_e^s/λ_s. $\lambda_s = 10^{-2}$, $\rho_s = 0.01$, $\lambda_{ap} = 10^{-2}$, $\rho_{ap} = 0.1$, $\alpha = 3.5$, $P_s = 15$ dBm, $P_{ap} = 25$ dBm,

by

$$\bar{C}_s = \int_0^\infty \left[\int_0^\infty \frac{2\pi\lambda_e^s}{\alpha\Lambda_1 y^{2/\alpha+1}} \exp\left\{ -\pi\lambda_e^s \Big/ \left(\Lambda_1 y^{2/\alpha} \right) \right\} \right.$$

$$\left. \frac{\pi\lambda_{ap}\left(1-\rho_{ap}\right)}{\Lambda_1 (2^x\left(1+y\right)-1)^{2/\alpha} + \pi\lambda_{ap}\left(1-\rho_{ap}\right)} dy \right]$$

$$\left[\int_0^\infty \frac{2\pi^2 \lambda_e^{ap} \lambda_{sk} \exp\left\{ -\pi\lambda_e^{ap} / \Lambda_2 y^{2/\beta} \right\}}{\beta\Lambda_2 y^{2/\beta+1} \left(\Lambda_2 (2^x\left(1+y\right)-1)^{2/\beta} + \pi\lambda_{sk} \right)} dy \right] dx, \tag{8.21}$$

with $\Lambda_1 = \left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}} \right) \pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)$, $\Lambda_2 = \lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)$.

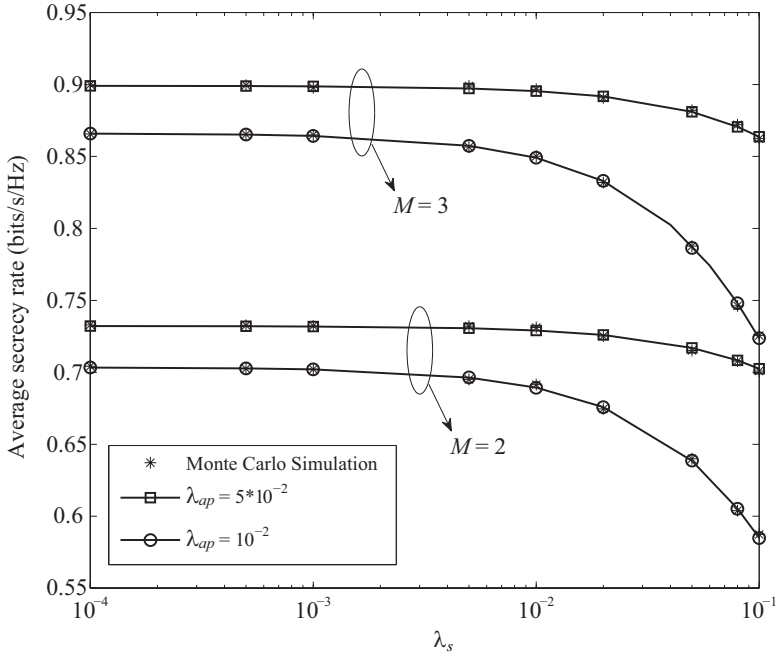

Figure 8.3: The average secrecy rate versus λ_s. $\rho_s = 0.05$, $\rho_{ap} = 0.5$, $\lambda_e^s = 10^{-3}$, $\alpha = 3.5$, $P_s = 15$ dBm, $P_{ap} = 25$ dBm,

8.4 Numerical Examples

In this section, we present numerical examples to show the average secrecy rate of three-tier WSN. We assume that the activity probability of relay $\rho_{ap} = 0.1$, the transmit power of sensor $P_s = 15$ dBm, the power spectral density of noise is -170 dBm/Hz, and the bandwidth is 1 MHz. For all figures below, we see a perfect match between the simulations and the exact analytical curves, which validate our analysis.

8.4.1 Average Secrecy Rate between the Sensor and relay

Figure 8.2 plots the average secrecy rate between the sensor and the relay versus λ_e^s/λ_s. The analytical results are obtained from (8.8). We first see that the average secrey rate decreases with increasing the density of eavesdroppers that intercepts the tranmission between sensor and relay, due to the detrimental effects of eavesdropping. We also see

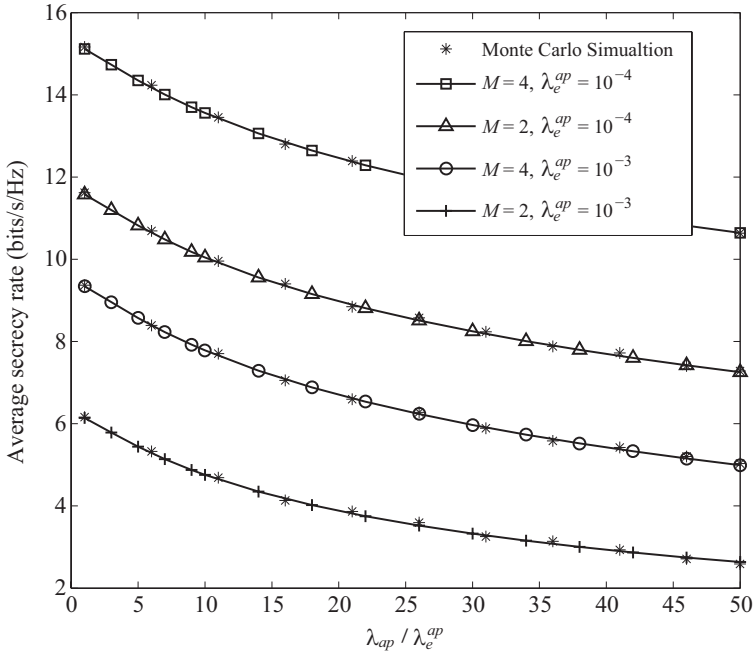

Figure 8.4: The average secrecy rate versus $\lambda_{ap}/\lambda_e^{ap}$. $\rho_{ap} = 0.1$, $\lambda_{sk} = 10^{-2}$, $\beta = 3.5$, $P_{ap} = 15$ dBm,

that the average secrecy rate increases with increasing the number of antennas at the relay, which results from the array again brought by using MRC at the relay.

Figure 8.3 plots the average secrecy rate between the sensor and the relay versus λ_s for various λ_{ap} and M. The analytical results are obtained from (8.8). An interesting observation is that for the same number of antennas M, the average secrecy rate is nearly invariable for $\lambda_s < 2 \times 10^{-3}$, since the interference from other sensors is much smaller than the interference from the active relays, and slightly increasing the interference from the sensor imposes negligible effect on the performance. However, when $\lambda_s > 2 \times 10^{-3}$, the interference from other sensors is comparable with the interference from the active relays, and increasing the interference from the sensor degrades the secrecy performance. We also observe that increasing λ_{ap} increases the average secrecy rate. This is because with more relays, the distance between the typical sensor and the typical relay becomes shorter, which improves the average secrecy rate. In additiona, we find that increasing λ_{ap} slows down the decreasing trend of average secrecy rate when λ_s increases.

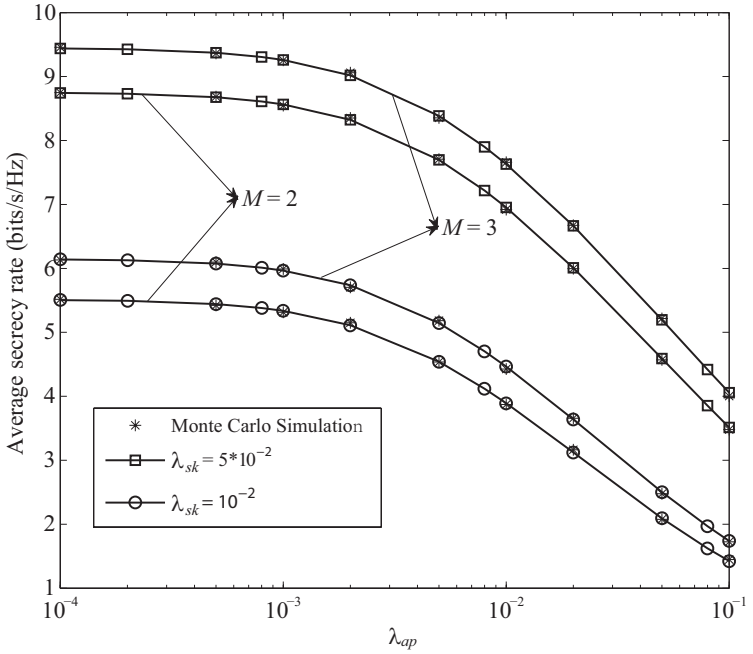

Figure 8.5: The average secrecy rate versus λ_{ap}. $\rho_{ap} = 0.1$, $\beta = 3$, $\lambda_e^{ap} = 10^{-3}$, $P_{ap} = 25$ dBm,

8.4.2 Average Secrecy Rate between the relay and Sink

Figure 8.4 plots the average secrecy rate between the relay and the sink versus $\lambda_e^{ap}/\lambda_{ap}$ for various λ_{ap} and M. The analytical results are obtained from (8.13). We first observe that the average secrecy rate decreases with increasing $\lambda_e^{ap}/\lambda_{ap}$, which indicates that more relays need to be deployed as the density of eavesdroppers increases, to combat eavesdropping. Second, with the same number of antennas at the relay, the average secrecy rate decreases with increasing λ_e^{ap}. The average secrecy rate between the relay and the sink improves with increasing the number of antennas at the relay M.

Figure 8.5 plots the average secrecy rate between the relay and the sink versus λ_{ap} for various λ_{sk} and M. The analytical results are obtained from (8.13). We observe that the average secrecy rate alters slightly for $\lambda_{ap} < 2 \times 10^{-3}$, and decreases with increasing λ_{ap} for $\lambda_{ap} > 2 \times 10^{-3}$. This can be explained by the fact that for $\lambda_{ap} < 2 \times 10^{-3}$, the interference from the active relays is relatively small compared with the

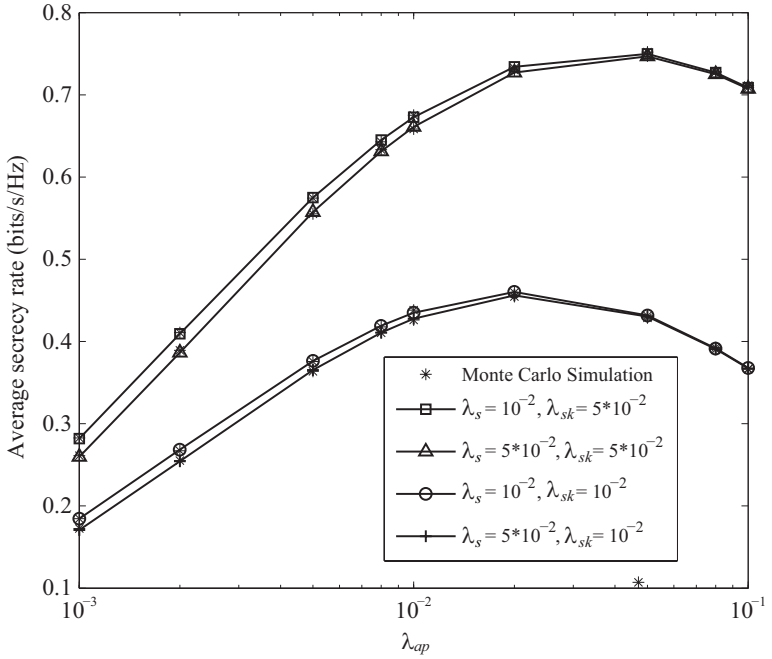

Figure 8.6: The average secrecy rate versus λ_{ap}. $P_s = 15$ dBm, $P_{ap} = 30$ dBm, $M = 2$, $\rho_s = 0.01$, $\rho_{ap} = 0.1$, $\alpha = 2.8$, $\beta = 3.2$, $\lambda_e^s = \lambda_e^{ap} = 5{*}10^{-3}$,

noise, and increasing the number of relays scarcely influence the performance. However, for $\lambda_{ap} > 2 \times 10^{-3}$, the interference from the relay imposes a dominant impact on the SINR between the relay and the sink, thus increasing the interference from the relays degrades the average secrecy rate. Another observation is that the average secrecy rate improves with increasing the density of sink, because the distance between the typical relay and the corresponding sink becomes shorter.

8.4.3 Overall Average Secrecy Rate

Figure 8.6 plots the overall average secrecy rate versus λ_{ap} for various λ_s and λ_{sk}. The analytical results are obtained from (8.18). Interestingly, we find that the overall average secrecy rate first increases, and then decreases with increasing λ_{ap}, which implies that there exists an optimal λ_{ap} to achieve the maximum average secrecy rate. This phenomenon can be well explained by the tradeoff between the benefits brought by the

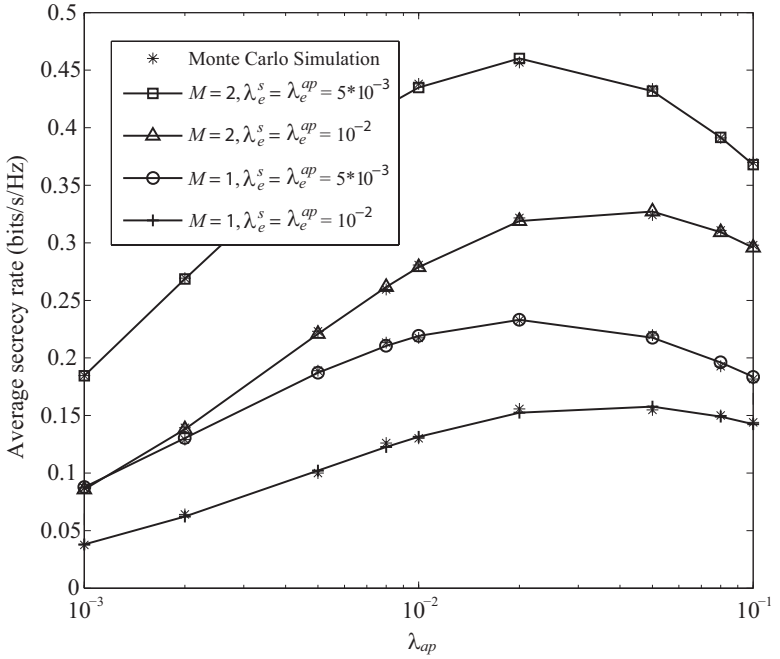

Figure 8.7: The average secrecy rate versus λ_{ap}. $P_s = 15$ dBm, $P_{ap} = 30$ dBm, $\rho_s = 0.01$, $\rho_{ap} = 0.1$, $\alpha = 2.8$, $\beta = 3.2$, $\lambda_s = \lambda_{sk} = 10^{-2}$,

shorter distance from the typical sensor to the typical relay and the detrimental effects caused by more interference from the active relays due to increasing λ_{ap}. It is also seen that the overall average secrecy rate can be improved by deploying more sinks, due to the shorter distance between the relay and the sink. It is further demonstrated that deploying more sensors in this network may not greatly degrade the average secrecy rate due to the low transmit power of sensors. More importantly, it is shown that the optimal λ_{ap} is more dependent on the λ_{sk}.

Figure 8.7 plots the overall average secrecy rate versus λ_{ap} for various λ_e^s, λ_e^{ap} and M. The analytical results are obtained from (8.18). Similar as Figure 8.6, we see that the overall average secrecy rate first increases, and then decreases with increasing λ_{ap}. As expected, the average secrecy rate decreases with increasing eavesdroppers. It is indicated that the optimal λ_{ap} for achieving the maximum average secrecy rate does not alter drastically with different λ_e^s and λ_e^{ap}.

8.5 Conclusions

Physical layer security in three-tier wireless sensor networks was introduced. The impacts of random locations and spatial densities of sensors, relays, sinks and external eavesdroppers on the secrecy performance were analyzed. New expressions for average secrecy rate were obtained. The results provide guidelines on the secure transmission in practical wireless sensor networks. Based on our analysis, the importance of using physical layer security in the three-tier wireless sensor networks was clearly established.

Chapter 9

Conclusions and Future Works

9.1 Contributions and Insights

This thesis concentrates on the physical layer security in wireless networks. There are three principal aspects in the thesis: 1) Since physical layer security exploits the properties of wireless channel such as fading, some practical channel fading have been investigated; 2) Antenna selection and opportunistic relaying technique have been utilized for security enhancement; 3) The potentials of physical layer security in the emerging networks such as cognitive radio networks, relay networks, and wireless sensor networks (WSNs) have been exploited. The main contributions and insights are as follows.

In Chapter 3, physical layer security in single-input multi-output wiretap channels under two-wave with diffuse power fading was investigated. New closed-form expressions for the exact and asymptotic average secrecy capacity and secrecy outage probability were derived. It was demonstrated that the high signal-to-noise ratio (SNR) slope is one. Particularly, the high SNR slope is not affected by the number of antennas at the legitimate receiver and eavesdropper. The impacts of the main channel and the eavesdropper's channel on the average secrecy capacity were characterized via the high SNR power offset. It is indicated that the secrecy diversity order is entirely dependent

on legitimate receiver's antennas. It also indicates that the detrimental effect of the eavesdroppers channel resides in the secrecy array gain. Furthermore, the performance gap for different number of antennas was quantified via their respective secrecy array gains.

In Chapter 4, a unified framework was presented to examine the secrecy performance for antenna selection techniques in multiple-input multiple-output (MIMO) wiretap channels. New exact closed-form expressions for the average secrecy rate and the secrecy outage probability were derived using the new cumulative distribution function and probability density function of the SNR with transmit antenna selection and generalized selection combining. It is shown that although the high SNR slope is independent of the network parameters, the high SNR power offset is dependent on the system parameters including transceiver antenna configuration and the fading parameters in the main and the eavesdropper's channels. An interesting conclusion is reached that a capacity ceiling is created when both the legitimate receiver and the eavesdropper are close to the transmitter. When the legitimate receiver is close to the transmitter, the full secrecy diversity order is achieved and is entirely determined by the antenna configuration and the fading parameters in the main channel. The impact of the eavesdropper is only reflected in the secrecy array gain. The secrecy diversity order collapses to zero when both the legitimate receiver and the eavesdropper are close to the transmitter.

In Chapter 5, fundamental questions were addressed surrounding the joint impact of two power constraints on the cognitive wiretap channel: 1) the maximum transmit power at the secondary transmitter, and 2) the peak interference power at PU. To address these constraints, new closed-form expressions for the exact and asymptotic secrecy outage probability were derived. Our expressions reveal important design insights surrounding the impact of the primary network on the secondary network in cognitive wiretap radio networks.

In Chapter 6, frequency selective fading was considered, in which multiple relays and multiple destinations coexist with a cluster of eavesdroppers. A two-stage relay

and destination selection was proposed to minimize the eavesdropping and maximize the signal power of the link between the relay and the destination. It is confirmed that the secrecy diversity gain is directly determined by the multipath diversity and the multiuser diversity between the relays and the destinations. The multiplexing gain is independent of the system and channel parameters such as the number of multipaths, relays, eavesdroppers, and destinations. Our high SNR analysis showed that when the average received power at the eavesdropper is proportional to the counterpart at the destination, both the secrecy diversity gain and the secrecy capacity slope collapse to zero, thereby creating a secrecy outage floor and a secrecy capacity ceiling.

In Chapter 7, the secure transmission with optimal power allocation (OPA) and cooperative jamming was analyzed in the two-hop amplify-and-forward untrusted relay network. Ergodic secrecy capacity (ESC) was characterized as a performance metric and compact expressions for asymptotic ESC were derived. Compared to the equal power allocation, OPA can achieve positive rate even at low SNR. For increasing antennas at source, there are no significant increase in ESC, and ESC approaches constant for moderately large antennas, which only depends on the average channel gain of the second hop and the transmit SNR of the system. For moderately large antennas at the destination, ESC increases with the number of antennas at the destination, when the number of antennas is massive, ESC only depends on the average channel gain of the first hop and the transmit SNR of the system.

In Chapter 8, a new analytical framework was presented to examine the implementation of physical layer security in three-tier WSNs. The locations and spatial densities of sensors, relays, sinks, and eavesdroppers are modeled using stochastic geometry. Each relay used the low-complexity maximal-ratio combining (MRC) to receive the sensor's data signals and maximal-ratio transmission (MRT) beamformer to transmit the signals. The secure transmissions between the active sensors and relays, and between the active access points and sinks were investigated. Using MRC/MRT at relays can enhance the secure transmission. Based on the proposed analysis and simulations, several important

observations are reached: 1) the average secrecy rate decreases as the number of sensors grows large, due to more interference from sensors, 2) the average secrecy rate increases with increasing the number of sinks, because of the shorter distances between the relays and their associated sinks, and 3) the overall average secrecy rate increases with increasing the number of relays, although it decreases the average secrecy rate between the relay and its associated sink. However, beyond a critical value, the overall average secrecy rate decreases with increasing the number of relays.

9.2 Future Works

In this subsection, two extensions of the current work are proposed. Furthermore, physical layer security in 5G networks is investigated.

9.2.1 Extensions of Current Work

9.2.1.1 Imperfect CSI

Current work in this thesis may also need to consider the impact of imperfect channel state information (CSI), although imperfect CSI wiretap channel is a challenging problem. The key performance parameters such as high SNR slope and power offset under imperfect CSI are not known and have not been examined in the existing literature.

In Chapter 5, the interference power at the primary receiver inflicted by the secondary transmitter must not exceed the maximal peak, however, this constraint may not be guaranteed under imperfect CSI [117]. New secure transmission designs may be demanded. The secrecy outage probability and average achievable secrecy rate in such scenario also need to be analyzed.

9.2.1.2 Multi-hop Secure Transmission with Trusted/Untrusted Relay

In this thesis, secure transmission was investigated in two-hop networks with external eavesdroppers (Chapters 6 and 8) and two-hop untrusted relay networks (Chapter 7). Such line of work may be extended to the multi-hop case, which is an interesting and practical research area. In [157], an multi-hop line work was considered and all the intermediate relays were assumed to be untrusted, it was shown that using the proposed transmission schedule, an end-to-end secrecy rate can be achieved in an information-theoretical way, which is independent of the number of hops. However, more research efforts are needed to fully understand this field before the application in practice.

9.2.2 Physical Layer Security in 5G Systems

Massive MIMO and millimeter wave (mmWave) are two promising techniques in 5G networks. The investigation of physical layer security in massive MIMO and mmWave systems is an appealing and highly rewarding research field.

9.2.2.1 Massive MIMO

Massive MIMO systems are emerging as a new research field and have attracted substantial interests from both scientists and industrialists. The benefits of the massive MIMO technique are realized by using very large antenna arrays (typically tens or even hundreds) at the transmitter and/or the receiver. Compared with the current counterpart, massive MIMO systems can bring high power and spectrum efficiency with low-complexity transmission designs. Random impairments such as small-scale fading and noise are averaged out when a large number of antennas are deployed at the base station (BS) [158]. Moreover, the interference, channel estimation errors, and hardware impairments [159] vanish when the number of antennas grows large, leaving only pilot contamination as the performance limit [160]. Therefore, massive MIMO opens up a

new and promising research avenue, extending the current research efforts in conventional MIMO systems to a new area. Specifically, we consider the following aspects:

- **Low Power Consumption:** In massive MIMO systems, the secrecy performance can be remarkably enhanced by adopting a reduced power consumption.
- **Time Division Duplex Operation:** Massive MIMO systems are recommended to operate in a time division duplex (TDD) mode [161]. As such, it becomes difficult for eavesdroppers to know the CSI between themselves and the BS, as well as the CSI from other users to the BS. Therefore, how to design secure transmission under the assumption of imperfect (or no) CSI at eavesdroppers is of practical importance in massive MIMO systems.
- **Secure Multiuser Communications:** In massive MIMO systems, each base station simultaneously communicates with multiple users. Each downlink message must be kept confidential from all the users other than the intended one, i.e., each receiver is seen as an eavesdropper for all messages other than its own. Therefore, it is pivotal to provide design guidelines and performance metrics of linear precoders in massive MIMO systems.

9.2.2.2 Millimeter Wave

In the 5G network, mmWave communication systems, operating in the frequency range of 30-300 GHz, have been recognized as a promising solution to remove the restriction and meet a thousand-fold capacity increase [63]. MmWave with physical layer security has at least the following merits:

- **Large Bandwidth:** MmWave communication systems provide GHz bandwidths. Therefore, the secrecy outage probability in the passive eavesdropping scenario is remarkably reduced if the transmitter sets a lower transmit secrecy rate in mmWave communications. Also, high secrecy throughput can be obtained with

large mmWave bandwidths.

- **Short-range Transmission:** Compared to the current microwave communication systems in the lower frequencies, mmWave signals in the higher frequencies experience an increase in free-space path loss by several orders of magnitude. Therefore, only geographically neighbouring eavesdroppers are able to overhear the signals, whereas geographically remote users cannot capture the data transmission.

- **Large Antenna Arrays:** For a fixed array aperture, the shorter wavelengths at the mmWave frequencies enable the mmWave BSs to pack more antennas. Therefore, mmWave systems with large antenna arrays offer a wealth of opportunities at the physical layer security to secure mmWave communication.

Based on the aforementioned factors, the aim of physical layer security design in mmWave communication systems is to fully exploit the potentials of these factors. In this design, several challenging tasks need to be solved.

First, the propagation characteristics at higher frequencies need to be precisely modeled. Indeed, an accurate and comprehensive quantification of the impact of path loss, blocking, penetration, and rain absorption on mmWave transmission enables network security designers to theoretically capture the properties of mmWave channels and address these properties in their design.

Second, new secure transmission schemes need to be developed. It has been shown that beamforming is a key enabler of mmWave mobile broadband service [162]. Since digital beamforming with a large number of radio frequency (RF) chains incurs a very high implementation cost and power consumption, secure mmWave transmission needs to be designed based on analog beamforming and RF beamforming with a small number of RF chains.

Third, some traditional techniques need to be re-designed. For example, artificial noise is proposed to enhance the security in traditional systems. The core idea behind

it is to transmit artificial noise in the null space of the receiver's channel, thus imposing no effect on the intended channel, whereas degrading the wiretap channels [72]. For mmWave systems equipped with large antenna arrays, the computation of the null space becomes infeasible, due to the high dimensional MIMO channel matrix. The use of random and independent artificial noise may be a promising solution since the independent artificial noise can be averaged out with large antenna arrays. As an external helper, the cooperative jammer can help to enhance the security by transmitting the jamming signal, in order to confound the eavesdroppers. In traditional systems, the information signal at the transmitter and jamming signal at the jammer are jointly designed, to mitigate the adverse effect of jamming on the legitimate receiver. Thanks to the mmWave networks' inherently noise-limited feature and massive MIMO's interference mitigation capability, the traditional design requirements for cooperative jamming may not be needed.

Appendix A

Proofs of in Chapter 4

A.1 Proof of Theorem 1

We first present the PDF and the CDF of the SNR of a single branch in the main channel with Nakagami-m fading as [163]

$$f\left(x\right)=\frac{x^{m_B-1}}{\left(m_B-1\right)!}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}e^{-\frac{m_B}{\bar{\gamma}_B}x} \tag{A.1.1}$$

and

$$F\left(x\right)=1-e^{-x\frac{m_B}{\bar{\gamma}_B}}\sum_{j=0}^{m_B-1}\frac{\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{j}}{j!}, \tag{A.1.2}$$

respectively. The marginal moment generating function (MGF) of (A.1.1) is given by [91]

$$\Phi\left(s,x\right)=\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}\sum_{i=0}^{m_B-1}\frac{x^{i}e^{-\left(s+\frac{m_B}{\bar{\gamma}_B}\right)x}}{i!\left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{m_B-i}}. \tag{A.1.3}$$

As shown in [91, 164], the MGF expression for the SNR γ after GSC is expressed as

$$\Phi_{\gamma}\left(s\right)=L_B\binom{N_B}{L_B}\times\int_0^{\infty}e^{-sx}f\left(x\right)\left(\Phi\left(s,x\right)\right)^{L_B-1}\left(F\left(x\right)\right)^{N_B-L_B}dx. \tag{A.1.4}$$

Here, the MGF is defined as $\Phi_\gamma(s) = \mathbb{E}[e^{-\gamma s}]$. In order to evaluate the integral in (A.1.4), we will rewrite $(\Phi(s,x))^{L_B-1}$ and $(F(x))^{N_B-L_B}$.

Based on (A.1.3), using the multinomial theorem [165], we rewrite $(\Phi(s,x))^{L_B-1}$ as

$$(\Phi(s,x))^{L_B-1} = \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B(L_B-1)} \sum_{\mathcal{S}_B^\Phi} a_k^\Phi \left(s + \frac{m_B}{\bar{\gamma}_B}\right)^{b_k^\Phi - m_B(L_B-1)} x^{b_k^\Phi} e^{-c_k^\Phi x}, \quad \text{(A.1.5)}$$

where $\mathcal{S}_B^\Phi = \left\{ \left(n_{k,0}^\Phi, \cdots, n_{k,m_B-1}^\Phi\right) \middle| \sum_{i=0}^{m_B-1} n_{k,i}^\Phi = L_B - 1 \right\}$, $a_k^\Phi = \frac{(L_B-1)!}{\prod_{i=0}^{m_B-1} n_{k,i}^\Phi!} \prod_{i=0}^{m_B-1} \left(\frac{1}{i!}\right)^{n_{k,i}^\Phi}$, $b_k^\Phi = \sum_{i=0}^{m_B-1} n_{k,i}^\Phi i$, and $c_k^\Phi = (L_B-1)\left(s + \frac{m_B}{\bar{\gamma}_B}\right)$.

Based on (A.1.2), we proceed to employ the multinomial theorem to express $(F(x))^{N_B-L_B}$ as

$$(F(x))^{N_B-L_B} = \sum_{\mathcal{S}_B^F} a_k^F \left(\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^F} x^{b_k^F} e^{-c_k^F x}, \quad \text{(A.1.6)}$$

where $\mathcal{S}_B^F = \left\{ \left(n_{k,0}^F, \cdots, n_{k,m_B}^F\right) \middle| \sum_{j=0}^{m_B} n_{k,j}^F = N_B - L_B \right\}$, $a_k^F = \frac{(N_B-L_B)!}{\prod_{j=0}^{m_B} n_{k,j}^F!} \prod_{j=0}^{m_B-1} \left(\frac{-1}{j!}\right)^{n_{k,j+1}^F}$, $b_k^F = \sum_{j=0}^{m_B-1} j n_{k,j+1}^F$, and $c_k^F = \frac{m_B}{\bar{\gamma}_B} \sum_{j=1}^{m_B} n_{k,j}^F$.

Substituting (A.1.1), (A.1.5), and (A.1.6) into (A.1.4), and applying [140, eq. (3.351.3)], $\Phi_\gamma(s)$ is derived as

$$\Phi_\gamma(s) = \frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B L_B} \sum_{\mathcal{S}_B^\Phi}\sum_{\mathcal{S}_B^F} a_k^\Phi a_k^F \left(\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^F} \frac{\Gamma(b_k^\Phi + b_k^F + m_B)\left(s + \frac{m_B}{\bar{\gamma}_B}\right)^{b_k^\Phi - m_B(L_B-1)}}{\left(s + c_k^\Phi + c_k^F + \frac{m_B}{\bar{\gamma}_B}\right)^{b_k^\Phi + b_k^F + m_B}}. \quad \text{(A.1.7)}$$

Let $F_\gamma(x)$ denote the CDF of γ, the Laplace transform of $F_\gamma(x)$ is given by $\mathcal{L}[F_\gamma(x)] =$

$\Phi_\gamma(s)/s$ [166]. Therefore, the Laplace transform of the CDF of γ is

$$\mathcal{L}\left[F_\gamma(x)\right] = \frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B L_B}\sum_{\mathcal{S}_B^\Phi}\sum_{\mathcal{S}_B^F} a_k^\Phi a_k^F$$
$$\left(\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^F}\frac{\Gamma(b_k^\Phi+b_k^F+m_B)}{(L_B)^{b_k^\Phi+b_k^F+m_B}}\frac{\left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^\Phi-m_B(L_B-1)}}{s\left(s+\frac{c_k^F}{L_B}+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^\Phi+b_k^F+m_B}}. \tag{A.1.8}$$

Using a partial fraction expansion [140, eq. (2.102)], we can rewrite (A.1.8) in an equivalent form. Then, taking the inverse Laplace transform of $\mathcal{L}\left[F_\gamma(x)\right]$ to obtain

$$F_\gamma(x) = \frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\sum_{\mathcal{S}}\sum_{n=0}^{m_B L_B+b_k^F} a_k^\Phi a_k^F\frac{\Gamma(b_k^\Phi+b_k^F+m_B)}{(L_B)^{b_k^\Phi+b_k^F+m_B}}\ell_n x^{\mu_n}e^{-\nu_n x}, \tag{A.1.9}$$

where $\mathcal{S}$ denotes

$$\mathcal{S} = \Bigg\{ \left(n_{k,0}^\Phi\cdots, n_{k,m_B-1}^\Phi, n_{k,0}^F,\cdots, n_{k,m_B}^F\right)\Big| \sum_{i=0}^{m_B-1} n_{k,i}^\Phi = L_B-1, \sum_{j=0}^{m_B} n_{k,j}^F = N_B-L_B\Bigg\},$$

and we define ℓ_n as

$$\ell_n = \begin{cases} \left(\frac{m_B}{\bar{\gamma}_B}\right)^{\mu_n}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F+1\right)^{-n_1} & n=0 \\ \left(\frac{m_B}{\bar{\gamma}_B}\right)^{\mu_n}\left(\Upsilon_1+\Upsilon_2-\frac{1-\mathrm{sgn}\left(c_k^F\right)}{(n-1)!}\right) & \\ \qquad 1\le n\le m_B(L_B-1)-b_k^\Phi & \\ \left(\frac{m_B}{\bar{\gamma}_B}\right)^{\mu_n}\left(\Upsilon_3+\Upsilon_4-\frac{1-\mathrm{sgn}\left(c_k^F\right)}{(n-1)!}\right) & \\ \qquad m_B(L_B-1)-b_k^\Phi < n\le m_B L_B+b_k^F \end{cases} \tag{A.1.10}$$

with $n_1 = b_k^{\Phi} + b_k^F + m_B$,

$$\Upsilon_1 = -\frac{\operatorname{sgn}\left(c_k^F\right)}{(n-1)!}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-n_1},$$

$$\Upsilon_2 = \frac{\operatorname{sgn}\left(c_k^F\right)}{(n-1)!}(-1)^{1-n_2}\sum_{l=1}^{n_1}\binom{l-n_2-1}{l-1}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-(n_1-l+1)}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F\right)^{n_2-l},$$

$$\Upsilon_3 = -\frac{\operatorname{sgn}\left(c_k^F\right)}{(n_2-1)!}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-(n_1-n_2+1)},$$

$$\Upsilon_4 = \frac{\operatorname{sgn}\left(c_k^F\right)}{(n_2-1)!}\sum_{l=1}^{m_B(L_B-1)-b_k^{\Phi}}(-1)^{l+1}\binom{n_1-n_2+l-1}{l-1}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F\right)^{-(n_1-n_2+l)},$$

where $n_2 = n - m_B\left(L_B - 1\right) + b_k^{\Phi}$. In (A.1.9), we also have

$$\mu_n = \begin{cases} 0 & n = 0 \\ n-1 & 1 \le n \le m_B\left(L_B-1\right) - b_k^{\Phi} \\ n - \operatorname{sgn}\left(c_k^F\right)\left(m_B\left(L_B-1\right) - b_k^{\Phi}\right) - 1 & \\ & m_B\left(L_B-1\right) - b_k^{\Phi} < n \le m_B L_B + b_k^F \end{cases}$$

and

$$\nu_n = \begin{cases} 0 & n = 0 \\ \frac{m_B}{\bar{\gamma}_B} & 1 \le n \le m_B\left(L_B-1\right) - b_k^{\Phi} \\ \left(\frac{c_k^F}{L_B} + \frac{m_B}{\bar{\gamma}_B}\right) & \\ & m_B\left(L_B-1\right) - b_k^{\Phi} < n \le m_B L_B + b_k^F \end{cases}$$

The CDF of γ_B with TAS and GSC is given by $F_{\gamma_B} = \left(F_{\gamma}\left(x\right)\right)^{N_A}$. Based on (A.1.9), and employing the multinomial theorem, we derive the CDF of γ_B as (4.4). Taking the derivative of the CDF in (4.4), we obtain the PDF of γ_B as (4.5).

A.2 Proof of Theorem 2

We start with the asymptotic CDF for the SNR of a single branch of the main channel. In the high SNR regime with $\bar{\gamma}_B \to \infty$, applying the Taylor series expansion truncated to the kth order given by $e^x = \sum_{j=0}^{k} \frac{x^j}{j!} + o\left(x^k\right)$ in (A.1.2), we obtain

$$\begin{aligned} F\left(x\right) &= 1 - e^{-x\frac{m_B}{\bar{\gamma}_B}} \left(e^{x\frac{m_B}{\bar{\gamma}_B}} - \frac{\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}}{m_B!} - o\left(\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}\right)\right) \\ &= \frac{\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}}{m_B!} + o\left(x^{m_B}\right). \end{aligned} \tag{A.2.1}$$

Substituting (A.1.1), (A.1.5), and (A.2.1) into (A.1.4) yields

$$\begin{aligned} \Phi_\gamma\left(s\right) = &\frac{L_B}{(m_B-1)!(m_B!)^{N_B-L_B}} \binom{N_B}{L_B} \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B} \\ &\sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B\left(N_B - L_B\right) + m_B - 1\right)!}{\left(L_B\right)^{b_k^\Phi + m_B(N_B-L_B)+m_B} \left(s + \frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B}}. \end{aligned} \tag{A.2.2}$$

It is shown in Appendix A that $\mathcal{L}\left[F_\gamma\left(x\right)\right] = \Phi_\gamma\left(s\right)/s$. Taking the inverse Laplace transform of $\mathcal{L}\left[F_\gamma\left(x\right)\right]$, F_γ is derived as

$$\begin{aligned} F_\gamma\left(x\right) = &\frac{L_B}{(m_B-1)!(m_B!)^{N_B-L_B}} \binom{N_B}{L_B} \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B} \\ &\sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B\left(N_B - L_B\right) + m_B - 1\right)!}{\left(L_B\right)^{b_k^\Phi + m_B(N_B-L_B)+m_B}} \left(\left(\frac{m_B}{\bar{\gamma}_B}\right)^{-m_B N_B} \right. \\ &\left. - \sum_{n=1}^{m_B N_B} \frac{\left(\frac{m_B}{\bar{\gamma}_B}\right)^{-(m_B N_B - n + 1)}}{(n-1)!} x^{n-1} e^{-\frac{m_B}{\bar{\gamma}_B}x} \right). \end{aligned} \tag{A.2.3}$$

Still employing the Taylor series expansion truncated to the kth order given by $e^x = \sum_{j=0}^{k} \frac{x^j}{j!} + o\left(x^k\right)$ in (A.2.3), we rewrite (A.2.3) as

$$F_\gamma(x) = \frac{L_B \binom{N_B}{L_B} \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B} x^{m_B N_B}}{(m_B-1)!(m_B!)^{N_B-L_B}(m_B N_B)!} \sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}}. \tag{A.2.4}$$

Based on (A.2.4), the asymptotic expression for the CDF of γ_B is $F_{\gamma_B}(x) = (F_\gamma(x))^{N_A}$ and the final expression is shown in (4.6).

A.3 Proof of Theorem 3

Substituting (4.12) into (4.10), we rewrite the average secrecy rate as

$$\bar{C}_s = \frac{1}{\ln 2} \int_0^\infty \left[\int_0^{x_1} \frac{F_{\gamma_E}(x_2)}{1+x_2} dx_2 \right] f_{\gamma_B}(x_1)\, dx_1. \tag{A.3.1}$$

Substituting (4.15) into (A.3.1), we transform (A.3.1) as

$$\bar{C}_s = \underbrace{\frac{1}{\ln 2} \int_0^\infty \ln(1+x_1)\, f_{\gamma_B}(x_1) dx_1}_{\omega_2} + \underbrace{\frac{1}{\ln 2} \int_0^\infty \int_0^{x_1} \frac{\chi_{\gamma_E}(x_2)}{1+x_2} f_{\gamma_B}(x_1) dx_2 dx_1}_{\omega_3}. \tag{A.3.2}$$

In the high SNR regime with $\bar{\gamma}_B \to \infty$, $\ln(1+x_1) \approx \ln(x_1)$, thereby the asymptotic expression for ω_2 can be written as Δ_1 in (4.17). Changing the order of integration in ω_3, we rewrite

$$\omega_3 = \frac{1}{\ln 2} \int_0^\infty \frac{\chi_{\gamma_E}(x_2)}{1+x_2} \left(1 - F_{\gamma_B}(x_2)\right) dx_2. \tag{A.3.3}$$

According to (4.6), when $\bar{\gamma}_B \to \infty$, $F_{\gamma_B}(x_2) \approx 0$. Hence, the asymptotic expression for ω_3 can be expressed as Δ_2 in (4.18). Based on (4.17), (4.18), and (A.3.2), we derive the asymptotic expression for the average secrecy rate as (4.16).

Appendix B

Proofs in Chapter 5

B.1 Proof of Theorem 1

We first provide the CDF and PDF of $Y = \max_{n=1,\ldots,N} Y_n$, where Y_n is i.i.d. exponential RV with parameter Ω_Y, which can be written as

$$F_Y(y) = \sum_{n=0}^{N} \binom{N}{n} (-1)^n e^{-\frac{ny}{\Omega_Y}} \tag{B.1}$$

and

$$f_Y(y) = \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{N}{\Omega_Y} (-1)^n e^{-\frac{(n+1)y}{\Omega_Y}}. \tag{B.2}$$

In addition, $f_X(x) = \frac{1}{\Omega_0} e^{-\frac{x}{\Omega_0}}$.

Based on (5.3), we note that when $X \leq \frac{\overline{\gamma}_p}{\overline{\gamma}_0}$, $\gamma_{\mathsf{M}} = \overline{\gamma}_0 Y_M, \gamma_{\mathsf{E}} = \overline{\gamma}_0 Y_E$, and when $X > \frac{\overline{\gamma}_p}{\overline{\gamma}_0}$, $\gamma_{\mathsf{M}} = \frac{\overline{\gamma}_p}{X} Y_M, \gamma_{\mathsf{E}} = \frac{\overline{\gamma}_p}{X} Y_E$. Hence, the secrecy outage probability in (5.12) can be

calculated as

$$P_{\mathsf{out}} = \underbrace{\int_0^{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}} \int_0^{\infty} F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) f_{\gamma_{\mathsf{E}}|\{X=x\}}\left(\gamma_{\mathsf{E}}\right) f_X\left(x\right) d\gamma_{\mathsf{E}} dx}_{\mathcal{J}_1}$$
$$+ \underbrace{\int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} \int_0^{\infty} F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) f_{\gamma_{\mathsf{E}}|\{X=x\}}\left(\gamma_{\mathsf{E}}\right) f_X\left(x\right) d\gamma_{\mathsf{E}} dx}_{\mathcal{J}_2}. \tag{B.3}$$

Based on (B.1), for $X \leq \frac{\overline{\gamma}_p}{\overline{\gamma}_0}$, we have

$$F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) = \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} (-1)^i e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_0 \Omega_1}},$$
$$f_{\gamma_{\mathsf{E}}|\{X=x\}}\left(\gamma_{\mathsf{E}}\right) = \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_0 \Omega_2} (-1)^j e^{-\frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_0 \Omega_2}}. \tag{B.4}$$

By substituting (B.4) into $\mathcal{J}_1$ of (B.3), $\mathcal{J}_1$ can be derived as

$$\mathcal{J}_1 = \int_0^{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}} f_X\left(x\right) dx \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_0 \Omega_2} (-1)^{i+j} \int_0^{\infty} e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_0 \Omega_1} - \frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_0 \Omega_2}} d\gamma_{\mathsf{E}}$$
$$= \left(1 - e^{-\frac{\overline{\gamma}_p}{\overline{\gamma}_0 \Omega_0}}\right) \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_0 \Omega_2} (-1)^{i+j} e^{-\frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_0 \Omega_1}} \left(\frac{i 2^{R_{\mathsf{s}}}}{\overline{\gamma}_0 \Omega_1} + \frac{j+1}{\overline{\gamma}_0 \Omega_2}\right)^{-1}. \tag{B.5}$$

For $X > \frac{\overline{\gamma}_p}{\overline{\gamma}_0}$, we have

$$F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) = \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} (-1)^i e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_p \Omega_1} x},$$
$$f_{\gamma_{\mathsf{E}}|\{X=x\}}\left(\gamma_{\mathsf{E}}\right) = \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} (-1)^j x e^{-\frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} x}. \tag{B.6}$$

By substituting (B.6) into $\mathcal{J}_2$ of (B.3), $\mathcal{J}_2$ can be derived as

$$\begin{aligned}
\mathcal{J}_2 &= \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} e^{-\frac{x}{\Omega_0}} \int_0^{\infty} x e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_p \Omega_1} x - \frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} x} d\gamma_{\mathsf{E}} dx \\
&= \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} x e^{-\frac{x}{\Omega_0}} e^{-\frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_p \Omega_1} x} \int_0^{\infty} e^{-\frac{i 2^{R_{\mathsf{s}}} x \gamma_{\mathsf{E}}}{\overline{\gamma}_p \Omega_1} - \frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} x} d\gamma_{\mathsf{E}} dx \\
&= \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p \Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \left(\frac{i 2^{R_{\mathsf{s}}}}{\overline{\gamma}_p \Omega_1} + \frac{j+1}{\overline{\gamma}_p \Omega_2} \right)^{-1} \frac{e^{-\frac{\overline{\gamma}_p}{\overline{\gamma}_0 \Omega_0} - \frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_0 \Omega_1}}}{\frac{1}{\Omega_0} + \frac{i(2^{R_{\mathsf{s}}}-1)}{\overline{\gamma}_p \Omega_1}}.
\end{aligned} \tag{B.7}$$

Substituting (B.5) and (B.7) into (B.3), we get the desired result (5.13).

Appendix C

Proofs in Chapter 6

C.1 A detailed derivation of Lemma 1

According to the order statistics, the PDF of $\gamma_2^{\min,\max}$ is given by

$$f_{\gamma_2^{\min,\max}}(x) = K(1 - F_{\gamma_2^{k,\max}}(x))^{K-1} f_{\gamma_2^{k,\max}}(x). \tag{C.1.1}$$

Binomial and multinomial formulas provide the following expression for $f_{\gamma_2^{k,\max}}(x)$:

$$\begin{aligned} f_{\gamma_2^{k,\max}}(x) = \frac{N}{(\tilde{\alpha}_2)^{N_2}(N_2-1)!} \sum_{j=0}^{N-1} \binom{N-1}{j} (-1)^j e^{-\frac{x(j+1)}{\tilde{\alpha}_2}} \\ \times \sum_{u_1,\ldots,u_{N_2}}^{j} \left(\frac{j!}{u_1! \ldots u_{N_2}!} \right) \frac{x^{N_2+\sum_{t=0}^{N_2-1} t u_{t+1}-1}}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{u_{t+1}}}. \end{aligned} \tag{C.1.2}$$

$$P_{out} = \int_0^\infty \Big[1 - e^{-(J_R-1+J_R\gamma)/\tilde{\alpha}_1} \sum_{l=0}^{N_1-1} \frac{1}{l!}\Big(\frac{(J_R-1+J_R\gamma)}{\tilde{\alpha}_1}\Big)^l\Big]^Q f_{\gamma_2^{\min,\max}}(\gamma)d\gamma$$
$$= \sum_{q=0}^{Q}\binom{Q}{q}(-1)^q \int_0^\infty e^{-q(J_R-1+J_R\gamma)/\tilde{\alpha}_1} \underbrace{\Big[\sum_{l=0}^{N_1-1} \frac{1}{l!}\Big(\frac{(J_R-1+J_R\gamma)}{\tilde{\alpha}_1}\Big)^l\Big]^q}_{J_1} f_{\gamma_2^{\min,\max}}(\gamma)d\gamma. \tag{C.2.1}$$

Again binomial and multinomial formulas lead us to get the following expression for $(1-F_{\gamma_2^{k,\max}}(x))^{K-1}$:

$$\begin{aligned}(1-F_{\gamma_2^{k,\max}}(x))^{K-1} &= \left[1-\left(1-e^{-x/\tilde{\alpha}_2}\sum_{l=0}^{N_2-1}\frac{1}{l!}\left(\frac{x}{\tilde{\alpha}_2}\right)^l\right)^N\right]^{K-1}\\ &= \sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\left(1-e^{-x/\tilde{\alpha}_2}\sum_{l=0}^{N_2-1}\frac{1}{l!}\left(\frac{x}{\tilde{\alpha}_2}\right)^l\right)^{kN}\\ &= \sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\sum_{m=0}^{Nk}\binom{Nk}{m}(-1)^m e^{-mx/\tilde{\alpha}_2}\\ &\times \sum_{v_1,\ldots,v_{N_2}}^{m}\left(\frac{m!}{v_1!\ldots v_{N_2}!}\right)\frac{x^{\sum_{t=0}^{N_2-1}tv_{t+1}}}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}.\end{aligned} \tag{C.1.3}$$

Multiplying (C.1.2) and (C.1.3) and after some manipulations, yields (6.8).

C.2 A detailed derivation of Theorem 1

Now substituting $f_{\gamma_2^{\min,\max}}(\gamma)$, which is derived in (6.8) and $F_{\gamma_1^{k^*,q^*}}(\gamma)$, which is derived in (6.5) into (6.12), we have (C.2.1). Using multinomial and binomial formulas, J_1 becomes

$$J_1 = \sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}\sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p\gamma^p. \tag{C.2.2}$$

Substituting (C.2.2) into (C.2.1), yields

$$P_{out} = \sum_{q=0}^{Q} \binom{Q}{q} (-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}} \sum_{w_1,\ldots,w_{N_1}}^{q} \frac{q!}{w_1!\ldots w_{N_1}!} \frac{\sum_{p=0}^{\tilde{L}_1} \binom{\tilde{L}_1}{p} (J_R-1)^{\tilde{L}_1-p} (J_R)^p}{\prod_{t=0}^{N_1-1} (t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \int_0^{\infty} e^{-qJ_R\gamma/\tilde{\alpha}_1} \gamma^p f_{\gamma_2^{\min,\max}}(\gamma) d\gamma. \quad \text{(C.2.3)}$$

Again using (6.8) into (C.2.3), we have (6.13).

C.3 A detailed derivation of Theorem 2

Applying the Taylor series expansion truncated to the N_1th order given by $e^x = \sum_{l=0}^{N_1} \frac{x^l}{l!} + O(x^{N_1})$, we derive the first order expansion of $F_{\gamma_1^{k^*,q^*}}(x)$, which is specified in (6.5), at high $\tilde{\alpha}_1$ as

$$\begin{aligned} F_{\gamma_1^{k^*,q^*}}(x) &= \left[1 - e^{-x/\tilde{\alpha}_1}\left(e^{x/\tilde{\alpha}_1} - \frac{1}{N_1!}\left(\frac{x}{\tilde{\alpha}_1}\right)^{N_1} - O((\frac{x}{\tilde{\alpha}_1})^{N_1})\right)\right]^Q \\ &= \frac{1}{(N_1!)^Q}\left(\frac{x}{\tilde{\alpha}_1}\right)^{QN_1} + O((\tilde{\alpha}_1)^{-QN_1}). \end{aligned} \quad \text{(C.3.1)}$$

In addition, the PDF expression $f_{\gamma_2^{\min,\max}}(x)$ in (8) needs to be written as

$$f_{\gamma_2^{\min,\max}}(x) = \hat{C}\widehat{\sum} \frac{x^{\tilde{N}_2-1}}{(\tilde{\alpha}_2)^{\tilde{N}_2}} e^{-\frac{\hat{\beta}x}{\tilde{\alpha}_2}} \mathrm{U}(x). \quad \text{(C.3.2)}$$

Substituting (C.3.1) and (C.3.2) into (6.12), the asymptotic secrecy outage probability is calculated as (C.3.3) which proves (6.15).

$$
\begin{aligned}
P_{out}^{\infty} &= \frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}\int_0^{\infty}\Big(\frac{J_R\gamma+J_R-1}{\tilde{\alpha}_1}\Big)^{QN_1}\frac{\gamma^{\tilde{N}_2-1}}{(\tilde{\alpha}_2)^{\tilde{N}_2}}e^{-\frac{\hat{\beta}\gamma}{\tilde{\alpha}_2}}d\gamma+O((\tilde{\alpha}_1)^{-QN_1}) \\
&= \frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}\sum_{l=0}^{QN_1}\binom{N_1}{l}\Big(\frac{1}{\tilde{\alpha}_1}\Big)^{QN_1}(J_R-1)^{QN_1-l}(J_R)^l\int_0^{\infty}\gamma^l\frac{\gamma^{\tilde{N}_2-1}}{\big(\tilde{\alpha}_1\big)^{\tilde{N}_2}}e^{-\frac{\hat{\beta}\gamma}{\tilde{\alpha}_2}}d\gamma+O((\tilde{\alpha}_1)^{-QN_1}) \\
&= \frac{C}{(N_1!)^Q}\widehat{\sum}\sum_{l=0}^{QN_1}\binom{QN_1}{l}\Big(\frac{1}{\tilde{\alpha}_1}\Big)^{QN_1}(J_R-1)^{QN_1-l}(J_R)^l(\tilde{\alpha}_2)^l\frac{(l+\tilde{N}_2-1)!}{(\hat{\beta})^{l+\tilde{N}_2}}+O\big((\tilde{\alpha}_1)^{-QN_1}\big) \\
&= (G_a\tilde{\alpha}_1)^{-QN_1}+O((\tilde{\alpha}_1)^{-QN_1}). \qquad \text{(C.3.3)}
\end{aligned}
$$

C.4 A detailed derivation of Corollary 2

The CDF of $\gamma_2^{\min,\max}$ is given by

$$
\begin{aligned}
F_{\gamma_2^{\min,\max}}(x) &= 1-(1-F_{\gamma_2^{k,\max}}(x))^K \\
&= 1-\sum_{k=0}^{K}\sum_{m=0}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m}e^{-mx/\tilde{\alpha}_2} \\
&\quad \sum_{v_1,\ldots,v_{N_2}}^{m}\left(\frac{m!}{v_1!\ldots v_{N_2}!}\right)\frac{x^{\sum_{t=0}^{N_2-1}tv_{t+1}}}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}. \qquad \text{(C.4.1)}
\end{aligned}
$$

In addition, the PDF of $\gamma_1^{k^*,q^*}$ is given by

$$
\begin{aligned}
f_{\gamma_1^{k^*,q^*}}(x) &= \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q \\
&\quad \sum_{w_1,\ldots,w_{N_1}}^{q}\left(\frac{q!}{w_1!\ldots w_{N_1}!}\right)\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \\
&\quad x^{N_1+\sum_{t=0}^{N_1-1}tw_{t+1}-1}e^{-\frac{x(q+1)}{\tilde{\alpha}_1}}\mathrm{U}(x). \qquad \text{(C.4.2)}
\end{aligned}
$$

The probability of non-zero achievable secrecy rate is given by

$$\begin{aligned} Pr(C_s > 0) &= \int_0^\infty F_{\gamma_2^{\min,\max}}(x) f_{\gamma_1^{k^*,q^*}}(x) dx \\ &= 1 - \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!} \sum_{k=0}^{K} \sum_{m=0}^{Nk} \sum_{q=0}^{Q-1} \binom{Q-1}{q} \binom{K}{k} \binom{Nk}{m} \\ &(-1)^{q+k+m} \sum_{v_1,\ldots,v_{N_2}}^{m} \left(\frac{m!}{v_1! \ldots v_{N_2}!} \right) \sum_{w_1,\ldots,w_{N_1}}^{q} \left(\frac{q!}{w_1! \ldots w_{N_1}!} \right) \\ &\frac{1}{\prod_{t=0}^{N_2-1} (t!(\tilde{\alpha}_2)^t)^{v_{t+1}}} \frac{1}{\prod_{t=0}^{N_1-1} (t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \int_0^\infty e^{-x(\frac{m}{\tilde{\alpha}_2} + \frac{q+1}{\tilde{\alpha}_1})} x^{\tilde{N}_1 - 1} dx \end{aligned} \quad \text{(C.4.3)}$$

which becomes (6.18).

C.5 A detailed derivation of Corollary 3

Based on (C.4.1), we first rewrite the CDF of $\gamma_2^{\min,\max}$ as

$$F_{\gamma_2^{\min,\max}}(x) = 1 + \tilde{F}_{\gamma_2^{\min,\max}}(x), \quad \text{(C.5.1)}$$

where

$$\begin{aligned} \tilde{F}_{\gamma_2^{\min,\max}}(x) = &\sum_{k=1}^{K} \sum_{m=1}^{Nk} \binom{K}{k} \binom{Nk}{m} (-1)^{k+m+1} e^{-mx/\tilde{\alpha}_2} \\ &\sum_{v_1,\ldots,v_{N_2}}^{m} \left(\frac{m!}{v_1! \ldots v_{N_2}!} \right) \frac{x^{\sum_{t=0}^{N_2-1} t v_{t+1}}}{\prod_{t=0}^{N_2-1} (t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}. \end{aligned}$$

Then, the ergodic secrecy rate is derived as (C.5.2). As $\tilde{\alpha}_1 \to \infty$, Θ_1 asymptotically becomes

$$\Theta_1^\infty = \log(\tilde{\alpha}_1) + \int_0^\infty \log\left(\frac{x_1}{\tilde{\alpha}_1}\right) f_{\gamma_1^{k^*,q^*}}(x_1)\, dx_1. \quad \text{(C.5.3)}$$

Substituting the PDF of $\gamma_1^{k^*,q^*}$ given in (C.4.2) into (C.5.3), and employing [140, eq. 4.352.1] given by $\int_0^\infty x^{\nu-1} e^{-\mu x} \log(x)\, dx = \frac{1}{\mu^\nu} \Gamma(\nu) \Big[\psi(\nu) - \log(\mu) \Big]$, we compute (C.5.3)

$$\bar{C}_s = \frac{1}{2\log(2)} \int_0^{\infty} \left[\int_0^{x_1} \frac{F_{\gamma_2^{\min,\max}}(x_2)}{1+x_2} dx_2 \right] f_{\gamma_1^{k^*,q^*}}(x_1)\, dx_1$$
$$= \frac{1}{2\log(2)} \Big[\underbrace{\int_0^{\infty} \log(1+x_1) f_{\gamma_1^{k^*,q^*}}(x_1) dx_1}_{\Theta_1} + \underbrace{\int_0^{\infty} \int_0^{x_1} \frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2} f_{\gamma_1^{k^*,q^*}}(x_1) dx_2 dx_1}_{\Theta_2} \Big]. \tag{C.5.2}$$

---

as

$$\Theta_1^{\infty} = \log(\tilde{\alpha}_1) + \frac{Q}{(N_1-1)!} \sum_{q=0}^{Q-1} \binom{Q-1}{q} (-1)^q$$
$$\sum_{w_1,\ldots,w_{N_1}}^{q} \left(\frac{q!}{w_1! \ldots w_{N_1}!}\right) \frac{1}{\prod_{t=0}^{N_1-1} (t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}} \Big[\psi(N_1+\tilde{L}_1) - \log(q+1) \Big]. \tag{C.5.4}$$

Changing the order of integration in Θ_2, we have

$$\Theta_2 = \int_0^{\infty} \frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2} (1 - F_{\gamma_1^{k^*,q^*}}(x_2)) dx_2. \tag{C.5.5}$$

According to the first order expansion of the CDF of $\gamma_1^{k^*,q^*}$ shown in (C.3.1), as $\tilde{\alpha}_1 \to \infty$, $F_{\gamma_1^{k^*,q^*}}(x_2) \approx 0$. Hence, the asymptotic expression for Θ_2 is given by

$$\Theta_2^{\infty} = \int_0^{\infty} \frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2} dx_2$$
$$= \sum_{k=1}^{K} \sum_{m=1}^{Nk} \binom{K}{k} \binom{Nk}{m} (-1)^{k+m+1} \sum_{v_1,\ldots,v_{N_2}}^{m} \left(\frac{m!}{v_1! \ldots v_{N_2}!}\right)$$
$$\frac{\Gamma(\sum_{t=0}^{N_2-1} tv_{t+1} + 1)}{\prod_{t=0}^{N_2-1} (t!(\tilde{\alpha}_2)^t)^{v_{t+1}}} \Psi\Big(\sum_{t=0}^{N_2-1} tv_{t+1} + 1, \sum_{t=0}^{N_2-1} tv_{t+1} + 1; m/\tilde{\alpha}_2\Big). \tag{C.5.6}$$

Substituting (C.5.6) and (C.5.4) into (C.5.2), we derive the asymptotic expression for the ergodic secrecy capacity as (6.26).

C.6 A detailed derivation of Corollary 4

In the case of $\tilde{\alpha}_1 \to \infty$ and $\tilde{\alpha}_2 \to \infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2} = \kappa$, the asymptotic ergodic secrecy rate can be easily obtained based on the proof of Corollary 3 in Appendix E. We only need to further provide an asymptotic expression for Θ_2^{∞} with $\tilde{\alpha}_2 \to \infty$. Observing Θ_1^{∞} in (C.5.3), an asymptotic expression for Θ_2^{∞} can be derived as

$$\Theta_{21}^{\infty} = -\log\left(\tilde{\alpha}_2\right) - \int_0^{\infty} \log\left(\frac{x_2}{\tilde{\alpha}_2}\right) f_{\gamma_2^{\min,\max}}\left(x_2\right) dx_2. \tag{C.6.1}$$

Substituting the PDF of $\gamma_2^{\min,\max}$ in (6.8) into (C.6.1), we obtain

$$\Theta_{21}^{\infty} = -\log(\tilde{\alpha}_2) - \hat{C}\widehat{\sum}\frac{\Gamma(\tilde{N}_2)}{(\hat{\beta})^{\tilde{N}_2}}[\psi(\tilde{N}_2) - \log(\hat{\beta})]. \tag{C.6.2}$$

Substituting the new asymptotic expression for Θ_2^{∞} in (C.6.2) and (C.5.4) into (C.5.2), we get (6.29).

Appendix D

Proof in Chapter 7

D.1 Derivation of (7.12)

We see that OPA can achieve perfect secrecy. Hence, based on (7.4) and (7.3), ESC in (7.10) can be rewritten as

$$\bar{C}_s = \frac{1}{2\ln 2}\left(\ell_1 - \ell_2\right), \tag{D.1}$$

where

$$\ell_1 = \int_0^\infty \int_0^\infty x_2 \ln\left(1 + \frac{\alpha^*\mu x_2}{\alpha^*\mu + 2 - \alpha^*}\right) f_{\gamma_{a,r}}\left(\mu x_2\right) f_{\gamma_{r,b}}\left(x_2\right) d\mu dx_2 \tag{D.2}$$

and

$$\ell_2 = \int_0^\infty \int_0^\infty x_2 \ln\left(1 + \frac{\alpha^*\mu}{(1-\alpha^*)}\right) f_{\gamma_{a,r}}\left(\mu x_2\right) f_{\gamma_{r,b}}\left(x_2\right) d\mu dx_2. \tag{D.3}$$

In addition, the PDF of $\gamma_{a,r}$ and the PDF of $\gamma_{r,b}$ is written as

$$f_{\gamma_{a,r}}(x) = \frac{x^{N_a-1}e^{-\frac{x}{\bar{\gamma}_{a,r}}}}{(N_a-1)!(\bar{\gamma}_{a,r})^{N_a}}, \tag{D.4}$$

$$f_{\gamma_{r,b}}(x) = \frac{1}{\bar{\gamma}_{r,b}} e^{-\frac{x}{\bar{\gamma}_{r,b}}}. \tag{D.5}$$

In the high SNR regime with $\gamma_0 \to \infty$, ℓ_1 is evaluated as

$$\begin{aligned}\ell_1 = &\underbrace{\int_0^\infty \int_0^\infty x_2 \ln \bar{\gamma}_{a,r} f_{\gamma_{a,r}}(\mu x_2) f_{\gamma_{r,b}}(x_2)\, d\mu dx_2}_{\Upsilon_1} + \\ &\underbrace{\int_0^\infty \int_0^\infty x_2 \ln\left(\frac{\alpha^*\mu}{\alpha^*\mu + 2 - \alpha^*}\right) f_{\gamma_{a,r}}(\mu x_2) f_{\gamma_{r,b}}(x_2)\, d\mu dx_2}_{\Upsilon_2} \\ &+ \underbrace{\int_0^\infty \int_0^\infty x_2 \ln \frac{x_2}{\bar{\gamma}_{a,r}} f_{\gamma_{a,r}}(\mu x_2) f_{\gamma_{r,b}}(x_2)\, d\mu dx_2}_{\Upsilon_3}.\end{aligned} \tag{D.6}$$

It is easily seen that $\Upsilon_1 = \ln \bar{\gamma}_{a,r}$. Substituting (D.4) and (D.5) into (D.6), and after some manipulations, we obtain Υ_2 as

$$\Upsilon_2 = N_a \frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}} \int_0^\infty \frac{\mu^{N_a-1} \ln\left(\frac{\alpha^*}{\alpha^*\mu+2-\alpha^*}\right)}{\left(\mu + \frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}}\right)^{(N_a+1)}} d\mu. \tag{D.7}$$

Using [140, Eq. (4.352.1)], Υ_3 is derived as $\Upsilon_3 = \psi(N_a)$.

Substituting Υ_1, Υ_2 and Υ_3 into (D.6), we first obtain ℓ_1. Then, ℓ_2 can be evaluated as

$$\ell_2 = N_a \frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}} \int_0^\infty \frac{\mu^{N_a-1} \ln\left(1 + \frac{\alpha^*\mu}{(1-\alpha^*)}\right)}{\left(\mu + \frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}}\right)^{(N_a+1)}} d\mu. \tag{D.8}$$

Plugging ℓ_1, ℓ_2, and the OPA factor given by (7.8) into (D.1), and after some manipulations, we arrive at the desired result shown in (7.12).

Appendix E

Proofs in Chapter 8

E.1 Proof of Lemma 1

From (8.1), the CDF of γ_{ap} is given by

$$\begin{aligned} F_{\gamma_{ap}}(\gamma_{th}) &= \int_0^\infty \Pr\left[\frac{\|\mathbf{h}_{s_0,ap_0}\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s} \leq \gamma_{th}\right] f_{|X_{s_0,ap_0}|}(r)\, dr \\ &= \int_0^\infty \Pr\left[\frac{\|\mathbf{h}_{s_0,ap_0}\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s} \leq \gamma_{th}\right] 2\pi\lambda_{ap} \\ &\quad (1-\rho_{ap})\, r \exp\left(-\pi\lambda_{ap}(1-\rho_{ap})\, r^2\right) dr, \end{aligned} \tag{E.1.1}$$

where $f_{|X_{s_0,ap_0}|}(r)$ is the PDF of the nearest distance between the relay and the typical sensor. The CDF of the relay SINR at distance r from its corresponding sensor is given

as

$$\begin{aligned}\Pr\left[\frac{\|\mathbf{h}_{s_0,ap_0}\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s}\leq\gamma_{th}\right]=&\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\Pr\left[\|\mathbf{h}_{s_0,ap_0}\|^2.\right.\right.\right.\\&\left.\left.\left.\leq\gamma_{th}r^{\alpha}\left(In_{ap}+\delta^2/P_s\right)\middle|\,\Phi_{s,a},\Phi_{ap,a}\right]\right\}\right\}\\=1-\sum_{m=0}^{M-1}\frac{1}{m!}&\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^{\infty}\left[\gamma_{th}r^{\alpha}\left(\tau+\delta^2/P_s\right)\right]^m\right.\right.\\&\left.\left.\exp\left[-\gamma_{th}r^{\alpha}\left(\tau+\delta^2/P_s\right)\right]d\Pr\left(In_{ap}\leq\tau\right)\right\}\right\}\end{aligned}\tag{E.1.2}$$

We then substitute $\left(-\left(\tau+\delta^2/P_s\right)\gamma_{th}\right)^m e^{-\left(\tau+\delta^2/P_s\right)\gamma_{th}^{\{s\}}r^{\alpha}}=\left.\frac{d^m\left(e^{-\gamma_{th}x\left(\tau+\delta^2/P_s\right)}\right)}{dx^m}\right|_{x=r^{\alpha}}$ into (E.1.2), we rewrite the CDF of the relay SINR at distance r from its corresponding sensor as

$$\begin{aligned}\Pr\left[\frac{\|\mathbf{h}_{s_0,ap_0}\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s}\leq\gamma_{th}\right]=&1-\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\right.\right.\\&\left.\left.\int_0^{\infty}\exp\left[-\gamma_{th}r^{\alpha}\left(\tau+\delta^2/P_s\right)\right]d\Pr\left(In_{ap}\leq\tau\right)\right\}\right\}\\&-\sum_{m=1}^{M-1}\frac{(r^{\alpha})^m}{m!(-1)^m}\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\right.\right.\\&\left.\left.\int_0^{\infty}\left.\frac{d^m\left(e^{-\gamma_{th}x\left(\tau+\delta^2/P_s\right)}\right)}{dx^m}\right|_{x=r^{\alpha}}d\Pr\left(In_{ap}\leq\tau\right)\right\}\right\}\\=1-&\exp\left(-\gamma_{th}r^{\alpha}\delta^2/P_s\right)\mathcal{L}_{In_{ap}}\left(\gamma_{th}r^{\alpha}\right)\\-\sum_{m=1}^{M-1}&\frac{(r^{\alpha})^m}{m!(-1)^m}\left.\frac{d^m\left(\exp\left(-\gamma_{th}x\delta^2/P_s\right)\mathcal{L}_{In_{ap}}\left(\gamma_{th}x\right)\right)}{dx^m}\right|_{x=r^{\alpha}}.\end{aligned}\tag{E.1.3}$$

Remind that $I_{s,ap}=\sum_{i\in\Phi_{s,a}\setminus\{s_0\}}\left|\frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|}\mathbf{h}_{i,ap_0}\right|^2|X_{i,ap_0}|^{-\alpha}$, using Slivnyak's theorem,

the Laplace transform of $I_{s,ap}$ is

$$\begin{aligned}\mathcal{L}_{I_{s,ap}}(s) &= \mathbb{E}_{\Phi_s}\left[\exp\left\{-s\sum_{i\in\Phi_{s,a}\setminus\{s_0\}}\left|\frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|}\mathbf{h}_{i,ap_0}\right|^2|X_{i,ap_0}|^{-\alpha}\right\}\right]\\ &\overset{(a)}{=}\exp\left\{-2\pi\lambda_s\rho_s\int_0^{\infty}\left(1-\mathcal{L}_{\frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|}\mathbf{h}_{i,ap_0}}\left(sy^{-\alpha}\right)\right)ydy\right\}\\ &\overset{(b)}{=}\exp\left\{-2\pi\lambda_s\rho_s\int_0^{\infty}\left(1-\frac{1}{1+sy^{-\alpha}}\right)ydy\right\}\\ &=\exp\left\{-\lambda_s\rho_s\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\},\end{aligned}\tag{E.1.4}$$

In (E.1.4), (a) follows from the generating functional of HPPP in [89], (b) follows from the fact that $\left|\frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|}\mathbf{h}_{i,ap_0}\right|^2\sim\exp(1)$.

Since $I_{ap,ap}=\mu\sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}}\left|\frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\|\mathbf{h}_{s_0,ap_0}\|}\mathbf{H}_{j,ap_0}\frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\|\mathbf{h}_{j,sk_j}\|}\right|^2|X_{j,ap_0}|^{-\alpha}$
$=\mu\sum_{j\in\Phi_{ap}\setminus\{ap_0\}}H_j^{ap,ap}|X_{j,ap_0}|^{-\alpha}$, the Laplace transform of $I_{ap,ap}$ is

$$\begin{aligned}\mathcal{L}_{I_{ap,ap}}(s) &\overset{(c)}{=}\exp\left(-\int_0^{\infty}\left[1-\mathbb{E}_h\left(\exp\left(-s\mu H_j^{ap,ap}y^{-\alpha}\right)\right)\right]\lambda_{ap}\rho_{ap}2\pi ydy\right)\\ &=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\mathbb{E}_h\left\{\left(H_j^{ap,ap}\right)^{\frac{2}{\alpha}}\right\}\Gamma\left(1-\frac{2}{\alpha}\right)s^{\frac{2}{\alpha}}\right\}\\ &\overset{(d)}{=}\exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\},\end{aligned}\tag{E.1.5}$$

where (c) follows from the generating functional of HPPP in [89], (d) follows from $H_j^{ap,ap}\sim\exp(1)$.

With the Laplace transform of $I_{s,ap}$ and $I_{ap,ap}$, we derive the Laplace transform of In_{ap} as

$$\begin{aligned}\mathcal{L}_{In_{ap}}(s) &= \mathcal{L}_{I_{s,ap}}(s)\,\mathcal{L}_{I_{ap,ap}}(s)\\ &=\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}.\end{aligned}\tag{E.1.6}$$

Substituting (E.1.6) into (E.1.3), we obtain

$$\Pr\left[\frac{\|\mathbf{h}_{s_0,ap_0}\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s}\leq\gamma_{th}\right]=1-\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\right.$$
$$\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{2/\alpha}r^2-\gamma_{th}r^{\alpha}\delta^2/P_s\right\}$$
$$-\sum_{m=1}^{M-1}\frac{\left(r^{\alpha}\right)^m}{m!(-1)^m}\frac{d^m\left(V\left(x\right)\right)}{dx^m}\bigg|_{x=r^{\alpha}}, \tag{E.1.7}$$

where $V\left(x\right)=\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+2/\alpha\right)\ \Gamma\left(1-2/\alpha\right)\left(\gamma_{th}x\right)^{2/\alpha}-\gamma_{th}x\delta^2/P_s\right\}$.

We then apply the Faà di Bruno's formula to solve the derivative of mth order as follows:

$$\Pr\left[\frac{\|\mathbf{h}_{s_0,ap_0}\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s}\leq\gamma_{th}\right]=1-\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\right.$$
$$\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)(\gamma_{th})^{2/\alpha}r^2-\gamma_{th}r^{\alpha}\delta^2/P_s\right\}-$$
$$\sum_{m=1}^{M-1}\frac{\left(r^{\alpha}\right)^m}{(-1)^m}\sum\frac{1}{\prod_{l=1}^{m}m_l!l!^{m_l}}\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\right.$$
$$\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)(\gamma_{th})^{2/\alpha}r^2-\gamma_{th}r^{\alpha}\delta^2/P_s\right\}$$
$$\left[-2/\alpha\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\right.$$
$$\left.\left(\gamma_{th}\right)^{\frac{2}{\alpha}}r^{(2-\alpha)}-\gamma_{th}\delta^2/P_s\right]^{m_1}\prod_{l=2}^{m}\left[-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\right.$$
$$\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{\frac{2}{\alpha}}\prod_{j=0}^{l-1}\left(2/\alpha-j\right)r^{2-l\alpha}\right]^{m_l} \tag{E.1.8}$$

Substituting (E.1.8) into (E.1.1),we derive the CDF of γ_{ap} in (8.6).

E.2 Proof of Lemma 2

From (8.2), the CDF of $\gamma_{s,e}$ is given by

$$
\begin{aligned}
F_{\gamma_{s,e}}(\gamma_{th}) &= \Pr\left\{ \max_{e_k \in \Phi_{s,e}} \left\{ \frac{|h_{s_0,e_k}|^2 |X_{s_0,e_k}|^{-\alpha}}{In_{s,e} + \delta^2/P_s} \right\} \leq \gamma_{th} \right\} \\
&= \mathbb{E}_{\Phi_{s,a}}\left\{ \mathbb{E}_{\Phi_{ap,a}}\left\{ \mathbb{E}_{\Phi_{s,e}}\left\{ \prod_{e_k \in \Phi_{s,e}} \Pr\left\{ \frac{|h_{s_0,e_k}|^2 |X_{s_0,e_k}|^{-\alpha}}{In_{s,e} + \delta^2/P_s} \leq \gamma_{th} \middle| \Phi_{s,a}, \Phi_{ap,a}, \Phi_{s,e} \right\} \right\} \right\} \right\} \\
&= \mathbb{E}_{\Phi_{s,a}}\left\{ \mathbb{E}_{\Phi_{ap,a}}\left\{ \mathbb{E}_{\Phi_{s,e}}\left\{ \prod_{e_k \in \Phi_{s,e}} \left(1 - \int_0^\infty e^{-\left(\tau + \delta^2/P_s\right)\gamma_{th}|X_{s_0,e_k}|^\alpha} d\Pr\left(In_{s,e} \leq \tau\right)\right) \right\} \right\} \right\} \\
&= \mathbb{E}_{\Phi_{s,e}}\left\{ \prod_{e_k \in \Phi_{s,e}} \left(1 - e^{-\delta^2 \gamma_{th}|X_{s_0,e_k}|^\alpha/P_s} \mathcal{L}_{In_{s,e}}\left(\gamma_{th}|X_{s_0,e_k}|^\alpha\right)\right) \right\} \\
&\overset{(a)}{=} \exp\left\{ -\lambda_e^s \int_{R^2} e^{-\delta^2\gamma_{th}|X_{s_0,e_k}|^\alpha/P_s} \mathcal{L}_{In_{s,e}}\left(\gamma_{th}|X_{s_0,e_k}|^\alpha\right) d\,|X_{s_0,e_k}| \right\} \\
&\overset{(b)}{=} \exp\left\{ -2\pi\lambda_e^s \int_0^\infty e^{-\delta^2\gamma_{th} r^\alpha/P_s} \mathcal{L}_{In_{s,e}}\left(\gamma_{th} r^\alpha\right) r dr \right\},
\end{aligned} \tag{E.2.1}
$$

where (a) follows from the generating functional of HPPP in [89], (b) is obtained by converting cartesian coordinates to polar coordinates.

Using the generating functional of HPPP in [89], $|h_{i,e_k}|^2 \sim \exp(1)$, and $H_j^{ap,e} = \left| \mathbf{h}_{j,e_k} \frac{\mathbf{h}_{j,sk_j}{}^\dagger}{\left\|\mathbf{h}_{j,sk_j}\right\|} \right|^2 \sim \exp(1)$, we derive the Laplace transform of $I_{s,e}$ and $I_{ap,e}$ as

$$
\begin{aligned}
\mathcal{L}_{I_{s,e}}(s) &= \exp\left(-\int_0^\infty \left[1 - \mathbb{E}_h\left(\exp\left(-s|h_{i,e_k}|^2 y^{-\alpha}\right)\right)\right] \lambda_s \rho_s 2\pi y dy \right) \\
&= \exp\left\{ -\lambda_s \rho_s \pi \Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha) s^{2/\alpha} \right\},
\end{aligned} \tag{E.2.2}
$$

and

$$\begin{aligned}\mathcal{L}_{I_{ap,e}}(s) &= \exp\left(-\int_0^\infty \left[1-\mathbb{E}_h\left(\exp\left(-s\mu H_j^{ap,e} y^{-\alpha}\right)\right)\right]\lambda_{ap}\rho_{ap}2\pi y dy\right)\\ &= \exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\mathbb{E}_h\left\{\left(H_j^{ap,e}\right)^{\frac{2}{\alpha}}\right\}\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}\\ &= \exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}, \end{aligned} \tag{E.2.3}$$

respectively.

With the Laplace transform of $I_{s,e}$ and $I_{ap,e}$, we derive the Laplace transform of $In_{s,e}$ as

$$\begin{aligned}\mathcal{L}_{In_{s,e}}(s) = \exp\Big\{&-\lambda_s\rho_s\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}-\lambda_{ap}\\ &\rho_{ap}\pi\mu^{2/\alpha}\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\Big\}. \end{aligned} \tag{E.2.4}$$

Substituting (E.2.4) into (E.4.1), we derive the CDF of $\gamma_{s,e}$ in (8.7).

E.3 Proof of Lemma 3

From (8.3), the CDF of γ_{sk} is given by

$$\begin{aligned}F_{\gamma_{sk}}(\gamma_{th}) &= \int_0^\infty \Pr\left[\frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}} \le \gamma_{th}\right] f_{|X_{ap_0,sk_0}|}(r)\,dr\\ &= \int_0^\infty \Pr\left[\frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}} \le \gamma_{th}\right] 2\pi\lambda_{sk} r\exp\left(-\pi\lambda_{sk}r^2\right)dr. \end{aligned} \tag{E.3.1}$$

where $f_{|X_{ap_0,sk_0}|}(r)$ is the PDF of the nearest distance between the sink and the typical relay.

The CDF of the sink SINR at distance r from its corresponding relay is derived as

$$\Pr\left[\frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}} \le \gamma_{th}\right] = \mathbb{E}_{\Phi_{ap,a}}\left\{\Pr\left[\|\mathbf{g}_{ap_0,sk_0}\|^2 \le \gamma_{th} r^{\beta}\left(In_{ap,sk}+\delta^2/P_{ap}\right)\middle|\, \Phi_{ap,a}\right]\right\}$$
$$= 1 - \sum_{m=0}^{M-1}\frac{1}{m!}\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^{\infty}\left[\gamma_{th} r^{\beta}\left(\tau+\delta^2/P_{ap}\right)\right]^m \right.$$
$$\left.\exp\left[-\gamma_{th} r^{\beta}\left(\tau+\delta^2/P_{ap}\right)\right] d\Pr\left(In_{ap,sk}\le\tau\right)\right\}. \tag{E.3.2}$$

Note that $\left(-\left(\tau+\delta^2/P_{ap}\right)\gamma_{th}\right)^m e^{-\left(\tau+\delta^2/P_{ap}\right)\gamma_{th}^{\{s\}} r^{\beta}} = \left.\frac{d^m\left(e^{-\gamma_{th}x\left(\tau+\delta^2/P_{ap}\right)}\right)}{dx^m}\right|_{x=r^{\beta}}$, we rewrite (E.3.2) as

$$\Pr\left[\frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}} \le \gamma_{th}\right] = 1 - \mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^{\infty}\exp\left[-\gamma_{th} r^{\beta}\left(\tau+\delta^2/P_{ap}\right)\right] d\Pr\left(In_{ap,sk}\le\tau\right)\right\}$$
$$- \sum_{m=1}^{M-1}\frac{\left(r^{\beta}\right)^m}{m!(-1)^m}\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^{\infty}\left.\frac{d^m\left(e^{-\gamma_{th}x\left(\tau+\delta^2/P_{ap}\right)}\right)}{dx^m}\right|_{x=r^{\beta}} d\Pr\left(In_{ap,sk}\le\tau\right)\right\}$$
$$= 1 - \exp\left(-\gamma_{th} r^{\beta}\delta^2\Big/P_{ap}\right)\mathcal{L}_{In_{ap,sk}}\left(\gamma_{th} r^{\beta}\right) - \sum_{m=1}^{M-1}\frac{\left(r^{\beta}\right)^m}{m!(-1)^m}$$
$$\left.\frac{d^m\left(\exp\left(-\gamma_{th}x\delta^2/P_{ap}\right)\mathcal{L}_{In_{ap,sk}}\left(\gamma_{th}x\right)\right)}{dx^m}\right|_{x=r^{\beta}}. \tag{E.3.3}$$

Since $In_{ap,sk} = \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}}\left|\mathbf{g}_{j,sk_0}\frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,sk_j}\right\|}\right|^2 |X_{j,sk_0}|^{-\beta}$, using the generating functional of HPPP and $\left|\mathbf{g}_{j,sk_0}\frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,sk_j}\right\|}\right|^2 \sim \exp(1)$, we derive the Laplace transform of $In_{ap,sk}$ as

$$\mathcal{L}_{In_{ap,sk}}(s) = \exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)s^{2/\beta}\right\}. \tag{E.3.4}$$

Substituting (E.3.4) into (E.3.3), we obtain

$$\Pr\left[\frac{\left\|\mathbf{g}_{ap_0,sk_0}\right\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}} \le \gamma_{th}\right] = 1-\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\right.$$
$$\left.\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}r^2-\gamma_{th}r^{\beta}\delta^2\Big/P_{ap}\right\}-\sum_{m=1}^{M-1}\frac{\left(r^{\beta}\right)^m}{m!(-1)^m}\frac{d^m\left(U\left(x\right)\right)}{dx^m}\Big|_{x=r^{\beta}}, \qquad \text{(E.3.5)}$$

where $U\left(x\right)=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}x\right)^{2/\beta}-\gamma_{th}x\delta^2/P_{ap}\right\}$.

We then apply the Faà di Bruno's formula to solve the derivative of mth order as follows:

$$\frac{d^m\left[\exp\left(U\left(x\right)\right)\right]}{dx^m}\Big|_{x=r^{\beta}} = \sum\frac{1}{\prod_{l=1}^{m}m_l!l!^{m_l}}\exp\left\{-\lambda_{ap}\rho_{ap}\pi\right.$$
$$\left.\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}r^2-\gamma_{th}r^{\beta}\delta^2\Big/P_{ap}\right\}\left[-\lambda_{ap}\right.$$
$$\left.\rho_{ap}\pi\frac{2}{\beta}\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}x^{2/\beta-1}-\gamma_{th}\delta^2/P_{ap}\right]^{m_1}$$
$$\prod_{l=2}^{m}\left[-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}\prod_{j=0}^{l-1}\left(2/\beta-j\right)x^{2/\beta-l}\right]^{m_l}. \qquad \text{(E.3.6)}$$

Based on (E.3.6), (E.3.5), and (E.3.1), we derive the CDF of γ_{sk} in (8.11).

E.4 Proof of Lemma 4

From (8.4), the CDF of $\gamma_{ap,e}$ is given by

$$
\begin{aligned}
F_{\gamma_{s,e}}(\gamma_{th}) &= \mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{e_k\in\Phi_{ap,e}}\Pr\left\{\frac{|g_{ap_0,e_k}|^2}{In_{ap,e}+\sigma^2/P_{ap}}|X_{ap_0,e_k}|^{-\beta}\le\gamma_{th}\middle|\Phi_{ap,a},\Phi_{ap,e}\right\}\right\}\right\} \\
&= \mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{e_k\in\Phi_{ap,e}}\left(1-\int_0^\infty e^{-\left(\tau+\sigma^2/P_{ap}\right)\gamma_{th}|X_{ap_0,e_k}|^\beta}\,d\Pr\left(In_{ap,e}\le\tau\right)\right)\right\}\right\} \\
&= \mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{e_k\in\Phi_{ap,e}}\left(1-e^{-\sigma^2\gamma_{th}|X_{ap_0,e_k}|^\beta/P_{ap}}\;\mathcal{L}_{In_{ap,e}}\left(\gamma_{th}|X_{ap_0,e_k}|^\beta\right)\right)\right\} \\
&\overset{(a)}{=} \exp\left\{-\lambda_e^{ap}\int_{R^2}e^{-\sigma^2\gamma_{th}|X_{ap_0,e_k}|^\beta/P_{ap}}\mathcal{L}_{In_{ap,e}}\left(\gamma_{th}|X_{ap_0,e_k}|^\beta\right)d\left|X_{ap_0,e_k}\right|\right\} \\
&\overset{(b)}{=} \exp\left\{-2\pi\lambda_e^{ap}\int_0^\infty e^{-\sigma^2\gamma_{th}r^\beta/P_{ap}}\mathcal{L}_{In_{ap,e}}\left(\gamma_{th}r^\beta\right)rdr\right\},
\end{aligned}
\tag{E.4.1}
$$

where (a) follows from the generating functional of HPPP in [89], (b) is obtained by converting cartesian coordinates to polar coordinates.

Using the generating functional of HPPP in [89], we derive the Laplace transform of $I_{ap,e}$ as

$$
\mathcal{L}_{I_{ap,e}}(s) = \exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)s^{2/\beta}\right\}. \tag{E.4.2}
$$

Plugging (E.4.2) into (E.4.1), we derive the CDF of $\gamma_{s,e}$ in (8.12).

References

[1] M. Elkashlan, T. Q. Duong, and H. H. Chen, "Guest editorial-Millimeter wave communications for 5G-Part I: Fundamentals," *IEEE Commun. Mag.*, vol. 52,

no. 9, 2014.

[2] ——, "Guest editorial-Millimeter wave communications for 5G-Part II: Applications," *IEEE Commun. Mag.*, vol. 53, no. 1, Jan. 2015.

[3] H. Zhang, A. F. Molisch, and J. Zhang, "Applying antenna selection in WLANs for achieving broadband multimedia communications," *IEEE Trans. Broadcasting*, vol. 52, no. 4, pp. 475–482, Dec. 2006.

[4] Q. Li, X. E. Lin, J. Zhang, and W. Roh, "Advancement of MIMO technology in WiMAX: from IEEE 802.16d/e/j to 802.16m," *IEEE Commun. Mag.*, vol. 47, no. 6, pp. 100–107, Jun. 2009.

[5] N. B. Mehta, S. Kashyap, and A. F. Molisch, "Antenna selection in LTE: from motivation to specification," *IEEE Commun. Mag.*, vol. 50, no. 10, pp. 144–150, 2012.

[6] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jan. 2012.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[8] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, 2010.

[9] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multi-antenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, 2011.

[10] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc of 45th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, Mar. 2011, pp. 1–5.

[11] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Communications*, vol. 6, no. 16, pp. 2676–2687, 2012.

[12] H. Jeon, S. W. McLaughlin, and J. Ha, "Secure communications with untrusted secondary users in cognitive radio networks," in *Proc of IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, Dec. 2012, pp. 1072–1078.

[13] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, 2011.

[14] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[15] K. J. Kim and T. A. Tsiftsis, "On the performance of cyclic prefix-based single-carrier cooperative diversity systems with best relay selection," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1269–1279, April 2011.

[16] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, 2015, accepted to appear.

[17] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2," Mar. 2013, version 11.5.0 [Online]. Available: www.3gpp.org.

[18] R. Pabst *et al.*, "Relay-based deployment concepts for wireless and mobile broadband radio," *IEEE Commun. Mag.*, vol. 42, no. 9, pp. 80–89, 2004.

[19] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[20] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[21] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[22] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[23] H. V. Poor, "Information and inference in the wireless physical layer,," *IEEE*

Wireless Commun., pp. 40–47, Feb. 2012.

[24] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[25] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, 2007, pp. 2466–2470.

[26] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[27] ——, "Secure transmission with multiple antennas–part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[28] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[29] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[30] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[31] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[32] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[33] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[34] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for

multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

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

[36] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

[37] J. Mitola and J. Maguire, G. Q., "Cognitive radio: making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[38] S. Haykin, "Cognitive radio: Brain-empowered wireles communications," *IEEE Trans. Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[39] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649 –658, Feb. 2007.

[40] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[41] K. J. R. Liu, A. K. Sadek, W. Su, and *et al.*, *Cooperative Communications and Networking*. New York: Cambridge University Press, 2009.

[42] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[43] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[44] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[45] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3,

pp. 1317–1322, Mar. 2011.

[46] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[47] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[48] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[49] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[50] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[51] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, Oct. 2012.

[52] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Outage performance for amplify-and-forward channels with an unauthenticated relay," in *IEEE Int Commun. Conf. (ICC)*, 2012, pp. 893–897.

[53] ——, "Secrecy analysis of unauthenticated amplify-and-forward relaying with antenna selection," in *IEEE Acoustics, Speech and Signal Processing (ICASSP)*, 2012, pp. 2481–2484.

[54] X. Li, M. Chen, and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," in *IEEE Int. Conf. Mechatronics and Automation (ICMA)*, 2005, pp. 1618–1623.

[55] S. Marano, V. Matta, and P. K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *IEEE Trans. Signal Process.*, vol. 57, no. 5,

pp. 1976–1986, May 2009.

[56] R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-layer security for distributed detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1118–1126, Aug 2012.

[57] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 839–850, May 2014.

[58] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[59] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[60] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, June 2014, pp. 2319–2324.

[61] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan 2015.

[62] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sept 2014.

[63] T. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[64] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *IEEE Proc.*, vol. 102, no. 3, pp. 366–385, March 2014.

[65] M. R. Akdeniz, Y. Liu, M. K. Samimi, S. Sun, S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation,"

IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1164–1179, June 2014.

[66] N. Valliappan, A. Lozano, and R. W. H. Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, Aug. 2013.

[67] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *IEEE Signal Process. Advances in Wireless Commun. (SPAWC)*, June 2014, pp. 115–119.

[68] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1312–1321, July 2005.

[69] A. Goldsmith, S. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[70] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug 2002.

[71] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept 2013.

[72] X. Zhou and M. R. Mckay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[73] G. D. Durgin, T. S. Rappaport, and D. A. de Wolf, "New analytical models and probability density functions for fading in wireless communications," *IEEE Trans. Commun.*, vol. 50, no. 6, pp. 1005–1015, June 2002.

[74] J. Frolik, "A case for considering hyper-Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 4, pp. 1235–1239, Apr. 2007.

[75] S. H. Oh, K. H. Li, and W. S. Lee, "Performance of BPSK pre-detection MRC systems over two-wave with diffuse power fading channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2772–2775, Aug. 2007.

[76] H. A. Suraweera, W. S. Lee, and S. H. Oh, "Performance analysis of QAM in a two-wave with diffuse power fading environment," *IEEE Commun. Lett.*, vol. 12, no. 2, pp. 109–111, Feb. 2008.

[77] S. Haghani, "Bit error rate of noncoherent MFSK with $S + N$ selection combining in two wave with diffuse power fading," in *Pro. Global Telecommun. Conf. (GLOBECOM)*, Houston, TX, Dec. 2011, pp. 1–6.

[78] Y. Lu, X. Wang, and N. Yang, "Outage probability of cooperative relay networks in two-wave with diffuse power fading channels," *IEEE Trans. Commun.*, vol. 60, no. 1, pp. 42–47, Jan. 2012.

[79] Y. Lu and N. Yang, "Symbol error rate of decode-and-forward relaying in two-wave with diffuse power fading channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3412–3417, Oct. 2012.

[80] A. Lodhi, F. Said, M. Dohler, and A. H. Aghvami, "Closed-form symbol error probabilities of STBC and CDD MC-CDMA with frequency-correlated subcarriers over Nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 57, no. 2, pp. 962–973, Mar. 2008.

[81] M. Z. I. Sarkar and T. Ratnarajah, "On the secrecy mutual information of Nakagami-m fading SIMO channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2010, pp. 1–5.

[82] B. Sklar, "Rayleigh fading channels in mobile digital communication systems part I: Characterization," *IEEE Commun. Mag.*, vol. 35, no. 7, pp. 90–100, 1997.

[83] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, 2009.

[84] J. G. Andrews, F. Baccelli, and R. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, November 2011.

[85] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550–560, April 2012.

[86] H.-S. Jo, Y. J. Sang, P. Xia, and J. Andrews, "Heterogeneous cellular networks with flexible cell association: A comprehensive downlink sinr analysis," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3484–3495, October 2012.

[87] J. G. Andrews, "Seven ways that hetnets are a cellular paradigm shift," *IEEE Commun. Mag.*, vol. 51, no. 3, pp. 136–144, March 2013.

[88] C. han Lee and M. Haenggi, "Interference and outage in Poisson cognitive networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1392–1401, April 2012.

[89] D. Stoyan, W. Kendall, and J. Mecke, "Stochastic geometry and its applications," *Wiley New York*, vol. 2, 1987.

[90] M. Haenggi, *Stochastic Geometry for Wireless networks.* Cambridge University Press, 2013.

[91] A. Annamalai and C. Tellambura, "A new approach to performance evaluation of generalized selection diversity receivers in wireless channels," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Fall 2001, pp. 2309–2313.

[92] M.-S. Alouini and M. K. Simon, "An MGF-based performance analysis of generalized selection combining over Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 401–415, Mar. 2000.

[93] Y. Ma and C. C. Chai, "Unified error probability analysis for generalized selection combining in Nakagami fading channels," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 11, pp. 2198–2210, Nov. 2000.

[94] R. K. Mallik and M. Z. Win, "Analysis of hybrid selection/maximal-ratio combining in correlated Nakagami fading," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1372–1383, Aug. 2002.

[95] X. Zhang and N. C. Beaulieu, "Performance analysis of generalized selection combining in generalized correlated Nakagami-m fading," *IEEE Trans. Commun.*, vol. 54, no. 11, pp. 2103–2112, Nov. 2006.

[96] Y. Ma, Z. Wang, and S. Pasupathy, "Asymptotic performance of hybrid-selection/maximal-ratio combining over fading channels," *IEEE Trans. Commun.*, vol. 54, no. 5, pp. 770–777, may 2006.

[97] I. Ahmed, A. Nasri, R. Schober, and R. K. Mallik, "Asymptotic performance of generalized selection combining in generic noise and fading," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 916–922, Apr. 2012.

[98] S.-I. Chu, "Performance of amplify-and-forward cooperative diversity networks with generalized selection combining over Nakagami-m fading channels," *IEEE Commun. Lett.*, vol. 16, no. 5, pp. 634–637, May 2012.

[99] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379–389, February 2007.

[100] P. L. Yeoh, M. Elkashlan, Z. Chen, and I. Collings, "Ser of multiple amplify-and-forward relays with selection diversity," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2078–2083, August 2011.

[101] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE Global Telecommun. Conf. (GLOBECOM)*, 2008, pp. 1–5.

[102] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[103] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept 2008.

[104] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[105] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[106] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, April 2013.

[107] D. Chen, S. Yin, Q. Zhang, M. Liu, and S. Li, "Mining spectrum usage data: A large-scale spectrum measurement study," in *Proc. ACM Int. Conf. on Mobile*

Computing and Networking, Beijing, China, Sep. 2009, pp. 13–24.

[108] M. Wellens, J. Wu, and P. Mahonen, "Evaluation of spectrum occupancy in indoor and outdoor scenario in the context of cognitive radio," in *Proc. Int. Conf. on Cognitive Radio Oriented Wireless Networks*, Orlando, FL, Jul. 2007, pp. 420–427.

[109] M. Lopez-Benitez, A. Umbert, and F. Casadevall, "Evaluation of spectrum occupancy in Spain for cognitive radio applications," in *Proc. IEEE Veh. Techno. Conf. Spring*, Barcelona, Spain, Apr. 2009, pp. 1–5.

[110] K. A. Qaraqe, H. Celebi, A. Gorcin, A. El-Saigh, H. Arslan, and M.-S. Alouini, "Empirical results for wideband multidimensional spectrum usage," in *Proc. IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun.*, Tokyo, Japan, Sep. 2009, pp. 1262–1266.

[111] M. H. Islam, C. L. Koh, S. W. Oh, X. Qing, Y. Y. Lai, C. Wang, Y.-C. Liang, B. E. Toh, F. Chin, G. L. Tan, and W. Toh, "Spectrum survey in Singapore: Occupancy measurements and analyses," in *Proc. Int. Conf. on Cognitive Radio Oriented Wireless Networks*, Singapore, May 2008, pp. 1–7.

[112] M. A. McHenry, "NSF spectrum occupancy measurements project summary," Shared Spectrum Co., Tech. Rep., Aug. 2005.

[113] V. N. Q. Bao, L. Q. Cuong, L. Q. Phu, T. D. Thuan, L. M. Trung, and N. T. Quy, "Spectrum survey in Vietnam: Occupancy measurements and analysis for cognitive radio applications," in *Proc. Advanced Techno. for Commun.*, Da Nang, Vietnam, Aug. 2011, pp. 135–143.

[114] J. Mitola and G. Q. Maguire, Jr., "Cognitive radio: making software radio more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[115] E. Biglieri, A. Goldsmith, L. J. Greenstein, N. B. Mandayam, and H. V. Poor, *Principles of Cognitive Radio*. Cambridge, UK: Cambridge University Press, 2013.

[116] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.

[117] H. A. Suraweera, P. J. Smith, and M. Shafi, "Capacity limits and performance

analysis of cognitive radio with imperfect channel knowledge," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1811–1822, May 2010.

[118] C. Zhong, T. Ratnarajah, and K.-K. Wong, "Outage analysis of decode-and-forward cognitive dual-hop systems with the interference constraint in Nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 60, pp. 2875–2879, Jul. 2011.

[119] T. W. Ban, W. Choi, B. C. Jung, and D. K. Sung, "Multi-user diversity in a spectrum sharing system," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 102–106, Jan. 2009.

[120] S. Kato, H. Harada, R. Funada, T. Baykas, C. S. Sum, J. Wang, and M. A. Rahman, "Single carrier transmission for multi-gigabit 60-GHz WPAN systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 8, pp. 1466–1478, Oct. 2009.

[121] IEEE P802.11ad/D0.1, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Enhancements for very high throughput in the 60GHz band," Jun. 2010.

[122] K. J. Kim and T. A. Tsiftsis, "Performance analysis of QRD-based cyclically prefixed single-carrier transmissions with opportunistic scheduling," *IEEE Trans. Veh. Technol.*, vol. 60, pp. 328–333, Jan. 2011.

[123] Y.-C. Liang, W. S. Leon, Y. Zeng, and C. Xu, "Design of cyclic delay diversity for single carrier cyclic prefix (SCCP) transmissions with block-iterative GDFE(BI-GDFE) receiver," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 677–684, Feb. 2008.

[124] D.-Y. Seol, U.-K. Kwon, and G.-H. Im, "Performance of single carrier transmission with cooperative diversity over fast fading channels," *IEEE Trans. Commun.*, vol. 57, pp. 2799–2807, Sep. 2009.

[125] F. Gao, A. Nallanathan, and C. Tellambura, "Blind channel estimation for cyclic-prefixed single-carrier systems by exploiting real symbol characteristics," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 2487–2498, Sep. 2007.

[126] Y. Zeng and T. S. Ng, "Pilot cyclic prefixed single carrier transmission communication: Channel estimation and equalization," *IEEE Signal Process. Lett.*, vol. 12, pp. 56–59, Jan. 2005.

[127] Y. Wang and X. Dong, "Frequency-domain channel estimation for SC-FDE in UWB communications," *IEEE Trans. Commun.*, vol. 54, pp. 2155–2163, Dec. 2006.

[128] H. Chergui, T. Ait-Idir, M. Benjillali, and S. Saoudi, "Joint-over-transmissions project and forward relaying for single carrier broadband MIMO ARQ systems," in *Proc. IEEE Veh. Techol. Conf.*, Yokohama, Japan, May 2011, pp. 1–5.

[129] K. J. Kim, T. A. Tsiftsis, and H. V. Poor, "Power allocation in cyclic prefixed single-carrier relaying systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2297–2305, Jul. 2011.

[130] H. Eghbali, S. Muhaidat, and N. Al-Dhahir, "A novel receiver design for single-carrier frequency domain equalization in broadband wireless networks with amplify-and-forward relaying," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 721–727, Mar. 2011.

[131] T.-H. Pham, Y.-C. Liang, A. Nallanathan, and H. Garg, "Optimal training sequences for channel estimation in bi-directional relay networks with multiple antennas," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 474–479, Feb. 2010.

[132] K. J. Kim and T. A. Tsiftsis, "On the performance of cyclic prefix-based single-carrier cooperative diversity systems with best relay selection," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1269–1279, Apr. 2011.

[133] K. J. Kim, T. Q. Duong, H. V. Poor, and L. Shu, "Performance analysis of cyclic prefixed single-carrier spectrum sharing relay systems in primary user interference," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6729–6734, Dec. 2012.

[134] K. J. Kim, T. Q. Duong, and X.-N. Tran, "Performance analysis of cognitive spectrum-sharing single-carrier systems with relay selection," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6435–6449, Dec. 2012.

[135] K. J. Kim, T. Q. Duong, M. Elkashlan, P. L. Yeoh, H. V. Poor, and M. H. Lee, "Spectrum sharing single-carrier in the presence of multiple licensed receivers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5223–5235, Oct. 2013.

[136] C.-T. Cheng, C. K. Tse, and F. C. M. Lau, "A delay-aware data collection network structure for wireless sensor networks," *IEEE Sensors Journal*, vol. 11, no. 3, pp.

699–710, March 2011.

[137] A. Rasheed and R. Mahapatra, "An energy-efficient hybrid data collection scheme in wireless sensor networks," in *2007. 3rd Int.l Conf. Intelligent Sensors, Sensor Networks and Inf.*, Dec 2007, pp. 703–708.

[138] T. Kwon and J. M. Cioffi, "Random deployment of data collectors for serving randomly-located sensors," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2556–2565, June 2013.

[139] A. Rasheed and R. Mahapatra, "The three-tier security scheme in wireless sensor networks with mobile sinks," *IEEE Trans. Parallel and Distributed Systems*, vol. 23, pp. 958–965, May 2012.

[140] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, C.A.: Academic Press, 2007.

[141] A. Lozano, A. Tulino, and S. Verdú, "High-SNR power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.

[142] M. Spivak, *Calculus*, 3rd ed. Houston, TX: Publish or Perish, 1994.

[143] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. New York: Dover Publications, 1970.

[144] R. H. Y. Louie, M. R. McKay, and I. B. Collings, "New performance results for multiuser optimum combining in the presence of Rician fading," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2348–2358, Aug. 2009.

[145] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2007, pp. 2466–2470.

[146] M. Yuksel and E. Erkip, "Diversity-Multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, 2011.

[147] S. Jin, M. R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[148] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge University Press, 2005.

[149] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[150] P. R. Davis, *Circulant Matrices*. New York: John Wiley, 1979.

[151] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[152] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[153] M. Abramovitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. New York: Dover, 1972.

[154] A. Lozano, A. M. Tulino, and S. Verdú, "High-SNR power offset in multiantenna communication," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, Jun. 2004, p. 287.

[155] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Outage performance for amplify-and-forward channels with an unauthenticated relay," in *IEEE Int Commun. Conf. (ICC)*, 2012, pp. 893–897.

[156] R. H. Y. Louie, Y. Li, H. A. Suraweera, and B. Vucetic, "Performance analysis of beamforming in two hop amplify and forward relay networks with antenna correlation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3132–3141, June 2009.

[157] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.

[158] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[159] E. Björnson, J. Hoydis, M. Kountouris, and M. Debbah, "Massive MIMO systems with non-ideal hardware: Energy efficiency, estimation, and capacity limits," http://arxiv.org/pdf/1307.2584v1.pdf.

[160] J. Zhu, R. Schober, and V. Bhargava, "Secure transmission in multi-cell massive MIMO systems," *IEEE Trans. Wireless Commun.*, no. 99, pp. 1–16, 2014.

[161] E. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[162] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, June 2011.

[163] D. B. da Costa and S. Aissa, "Cooperative dual-hop relaying systems with beamforming over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3950–3954, Aug. 2009.

[164] Y. Ma and S. Pasupathy, "Efficient performance evaluation for generalized selection combining on generalized fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 29–34, Jan. 2004.

[165] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*. New York: Addison-Wesley, 1989.

[166] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1980–1983, Nov. 2004.