Physical layer security in emerging wireless communication systems

Wang, Wei

2018

Wang, W. (2018). Physical layer security in emerging wireless communication systems.
Doctoral thesis, Nanyang Technological University, Singapore.

<http://hdl.handle.net/10356/75652>

<https://doi.org/10.32657/10356/75652>

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

SINGAPORE

**PHYSICAL LAYER SECURITY IN EMERGING
WIRELESS COMMUNICATION SYSTEMS**

WANG WEI

**SCHOOL OF ELECTRICAL AND ELECTRONIC
ENGINEERING**

2018

Physical Layer Security in Emerging Wireless Communication Systems

WANG WEI

School of Electrical and Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfilment of the requirements for the degree of
Doctor of Philosophy

2018

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor, Prof. Teh Kah Chan, for giving me this opportunity to pursue my PhD at Nanyang Technological University (NTU), and for the patient guidance, encouragement and advice he has provided throughout my Ph.D study and research. Without his unselfish help, I could never conduct my doctoral research in NTU. I have been extremely lucky to have a supervisor who cared so much about my work, and who responded to my questions and queries so promptly.

Secondly, I would like to thank my co-supervisor, Prof. Li Kwok Hung, for his insightful comments and constructive suggestions. The discussions with Prof. Li really benefit me and inspire me to rethink my problems from different perspectives. His nice personality and encouragement always gave me power to move ahead.

I would also like to thank my former supervisor, Prof. Liao Guisheng at Xi-dian University for his invaluable guidance and long lasting encouragement. The graduate studies with him stimulated my interests in exploring the unknowns and paved the way for my PhD research. I was so lucky to participate in a big project and got chances to meet those outstanding researchers. His hard working attitude and profound knowledge have influenced significantly on my future academic career.

My sincere thanks also go to Prof. Lu Rongxing (former NTU professor), Prof. Li Dong (Chongqing University), Dr. Luo Sheng (Shenzhen University), Dr. Liu Aifei (Harbin Engineering University), and Dr. Han Shiying (Nankai University)

for the insightful discussions and valuable comments to my work.

I thank my fellow labmates in INFINITUS for the stimulating discussions and all the fun we have had in the last years, including Dr. Zhang Zhiyu, Dr. Tran Xuan Tuong, Dr. Yang Rong, Dr. Zhao Ming, Dr. Bi Hui, Dr. Ma Lijia, Cheng Yanyu, Li Beibei, Wang Guoming, Shao Hongxin, Wang Yang, Zhang Heng, Sun Meng, Gao Yumeng, Zhang Zecen, Liu Ji. The days with you at Singapore were so wonderful. Also I thank my best friends in China: Dr. Liu Songyang, Xu He, Xiang Li, Wang Mingjie, Hu Xiaolong, Gao Bo, Wang Zhao, He Ting, Li Jinqiang, Wu Jiangtao, and Hu Bolin.

Last but not the least, I would like to thank my parents and my sister for supporting me spiritually through my life. In particular, I must thank my wife, Mrs WANG Yirui, without whose love and encouragement, I would not have finished this work.

Abstract

Security has become an increasingly significant and urgent issue in wireless networks. The growing computational capability of the eavesdropper (Eve) and more and more complicated secure key management in large scale and heterogeneous networks, pose more and more stringent requirement to the cryptographic protocols. As a new design paradigm, physical layer security has been recognised as a promising solution to enhance the security of wireless links relying on the channel properties and advanced signal processing, and can act as either an alternative or a complementary solution to the conventional cryptographic methods. Without complicated secure key generation and management, physical layer security is quite suitable for the large scale distributed networks. In this thesis, we aim to improve the secrecy performance in emerging wireless communication systems relying on different physical layer security techniques.

Firstly, the security of an amplify-and-forward successive relaying network with multiple untrusted relay nodes is investigated, where the conventional detrimental inter-relay interference is exploited to jam the untrusted nodes without assistance of external helpers. Considering different complexity requirements, several relay selection schemes are proposed, and the closed-form expressions of the lower bound of the secrecy outage probability and the maximum secrecy diversity order are derived accordingly. It is shown that the maximum secrecy diversity order of $N - 1$ can be achieved for an N relay nodes network.

Secondly, the artificial noise (AN) aided secure transmission strategy for a multiple-input single-output multiple-Eve (MISOME) system with a secure user

(Bob) and a normal user (NU) is investigated. The power allocations among Bob, NU and AN, as well as the wiretap code rates, are jointly optimized to maximize the effective secrecy throughput (EST), under the average throughput constraint of NU. An alternative optimization algorithm with guaranteed convergence is proposed to obtain the optimal parameters. It is shown that the EST increases with the transmitting power and the number of transmit antennas, and decreases with the throughput constraint of NU, and the EST can be improved through injecting AN and concurrent transmission of Bob and NU.

Thirdly, physical layer security in a multi-antenna small-cell network is investigated, where the multi-antenna base stations (BSs), cellular users, and Eves are all randomly distributed according to independent Poisson point processes. Stochastic geometry is applied to analyze the connection and secrecy outage probabilities and the average achievable secrecy rate. The impact of different parameters, including power allocation, BS and Eve density, and the adaptive eavesdropping or jamming on the secrecy performance is analyzed. It is shown that the average secrecy rate is a quasi-concave function of the power allocation factor and monotonically decreases with the ratio of the Eve-BS density.

Finally, we study the physical layer security in a large-scale heterogeneous network consisting of both sub-6 GHz massive multi-input multi-output (MIMO) macro cells and millimeter wave (mmWave) small cells. By considering pilot spoofing attacks from the Eves, the coverage and secrecy probabilities are derived using stochastic geometry and the conditions under which the millimeter wave tier outperforms the sub-6 GHz counterpart are discussed in terms of both coverage and secrecy. It is shown that the mmWave small cell can provide better coverage performance in the high transmission code-rate region, and the secrecy performance of the mmWave system outperforms the sub-6 GHz counterpart in the low redundant rate region, which reveals the advantage of using mmWave for secure communication.

Table of Contents

Acknowledgment	ii
Abstract	iv
Table of Contents	vi
List of Figures	xi
List of Tables	xv
List of Symbols	xvi
List of Abbreviations	xviii
1 Introduction	1
1.1 Background	1
1.2 Research Motivation	3
1.2.1 Untrusted Relaying System	3
1.2.2 Throughput Maximization in MISOME Channels	4
1.2.3 Security in Heterogeneous Networks	5
1.2.4 Impact of Active Attack	6
1.3 Related Works	7
1.3.1 Security in Cooperative Relaying Networks	7
1.3.2 Security in Multi-Antenna Systems	10
1.3.3 Security in Heterogeneous Networks	13

1.3.4	Physical Layer Security with Active Attack	15
1.4	Thesis Contributions and Organization	16
2	Fundamental Concepts	20
2.1	Fundamentals of Physical Layer Security	20
2.1.1	Shannon's Perfect Secrecy	20
2.1.2	Wyner Wiretap Channel	21
2.1.3	Single-Antenna Wiretap Channel	22
2.1.4	MIMO Wiretap Channel	24
2.1.5	Untrusted Relay Channel	26
2.2	Stochastic Geometry	28
2.3	Game Theory	31
2.4	mmWave Communication	33
3	Secure Successive AF Relaying Network with Untrusted Nodes	36
3.1	Introduction	36
3.2	System Model and Problem Statement	37
3.3	Relay Selection Rules with Untrusted Nodes	41
3.3.1	Optimal Successive Relay Selection	41
3.3.2	Max-Min Relay Selection	42
3.3.3	Max-Interference Relay Selection	42
3.3.4	Partial Relay Selection	42
3.4	Secrecy Outage Performance and Asymptotic Analysis	43
3.4.1	Benchmark Single-Path Relay Selection Scheme	43
3.4.2	Max-Min Relay Selection	45
3.4.3	Max-Interference Relay Selection	48
3.4.4	Partial Relay Selection	50
3.5	Numerical Results and Discussions	51
3.6	Summary	55

4	Secrecy Throughput Maximization for MISOME Wiretap Channels	57
4.1	Introduction	57
4.2	System Model and Problem Statement	58
4.2.1	System Model and Preliminary	58
4.2.2	Problem Statement	61
4.3	Non-Adaptive Transmission Scheme	63
4.3.1	Optimization for Normal User	64
4.3.2	Power Allocation Optimization for Bob	67
4.3.3	Code Rate Optimization	70
4.4	Adaptive Transmission Scheme	72
4.5	Numerical Results and Discussions	75
4.6	Summary	78
5	Physical Layer Security in Multi-Antenna Small-Cell Networks	80
5.1	Introduction	80
5.2	System Model	81
5.2.1	User Association and Channel Model	82
5.2.2	Wiretap Code and AN Transmission Scheme	83
5.2.3	SIR Expression and Preliminary	84
5.3	Outage Probability Analysis	85
5.3.1	Connection Outage Probability	85
5.3.2	Secrecy Outage Probability	89
5.4	Secrecy Area Spectral Efficiency Analysis	91
5.4.1	Fixed-Rate Transmission	91
5.4.2	Adaptive-Rate Transmission	92
5.5	Extension to Dense Network	94
5.6	Impact of Adaptive Eves	97
5.6.1	Outage Probability Analysis	99
5.6.2	Stackelberg Game Formulation	102

5.7	Numerical Results and Discussions	106
5.8	Summary	117
6	Physical Layer Security in Heterogeneous Networks with Pilot Attack	119
6.1	Introduction	119
6.2	System Model	120
6.2.1	Sub-6 GHz Channel Model	120
6.2.2	mmWave Channel Model	122
6.2.3	Mobile Association Rule	126
6.2.4	Performance Metrics	127
6.3	Coverage Performance Analysis	128
6.3.1	Sub-6 GHz Tier	129
6.3.2	mmWave Tier	132
6.4	Secrecy Performance Analysis	136
6.4.1	Sub-6 GHz Tier	136
6.4.2	mmWave Tier	138
6.5	Numerical Results and Discussions	139
6.6	Summary	145
7	Conclusions and Future Works	146
7.1	Conclusions	146
7.2	Future Works	148
	Appendix A Proofs of Theorems in Chapter 3	150
A.1	Proof of Theorem 3.1	150
A.2	Proof of Theorem 3.2	151
A.3	Proof of Theorem 3.3	153
	Appendix B Proofs of Theorems in Chapter 4	155
B.1	Proof of Theorem 4.1	155

B.2	Proof of Theorem 4.2	157
B.3	Proof of Theorem 4.3	158
Appendix C Proofs of Theorems and Propositions in Chapter 5		160
C.1	Proof of Theorem 5.1	160
C.2	Proof of Proposition 5.2	162
C.3	Proof of Theorem 5.2	163
C.4	Proof of Proposition 5.3	164
C.5	Proof of Theorem 5.3	165
C.6	Proof of Proposition 5.4	166
Appendix D Proofs of Propositions in Chapter 6		168
D.1	Derivation of Equation (6.32)	168
D.2	Proof of Proposition 6.1	170
D.3	Proof of Proposition 6.3	171
D.4	Proof of Proposition 6.4	172
Author's Publications		174
Bibliography		176

List of Figures

2.1	Shannon's model of a secrecy system.	20
2.2	The wiretap channel model.	21
2.3	The general DMC broadcast wiretap channel model.	22
2.4	The Gaussian MIMO wiretap channel.	25
2.5	The untrusted relay channel model.	27
2.6	A random network model, where the solid circles and squares denote the BSs and users, respectively.	29
2.7	Illustration of a heterogeneous network.	34
3.1	Successive relaying model, where only nodes i and j are activated: (a) transmission in the odd time slot, (b) transmission in the even time slot.	37
3.2	Secrecy outage probability vs SNR for different schemes, with $N =$ 3 , $L = 50$, and $\bar{R} = 2$ bps/Hz.	52
3.3	Secrecy outage probability vs SNR for different schemes, with $N =$ 4 , $L = 50$, and $\bar{R} = 2$ bps/Hz.	53
3.4	Secrecy outage probability vs SNR for different N , with $L = 50$, and $\bar{R} = 2$ bps/Hz.	54
3.5	Secrecy outage probability vs the target secrecy rate for different N , with $L = 50$ and SNR=20 dB.	54
3.6	Secrecy outage probability vs IRI for different transmit power levels, where $N = 4$, $L = 50$, and $\bar{R} = 2$ bps/Hz.	55

3.7	Ergodic secrecy rate vs SNR for different schemes, where $N = 4$, $L = 10$, and 50.	56
4.1	The MISOME wiretap channel model.	58
4.2	The CDF of γ_E , where $N = 8$, $P=10$ dB, $\phi_b = 0.5$, and $\phi_u = 0.3$. . .	62
4.3	The EST vs. ϕ_b for different parameters, with $\bar{P} = 10$ dB, $M = 5$, and $\tau = 1$ bps/Hz.	69
4.4	The optimal value of ϕ_b vs. N , with $R_b = 4$ bps/Hz, $R_s = 3$ bps/Hz, $M = 10$, and $\tau = 2$ bps/Hz.	70
4.5	The EST vs. R_s with different parameters, where $M = 5$ and $\tau = 2$ bps/Hz.	71
4.6	The EST vs. ϕ_b with different parameters, where $N = 10$, $M = 3$, $R_b = 5$ bps/Hz, and $\phi_u = 0.2$	74
4.7	The EST of the non-adaptive scheme vs. N with different trans- mitting power, where $M = 5$ and $\tau = 5$ bps/Hz.	76
4.8	The EST of the non-adaptive and adaptive transmission schemes vs. $\bar{P}$ with different N and τ , where $M = 5$	77
4.9	The EST of the non-adaptive and adaptive transmission schemes vs. τ with different parameters, where $\bar{P} = 20$ dB.	77
4.10	The secrecy performance comparison among different schemes, where $M = 5$ and $\tau = 4$ bps/Hz.	78
5.1	A small cell network model, where the BSs, cellular users, and Eves are distributed according to three independent homogeneous PPPs. . .	81
5.2	A multi-cell cellular network model, where each Eve can act as either a passive Eve or an active jammer.	98
5.3	The secrecy throughput vs. the secrecy rate R_s with different λ_e , where $\mu = 1.5$, $\epsilon = 0.1$, and $R_t = 2$ bps/Hz.	106
5.4	Connection outage probability vs. λ_b with different λ_u and λ_e	108
5.5	Secrecy outage probability vs. λ_b with different λ_u and λ_e	108

5.6	Connection and secrecy outage probabilities vs. ϕ , where $\lambda_b = 0.0002$ and $\lambda_u = 0.001$	109
5.7	Secrecy area spectral efficiency vs λ_b , where $\lambda_e = 0.00025$ and $\epsilon = 0.1$.	110
5.8	The optimal power allocation vs λ_b , where $\lambda_e = 0.00025$ and $\epsilon = 0.1$.	111
5.9	Average secrecy rate vs. N , where $\lambda_u = 0.001$	111
5.10	Average secrecy rate under different Eve density and path loss factor, where $\lambda_b = 0.0002$	112
5.11	Average secrecy rate vs. ϕ , where $\lambda_u = 0.0005$	112
5.12	Average secrecy rate vs. number of users K , where $\lambda_b = 0.0002$, $\lambda_e = 0.0003$, and $\lambda_u = 0.004$	113
5.13	SASE vs. number of users K , where $\lambda_b = 0.0002$, $\lambda_e = 0.0003$, and $\lambda_u = 0.004$	114
5.14	The secure transmission probability under different schemes, where $\lambda_b = 0.001$, $\lambda_u = 0.002$, $\phi = 0.5$, $R_t = 2$ bps/Hz, and $R_s = 1$ bps/Hz.	114
5.15	The feasible region under different λ_b , where $\lambda_u = 0.002$, $\phi = 0.5$, $R_t = 2$ bps/Hz, and $R_s = 1$ bps/Hz.	115
5.16	The secure transmission probability under different schemes, where $\lambda_u = 0.002$ and $R_t = 2$ bps/Hz.	116
5.17	The secrecy throughput under different schemes, where $\lambda_u = 0.002$ and $R_t = 2$ bps/Hz.	116
6.1	Beam sweeping based beam alignment.	124
6.2	The association probability under different threshold and SBS density, where $\lambda_\mu = 10$ BSs/km ² , $P_\mu = 43$ dBm, $P_m = 30$ dBm, $K = 10$.	127
6.3	The coverage probability versus the MBS density, where $N_\mu = 64$, $\alpha_\mu = 2.6$, $K = 2$, $\phi = 0.7$, and $R_b = 20$ Mbps.	132
6.4	The success probability of beam alignment.	134
6.5	The coverage probability of the sub-6 GHz tier and the mmWave tier under different CSI cases, where $\lambda_\mu = \lambda_m = \lambda_E = 20$ BSs/km ² , $\phi = 0.7$, $K = 1$	140

6.6	The coverage performance comparison between the sub-6 GHz tier and the mmWave tier, where $\lambda_E = 20$ BSs/km ² , $\phi = 0.7$, $K = 1$. . .	141
6.7	The secrecy probability of the sub-6 GHz tier and the mmWave tier under different CSI cases, where $\lambda_\mu = \lambda_m = \lambda_E = 20$ BSs/km ² , $\phi = 0.7$, $K = 1$	142
6.8	The secrecy performance comparison between the sub-6 GHz tier and the mmWave tier, where $\lambda_E = 20$ BSs/km ² , $\phi = 0.7$, $K = 1$. . .	143
6.9	The coverage probability of a typical user, where $\lambda_\mu = 20$ BSs/km ² , $\lambda_E = 40$ BSs/km ² , $P_\mu = 43$ dBm, $\phi = 0.7$, $K = 10$, $\tau = -10$ dBm. .	144
6.10	The secrecy probability of a typical user, where $P_\mu = 43$ dBm, $\phi = 0.7$, $K = 10$, $R_e = 5$ Mbps, $\tau = -10$ dBm.	144

List of Tables

3.1	The Transmission Protocol of AF Successive Relaying, when L is even.	39
-----	--	----

List of Symbols

Throughout this thesis, bold symbols in capital and lower-case letter denote matrices and vectors, respectively. Specifically, the special functions listed below follow the definition in [1].

$(\cdot)^T$	Transpose operation
$(\cdot)^*$	Conjugate
$(\cdot)^H$	Conjugate transpose
$\mathbf{A}^\dagger$	Inverse of a matrix $\mathbf{A}$
$\mathbf{I}_N$	$N \times N$ identity matrix
$ \cdot $	Absolute
$\ \cdot\ $	Euclidean norm
$\mathbb{P}(\cdot)$	Probability
$\mathbb{1}(\cdot)$	Indicator function
$\mathcal{CN}(\mu, \sigma^2)$	Gaussian distribution with mean μ and variance σ^2
$\text{Exp}(\lambda)$	Exponential distribution with mean $1/\lambda$
$\text{Gamma}(N, \lambda)$	Gamma distribution with shape N and rate λ
$\gamma(a, x)$	Lower incomplete gamma function
$\Gamma(a, x)$	Upper incomplete gamma function
${}_2F_1(\cdot)$	Gauss hypergeometric function
$\text{erf}(\cdot)$	Error function

$B(\cdot)$	Beta function
$B_x(p, q)$	Incomplete beta function
$\ \cdot\ _1$	the l_1 induced matrix norm
$D_n(\cdot)$	Parabolic cylinder function
$\text{Ei}(\cdot)$	Exponential integral function
$[x]^+$	Maximum between x and zero, i.e., $\max(x, 0)$

List of Abbreviations

5G	Fifth Generation
AF	Amplify-and-Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BS	Base Station
CDF	Cumulative Distribution Function
CSI	Channel State Information
D2D	Device-to-Device
ESC	Ergodic Secrecy Capacity
ESR	Ergodic Secrecy Rate
EST	Effective Secrecy Throughput
FD	Full-Duplex
HD	Half-Duplex
HetNet	Heterogeneous Network
i.i.d.	Independent and Identically Distributed
IoT	Internet of Things
IoV	Internet of Vehicles
IRI	Inter-Relay Interference

LoS	Line-of-Sight
MIMO	Multiple-Input Multiple-Output
MIMOME	Multiple-Input Multiple-Output Multiple-Eve
MISO	Multiple-Input Single-Output
MISOME	Multiple-Input Single-Output Multiple-Eve
MMSE	Minimum Mean Square Error
mmWave	Millimeter Wave
MRT	Maximum-Ratio Transmission
NE	Nash Equilibrium
NLoS	Non-Line-of-Sight
PDF	Probability Density Function
PPP	Poisson Point Process
RCI	Regularized Channel Inversion
SASE	Secrecy Area Spectral Efficiency
SDP	Semi-Definite Programming
SI	Self-Interference
SINR	Signal-to-Interference-plus-Noise Ratio
SIR	Signal-to-Interference Ratio
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
TDD	Time-Division Duplex
ZFBF	Zero-Forcing Beamforming

Chapter 1

Introduction

1.1 Background

Driven by the ever-increasing smart applications and the proliferation of smart devices, the next generation (fifth generation, 5G) wireless network is envisioned to support magnitudes of increase in data rates and connectivity, with an extremely low latency and energy consumption [2, 3]. For example, the emerging multimedia entertainment applications, such as augmented reality, mobile video or audio streaming, and online gaming, usually require Gbps of data rate transmission, which results in an exponential growth in mobile data traffic. Apart from providing a very high data rate for a large number of users, 5G network is also responsible for supporting massive simultaneous connections of various sensors encompassing Internet of Things (IoT), Internet of vehicles (IoV), ehealthcare, and smart metering. To achieve these goals, some candidate technologies, such as network densification (small cell network), millimeter wave (mmWave) communication, and massive multiple-input multiple-output (MIMO), are expected to be adopted in 5G [2–4].

Meanwhile, in the 5G enabled connected society, a variety of confidential and sensitive services, e.g. transaction records, private health data and activity history, will be transmitted through the wireless networks. However, the open and

broadcast nature of the wireless medium grants opportunities for external eavesdroppers (Eves) to overhear the confidential information, which incurs severe security threats. Therefore, security and privacy become more and more significant for the connected society.

Previously, security is realized through secret key based cryptographic technology at the network layer [5–7] by assuming that the computational capability of the adversary is limited [6] and secure key generation and distribution can be guaranteed [7]. In these protocols, the information is first encrypted with a secret key at the transmitter side and then decrypted at the receiver side with corresponding secret key. Due to the absence of the secrecy key or limited computational capability, the Eves can not correctly decrypt the ciphertext. However, the growing computational capability of the Eves, more and more connected lightweight resource-constrained devices, together with the rapid evolution of large scale and heterogeneous networks (HetNets), pose more and more stringent requirements to the implementation of the cryptographic protocols and thus limit the application in future wireless networks.

Motivated by these challenges, physical layer approaches relying on the characteristics of wireless channels, such as noise and fading, have been recognised as promising solutions to enhance security in emerging wireless networks. Without using cryptographic protocols, physical layer security mechanisms are quite suitable for the emerging distributed large scale networks. With advanced signal processing, physical layer security can provide a robust solution for enhancing wireless security and can act as either an alternative or a complementary solution to the conventional cryptographic techniques. Recently, this information-theoretical based security approach has received extensive research interests from both industry and academia [8–13].

In general, physical layer security techniques can be divided into two branches, i.e., physical layer secure key generation [14–18] and keyless secure transmission schemes [9, 11–13]. Relying on channel reciprocity and the fact that a passive

Eve who is separated larger than half-wavelength away from the legitimate user will obtain uncorrelated channel measurements in a rich scattering environment, secret key can be generated at legitimate nodes. However, the key generation rate is highly dependent on the channel dynamics and variations and group key generation remains a challenging issue due to the different channel characteristics among different users, resulting in a limited application of physical layer key generation in large scale multi-user networks. In this thesis, we focus on secrecy enhancement for the keyless transmission schemes in the presence of both passive and active Eves in emerging wireless communication systems, including relaying system, multi-antenna system, and HetNets.

1.2 Research Motivation

In this section, the research motivations of physical layer security in different wireless systems are highlighted.

1.2.1 Untrusted Relaying System

Different from wireline communications that are free of interference, channel impairments arising from multi-path fading and co-channel interference make it a great challenge for reliable communications through wireless channels. Cooperative communication is a promising solution to mitigate the fading effect and improve the diversity and reliability of wireless transmissions, especially for systems without multiple antennas, such as ad hoc and wireless sensor networks. In particular, relay nodes within the coverage of the access point can be used either to improve the service quality of the main channel by relaying the information or to degrade the wiretap channel by injecting jamming signals to Eves. In this sense, cooperative relaying is an effective approach to improve the secrecy performance of wireless transmissions.

However, due to the half-duplex (HD) operation in a relay system, each Eve

has two opportunities to intercept the information. Moreover, the relay nodes, usually belonging to a third party operators, may be untrustworthy, i.e., the relay nodes may try to decode the received information as they have different security clearance from the source-destination pair. In this case, the relay nodes can be regarded as potential Eves. It has shown that employing the untrusted node can achieve a higher secrecy rate than just treating it as Eve [19–21].

Through dedicated transmission schedule, compute-and-forward relaying, and nested lattice coding strategy, it was shown in [22] that the positive end-to-end secrecy rate can be achievable independent of the number of hops. However, for the common AF relaying protocol with Gaussian signaling without utilizing the structured codes, the ergodic secrecy capacity (ESC) has been shown to decrease with the number of untrusted relay nodes in [23], and the achievable diversity order in a multi-relay network with destination aided jamming has proven to be limited to one, regardless of the number of untrusted nodes [24]. Hence, how to achieve secure transmission and how to improve the diversity in an untrusted relaying system remain very challenging. In light of this motivation, part of this thesis is focused on improving the diversity order of the untrusted relaying system, which will be presented in Chapter 3.

1.2.2 Throughput Maximization in MISOME Channels

Multiple-antenna technology has been shown to be able to effectively boost the secrecy performance by exploiting the spatial degrees of freedom. The beamforming, power allocation, and artificial noise (AN) design have been investigated relying on advanced optimization methods with perfect or imperfect channel state information (CSI) assumptions. Note that due to the passive and hidden property of Eves, even imperfect CSI of Eves is unlikely to be obtained at the transmitter side. With statistical CSI of Eves, security performance can be measured statistically with ergodic secrecy rate (ESR) [25] or secrecy outage probability (SOP) [26]. Considering the challenges in deriving the probability statistics of the signal-to-

interference-plus-noise ratios (SINRs) [27,28], ergodic secrecy performance analysis is usually conducted with the aid of large-system analysis.

On the other hand, in multi-user scenarios, the inter-user interference arising from concurrent multi-stream transmission over the broadcast channel makes the design and optimization of secure communication more complicated. Both of the inter-user interference and information leakage should be carefully dealt with to meet various requirements of different users, especially in the scenarios with mixed secure users (Bob) and normal users. Recent studies also reveal the significance of wiretap code rates on the secrecy performance [29–31], which motivates a joint optimization of code rates in conventional beamforming and power allocation design.

Considering the coexistence of secure users and normal users, the optimal power allocation and code rates that maximize the secrecy capacity of the secure user under the normal user’s throughput constraint remain unexplored, which motivates the work in Chapter 4. It is crucial to note that in this model, the conventional inter-user interference can be used to confuse the Eve, which may benefit the whole system if the parameters are properly designed. Due to the throughput constraint of the normal user, the optimization becomes more challenging than existing schemes.

1.2.3 Security in Heterogeneous Networks

The increasingly densely deployed low-power small cell base stations (BSs) driven by the increasing data traffic in small areas makes the coverage of cellular BSs more and more irregular, resulting in the deviation of the conventional hexagonal grid BS model from their real deployment. Therefore, random spatial models, such as the Poisson point process (PPP) model, have been recently adopted to analyze cellular networks. It has been shown that the user’s SINR in a real deployment is upper bound by that in the ideal grid model and is lower bounded by that of the random model [32]. In addition, the upper bound and lower bound have similar

accuracy. Relying on the tractability of PPP models, notable analytical results and performance insights can be obtained by leveraging stochastic geometry tools [33].

However, the large-scale random network makes security more and more challenging due to the complicated key generation and management, which motivates the application of physical layer security in this case. On the other hand, in conventional networks, Eves are assumed to be fixed, which is a too optimistic assumption since Eves may be randomly located to achieve maximal revenue and reduce the risk to be detected at the same time. The spatial randomness of Eves can also be captured by the PPP model. Note that physical layer security has been investigated recently in both ad hoc networks [34, 35] and cellular networks [36, 37]. For the cellular system, the introduction of AN for enhancing security makes it more challenging to characterize the inter-cell interference and the achievable secrecy rate and outage performance. Motivated by this, the power allocation, impact of system parameters, and adaptive eavesdropping or jamming on the secrecy performance are evaluated in Chapter 5 for a small cell network, and in Chapter 6 for a heterogeneous network.

1.2.4 Impact of Active Attack

Most of the existing works on physical-layer security assume that the Eves are totally passive. In practice, the Eves may be much smarter than what we have assumed, i.e., in addition to overhearing the information transmission, they can also adaptively act as smart jammers by sending some jamming signals to confuse the legitimate receivers [38–41]. It has been shown that a full-duplex (FD) active Eve with jamming and eavesdropping capability can greatly decrease the achievable secrecy rate [40]. For a random network with multiple HD Eves, those Eves who are far away from the BS can act as jammers since the eavesdropping capacity will be determined by the nearest Eve. To maximize the Eve’s revenue (SOP or eavesdropping capacity), the jamming interference to the passive Eves should be managed properly and the optimal strategy of each Eve should be determined

adaptively. The fundamental question that whether an Eve should act as a passive Eve or an active jammer and the conditions enable adaptive eavesdropping is investigated in Chapter 5.

On the other hand, Eves may also launch jamming attacks during the channel training phase by sending the same pilot sequence to confound the transmitter about the channel to be estimated, resulting in an imperfect channel estimation and more information leakage at the Eves [42,43]. In particular, when the jamming power is strong enough, the estimated channel will be dominated by the Eve's channel and thus the beamformer will beam towards the Eve, making conventional beamforming and AN based secure transmission schemes ineffective [44]. The pilot attack or pilot contamination attack makes security even more challenging in mmWave communication systems since the mmWave transmitting beam may not be perfectly aligned with the receiving beam in the presence of pilot attacks.

The impact of pilot attack on the secrecy performance in conventional cellular network and the mmWave system has not been investigated. Integrating this issue with conventional pilot contamination, physical layer security in a multi-cell HetNet consisting of both conventional massive MIMO macro cells and mmWave enables small cells is investigated in Chapter 6.

1.3 Related Works

In this section, some related works of the aforementioned topics in physical layer security will be presented.

1.3.1 Security in Cooperative Relaying Networks

For a simple four-node network with one source, one destination, one Eve and one helper, when the source-to-destination direct link is available, the fundamental question that whether to use the external helper node as an information relay or a friendly jammer has been discussed in [45] and [46]. The secrecy capacity and

optimal power allocations at the source and the helper were investigated in [45] for both individual and joint power constraints. The effect of the position of the relay node has been discussed in [47], it has been shown that employing a relay node will improve the secrecy performance, and the improvement increases with the path loss. Moreover, it has been shown that the randomize-and-forward relaying scheme always outperforms the decode-and-forward (DF) scheme.

For the scenario that multiple cooperative nodes are available, cooperative relaying [48], cooperative jamming [49–52], and hybrid relaying and jamming schemes [53–57] have been developed to improve the secrecy performance. When the instantaneous CSI of Eves is available, null space beamforming has been employed at the relay nodes to nullify the information leakage to Eve in [58, 59]. In [48], the achievable secrecy rate was maximized under the total power constraint and it has been shown that relay cooperation can significantly enhance the secrecy performance. However, in practice, it is difficult to obtain the CSI of the Eves due to the passive eavesdropping property. Without knowing the Eves' CSI, joint relay and jammer selection and jamming precoding were proposed to improve the security in single antenna and multi-antenna cases, respectively in [60]. With the assumption that only the statistical CSI of Eve is available, ESC [54, 61] and SOP [47, 55, 61–65] are common secrecy performance measurements corresponding to delay tolerant or adaptive rate transmission and delay sensitive or fixed rate transmission scenarios, respectively. In [54], the best node was selected among all the candidates to forward the information while the others acted as friendly jammers to confuse Eve, and the ESR was maximized by optimizing the power allocation between information and jamming signals. The impact of relay or jammer selection on the secrecy performance was discussed in [62], and the exact expressions of the SOP were derived for three different transmission schemes, i.e., direct transmission, amplify-and-forward (AF) relaying, and cooperative jamming schemes. When all the nodes are equipped with multiple antennas, the impact of antenna selection on the secrecy performance has also been evaluated in [61].

Destination assisted jamming power allocation was optimized in [64] to minimize the SOP. A multi-relay selection was also considered in [55,65] to further improve the SOP performance by jointly optimizing the power allocation factor and the number of selected relay nodes.

With recent advances in self-interference (SI) cancellation technologies, e.g., natural isolation, auxiliary antenna, time domain cancelation, and space cancelation techniques (see [66–68] and references therein), researchers have shown the feasibility of in-band FD wireless communication, which allows radios to receive and transmit on the same frequency band simultaneously, and thus doubles the spectrum efficiency. Physical layer security with FD relay was considered in [56], and analysis has shown that FD relay networks can achieve better secrecy performance than the counterpart of HD relay networks, if the SI can be well suppressed. Joint cooperative relaying and jamming protocol based on FD relay to increase the source-destination secrecy rate was presented in [69,70]. In this protocol, the FD relay will first receive data and jam the Eve simultaneously, and then the relay forwards the data with the source jamming the Eve. Achievable secrecy rates of the proposed scheme in the presence of different Eves and SI have been derived and compared with traditional HD relaying scheme. Significant improvements in the secrecy rate over the HD relay can be achieved. These results have been extended to multi-hop relaying systems [71], two-way relaying [72], and MIMO FD relaying systems [73].

For an untrusted relaying system, the fundamental question that whether cooperation with the untrusted node can improve the secrecy rate was explored in [20]. It was shown that, using the untrustworthy node could achieve a higher secrecy rate than just treating it as an Eve. In [23], the closed-form expression of the lower bound of the ESC was derived for an AF relaying system with both single and multiple untrustworthy nodes. However, it has been shown that, when the relay nodes are untrustworthy, increasing the number of relay nodes will worsen the secrecy performance, which is in contrast with conventional results of trusted

nodes. The capacity scaling law and achievable diversity order were derived in [24] for an untrusted relay network with multiple nodes. It has been proved that when destination intended jamming was considered, the achievable diversity order for either the distributed beamforming scheme or the opportunistic relaying scheme is limited to one, regardless of the number of untrusted nodes. The optimal power allocation between the source and the destination aided jamming was investigated in [74], and both asymptotic and large system analyses were presented. When the source-to-destination direct link is available, switching between the direct link and the triangle link was considered in [75], and the closed-form expression of the lower bound of SOP was derived. It has been shown that when the required secrecy rate was larger than a certain threshold value, employing the untrusted relay would be unnecessary. The results were extended to a MIMO case [76, 77], and joint source and relay beamforming design was considered. In [76], the conditions under which the cooperative scheme could achieve a higher secrecy rate than the noncooperative scheme were derived in both low and high signal-to-noise ratio (SNR) regimes of the source-relay and relay-destination links. A two-way relay model was incorporated in [77], and the two-phase and three-phase transmission strategies were compared.

1.3.2 Security in Multi-Antenna Systems

The secrecy capacity is defined as the maximum secrecy transmission rate at which the Eve cannot decode any information. It was proved that in an additive white Gaussian noise (AWGN) channel, the secrecy capacity was equal to the capacity difference between the main channel and that of the wiretap channel [78]. Hence, positive secrecy capacity is achievable only if the wiretap channel is a degraded version of the main channel. By exploiting the spatial degrees of freedom, multi-antenna techniques can effectively boost the secrecy performance either by enhancing channel quality to the legitimate destination through transmit beamforming and antenna selection or by deteriorating the channel condition to

the Eve through deliberately injecting AN, and have received extensive research efforts over the past years [9, 11, 12, 79].

When perfect CSI is known to all terminals, the beamforming strategy has been proven to be able to achieve the secrecy capacity of the multiple-input single-output multiple-Eve (MISOME) wiretap channel [80], where the source and Eves are equipped with multiple antennas and the receiver has only one antenna. The result was extended to MIMO multiple-Eve (MIMOME) wiretap channels in [81]. It was shown that through independent coding across the parallel channels obtained by generalized singular value decomposition, the secrecy capacity can be achieved. However, the results are based on the perfect CSI assumption, which is usually not the case in practice, especially for the Eves due to their passive property. Fortunately, it has been proved in [82] that positive secrecy rate is achievable even when the Eve's CSI is completely unknown to the legitimate transmitter, as long as Eve has fewer antennas than the transmitter and its intended receiver. Based on the deterministic model, robust beamforming methods were also developed in [83] considering both perfect and imperfect CSI of the main and Eve's channel. Robust transmission covariance design for MISO wiretap channels with cooperative jamming was investigated in [84] considering the imperfect CSI of Eve's channel. To reduce the CSI overheads, transmit antenna selection was also considered in [85–87].

Note that both the transmit beamforming and antenna selection techniques aim to enhance the capacity of the main channel. To further improve the secrecy performance, interference or AN [88] can also be exploited to degrade the capacity of Eve. When perfect CSI of the legitimate and Eve's channels is available, a closed-form expression of an achievable secrecy rate was derived and power allocation between the information signal and AN was optimized in [89]. Joint optimization of the transmit signal and AN covariances for secrecy rate maximization was considered in [90] by using semi-definite programming (SDP) approach with both perfect and imperfect Eve's CSI. To deal with imperfect CSI in both the main and

wiretap channels, Tang *et al.* [91] proposed a robust beamforming scheme to maximize the worst-case secrecy rate via SDP. AN-aided beamforming with limited feedback from a legitimate single-antenna receiver was considered in [92], and the optimal allocation strategy of feedback bits was explored. Considering statistical CSI of the wiretap channel and perfect legitimate CSI, achievable secrecy rate was maximized with beamforming and power allocation in MISO [93] and MIMO [94] systems. Secrecy constrained throughput maximization was investigated in [95] over slow fading channels, and transmit power allocation and the rate parameters were jointly optimized with both fixed-rate transmission and adaptive-rate transmission schemes.

In MIMO multi-user broadcast channels, the secrecy capacity is affected by both the desired signal and inter-user interference, which makes the secure transmission more challenging. The capacity region of the two user Gaussian MIMO broadcast channel with common and confidential messages were derived in [96]. In [97,98], it was assumed that any intended user was also a potential Eve to other users, and the achievable secrecy sum rate was maximized with the regularized channel inversion (RCI) precoder. The closed-form expression for the optimal regularization parameter was obtained with the aid of large-system analysis. In the multiuser downlink with a passive Eve, the ergodic secrecy sum rate was derived when the source node was equipped with massive antennas [27,28]. When the users' CSI is not perfectly known, it has been shown that more power should be allocated to AN with the increase of the channel estimation errors [28]. Wang *et al.* considered joint power and subcarrier allocation in a multi-user downlink orthogonal frequency-division multiple access (OFDMA) network with coexistence of Bob and normal users (NUs) [99], where Bob and NUs require secure and normal data services, respectively. The average aggregate data rate of all NUs is maximized under the constraint of secrecy rate of Bob.

Recently, physical layer security was also extended to massive MIMO systems [100]. When the BS is equipped with large number of antennas, simple

precoding/combining yields large gains in spectrum and energy efficiency since the channels to different users become quasi-orthogonal. Physical layer security in a single cell downlink massive MIMO system was discussed in [101]. It was shown that the secrecy capacity could be enhanced by increasing the number of BS antennas. However, for a multi-cell case, it was shown that the ESR suffered a ceiling effect due to the presence of pilot contamination [102]. It also revealed that AN was necessary to achieve a positive ESR and the random AN transmission scheme could achieve similar performance with the conventional null-space based AN transmission scheme.

1.3.3 Security in Heterogeneous Networks

Under the framework of stochastic geometry, physical layer security has been investigated taking the spatial randomness of nodes into account in single cell networks [103–109], ad hoc networks [34, 35, 110, 111], and multi-cell networks [36, 37, 112–114], respectively.

The transmission SOP was derived in a multi-antenna transmission system with Poisson distributed Eves in [103], and it revealed that a slight increase in the number of transmit antennas can effectively decrease the outage probability. The effect of spatial randomly distributed Eves on the AN power allocation and the wiretap code rate in a multi-input single-output (MISO) system was discussed under perfect CSI [104] and imperfect CSI [105] assumptions, respectively. In [106], when both the legitimate nodes and Eves were randomly located, the secure connectivity was derived for both non-colluding and colluding Eves. Physical layer security in a random wireless network with source protected zone and interferer protected zone was explored in [107], and the ergodic capacity of the legitimate user and Eve was derived. It was shown that the use of a protect zone can greatly improve the secrecy performance in different scenarios. Secure transmission in a relay wiretap channel in the presence of spatial randomly distributed non-colluding Eves was discussed in [108] and [109]. Closed-form expressions for the transmis-

sion outage probability and SOP were derived, and asymptotic analysis when the number of antennas at the source grows sufficiently large was also conducted. The SOP constrained secrecy throughput was analyzed and analytical solutions were obtained.

For a large scale random ad-hoc network, the tradeoff between connectivity and secrecy was analyzed in [34] and [35]. It was shown that significant throughput was sacrificed in order to achieve a high level security. Average secrecy rate in a three-tier wireless sensor network was derived in [110], it was shown that multiple antennas at the access points can enhance the security, while there was an optimal access point density maximizing the average secrecy rate due to the increased interference brought by more access points. Recently, the study on security was also extended to mmWave ad hoc networks by incorporating mmWave channel characteristics, random blockages, and antenna patterns [111]. It has revealed that low mmWave frequency could achieve better secrecy performance in a low transmit power region, whereas higher mmWave frequency is desirable when the transmit power was increased. Moreover, it was shown that the eavesdropping capacity increased with the receiving beam width.

For the multi-cell heterogeneous network, characterizing the inter-cell or inter-tier interference is more challenging. However, it is worth noting that the interference also interferes with the Eves, which may be beneficial to the whole system from the perspective of security. In [36], Wang *et al.* evaluated the secrecy performance of cellular networks considering the cell association and information exchange among BSs, and provided tractable results for the achievable secrecy rate under different assumptions on the information of Eves' locations. Physical layer security in downlink cellular networks was investigated in [37] and the achievable secrecy rate with RCI precoding was analyzed with the aid of large-system analysis. Due to the inter-cell interference, the secrecy rate does not always increase and there exists an optimal BS density that maximizes the secrecy rate. In [112], the secrecy performance in an AN-aided multi-antenna multi-tier HetNet

was also investigated under an access threshold-based association scheme. It was shown that both the connection and secrecy outage performance can be improved by deploying more pico or femto BSs. The effect of device-to-device (D2D) communication on secrecy performance of the cellular network was explored in [113]. The feasible regions of D2D parameters were derived for both strong and weak performance guaranteed criteria. In [114], the secure connection probability was analyzed in a noise-limited mmWave cellular network for both non-colluding and colluding Eves.

1.3.4 Physical Layer Security with Active Attack

For a HD Eve, even though jamming could effectively interfere with the legitimate transmission, the Eve cannot overhear anything and may be exposed to Alice. On the other hand, passive eavesdropping will hide Eve's position, but sometimes the eavesdropping capacity will be very low if Eve is far away from Alice. From the perspective of Eves, whether to eavesdrop or jam is formulated by a game theoretical approach in [38, 39, 115]. In [38], the interactions between Alice and an active Eve was modeled as a zero-sum game using ESR as the payoff function and the existence of Nash equilibrium (NE) was examined. To improve the secrecy and reliability, Garnaev *et al.* [39] introduced a time slot in the transmission protocol to detect the malicious threat, and two stochastic games were proposed. In [116], the transmission rate and beamformer were discussed in MISO channels against opportunistic eavesdropping or jamming attack. For Eves with FD capability, jamming and eavesdropping attacks can be launched simultaneously, which may greatly degrade the achievable secrecy rate as long as the self-interference can be well suppressed. In [40], a hierarchical game framework was formulated to analyze the power allocation of the transmitter and the Eve. In [117], achievable secrecy degrees of freedom was characterized considering FD receiver and an FD active Eve. It was revealed that positive secrecy degrees of freedom could be achieved only if the number of antennas of the FD receiver is larger than that of the Eves.

To improve the eavesdropping capacity at Eve's side, smart active Eves may also jam the channel training phase by sending the same pilot sequence, resulting in an imperfect channel estimation about the legitimate channel and enhanced signal reception at the Eve [42, 43]. The impact of pilot contamination attack on the secrecy performance was evaluated in [42], it was shown that the smart FD Eve can achieve desired eavesdropping and also degrade the legitimate users simultaneously. In [43], by incorporating pilot contamination and pilot attack from multi-antenna active Eves in a time-division duplex (TDD) multi-cell multi-user massive MIMO system, the asymptotic achievable secrecy rate was derived with matched filter precoding and AN with the aid of large system analysis. It was proved that the impact of the active Eve can be completely eliminated when the transmit correlation matrices of the users and the Eve are orthogonal, and robust design against the pilot contamination attack was also developed.

1.4 Thesis Contributions and Organization

The main contributions of this thesis are summarized as follows:

- In Chapter 3, a successive relaying scheme is proposed to improve the secrecy performance of an AF relaying network with multiple untrusted relay nodes. The main motivation is to investigate the maximum achievable secrecy diversity order considering relay eavesdropping, by assuming perfect inter-relay interference (IRI) cancellation at the destination. In the successive relaying scheme, the multi-antenna source node transmits to two selected nodes alternately with zero-forcing beamforming (ZFBF), and the IRI is used to jam the untrusted nodes without external helpers. Several relay selection schemes are proposed, and the closed-form expressions of the lower bound of SOP are derived accordingly. Asymptotic analysis is also conducted to obtain some insights. It is shown that the proposed scheme can achieve a maximum secrecy diversity order of $N - 1$, for a N nodes network, which

greatly outperforms the conventional relaying scheme. Moreover, the spectral efficiency is improved dramatically with the successive relaying scheme.

- In Chapter 4, the secure transmission strategy for a MISOME system with coexistence of Bob and an NU is investigated. The NU and Bob require normal and secure data transmissions, respectively, and thus the stream for the NU can be exploited to confuse the Eves. To guarantee the security of Bob, AN is also deliberately injected into the null space of Bob and NU. The power allocation among Bob, NU and AN, as well as the wiretap code rates, are jointly optimized to maximize the effective secrecy throughput (EST), under the average throughput constraint of NU. Both non-adaptive and adaptive transmission schemes are proposed, based on the statistical and instantaneous CSI of the legitimate channels, respectively. An alternative optimization algorithm is proposed to obtain the optimal parameters. It is proven that the EST is a quasi-concave function of the secrecy rate and the power allocated to Bob, and for fixed wiretap code rates, the optimal power allocation is derived in a closed-form expression. Numerical results show that the EST increases with the increase in transmitting power and the number of transmit antennas, and decreases with the throughput constraint of the NU. Improved EST can be achieved through injecting AN and concurrent transmission of Bob and NU.
- In Chapter 5, AN-aided physical layer security in a multi-antenna small-cell network is investigated, considering the spatial randomness of the nodes. By leveraging the stochastic geometry tools, we derive the closed-form expressions of the connection and secrecy outage probabilities, and then comprehensively analyze the impact of different parameters through asymptotic analysis. It shows that deploying more BSs will improve the connection and secrecy outage performance. For a fixed-rate transmission, the condition under which AN becomes unnecessary is derived. We also derive a lower bound of the average achievable secrecy rate, which is shown to be a quasi-concave

function of the power allocation factor and a monotonic decreasing function of the ratio of the Eve-BS density. In the high cell-load case with ZFBF multi-user transmission, the achievable average secrecy rate is also derived. It is shown that the optimal number of users maximizing the secrecy area spectral is a fixed portion of the number of transmit antennas. Finally, we investigate the impact of adaptive Eves with eavesdropping and jamming capability on the secrecy performance by assuming that those Eves who are far away from the BSs act as smart jammers to degrade the reception of cellular users. The feasible region that enables adaptive eavesdropping is derived and the optimal strategies for the BS and each Eve are analyzed under the framework of the Stackelberg game.

- In Chapter 6, we study the security performance in a sub-6 GHz and mmWave hybrid heterogeneous network. By considering pilot spoofing attacks from the Eves, we analyze the coverage and secrecy probabilities using stochastic geometry. Specifically, we show that, for the sub-6 GHz tier, increasing the number of BS antennas is more effective than increasing BS density in improving the coverage performance, whereas densifying BS is more effective for security enhancement. In the presence of pilot contamination and pilot spoofing attack, densifying the BS will not always improve the coverage performance for the sub-6 GHz massive MIMO tier. For the mmWave tier, we first derive the success probability of beam alignment based on a beam sweeping based channel training model. Following that, the conditions under which the millimeter wave tier outperforms the sub-6 GHz counterpart are discussed in terms of both coverage and secrecy. Our results reveal that an mmWave tier can provide better coverage and secrecy performance in high code-rate and low redundant rate regions.

The thesis is organized as follows. Chapter 2 reviews the fundamental concepts in physical layer security design and analysis, including the principles of physical layer security, stochastic geometry, game theory, and mmWave communications.

Chapter 3 discusses the exploitation of interference in successive relaying network to increase the secrecy performance in untrusted relaying system, with an emphasis on relay pair selection and secrecy diversity order analysis. Chapter 4 focuses on secrecy throughput maximization transmission strategy in MISOME channels and discuss the optimal power allocation and code rate design. Chapter 5 investigates physical layer security in a multi-antenna small-cell network, and analyze the impact of different parameters on the secrecy performance. As an extension, Chapter 6 evaluates the coverage and security performance in a heterogeneous network consisting of both sub-6 GHz macro cells and mmWave small cells, taking the pilot attack and pilot contamination into account. Chapter 7 concludes this thesis and elaborates several interesting and promising directions of the future works. Finally, the Appendices present the detailed proofs from previous chapters.

Chapter 2

Fundamental Concepts

2.1 Fundamentals of Physical Layer Security

2.1.1 Shannon's Perfect Secrecy

The information theoretical security was first introduced in Shannon's seminal work in 1949 [118]. As shown in Fig. 2.1, the source message W is first encrypted to a ciphertext X using a key K and then transmitted through the channel to the legitimate receiver (Bob), while Eve gets access to X and attempts to recover the original message W . The system is said to have *perfect secrecy*, if for the Eve, the *a posteriori* probability of W given X is equal to the *a priori* probabilities of W for all X , i.e.,

$$H(W | X) = H(W), \text{ or, } I(W; X) = 0. \quad (2.1)$$

Figure 2.1: Shannon's model of a secrecy system.

Figure 2.2: The wiretap channel model.

$H(W | X)$ is called *equivocation* in [118], which measures Eve's uncertainty about W when it observes X . Equation (2.1) implies that the perfect secrecy is achieved when the ciphertext X is statistically independent with the message W , i.e., Eve cannot extract any new information about W based on the observation of X . This security is in the sense of information theory, and is the strongest notion of security we can achieve. However, to achieve perfect secrecy, the key size should be at least as large as the message size, i.e., $H(W) \leq H(K)$, which makes it very difficult to implement in practice.

2.1.2 Wyner Wiretap Channel

The wiretap channel model was proposed in [119]. As shown in Fig. 2.2, Alice encodes a message W to a codeword X^n and transmits it through a noisy discrete memoryless channel (DMC) (main channel) to Bob, where the message is uniformly distributed over the message set $\{1, 2, \dots, 2^{nR}\}$, with R and n denoting the communication rate and the block length. The observation of Bob is denoted as Y^n , which is subsequently passed through a wiretap channel and received by Eve as Z^n . The perfect secrecy condition was denoted by

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(W; Z^n) = 0. \quad (2.2)$$

Note that it only requires the block-length-normalized mutual information at Eve vanishes when the block length goes to infinity, thus (2.2) is termed as weak

Figure 2.3: The general DMC broadcast wiretap channel model.

secrecy condition. It can also be extended to a strong secrecy condition as

$$\lim_{n \rightarrow \infty} I(W; Z^n) = 0. \quad (2.3)$$

Note that both the weak and strong secrecy in (2.2) and (2.3) are relaxed by the infinite block length compared to Shannon's perfect secrecy.

2.1.3 Single-Antenna Wiretap Channel

Secrecy capacity is the most common performance metrics in physical layer security to characterize the secrecy transmission efficiency, which is defined as the supremum of the communication rates at which reliability and security can be achieved simultaneously. For a general DMC broadcast wiretap channel, as shown in Fig. 2.3, the secrecy capacity was mathematically expressed as [120]

$$C_s = \max_{P_{UX}P_{YZ|X}} (I(U; Y) - I(U; Z)), \quad (2.4)$$

where U is an auxiliary variable satisfying the Markov chain $U \rightarrow X \rightarrow (Y, Z)$. Equation (2.4) implies that the secrecy capacity can be characterized by the largest capacity difference between the main channel and wiretap channel. However, due to the existence of U , it is difficult to optimize this general secrecy capacity. In Wyner's original work, the wiretap channel is a degraded version of the main channel, X and Z are conditionally independent given Y , i.e., $P_{YZ|X} = P_{Y|X}P_{Z|Y}$, and X, Y, Z satisfy the Markov chain $X \rightarrow Y \rightarrow Z$. Then the secrecy capacity

is simplified as

$$C_s = \max_{p(X)} (I(X; Y) - I(X; Z)). \quad (2.5)$$

Hence, secrecy capacity is usually obtained by solving a non-convex optimization problem over all possible distributions $p(X)$.

To get some closed-form expressions of secrecy capacity, AWGN wiretap channel was further investigated and thus (2.5) can be simplified as [78]

$$C_s = [C_b - C_e]^+, \quad (2.6)$$

where C_b and C_e are the main channel capacity and eavesdropping capacity, respectively.

The above secrecy capacity is only defined for fixed channels. To measure the average secrecy capacity in fading channels, ESC is the main performance metrics. For a single-input single-output (SISO) channel wiretapped by a single antenna Eve in the presence of AWGN noise, the received signals at Bob and Eve are given by

$$\begin{aligned} y_b &= h_b x + n_b, \\ y_e &= h_e x + n_e, \end{aligned} \quad (2.7)$$

where h_b and h_e denote the independent identically distributed (i.i.d.) channel fading coefficients, n_b and n_e are AWGN components with zero-mean and variances σ_b^2 and σ_e^2 , respectively. In addition, the transmit signal satisfies the power constraint, i.e., $\mathbb{E}[x^2] \leq P$. Then the secrecy capacity can be expressed as

$$C_s = \max_{\mathbb{E}[P_t] \leq P} \mathbb{E} \left[\log_2 \left(1 + \frac{P_t |h_b|^2}{\sigma_b^2} \right) - \log_2 \left(1 + \frac{P_t |h_e|^2}{\sigma_e^2} \right) \right]^+. \quad (2.8)$$

Note that when the instantaneous CSI of both channels is available at the transmitter side, the transmit power is optimized over the h_b and h_e , while when only the instantaneous CSI of the main channel and statistical CSI of the wiretap

channel is available, the optimization is based on h_b only.

For the quasi-static fading channels, encoding over multiple channel blocks may not be suitable for delay-critical applications. Moreover, due to the fading effect, secrecy cannot be always guaranteed. In this case, the SOP becomes a more suitable performance metric. The secrecy outage probability characterizes the event when the instantaneous secrecy capacity C_s cannot support a target secrecy rate R_s , i.e., $p_{so} = \mathbb{P}(C_s < R_s)$. In practice, with the instantaneous CSI of the main channel, Alice may adaptively change its transmission rate to satisfy the SOP requirement. In this case, secrecy throughput can be used to characterize the achievable secrecy rate over all channel realizations subject to a fixed SOP.

Note that to evaluate the secrecy more efficiently, sometimes we simply use the Gaussian signal and evaluate the achievable secrecy rate, which is defined as

$$R_s = [R_b - R_e]^+, \quad (2.9)$$

where R_b and R_e are the achievable rates of the main and wiretap channels with Gaussian codebook, respectively.

2.1.4 MIMO Wiretap Channel

Consider a Gaussian MIMO wiretap channel as shown in Fig. 2.4, where the transmitter, legitimate receiver, and eavesdropper are equipped with N_t , N_r , and N_e antennas, respectively. Then the received signals at the legitimate receiver and the eavesdropper are given by

$$\mathbf{y}_b = \mathbf{H}_b \mathbf{x} + \mathbf{n}_b \quad (2.10)$$

and

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x} + \mathbf{n}_e, \quad (2.11)$$

Figure 2.4: The Gaussian MIMO wiretap channel.

respectively, where $\mathbf{H}_b \in \mathbb{C}^{N_r \times N_t}$, $\mathbf{H}_e \in \mathbb{C}^{N_r \times N_e}$ are the MIMO channels with each entry being a complex Gaussian component. $\mathbf{n}_b$ and $\mathbf{n}_e$ are the AWGN vector with zero mean and unit variance. $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$ is the transmit signal vector with covariance $\mathbb{E}[\mathbf{x}\mathbf{x}^H] = \mathbf{Q}$ with average power constraint $\text{tr}(\mathbf{Q}) \leq P$.

When full CSI of Bob and Eve is available at the transmitter side, the secrecy capacity is given by [81]

$$C_s = \max_{\mathbf{Q} \succeq \mathbf{0}, \text{tr}(\mathbf{Q}) \leq P} \log \det(\mathbf{I} + \mathbf{H}_b \mathbf{Q} \mathbf{H}_b^H) - \log \det(\mathbf{I} + \mathbf{H}_e \mathbf{Q} \mathbf{H}_e^H), \quad (2.12)$$

where $\det(\cdot)$ denotes the determinant operation. In [81, 121], it was shown that an asymptotically optimal (high SNR) scheme is to apply a transmit precoder based upon the generalized singular value decomposition (GSVD) of the pencil $(\mathbf{H}_b, \mathbf{H}_e)$, which decomposes the system into parallel channels. For a simplified case that Bob is only equipped with one antenna, i.e., $N_r = 1$, the optimal transmit beamformer is obtained as the generalized eigenvector corresponding to the largest generalized eigenvalue of $(\mathbf{h}_b, \mathbf{H}_e)$. Moreover, it was proved that the ergodic secrecy rate strictly increases with the SNR [25].

However, the CSI of Eve may not be available in practice due to the passive property of Eve, when only the statistical channel information of Eve is available

at the transmitter, i.e., $\mathbf{H}_e \sim (\mathbf{0}, \mathbf{\Sigma}_e)$, then the ergodic secrecy rate is

$$C_s = \max_{\mathbf{Q} \succeq \mathbf{0}, \text{tr}(\mathbf{Q}) \leq P} \mathbb{E}_{\mathbf{H}_e} [\log \det(\mathbf{I} + \mathbf{H}_b \mathbf{Q} \mathbf{H}_b^H) - \log \det(\mathbf{I} + \mathbf{H}_e \mathbf{Q} \mathbf{H}_e^H)]. \quad (2.13)$$

In this case, AN may be injected into the nullspace of the legitimate channel to degrade the reception of the Eve [88]. Note that when perfect CSI of the legitimate channel is not available due to the imperfect feedback in FDD systems or imperfect channel estimation in TDD systems, more information will be leaked to Eves, resulting in severe secrecy degradation [122, 123], and thus robust solutions are required [83, 84].

2.1.5 Untrusted Relay Channel

The relay channel with colocated Eve was first considered in [124], where the source node wishes to use the relay channel to send confidential information to the destination without information leakage to the relay node. In [20], the achievable region of rate pairs (R_1, R_e) was derived for the general untrusted relay channel. For a Gaussian relay channel case with compress-and-forward protocol and orthogonal relay-to-destination channel as shown in Fig. 2.5,

$$\begin{cases} Y_D = X + Z_D, Y_r = aX + Z_r, \\ Y_R = bX_r + Z_R. \end{cases} \quad (2.14)$$

where Z_D , Z_r , and Z_R are independent real Gaussian random variables with zero mean and unit variance. a and b are the channel gains. Then by assuming that $X \sim \mathcal{CN}(0, p)$, $X_r \sim \mathcal{CN}(0, P_r)$, the achievable rate region is given by [20]

$$\bigcup_{0 \leq p \leq P} \left\{ \begin{array}{l} 0 \leq R_e \leq R_1 < C(p + \frac{a^2 p}{1 + \sigma^2}) \\ R_e \leq C(p + \frac{a^2 p}{1 + \sigma^2}) - C(a^2 p) \end{array} \right\}, \quad (2.15)$$

where

$$\sigma^2 = \frac{(a^2 + 1)p + 1}{b^2 P_r (p + 1)}. \quad (2.16)$$

Figure 2.5: The untrusted relay channel model.

It then can be concluded that positive secrecy rate can be achieved if the relay-to-destination channel gain, b , is large enough. Note that the relay node may also employ AF protocol, for a standard AF relaying protocol with channel fading, the secrecy rate is given by [23]

$$C_s = \left[\frac{1}{2} \log \left(1 + \frac{\gamma_{sr} \gamma_{rd}}{1 + \gamma_{sr} + \gamma_{rd}} \right) - \frac{1}{2} \log(1 + \gamma_{sr}) \right]^+, \quad (2.17)$$

where γ_{sr} and γ_{rd} denote the effective SNR of the source-to-relay and relay-to-destination channel, respectively. From (2.17), we can observe that the secrecy capacity is always zero. However, it was proved in [19] that positive secrecy rate can be achieved through destination-aided jamming or cooperative jamming from external nodes. The ergodic secrecy capacity was analyzed in [23, 74] through large system analysis.

For a relaying network with multiple untrusted relay nodes, the achievable secrecy capacity with destination-aided jamming and distributed beamforming (DBF) or opportunistic relaying (OR) was given by [24]

$$C_s^{DBF} = \left[\frac{1}{2} \log \left(1 + \sum_{k=1}^K \frac{\rho_s \rho_r \gamma_{sk} \gamma_{kd}}{1 + \rho_s \gamma_{sk} + (\rho_d + \rho_r) \gamma_{kd}} \right) - \frac{1}{2} \log \left(1 + \max_k \frac{\rho_s \gamma_{sk}}{1 + \rho_d \gamma_{kd}} \right) \right]^+ \quad (2.18)$$

and

$$C_s^{OR} = \left[\frac{1}{2} \log \left(1 + \max_k \frac{\rho_s \rho_r \gamma_{sk} \gamma_{kd}}{1 + \rho_s \gamma_{sk} + (\rho_d + \rho_r) \gamma_{kd}} \right) - \frac{1}{2} \log \left(1 + \max_k \frac{\rho_s \gamma_{sk}}{1 + \rho_d \gamma_{kd}} \right) \right]^+, \quad (2.19)$$

respectively, where ρ_s , ρ_r , and ρ_d denote the normalized transmit power of the source, relay, and destination node, respectively. In addition, $\gamma_{sk} = |h_{sk}|^2$, $\gamma_{kd} = |h_{kd}|^2$. Through asymptotic analysis at high SNR regions, it was shown that

$$\begin{cases} C_s^{DBF} \sim \frac{1}{2} \log K, \\ C_s^{OR} \sim \frac{1}{2} \log \frac{3}{2}, \end{cases} \quad (2.20)$$

which reveals that the DBF can achieve the same scaling law as of the trusted relay nodes case. Moreover, for the secrecy diversity order, it was derived as follows

$$\begin{cases} \mathcal{P}_{out}^{DBF} \sim G_0^{-K+1} \frac{1}{\rho} + \mathcal{O}(\frac{1}{\rho^2}), \\ \mathcal{P}_{out}^{OR} \sim G_1 \frac{K^2}{K-1} \frac{1}{\rho} + \mathcal{O}(\frac{1}{\rho^2}), \end{cases} \quad (2.21)$$

where G_0 and G_1 stand for the constant. Therefore, both the DBF scheme and the OR scheme can only achieve a secrecy diversity order of one.

2.2 Stochastic Geometry

Stochastic geometry is a powerful tool to characterize the spatial randomness in future wireless networks, including location, fading, shadowing, and power control. Due to the tractability of PPP models, stochastic geometry analysis with PPP models can also produce closed-form analytical results, providing very useful insights for network design which are usually very difficult to obtain from computation intensive simulations.

Point process (PP) is the basic spatial model to model the spatial randomness of BSs and users in a large-scale network, which is defined as a measurement mapping Φ from some probability spaces to the space of point measures on area A . As shown in Fig. 2.6, suppose that the BSs are extracted from a two-dimension PP $\Phi = \{x_i, i \in \mathbb{N}\}$, where x_i represents the location of the i th BS, and the position of users follow an independent PP. With the nearest BS association rule,

Figure 2.6: A random network model, where the solid circles and squares denote the BSs and users, respectively.

the received signal at a certain user can be expressed as

$$y_0 = \sqrt{P}h_0s_0 + \underbrace{\sum_{i \in \Phi \setminus \{0\}} \sqrt{P}h_i s_i}_I + n_0, \quad (2.22)$$

where h_i denotes the channel fading coefficients, consisting of both small-scale fading and the distance dependent path loss. Note that due to the random number and locations of interferers, it is mathematically intractable to derive the probability density function (PDF) of I using conventional methods.

Thanks to the tractable results from Campbell's theorem [125, Theorem 4.1] and the probability generating functional (PGFL) [125, Definition 4.3] using stochastic geometry, the interference property can be statistically characterized using the characteristic or moment functions.

Theorem 2.1 (Campbell's Theorem). *Let Φ be a PP in $\mathbb{R}^d$ and $f : \mathbb{R}^d \rightarrow \mathbb{R}$ be a measurable function, then*

$$\mathbb{E} \left[\sum_{x_i \in \Phi} f(x_i) \right] = \int_{\mathbb{R}^d} f(x) \Lambda(dx), \quad (2.23)$$

where $\Lambda(dx)$ is the intensity measure of Φ . In case of PPs in $\mathbb{R}^2$, it reduces to

$$\mathbb{E} \left[\sum_{x_i \in \Phi} f(x_i) \right] = \int_{\mathbb{R}^2} f(x) \lambda(x) dx, \quad (2.24)$$

Definition 2.1. Let $\mathcal{F}$ be a family of all measurable functions $f : \mathbb{R}^d \mapsto [0, 1]$ such that $1 - f$ has bounded support. For $f \in \mathcal{F}$, the PGFL of the PP Φ is defined as

$$G(v) \triangleq \mathbb{E} \left[\prod_{x_i \in \Phi} f(x_i) \right] = \int_{\mathcal{N}} \prod_{x \in \varphi} f(x) P(d\varphi). \quad (2.25)$$

While the Campbell's theorem takes an expectation over a random sum, and can be used to calculate the mean and variance of the aggregate interference power, the PGFL takes an expectation over a random product and may be used to evaluate the characteristic function. To obtain some tractable results about the PGFL, a special kind of PP has been widely used in wireless networks, which is defined as follows.

Definition 2.2 (Poisson point process (PPP)). A PP $\Phi = \{x_i\} \subset \mathbb{R}^d$ is a PPP if and only if the number of points inside any compact set $\mathcal{B} \subset \mathbb{R}^d$ is a Poisson random variable, and the number of points in disjoint sets are independent. In particular, if the intensity measure satisfies $\Lambda(A) = \lambda |A|$, then Φ is a homogenous PPP with intensity λ .

Following this definition, additional operations on a PPP such as superposition, thinning and displacement result in invariant laws, which greatly facilitate the theoretical analysis in practice. Particularly, by relating the PGFL with the Laplace transform of interference, the average performance of random networks, like the coverage probability and outage probability can be evaluated more efficiently.

Lemma 2.1. For a PPP $\Phi \subset \mathbb{R}^d$ with intensity measure Λ , then the PGFL becomes

$$\mathbb{E} \left[\prod_{x_i \in \Phi} f(x_i) \right] = \exp \left(- \int_{\mathbb{R}^d} (1 - f(x)) \Lambda(dx) \right). \quad (2.26)$$

2.3 Game Theory

Game theory is another important tool in security areas to study the interaction and competitive decision-making process between legitimate transmitters and smart Eves or attackers. Since the legitimate transmitter and the Eves or attackers usually have conflict interests and they are unlikely to coordinate the actions before the game in practice, the interactive process is usually considered within the framework of non-cooperative game, which models the competitive situation where each player takes its decision independently of the other players. In this section, we briefly summarize some most important concepts in non-cooperative game to facilitate the description in Chapter 5, more detailed descriptions and proofs can be found in [126].

Definition 2.3. *A strategic non-cooperative game is a triplet $G = (\mathcal{N}, \mathcal{S}_i, u_i), i \in \mathcal{N}$, where*

- $\mathcal{N}$ is a finite set of players, i.e., $\mathcal{N} = \{1, 2, \dots, N\}$;
- $\mathcal{S}_i$ is a set of strategies for player i ;
- $u_i : \mathcal{S} \rightarrow \mathbb{R}$ is the utility function of player i , $\mathcal{S}$ is the Cartesian product of all the strategy set.

Following this, denote $\mathbf{s}_{-i} = [s_j]_{j \in \mathcal{N}, j \neq i}$ as the strategies of all players except i , and $\mathbf{s} = (s_i, \mathbf{s}_{-i})$ as a strategy profile. When the set of each player's strategy $\mathcal{S}_i$ is finite, the game is called a finite game. In addition, if all the elements (the number of players, the strategy space, and payoff function, etc.) are common knowledge to all players, it is also referred as a game with complete information, otherwise the game is said to be an incomplete information game.

The solution of a non-cooperative game is usually characterized by NE, which defines a strategy profile that none of the players can unilaterally change its strategy to increase its payoff or utility, if the other players maintain their current strategies. For a pure strategy non-cooperative game, NE can be mathematically

expressed as

$$u_i(s_i^*, \mathbf{s}_{-i}^*) \geq u_i(s_i, \mathbf{s}_{-i}^*), \forall s_i \in \mathcal{S}_i. \quad (2.27)$$

The NE can also be characterized by the best-response function, specifically a strategy profile $\mathbf{s}^* \in \mathcal{S}$ is a NE of a non-cooperative game if and only if every user's strategy is a best response to the other player's strategies. Then the existence and uniqueness of NE can be characterized by the following theorems.

Definition 2.4. [126, 127] A function $g : \mathcal{S} \rightarrow \mathbb{R}_+^N$ is said to be standard if it satisfies

- *Monotonicity:* $\forall \mathbf{s}, \mathbf{s}' \in \mathcal{S}, \mathbf{s} \leq \mathbf{s}' \Rightarrow g(\mathbf{s}) \leq g(\mathbf{s}')$;
- *Scalability:* $\forall \alpha > 0, \mathbf{s} \in \mathcal{S}, g(\alpha \mathbf{s}) \leq \alpha g(\mathbf{s})$.

Following this definition, we can obtain two important properties for a standard function: 1) if the fixed point exists, then it is unique; 2) the fixed-point iteration will eventually converge to this unique fixed point. Then the following theorem can be proved.

Theorem 2.2. *If the best-response functions of a non-cooperative game are standard functions for all players, then the game has a unique Nash equilibrium in pure strategies.*

For the cases that the best-response function cannot be expressed in closed form, the existence of the NE can be guaranteed by the following theorem.

Theorem 2.3. *A non-cooperative game in strategic form has at least one pure-strategy Nash equilibrium if the following conditions are satisfied:*

- *the strategy space $\mathcal{S}_i$ is non-empty, compact and convex subset of the Euclidean space;*
- *the utility function $u_i(s_i, \mathbf{s}_{-i}^*)$ is continuous in the strategy profile;*
- *each player's utility function $u_i(s_i, \mathbf{s}_{-i}^*)$ is quasi-concave in its own strategy s_i .*

2.4 mmWave Communication

Network densification through the massive deployment of small cells is a key technique to improve the capacity, coverage, and spectrum and energy efficiency. In addition, by enabling mmWave communications at the small cell BSs, significant capacity enhancement can be achieved by utilizing the vast available spectrum at mmWave frequencies. In particular, the high throughput mmWave links provide cost-efficient wireless backhauls for small cell BSs in areas where it is too costly to install wire or fiber connections. Due to the high carrier frequencies, the mmWave signals are more sensitive to blockage and cannot penetrate through buildings. Hence, to realize universal coverage, it is more likely that mmWave small-cell will co-exist with traditional sub-6 GHz macro-cell network [128,129], as shown in Fig. 2.7.

To characterize the blockage of mmWave signal, the ball model [130], line-of-sight (LoS) ball model [131], two-ball blockage model [132], and the exponential blockage model [129,133] have been proposed in mmWave networks. Specifically, for the ball blockage model in [130], a link with distance r is a LoS link with probability $p_L(r)$, which is given by

$$p_L(r) = \begin{cases} C, & \text{if } r \leq D \\ 0, & \text{otherwise,} \end{cases} \quad (2.28)$$

where $0 \leq C \leq 1$ and D are environment dependent constants and can be obtained through field measurement.

Due to the blockage effect, different path loss laws should be adopted for LoS or non-LoS (NLoS) links in mmWave communications, i.e.,

$$PL = \begin{cases} c_L R^{-\alpha_L}, & \text{for LoS link,} \\ c_N R^{-\alpha_N}, & \text{otherwise.} \end{cases} \quad (2.29)$$

Figure 2.7: Illustration of a heterogeneous network.

Note that c_L and c_N are path losses for LoS and NLoS links at a reference distance. To compensate the severe path loss, mmWave BSs are usually equipped with large antenna arrays and implement directional beamforming. For the ease of analysis, the antenna pattern is usually approximated by a sectored antenna model

$$G(\theta) = \begin{cases} G_A, & \text{if } |\theta| \leq \theta_A, \\ g_A, & \text{otherwise.} \end{cases} \quad (2.30)$$

where θ_A is the main lobe beamwidth, and G_A and g_A are array gains of the main lobe and side lobe, respectively. With directional beamforming, Rayleigh fading assumption is not suitable for mmWave systems anymore and in most cases it is reasonable to neglect the small-scale fading.

Since mmWave channels usually have limited scattering, geometric channel models with L paths are usually adopted [134–136]. With this model, the channel between an N_{BS} antenna BS and N_{MS} antenna user can be expressed as

$$\mathbf{H} = \sum_{l=1}^L \beta_l \mathbf{a}_{BS}(\theta_l) \mathbf{a}_{MS}(\varphi_l), \quad (2.31)$$

where β_l is the channel gain of the l th path, $\mathbf{a}_{BS}(\cdot)$ and $\mathbf{a}_{MS}(\cdot)$ are the steering vectors at the BS and user, with $\theta^l, \varphi^l \in [0, 2\pi]$ being the angle of arrival (AoA) or angle of departure (AoD) at the BS and user. For a uniform linear array (ULA) with element spacing d , the steering vector can be expressed as

$$\mathbf{a}_{BS}(\theta_l) = \left[1, e^{-j\frac{2\pi}{\lambda}d\sin(\theta_l)}, \dots, e^{-j\frac{2\pi}{\lambda}(N_{BS}-1)d\sin(\theta_l)} \right]^T. \quad (2.32)$$

Chapter 3

Secure Successive AF Relaying Network with Untrusted Nodes

3.1 Introduction

In this chapter, the secrecy performance of an AF relaying network with multiple untrusted relay nodes is investigated. The untrusted nodes can help to forward the received signal and they may also try to decode such information, which can be regarded as potential Eves. To improve the achievable secrecy diversity order, we propose a successive relaying scheme, where the multi-antenna source transmits to two selected relay nodes alternately and each node forwards the received information to the destination subsequently. Through proper scheduling, the conventional detrimental IRI can be used to jam the untrusted nodes without external helpers. Considering different complexity requirements, several relay selection schemes are proposed, and the closed-form expressions of the lower bound of SOP are derived accordingly. Asymptotic analysis is also conducted to derive the achievable diversity order. It is shown that a maximum secrecy diversity order of $N - 1$ can be achieved for a N relay nodes system with the proposed relay selection scheme. Moreover, the spectral efficiency is improved dramatically with the successive relaying scheme.

Figure 3.1: Successive relaying model, where only nodes i and j are activated: (a) transmission in the odd time slot, (b) transmission in the even time slot.

3.2 System Model and Problem Statement

We consider an AF HD relaying network, where a source (S) communicates with a destination (D) with the assistance of N relay nodes, as shown in Fig. 3.1. The relay nodes act both as cooperative helpers and potential Eves, but they are non-colluding and do not make any malicious attack. Each node except S is equipped with one antenna each, and S is equipped with N_T antennas. It is understood that there is no direct link between S and D due to the long distance between them. All the channels are assumed to be quasi-static block-fading channels, where channel fading coefficients remain unchanged during a fading block of L time slots, but change randomly from one block to another. The value of L is assumed to vary randomly. We also assume that perfect CSI of all channels is available, as assumed in [137], and relay selection is done before each transmission based on different selection criteria described in the next section. Channel reciprocity is also assumed.

In certain fading block, we assume that only the i th relay (R_i) and the j th relay (R_j) are activated, and all the remaining relay nodes keep silent. Without loss of generality, we assume that in the even time slot, S sends signal $\mathbf{x}(t)$ to R_j and R_i forwards the previously received signal $y_{R_i}(t-1)$ to D, where $\mathbf{x}(t) = \mathbf{w}(t)s(t)$, $\mathbf{w}(t)$ and $s(t)$ are the beamforming vector and data symbol in the t th time slot, respectively, and $\mathbb{E}[|s(t)|^2] = 1$. Thus, the IRI from R_i can confuse the decoding

of R_j , as long as R_j does not know $y_{R_i}(t-1)$. In practice, this can be realized by ZFBF at the source, i.e., [138]

$$\mathbf{w}(t) = \frac{\left(\mathbf{I} - \bar{\mathbf{H}}_k (\bar{\mathbf{H}}_k^H \bar{\mathbf{H}}_k)^\dagger \bar{\mathbf{H}}_k^H\right) \mathbf{h}_k^*}{\left\| \left(\mathbf{I} - \bar{\mathbf{H}}_k (\bar{\mathbf{H}}_k^H \bar{\mathbf{H}}_k)^\dagger \bar{\mathbf{H}}_k^H\right) \mathbf{h}_k^* \right\|}, \quad (3.1)$$

where $k = j$ when t is even and $k = i$ otherwise. Note that $\mathbf{h}_i = [h_1, \dots, h_N]^T$ and $h_i \sim \mathcal{CN}(0, \delta_h^2)$ denotes the fading channel from the S to R_i , and $\bar{\mathbf{H}}_k$ is the channel matrix from S to all the relay nodes except the k th one. For the feasibility of ZFBF, the number of antennas at S, N_T , must be no less than the number of untrusted relay nodes, N . Similarly, in the odd time slot, where t is odd, S sends signal $\mathbf{x}(t)$ to R_i and R_j forwards the previously received signal $y_{R_j}(t-1)$ to D, causing interference to the decoding of R_i . In this case, the detrimental IRI becomes a beneficial factor to the secrecy of the system. The received signals at R_i and R_j in the t th time slot ($t \geq 2$) can be written respectively as

$$y_{R_i}(t) = \sqrt{P_s} \mathbf{h}_i^T \mathbf{x}(t) + \sqrt{P_r} \alpha_{ji} x_{R_j}(t) + n_{R_i}(t), \quad t \text{ odd}, \quad (3.2)$$

and

$$y_{R_j}(t) = \sqrt{P_s} \mathbf{h}_j^T \mathbf{x}(t) + \sqrt{P_r} \alpha_{ij} x_{R_i}(t) + n_{R_j}(t), \quad t \text{ even}, \quad (3.3)$$

where P_s and P_r are the transmit power levels of S and the relay, respectively. Note that $g_i \sim \mathcal{CN}(0, \delta_g^2)$ denotes the fading channel from R_i to D. Similar definition applies to g_j . $\alpha_{ij} \sim \mathcal{CN}(0, \delta_a^2)$ denotes the IRI channel between the i th relay and the j th relay. $n_{R_i}(t)$ and $n_{R_j}(t)$ are the zero-mean additive Gaussian noise at relay nodes R_i and R_j with variance σ^2 . $x_{R_j}(t) = \beta_j(t) y_{R_j}(t-1)$, and $x_{R_i}(t) = \beta_i(t) y_{R_i}(t-1)$ are the transmitted signal from the relay nodes R_j and R_i , respectively, where $\beta_j(t)$ and $\beta_i(t)$ are the power scaling gains used to normalize the power of the transmitted signal at the relay nodes and are given by

$$\beta_j(t) = \sqrt{\frac{1}{P_s |\mathbf{h}_j^T \mathbf{w}_j|^2 + P_r |\alpha_{ij}|^2 + \sigma^2}}, \quad t \text{ is odd}, \quad (3.4)$$

Table 3.1: The Transmission Protocol of AF Successive Relaying, when L is even.

No. Node	1	2	3	...	$L-1$	L
S	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	...	$\mathbf{x}_{L-1}$	
R_i	Rx: $y_{R_i,1}$	Tx: $x_{R_i,1}$	Rx: $y_{R_i,3}$ $\tilde{x}_{R_j,2}$	...	Rx: $y_{R_i,L-1}$ $\tilde{x}_{R_j,L-2}$	Tx: $x_{R_i,L-1}$
R_j		Rx: $y_{R_j,2}$ $\tilde{x}_{R_i,1}$	Tx: $x_{R_j,2}$	...	Tx: $x_{R_j,L-2}$	Rx: $\tilde{x}_{R_i,L-1}$
D		Rx: $y_{D,2}$	Rx: $y_{D,3}$	...	Rx: $y_{D,L-1}$	Rx: $y_{D,L}$

and

$$\beta_i(t) = \sqrt{\frac{1}{P_s |\mathbf{h}_i^T \mathbf{w}_i|^2 + P_r |\alpha_{ji}|^2 + \sigma^2}}, \quad t \text{ is even}, \quad (3.5)$$

respectively. Following that, the received signal at the destination in even and odd time slots can be expressed as

$$\begin{aligned} y_D(t) = & \sqrt{P_s P_r} g_i \beta_i(t) \mathbf{h}_i^T \mathbf{x}(t-1) + P_r g_i \beta_i(t) \alpha_{ji} x_{R_j}(t-1) \\ & + \sqrt{P_r} g_i \beta_i(t) n_{R_i}(t-1) + n_D(t), \end{aligned} \quad (3.6)$$

and

$$\begin{aligned} y_D(t) = & \sqrt{P_s P_r} g_j \beta_j(t) \mathbf{h}_j^T \mathbf{x}(t-1) + P_r g_j \beta_j(t) \alpha_{ij} x_{R_i}(t-1) \\ & + \sqrt{P_r} g_j \beta_j(t) n_{R_j}(t-1) + n_D(t), \end{aligned} \quad (3.7)$$

respectively, where $n_D(t)$ is the zero-mean additive Gaussian noise at D with variance σ^2 . Notice that, in the first time slot, S sends non-information bearing signal, since security in this slot cannot be guaranteed without IRI. Thus, the received signal at D in the second time slot is not considered when calculating the secrecy rate. The whole transmission procedure is shown in Table 3.1. In Table 3.1, $\tilde{x}_{R_i}(t)$ denotes the received signal of $x_{R_i}(t)$ after passing through the IRI channel. Similar definition applies to $\tilde{x}_{R_j}(t)$.

It can be seen from (3.6) and (3.7) that the received signal contains IRI. Assume that the destination can store the received signal of the previous slot, and the IRI channel is available, then interference cancellation methods [137] can be applied

at each time slot. As $x_{R_i}(t) = (y_D(t) - n_D(t))/(\sqrt{P_r}g_i)$, the received signals after IRI cancellation in even and odd time slots can be rewritten as

$$\begin{aligned} \tilde{y}_D(t) = & \sqrt{P_s P_r} g_i \beta_i(t) \mathbf{h}_i^T \mathbf{w}_i s(t-1) - \sqrt{P_r} g_i \beta_i(t) \alpha_{ji} n_D(t-1)/g_j \\ & + \sqrt{P_r} g_i \beta_i(t) n_{R_i}(t-1) + n_D(t), \end{aligned} \quad (3.8)$$

and

$$\begin{aligned} \tilde{y}_D(t) = & \sqrt{P_s P_r} g_j \beta_j(t) \mathbf{h}_j^T \mathbf{w}_j s(t-1) - \sqrt{P_r} g_j \beta_j(t) \alpha_{ij} n_D(t-1)/g_i \\ & + \sqrt{P_r} g_j \beta_j(t) n_{R_j}(t-1) + n_D(t), \end{aligned} \quad (3.9)$$

respectively. Notice that even though the IRI is removed, the noise component cannot be cancelled. To facilitate the analysis, we assume that both the signal from S and the IRI are much stronger than the noise components, and the noise effect can be ignored. Therefore, the SNR at the destination can be expressed as

$$\gamma_{D,t} \approx \begin{cases} \frac{\gamma_{si}\gamma_{id}}{\gamma_{si}+\gamma_{ij}}, & 4 \leq t \leq L, t \text{ is even}, \\ \frac{\gamma_{sj}\gamma_{jd}}{\gamma_{sj}+\gamma_{ij}}, & 3 \leq t \leq L, t \text{ is odd}, \end{cases} \quad (3.10)$$

where $\gamma_{sm} = \bar{P}_s |\mathbf{h}_m^T \mathbf{w}_m|^2$, $\gamma_{md} = \bar{P}_r |g_m|^2$, $\gamma_{mn} = \bar{P}_r |\alpha_{mn}|^2$, $m, n \in \{i, j\}$ and n is the complement of m . Note that $\bar{P}_s = \frac{P_s}{\sigma^2}$ and $\bar{P}_r = \frac{P_r}{\sigma^2}$ are the normalized transmit power levels. Similarly, the SNR at the untrusted relay can be approximated by

$$\gamma_{R,t} \approx \begin{cases} \frac{\gamma_{sj}}{\gamma_{ij}}, & 2 \leq t \leq L-1, t \text{ is even}, \\ \frac{\gamma_{si}}{\gamma_{ij}}, & 3 \leq t \leq L-1, t \text{ is odd}. \end{cases} \quad (3.11)$$

With the beamforming vector in (3.1), we know that $\gamma_{sk} \sim \text{Gamma}(M, \lambda_h)$, where $M = N_T - N + 1$, $\lambda_h = 1/(\bar{P}_s \delta_h^2)$. A similar proof can be found in Appendix C of [138]. Then the instantaneous secrecy rate can be calculated by [139]

$$R_t = [\log_2(1 + \gamma_{D,t}) - \log_2(1 + \gamma_{R,t-1})]^+, 3 \leq t \leq L. \quad (3.12)$$

Since the first packet from the S does not contain any useful information, D can discard it. We thus calculate the secrecy rate starting from the third time slot. For a given target secrecy rate $\bar{R}$, SOP denotes the probability that the instantaneous secrecy rate is lower than $\bar{R}$, i.e., $P_{out,t} = \mathbb{P}(R_t < \bar{R})$. Thus, the average SOP over one block time is

$$P_{out} = \begin{cases} \frac{L-2}{2L}P_{out,odd} + \frac{L-2}{2L}P_{out,even}, & L \text{ is even,} \\ \frac{L-1}{2L}P_{out,odd} + \frac{L-3}{2L}P_{out,even}, & L \text{ is odd,} \end{cases} \quad (3.13)$$

where $P_{out,odd}$ and $P_{out,even}$ denote the SOP in odd and even time slots, respectively. When L is large enough¹, it can be approximated by

$$P_{out} \approx \frac{1}{2}P_{out,odd} + \frac{1}{2}P_{out,even}. \quad (3.14)$$

3.3 Relay Selection Rules with Untrusted Nodes

3.3.1 Optimal Successive Relay Selection

Since our target is to minimize the SOP, the optimal pair of the i th and j th nodes must be selected jointly according to the following criterion:

$$(i_{OS}, j_{OS}) = \arg \min_{i,j \in \mathcal{N}, i \neq j} P_{out}. \quad (3.15)$$

Note that the CSI of all relaying links as well as that of all inter-relay links has to be acquired. Moreover, due to the equal contribution of the two SOPs in the even and odd time slots, it is not straightforward to select the optimal relay nodes. Even though an exhaustive search method can be applied to select the optimal relay pair, it is impossible to derive the theoretical SOP expression. To facilitate the theoretical analysis and reduce the complexity, several sub-optimal selection

¹In [137], an example shows that for a scenario that given that the carrier frequency $f_c = 700$ MHz, the mobility velocity $v = 3$ km/h, and time slot duration $t_s = 1$ ms, L is found to be $L = 52$. Thus, we can conclude that this approximation holds in many practical cases.

methods are presented in the subsequent subsections.

3.3.2 Max-Min Relay Selection

Since the total SOP is determined by the worst case of either in odd or even time slots, we propose to use the max-min relay pair selection criterion which has been used in HD and FD relay systems [140], [141], by considering the two paths simultaneously, i.e.,

$$(i_{MM}, j_{MM}) = \arg \max_{i,j \in \mathcal{N}, i \neq j} \{\min\{R_{odd}, R_{even}\}\}, \quad (3.16)$$

where R_{odd} and R_{even} denote the secrecy rates in odd and even time slots, respectively.

With this selection scheme, theoretical analysis becomes possible, and theoretical SOP may be derived. However, this relay selection criterion still requires an exhaustive search, which is rather difficult to realize in practical systems especially when the number of relays is large. This motivates us to design the sub-optimal relay selection strategies with a lower complexity.

3.3.3 Max-Interference Relay Selection

In a conventional successive relay system, the IRI is detrimental to the system, whereas in our case, it is used as a source of jamming to degrade the Eve. Thus, we can simply select the relay pair with maximum IRI, i.e.,

$$(i_{MI}, j_{MI}) = \arg \max_{i,j} \{\gamma_{ij}\}. \quad (3.17)$$

3.3.4 Partial Relay Selection

As has been considered in [141], partial relay selection is an effective way to reduce the overhead by only considering the source-to-relay channel or relay-to-destination channel. For the proposed system, since the relay nodes are not trust-

worthy, we can simply select two nodes based on the channel quality from the relay to the destination, i.e.,

$$(i_{PRS}, j_{PRS}) = \left\{ (i, j) \left| |g_i|^2, |g_j|^2 \geq \max_{k \in \mathcal{N} \setminus \{i, j\}} |g_k|^2 \right. \right\}. \quad (3.18)$$

3.4 Secrecy Outage Performance and Asymptotic Analysis

In this section, closed-form expressions of the lower bound of the SOP are derived for different relay selection criteria presented in Section 3.3. The performance of the benchmark single-path relaying scheme is also presented first. To get some insights about the successive relaying scheme on the secrecy performance, asymptotic analysis is also conducted and the achievable diversity order is given.

3.4.1 Benchmark Single-Path Relay Selection Scheme

In the conventional single-path AF relaying network, where a single-antenna source communicates with a single-antenna destination with the assistance of multiple non-colluding untrusted relay nodes, the diversity order has been analyzed in [24]. Here, for comparisons, we present the SOP of the system with a multi-antenna source. To reduce the capacity of the untrusted relay, ZFBF is also adopted to nullify the information leakage to other nodes. Since the relay nodes are not trustworthy, the popular max-min criterion may not be the optimal scheme. In order to improve the jamming effect, we simply select the active node by the following criterion:

$$i_{SP} = \arg \max_{i \in \mathcal{N}} |g_i|^2. \quad (3.19)$$

Assume that $P_d = (\theta - 1)P_r$, where $\theta > 1$, then $\gamma_J = (\theta - 1)\gamma_{id}$. The end-to-end SNR and the SNR of the untrusted relays with destination aided jamming are

given by [24]

$$\gamma_{s,i,d} = \frac{\gamma_{si}\gamma_{id}}{\gamma_{si} + \gamma_{id} + \gamma_J + 1}, \quad (3.20)$$

and

$$\gamma_e = \frac{\gamma_{si}}{\gamma_J + 1}, \quad (3.21)$$

respectively. The cumulative distribution function (CDF) of γ_{id} is given by

$$F_{\gamma_{id}}(x) = (1 - e^{-\lambda_g x})^N, \quad (3.22)$$

where $\lambda_g = 1/(\bar{P}_r \delta_g^2)$. Then we have

$$\begin{aligned} P_{out}^{SP} &= \mathbb{P} \left(\frac{1 + \gamma_{s,i,d}}{1 + \gamma_e} < \bar{\gamma} \right) \\ &\approx \mathbb{P} \left(\frac{(\theta - 1)\gamma_{si}\gamma_{id}^2}{(\gamma_{si} + \theta\gamma_{id})(\gamma_{si} + (\theta - 1)\gamma_{id})} < \bar{\gamma} \right) \end{aligned} \quad (3.23)$$

where $\bar{\gamma} = 2^{\bar{R}}$. After some mathematical manipulations, we can obtain the following theorem.

Theorem 3.1. *The SOP of the conventional single-path AF relaying with destination aided jamming is lower bounded by*

$$\begin{aligned} \mathcal{P}_{LB}^{SP} &= 1 + e^{-\lambda_h \theta x} \sum_{m=M}^{\infty} \frac{(\lambda_h \theta x)^m}{m!} \left[1 - (1 - e^{-\lambda_g \theta x})^N \right] \\ &\quad - \sum_{m=M}^{\infty} \widetilde{\sum}_1 \lambda_g \frac{(\lambda_h \mu)^m}{m!} \left[(2p)^{-(\frac{\tilde{m}}{2})} \Gamma(\tilde{m}) e^{\frac{q^2}{8p}} D_{-\tilde{m}} \left(\frac{q}{\sqrt{2p}} \right) \right. \\ &\quad \left. - e^{\frac{q^2}{4p}} \sum_{j=0}^{2m} \binom{2m}{j} (-\zeta)^j \left(\frac{\gamma(n, p\epsilon'^2)}{2p^n} - \frac{\gamma(n, p\zeta^2)}{2p^n} \right) \right], \end{aligned} \quad (3.24)$$

where $\mu = \frac{\theta-1}{\bar{\gamma}}$, $p = \frac{(\theta-1)\lambda_h}{\bar{\gamma}}$, $q = \lambda_g + i\lambda_g - \theta\lambda_h$, $\tilde{m} = 2m + 1$, $n = \frac{2m-j+1}{2}$, $\zeta = \frac{q}{2p}$, $\epsilon' = \frac{\theta\bar{\gamma}}{\theta-1} + \zeta$.

$$\widetilde{\sum}_1 = \sum_{i=0}^{N-1} \binom{N-1}{i} (-1)^i N. \quad (3.25)$$

Proof. Please refer to Appendix A.1. ■

Note that the multiple summations and the complex forms of the Parabolic cylinder function make it difficult to obtain the exact diversity order; therefore, we only show the numerical results in the next section.

3.4.2 Max-Min Relay Selection

From (3.16), we observe that for the max-min selection scheme, the SOP is determined by the worst case of either the odd or even time slots. If the node pair (i, j) is selected, from (3.10) and (3.11), we have

$$\gamma_{even} \approx \frac{\gamma_{id}\gamma_{si}\gamma_{ij}}{(\gamma_{si} + \gamma_{ij})^2} \stackrel{(a)}{<} \gamma_{id} \min \left\{ \frac{\gamma_{si}}{\gamma_{ij}}, \frac{\gamma_{ij}}{\gamma_{si}} \right\} \triangleq \gamma_{even,UB}, \quad (3.26)$$

where (a) holds due to the fact that $\frac{ab}{(a+b)^2} < \min(\frac{a}{b}, \frac{b}{a})$. Similarly, for the odd time slots,

$$\gamma_{odd,UB} = \gamma_{jd} \min \left\{ \frac{\gamma_{sj}}{\gamma_{ij}}, \frac{\gamma_{ij}}{\gamma_{sj}} \right\}. \quad (3.27)$$

Define $X_{ij} = \gamma_{even,UB}$, $Y_{ij} = \gamma_{odd,UB}$, and $A_{ij} = \min(X_{ij}, Y_{ij})$, then

$$P_{out}^{MM} > \mathbb{P} \left(\max_{i,j} A_{i,j} < \bar{\gamma} \right) \triangleq \mathcal{P}_{LB}^{MM}. \quad (3.28)$$

Notice that X_{ij} and Y_{ij} are correlated with each other due to the identical IRI channel, thus it is nontrivial if not impossible to derive the CDF of their minimum value, A_{ij} . On the other hand, the joint pair selection incurs correlation among each of the selected pairs, and makes it a challenge to derive the exact expression of the SOP. Notice that the relay nodes are usually quite close to each other compared with the source-to-relay and relay-to-destination distances, thus we can assume that all the IRI channel gains are the same. In this way, the optimal relay will be independent of γ_{ij} . Let $\gamma_{ij} = \gamma_a, \forall i, j$, then X_{ij} and Y_{ij} become

independent, and the max-min selection criterion can be expressed as

$$(i_{MM}, j_{MM}) = \arg \max_{i,j \in \mathcal{N}, i \neq j} \left\{ \min \left\{ \min \left(\frac{\gamma_{si}\gamma_{id}}{\gamma_a}, \frac{\gamma_a\gamma_{id}}{\gamma_{si}} \right), \min \left(\frac{\gamma_{sj}\gamma_{jd}}{\gamma_a}, \frac{\gamma_a\gamma_{jd}}{\gamma_{sj}} \right) \right\} \right\} \quad (3.29)$$

Since X_{ij} and Y_{ij} are identically distributed, the maximum SNR using the above selected relay pair becomes the second largest value of $\min \left\{ \frac{\gamma_{sl}\gamma_{ld}}{\gamma_a}, \frac{\gamma_a\gamma_{ld}}{\gamma_{sl}} \right\}, \forall l$. Therefore, the lower bound of the SOP can be derived as follows.

Theorem 3.2. *The lower bound of the SOP with the max-min relay selection scheme is given by*

$$\mathcal{P}_{LB}^{MM} = Np_0^{N-1} - (N-1)p_0^N, \quad (3.30)$$

where

$$\begin{aligned} p_0 = & 1 - e^{-\lambda_g \bar{\gamma}} + \lambda_g \mu_1^M \phi_M(\bar{\gamma}, \mu_1, \lambda_g) + \lambda_g M \mu_2 v(\bar{\gamma}, \mu_2, \lambda_g) \\ & - \lambda_g \sum_{n=2}^M \binom{M}{n} (-\mu_2)^n \phi_n(\bar{\gamma}, \mu_2, \lambda_g), \end{aligned} \quad (3.31)$$

with $\mu_1 = \frac{\lambda_h \bar{\gamma}}{\lambda_a}$, $\mu_2 = \frac{\lambda_a \bar{\gamma}}{\lambda_h}$, $\lambda_a = \frac{1}{P_r \sigma_a^2}$, and

$$\begin{cases} v(x, \mu, \lambda) = e^{\mu\lambda} \text{Ei}(-(x + \mu)\lambda), \\ \phi_n(x, \mu, \lambda) = e^{-\lambda x} \sum_{k=1}^{n-1} \frac{(k-1)!(-\lambda)^{n-k-1}}{(n-1)!(x+\mu)^k} - \frac{(-\lambda)^{n-1}}{(n-1)!} e^{\mu\lambda} \text{Ei}(-(x + \mu)\lambda). \end{cases} \quad (3.32)$$

Proof. Please refer to Appendix A.2. ■

To get some insights, the asymptotic analysis is given. To facilitate the analysis, we assume that $\lambda_h = \lambda_g = k\lambda_a \triangleq \rho^{-1}$. The diversity order of the secure communication is given by

$$d = - \lim_{\rho \rightarrow \infty} \frac{\log P_{out}}{\log \rho}. \quad (3.33)$$

Thus the diversity order can be derived as follows.

Corollary 3.1. *The diversity order of the max-min relay selection scheme is $N-1$.*

Proof. Since $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$, and from [1, eq. (8.214.1)], for $x < 0$, we have

$$\text{Ei}(x) \approx C + \ln(-x) + \sum_{k=1}^{\infty} \frac{x^k}{k \cdot k!} = C + O(x), \quad (3.34)$$

where C is the Euler constant. Thus,

$$v(x, \beta, \lambda) \approx C + O(\lambda), \quad (3.35)$$

and

$$\phi_n(x, \beta, \lambda) \approx \frac{1}{(n-1)(x+\beta)^{n-1}} + O(\lambda). \quad (3.36)$$

After some mathematical manipulations, we can obtain

$$p_0 = G^{MM} \rho^{-1} + O(\rho^{-1}), \quad (3.37)$$

where

$$G^{MM} = \bar{\gamma} + \frac{\mu_1^M}{(M-1)(\bar{\gamma} + \mu_1)^{M-1}} + M\mu_2 C - \sum_{n=2}^M \binom{M}{n} \frac{(-\mu_2)^n}{(n-1)(\bar{\gamma} + \mu_1)^{n-1}}. \quad (3.38)$$

By substituting (3.37) into (3.30), one can readily obtain the conclusion. ■

Note that even though the diversity order analysis is based on the approximation that each IRI channel gain is identical, we can prove that it still holds for the general case. As we know, the diversity order reflects the number of independent fading paths between the source and the destination. By replacing γ_a in (3.29) with γ_{ij} , we can find that the received SNR will approach zero only if at least $N-1$ independent source-to-relay and relay-to-destination links suffer from deep fading. Therefore, the diversity order of the max-min selection scheme is $N-1$. The proof is shown as follows using the mathematical induction method.

Proof. Step 1: When $N = 2$, we can readily obtain the conclusion.

Step 2: Suppose that when $N = K$, there are at least $K - 1$ channels suffer from deep fading to make the received SNR approach zero. Without loss of generality, let $\gamma_{s1} = \gamma_{s2} = \dots = \gamma_{s,K-1} \rightarrow 0$, and $A_{ij} \rightarrow 0, \forall i, j \in \{1, 2, \dots, K\}$.

Step 3: When N is increased to $K + 1$, we have $\binom{K+1}{2} - \binom{K}{2} = K$ more pairs, i.e., $A_{\tilde{K}1}, \dots, A_{\tilde{K}K}$, where $\tilde{K} = K + 1$. To make the total SNR approach zero, $A_{\tilde{K}1}, \dots, A_{\tilde{K}K} \rightarrow 0$ must hold. From (3.26) and (3.27), we have

$$A_{\tilde{K}k} = \min \left\{ \gamma_{odd}^{\tilde{K}k}, \gamma_{even}^{\tilde{K}k} \right\}, \forall k = 1, \dots, \tilde{K}, \quad (3.39)$$

where $\gamma_{odd}^{\tilde{K}k} = \min \left\{ \frac{\gamma_{s\tilde{K}}\gamma_{\tilde{K}d}}{\gamma_{\tilde{K}k}}, \frac{\gamma_{\tilde{K}k}\gamma_{\tilde{K}d}}{\gamma_{s\tilde{K}}} \right\}$, $\gamma_{even}^{\tilde{K}k} = \min \left\{ \frac{\gamma_{sk}\gamma_{kd}}{\gamma_{\tilde{K}k}}, \frac{\gamma_{\tilde{K}k}\gamma_{kd}}{\gamma_{sk}} \right\}$. Based on the assumption of step 2, we have $A_{\tilde{K}1} = A_{\tilde{K}2} = \dots = A_{\tilde{K},K-1} \rightarrow 0$. To make $A_{\tilde{K}K} \rightarrow 0$, at least one more channel gain needs to be zero. Thus, there must be at least K channels to be zero to make the total SNR approach zero, i.e., the conclusion holds when $N = K + 1$.

This completes the proof. ■

3.4.3 Max-Interference Relay Selection

From (3.17), we know that the relay node pair selected by the max-interference relay selection criterion is only determined by the IRI channel, thus, the SOPs in both even and odd time slots are identical. Since the SOP in the even time slot is lower bounded by

$$P_{out}^{MI} > \mathbb{P} \left(\gamma_{id} \min \left\{ \frac{\gamma_{si}}{\gamma_{ij}}, \frac{\gamma_{ij}}{\gamma_{si}} \right\} < \bar{\gamma} \right) \triangleq \mathcal{P}_{LB}^{MI}, \quad (3.40)$$

then the lower bound of the SOP can be derived similar to Theorem 3.2, which is given by the following theorem.

Theorem 3.3. *The SOP with max-interference relay selection scheme is lower*

bounded by

$$\begin{aligned} \mathcal{P}_{LB}^{MI} = & 1 - \widetilde{\sum} \lambda_g \beta_1^M \phi_M(\bar{\gamma}, \beta_1, \lambda_g) + \widetilde{\sum} e^{-\lambda_g \bar{\gamma}} \\ & - \widetilde{\sum} \lambda_g \left[M \beta_2 v(\bar{\gamma}, \beta_2, \lambda_g) - \sum_{n=2}^M \binom{M}{n} (-\beta_2)^n \phi_n(\bar{\gamma}, \beta_2, \lambda_g) \right], \end{aligned} \quad (3.41)$$

where $\beta_1 = \frac{\lambda_h \bar{\gamma}}{i \lambda_a}$, $\beta_2 = \frac{i \lambda_a \bar{\gamma}}{\lambda_h}$, and

$$\widetilde{\sum} = \sum_{i=1}^N \binom{N}{i} (-1)^i. \quad (3.42)$$

Proof. Please refer to Appendix 3.3. ■

Corollary 3.2. *The diversity order of the max-interference relay selection scheme is 1.*

Proof. From the proof of Corollary 3.1, we already know that both $v(x, \beta, \lambda)$ and $\phi_n(x, \beta, \lambda)$ contain constant terms. Note that

$$\sum_{k=0}^{N-1} \binom{N-1}{k} (-1)^k = 0. \quad (3.43)$$

Thus,

$$\mathcal{P}_{LB}^{MI} = G^{MI} \rho^{-1} + O(\rho^{-1}), \quad (3.44)$$

where

$$\begin{aligned} G^{MI} = & \bar{\gamma} - \widetilde{\sum} \frac{\beta_1^M}{(M-1)(\bar{\gamma} + \beta_1)^{M-1}} \\ & - \widetilde{\sum} \left[M \beta_2 C - \sum_{n=2}^M \binom{M}{n} \frac{(-\beta_2)^n}{(n-1)(\bar{\gamma} + \beta_2)^{n-1}} \right]. \end{aligned} \quad (3.45)$$

This completes the proof. ■

3.4.4 Partial Relay Selection

Compared with the max-interference relay selection scheme, the CDF of γ_{jd} becomes [142]

$$F_{\gamma_{jd}}(x) = \sum_{i=N-1}^N \binom{N}{i} (1 - e^{-\lambda_g x})^i e^{-(N-i)\lambda_g x}. \quad (3.46)$$

Then we can obtain the following theorem.

Theorem 3.4. *The SOP with the partial relay selection scheme is lower bounded by*

$$\begin{aligned} \mathcal{P}_{\tau, LB}^{PRS} = & 1 + \widetilde{\sum}_{\tau} \lambda_g \mu_1^M \phi_M(\mu_1, \lambda_{\tau}) - \widetilde{\sum}_{\tau} \frac{\lambda_g e^{-\lambda_{\tau} \bar{\gamma}}}{\lambda_{\tau}} \\ & + \widetilde{\sum}_{\tau} \lambda_g \left[M \mu_2 v(\mu_2, \lambda_{\tau}) - \sum_{n=2}^M \binom{M}{n} (-\mu_2)^n \phi_n(\mu_2, \lambda_{\tau}) \right], \end{aligned}$$

where $\tau = 1$ for even time slots, and $\tau = 2$ otherwise. Note that $\lambda_1 = (i+1)\lambda_g$, $\lambda_2 = (i+2)\lambda_g$, and

$$\widetilde{\sum}_2 = \sum_{i=0}^{N-2} \binom{N-2}{i} (-1)^i N(N-1). \quad (3.47)$$

Proof. The proof is similar to Theorem 3.3, and is omitted for brevity. ■

With Theorem 3.4, we can derive the following corollary.

Corollary 3.3. *The diversity order of the partial relay selection scheme is 1.*

Proof. The proof is similar to that of Corollary 3.2. By using the following fact

$$\begin{aligned} \sum_{k=0}^{N-1} \binom{N-1}{k} \frac{N(-1)^k}{k+1} &= \sum_{k=0}^{N-1} \frac{(N-1)!}{k!(N-k-1)!} \frac{N(-1)^k}{k+1} \\ &= \sum_{k=0}^{N-1} \frac{N!(-1)^k}{(k+1)!(N-(k+1))!} \\ &\stackrel{(b)}{=} - \sum_{n=1}^N \binom{N}{n} (-1)^n = 1, \end{aligned} \quad (3.48)$$

where (b) is obtained by replacing $k + 1$ as n , we have

$$\mathcal{P}_{\tau, LB}^{PRS} = G_{\tau}^{PRS} \rho^{-1} + O(\rho^{-1}), \quad (3.49)$$

where

$$G_{\tau}^{PRS} = \widetilde{\sum}_{\tau} \left[\frac{\mu_1^M}{(M-1)(\bar{\gamma} + \mu_1)^{M-1}} + M\mu_2 C - \sum_{n=2}^M \binom{M}{n} \frac{(-\mu_2)^n}{(n-1)(\bar{\gamma} + \mu_2)^{n-1}} \right]. \quad (3.50)$$

This completes the proof. ■

3.5 Numerical Results and Discussions

In this section, simulation results are presented to validate the performance of the proposed schemes. We assume that all channels experience Rayleigh block fading with block length L being 50. The number of antennas of the source, N_T , is set to be 10, whereas the number of the intermediate untrusted nodes, N , is set to be either 3 or 4. The noise variances at the relay nodes and D are set to be 1, i.e., $\sigma^2 = 1$. The power level of the source is set to be the same with the relay node, i.e., $\bar{P}_s = \bar{P}_r$, and varies from 10 dB to 40 dB. We use SNR to denote the power levels. A symmetric channel is considered, i.e., $\delta_h^2 = \delta_g^2 = 1$, and the IRI channel gain is set as $\delta_a^2 = 20\delta_h^2$.

Figure 3.2 plots the SOP versus SNR for different schemes, i.e., the single-path (SP) relaying scheme, the max-min (MM) relay selection scheme, the max-interference (MI) relay selection scheme, the partial relay selection (PRS) scheme, and the optimal relay selection scheme, when $N = 3$, $N_T = 10$, $L = 50$, and target secrecy rate $\bar{R} = 2$ bps/Hz. For the SP relaying scheme, we assume $P_d = P_r$, i.e., $\theta = 1$ for a fair comparison. We observe that the MM relay selection scheme achieves the best performance, which is quite close to the optimal selection scheme obtained by an exhaustive search. Besides, all the three different successive

Figure 3.2: Secrecy outage probability vs SNR for different schemes, with $N = 3$, $L = 50$, and $\bar{R} = 2$ bps/Hz.

relaying schemes outperform the conventional SP relaying scheme even though the destination assisted jamming is used. This shows the superiority of using successive relaying scheme for security in untrusted relay systems. In addition, the PRS scheme is much better than the MI relay selection scheme under the given parameters. This is because when the IRI is large enough, the capacity of the main channel is limited by the relay-to-destination link, the better the relay-to-destination channel, the higher capacity of the main channel will be. Since the MI scheme always selects the node pair with the strongest IRI, as the IRI increases, the power left for the useful signal will be lower. We also observe that the diversity order achieved by the MM schemes is equal to 2, while other successive relaying schemes can only achieve a diversity order of 1, which validates the theoretical analysis in Section 3.4. Moreover, the exact SOP curves are given by Monte Carlo simulations and they match well with the theoretical results.

When N is increased to 4, the SOP results for different schemes are also evaluated, as shown in Fig. 3.3. Similar conclusions can be obtained. We can observe that a diversity order of larger than one can be achieved by the conventional SP relaying scheme, and it gradually approaches the MI scheme in high SNR region.

Figure 3.3: Secrecy outage probability vs SNR for different schemes, with $N = 4$, $L = 50$, and $\bar{R} = 2$ bps/Hz.

The diversity order achieved by the MM scheme is equal to 3, while other successive relaying schemes can only achieve a diversity order of 1, which coincides with the theoretical results.

In Fig. 3.4, we plot the SOP of the proposed MM scheme versus different values of N . We can observe that increasing the number of untrusted relay nodes will improve the secrecy performance, which is different from the conventional SP relaying scheme. This is because, for the conventional SP relaying scheme, increasing the number of the untrusted relays will increase the Eve's capacity since the eavesdropped information is determined by the maximum one among all the relay nodes. For the proposed system, since ZFBF is performed at the source, only the selected relay node can receive the signal from S. Thus, the capacity of the source-to-destination channel increases more than that of the eavesdropping capacity by increasing the number of untrusted relays, due to the increased diversity order. In Fig. 3.5, the SOP of the proposed MM scheme versus the target secrecy rate is shown, and similar conclusion can be obtained.

The effect of IRI on the SOP performance is evaluated in Fig. 3.6, where different transmit power levels are assumed. We observe that, in the low IRI

Figure 3.4: Secrecy outage probability vs SNR for different N , with $L = 50$, and $\bar{R} = 2$ bps/Hz.

Figure 3.5: Secrecy outage probability vs the target secrecy rate for different N , with $L = 50$ and SNR=20 dB.

Figure 3.6: Secrecy outage probability vs IRI for different transmit power levels, where $N = 4$, $L = 50$, and $\bar{R} = 2$ bps/Hz.

region, increasing the IRI will greatly decrease the SOP. If IRI level is larger than 10 (i.e., $\delta_a^2/\delta_h^2 > 10$), increasing IRI will slightly degrade the SOP. This is because when IRI is strong enough, increasing the IRI further will reduce the useful signal power. Thus, the capacity of the main channel will be decreased due to the relay power constraint.

Lastly, the ESC is simulated with different schemes and different lengths of block fading L , as shown in Fig. 3.7. We observe that the proposed successive relaying scheme outperforms the conventional SP relaying scheme due to the successive transmission. With the increase of L , the secrecy rate is almost doubled with the successive relaying scheme, which further demonstrates the superiority of the successive relaying scheme.

3.6 Summary

In this chapter, a successive relaying scheme has been proposed to secure the AF relaying network with multiple untrusted nodes, where the detrimental IRI is used as a beneficial source to jam the untrusted nodes. To reduce the information leakage, ZFBF is used at the source node, and relay selection is implemented to

Figure 3.7: Ergodic secrecy rate vs SNR for different schemes, where $N = 4$, $L = 10$, and 50.

minimize the SOP. Considering different CSI availability and complexity, different relay pair selection schemes have been proposed. The closed-form expressions of the lower bound of SOP for different schemes are derived and diversity order analysis is presented as well. It has been shown that the SOP of the proposed max-min relay pair selection scheme approaches that of the optimal scheme, and a diversity order of $N - 1$ can be achieved, which greatly outperforms the existing schemes. Therefore, by employing the successive relaying scheme, secrecy performance can be improved by increasing the number of untrusted nodes.

Chapter 4

Secrecy Throughput

Maximization for MISOME

Wiretap Channels

4.1 Introduction

In this chapter, the secure transmission strategy for a MISOME system with coexistence of Bob and normal user (NU) is investigated. The NU and Bob require normal and secure data transmissions, respectively, and thus the stream for NU can be exploited to confuse the Eves. To guarantee the security of Bob, AN is also deliberately injected into the null space of Bob and NU. The power allocation among Bob, NU and AN, as well as the wiretap code rates, are jointly optimized to maximize the EST, under the average throughput constraint of NU. Both non-adaptive and adaptive transmission schemes are proposed, based on the statistical and instantaneous CSI of the legitimate channels, respectively. It is proven that the EST is a quasi-concave function of the secrecy rate and the power allocated to Bob, and for fixed wiretap code rates, the optimal power allocation is derived in a closed-form expression. An alternative optimization algorithm with guaranteed convergence is proposed to obtain the optimal parameters. Numerical results show

Figure 4.1: The MISOME wiretap channel model.

that the EST increases with the transmitting power and the number of transmit antennas, and decreases with the throughput constraint of NU. Improved EST can be achieved through injecting AN and concurrent transmission of Bob and NU.

4.2 System Model and Problem Statement

4.2.1 System Model and Preliminary

We consider secure communication between Alice and Bob in the presence of a NU and multiple non-colluding Eves. Alice has N antennas while Bob, NU, and Eves are all equipped with one antenna each, as shown in Fig. 4.1. All wireless channels, including the main (Alice to Bob) and wiretap channels (Alice to Eves), experience Rayleigh fading. The channel vector related to legitimate node k is expressed as $\mathbf{h}_k \in \mathbb{C}^{N \times 1}$, where $\mathbf{h}_k$, $k \in \{b, u\}$, is the fading coefficient vector with i.i.d. entries $h_{k,l} \sim \mathcal{CN}(0, \delta_k^2)$. The channel vector related to the i th Eve node is expressed as $\mathbf{g}_i \in \mathbb{C}^{N \times 1}$, where $\mathbf{g}_i$ is the fading coefficient vector with i.i.d. entries $g_{i,j} \sim \mathcal{CN}(0, \delta_g^2)$. We also assume that global CSI of all the legitimate channels and the statistical CSI of the Eves is available due to the passive eavesdropping, which is a very generic assumption and has been adopted in most of the works in physical-layer security [29–31, 89, 90, 92, 93, 95, 104, 138, 143–146].

Since Bob requires higher security clearance, with the instantaneous CSI of Bob, Alice adopts maximum-ratio transmission (MRT), i.e., the weighting vector for Bob's message is $\mathbf{w}_b = \frac{\mathbf{h}_b^*}{\|\mathbf{h}_b^*\|}$. To eliminate the interference to Bob, the beamformer of NU should lie in the null space of $\mathbf{h}_b$, i.e.,

$$\mathbf{w}_u = \frac{(\mathbf{I} - \mathbf{h}_b(\mathbf{h}_b^H \mathbf{h}_b)^{\dagger} \mathbf{h}_b^H) \mathbf{h}_u^*}{\|(\mathbf{I} - \mathbf{h}_b(\mathbf{h}_b^H \mathbf{h}_b)^{\dagger} \mathbf{h}_b^H) \mathbf{h}_u^*\|}. \quad (4.1)$$

To improve the secrecy performance, Alice also injects AN into the null space of $[\mathbf{h}_b, \mathbf{w}_u]^T$ to avoid interfering with Bob and NU. Thus, the transmitted signal of Alice can be expressed as

$$\mathbf{x} = \sqrt{\phi_b P} \mathbf{w}_b s_b + \sqrt{\phi_u P} \mathbf{w}_u s_u + \sqrt{\frac{\phi_n P}{N-2}} \mathbf{V} \mathbf{n}_a, \quad (4.2)$$

where ϕ_b , ϕ_u , and ϕ_n are power allocations for Bob, NU, and AN, respectively. $\mathbf{V} \in \mathbb{C}^{N \times (N-2)}$ is the null space of Bob and NU, $\mathbf{n}_a \in \mathbb{C}^{(N-2) \times 1}$ denotes the AN vector with i.i.d. entries $n_{a,i} \sim \mathcal{CN}(0, 1)$. Following that, the received signals at Bob and NU can be expressed as

$$y_b = \sqrt{\phi_b P} \mathbf{h}_b^T \mathbf{w}_b s_b + n_b \quad (4.3)$$

and

$$y_u = \sqrt{\phi_u P} \mathbf{h}_u^T \mathbf{w}_u s_u + \sqrt{\phi_b P} \mathbf{h}_u^T \mathbf{w}_b s_b + n_u, \quad (4.4)$$

respectively, where n_b and n_u are the zero-mean additive Gaussian noise at Bob and NU with variance σ_b^2 and σ_u^2 . The received signal at the i th Eve is

$$y_{E_i} = \sqrt{\phi_b P} \mathbf{g}_i^T \mathbf{w}_b s_b + \sqrt{\phi_u P} \mathbf{g}_i^T \mathbf{w}_u s_u + \sqrt{\phi_n P} \mathbf{g}_i^T \mathbf{V} \mathbf{n}_a + n_i, \quad (4.5)$$

where n_i is the zero-mean additive Gaussian noise at the i th Eve with variance $\sigma_{e,i}^2$. Since Eve is totally passive and the noise level is not available to Alice, we assume that all the Eves have the same noise power, i.e., $\sigma_{e,i}^2 = \sigma_e^2, \forall i$. Following

that, the SNRs at Bob, NU, and the i th Eve are given by

$$\gamma_b = \frac{\phi_b P |\mathbf{h}_b^T \mathbf{w}_b|^2}{\sigma_b^2}, \quad (4.6)$$

$$\gamma_u = \frac{\phi_u P |\mathbf{h}_u^T \mathbf{w}_u|^2}{\phi_b P |\mathbf{h}_u^T \mathbf{w}_b|^2 + \sigma_u^2}, \quad (4.7)$$

and

$$\gamma_{E,i} = \frac{\phi_b P |\mathbf{g}_i^T \mathbf{w}_b|^2}{\phi_u P |\mathbf{g}_i^T \mathbf{w}_u|^2 + \frac{\phi_b P}{N-2} \|\mathbf{g}_i^T \mathbf{V}\|^2 + \sigma_e^2}, \quad (4.8)$$

respectively. Since the Eves are non-colluding, the maximal eavesdropped information is determined by the maximal SNR among all the Eves, i.e., $\gamma_E = \max_i \{\gamma_{E,i}\}$.

Remark 4.1. For the case that each Eve is equipped with multiple antennas, the Eve can employ the minimum mean square error (MMSE) reception, resulting in a similar expression of $\gamma_{E,i}$ to (4.8). For the sake of analysis, we only consider single-antenna Eves.

Based on the above description, we have the following statistics of γ_b , γ_u , and γ_E . Due to the MRT operation, from (4.6), we can conclude that $\gamma_b \sim \text{Gamma}(N, \lambda_b)$, where $\lambda_b = \frac{\zeta_b}{\phi_b}$, $\zeta_b = \frac{\sigma_b^2}{P\delta_b^2}$. For the CDF of γ_u , and γ_E , we have the following lemmas.

Lemma 4.1. *The CDF of γ_u is given by*

$$F_{\gamma_u}(y) = 1 - \sum_{n=0}^{N-2} \frac{\lambda_{u_2} (\lambda_{u_1} y)^n}{(\lambda_{u_1} y + \lambda_{u_2})^{n+1}} e^{-\lambda_{u_1} y \sigma_u^2} \sum_{m=0}^n \frac{(\sigma_u^2 (\lambda_{u_1} y + \lambda_{u_2}))^m}{m!}, \quad (4.9)$$

where $\lambda_{u_1} = \frac{\sigma_u^2}{\phi_u P \delta_u^2}$ and $\lambda_{u_2} = \frac{\sigma_u^2}{\phi_b P \delta_u^2}$.

Proof. Since $\mathbf{h}_b$ and $\mathbf{h}_u$ are independent with complex Gaussian entries, from (4.1), we can conclude that $\mathbf{w}_b$ and $\mathbf{w}_u$ are uncorrelated and independent. Thus, $A = |\mathbf{h}_u^T \mathbf{w}_u|^2 \sim \text{Gamma}(N-1, \frac{1}{\delta_u^2})$, and $B = |\mathbf{h}_u^T \mathbf{w}_b|^2 \sim \text{Exp}(\frac{1}{\delta_u^2})$ are independent.

Thus,

$$F_{\gamma_u}(y) = \mathbb{P} \left(\frac{\frac{\phi_u P A}{\sigma_u^2}}{\frac{\phi_b P B}{\sigma_u^2} + 1} < y \right). \quad (4.10)$$

Substituting the PDF expressions of A and B into (4.10), and with the aid of [1, eq. (3.351.2)], (4.9) can be obtained. ■

Lemma 4.2. *The CDF of $\gamma_{E,i}$ is given by*

$$F_{\gamma_{E,i}}(z) = 1 - \frac{e^{-\frac{\sigma_e^2 z}{\phi_b P \delta_g^2}}}{\left(1 + \frac{\phi_u}{\phi_b} z\right) \left(1 + \frac{\phi_n z}{\phi_b (N-2)}\right)^{N-2}}. \quad (4.11)$$

Proof. The proof can be obtained by using the CDF of an indefinite Hermitian quadratic form in a random vector. A similar proof can be found in the Appendix of [93, 147]. ■

Thus, the CDF of γ_E can be expressed as

$$F_{\gamma_E}(z) = \left(1 - \frac{e^{-\frac{\sigma_e^2 z}{\phi_b P \delta_g^2}}}{\left(1 + \frac{\phi_u}{\phi_b} z\right) \left(1 + \frac{\phi_n z}{\phi_b (N-2)}\right)^{N-2}} \right)^M. \quad (4.12)$$

Figure 4.2 verifies the CDF of γ_E , we can observe that the theoretical results match well with the simulated ones.

4.2.2 Problem Statement

To guarantee secure transmission, Alice adopts the Wyner's encoding scheme, where the transmission rate and secrecy rate are R_b and R_s , respectively. The difference between R_b and R_s is used as a redundancy rate against eavesdropping, and perfect secrecy is possible only if the capacity of Eve is less than the redundancy rate $R_b - R_s$. Specifically, a transmission outage occurs if the instantaneous capacity of Bob is lower than the transmission rate, i.e., $C_b < R_b$. The probabilities of the transmission outage and secrecy outage are denoted as p_{to} and p_{so} ,

Figure 4.2: The CDF of γ_E , where $N = 8$, $P=10$ dB, $\phi_b = 0.5$, and $\phi_u = 0.3$.

respectively. Then the EST can be expressed as [29]

$$T = R_s(1 - p_{to})(1 - p_{so}). \quad (4.13)$$

Our goal is to optimize the code rates and the power allocations to maximize the EST. In the following, two schemes, namely the non-adaptive transmission scheme and the adaptive transmission scheme are proposed [148], relying on the statistical and instantaneous CSI of the legitimate channels, respectively.

For the non-adaptive transmission scheme, all the parameters are optimized based on the statistical CSI of the legitimate channels and they are fixed for each channel realization. In addition, Alice transmits information to NU only if the received SNR at NU is larger than the predesigned threshold, R_u . Otherwise the signal transmitted to NU will be replaced by another stream of AN with the power

allocated to NU. Thus the EST maximization problem can be formulated as

$$\begin{aligned}
 & \max_{\substack{\phi_b, \phi_u, \\ R_b, R_s, R_u}} T \\
 & s.t. \quad R_u \mathbb{P}(\log_2(1 + \gamma_u) > R_u) \geq \tau, \\
 & \quad \phi_b + \phi_u \leq 1, \quad 0 \leq \phi_b, \phi_u \leq 1,
 \end{aligned} \tag{4.14}$$

where τ is the average throughput constraint of NU.

For the adaptive transmission scheme, all the parameters are optimized based on the instantaneous CSI of the legitimate channels. Hence, Alice can adaptively set $R_b = C_b$ to avoid transmission outage. Then the EST becomes $T = R_s(1 - p_{so})$, and (4.14) reduces to

$$\begin{aligned}
 & \max_{\phi_b, \phi_u, R_s} R_s(1 - p_{so}) \\
 & s.t. \quad \log_2(1 + \gamma_u) \geq \tau, \\
 & \quad \phi_b + \phi_u \leq 1, \quad 0 \leq \phi_b, \phi_u \leq 1.
 \end{aligned} \tag{4.15}$$

Moreover, the average throughput constraint of the NU in (4.14) should be changed as an instantaneous throughput constraint, thus the threshold R_u is not required. Note that if the instantaneous throughput constraint of NU is too large, the problem may be infeasible. In this case, Alice will cease transmission.

4.3 Non-Adaptive Transmission Scheme

As stated earlier, the transmission outage probability can be calculated as

$$p_{to} = \mathbb{P}(\log_2(1 + \gamma_b) < R_b) = 1 - e^{-\lambda_b \bar{\gamma}_b} \sum_{n=0}^{N-1} \frac{(\lambda_b \bar{\gamma}_b)^n}{n!}, \tag{4.16}$$

where $\bar{\gamma}_b = 2^{R_b} - 1$. Similarly, with the aid of the CDF of γ_E given in (4.12), the SOP can be expressed as

$$p_{so} = 1 - \left(1 - \frac{e^{-\frac{\sigma_e^2 \bar{\gamma}_e}{\phi_b P \delta_g^2}}}{\left(1 + \frac{\phi_u}{\phi_b} \bar{\gamma}_e\right) \left(1 + \frac{\phi_n \bar{\gamma}_e}{\phi_b (N-2)}\right)^{N-2}} \right)^M, \quad (4.17)$$

where $\bar{\gamma}_e = 2^{R_b - R_s} - 1$.

From (4.16) and (4.17), we can observe that the optimization problem (4.14) are complicated functions of R_b , R_s , R_u , ϕ_b , and ϕ_u , which is difficult to solve directly. In the following, we adopt an alternative optimization procedure to find the optimal solution. We first optimize the parameters that belong to NU, i.e., R_u and ϕ_u for fixed R_b , R_s , and ϕ_b . Once R_u and ϕ_u are obtained, the throughput constraint can be removed. Then ϕ_b , R_s , and R_b can be optimized iteratively.

4.3.1 Optimization for Normal User

In this subsection, we focus on optimizing the parameters for NU with fixed R_b , R_s , and ϕ_b . From the first constraint of (4.14), we can derive the minimum ϕ_u that meets the average throughput constraint of NU, which is given by

$$\phi_{u,\min} = \bar{\gamma}_u \phi_b \left(\left(1 - \frac{\tau}{R_u} \right)^{-\frac{1}{N-1}} - 1 \right), \quad (4.18)$$

where $\bar{\gamma}_u = 2^{R_u} - 1$.

Proof. From (4.9), we can obtain the transmission probability of the NU, which is shown to be too complicated to analyze. Note that the interference from Alice to NU is usually much stronger than the noise. Thus the noise component in (4.10)

can be ignored. Hence, we have

$$F_{\gamma_u}(y) \approx \mathbb{P}\left(\frac{\phi_u A}{\phi_b B} < y\right) = 1 - \sum_{n=0}^{N-2} \frac{\frac{1}{\phi_b \delta_u^2} \left(\frac{1}{\phi_u \delta_u^2} y\right)^n}{\left(\frac{1}{\phi_u \delta_u^2} y + \frac{1}{\phi_b \delta_u^2}\right)^{n+1}} = \left(\frac{\phi_b y}{\phi_b y + \phi_u}\right)^{N-1}. \quad (4.19)$$

Thus, we have the following derivation:

$$\begin{aligned} \mathbb{P}(\log_2(1 + \gamma_u) > R_u) &\geq \frac{\tau}{R_u}, \\ \Leftrightarrow 1 - \mathbb{P}(\log_2(1 + \gamma_u) < R_u) &\geq \frac{\tau}{R_u} \\ \Rightarrow \left(\frac{\phi_b \bar{\gamma}_u}{\phi_b \bar{\gamma}_u + \phi_u}\right)^{N-1} &\leq 1 - \frac{\tau}{R_u}, \\ \Rightarrow \phi_u &\geq \bar{\gamma}_u \phi_b \left(\left(1 - \frac{\tau}{R_u}\right)^{-\frac{1}{N-1}} - 1\right). \end{aligned} \quad (4.20)$$

This completes the proof. ■

Note that the throughput constraint should satisfy $0 < \phi_{u,\min} < 1$. Otherwise, the problem is infeasible. For fixed R_b , R_s , and ϕ_b , we can prove that p_{so} first decreases and then increases with the increase in ϕ_u . The minimum SOP can be achieved at $\phi_u = \frac{1-\phi_b}{N-1}$. Thus the optimal value of ϕ_u that maximizes the EST is given by

$$\phi_u^* = \max\left(\frac{1-\phi_b}{N-1}, \phi_{u,\min}\right). \quad (4.21)$$

When $\phi_{u,\min} > \frac{1-\phi_b}{N-1}$, the EST is a monotonically decreasing function of ϕ_u . We need to optimize R_u to minimize $\phi_{u,\min}$ and maximize the objective function. Note that the minimization of $\phi_{u,\min}$ on one hand will minimize the SOP, and on the other hand it will enlarge the feasible region of ϕ_b . Both of these are beneficial to the EST maximization. Then the optimization problem can be formulated as

$$\min_{R_u} \phi_{u,\min}. \quad (4.22)$$

To obtain some analytical results, we resort to optimize its upper bound. From

(4.18), we have

$$\phi_{u,\min} < \phi_{u,\min}^U = 2^{R_u} \phi_b \left(\frac{1}{x} - 1 \right) \triangleq f(R_u), \quad (4.23)$$

where $x = \left(1 - \frac{\tau}{R_u}\right)^{\frac{1}{N-1}}$. By taking the first derivative of $f(R_u)$, we have

$$\frac{\partial f(R_u)}{\partial R_u} = 2^{R_u} \phi_b \left[\ln 2 \left(\frac{1}{x} - 1 \right) + \frac{1}{N-1} \frac{\tau}{R_u^2 x^N} \right]. \quad (4.24)$$

By setting the above equation to zero, we can obtain the optimal R_u by finding the root of the following function:

$$y(x) \triangleq \ln 2(x^{N-1} - x^N) + \frac{x^{2N-2} - 2x^{N-1} + 1}{\tau(N-1)}. \quad (4.25)$$

Using the Descartes' rule [149], we can conclude that $y(x) = 0$ has two positive roots. In addition, we can find that $y(1) = 0$ and $y(x) > 0$ for $x > 1$. Therefore, there must exist a single positive root within $(0, 1)$. Then the optimal R_u^* can be obtained through solving (4.25) numerically, such as by using the bisection searching method. Substituting R_u^* into (4.18), we can obtain the minimum of $\phi_{u,\min}$. Then we have the following corollary.

Corollary 4.1. *For fixed R_b and R_s , the optimal value of ϕ_u that maximizes the EST becomes $\frac{1-\phi_b}{N-1}$ when $\tau \leq \tau_0$, where*

$$\tau_0 = R_u^* \left(1 - \left(\frac{1-\phi_b}{N-1} \frac{1}{\phi_b \bar{\gamma}_u^*} + 1 \right)^{-(N-1)} \right), \quad (4.26)$$

with $\bar{\gamma}_u^* = 2^{R_u^*} - 1$. Moreover, ϕ_u^* approaches zero when N approaches infinity.

Proof. When $\tau \leq \tau_0$, the minimum power required by NU, $\phi_{u,\min}$, is less than $\frac{1-\phi_b}{N-1}$, and thus, from (4.21), the optimal value of ϕ_u becomes $\frac{1-\phi_b}{N-1}$. When $N \rightarrow \infty$, from (4.21) and (4.18), we can conclude that ϕ_u approaches zero. ■

Remark 4.2. Corollary 4.1 implies that when the average throughput requirement of the normal user is less than τ_0 , it is better to equally allocate the power of NU

and each stream of the artificial noise. This is due to the function

$$f(\phi_u) = \left(1 + \frac{\phi_u}{\phi_b} \bar{\gamma}_e\right)^{-1} \left(1 + \frac{\phi_n \bar{\gamma}_e}{\phi_b(N-2)}\right)^{-(N-2)} \quad (4.27)$$

is Schur-convex [150], and thus the minimum value of p_{so} is achieved when the power of each stream is equally distributed. From (4.18), we can also observe that $\phi_{u,\min}$ is a monotonically increasing function of the throughput requirement τ . With the increase of τ , $\phi_{u,\min}$ will increase, i.e., more power should be allocated in the stream of the normal user.

4.3.2 Power Allocation Optimization for Bob

Once R_u^* and ϕ_u^* are obtained, we then focus on optimizing ϕ_b . Due to the complex form of (4.16) and (4.17), it is not straightforward to determine the concavity of T w.r.t. ϕ_b , for fixed R_b and R_s . In the following, we prove that the EST is a quasi-concave function of ϕ_b by showing that it satisfies the second order condition of the quasi-concave function given by the following lemma.

Lemma 4.3. [151, Section 3.4.3] $f(x)$ is a quasi-concave function on $\mathbb{R}$, if and only if

$$\frac{\partial f(x)}{\partial x} = 0 \Rightarrow \frac{\partial^2 f(x)}{\partial x^2} \leq 0. \quad (4.28)$$

We first define $\beta = \frac{\zeta_e}{\phi_b} - 1$, $\zeta_e = \frac{\sigma_e^2}{P\delta_g^2} + 1$, then based on Lemma 4.3, we have the following theorem.

Theorem 4.1. For fixed code rates and ϕ_u , the EST, $T(\phi_b)$, is a quasi-concave function of ϕ_b , and the optimal ϕ_b that maximizes the EST is given by

$$\phi_b^* = \min(\phi_b^o, 1 - \phi_u), \quad (4.29)$$

where

$$\begin{cases} \phi_b^o \approx \frac{\mu_1}{W(\mu_1 e^{\mu_1} \mu_2^{\frac{1}{N}})}, \\ \mu_1 = \frac{\bar{\gamma}_e - \zeta_b \bar{\gamma}_b}{N}, \\ \mu_2 = \frac{M \bar{\gamma}_e (N-1)! e^{\zeta_b \bar{\gamma}_b}}{\bar{\gamma}_b^{N-1} \zeta_b^{N+1}}. \end{cases} \quad (4.30)$$

Note that $W(x)$ is the Lambert W -function [152].

Proof. Please refer to Appendix B.1. ■

Combining (4.29) and (4.21), we can obtain the optimal power allocations as follows.

Theorem 4.2. *For fixed wiretap code rates, the optimal values of ϕ_b and ϕ_u that maximize the EST are determined by*

$$\phi_b^* = \begin{cases} \phi_b^o, & \text{if } \phi_b^o \leq \frac{1}{\eta+1}, \\ \frac{1}{\eta+1}, & \text{otherwise.} \end{cases} \quad (4.31)$$

$$\phi_u^* = \begin{cases} \phi_b^o \eta, & \text{if } \phi_b^o \leq \frac{1}{\eta+1}, \tau \geq \tau_0^o, \\ 1 - \frac{1 - \phi_b^o}{N-1}, & \text{if } \phi_b^o \leq \frac{1}{\eta+1}, \tau < \tau_0^o, \\ \frac{\eta}{\eta+1}, & \text{otherwise.} \end{cases} \quad (4.32)$$

where $\eta = \bar{\gamma}_u^* \left(\left(1 - \frac{\tau}{R_u^*} \right)^{-\frac{1}{N-1}} - 1 \right)$, τ_0^o is obtained by substituting $\phi_b = \phi_b^o$ into (4.26).

Proof. Please refer to Appendix B.2. ■

Remark 4.3. The third condition of (4.32) states that injecting AN is unnecessary in this case. This will happen either when the redundancy rate is very large or the throughput requirement of NU is very high. For the former case, the SOP, p_{so} , will approach zero, and the EST becomes an increasing function w.r.t. ϕ_b . For the latter case, with the increase of the throughput requirement of NU, ϕ_u^* will

Figure 4.3: The EST vs. ϕ_b for different parameters, with $\bar{P} = 10$ dB, $M = 5$, and $\tau = 1$ bps/Hz.

increase, and the available power for Bob and AN will decrease. Thus, the power allocated to AN will asymptotically approach zero in those two cases.

Figure 4.3 shows the EST versus ϕ_b with different system configurations, where the noise variances at Bob, NU and Eves are assumed to be the same, i.e., $\sigma_b^2 = \sigma_u^2 = \sigma_e^2 = \sigma^2$, and the transmitting power of the source is normalized by the noise variance, denoted as $\bar{P}$ in the following simulations, i.e., $\bar{P} = P/\sigma^2$. Note that R_b and R_s are fixed and are different among the four simulations. We can observe that the EST is a quasi-concave function w.r.t. ϕ_b , which validates Theorem 4.1. Moreover, the theoretical optimal value of ϕ_b obtained by (4.31) is quite close to the simulation results, and the gap decreases with the increase of the number of transmit antennas, N .

So far, we have derived the optimal power allocations. We then conduct the asymptotic analysis to provide some insights.

Corollary 4.2. *For fixed R_b and R_s , the optimal power allocation ϕ_b approaches zero when N or P approaches infinity.*

Proof. When $N \rightarrow \infty$, $\eta \rightarrow 0$, $\mu_2 \rightarrow \infty$, from (4.30), we know $\phi_b^o \rightarrow 0$. Thus, $\phi_b^* = \phi_b^o \rightarrow 0$. Similarly, we can obtain the conclusion when P approaches infinity. ■

Figure 4.4: The optimal value of ϕ_b vs. N , with $R_b = 4$ bps/Hz, $R_s = 3$ bps/Hz, $M = 10$, and $\tau = 2$ bps/Hz.

The asymptotic behavior of ϕ_b can be explained as follows. From (4.16), when N or P approaches infinity, the transmission outage probability p_{to} will approach zero. In this case, $T \approx R_s(1 - p_{so})$. Thus,

$$\frac{\partial T}{\partial \phi_b} \approx -R_s \frac{\partial p_{so}}{\partial \phi_b} < 0. \quad (4.33)$$

This indicates that the EST becomes a monotonically decreasing function of ϕ_b . Hence, the optimal ϕ_b will asymptotically approach 0 with the increase in transmitting power and the number of transmit antennas, as shown in Fig. 4.4.

4.3.3 Code Rate Optimization

With the obtained ϕ_b^* , ϕ_u^* , and R_u^* in the last subsection, we need to optimize R_s . Similar to Theorem 4.1, we have the following property of the EST w.r.t. R_s .

Theorem 4.3. *For fixed power allocation, the EST is a quasi-concave function of R_s , and the optimal value of R_s is determined by*

$$R_s^* = \min(R_b, R_s^o), \quad (4.34)$$

Figure 4.5: The EST vs. R_s with different parameters, where $M = 5$ and $\tau = 2\text{bps/Hz}$.

where R_s^o is the root of the following equation

$$1 - e^{-\beta\bar{\gamma}_e} - \ln 2 R_s M \beta (\bar{\gamma}_e + 1) e^{-\beta\bar{\gamma}_e} = 0. \quad (4.35)$$

Proof. Please refer to Appendix B.3. ■

Figure 4.5 shows the EST versus the secrecy rate R_s for fixed R_b and ϕ_b . We can observe that the EST is a quasi-concave function w.r.t. R_s and the theoretical results of the optimal R_s are quite close to the simulation results, which verifies the conclusion in Theorem 4.3. This is because the SOP is a decreasing function of R_s , and the EST, defined as the product of the secrecy rate R_s and the SOP, first increases and then decreases with increasing R_s . Moreover, we observe that the optimal R_s increases with the growth of transmitting power and number of transmit antennas, N , which means that a higher secrecy rate can be adopted.

So far, we have solved the optimal power allocations ϕ_b and ϕ_u , and the secrecy rate R_s . Next, we need to determine R_b . Similar to Theorems 4.1 and 4.3, we can prove that the EST is also a quasi-concave function w.r.t. R_b , this is because the transmission outage probability monotonically increases with the increase of R_b , whereas the SOP is a monotonic decreasing function of R_b for fixed power

allocations and secrecy rate. Therefore, the EST first increases and then decreases with the increase of R_b . The optimal value of R_b can be obtained through bisection searching. Since the EST is quasi-concave w.r.t. different parameters, according to [153], the convergence of the proposed alternative algorithm to a stationary point can be guaranteed. The whole procedure of the non-adaptive transmission scheme is summarized in Algorithm 1.

Algorithm 1 Non-adaptive scheme for EST maximization

- 1: Initialization: $N, M, R_b^{min}, R_b^{max}, \tau$, and the accuracy ϵ ;
 - 2: Calculate x numerically according to (4.25), and then obtain the transmission threshold R_u ;
 - 3: Set $R_b \in [R_b^{min}, R_b^{max}]$, $R_s \in (0, R_b]$;
 - 4: $i = 1$, compute ϕ_b^o and $\phi_{u,min}$ with (4.30) and (4.18), respectively, and determine ϕ_b^* and ϕ_u^* with Theorem 4.2;
 - 5: Given ϕ_b^* and ϕ_u^* , determine R_s^* with (4.34);
 - 6: Compute the EST in the i th iteration, $T(i)$, by (4.13);
 - 7: Set $i = i + 1$, $R_s = R_s^*$, repeat Steps 4 to 6 till $|T(i + 1) - T(i)| \leq \epsilon$;
 - 8: Using the bisection searching method, repeat Steps 4 to 7 to find the optimal R_b^* .
-

4.4 Adaptive Transmission Scheme

In this section, we will optimize the parameters for the adaptive transmission scheme. In this scheme, the instantaneous CSI of the legitimate channels is available at Alice. Thus both the code rates and the power allocations are changed dynamically based on the channel realizations. With the CSI of Bob, R_b is set as C_b , where $C_b = \log_2(1 + \tilde{\gamma}_b)$ is the instantaneous SNR of Bob, with $\tilde{\gamma}_b = \phi_b \gamma_0$, $\gamma_0 = \frac{P|\mathbf{h}_b^T \mathbf{w}_b|^2}{\sigma_b^2}$. Therefore, the transmission outage disappears in this case. The

SOP becomes

$$p_{so} = \mathbb{P}(C_e > C_b - R_s | \tilde{\gamma}_b) = 1 - (1 - e^{-\beta \tilde{\gamma}_{A,e}})^M, \quad (4.36)$$

where $\tilde{\gamma}_{A,e} = 2^{-R_s}(1 + \tilde{\gamma}_b) - 1$. To solve the EST maximization problem in (4.15), we also adopt the alternative optimization method. From the first constraint of (4.15), we can derive the minimum ϕ_u that satisfies the average throughput requirement as

$$\phi_{u,\min} = \frac{\phi_b P |\mathbf{h}_u^T \mathbf{w}_b|^2 + \sigma_u^2}{P |\mathbf{h}_u^T \mathbf{w}_u|^2} (2^r - 1). \quad (4.37)$$

Similar to the optimization for the non-adaptive scheme, we have the following theorem.

Theorem 4.4. *The EST is a quasi-concave function w.r.t. ϕ_b , and the critical point of ϕ_b is given by*

$$\phi_b^o = \sqrt{\frac{2^{R_s} - 1}{\gamma_0}}. \quad (4.38)$$

Proof. The quasi-concave property can be proved similar to the proof of Theorem 4.1, and is omitted here. Hence, the optimal value of ϕ_b that maximizes the EST can be obtained numerically, which lies either on the critical point or the boundary. Note that the critical point can be calculated by setting the first order derivative to zero, after some mathematical manipulations, we obtain (4.38). ■

Then we have the following theorem.

Theorem 4.5. *For fixed R_s , the optimal values of ϕ_b and ϕ_u that maximize the EST are determined by*

$$\phi_b^* = \begin{cases} \phi_b^o, & \text{if } \phi_b^o \leq \frac{1}{\xi+1}, \\ \frac{1}{\xi+1}, & \text{otherwise.} \end{cases} \quad (4.39)$$

Figure 4.6: The EST vs. ϕ_b with different parameters, where $N = 10$, $M = 3$, $R_b = 5$ bps/Hz, and $\phi_u = 0.2$.

$$\phi_u^* = \begin{cases} \phi_b^o \xi, & \text{if } \phi_b^o \leq \frac{1}{\xi+1}, \tau \geq \tau_a, \\ 1 - \frac{1-\phi_b^o}{N-1}, & \text{if } \phi_b^o \leq \frac{1}{\xi+1}, \tau < \tau_a, \\ \frac{\eta}{\eta+1}, & \text{otherwise.} \end{cases} \quad (4.40)$$

where $\xi = \frac{|\mathbf{h}_u^T \mathbf{w}_b|^2}{|\mathbf{h}_u^T \mathbf{w}_u|^2} (2^\tau - 1)$, $\tau_a = \log_2 \left(1 + \frac{1-\phi_b}{(N-1)\phi_b \xi} \right)$.

Proof. The proof is similar to the proof of Theorem 4.2, and is omitted here. ■

Figure 4.6 shows the EST versus ϕ_b for fixed R_b and different R_s , we can observe that the EST is a quasi-concave function w.r.t. ϕ_b for the adaptive transmission scheme, and the optimal value that maximizes the EST matches with the theoretical result obtained by Theorem 4.5. In addition, we can observe that the optimal value of ϕ_b shifts to the left and the EST improves when γ_0 increases, which indicates that less power is required for Bob. Hence, the available power for jamming will increase, and the EST can be improved.

Similar to the non-adaptive scheme, with the obtained ϕ_b , we can determine R_s with (4.34). The whole procedure of the adaptive scheme is summarized in Algorithm 2.

Algorithm 2 Adaptive scheme for EST Maximization

-
- 1: Initialization: N , M , τ , and the accuracy ϵ ;
 - 2: Calculate $C_b^{max} = \log_2(1 + \gamma_0)$, set $R_s \in (0, C_b^{max}]$;
 - 3: $i = 1$, compute ϕ_b^o with (4.38), and determine ϕ_b^* and ϕ_u^* with Theorem 4.5;
 - 4: Given ϕ_b^* and ϕ_u^* , determine R_s^* with (4.34);
 - 5: Compute the EST in the i th iteration, $T(i)$, by (4.13);
 - 6: Set $i = i + 1$, $R_s = R_s^*$, repeat Steps 3 to 5 till $|T(i + 1) - T(i)| < \epsilon$;
-

4.5 Numerical Results and Discussions

In this section, numerical results are presented to show the performance of the proposed schemes. We assume that all channels experience Rayleigh fading, and the channel variations are the same, i.e., $\delta_b^2 = \delta_u^2 = \delta_g^2 = 1$. As mentioned in Section 4.3, the noise variances at Bob, NU and Eves are assumed to be the same, i.e., $\sigma_b^2 = \sigma_u^2 = \sigma_e^2 = \sigma^2$, and the normalized transmitting power, $\bar{P}$, varies from 10 dB to 40 dB. The accuracy level is $\epsilon = 0.1$.

In Fig. 4.7, we evaluate the EST achieved by the non-adaptive transmission scheme versus the number of transmit antennas N , with ϕ_b calculated by the theoretical result in Theorem 4.2 and the numerical searching, under different transmitting power levels. We can observe that the EST rises with the increase in N , because a larger N not only improves the capacity of Bob and NU, but also leverages more degrees of freedom to jam Eve. Moreover, we also observe from Fig. 4.7 that the achievable EST enhances with the increase of the transmitting power, which is quite straightforward. Note that the theoretical results match well with the numerical results, verifying the accuracy of our solution.

The secrecy performance of the non-adaptive scheme and the adaptive transmission scheme is compared in Fig. 4.8. We can observe that the EST achieved by the adaptive transmission scheme outperforms that of the non-adaptive scheme. This is because, in the adaptive transmission scheme, all the parameters are adaptively adjusted based on the instantaneous CSI of the legitimate channel, while

Figure 4.7: The EST of the non-adaptive scheme vs. N with different transmitting power, where $M = 5$ and $\tau = 5$ bps/Hz.

these parameters are fixed in the non-adaptive transmission scheme. Thus, the performance improvement is achieved at the cost of higher complexity. In addition, we observe that the EST of both the non-adaptive and adaptive transmission schemes increases with the increase of transmitting power. This is because linearly scaling of the power allocations will increase the capacity of Bob without affecting capacities of NU and Eves.

The achievable EST versus the throughput constraint of NU, τ , is shown in Fig. 4.9. We can observe that a trade-off exists between the EST and τ , for both the non-adaptive scheme and the adaptive scheme. When τ is small, increasing τ will not definitely decrease the EST for the non-adaptive transmission scheme. This is because the optimal ϕ_b lies on the critical point for small τ . With the increase of τ , the available power for Bob decreases and the optimal ϕ_b that maximizes the EST moves to the boundary, and the EST decreases. For the adaptive scheme, similar conclusions can be attained. We can also observe that increasing the number of transmit antennas will result in higher EST.

Lastly, the secrecy performance of different schemes is compared in Fig. 4.10, where the scheme without NU can be regarded as a special case of the non-adaptive

Figure 4.8: The EST of the non-adaptive and adaptive transmission schemes vs. $\bar{P}$ with different N and τ , where $M = 5$.

Figure 4.9: The EST of the non-adaptive and adaptive transmission schemes vs. τ with different parameters, where $\bar{P} = 20$ dB.

Figure 4.10: The secrecy performance comparison among different schemes, where $M = 5$ and $\tau = 4$ bps/Hz.

scheme under the throughput constraint $\tau = 0$. It can thus be regarded as an upper bound for the non-adaptive scheme, and we can observe that the gap between the two schemes narrows with the increasing number of transmit antennas, N , for a fixed τ . Accordingly, it is better to employ more antennas at the source to increase the EST when the throughput constraint is very large. We can also observe that the EST performance deteriorates without injecting AN, showing the importance of AN for secure transmission.

4.6 Summary

In this chapter, the secure transmission strategy in a MISOME wiretap channel, where Bob coexists with a normal user, has been investigated. The power allocation among Bob, NU, and artificial noise, as well as the wiretap code rates are jointly optimized to maximize the EST, under the average throughput constraint of the normal user. An alternative optimization algorithm has been proposed to obtain the optimal parameters for both the non-adaptive and adaptive transmission schemes, based on the statistical and instantaneous CSI of the legitimate

channels, respectively. For fixed code rates, closed-form expressions for the power allocation have been derived. It has been shown that more power should be allocated to the normal user with the increase of its throughput constraint, and the power allocated to the secure user asymptotically approaches zero when the transmitting power or the number of transmit antennas approaches infinity. Moreover, improved EST can be achieved through injecting AN and concurrent transmission of Bob and normal user.

Chapter 5

Physical Layer Security in Multi-Antenna Small-Cell Networks

5.1 Introduction

In this chapter, physical layer security in a multi-antenna small-cell network is investigated, where the spatial distributions of the multi-antenna BSs, cellular users, and Eves are modelled by three independent Poisson point processes. To improve the secrecy performance, AN-aided transmission is adopted at each BS. Based on the stochastic geometry, we first derive the closed-form expressions of the connection and secrecy outage probabilities, and then analyze the impact of different parameters through asymptotic analysis. It is shown that the connection outage probability decreases with an increase of the BS density and the number of the antennas at each BS. The SOP decreases and asymptotically converges to a constant value with an increase of the BS density. The secrecy area spectral efficiency (SASE) is analyzed for both fixed and adaptive-rate transmission schemes. Specifically, the AN transmission region is deduced for a fixed-rate transmission scheme, which reveals the benefits of inter-cell interference to the system's secrecy

Figure 5.1: A small cell network model, where the BSs, cellular users, and Eves are distributed according to three independent homogeneous PPPs.

performance. A semi closed-form expression of the lower bound of the average secrecy rate is also derived, which is shown to be a quasi-concave function of the power allocation factor and a monotonic decreasing function of the ratio of the Eve-BS density. We then extend the study to a high cell-load case by adopting the ZFBF scheme to support multi-user transmission, and the optimal number of users maximizing the SASE is discussed, which is shown to be a fixed portion of the number of transmit antennas. Finally, we investigate the impact of adaptive Eves with eavesdropping and jamming capability on the secrecy performance by assuming that those Eves who are far away from the BSs act as smart jammers to degrade the reception of cellular users. The feasible region that enables adaptive eavesdropping is derived and the optimal strategies for the BS and each Eve are analyzed under the framework of the Stackelberg game.

5.2 System Model

As shown in Fig. 5.1, we consider secure downlink communication in a cellular network, where each BS wants to deliver confidential information to its associated

cellular users in the presence of Eves. The BSs, cellular users, and Eves are distributed according to three independent homogeneous PPPs in $\mathbb{R}^2$, denoted as Φ_b , Φ_u , and Φ_e , with intensities λ_b , λ_u , and λ_e , respectively. Each BS is equipped with N antennas and the cellular users and Eves are equipped with one antenna each. The Eves only passively overhear the information from the BSs without malicious attacks and they are assumed to be non-colluding. Universal frequency reuse is assumed, thus we only consider the interference-limited case and the thermal noise is neglected as compared with the aggregate interference from other BSs [35, 154–158].

5.2.1 User Association and Channel Model

We assume that each user is associated with the nearest BS. As mentioned in [154], there may be some BSs that do not have any users to serve. These BSs will not transmit any signal and they are called inactive BSs. The probability that a BS being active is denoted as p_a , which can be given by [154, 159]

$$p_a = 1 - \left(1 + \frac{\rho}{\mathcal{A}_0}\right)^{-\mathcal{A}_0}, \quad (5.1)$$

where $\mathcal{A}_0 = 3.5$ for the nearest BS association scheme and $\rho = \frac{\lambda_u}{\lambda_b}$ denotes the cell load.

We assume that each BS has perfect CSI knowledge of its associated users and only the statistical CSI of Eves is available. This is a common assumption made in the literature of physical layer security [35, 105, 106, 109, 112, 158]. All the wireless channels are assumed to experience independent small-scale Rayleigh fading as well as a large-scale fading with a path loss exponent of $\alpha > 2$. The channel from the i th BS to the k th associated user in the j th cell is denoted as $\mathbf{h}_{ij}^{(k)}(r_{ij}^{(k)})^{-\frac{\alpha}{2}}$, where the small scale fading vector $\mathbf{h}_{ij}^{(k)} \in \mathbb{C}^{N \times 1}$ has i.i.d. entries $\mathcal{CN}(0, 1)$, and $r_{ij}^{(k)}$ denotes the corresponding distance. Similarly, the eavesdropping channel from the i th BS to the l th Eve is denoted as $\mathbf{g}_{i,e_l}r_{i,e_l}^{-\frac{\alpha}{2}}$, where the i.i.d. entries in the

small scaling fading vector follow $g_{i,e_l} \sim \mathcal{CN}(0, 1)$.

Since there may be multiple users in a cell, in this chapter, we first investigate the single-user case where the BSs randomly choose one user to serve at each time slot with intra-cell time division multiple access, and then extend to a multi-user case in Section 5.5.

5.2.2 Wiretap Code and AN Transmission Scheme

To improve the secrecy performance, each BS adopts Wyner's encoding scheme with transmission rate R_t and secrecy rate R_s . The difference between R_t and R_s is used to measure the redundancy rate against eavesdropping. For a typical user in a cell, reliable connection is achieved only if the instantaneous capacity is larger than the transmission rate, i.e., $C_u > R_t$, and secrecy outage occurs if the instantaneous capacity of Eve is larger than the redundancy rate, i.e., $C_e > R_t - R_s$. To degrade the eavesdropping capacity, AN is deliberately injected into the null space of the intended user's channel without interfering the intended receiver. Then the transmitted signal at the i th BS can be expressed as

$$\mathbf{x}_i = \sqrt{\phi P} \mathbf{w}_i s_i + \sqrt{(1 - \phi)P} \mathbf{G}_i \mathbf{n}_a, \quad (5.2)$$

where ϕ is the power allocation between the information bearing signal and AN, P is the total transmit power, s_i is the information bearing signal with $\mathbb{E}[|s_i|^2] = 1$, $\mathbf{n}_a$ is an AN vector with i.i.d. entries $n_a \sim \mathcal{CN}(0, \frac{1}{N-1})$. $\mathbf{w}_i = \frac{\mathbf{h}_{i,i}^*}{\|\mathbf{h}_{i,i}^*\|}$ is the beamforming vector of the i th BS, $\mathbf{G}_i \in \mathbb{C}^{N \times (N-1)}$ is a weighting matrix for the AN. Note that the superscript (k) is omitted without causing confusion for the ease of notation for the single-user case. $\mathbf{G}_i$ lies in the null space of $\mathbf{h}_{i,i}$ and its columns are mutually orthogonal. We assume that each BS uses the same power allocation factor to facilitate the following analysis.

5.2.3 SIR Expression and Preliminary

We assume that a typical user is located at the origin and its associated BS is denoted as the 0th BS. In the following, we will analyze the performance of the typical user and the obtained results also apply to a general user based on the Slivnyak's theorem [125]. Hence, the received signal-to-interference ratio (SIR) at the typical user can be expressed as

$$\gamma_{u_0} = \frac{\phi P |\mathbf{h}_{0,0}^T \mathbf{w}_0|^2 r_{0,0}^{-\alpha}}{I_B}, \quad (5.3)$$

where the interference term is given by

$$I_B = \sum_{i \in \Phi_b^a \setminus \{0\}} \phi P \left[|\mathbf{h}_{i,0}^T \mathbf{w}_i|^2 + \xi_i \|\mathbf{h}_{i,0}^T \mathbf{G}_i\|^2 \right] r_{i,0}^{-\alpha}. \quad (5.4)$$

Note that Φ_b^a is the active BS set, and $\xi = \frac{\phi^{-1}-1}{N-1}$. Similarly, the received SIR at the k th Eve can be expressed as

$$\gamma_{e_l} = \frac{\phi P |\mathbf{g}_{0,e_l}^T \mathbf{w}_0|^2 r_{0,e_l}^{-\alpha}}{\xi \phi P \|\mathbf{g}_{0,e_l}^T \mathbf{G}_0\|^2 r_{0,e_l}^{-\alpha} + I_{B,e_l}}, \quad (5.5)$$

where the interference is given by

$$I_{B,e_l} = \sum_{i \in \Phi_b^a \setminus \{0\}} \phi P \left[|\mathbf{g}_{i,e_l}^T \mathbf{w}_i|^2 + \xi \|\mathbf{g}_{i,e_l}^T \mathbf{G}_i\|^2 \right] r_{i,e_l}^{-\alpha}. \quad (5.6)$$

Since the Eves are non-colluding, the maximal eavesdropped information is determined by the maximal SIR among all the Eves, i.e., $\gamma_E = \max_l \{\gamma_{e_l}\}$.

Based on the above assumptions, we have $|\mathbf{h}_{0,0}^T \mathbf{w}_0|^2 \sim \text{Gamma}(N, 1)$ and $\|\mathbf{h}_{i,0}^T \mathbf{G}_i\|^2 \sim \text{Gamma}(N-1, 1)$. Since $\mathbf{w}_0$ is independent of the eavesdropping channel, we have $|\mathbf{g}_{i,e_l}^T \mathbf{w}_i|^2 \sim \text{Exp}(1)$. With these probability statistics, in the next section, we will present the connection and secrecy outage probabilities.

5.3 Outage Probability Analysis

5.3.1 Connection Outage Probability

The connection outage probability can be calculated by

$$\begin{aligned}
 p_{co} &= \mathbb{P}(C_u < R_t) = \mathbb{P}(\gamma_{u_0} < \bar{\gamma}) \\
 &= \mathbb{P}\left(|\mathbf{h}_{0,0}^T \mathbf{w}_0|^2 < \frac{\bar{\gamma} I_{B r_{0,0}^\alpha}}{\phi P}\right) \\
 &\stackrel{(a)}{=} 1 - \sum_{n=0}^{N-1} \mathbb{E}_{r_{0,0}} \mathbb{E}_{I_B} \left[\frac{1}{n!} \left(\frac{\bar{\gamma} I_{B r_{0,0}^\alpha}}{\phi P} \right)^n e^{-\frac{\bar{\gamma} I_{B r_{0,0}^\alpha}}{\phi P}} \right] \\
 &\stackrel{(b)}{=} 1 - \sum_{n=0}^{N-1} \mathbb{E}_{r_{0,0}} \left[\frac{(-1)^n s^n}{n!} \frac{d^n \mathcal{L}_{I_B}(s)}{ds^n} \right],
 \end{aligned} \tag{5.7}$$

where $\bar{\gamma} = 2^{R_t} - 1$, (a) is due to the fact that $|\mathbf{h}_{0,0}^T \mathbf{w}_0|^2 \sim \text{Gamma}(N, 1)$, (b) follows from $\mathbb{E}[I^n e^{-sI}] = (-1)^n d^n \mathcal{L}_I(s) / ds^n$. Then we have the following theorem.

Theorem 5.1. *The connection outage probability with AN is given by*

$$p_{co} = 1 - \frac{1}{p_a} \left\| \left[\left(k_0 + \frac{1}{p_a} \right) \mathbf{I} - \mathbf{Q}_N \right]^{-1} \right\|_1, \tag{5.8}$$

where

$$\mathbf{Q}_N = \begin{bmatrix} 0 & & & & \\ k_1 & 0 & & & \\ k_2 & k_1 & 0 & & \\ \vdots & & & \ddots & \\ k_{N-1} & k_{N-2} & \dots & k_1 & 0 \end{bmatrix}. \tag{5.9}$$

Note that $k_0 = \Omega_1 - \Omega_2$, where

$$\Omega_1 = \begin{cases} \bar{\gamma}^\delta \kappa_{N+1}, & \text{if } \xi = 1, \\ \frac{\bar{\gamma}^\delta \kappa_2}{(1-\xi)^{N-1}} - \sum_{n=0}^{N-2} \frac{\bar{\gamma}^\delta \xi^{1+\delta} \kappa_{n+2}}{(1-\xi)^{N+n-1}}, & \text{otherwise.} \end{cases} \tag{5.10}$$

$$\Omega_2 = \begin{cases} 1 - \frac{\delta \varphi_0(N, \bar{\gamma})}{(N+\delta)\bar{\gamma}^N}, & \text{if } \xi = 1, \\ 1 - \frac{\delta}{(1-\xi)^{N-1}} \frac{\varphi_0(1, \bar{\gamma})}{(1+\delta)\bar{\gamma}} + \sum_{n=0}^{N-2} \frac{\delta \varphi_0(n+1, \xi \bar{\gamma})}{(n+1+\delta)\xi^n (1-\xi)^{N+n-1} \bar{\gamma}^{n+1}}, & \text{otherwise.} \end{cases} \quad (5.11)$$

$$k_i = \begin{cases} \frac{\delta \bar{\gamma}^i}{(i-\delta)} \binom{N+i-1}{N-1} \varphi_i(N, \bar{\gamma}), & \text{if } \xi = 1, \\ \frac{\delta \bar{\gamma}^i}{(i-\delta)} \frac{\varphi_i(1, \bar{\gamma})}{(1-\xi)^{N-1}} - \sum_{n=0}^{N-2} \binom{n+i}{n} \frac{\delta \bar{\gamma}^i}{(i-\delta)} \frac{\xi^{i+1} \varphi_i(n-1, \bar{\gamma})}{(1-\xi)^{N-n-1}}, & \text{otherwise.} \end{cases} \quad (5.12)$$

In addition, $\delta = \frac{2}{\alpha}$, $\kappa_n \triangleq \frac{\Gamma(n-1+\delta)\Gamma(1-\delta)}{\Gamma(n-1)}$, $\varphi_0(a, x) = {}_2F_1(a, a + \delta; a + 1 + \delta; -x^{-1})$, $\varphi_i(a, x) = {}_2F_1(a + i, i - \delta; i - \delta + 1; -x)$.

Proof. Please refer to Appendix C.1. ■

In addition, we provide a lower bound of the connection outage probability with the aid of Alzer's inequality [160], which is given by the following lemma.

Lemma 5.1. *If $X \sim \text{Gamma}(N, 1)$, then the CDF is lower bounded by*

$$F(X < x) \geq (1 - e^{-vx})^N, \quad (5.13)$$

where $v = (N!)^{-\frac{1}{N}}$.

Then we can obtain the following proposition.

Proposition 5.1. *The connection outage probability is lower bounded by*

$$p_{co}^L = \frac{1}{p_a k_0 v^\delta} B\left(\frac{1}{p_a k_0 v^\delta}, N + 1\right). \quad (5.14)$$

Proof. The proof can be readily obtained by using Lemma 5.1. ■

Based on Theorem 5.1, we can obtain the following property.

Property 5.1. *The connection outage probability is a decreasing function w.r.t. the BS density, λ_b .*

Proof. The proof is similar to the case without security issue in [154]. Define

$$\mathbf{A} = \frac{1}{p_a} \left[\left(k_0 + \frac{1}{p_a} \right) \mathbf{I} - \mathbf{Q}_N \right]^{-1}, \quad (5.15)$$

and with the aid of the properties of Toeplitz matrix, we have

$$\frac{\partial p_{co}}{\partial p_a} = -\frac{\partial \|\mathbf{A}\|_1}{\partial p_a} = -\frac{1}{p_a}(\|\mathbf{A}^2\|_1 - \|\mathbf{A}\|_1). \quad (5.16)$$

Since $\|\mathbf{A}^2\|_1 \leq \|\mathbf{A}\|_1^2$, we have

$$\frac{\partial p_{co}}{\partial p_a} \geq -\frac{1}{p_a}(\|\mathbf{A}\|_1^2 - \|\mathbf{A}\|_1) = \frac{p_{co}}{p_a} \|\mathbf{A}\|_1 \geq 0. \quad (5.17)$$

Combining with (5.1), we have $\frac{\partial p_{co}}{\partial \lambda_b} \leq 0$. ■

Property 5.1 implies that for the general AN-aided transmission scheme, deploying more BSs will improve the transmission reliability. This is because although increasing λ_b will increase both the signal power and interference power, the average received aggregate interference can be shown to scale with the BS density as $(\lambda_b p_a)^{\frac{\alpha}{2}}$. For a fixed user density, p_a will decrease with λ_b . However, since each user associates to the nearest BS, the average received signal power scales as $(\lambda_b)^{\frac{\alpha}{2}}$. Thus, the signal power increases faster than the interference power and the connection outage probability will be decreased by increasing the BS density.

From Theorem 5.1, we know that k_0 and k_i are complex functions of N and ϕ , which impedes the performance analysis. To show the impact of power allocation and number of transmit antennas on the connection outage performance, we derive the asymptotic expression of p_{co} . When the number of antennas at each BS approaches infinity, we have the following lemma.

Lemma 5.2. $\lim_{N \rightarrow \infty} \|\mathbf{h}_{0,0}^T \mathbf{w}_0\|^2 = N$, and $\lim_{N \rightarrow \infty} \|\mathbf{h}_{i,0}^T \mathbf{G}_i\|^2 = N - 1$.

Proof. Since $\|\mathbf{h}_{0,0}^T \mathbf{w}_0\|^2 \sim \text{Gamma}(N, 1)$, $\|\mathbf{h}_{i,0}^T \mathbf{G}_i\|^2 \sim \text{Gamma}(N - 1, 1)$, Lemma 5.2 can be easily obtained. ■

Then we have the following proposition.

Proposition 5.2. *The asymptotic connection outage probability with AN is given*

by

$$p_{co}^\infty = \int_0^\infty \frac{1}{2} \left[1 - \operatorname{erf} \left(\frac{\ln(\frac{\phi PN}{\bar{\gamma} r_{0,0}^\alpha}) - \mu}{\sqrt{2}\sigma} \right) \right] f_{r_{0,0}}(r) dr, \quad (5.18)$$

where

$$\begin{cases} \mu = \ln \mu_I - \frac{1}{2}\sigma^2, \\ \sigma^2 = \ln \left(1 + \frac{\sigma_I^2}{\mu_I^2} \right), \end{cases} \quad (5.19)$$

and

$$\begin{cases} \mu_I = \frac{2\pi\lambda_b p_a P}{(\alpha-2)r_{0,0}^{\alpha-2}}, \\ \sigma_I^2 = \frac{2\pi\lambda_b p_a \phi^2 P^2}{(\alpha-1)r_{0,0}^{2(\alpha-1)}}. \end{cases} \quad (5.20)$$

Proof. Please refer to Appendix C.2. ■

Based on Proposition 5.2, the impact of N and ϕ on the connection outage probability can be deduced by the following property.

Property 5.2. *The connection outage probability is a decreasing function w.r.t. N and ϕ .*

Proof. From (5.19), we know that

$$\frac{\sigma_I^2}{\mu_I^2} = \frac{(\alpha-2)^2 \phi^2}{2\pi\lambda_b p_a (\alpha-1)r_{0,0}^2}. \quad (5.21)$$

Denote $f = \frac{\ln(\frac{\phi PN}{\bar{\gamma} r_{0,0}^\alpha}) - \mu}{\sigma}$, then

$$f = \frac{\ln \left(\frac{PN \sqrt{2\pi\lambda_b p_a (\alpha-1)r_{0,0}^2}}{\bar{\gamma} r_{0,0}^\alpha (\alpha-2)} \sqrt{e^{\sigma^2} - 1} \right) - \mu}{\sigma}. \quad (5.22)$$

We can prove that $\frac{\partial f}{\partial \sigma} > 0$, hence, we have

$$\frac{\partial f}{\partial \phi} = \frac{\partial f}{\partial \sigma} \frac{\partial \sigma}{\partial \phi} > 0. \quad (5.23)$$

Since the error function is a monotonic increasing function, we can conclude that

p_{co} decreases with ϕ . ■

Property 5.2 can be explained as follows. Since each BS uses a fixed power transmission scheme, the average received aggregate interference is independent of ϕ and N . However, by increasing ϕ or N , the received signal power will be enhanced, thus p_{co} will be decreased. Property 5.2 can also be proved using the lower bound, which is given as follows.

Proof. By using the binomial expansion, we have

$$p_{co}^L = 1 + \sum_{n=1}^N \binom{N}{n} \frac{(-1)^n}{1 + np_a k_0 v^\delta}. \quad (5.24)$$

By taking the first-order derivative w.r.t. k_0 , we have

$$\frac{\partial p_{co}^L}{\partial k_0} = \sum_{n=1}^N \binom{N}{n} \frac{(-1)^n}{1 + np_a k_0 v^\delta} \frac{-np_a v^\delta}{1 + np_a k_0 v^\delta}. \quad (5.25)$$

Since $p_{co}^L \leq 1$, we have $\frac{\partial p_{co}^L}{\partial k_0} \geq 0$. When N approaches infinity, $\|\mathbf{h}_{i,0}^T \mathbf{G}_i\|^2 = N - 1$, X_i in Appendix C.1 becomes $X_i = \phi P |\mathbf{h}_{i,0}^T \mathbf{w}_i|^2 + (1 - \phi)P$ and χ becomes $\chi = \frac{\beta}{1 + \phi P_s}$, where $\beta = e^{\frac{1-\phi}{\phi}}$. Following that, we can derive k_0 as

$$k_0 = \beta \bar{\gamma}^\delta \kappa_2 + \beta \frac{\delta}{1 + \delta} \frac{\varphi_0(1, \bar{\gamma})}{\bar{\gamma}} + \tau_j. \quad (5.26)$$

Thus $\frac{\partial k_0}{\partial \phi} < 0$, $\frac{\partial p_{co}^L}{\partial \phi} \leq 0$ will always hold, this completes the proof. ■

5.3.2 Secrecy Outage Probability

The secrecy outage probability is given by

$$\begin{aligned} p_{so} &= \mathbb{P}(\gamma_E > \bar{\gamma}_e) = 1 - \mathbb{P}\left(\max_{e_l \in \Phi_e} \gamma_{e_l} < \bar{\gamma}_e\right) \\ &= 1 - \mathbb{E}_{\Phi_e} \left[\prod_{e_l \in \Phi_e} \mathbb{P}(\gamma_{e_l} < \bar{\gamma}_e) \right], \end{aligned} \quad (5.27)$$

where $\bar{\gamma}_e = 2^{R_t - R_s} - 1$. In this subsection, a closed-form expression of the SOP is derived and asymptotic analysis is also conducted to analyze the impact of different parameters.

Theorem 5.2. *The secrecy outage probability with AN is given by*

$$p_{so} = 1 - \exp \left(-\frac{\pi \lambda_e}{\Theta} (1 + \bar{\gamma}_e \xi)^{1-N} \right), \quad (5.28)$$

where $\Theta = \pi \lambda_b p_a \bar{\gamma}_e^\delta \varpi$ and

$$\varpi = \begin{cases} \kappa_{N+1}, & \text{if } \xi = 1, \\ \frac{\kappa_2}{(1-\xi)^{N-1}} - \sum_{n=0}^{N-2} \frac{\xi^{1+\delta} \kappa_{n+2}}{(1-\xi)^{N-n-1}}, & \text{otherwise.} \end{cases} \quad (5.29)$$

Proof. Please refer to Appendix C.3. ■

From Theorem 5.2, we know that the BS density only affects Θ . It can be proven that Θ increases with an increase of λ_b . Then we can obtain the following property.

Property 5.3. *The secrecy outage probability is a decreasing function w.r.t. the BS density λ_b and it converges to a constant value when λ_b is large enough.*

This property implies that deploying more BSs will improve the secrecy performance. This is because although the aggregate interference received at each Eve can be shown to scale with the BS density as $(\lambda_b p_a)^{\frac{\alpha}{2}}$, the maximal eavesdropped signal power scales strictly less than $(\lambda_b p_a)^{\frac{\alpha}{2}}$ since the positions of Eves follow a PPP. Thus, the secrecy outage probability will be decreased by increasing the BS density. Note that when the BS density is large enough, $\lambda_b p_a$ will approach λ_u and p_{so} will converge to

$$\bar{p}_{so} = 1 - \exp \left(-\frac{\pi \lambda_e}{\bar{\Theta}} (1 + \bar{\gamma}_e \xi)^{1-N} \right), \quad (5.30)$$

where $\bar{\Theta} = \pi \lambda_u \bar{\gamma}_e^\delta \varpi$. Therefore, further increasing λ_b will not improve the secrecy

outage performance.

To evaluate the effect of ϕ and N on the secrecy outage performance, we first study the asymptotic expression of p_{so} in a large-system case, i.e., when the BSs are equipped with a large number of antennas.

Proposition 5.3. *The asymptotic secrecy outage probability with AN is given as*

$$p_{so}^{\infty} = 1 - \exp\left(-\frac{\pi\lambda_e}{\Theta^{\infty}}e^{-(\phi^{-1}-1)\bar{\gamma}_e}\right), \quad (5.31)$$

where $\Theta^{\infty} = \pi\lambda_b p_a \bar{\gamma}_e^{\delta} \Gamma(1-\delta)\Gamma(1+\delta, \phi^{-1}-1)e^{\phi^{-1}-1}$.

Proof. Please refer to Appendix C.4. ■

With the aid of Proposition 5.3, we can obtain the following property.

Property 5.4. *The secrecy outage probability is an increasing function w.r.t. ϕ and it is independent of N .*

The reason is similar to the case for connection outage performance. Since each BS uses a fixed power transmission scheme, the average received aggregate interference is independent of ϕ and the Eve's signal power increases with ϕ . Hence, by increasing ϕ , p_{so} will be decreased. Since the eavesdropping channel is independent with the main channel and the average aggregate interference to Eve is also independent with N , thus the secrecy outage probability is independent of N .

5.4 Secrecy Area Spectral Efficiency Analysis

5.4.1 Fixed-Rate Transmission

When each BS adopts Wyner's encoding scheme and uses fixed code rate transmission, the SASE, defined as the average number of successfully transmitted secrecy

bits per second per Hz in a unit area, can be expressed as [154, 161]

$$T = \lambda_b p_a (1 - p_{co}) R_s. \quad (5.32)$$

Our goal is to optimize the power allocation factor to maximize the SASE subject to the secrecy outage constraint, which can be formulated as

$$\max_{\phi} T \quad s.t. \quad p_{so} \leq \epsilon. \quad (5.33)$$

With the properties obtained in Section 5.3, we observe that SASE is an increasing function of ϕ and the optimal value of ϕ is determined by the secrecy outage constraint. From Property 5.4, we know that p_{so} monotonically increases with ϕ , and thus the optimal value of ϕ can be obtained through bisection search method.

Using the asymptotic expression of p_{so} , we can obtain the following corollary.

Corollary 5.1. *It is unnecessary to inject AN if the following condition is satisfied:*

$$\frac{\lambda_e}{\lambda_b p_a \tilde{\gamma}_e^\delta} \leq -\kappa_2 \ln(1 - \epsilon). \quad (5.34)$$

Proof. Since p_{so} and the objective function are monotonic increasing functions w.r.t. ϕ , the optimal value of ϕ will be 1 if the worst-case secrecy outage satisfies the constraint. By substituting $\phi = 1$ into the constraint, we can obtain (5.34). ■

Corollary 5.1 infers that under some conditions, the BS should transmit useful signal with full power without injecting AN. This phenomenon is very straightforward, since the inter-cell interference can be used as a source of jamming to confound the Eves. This provides very useful insight for practical system designs.

5.4.2 Adaptive-Rate Transmission

For systems with adaptive-rate transmission schemes, the BS can adaptively adjust the encoder rate based on the instantaneous CSI of the legitimate channels. Thus

the connection outage can be avoided. In this case, the average data rate is a more practical performance metric. Note that the average achievable secrecy rate of a typical user and the SASE can be expressed as

$$R = \mathbb{E} \left[\{R_u - R_e\}^+ \right], \quad (5.35)$$

and

$$T = \lambda_b p_a R, \quad (5.36)$$

respectively, where $R_u = \log(1 + \gamma_{u_0})$ and $R_e = \log(1 + \gamma_E)$. With the aid of the lemma in [162], we have the following theorem.

Theorem 5.3. *The average secrecy rate of a typical user is lower bounded by*

$$R_L = \int_0^\infty \frac{1}{\ln 2} \frac{1 - (1+z)^{-N}}{z(1+p_a \Xi)} dz - \int_0^\infty \frac{1 - F(z)}{\ln 2(1+z)} dz, \quad (5.37)$$

where

$$\Xi = \begin{cases} \frac{1}{(1+z)^N} + z^\delta N \psi\left(\frac{z}{1+z}; N\right) - 1, & \text{if } \xi = 1, \\ \frac{1}{(1+z)(1+\xi z)^{N-1}} + \frac{z^\delta \psi\left(\frac{z}{1+z}; 1\right)}{(1-\xi)^{N-1}} - \sum_{n=0}^{N-2} \frac{(n+1)z^\delta \xi^{1+\delta}}{(1-\xi)^{N-n-1}} \psi\left(\frac{\xi z}{1+\xi z}; n+1\right) - 1, & \text{otherwise.} \end{cases} \quad (5.38)$$

and

$$F(z) = \exp \left(- \frac{\lambda_e e^{-(\frac{1}{\phi}-1)(z+1)}}{\lambda_b p_a \Gamma(1-\delta) \Gamma\left(1+\delta, \frac{1}{\phi}-1\right) z^\delta} \right). \quad (5.39)$$

Note that $\psi(x; n) = B_x(1-\delta, n+\delta)$.

Proof. Please refer to Appendix C.5. ■

Notice that even though (5.37) is not in closed form, it is very efficient to calculate. Based on Theorem 5.3, we have the following corollary.

Corollary 5.2. *R_L is a quasi-concave function w.r.t. the power allocation ϕ and is a monotonic decreasing function w.r.t. the ratio of the Eve-BS density, $\frac{\lambda_e}{\lambda_b}$.*

Proof. When $\xi \neq 1$, from (C.29) in Appendix C.5, we have

$$\vartheta = 1 - \frac{(1 + \xi u^{-\frac{\alpha}{2}})^{1-N}}{1 + u^{-\frac{\alpha}{2}}}. \quad (5.40)$$

From [150], we know that $(1 + \xi u^{-\frac{\alpha}{2}})^{1-N}$ is Schur-convex w.r.t. ξ , thus Ξ is concave (convex) w.r.t. ξ (ϕ), i.e., the first integration in (5.37) is a concave function of ϕ . We can also prove that the second integration in (5.37) is a quasi-convex function of ϕ , since p_{so} is a quasi-convex function of ϕ as shown in Fig. 5.6. Hence, R_L is a quasi-concave function of ϕ . From (5.39), we know that $F(x)$ is a monotonic decreasing function of $\frac{\lambda_e}{\lambda_b}$, and all the other variables are independent of $\frac{\lambda_e}{\lambda_b}$. Hence we can conclude that R_L is a monotonic decreasing function of $\frac{\lambda_e}{\lambda_b}$. ■

With the aid of Corollary 5.2, we can conclude that, for the adaptive-rate transmission scheme, the optimal ϕ that maximizes the SASE can be obtained through a numerical search, which lies either on the critical point or the boundary. Due to the complex form of Ξ and the integration, the closed-form expression of ϕ is mathematically intractable, and we only present some numerical results.

5.5 Extension to Dense Network

In the last two sections, we have analyzed the outage and secrecy rate performance of the small-cell network in a low cell-load case, where each BS serves up to one user in a time slot. In this section, we extend to a high cell-load case with multi-user transmission and investigate the achievable sum secrecy rate.

When the cell load is very high, each BS will always have users to serve, then the probability of a BS being active will converge to 1. In addition, to improve the sum secrecy throughput, we assume that each BS can support K users simultaneously through ZFBF, where $K \leq N$. For simplicity, we consider that the total transmit power of each BS is P , and a fraction of the total power, ϕP , is equally allocated among the K users. Denote $\mathbf{h}_{i,j}^{(k)}$ as the channel from the i th BS to the k th user in the j th cell, and the corresponding beamforming vector

is given by $\mathbf{w}_{i,i}^{(k)}$. Then $\mathbf{w}_{i,i}^{(k)}$ equals to the k th normalized column of $\mathbf{H}_i(\mathbf{H}_i^H \mathbf{H}_i)^\dagger$, where $\mathbf{H}_i = [\mathbf{h}_{i,i}^{(0)}, \mathbf{h}_{i,i}^{(1)}, \dots, \mathbf{h}_{i,i}^{(K-1)}]$ [157]. Following that, the SIR at the typical user becomes

$$\tilde{\gamma}_{u_0} = \frac{\frac{\phi P}{K} \left| \mathbf{h}_{0,0}^{(0)T} \mathbf{w}_{0,0}^{(0)} \right|^2 (r_{0,0}^{(0)})^{-\alpha}}{\tilde{I}_B}, \quad (5.41)$$

where the interference term is given by

$$\tilde{I}_B = \sum_{i \in \Phi_b^a \setminus \{0\}} \phi P \left[\sum_{k=0}^{K-1} \frac{\left| \mathbf{h}_{i,0}^{(0)T} \mathbf{w}_{i,i}^{(k)} \right|^2}{K} + \zeta \left\| \mathbf{h}_{i,0}^{(0)T} \mathbf{V}_i \right\|^2 \right] (r_{i,0}^{(0)})^{-\alpha}. \quad (5.42)$$

Note that when $K \neq N$, $\zeta = \frac{\phi^{-1}-1}{N-K}$, else $\zeta = 0$. $\mathbf{V}_i$ denotes the null space of $\mathbf{H}_i$.

Similarly, the received SIR at the k th Eve can be expressed as

$$\tilde{\gamma}_{e_l} = \frac{\frac{\phi P}{K} \left| \mathbf{g}_{0,e_l}^T \mathbf{w}_{0,0}^{(0)} \right|^2 r_{0,e_l}^{-\alpha}}{\phi P \left(\sum_{k=1}^{K-1} \frac{\left| \mathbf{g}_{0,e_l}^T \mathbf{w}_{0,0}^{(k)} \right|^2}{K} + \zeta \left\| \mathbf{g}_{0,e_l}^T \mathbf{V}_0 \right\|^2 \right) r_{0,e_l}^{-\alpha} + \tilde{I}_{B,e_l}}, \quad (5.43)$$

where the interference is given by

$$\tilde{I}_{B,e_l} = \sum_{i \in \Phi_b^a \setminus \{0\}} \phi P \left[\sum_{k=0}^{K-1} \frac{\left| \mathbf{g}_{i,e_l}^T \mathbf{w}_{i,i}^{(k)} \right|^2}{K} + \zeta \left\| \mathbf{g}_{i,e_l}^T \mathbf{V}_i \right\|^2 \right] r_{i,e_l}^{-\alpha}. \quad (5.44)$$

Based on the above assumptions, we have $\left| \mathbf{h}_{0,0}^{(0)T} \mathbf{w}_{0,0}^{(0)} \right|^2 \sim \text{Gamma}(M, 1)$, where $M = N - K + 1$, $\sum_{k=0}^{K-1} \left| \mathbf{h}_{i,0}^{(0)T} \mathbf{w}_{i,i}^{(k)} \right|^2 \sim \text{Gamma}(K, 1)$, and $\left\| \mathbf{h}_{i,0}^{(0)T} \mathbf{V}_i \right\|^2 \sim \text{Gamma}(N - K, 1)$. Similar to the low cell-load case, we can derive the following theorem.

Theorem 5.4. *The average secrecy rate of a typical user with ZFBF is lower bounded by*

$$R_L^{MU} = \int_0^\infty \frac{\left(1 - \left(1 + \frac{z}{K}\right)^{-M}\right)}{\ln 2 \tilde{\Xi} z} dz - \int_0^\infty \frac{1 - \tilde{F}(z)}{\ln 2(1+z)} dz, \quad (5.45)$$

where

$$\tilde{F}(z) = \exp \left(-\frac{\lambda_e \phi^\delta e^{(1-\frac{K}{\phi})z}}{\lambda_b p_a \Gamma(1-\delta)(Kz)^\delta} \right), \quad (5.46)$$

and

$$\tilde{\Xi} = \begin{cases} C_1 : \frac{N^N}{(N+z)^N} + z^\delta N^{1-\delta} \psi \left(\frac{z}{N+z}; N \right), \\ C_2 : \widehat{\sum}_0 K^N \Gamma(N) \left[\frac{1}{(K+z)^N} + \frac{z^\delta N}{K^{(N+\delta)}} \psi \left(\frac{z}{K+z}; N \right) \right], \\ C_3 : \widehat{\sum}_1 \left[\frac{1}{(K+z)^{\tilde{m}}} + \frac{z^\delta \tilde{m}}{K^{\tilde{m}+\delta}} \psi \left(\frac{z}{K+z}; \tilde{m} \right) \right] - \widehat{\sum}_2 \left[\frac{1}{(1+\zeta z)^{\tilde{n}}} + z^\delta \tilde{n} \zeta^\delta \psi \left(\frac{\xi z}{1+\xi z}; \tilde{n} \right) \right]. \end{cases} \quad (5.47)$$

Note that C_1 denotes the condition $N = K$, C_2 and C_3 correspond to the conditions when $K \neq N$ with $K\zeta = 1$ and $K\zeta \neq 1$, respectively, and

$$\begin{cases} \widehat{\sum}_0 = \sum_{m=0}^{K-1} \binom{K-1}{m} \frac{(-1)^m}{\tilde{N} \Gamma(K) \Gamma(N-K)}, \\ \widehat{\sum}_1 = \sum_{m=0}^{K-1} \binom{K-1}{m} \frac{(-1)^m \zeta^m K^K \Gamma(\tilde{N})}{\Gamma(K) \Gamma(N-K) (1-K\zeta)^{\tilde{N}}} \Gamma(\tilde{m}), \\ \widehat{\sum}_2 = \sum_{m=0}^{K-1} \binom{K-1}{m} \frac{(-1)^m \zeta^m K^K \Gamma(\tilde{N})}{\Gamma(K) \Gamma(N-K) (1-K\zeta)^{\tilde{N}}} \sum_{n=0}^{\tilde{N}-1} \frac{(1-K\zeta)^n \zeta^{\tilde{m}} \Gamma(\tilde{n})}{n!}. \end{cases} \quad (5.48)$$

Proof. The proof is similar to the proof of Theorem 5.3 and is omitted here. $\blacksquare$

Following that, the SASE maximization problem can be formulated as

$$\begin{aligned} \max_{\phi, K} \quad & T_L^{MU} = \lambda_b K R_L^{MU} \\ \text{s.t.} \quad & 0 < \phi \leq 1, 1 \leq K \leq N. \end{aligned} \quad (5.49)$$

The closed-form solutions of ϕ and K are mathematically intractable. However, since the average received aggregate interference from other BSs is independent of K , from (5.41) and (5.43), we can observe that the SIR of the typical user and Eve scale as $(N-K+1)/K$ and $1/K$, respectively. Thus, we can prove that R_L^{MU} monotonically decreases with K . For a medium-to-large value of N , the SASE will first increase and then decrease with the increase of K . Hence, the optimal number of users can be found through some numerical searching methods.

5.6 Impact of Adaptive Eves

Compared to the instantaneous small-scale channel fading effects, the path loss is a more stable and dominant channel impairment factor in the considered scenario [163]. Hence, when multiple Eves are randomly distributed in the network, the eavesdropping capacity will be determined by the one with the nearest distance to the corresponding BS. In this section, we will investigate the impact of adaptive Eves with jamming and eavesdropping capability on the secrecy performance. Specifically, we assume that each Eve can adaptively act as a passive Eve or an active jammer based on their positions. The set of nearest Eves to the active BSs is called passive Eves, denoted as Φ_E , with an effective intensity being equal to the intensity of the active BSs, i.e., $\lambda_E = \lambda_b p_a$. The remaining Eve nodes can then act as active jammers to transmit some jamming signals to further degrade the reception of the legitimate users¹. Note that the jamming signal not only degrades the legitimate users but also interferes with the Eves. To mitigate the effect of jamming to the Eves, we assume that each Eve has a guard zone and those jammers fall into this region will be prohibited from transmitting. The size of the guard zone area is determined by the BS-Eve distance, i.e., $R = \mu R_0$, where R_0 denotes the distance from Eve to the nearest active BS and μ is a constant and identical for every Eve, as shown in Fig. 5.2. Therefore, the set of active jammers can be considered as a Poisson hole process with primary intensity $\lambda_b p_a$ and secondary intensity $\lambda_e - \lambda_b p_a$. Consequently, the intensity of the Poisson hole process can be approximated by [107]

$$\lambda_j \approx (\lambda_e - \lambda_b p_a) \exp(-\pi \lambda_b p_a \mu \bar{R}^2), \quad (5.50)$$

where $\bar{R} = 1/(2\sqrt{\lambda_e})$ is the mean value of R . To facilitate the theoretical analysis, the Poisson hole process can be approximated by a PPP with intensity of λ_j .

In practice, all the Eves may first estimate their distances to the active BSs

¹For the rest of this chapter, we will refer the “passive eavesdropper” as “eavesdropper” and the “active jammer” as “jammer” for simplicity.

Figure 5.2: A multi-cell cellular network model, where each Eve can act as either a passive Eve or an active jammer.

by using the GPS devices, and then broadcast this information to other Eves. Denote the distance between the m th Eve and the n th BS as d_{nm} , after the m th Eve receives all the distance information, it can make the eavesdropping or jamming decision by comparing the distance. Thus the eavesdropper set can be determined in a distributed manner. After that, each passive Eve sends a signal with a constant power² and those jammers who receive this signal is prohibited from transmitting jamming signal.

Remark 5.1. Our work can be extended to the case with cooperative transmission among jammers to mitigate the interference to the Eves when the guard zone does not exist. To reduce the overhead and facilitate the analysis, we only consider the uncoordinated transmission scheme.

Remark 5.2. We assume that the Eves are unselfish, i.e., when they are far from the BS, they are willing to act as jammers. Since the positions of Eves follow a PPP, each Eve has an equal probability to act as jammer. Even though the maximal eavesdropping rate may be degraded by the jamming interference, the

²The transmit power is determined by the size of the guard zone.

jamming action is beneficial to the Eves as long as the jamming is much more severe to the legitimate users.

5.6.1 Outage Probability Analysis

With adaptive eavesdropping, the received SIR at the typical user in (5.3) becomes

$$\gamma_{u_0} = \frac{\phi P |\mathbf{h}_{0,0}^T \mathbf{w}_0|^2 r_{0,0}^{-\alpha}}{I_B + I_J}, \quad (5.51)$$

where

$$I_J = \sum_{j \in \Phi_j} P_j |f_{j,0}|^2 r_{j,0}^{-\alpha}. \quad (5.52)$$

Note that $f_{j,0} \sim \mathcal{CN}(0, 1)$ denotes the interfering channel fading vector from the j th jammer to the typical user. Similarly, the received SIR at the l th Eve becomes

$$\gamma_{e_l} = \frac{\phi P |\mathbf{g}_{0,e_l}^T \mathbf{w}_0|^2 r_{0,e_l}^{-\alpha}}{\xi \phi P \|\mathbf{g}_{0,e_l}^T \mathbf{G}_0\|^2 r_{0,e_l}^{-\alpha} + I_{B,e_l} + I_{J,e_l}}, \quad (5.53)$$

where

$$I_{J,e_l} = \sum_{j \in \Phi_j} P_j |g_{j,e_l}|^2 r_{j,e_l}^{-\alpha}. \quad (5.54)$$

Following similar procedure in Section 5.3.1, we can obtain the following theorem.

Theorem 5.5. *The connection outage probability with adaptive eavesdropping is given by*

$$p_{co}^A = 1 - \left\| \left((1 + p_a k_0^A) \mathbf{I} - p_a \mathbf{Q}_N^A \right)^{-1} \right\|_1, \quad (5.55)$$

where $k_0^A = k_0 + \Omega_0$, $k_i^A = k_i + \Omega_J$, $\eta = \frac{P_j}{\phi P}$, and

$$\begin{cases} \Omega_0 = \frac{\lambda_j \kappa_2}{\lambda_b p_a} (\eta \bar{\gamma})^\delta, \\ \Omega_J = \frac{\lambda_j \delta}{\lambda_b p_a} (\eta \bar{\gamma})^\delta B(i - \delta, 1 + \delta). \end{cases} \quad (5.56)$$

Proof. The Laplace transform of I_J can be expressed as

$$\mathcal{L}_{I_J}(s) = \exp \left(-2\pi\lambda_j \int_0^\infty \left(1 - \frac{1}{1 + sP_j r^{-\alpha}} \right) r dr \right). \quad (5.57)$$

Hence, we have

$$\mathcal{L}_I(s) = \exp \left(-2\pi\lambda_b p_a \left[\int_{r_{0,0}}^\infty (1 - \chi) r dr + \frac{\lambda_j}{\lambda_b p_a} \int_0^\infty \left(1 - \frac{1}{1 + sP_j r^{-\alpha}} \right) r dr \right] \right). \quad (5.58)$$

Similar to the proof in Appendix C.1, we can obtain Theorem 5.5. $\blacksquare$

For the adaptive eavesdropping scheme, due to the adaptive eavesdropping, the positions of the effective Eves do not follow the PPP and thus the exact SOP is difficult to be obtained if not impossible. In the following, we give a lower bound.

Theorem 5.6. *The secrecy outage probability for the adaptive eavesdropping scheme is lower bounded by*

$$p_{so}^A \geq \frac{\lambda_e}{\lambda_e + \Theta + \Theta_J} (1 + \bar{\gamma}_e \xi)^{1-N}, \quad (5.59)$$

where

$$\Theta_J = \lambda_j \left(\kappa_2 (\eta \bar{\gamma}_e)^\delta - \mu^2 + \frac{\delta}{1 + \delta} \frac{\mu^{2+\alpha}}{\eta \bar{\gamma}_e} \varphi_0(1, \eta \bar{\gamma}_e \mu^\alpha) \right). \quad (5.60)$$

Proof. Similar to the proof in Appendix C.3, the SOP is given by

$$p_{so} = \mathbb{P}(\gamma_E > \bar{\gamma}_e) = 1 - \mathbb{E}_{\Phi_b} \left[\mathbb{E}_{\Phi_e} \left[\prod_{e_l \in \Phi_e} \mathbb{P}(\gamma_{e_l} < \bar{\gamma}_e \mid \Phi_b) \right] \right] \quad (5.61)$$

and

$$\mathbb{P}(\gamma_{e_l} < \bar{\gamma}_e) = 1 - (1 + \bar{\gamma}_e \xi)^{1-N} \mathcal{L}_{I_{e_l}} \left(\frac{\bar{\gamma}_e r_{0,e_l}^\alpha}{\phi P} \right), \quad (5.62)$$

where

$$\mathcal{L}_{I_{J,e_l}}(s) = \exp \left(-2\pi\lambda_j \int_{\mu r_{0,e_l}}^{\infty} \left(1 - \frac{1}{1 + sP_j r^{-\alpha}} \right) r dr \right). \quad (5.63)$$

Since the maximal eavesdropping capacity is usually determined by the nearest Eve, then we have

$$p_{so}^A \geq \mathbb{E}_{r_{0,e_l}} [\mathbb{P}(\gamma_{e_l} > \bar{\gamma}_e)] = \int_0^{\infty} f_{r_{0,e_l}}(r) e^{-(\Theta_b + \Theta_j)r^2} dr, \quad (5.64)$$

where $f_{r_{0,e_l}}(r)$ is the PDF of the distance from the Eves to the nearest active BSs, and is given by

$$f_{r_{0,e_l}}(r) = 2\pi\lambda_e r e^{-\pi\lambda_e r^2}. \quad (5.65)$$

Combining the above results, we can obtain Theorem 5.6. This completes the proof. ■

By using the lower bound in Proposition 5.1, we can obtain the following property.

Property 5.5. *The connection outage probability is a decreasing function of μ , and the secrecy outage probability is an increasing function of μ .*

Property 5.5 implies that the transmission reliability will be improved by increasing the radius of Eve's guard zone μ . This is because increasing μ will decrease the intensity of jammers, and thus the received average aggregate jamming power will be decreased. While the SOP will be decreased due to the increased interference as well as the reduced Eves, when some of the Eves act as jammers. Hence, the Eves should be scheduled carefully to maximize its own benefit. From the perspective of the Eves, the secure transmission probability should not be increased by changing the roles, i.e., $p_{st}^A < p_{st}$, which can be regarded as a strong guaranteed criterion for the Eves. Due to the complicated forms of the outage probabilities, the exact expression of the feasible region is difficult to be obtained, and only approximated results are presented in this section.

Proposition 5.4. *When $\Theta_j \ll \Theta_b$, the feasible region for adaptive eavesdropping is constrained by*

$$\mathcal{F}_s = \left\{ (\lambda_e, P_j) : \frac{\lambda_e}{\Theta_b(1-\xi)^{N-1}} < -W_m(-\theta e^{-1}) - 1 \right\}, \quad (5.66)$$

where $\theta = \frac{1-p_{co}^A}{1-p_{co}} \leq 1$.

Proof. Please refer to Appendix C.6. ■

Corollary 5.3. *When $N = 1$, the feasible region becomes*

$$\mathcal{F}_s = \left\{ (\lambda_e, P_j) : \frac{\lambda_e}{\lambda_b p_a \kappa_2 \bar{\gamma}_e^\delta} < -W_m \left(\frac{-e^{-1} \lambda_b p_a}{\lambda_b p_a + \lambda_j \eta^\delta} \right) - 1 \right\}. \quad (5.67)$$

Proof. When $N = 1$, there is no extra degree of freedom for AN, i.e., $\phi = 1$. By substituting the results in the previous section, we can obtain (5.67). ■

With the aid of the derived feasible region, the Eves can determine the optimal eavesdropping strategy for fixed parameters. Since both the BS and Eves may adaptively adjust their parameters to maximize their own performance, the optimal parameters for both sides need to be optimized, which will be discussed in the next section.

5.6.2 Stackelberg Game Formulation

In this subsection, the interactions between the BSs and Eves are formulated under the framework of a Stackelberg game, and the optimal power allocations, secrecy rate of the BSs, and the radius of the guard zone are derived by analyzing the equilibrium of the game.

Stackelberg game is a strategic game that consists of a leader and several followers competing with each other for certain resources. Since each BS wants to maximize its secrecy rate, and the Eves want to minimize the secure transmission probability (or equivalently maximize the wiretap rate) by adaptively changing its jamming strategy, hence, Stackelberg game model is applied in this scenario,

where we formulate the Eve as the leader and the BS as the follower. The Eve first imposes an eavesdropping strategy by elaborately setting a guard zone to enlarge the eavesdropping, then the BS updates its power allocation and secrecy code rate to maximize its individual utility based on the eavesdropping strategy. Based on this model, the revenue functions of the BS and the Eves are $U_B(\mu, \phi, R_s) = T$ and $U_E(\mu, \phi, R_s) = 1 - p_{st}$, respectively. For the BSs, the problem can be formulated as

$$\begin{aligned} \max_{R_s, \phi} \quad & (1 - p_{co})R_s \\ \text{s.t.} \quad & p_{so} \leq \epsilon. \end{aligned} \tag{5.68}$$

For the Eve, the problem can be formulated as

$$\begin{aligned} \max_{\mu} \quad & 1 - (1 - p_{co})(1 - p_{so}) \\ \text{s.t.} \quad & \lambda_j P_j \leq \mathcal{I}. \end{aligned} \tag{5.69}$$

where $\mathcal{I}$ is the average jamming power constraint guaranteeing that the jammers cannot be detected by the legitimate users. To avoid being detected by the users and to reduce the jamming interference to other Eves, each Eve must adaptively change the guard zone and the jamming power. Note that to facilitate the analysis, P_j is fixed in this section.

Stackelberg Equilibrium

The Stackelberg equilibrium of a Stackelberg game is defined as a set of solutions at which none of the game players, i.e., the BS or Eves, can further improve its utility by changing only its own strategy. Therefore, the Stackelberg equilibrium of the Stackelberg game formed by (5.68) and (5.69) can be defined as follows

$$U_B(\mu^*, \phi^*, R_s^*) \geq U_B(\mu^*, \phi, R_s), \tag{5.70}$$

$$U_E(\mu^*, \phi^*, R_s^*) \geq U_E(\mu, \phi^*, R_s^*). \tag{5.71}$$

For the proposed game, the equilibrium can be obtained as follows: For a given

μ , problem (5.68) is solved first. Then, with the obtained best response functions $\phi^*(\mu)$ and $R_s^*(\mu)$, we solve (5.69) for the optimal μ . Due to the complicated forms of the outage probability, explicit expressions of $\phi^*(\mu)$ and $R_s^*(\mu)$ are hard to obtain, and thus we solve it through an iterative algorithm.

Stackelberg Equilibrium Solution

Now we solve the follower's problem first. The follower's problem (5.68) can be decomposed into two steps: maximize $1 - p_{co}$ over variable ϕ , and then maximize over the remaining variable R_s . In the following, we optimize (5.68) step by step.

Step 1: Given R_s , (5.68) can be rewritten as

$$\min_{\phi} p_{co} \quad s.t. \quad p_{so} \leq \epsilon. \quad (5.72)$$

Since p_{co} monotonically decreases w.r.t. ϕ and p_{so} increases w.r.t. ϕ , the optimal value of ϕ to minimize (5.72) is achieved when equality holds, i.e., $p_{so} = \epsilon$.

Step 2: Denote the optimal value in step 1 as $\phi^*(R_s)$, and substitute it into the connection outage expression, we have

$$\max_{R_s} T(R_s) = (1 - p_{co}^*(R_s))R_s. \quad (5.73)$$

Then we have the following proposition.

Proposition 5.5. *The secrecy throughput $T(R_s)$ is a quasi-concave function of R_s , and the optimal value R_s^* can be obtained numerically.*

Proof. Take the first derivative of $T(R_s)$ w.r.t. R_s , we have

$$T'(R_s) = \frac{\partial T}{\partial R_s} = 1 - p_{co}^*(R_s) - R_s \frac{\partial p_{co}^*(R_s)}{\partial R_s}, \quad (5.74)$$

where

$$\frac{\partial p_{co}^*(R_s)}{\partial R_s} = \frac{\partial p_{co}^*(R_s)}{\partial \phi} \frac{\partial \phi}{\partial R_s}. \quad (5.75)$$

Let $p_{so} = 1 - f(\bar{\gamma}_e) = 1 - f(2^{R_t - R_s} - 1)$, from (5.59), we have

$$1 - f(2^{R_t - R_s} - 1) = \epsilon \Leftrightarrow R_t - R_s = \log_2(1 + f^{-1}(1 - \epsilon)). \quad (5.76)$$

Denote $\Psi(\phi) = f^{-1}(1 - \epsilon)$, similar to the proof of Lemma 2 in [104], we can prove that $\Psi(\phi)$ is a monotonic increasing function of ϕ . Then we have

$$\frac{\partial \phi}{\partial R_s} = \frac{\partial \phi}{\partial \Psi} \frac{\partial \Psi}{\partial R_s} < 0, \quad (5.77)$$

thus $\frac{\partial p_{co}^*(R_s)}{\partial R_s} > 0$. Since $T'(0) > 0$, $T'(\infty) < 0$, there exists a unique R_s^* that makes T' first positive and then negative after R_s exceeds R_s^* . Thus, T is a first-increasing-then-decreasing function of R_s , i.e., T is a quasi-concave function of R_s and the optimal value that maximizes T is R_s^* . Since the explicit expressions of T' is difficult to be obtained, we can obtain R_s^* numerically. ■

Corollary 5.4. *There exists an equilibrium for the Stackelberg game.*

Proof. Based on Proposition 5.5, for a fixed μ , the optimal secrecy rate R_s and power allocation ϕ is unique. According to [164], the equilibrium exists for a two-player Stackelberg game as long as the best-response strategy set of the follower is a singleton. Hence, the existence of the equilibrium can be guaranteed. ■

The secrecy rate versus R_s under different λ_e is shown in Fig. 5.3, where a secrecy outage probability of $\epsilon = 0.1$ is satisfied. We can observe that the secrecy rate is a quasi-concave function of R_s , which validates Proposition 5.5. This is because by increasing R_s , the SOP p_{so} will be increased and thus the power allocation ϕ should be decreased to satisfy the secrecy outage constraint. Thus, p_{co} will be increased and the secrecy throughput will first increase and then decrease with the increase of R_s .

So far we have obtained the optimal power allocation and the secrecy rate for a fixed eavesdropping policy, we then need to solve the Eve's problem to determine the optimal guard zone. Since the Eve is the leader, it should take the

Figure 5.3: The secrecy throughput vs. the secrecy rate R_s with different λ_e , where $\mu = 1.5$, $\epsilon = 0.1$, and $R_t = 2$ bps/Hz.

follower's reactions into account. Similar to Proposition 5.5, we can prove that for fixed ϕ and R_s , U_E is also a quasi-concave function of μ . Due to the lack of explicit expressions of ϕ and R_s , the optimal value of μ can only be obtained through a numerical method. Since both the revenue functions are quasi-concave functions, for a given μ , the optimal power allocation and secrecy rate are unique. Hence, there is a unique equilibrium for the proposed game, which can be obtained through the proposed iterative algorithm shown in Algorithm 3.

5.7 Numerical Results and Discussions

In this section, simulation results are presented to verify the theoretical analysis. We assume that the BSs, cellular users and Eves are distributed according to three independent PPPs. The transmitting power of each BS is 20 dBm with a power allocation factor $\phi = 0.7$, and the noise is ignored. The number of transmit antenna of each BS is $N = 8$ and the wiretap code rates are set to be $R_t = 3$ bps/Hz and $R_s = 1.5$ bps/Hz, respectively, unless stated otherwise. In addition, the path loss exponent is set to be 4, unless stated otherwise.

Algorithm 3 Iterative algorithm finding the Stackelberg equilibrium

```
1: Initialization:  $\mu_{\min}, \mu_{\max}, \Delta R_s, \Delta\mu, R_t$ ;  
2:  $t = 0, \mu(t) = \mu_{\min}$ ;  
3: while  $\mu(t+1) \in [\mu_{\min}, \mu_{\max}]$  do  
4:    $R_s = R_t$ ;  
5:   while  $R_s \in (0, R_t]$  do;  
6:     Calculate  $\phi^*(R_s)$  by solving  $p_{so}^A = \epsilon$  with a bisection method;  
7:     Substitute  $\phi^*(R_s)$  into  $p_{co}^A$  and obtain  $T$ ;  
8:      $R_s = R_s - \Delta R_s$ ;  
9:   endwhile  
10:  Find  $R_s^*(t)$  and  $\phi^*(t)$  that maximize  $T$  ;  
11:  Calculate  $p_{st}^A(t), \mu(t+1) = \mu(t) + \Delta\mu$ ;  
12: endwhile  
13: Find  $\mu^*$  that minimize  $p_{st}^A$ , and then  $\phi^*, R_s^*$ , and  $T^*$ .
```

Figures 5.4 and 5.5 shows the connection and secrecy outage probabilities versus the BS density, λ_b , with different system configurations. We can observe that the connection and secrecy outage probabilities decrease with the increase of λ_b , which infers that deploying more BSs can improve the performance. The theoretical results obtained by (5.8) and (5.28) match well with the simulation results and are quite close to the asymptotic results. This validates Theorems 5.1 and 5.2. We also observe that for fixed values of N and λ_b , by increasing the density of the cellular users, the connection outage probability will be increased and the SOP will be decreased as well. This is because the BS active probability will be increased by increasing the density of cellular users, hence the inter-cell interference will increase. Moreover, we observe that the SOP increases with the increase of the density of Eves and asymptotically converge to a constant value with the increase of λ_b , which validates the theoretical analysis.

The effect of power allocation factor ϕ on the outage probabilities is evaluated in Fig. 5.6. We can observe that increasing ϕ will decrease the connection outage

 Figure 5.4: Connection outage probability vs. λ_b with different λ_u and λ_e .

 Figure 5.5: Secrecy outage probability vs. λ_b with different λ_u and λ_e .

Figure 5.6: Connection and secrecy outage probabilities vs. ϕ , where $\lambda_b = 0.0002$ and $\lambda_u = 0.001$.

probability and increase the SOP. This is because the received useful signal powers at the typical user and Eves are proportional to ϕ , while the aggregate interference is independent of ϕ . Moreover, we observe that the connection outage probability decreases with an increase of the number of transmit antennas due to the multi-antenna gain.

In Fig. 5.7, the SASE results are plotted versus BS density with different cell loads, where the optimal power allocation factor is calculated through a bisection search. We can observe that the SASE improves by increasing the density of BSs or cellular users. This is because deploying more BSs will decrease p_{co} and p_{so} simultaneously, which has been verified in the previous section. As for the cell load, on one hand, increasing the cell load will increase the BS active probability p_a which will increase p_{co} ; on the other hand, increasing λ_u will cause p_{so} to decrease and thus the optimal value of ϕ is increased, as shown in Fig. 5.8. The aggregate effect of these two factors will cause p_{co} to decrease and the SASE is thus improved. The AN transmission region is also shown in Fig. 5.8. We can observe that the optimal value of ϕ increases with λ_b and λ_u , and it approaches 1. This implies that in a dense network, the inter-cell interference can be used as a

Figure 5.7: Secrecy area spectral efficiency vs λ_b , where $\lambda_e = 0.00025$ and $\epsilon = 0.1$.

source of jamming without transmitting AN.

In Fig. 5.9, we evaluate the average secrecy rate of a typical user versus λ_b for fixed cellular user density and power allocation factor, in a low cell-load case. We can observe that increasing the BS density or the number of transmit antennas can improve the average secrecy rate. This is consistent with the analytical results presented in Section 5.4. In addition, the analytical lower bound is in good agreement with the simulation results. The impact of the number of antennas at each BS, the path loss factor, and power allocation on the average secrecy rate is presented in Fig. 5.10 and Fig. 5.11, respectively. We can observe that by increasing the number of BS antennas, the average secrecy rate will be increased due to the increased antenna gain. On the other hand, a larger path loss factor can achieve a higher secrecy rate due to the reduced inter-cell interference. Moreover, we can observe that the SASE is a quasi-concave function of ϕ and the optimal power allocation decreases with an increase of λ_e/λ_b , which validates the conclusion in Corollary 5.2.

When the cell load is very high, the average achievable secrecy rate versus the number of users is presented in Fig. 5.12. We can observe that the average secrecy

Figure 5.8: The optimal power allocation vs λ_b , where $\lambda_e = 0.00025$ and $\epsilon = 0.1$.

Figure 5.9: Average secrecy rate vs. N , where $\lambda_u = 0.001$.

Figure 5.10: Average secrecy rate under different Eve density and path loss factor, where $\lambda_b = 0.0002$.

Figure 5.11: Average secrecy rate vs. ϕ , where $\lambda_u = 0.0005$.

Figure 5.12: Average secrecy rate vs. number of users K , where $\lambda_b = 0.0002$, $\lambda_e = 0.0003$, and $\lambda_u = 0.004$.

rate of a typical user decreases with an increase of the number of users. This is because the total transmit power for the users is fixed and equally allocated among all the users, increasing K will decrease the available power of the typical user. We also observe that the average secrecy rate increases with an increase of the number of transmit antennas. This demonstrates the advantage of multi-antenna techniques. In addition, the derived lower bound expression of the average secrecy rate is shown to be very close to the simulations. We then show the achievable SASE for the fixed power allocation scheme in Fig. 5.13. We can observe that the optimal number of users increases with the number of transmit antennas, which is approximately $0.6N$.

The secure transmission probability performance versus λ_e and μ is shown in Fig. 5.14, for both the conventional eavesdropping scheme and the adaptive eavesdropping scheme. We can observe that by adaptively acting as an active jammer when it is far away from the active BSs, the secure transmission probability can be degraded, which is beneficial to the Eves. The feasible regions that enable adaptive eavesdropping are also given in Figs. 5.14 and 5.15. We can observe that by increasing λ_b , both the minimum and maximum values of λ_e that enable

Figure 5.13: SASE vs. number of users K , where $\lambda_b = 0.0002$, $\lambda_e = 0.0003$, and $\lambda_u = 0.004$.

Figure 5.14: The secure transmission probability under different schemes, where $\lambda_b = 0.001$, $\lambda_u = 0.002$, $\phi = 0.5$, $R_t = 2$ bps/Hz, and $R_s = 1$ bps/Hz.

Figure 5.15: The feasible region under different λ_b , where $\lambda_u = 0.002$, $\phi = 0.5$, $R_t = 2$ bps/Hz, and $R_s = 1$ bps/Hz.

adaptive eavesdropping will be increased. This is because the minimum value of λ_e is proportional to $\lambda_b p_a$ according to (5.50). Since p_{st} is affected by both p_{co} and p_{so} , for the adaptive eavesdropping strategy, p_{co} will be increased and p_{so} will be decreased compared with the conventional scheme. By increasing λ_b , the connection outage probability will be decreased since the inter-cell interference will be increased and thus p_{co} becomes more robust to external jamming, resulting in an increase of the maximum value of λ_e . When λ_e exceeds the maximal value, the secure transmission probability will be dominated by p_{so} , and p_{st} will be increased by the adaptive eavesdropping scheme.

Finally, the utility performance of the Eves and the BSs, i.e., the secure transmission probability and the secrecy throughput is evaluated through solving the formulated Stackelberg game. We consider the conventional eavesdropping scheme as a benchmark scheme, i.e., all Eves are passive and the optimal power allocation and secrecy code rate are optimized by solving (5.68). From Fig. 5.16, we can observe that the secure transmission probability decreases with λ_e . This is quite straightforward since both p_{co} and p_{so} increase with λ_e , as has been shown previously. In addition, we observe that the conventional scheme achieves higher

Figure 5.16: The secure transmission probability under different schemes, where $\lambda_u = 0.002$ and $R_t = 2$ bps/Hz.

Figure 5.17: The secrecy throughput under different schemes, where $\lambda_u = 0.002$ and $R_t = 2$ bps/Hz.

secrecy transmission probability than the adaptive eavesdropping scheme, and a up to 56% secrecy transmission probability degradation can be achieved when $\lambda_e = 0.003$, $\lambda_b = 0.0005$. This shows the superiority of adaptive eavesdropping for Eves. Moreover, we can observe that the secure transmission probability level increases and the gap between the conventional scheme and the adaptive eavesdropping scheme narrows by increasing λ_b . This is because as λ_b increases, the number of active BSs will be increased, and thus the number of active jammers will be decreased, resulting in the adaptive eavesdropping scheme approaching the conventional scheme. The corresponding secrecy throughput performance for the BSs is shown in Fig. 5.17 and similar conclusions can be obtained.

5.8 Summary

In this chapter, an AN-aided secure transmission scheme in a multi-antenna small-cell network has been investigated. The BSs, cellular users, and Eves are assumed to follow independent PPPs. Closed-form expressions of the connection and secrecy outage probabilities have been derived and comprehensive analysis has been conducted with the aid of large system analysis to show the impact of different system parameters. Some useful insights have been obtained. We have also derived the lower bound expression of the average secrecy rate and it is efficient to evaluate. When the cell load is very high, a multi-user ZFBF scheme has been proposed and a lower bound expression of the average secrecy rate has been derived. Following that, the optimal number of users that maximizes the secrecy area spectral efficiency has been obtained numerically and it has been shown to be a fixed portion of the number of transmit antennas. Finally, the impact of adaptive Eves with eavesdropping and jamming capability on the secrecy performance has also been investigated, and the condition that enables adaptive eavesdropping has been obtained. The optimal parameters for the BSs and the Eves, i.e., the power allocation factor and the secrecy rate, as well as the radius of the guard zone

around each Eve, are obtained by using a Stackelberg game theoretical approach.

Chapter 6

Physical Layer Security in Heterogeneous Networks with Pilot Attack

6.1 Introduction

In this chapter, we study the physical layer security performance in a sub-6 GHz massive MIMO macro cell and mmWave small cell hybrid heterogeneous network. By considering pilot spoofing attacks from the Eves, we analyze the coverage and secrecy probabilities using stochastic geometry. Specifically, we show that due to the existence of pilot contamination and pilot spoofing attack, densifying the macro cells will not always improve the coverage performance for the sub-6 GHz massive MIMO system. For the mmWave system, we first derive the success probability of beam alignment based on a beam sweeping based channel training model. Following that, the conditions under which the millimeter wave system outperforms the sub-6 GHz counterpart are discussed in terms of both coverage and secrecy. Our results reveal that the mmWave small cell can provide better coverage performance in the high code-rate transmission region, and the secrecy performance of the mmWave system outperforms the sub-6 GHz counterpart in

the low redundant rate region.

6.2 System Model

We consider secure communication in a TDD downlink cellular network, consisting of both sub-6 GHz macro cells and mmWave small cells¹. The positions of the macro-cell BSs (MBSs) and the small-cell BSs (SBSs) are distributed according to independent Poisson Point Processes (PPPs) Φ_μ and Φ_m , with intensities λ_μ and λ_m , respectively. Each MBS is equipped with massive antennas (N_μ antennas) and each SBS is equipped with N_m antennas. The users are randomly distributed according to an independent PPP with sufficiently high density, and each user can operate in either sub-6 GHz or mmWave opportunistically, as assumed in [128, 129]. We assume that the downlink communication is eavesdropped by some non-colluding Eves whose locations are randomly distributed according to an independent PPP Φ_E with intensity λ_E . Different from [129], each Eve can launch a pilot attack during the uplink channel training process for both MBSs and SBSs. In addition, each Eve can eavesdrop the communication in both sub-6 GHz and mmWave bands. Universal frequency reuse is adopted among different cells.

6.2.1 Sub-6 GHz Channel Model

We assume that all sub-6 GHz channels experience independent and identically distributed (i.i.d.) Rayleigh fading as well as a large-scale path loss with a path loss exponent of α_μ . The channel from the k th user in the j th cell to the i th MBS is denoted by

$$\mathbf{h}_{ij}^{(k)} = \sqrt{X_{ij}^{(k)}} \mathbf{u}_{ij}^{(k)}, \quad (6.1)$$

¹This will be possible in future 5G networks, where both sub-6 GHz and mmWave band will be used and the mmWave small cells are overlaid under the sub-6 GHz macro cells.

where $X_{ij}^{(k)}$ denotes the path loss from the k th user in the j th cell to the i th MBS, $\mathbf{u}_{ij}^{(k)}$ is the corresponding small-scale fading vector with distribution $\mathcal{CN}(\mathbf{0}, \mathbf{I})$. Note that the path loss can be calculated by

$$X_{ij}^{(k)} = c_\mu (R_{ij}^{(k)})^{-\alpha_\mu}, \quad (6.2)$$

where c_μ is the path loss at a reference distance, which is frequency dependent and is commonly set as $(\frac{c}{4\pi f_c})^2$.

We assume perfect synchronization and the downlink channel state information (CSI) can be obtained through the uplink pilot based training method due to channel reciprocity. We assume that the MBS assigns orthogonal pilots for all the K users within its cell, and the k th user in each cell is assigned with the same pilot. Denote $\mathcal{N}_k$ as the point process formed by the location of the k th user in each cell, it is clear that $\mathcal{N}_k$ is non-stationary (non-PPP) due to the correlation with the MBS process. To simplify the analysis, the other-cell scheduled users for the 0th MBS in $\mathcal{N}_k$ is modelled as an inhomogeneous PPP with a density function as has been assumed in [165, 166]

$$\lambda_u(r) = \lambda_\mu(1 - e^{-\pi\lambda_\mu r^2}). \quad (6.3)$$

where r denotes the distance to the 0th MBS. To further facilitate the analysis, we adopt the exclusion ball model proposed in [167], and assume that $\mathcal{N}_k$ is a homogeneous PPP with density λ_μ outside an exclusion ball centered at the 0th MBS with radius $R_{eq} = \sqrt{1/(\pi\lambda_\mu)}$. In addition, $\mathcal{N}_k$ and $\mathcal{N}_{k'}$ are independent for $k \neq k'$.

In the uplink training stage, after correlating the received signal with the corresponding pilot sequence, the observed channel from the i th MBS to the k th user

can be expressed as

$$\mathbf{y}_{ii}^{(k)} = \sum_{j \in \Phi_\mu} \sqrt{P_p} \mathbf{h}_{ij}^{(k)} + \sum_{l \in \Phi_e^{(k)}} \sqrt{P_e} \mathbf{h}_{ie}^{(l)} + \mathbf{n}_i, \quad (6.4)$$

where P_p and P_e denote the uplink transmitting power levels of the user and Eve, respectively. $\Phi_e^{(k)}$ is the set of Eves launching pilot attack for user k , $\mathbf{n}_i$ is the noise with $\mathcal{CN}(0, \sigma^2)$. Note that since each Eve will randomly choose the pilot sequence from the K sequences, the effective density of $\Phi_e^{(k)}$ is $\lambda_e^\mu = \frac{\lambda_E}{K}$ according to the independent thinning of PPP. Since the channels are assumed to be i.i.d. Rayleigh faded, the channel of the k th user in the i th cell can be estimated by an MMSE estimator [167, 168]

$$\bar{\mathbf{h}}_{ii}^{(k)} = \frac{\sqrt{P_p} X_{ii}^{(k)}}{\Sigma_{ii}^{(k)}} \mathbf{y}_{ii}^{(k)}, \quad (6.5)$$

where $\Sigma_{ii}^{(k)} = \sum_{j \in \Phi_\mu} P_p X_{ij}^{(k)} + \sum_{l \in \Phi_e^{(k)}} P_e X_{ie}^{(l)} + \sigma^2$. Then the channel error is

$$\hat{\mathbf{h}}_{ii}^{(k)} = \mathbf{h}_{ii}^{(k)} - \bar{\mathbf{h}}_{ii}^{(k)} \sim \mathcal{CN} \left(\mathbf{0}, X_{ii}^{(k)} \left(1 - \frac{P_p X_{ii}^{(k)}}{\Sigma_{ii}^{(k)}} \right) \mathbf{I} \right). \quad (6.6)$$

6.2.2 mmWave Channel Model

For the mmWave channels, due to the highly directional transmission, small-scale fading is usually ignored [169] and only path loss and blockage effect are considered. Due to the small wavelength, mmWave communication is sensitive to blockage and the link between an SBS and the mmWave user (mmUE) can be either LoS or NLoS link. We adopt the blockage model in [131] and the link between a mmUE and the SBS at a distance r is LoS or NLoS with probabilities

$$\begin{cases} p_L(r) = e^{-\beta r}, \\ p_N(r) = 1 - e^{-\beta r}. \end{cases} \quad (6.7)$$

respectively, where β is an environment dependent constant.

Since the shorter mmWave wavelength enables to fit more antenna elements for a fixed antenna aperture, each mmUE is considered to be equipped with a small antenna array. We assume that both the SBS and mmUEs are equipped with only a single RF chain [136], and thus analog beamforming is adopted. For mathematical tractability, we approximate the antenna pattern by a sectorized beam pattern similar to [130, 131]. Denote the main lobe gain, side lobe gain, and beamwidth of mmUE as G_U , g_U , θ_U , respectively. Similar definitions apply to the SBS with G_{BS} , g_{BS} , θ_{BS} , and Eve with G_E , g_E , θ_E , respectively. To further simplify the subsequent analysis, we consider zero side lobe for the SBS². Denote the channel from the k th mmUE in the j th cell to the i th SBS as $\mathbf{H}_{ij}^{(k)}$, similar to [134–136], we adopt a geometric channel model with a single path, which can be expressed as

$$\mathbf{H}_{ij}^{(k)} = \sqrt{Y_{ij}^{(k)}} \mathbf{a}_S(\theta_{ij}^{(k)}) \mathbf{a}_U(\varphi_{ij}^{(k)}), \quad (6.8)$$

where $\mathbf{a}_S(\cdot)$ and $\mathbf{a}_U(\cdot)$ are the steering vectors at the SBS and mmUE, $\theta_{ij}^{(k)}$ and $\varphi_{ij}^{(k)}$ are the angle of arrival (AoA) and angle of departure (AoD) at the SBS and mmUE. The AoAs and AoDs of all links are uniformly distributed in $[0, 2\pi]$. Note that $Y_{ij}^{(k)}$ is the path loss between mmUE and SBS and is given by

$$Y_{ij}^{(k)} = \begin{cases} c_L (R_{ij}^{(k)})^{-\alpha_L}, & \text{for LoS link,} \\ c_N (R_{ij}^{(k)})^{-\alpha_N}, & \text{otherwise.} \end{cases} \quad (6.9)$$

Note that c_L and c_N are the path loss for LoS and NLoS links at a reference distance. To align the transmit and receive beams, a codebook based sweeping method is considered.

Similar to [135], we assume that each SBS has a codebook of N_c possible beamforming vectors $\mathbf{v}_1, \dots, \mathbf{v}_{N_c}$, and the patterns of these beamforming vectors have non-overlapping main lobes. Hence, the angular domain can be divided by

²This assumption is reasonable since mmWave BS usually use very large antenna array and the front-to-back ratio can be larger than 30dB [170]. Note that similar assumption has also been adopted in [135, 171].

Figure 6.1: Beam sweeping based beam alignment.

the main lobes of the beamforming patterns into N_c sectors, and the n th angular sector is defined as $[\frac{2\pi(n-1)}{N_c}, \frac{2\pi n}{N_c}]$. Similar definitions apply to mmUE and Eves, where each mmUE and Eve has M_c and M_e beamforming vectors, denoted by $\mathbf{f}_1, \dots, \mathbf{f}_{M_c}$ and $\mathbf{t}_1, \dots, \mathbf{t}_{M_e}$, respectively. Define the set of AoA covered by the main lobe of $\mathbf{v}_n$ as $\mathcal{R}_n$, i.e., $\mathcal{R}_n = \{\theta \in [0, 2\pi] \mid |\mathbf{a}_S(\theta)\mathbf{v}_n|^2 = G_{BS}\}$. Then the AoD covered by the main lobe of $\mathbf{f}_m$ and $\mathbf{t}_l$ are $\mathcal{T}_m = \{\varphi \in [0, 2\pi] \mid |\mathbf{a}_U(\varphi)\mathbf{f}_m|^2 = G_U\}$ and $\mathcal{T}_{E,l} = \{\varphi \in [0, 2\pi] \mid |\mathbf{a}_E(\varphi)\mathbf{t}_l|^2 = G_E\}$, respectively. Following that, the average beamforming gains for the mmUE and Eve are given by

$$D_U = g_U + \frac{\theta_U}{2\pi}(G_U - g_U) \quad (6.10)$$

and

$$D_E = g_E + \frac{\theta_E}{2\pi}(G_E - g_E), \quad (6.11)$$

respectively. The SBS and the mmUE are assumed to be perfectly synchronized. Similar to [172], in the uplink training, the mmUE sends the pilot towards its serving SBS, and SBS sweeps the beams in each sector and determines the beamforming direction for its associated users by steering to the beam sector that achieves maximal signal power, as shown in Fig. 6.1. We assume that orthogonal pilot sequences are assigned among different mmUEs, i.e., no pilot contamination

is present. This is because: 1) each SBS will serve only one mmUE in each time slot due to the single RF chain; 2) those nearby SBSs will be assigned orthogonal pilot sequences and those far way SBSs will cause minor interference due to the severe path loss. This is different from the sub-6 GHz system where usually multiple users are served by an MBS. On the other hand, we assume that the Eves have perfectly synchronized with the SBS and randomly selects one pilot sequence to confound the SBS³.

Without loss of generality, we assume that the AoA of the typical mmUE is located in the first sector of the SBS. Then the received signal in the n th sector in the beam sweeping process after correlating with the corresponding pilot is approximated by

$$y_n = \mathbb{1}(n = 1) \sqrt{P_p} \mathbf{v}_n^H \mathbf{H}_{00}^{(0)} \mathbf{f}_m + \sum_{l \in \Phi_e^m} \sqrt{P_e} \mathbf{v}_n^H \mathbf{H}_{0e}^{(l)} \mathbf{t}_l + \mathbf{v}_n^H \mathbf{n}_i, \quad (6.12)$$

where $\mathbb{1}(\cdot)$ is the indicator function, $\mathbf{v}_n$ is the beamforming vector for the n th sector, $\mathbf{H}_{0e}^{(l)} = \sqrt{Y_{0e}^{(l)}} \mathbf{a}_S(\theta_{0e}^{(l)}) \mathbf{a}_E(\varphi_{0e}^{(l)})$ denotes the Eve's channel. Φ_e^m denotes the Eves that share the same pilot with the mmUE and whose AoAs lie within the main lobe of the first beamforming vector of SBS. With the zero side lobe of SBS and the independent thinning of PPP, the effective intensity of Φ_e^m is $\lambda_e^m = \frac{\lambda_E}{K} \frac{\theta_{BS}}{2\pi}$. Then the average received signal power in the n th sector can be expressed as

$$E_n = \mathbb{1}(n = 1) P_p Y_{00}^{(0)} G_{BS} G_U + \sum_{l \in \Phi_e^m} P_e Y_{0e}^{(l)} G_{BS} D_E + \sigma_m^2. \quad (6.13)$$

After sweeping all the beam sectors, the SBS will select the optimal beamforming vector by

$$\mathbf{v}_{n^*} = \arg \max_{n=1, \dots, N_c} E_n. \quad (6.14)$$

The success probability of beam pairing is defined as $p_s = \mathbb{P}(n^* = 1)$.

³The Eves have perfect knowledge about all the pilot sequences used by mmUEs.

6.2.3 Mobile Association Rule

Each user is assumed to be associated to the BS providing the largest average received signal power (ARSP), and the users are offloaded to the macro-cell when the ARSP from the mmWave BS is below a threshold τ . The ARSP of a typical user associated with each tier is defined as

$$\begin{cases} \text{ARSP}_\mu = \frac{P_\mu}{K} N_\mu X_{00}^{(0)}, \\ \text{ARSP}_m = P_m G_M Y_{00}^{(0)}. \end{cases} \quad (6.15)$$

To derive the association probability, we first check the path loss property, given in the following lemma.

Lemma 6.1. *The complementary cumulative distribution function (CCDF) of the path loss from a typical user to the nearest MBS and SBS is given by [112, 128, 129]*

$$\bar{F}_{X_{00}^{(0)}}(x) = 1 - \exp\left(-\pi\lambda_\mu \left(\frac{c_\mu}{x}\right)^{\frac{2}{\alpha_\mu}}\right), \quad (6.16)$$

and

$$\bar{F}_{Y_{00}^{(0)}}(y) = 1 - \exp\left(-\pi\lambda_m \Lambda\left(\frac{1}{y}\right)\right), \quad (6.17)$$

respectively, where

$$\Lambda(y) = 2 \frac{\gamma(2, \beta(c_L y)^{\frac{1}{\alpha_L}}) - \gamma(2, \beta(c_N y)^{\frac{1}{\alpha_N}})}{\beta^2} + (c_N y)^{\frac{2}{\alpha_N}}. \quad (6.18)$$

Lemma 6.2. *The probability that a typical user is associated with the sub-6 GHz tier is given by*

$$\mathcal{A}_\mu = 1 - \pi\lambda_m (\Xi_L - \Xi_N), \quad (6.19)$$

where

$$\Xi_s = \int_0^{\frac{PG_M}{\tau}} f_s(l) e^{-\pi\lambda_m \Lambda(l) - \pi\lambda_\mu (c_\mu \vartheta l)^{\frac{2}{\alpha_\mu}}} dl, s = \{L, N\}, \quad (6.20)$$

Figure 6.2: The association probability under different threshold and SBS density, where $\lambda_\mu = 10$ BSs/km², $P_\mu = 43$ dBm, $P_m = 30$ dBm, $K = 10$.

$$f_s(l) = \frac{2c_s^{\frac{2}{\alpha_s}}}{\alpha_s} \left(\frac{l^{\frac{2}{\alpha_s}-1}}{e^{\beta(c_s l)^{\frac{1}{\alpha_s}}}} - \mathbb{1}(s = N)l^{\frac{2}{\alpha_s}-1} \right), \quad (6.21)$$

$$\text{and } \vartheta = \frac{P_\mu N_\mu K}{P_m G_M}.$$

Proof. The proof is omitted here. ■

We can readily prove the analysis in Lemma 6.2, as shown in Fig. 6.2. We can observe that the theoretical results match well with the simulations and by increasing the density of mmWave BSs, the association probability to the mmWave tier is increased.

6.2.4 Performance Metrics

We assume that both MBS and SBS use Wyner's encoding scheme for secure information transmission, as has been adopted in [114, 173, 174]. Let R_b and R_s denote the transmitted codeword rate and secrecy rate, respectively, then the rate difference $R_e \triangleq R_b - R_s$ can be regarded as the intentionally added redundancy to provide secrecy against eavesdropping. Particularly, we consider a fixed-rate transmission, i.e., the rate of the codeword R_b and the rate of the secrecy in-

formation R_s are determined before transmission. Due to the channel variance, connection and secrecy cannot be always guaranteed. Specifically, the coverage probability is defined as the probability that the instantaneous capacity is larger than R_b , i.e.,

$$p_{cov} = \mathbb{P}(W \log_2(1 + \text{SINR}) > R_b) = \mathbb{P}(\text{SINR} > T), \quad (6.22)$$

where $T = 2^{\frac{R_b}{W}} - 1$. Similarly, the secrecy probability is defined as the probability that the eavesdropping capacity C_e is below the redundancy rate R_e . Since the Eves are non-colluding, the secrecy probability can be expressed as

$$\begin{aligned} p_{sec} &= \mathbb{P}\left(\max_{l \in \Phi_E} W \log_2(1 + \text{SINR}_{e_l}) < R_e\right) \\ &= \mathbb{P}\left(\max_{l \in \Phi_E} \text{SINR}_{e_l} < T_e\right), \end{aligned} \quad (6.23)$$

where $T_e = 2^{\frac{R_b - R_s}{W}} - 1$. Thus, the rate coverage and secrecy probability of a typical user can be expressed as

$$p_{cov} = \mathcal{A}_\mu p_{cov}^\mu + \mathcal{A}_m p_{cov}^m \quad (6.24)$$

and

$$p_{sec} = \mathcal{A}_\mu p_{sec}^\mu + \mathcal{A}_m p_{sec}^m, \quad (6.25)$$

respectively, where p_{cov}^μ , p_{cov}^m , p_{sec}^μ , and p_{sec}^m denote the coverage and secrecy in the sub-6 GHz tier and the mmWave tier, respectively.

6.3 Coverage Performance Analysis

In this section, we analyze the conditional coverage performance when the typical user is associated to the sub-6 GHz tier and the mmWave tier.

6.3.1 Sub-6 GHz Tier

We assume that each MBS serves K users simultaneously by using MRT precoding and null space based AN transmission is adopted. For simplicity, we consider equal power allocation among the K users, then the transmitted signal at the i th BS can be expressed as

$$\mathbf{x}_i = \sum_{k=0}^{K-1} \sqrt{\frac{\phi P_\mu}{K}} \mathbf{w}_{ii}^{(k)} s_{ii}^{(k)} + \sqrt{(1-\phi)P_\mu} \mathbf{V}_i \mathbf{n}_a, \quad (6.26)$$

where ϕ is the power allocation between the information bearing signal and the AN, P_μ is the total transmit power, $s_{ii}^{(k)}$ is the information bearing signal with $\mathbb{E} \left[\left| s_{ii}^{(k)} \right|^2 \right] = 1$, $\mathbf{n}_a$ is an artificial noise vector with i.i.d. entries $n_a \sim \mathcal{CN}(0, \frac{1}{N_\mu - K})$. Note that $\mathbf{w}_{ii}^{(k)}$ denotes the beamforming vector of the k th user at the i th BS, $\mathbf{V}_i \in \mathbb{C}^{N_\mu \times (N_\mu - K)}$ denotes the null space of $\bar{\mathbf{H}}_i$, where $\bar{\mathbf{H}}_i = [\bar{\mathbf{h}}_{ii}^{(0)}, \bar{\mathbf{h}}_{ii}^{(1)}, \dots, \bar{\mathbf{h}}_{ii}^{(K-1)}]$. Then the received signal at the typical user can be expressed as

$$\begin{aligned} y_{00}^{(0)} &= \sqrt{\bar{P}_\mu} \bar{\mathbf{h}}_{00}^{(0)H} \mathbf{w}_{00}^{(0)} s_{00}^{(0)} + \sqrt{\bar{P}_\mu} \hat{\mathbf{h}}_{00}^{(0)H} \mathbf{w}_{00}^{(0)} s_{00}^{(0)} + \sum_{k=1}^{K-1} \sqrt{\bar{P}_\mu} \mathbf{h}_{00}^{(0)H} \mathbf{w}_{00}^{(k)} s_{00}^{(k)} + \\ &+ \sum_{i \in \Phi_\mu \setminus \{0\}} \left[\sum_{k=0}^{K-1} \sqrt{\bar{P}_\mu} \mathbf{h}_{i0}^{(0)H} \mathbf{w}_{ii}^{(k)} s_{ii}^{(k)} + \sqrt{(1-\phi)P_\mu} \mathbf{h}_{i0}^{(0)H} \mathbf{V}_i \mathbf{n}_a \right] + n_0, \end{aligned} \quad (6.27)$$

where $\bar{P}_\mu = \frac{\phi P_\mu}{K}$, $\mathbf{h}_{ij}^{(k)}$ denotes the downlink channel from the i th BS to the k th user in the j th cell. We assume that each BS adopts $\mathbf{w}_{ii}^{(k)}$ as a scaled version of the channel estimation given by

$$\mathbf{w}_{ii}^{(k)} = \frac{\bar{\mathbf{h}}_{ii}^{(k)}}{\left| \bar{\mathbf{h}}_{ii}^{(k)} \right|} = \frac{\mathbf{y}_{ii}^{(k)}}{\left| \mathbf{y}_{ii}^{(k)} \right|}. \quad (6.28)$$

Then the SINR of the typical user can be expressed as

$$\text{SINR}_0^\mu = \frac{\left| \bar{\mathbf{h}}_{00}^{(0)H} \mathbf{w}_{00}^{(0)} \right|^2}{I_0 + I_i + \frac{\sigma_\mu^2}{\bar{P}_\mu}}, \quad (6.29)$$

where

$$\begin{aligned}
 I_0 &= \mathbb{E} \left| \widehat{\mathbf{h}}_{00}^{(0)H} \mathbf{w}_{00}^{(0)} \right|^2 + \sum_{k=1}^{K-1} \mathbb{E} \left| \mathbf{h}_{00}^{(0)H} \mathbf{w}_{00}^{(k)} \right|^2 \\
 &= \frac{\mathbb{E} \left| \widehat{\mathbf{h}}_{00}^{(0)H} \mathbf{y}_{00}^{(0)} \right|^2}{\left| \mathbf{y}_{00}^{(0)} \right|^2} + \sum_{k=1}^{K-1} \frac{\mathbb{E} \left| \mathbf{h}_{00}^{(0)H} \mathbf{y}_{00}^{(k)} \right|^2}{\left| \mathbf{y}_{00}^{(k)} \right|^2},
 \end{aligned} \tag{6.30}$$

$$\begin{aligned}
 I_i &= \sum_{i \in \Phi_\mu \setminus 0} \left[\sum_{k=0}^{K-1} \mathbb{E} \left| \mathbf{h}_{i0}^{(0)H} \mathbf{w}_{ii}^{(k)} \right|^2 + K\xi \left| \mathbf{h}_{i0}^{(0)H} \mathbf{v}_i \right|^2 \right] \\
 &= \sum_{i \in \Phi_\mu \setminus 0} \left[\sum_{k=0}^{K-1} \frac{\mathbb{E} \left| \mathbf{h}_{i0}^{(0)H} \mathbf{y}_{ii}^{(k)} \right|^2}{\left| \mathbf{y}_{ii}^{(k)} \right|^2} + K\xi \left| \mathbf{h}_{i0}^{(0)H} \mathbf{v}_i \right|^2 \right],
 \end{aligned} \tag{6.31}$$

and $\xi = \frac{\phi^{-1}-1}{N_\mu-K}$. Since universal frequency reuse is adopted, we only consider the interference-limited case and the thermal noise is neglected. By substituting the previous results into (6.29), the SIR can be approximated by

$$\text{SIR}_0^\mu \approx \frac{P_p(N_\mu + 1)(X_{00}^{(0)})^2}{X_{00}^{(0)}\Delta_0 + \Sigma_{00}^{(0)} \left((K-1)X_{00}^{(0)} + \Delta_1 + (1 + \xi_0)\Delta_2 \right)}, \tag{6.32}$$

where $\xi_0 = \frac{\phi^{-1}-1}{N_\mu}$. Note that $\Delta_0 = \sum_{j \in \Phi_\mu \setminus 0} P_p X_{0j}^{(0)} + \sum_{l \in \Phi_e^{(0)}} P_e X_{0e}^{(l)} + \sigma^2$, $\Delta_1 = P_p \sum_{i \in \Phi_\mu \setminus 0} (X_{i0}^{(0)})^2 / \Sigma_{ii}^{(0)}$, and $\Delta_2 = K \sum_{i \in \Phi_\mu \setminus 0} X_{i0}^{(0)}$.

Proof. Please refer to Appendix D.1. ■

Following that, the coverage probability can be derived as follows.

Proposition 6.1. *The rate coverage probability of the typical user associated with the sub-6 GHz tier in the presence of pilot contamination and attack is approximated by*

$$\begin{aligned}
 p_{cov}^\mu &\approx \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} \exp \left(-\frac{nvTA_4}{A_0} \right) \\
 &\quad \int_0^\infty \exp \left(-\frac{nvT(A_1 t^{\frac{\alpha_\mu}{2}} + A_2 t + A_3 t^{1+\frac{\alpha_\mu}{2}})}{A_0} \right) f(t) dt,
 \end{aligned} \tag{6.33}$$

where $f(t) = \pi\lambda_\mu e^{-\pi\lambda_\mu t}$, $v = (N!)^{-\frac{1}{N}}$, N is the number of terms used in the approximation. Note that $A_0 = P_p(N_\mu + 1)c_\mu^2$, $A_1 = K\bar{\Delta}_0 c_\mu$, $A_2 = P_p a_3 + (1 + \xi_0)K P_p c_\mu a_4$, $A_3 = (1 + \xi_0)K\bar{\Delta}_0 a_4$, $A_4 = (K - 1)P_p c_\mu^2$, $\bar{\Delta}_0 = P_p a_1 + P_e a_2 + \sigma^2$. In addition, $a_1 = \frac{2c_\mu(\pi\lambda_\mu)^{\frac{\alpha_\mu}{2}}}{\alpha_\mu - 2}$, $a_2 = \frac{4c_\mu(\pi\lambda_e^\mu)^2}{\alpha_\mu - 2} \int_0^\infty r^{3-\alpha_\mu} e^{-\pi\lambda_e^\mu r^2} dr$, $a_3 = \frac{\pi\lambda_\mu c_\mu^2}{\alpha_\mu - 1}$, and $a_4 = \frac{2\pi c_\mu \lambda_\mu}{\alpha_\mu - 2}$.

Proof. Please refer to Appendix D.2. ■

From (6.33), we can prove that the coverage probability of the sub-6 GHz tier is an increasing function of N_μ . However, the impact of MBS density λ_μ on the coverage probability can not be readily obtained due to the complicated expression in (6.33). Here we provide some intuitive explanations. For a weak pilot attack (e.g., density of Eves is very low), by increasing the MBS density, the pilot contamination will be increased. Thus, the received signal power of a typical user scales strictly less than $\lambda_\mu^{\frac{\alpha_\mu}{2}}$, but the interference power scales larger than $\lambda_\mu^{\frac{\alpha_\mu}{2}}$, resulting in a decrease in coverage performance. However, when the pilot attack from Eves dominates pilot contamination, we can observe that $\Sigma_{00}^{(0)} \approx \Delta_0 \approx \sum_{l \in \Phi_e^{(0)}} P_e X_{0e}^{(l)}$, both of them scales strictly less than $\lambda_\mu^{\frac{\alpha_\mu}{2}}$. On the other hand, the numerator in (6.32) scales as $\lambda_\mu^{\alpha_\mu}$. In this case, by increasing the MBS density, the coverage performance will be improved. The coverage probability under different Eve density is evaluated in Fig. 6.3. We can observe that when λ_E is very small, the coverage probability gradually decreases to a constant, whereas for a large λ_E , the coverage first increases and then converges to a constant, which validated the analysis.

Remark 6.1. For the cases without pilot reuse, i.e., all the users are assigned with orthogonal pilot sequences and only pilot attack is present, a_1 and a_3 reduce to 0. For the perfect CSI case without pilot attack and pilot contamination, a_1 , a_2 , and a_3 reduce to 0.

Figure 6.3: The coverage probability versus the MBS density, where $N_\mu = 64$, $\alpha_\mu = 2.6$, $K = 2$, $\phi = 0.7$, and $R_b = 20$ Mbps.

6.3.2 mmWave Tier

In this subsection, we characterize the coverage performance of the mmWave tier taking into the account the impact of the pilot attack. Due to the single-path channel model and the zero SBS side lobe assumptions, we first define the following two events: 1) the SBS and mmUE beams are successfully aligned (SA event), which captures the case of the beamforming pair with the maximal SBS and mmUE beamforming gains, i.e., $D_{BS} = G_{BS}$ and $D_U = G_U$, and 2) the SBS and mmUE beams are unsuccessfully aligned (UA event), which captures the case of the beamforming pair with SBS main lobe gain and mmUE side lobe gain, i.e., $D_{BS} = G_{BS}$ and $D_U = g_U$. Then the coverage probability can be expressed as

$$p_{cov}^m = \mathbb{P}(\text{SINR}_0^m > T \mid \text{SA})\mathbb{P}(\text{SA}) + \mathbb{P}(\text{SINR}_0^m > T \mid \text{UA})\mathbb{P}(\text{UA}). \quad (6.34)$$

The SINR of the typical user under the SA and UA cases can be expressed as

$$\text{SINR}_{0,\text{SA}}^m = \frac{P_m G_{BS} G_U Y_{00}^{(0)}}{I_m + N_0}, \quad (6.35)$$

and

$$\text{SINR}_{0,\text{UA}}^m = \frac{P_m G_{BS} g_U Y_{00}^{(0)}}{I_m + N_0}, \quad (6.36)$$

respectively, where $I_m = \sum_{i \in \Phi_m^{(1)} \setminus \{0\}} P_m G_{BS} D_U Y_{i0}^{(0)}$. Note that $\Phi_m^{(1)}$ denotes the interfering SBSs whose AoAs lie within the main lobe, based on the independent thinning of PPP, the effective intensity of $\Phi_m^{(1)}$ is $\lambda_m^{(1)} = \lambda_m \theta_{BS}/2\pi$.

Lemma 6.3. *The success probability of beam alignment is lower bounded by*

$$p_s \geq \left(1 - \int_0^\infty e^{-\pi \lambda_m \Lambda(\frac{x}{\alpha_E})} f_{Y_E^{-1}}(x) dx\right)^{N_c-1}. \quad (6.37)$$

Note that

$$f_{Y_E^{-1}}(x) = \pi \lambda_m^m \Lambda'(x) e^{-\pi \lambda_m^m \Lambda(x)}, \quad (6.38)$$

where $\Lambda'(x)$ is the first derivative of $\Lambda(x)$ and $\alpha_E = \frac{P_e D_E}{P_p G_U}$.

Proof. The received pilot attack signal power can be approximated by the received power from the nearest Eve, i.e.,

$$\sum_{l \in \Phi_e^m} Y_{0e}^{(l)} \approx \max_{l \in \Phi_e^m} (Y_{0e}^{(l)}) \triangleq Y_E. \quad (6.39)$$

Since the Eve's position is independent with the mmUE, Y_E follows a similar distribution with $Y_{00}^{(0)}$. Hence the success probability can be approximated as

$$\begin{aligned} p_s &= \mathbb{P}\left(E_1 \geq \max_{n=2, \dots, N_c} E_n\right) \\ &\geq \left[\mathbb{P}\left(P_p Y_{00}^{(0)} G_{BS} G_U \geq P_e G_{BS} D_E Y_E\right)\right]^{N_c-1} \\ &= \left[\mathbb{P}\left(Y_{00}^{(0)} \geq \alpha_E Y_E\right)\right]^{N_c-1} \\ &= \left(1 - \int_0^\infty e^{-\pi \lambda_m \Lambda(\frac{x}{\alpha_E})} f_{Y_E^{-1}}(x) dx\right)^{N_c-1}. \end{aligned} \quad (6.40)$$

By substituting the result in Lemma 6.1, we can obtain (6.37). ■

The success probability of beam alignment versus the Eve's density is shown in Fig. 6.4, with the parameters given in Section 6.5. We can observe that the gap

Figure 6.4: The success probability of beam alignment.

between the theoretical results and simulation results is negligible. In addition, the success probability increases with λ_m and decreases with λ_E . This is because Y_E increases with λ_E and $Y_{00}^{(0)}$ increases with λ_m .

Proposition 6.2. *The rate coverage probability of the typical user associated with the mmWave tier is lower bounded by*

$$p_{cov}^m \geq p_s \left[1 - \int_0^\infty e^{-\Lambda_m(0, A_m)} f_{(Y_{00}^{(0)})^{-1}}(x) dx \right], \quad (6.41)$$

where $f_{(Y_{00}^{(0)})^{-1}}(x)$ is the pdf of the path loss from the mmUE to SBS and can be derived from Lemma 6.1. Note that $A_m = \frac{P_m G_{BS} G_U}{uT(\sigma_m^2 + \mu_I)}$, μ_I is the average value of the inter user interference and is given by

$$\mu_I = 2\pi\lambda_m^{(1)} P_m G_{BS} D_U \left[c_L \int_{(c_L x)^{\frac{1}{\alpha_L}}}^\infty t^{1-\alpha_L} e^{-\beta t} dt + c_N \int_{(c_N x)^{\frac{1}{\alpha_N}}}^\infty t^{1-\alpha_N} (1 - e^{-\beta t}) dt \right]. \quad (6.42)$$

Proof. When the beams are not aligned, the SINR is usually very low, hence the coverage probability will be dominated by the SA case, i.e.,

$$p_{cov}^m \geq \mathbb{P}(\text{SINR}_0^m > T \mid \text{SA}) \mathbb{P}(\text{SA}). \quad (6.43)$$

Conditioning on the success beam alignment, the SINR coverage probability can be derived as

$$\begin{aligned}\mathbb{P}(\text{SINR}_0^m > T \mid \text{SA}) &= \mathbb{P}\left(Y_{00}^{(0)} \geq \frac{T(I_m + \sigma_m^2)}{P_m G_{BS} G_U}\right) \\ &= \mathbb{E}_{Y_{00}^{(0)}} \left[1 - \exp\left(-\pi \lambda_m \Lambda\left(\frac{P_m G_{BS} G_U}{T(\sigma_m^2 + I_m)}\right)\right) \right],\end{aligned}\quad (6.44)$$

and the interference term can be approximated by

$$\begin{aligned}\mu_I &= \sum_{i \in \Phi_m^{(1)} \setminus \{0\}} P_m G_{BS} D_U Y_{i0}^{(0)} \\ &= 2\pi \lambda_m^{(1)} P_m G_{BS} D_U \int_{(\frac{c}{Y_{00}^{(0)}})^{\frac{1}{\alpha}}}^{\infty} cr^{-\alpha} p(r) dr.\end{aligned}\quad (6.45)$$

By considering both the LoS and NLoS cases, (6.45) can be calculated. By taking an average of (6.45) over $Y_{00}^{(0)}$, we can obtain (6.41). $\blacksquare$

Corollary 6.1. *When only the LoS link is considered, i.e., $p_L(r) = \mathbb{1}(r < R_L)$, the rate coverage probability reduces to*

$$p_{cov}^m = p_s(1 - e^{-\pi \lambda_m \varpi^2}), \quad (6.46)$$

where $\varpi = \min\left(R_L, \left(\frac{P_m G_{BS} G_U c_L}{T \sigma_m^2}\right)^{\frac{1}{\alpha_L}}\right)$,

Proof. When only the LoS link is present, by analyzing the intensity measure of the path loss process [128], we can obtain

$$\Lambda(x) = \min(R_L^2, (c_L x)^{\frac{2}{\alpha_L}}). \quad (6.47)$$

Then the conditional rate coverage probability under SA becomes

$$\mathbb{P}\left(X_{00}^{(0)} \geq \frac{T \sigma_m^2}{P_m G_{BS} G_U}\right) = 1 - e^{-\pi \lambda_m \varpi^2}. \quad (6.48)$$

By multiplying the success probability, we can obtain (6.46). $\blacksquare$

For the special case that only the LoS link with $p_L(r) = \mathbb{1}(r < R_L)$, we can also obtain the following corollary.

Corollary 6.2. *The necessary condition that enables the coverage performance of the mmWave tier to outperform the counterpart of the sub-6 GHz tier in the presence of the pilot attack is given by*

$$\lambda_m \geq \frac{-\ln(1 - p_{cov}^\mu/p_s)}{\pi\varpi^2}. \quad (6.49)$$

Since the beam alignment success probability monotonically increases with λ_m , we can observe from (6.49) that it is always possible to enable the coverage performance in the mmWave tier to outperform that of the sub-6 GHz tier, as long as the mmWave tier is still noise-limited.

6.4 Secrecy Performance Analysis

6.4.1 Sub-6 GHz Tier

For the Eves, we consider the worst case by assuming that they have zero noise power and also have multi-user decoding capability [35, 112, 114], i.e., they can resolve the concurrent transmission of information signals from nearby BSs using successive interference cancellation, and thus the SIR of the l th Eve can be expressed as

$$\begin{aligned} \text{SIR}_{e_l}^\mu &= \frac{\bar{P}_\mu \left| \mathbf{g}_{0e}^{(l)H} \mathbf{w}_{00}^{(0)} \right|^2}{\sum_{i \in \Phi_\mu} \phi P_\mu \xi \left| \mathbf{g}_{ie}^{(l)H} \mathbf{V}_i \right|^2} \\ &= \frac{\left| \mathbf{g}_{0e}^{(l)H} \mathbf{y}_{00}^{(0)} \right|^2}{\left| \mathbf{y}_{00}^{(0)} \right|^2 \sum_{i \in \Phi_\mu} \xi K \left| \mathbf{g}_{ie}^{(l)H} \mathbf{V}_i \right|^2}. \end{aligned} \quad (6.50)$$

Following similar procedures for coverage performance analysis, we can derive the secrecy outage probability which is given by the following proposition.

Proposition 6.3. *The secrecy probability of the typical user associated with the sub-6 GHz tier with pilot contamination and attack is lower bounded by*

$$p_{sec}^\mu \geq \exp(-\pi\lambda_E\Theta), \quad (6.51)$$

where Θ is given by

$$\Theta = \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} \int_0^\infty e^{-\frac{nvT_e B_0}{B_1 t^{-\frac{\alpha_\mu}{2}} + B_2 t^{-\alpha_\mu}}} dt. \quad (6.52)$$

Note that N is the number of terms used for calculation, $v = (N!)^{-\frac{1}{N}}$, and $B_0 = \xi_0 a_4 K \bar{\Delta}$, $B_1 = \bar{\Delta} c_\mu$, $B_2 = N_\mu P_e c_\mu^2$, $\bar{\Delta} = \bar{\Delta}_0 + 2P_p \pi \lambda_\mu c_\mu \int_0^\infty r^{1-\alpha_\mu} e^{-\pi \lambda_\mu r^2} dr$.

Proof. Please refer to Appendix D.3. ■

Then we can obtain the following property.

Property 6.1. *The secrecy probability of the AN-aided sub-6 GHz system is an increasing function of the MBS density λ_μ and is a decreasing function of N_μ and the Eve's density λ_E .*

The property of λ_E can be readily proved. Since the distance from the l th Eve to the i th MBS $\sum_{i \in \Phi_\mu} X_{ie}^{(l)}$ scales as $\lambda_\mu^{\frac{\alpha_\mu}{2}}$, and $X_{0e}^{(l)}$ is independent with λ_μ due to the Slivnyak's theorem, then from (D.15), we can observe that the SIR of the l th Eve decreases with λ_μ . On the other hand, since the Eves are assumed to be able to resolve the information from nearby BSs, the average aggregate interference power will be independent with N_μ . Therefore, the SIR of the l th Eve increases with N_μ , as shown in (D.14).

Remark 6.2. When only pilot contamination is present, $B_2 = 0$, $a_2 = 0$, the integration in Θ produces a closed-form expression. In particular, for the perfect CSI case, $B_1 = c_\mu$, and $B_2 = 0$.

6.4.2 mmWave Tier

For the mmWave system, since the Eves can resolve information from different SBSs, then the SNR of the l th Eve can be expressed as

$$\text{SNR}_{e_l}^m = \frac{P_m D_{BS} D_E X_{0e}^{(l)}}{\sigma_m^2}. \quad (6.53)$$

Due to the existence of the pilot attack, the exact expression of the secrecy probability is nontrivial to be derived. However, since all the Eves are non-colluding, the maximal SNR is usually determined by the nearest Eve. Then the approximated expression of the secrecy probability of the mmWave system can be derived, which is given by the following proposition.

Proposition 6.4. *The secrecy probability of the typical user associated with the mmWave tier with pilot attack is approximated by*

$$p_{sec}^m \approx p_s e^{-\pi \lambda_E \frac{\theta_{BS}}{2\pi} \Lambda(\mu)} + (1 - p_s) e^{-\pi \lambda_E \Lambda(\mu)}, \quad (6.54)$$

where $\mu = \frac{P_m G_{BS} D_E}{T_e \sigma_m^2}$.

Proof. Please refer to Appendix D.4. ■

Note that the success probability of beam alignment is usually close to 1, and the secrecy probability under the SA case is much larger than the UA case. This is because in the UA case the SBS beam is steered to the Eve. Hence the secrecy probability will be dominated by the first term in (6.54), and we can obtain the following property.

Property 6.2. *The secrecy probability is a decreasing function of the Eve's density λ_E and is an increasing function of λ_m .*

Remark 6.3. From (6.54), we observe that the mmWave system can achieve a secrecy probability ϱ if

$$p_s \geq \varrho e^{\pi \lambda_E \frac{\theta_{BS}}{2\pi} \Lambda(\mu)}. \quad (6.55)$$

In addition, the secrecy probability achieved by the mmWave small cell outperforms the sub-6 GHz counterpart, when $p_{sec}^\mu = \varrho$ and p_s satisfies (6.55).

Due to the complicated expression of the secrecy probability for the sub-6 GHz tier and the mmWave tier, it is difficult to directly obtain the explicit expressions of the conditions that enable the mmWave tier to outperform the sub-6 GHz tier. Hence, we only compare the performance through numerical results in the next section.

6.5 Numerical Results and Discussions

In this section, simulation results are presented to verify the theoretical analysis. We assume that the sub-6 GHz carrier frequency is 1 GHz with a bandwidth of 20 MHz and the mmWave system operates in 28 GHz with a bandwidth of 1 GHz. The path loss exponent is set as $\alpha_\mu = 2.6$, $\alpha_L = 2$, $\alpha_N = 2.9$, respectively, and the LoS probability parameter is $1/\beta = 20$. In addition, the path loss constant is set to be $c_\mu = -38.46$ dB, $c_L = -61.4$ dB, and $c_N = -72$ dB, respectively. The MBS is equipped with $N_\mu = 64$ antennas and the mmWave antenna beam patterns of the SBS, mmUE, and Eve are $(G_{BS}, \theta_{BS}) = (10 \text{ dB}, \frac{2\pi}{N_m})$, $(G_U, g_U, \theta_U) = (3 \text{ dB}, -3 \text{ dB}, \frac{2\pi}{3})$, $(G_E, g_E, \theta_E) = (10 \text{ dB}, -5 \text{ dB}, \frac{\pi}{3})$, respectively. The noise power is calculated by $\sigma^2 = -174 + 10 \log_{10}(BW) + N_f$ with the noise figure $N_f = 10$ dB. The transmitting power levels of the MBS and SBS are $P_\mu = P_m = 30$ dBm, respectively, unless stated otherwise. The pilot transmitting power levels of the user and Eve are $P_p^\mu = P_e^\mu = 30$ dBm, and $P_p^m = P_e^m = 30$ dBm.

We first verify the coverage probability of the sub-6 GHz system and mmWave system under different CSI conditions in Fig. 6.5. We can observe that the approximation for the sub-6 GHz system match well with the simulation results and the mmWave lower bound strictly follows the trend of the simulations with a small gap, which validate the theoretical analysis. We can observe that the coverage per-

Figure 6.5: The coverage probability of the sub-6 GHz tier and the mmWave tier under different CSI cases, where $\lambda_\mu = \lambda_m = \lambda_E = 20$ BSs/km², $\phi = 0.7$, $K = 1$.

formance is severely degraded by the pilot attack and contamination. Comparing the coverage performance between the sub-6 GHz tier and the mmWave tier, we can observe that the sub-6 GHz system outperforms the mmWave counterpart at low data rate region, whereas the mmWave system outperforms the sub-6 GHz system at high data rate region. This is because mmWave system with much larger band width can achieve much higher capacity than the sub-6 GHz system. However, mmWave signals also suffer severe path loss and blockage, which greatly limits the coverage performance at low data rate region.

We then present the coverage performance comparison between the sub-6 GHz tier and the mmWave tier under different BS density and antenna configurations in Fig. 6.6. For fair comparisons, we assume that each MBS only serves one user in each time slot, i.e., $K = 1$. We observe that both increasing the number of antennas at MBS and densifying the MBS density can improve the coverage performance of the sub-6 GHz system under the given parameters, which has been explained in Section 6.3.1. More importantly, we also observe that increasing the number of antennas at MBS is more effective than densifying the MBS density for coverage improvement, due to the pilot contamination. For example, when

Figure 6.6: The coverage performance comparison between the sub-6 GHz tier and the mmWave tier, where $\lambda_E = 20$ BSs/km², $\phi = 0.7$, $K = 1$.

$\lambda_\mu = 10^{-5}$, increasing the number of antennas at MBS from 40 to 160, we can achieve 37% performance improvement, whereas densifying MBS to 4×10^{-5} can only obtain a gain of 15.7%. On the other hand, by increasing the SBS density, the mmWave coverage performance will be improved and can also outperform the sub-6 GHz counterpart. This is because increasing λ_m not only improves the success probability of the beam alignment but also increases the average received signal power since the mmWave network is usually noise limited.

The corresponding secrecy performance is presented in Fig. 6.7. For the sub-6 GHz system, we can observe that the derived lower bound follows the trend of the simulation results, and the secrecy probability under the perfect CSI case outperforms the other two cases. This is because, on one hand, the AN is perfectly injected in the null space of the intended user's channel when the user's CSI is perfectly acquired, on the other hand, both the pilot contamination and pilot attack will steer the beamforming vector to deviate from the user's channel, resulting in more information leakage. However, the secrecy probability with both pilot contamination and pilot attack outperforms the case that has only pilot attack. This is because when only pilot attack is present, the beamformer at the MBS

Figure 6.7: The secrecy probability of the sub-6 GHz tier and the mmWave tier under different CSI cases, where $\lambda_\mu = \lambda_m = \lambda_E = 20$ BSs/km², $\phi = 0.7$, $K = 1$.

will move towards the Eve more thus increasing its received signal power. For the mmWave system, we can also observe that the pilot attack can greatly increase the eavesdropping capacity resulting in a lower secrecy probability compared with the no pilot attack case. Note that due to the approximation of the beam alignment success probability, there exists a small gap between the simulation and theoretical results. Different from the coverage performance, we can observe from Fig. 6.7 that at a low redundant rate region, the mmWave system always outperforms the sub-6 GHz system. This is because the directional transmission of mmWave signal is more resistant to eavesdropping, which shows the advantages of using mmWave to secure transmission. While at a high redundant rate region, the sub-6 GHz system gradually outperforms the mmWave system. This is because the AN and inherent inter-cell interference in the sub-6 GHz system can degrade the Eves and thus limits the maximal eavesdropping capacity.

Similar to Fig. 6.6, the secrecy performance comparison between the sub-6 GHz tier and the mmWave tier is presented in Fig. 6.8. We can observe that the secrecy performance will be improved by increasing the MBS density and is degraded by increasing the number of antennas at MBS, which validate Property

Figure 6.8: The secrecy performance comparison between the sub-6 GHz tier and the mmWave tier, where $\lambda_E = 20$ BSs/km², $\phi = 0.7$, $K = 1$.

6.1. Hence, densifying MBS is more effective than increasing MBS antennas in improving the secrecy performance in the sub-6 GHz tier. Moreover, we observe that by densifying SBS, it is always possible for the mmWave tier outperforms the sub-6 GHz tier.

Lastly, the coverage and secrecy probabilities of a typical user are evaluated in Figs. 6.9 and 6.10, respectively. From Fig. 6.9, we can observe that by increasing the SBS density λ_m , the coverage performance will be improved, which is straightforward. However, increasing the number of antennas at MBS will not always improve the coverage performance. Since increasing N_μ will force more users to be associated with the sub-6 GHz tier, and the mmWave tier achieves better coverage performance at high data rate region as has been explained before. Thus, the coverage performance will be degraded by increasing N_μ when the target rate R_b is very high. For the secrecy performance, since the secrecy probability increases with the BS density in either the sub-6 GHz tier or the mmWave tier, we can observe that the secrecy performance will be improved by either increasing MBS density or SBS density, as shown in Fig. 6.10.

Figure 6.9: The coverage probability of a typical user, where $\lambda_\mu = 20$ BSs/km², $\lambda_E = 40$ BSs/km², $P_\mu = 43$ dBm, $\phi = 0.7$, $K = 10$, $\tau = -10$ dBm.

Figure 6.10: The secrecy probability of a typical user, where $P_\mu = 43$ dBm, $\phi = 0.7$, $K = 10$, $R_e = 5$ Mbps, $\tau = -10$ dBm.

6.6 Summary

In this chapter, the physical layer security in a sub-6 GHz and mmWave hybrid network has been investigated, where all the nodes are distributed according to independent PPPs. By taking into account the pilot attack from the Eves, we provide an analytical framework to characterize the coverage and secrecy probabilities. For the sub-6 GHz tier, it has revealed that increasing the number of MBS antennas is more effective than increasing MBS density in improving the coverage performance, whereas densifying MBS is more effective for security enhancement. Moreover, it has shown that the coverage and secrecy in the mmWave tier can outperform the sub-6 GHz counterpart through densifying the SBS.

Chapter 7

Conclusions and Future Works

7.1 Conclusions

Without using complicated cryptographic protocols, security can be achieved at physical layer by exploiting the random and fading nature of wireless mediums. Physical layer security techniques provide essential benefits to wireless systems, and pave the way for the future networked society. In this thesis, we have investigated security enhancement techniques in emerging wireless communication systems, by using the physical layer security methods. The main contributions and conclusions are summarized as follows.

We have proposed to use the successive relaying scheme to improve the secrecy performance of an AF relaying network with untrusted relay nodes in Chapter 3. Considering different complexity requirement, we have proposed several relay pair selection schemes and derived the corresponding closed-form expression of the lower bound of the SOP. Some useful insights have also been provided through asymptotic diversity order analysis. It has revealed that, the proposed scheme can achieve a maximum diversity order of $N - 1$, where N is the number of untrusted relay nodes, which shows a great improvement compared with existing schemes.

In Chapter 4, we have investigated the secrecy throughput maximization strategy in a two-user MISOME wiretap channel through joint optimization of power

allocation and wiretap code rates. Both the normal data stream and AN are employed to jam the Eves and both non-adaptive and adaptive transmission schemes are proposed. It is proven that the effective secrecy throughput is a quasi-concave function of the secrecy rate and the power allocated to Bob, and for fixed wiretap code rates, the optimal power allocation is derived in a closed-form expression. Moreover, it has been shown that improved secrecy throughput can be achieved through injecting AN and concurrent transmission of Bob and the normal user.

Following that, we have investigated physical layer security in AN-aided multi-antenna small-cell networks in Chapter 5, considering the spatial randomness of different nodes. By leveraging the stochastic geometry tools, closed-form expressions of the connection and secrecy outage probabilities are derived and the impact of different parameters is analyzed. It reveals that in a low cell-load case, deploying more BSs will improve the connection and secrecy outage performance. For a fixed-rate transmission scheme, the condition under which AN becomes unnecessary is given. We also derive a semi closed-form expression of the lower bound of the achievable average secrecy rate, which is shown to be a quasi-concave function of the power allocation factor and a monotonic decreasing function of the ratio of the Eve-BS density. We have further investigated the impact of adaptive eavesdropping or jamming strategy from the perspective of Eves, where Eves far away from the BSs adaptively act as jammers to interfere with the legitimate users. It has been shown that the secure transmission probability and the secrecy throughput will be degraded severely with smart jamming.

Lastly, we have studied the physical layer security in a hybrid sub-6 GHz and mmWave large-scale heterogeneous network in Chapter 6, with massive antennas at the sub-6 GHz BSs. By considering pilot spoofing attacks from the Eves, we have analyzed the coverage and secrecy performance using stochastic geometry. It has been shown that densifying the macro cells will not improve the coverage performance for the sub-6 GHz massive MIMO system in the presence of pilot contamination. For the sub-6 GHz tier, increasing the number of BS antennas is

more effective than increasing BS density in improving the coverage performance, whereas densifying BS is more effective for security enhancement. Moreover, the mmWave tier may outperform the sub-6 GHz counterpart in terms of both coverage and secrecy through densifying the base stations. Meanwhile, the mmWave small cell can provide better coverage performance in the high transmission code-rate region, whereas the secrecy performance of the mmWave system outperforms the sub-6 GHz counterpart in the low redundant rate region, which reveals the advantage of using mmWave for secure communication.

7.2 Future Works

There are some potential research directions that can be extended based on the insights presented in this thesis. Firstly, in this thesis, the exploitation of AN relies on the perfect CSI of the main channel [173, 175], which may not be available in practice. Thus, the secure transmission scheme in the presence of CSI errors, arising from imperfect feedback [92], pilot contamination in massive MIMO [43, 102], or pilot attacks [42], still needs further investigation. We have learnt from Chapter 6 that pilot contamination and pilot attack may greatly degrade the coverage and secrecy performance of the massive MIMO system, however, the detection and mitigation of such attacks remain a very challenging issue. An energy ratio detector was proposed in [44] by comparing the received signal power at the transmitter and receiver, however it requires a secure feedback link. A jamming resistant receiver scheme was proposed in massive MIMO uplink, and the jamming channel was estimated by exploiting the unused pilot sequence in [176], but it cannot be applied in multiple Eves or jammers case. Efficient detection and mitigation of pilot attacks are critical to recover the secure transmission and deserve more research attention.

Secondly, the effectiveness of AN also relies on the assumption that the number of antennas at the transmitter side is larger than that of Eves [88, 173]. This

assumption may not hold anymore in scenarios with a large number of colluding Eves or an Eve with massive antennas. It is interesting to investigate whether it is possible to achieve positive secrecy in the presence of massive antenna Eves and the corresponding secrecy enhancement techniques. In addition, the exploitation of AN incurs more power consumption, which may decrease the energy efficiency, the energy efficient power allocation with security constraints is also an interesting direction.

Thirdly, in large scale networks, the spatial randomness of the network nodes are modeled by the PPP model in Chapters 5 and 6 for the ease of tractability. One insight we have learnt is that the inter-cell interference can be used to secure the transmission without using artificial noise in the dense network. However, the inter-cell interference degrades both the legitimate user and the Eves, and thus greatly limits the achievable secrecy performance. To further enhance the secrecy capacity, advanced inter-cell interference management techniques, such as BS cooperation or coordination [155, 177], advanced precoding design with cell-edge user awareness [178] or interference leakage control [179], and optimal power control and power allocation at different BSs are promising solutions that worth more research efforts.

Moreover, in Chapter 6, the mmWave system is assumed to have only single RF chain and thus analog beamforming is employed. In practice, the mmWave BS and user may be equipped with multiple RF chains and the number of RF chains is usually less than the number of antennas, thus mmWave system usually adopts hybrid beamforming techniques to support multiple streams. Effective physical layer transmission methods are thus needed considering the unique features of mmWave systems.

Appendix A

Proofs of Theorems in Chapter 3

A.1 Proof of Theorem 3.1

Based on (3.23), we have

$$P_{out}^{SP} \stackrel{(c)}{>} \mathbb{P} \left(\frac{\gamma_{id}}{\gamma_{si} + \theta \gamma_{id}} \min\{\gamma_{si}, (\theta - 1)\gamma_{id}\} < \bar{\gamma} \right) > \mathcal{P}_{LB}^{SP}.$$

where (c) comes from the fact that $\frac{xy}{x+y} < \min(x, y)$,

$$\begin{aligned} \mathcal{P}_{LB}^{SP} &= \underbrace{\mathbb{P}(\gamma_{si} < (\theta - 1)\gamma_{id}, \gamma_{si} < \theta\bar{\gamma})}_{I_1} \\ &\quad + \underbrace{\mathbb{P}\left((\theta - 1)\gamma_{id} < \gamma_{si} < \theta\gamma_{id}, \gamma_{id} < \frac{\theta}{\theta - 1}\bar{\gamma}\right)}_{I_2} \\ &\quad + \underbrace{\mathbb{P}\left(\gamma_{si} > \theta\gamma_{id}, \gamma_{si} > \frac{\theta - 1}{\bar{\gamma}}\gamma_{id}^2\right)}_{I_3} \end{aligned} \tag{A.1}$$

Reformulating (A.1), we can obtain

$$\mathcal{P}_{LB}^{SP} = 1 + F_{\gamma_{si}}(\theta\bar{\gamma}) [1 - F_{\gamma_{id}}(\theta\bar{\gamma})] - \underbrace{\int_{\epsilon}^{\infty} f_{\gamma_{id}}(u) F_{\gamma_{si}}(\mu u^2) du}_{I_{A_1}},$$

where $\epsilon = \frac{\theta\bar{\gamma}}{\theta-1}$, and I_{A_1} can be calculated by

$$\begin{aligned}
 I_{A_1} &= \int_0^\infty f_{\gamma_{id}}(u) F_{\gamma_{si}}(\mu u^2) du - \int_0^\epsilon f_{\gamma_{id}}(u) F_{\gamma_{si}}(\mu u^2) du \\
 &= \sum_{m=M}^\infty \sum_{i=0}^{N-1} \binom{N-1}{i} (-1)^i N \lambda_g \left(\underbrace{\int_0^\infty e^{-pu^2-qu} u^{2m} du}_{I_{A_2}} - \underbrace{\int_0^\epsilon e^{-pu^2-qu} u^{2m} du}_{I_{A_3}} \right).
 \end{aligned} \tag{A.2}$$

Using the results in [1, eq. (3.462)], we have

$$I_{A_2} = (2p)^{-\left(\frac{\tilde{m}}{2}\right)} \Gamma(\tilde{m}) e^{\frac{q^2}{8p}} D_{-\tilde{m}}\left(\frac{q}{\sqrt{2p}}\right) \tag{A.3}$$

and

$$I_{A_3} = e^{\frac{q^2}{4p}} \sum_{j=0}^{2m} \binom{2m}{j} (-\zeta)^j \left(\frac{\gamma(n, p\epsilon'^2)}{2p^n} - \frac{\gamma(n, p\zeta^2)}{2p^n} \right), \tag{A.4}$$

Combining the above results, Theorem 3.1 can be obtained.

A.2 Proof of Theorem 3.2

Let $X = \min\left\{\frac{\gamma_{sl}\gamma_{ld}}{\gamma_a}, \frac{\gamma_a\gamma_{ld}}{\gamma_{sl}}\right\}$, and $X_0 = \min\{X_1, X_2\}$, with $X_1 = \frac{\gamma_{sl}}{\gamma_a}$, $X_2 = \frac{\gamma_a}{\gamma_{sl}}$, we have

$$\begin{aligned}
 F_{X_0}(x) &= \mathbb{P}(X_0 < x) \\
 &= \mathbb{P}(X_1 < x, \gamma_{sl} < \gamma_a) + \mathbb{P}(X_2 < x, \gamma_{sl} > \gamma_a) \\
 &= \mathbb{P}\left(\frac{\gamma_{sl}}{\gamma_a} < x, \gamma_{sl} < \gamma_a\right) + \mathbb{P}\left(\frac{\gamma_a}{\gamma_{sl}} < x, \gamma_{sl} > \gamma_a\right) \\
 &= \begin{cases} F_{X_1}(x) + F_{X_2}(x), & x < 1, \\ 1, & \text{otherwise.} \end{cases}
 \end{aligned} \tag{A.5}$$

where

$$F_{X_1}(x) = \frac{\lambda_h^M}{(\lambda_h + \frac{\lambda_a}{x})^M} \quad (\text{A.6})$$

and

$$F_{X_2}(x) = 1 - \frac{\lambda_h^M}{(\lambda_h + \lambda_a x)^M}. \quad (\text{A.7})$$

Proof. Because γ_{sl} and γ_a are independent of each other, and $F_{\gamma_a}(x) = 1 - e^{-\lambda_a x}$ with $\lambda_a = 1/(P_r \sigma_a^2)$, then

$$F_{X_1}(x) = \int_0^\infty F_{\gamma_{sl}}(xy) f_{\gamma_a}(y) dy. \quad (\text{A.8})$$

After some mathematical manipulations, (A.6) can be obtained. In the same way, we can derive (A.7). ■

Since γ_{ld} is independent with γ_{sl} and γ_a , we have

$$\begin{aligned} F_X(x) &= \mathbb{P}(\gamma_{ld} X_0 < x) \\ &= \int_0^\infty F_{X_0}\left(\frac{x}{y}\right) f_{\gamma_{ld}}(y) dy \\ &= \int_0^x f_{\gamma_{ld}}(y) dy + \underbrace{\int_x^\infty F_{X_1}\left(\frac{x}{y}\right) f_{\gamma_{ld}}(y) dy}_{I_{B_1}} + \underbrace{\int_x^\infty F_{X_2}\left(\frac{x}{y}\right) f_{\gamma_{ld}}(y) dy}_{I_{B_2}}. \end{aligned} \quad (\text{A.9})$$

Substituting (A.6) and (A.7) into (A.9), by using [1, eq. (3.353.1)], we have

$$\begin{aligned} I_{B_1} &= \int_x^\infty \frac{\lambda_h^M}{(\lambda_h + \frac{\lambda_a}{x} y)^M} \lambda_g e^{-\lambda_g y} dy \\ &= \lambda_g \mu_{x_1}^M \int_x^\infty \frac{e^{-\lambda_g y}}{(y + \mu_{x_1})^M} dy \\ &= \lambda_g \mu_{x_1}^M \phi_M(x, \mu_{x_1}, \lambda_g), \end{aligned} \quad (\text{A.10})$$

where $\mu_{x_1} = \frac{\lambda_h x}{\lambda_a}$. Similarly, by using [1, eq. (3.352.2), eq. (3.353.1)], we have

$$\begin{aligned}
 I_{B_2} &= \int_x^\infty \left(1 - \frac{\lambda_h^M}{(\lambda_h + \frac{\lambda_a x}{y})^M} \right) \lambda_g e^{-\lambda_g y} dy \\
 &= e^{-\lambda_g x} - \lambda_g \int_x^\infty e^{-\lambda_g y} \left(1 - \frac{\mu_{x_1}}{y + \mu_2} \right)^M dy \\
 &= \lambda_g M \mu_{x_2} v(x, \mu_{x_2}, \lambda_g) - \lambda_g \sum_{n=2}^M \binom{M}{n} (-\mu_{x_2})^n \phi_n(x, \mu_{x_2}, \lambda_g),
 \end{aligned} \tag{A.11}$$

where and $\mu_{x_2} = \frac{\lambda_a x}{\lambda_h}$. Thus,

$$\begin{aligned}
 F_X(x) &= 1 - e^{-\lambda_g x} + \lambda_g \mu_{x_1}^M \phi_M(x, \mu_{x_1}, \lambda_g) \\
 &\quad + \lambda_g \left(M \mu_{x_2} v(x, \mu_{x_2}, \lambda_g) - \sum_{n=2}^M \binom{M}{n} (-\mu_{x_2})^n \phi_n(x, \mu_{x_2}, \lambda_g) \right).
 \end{aligned} \tag{A.12}$$

According to the order statistics [142], we have

$$\mathcal{P}_{LB}^{MM} = F_{\gamma_{i^* j^*}}(\bar{\gamma}) = N F_X^{N-1}(\bar{\gamma}) - (N-1) F_X^N(\bar{\gamma}). \tag{A.13}$$

This completes the proof.

A.3 Proof of Theorem 3.3

Defining $Z_1 = \frac{\gamma_{si}}{\gamma_{ij}}$, $Z_2 = \frac{\gamma_{ij}}{\gamma_{si}}$, and $Z = \min\{Z_1, Z_2\}$, similar to (A.5), we have

$$F_Z(z) = \begin{cases} F_{Z_1}(z) + F_{Z_2}(z), & z < 1, \\ 1, & \text{otherwise,} \end{cases} \tag{A.14}$$

where

$$F_{Z_1}(z) = \sum_{i=1}^N \binom{N}{i} (-1)^{i+1} \frac{\lambda_h^M}{(\lambda_h + \frac{i \lambda_{ij}}{z})^M} \tag{A.15}$$

and

$$F_{Z_2}(z) = \sum_{i=0}^N \binom{N}{i} (-1)^i \frac{\lambda_h^M}{(\lambda_h + i \lambda_{ij} z)^M}. \tag{A.16}$$

Proof. According to the selection criterion (3.17), the CDF of γ_{ij} is given by

$$F_{\gamma_{ij}}(x) = (1 - e^{-\lambda_{ij}x})^N, \quad (\text{A.17})$$

where $\lambda_{ij} = \lambda_a$. After some mathematical manipulations, (A.15) and (A.16) can be obtained. ■

Since γ_{id} and A are independent, similar to (A.9),

$$\mathcal{P}_{LB}^{MI} = \int_0^{\bar{\gamma}} f_{\gamma_{id}}(y) dy + \int_{\bar{\gamma}}^{\infty} \left[F_{Z_1} \left(\frac{\bar{\gamma}}{y} \right) + F_{Z_2} \left(\frac{\bar{\gamma}}{y} \right) \right] f_{\gamma_{id}}(y) dy. \quad (\text{A.18})$$

Substituting (A.15) and (A.16) into (A.18), we have

$$\int_{\bar{\gamma}}^{\infty} F_{Z_1} \left(\frac{\bar{\gamma}}{y} \right) f_{\gamma_{id}}(y) dy = -\widetilde{\sum} \lambda_g \beta_1^M \phi_M(\bar{\gamma}, \beta_1, \lambda_g). \quad (\text{A.19})$$

Repeating the same procedure, we can obtain

$$\begin{aligned} & \int_{\bar{\gamma}}^{\infty} F_{Z_2} \left(\frac{\bar{\gamma}}{y} \right) f_{\gamma_{id}}(y) dy \\ &= 1 - F_{\gamma_{id}}(\bar{\gamma}) + \widetilde{\sum} \left[e^{-\lambda_g \bar{\gamma}} + \lambda_g v(\bar{\gamma}, \beta_2, \lambda_g) + \lambda_g \sum_{n=2}^M \binom{M}{n} (-\beta_2)^n \phi_n(\bar{\gamma}, \beta_2, \lambda_g) \right]. \end{aligned} \quad (\text{A.20})$$

Appendix B

Proofs of Theorems in Chapter 4

B.1 Proof of Theorem 4.1

As per the definition of EST, we have

$$\frac{\partial T}{\partial \phi_b} = R_s \left[-(1 - p_{so}) \frac{\partial p_{to}}{\partial \phi_b} - (1 - p_{to}) \frac{\partial p_{so}}{\partial \phi_b} \right] \quad (\text{B.1})$$

and

$$\frac{\partial^2 T}{\partial \phi_b^2} = R_s \left[2 \frac{\partial p_{to}}{\partial \phi_b} \frac{\partial p_{so}}{\partial \phi_b} - (1 - p_{so}) \frac{\partial^2 p_{to}}{\partial \phi_b^2} - (1 - p_{to}) \frac{\partial^2 p_{so}}{\partial \phi_b^2} \right]. \quad (\text{B.2})$$

Due to the complicated expressions of p_{to} and p_{so} w.r.t. ϕ_b , (B.2) is too complex to be analyzed. To facilitate the proof, notice that ϕ_u^* approaches zero when N is very large due to the result of Corollary 4.1. In addition, $\lim_{n \rightarrow \infty} (1 + \frac{z}{n})^n = e^z$. Thus, when N is very large, we have

$$p_{so} = 1 - F_{\gamma_E}(\bar{\gamma}_e) \approx 1 - \chi^M, \quad (\text{B.3})$$

where $\chi = 1 - e^{-\beta \bar{\gamma}_e}$. Define $t = N - \lambda_b \bar{\gamma}_b$, we can obtain

$$\frac{\partial p_{to}}{\partial \phi_b} = -\frac{(\lambda_b \bar{\gamma}_b)^{N-1}}{(N-1)!} \frac{\zeta_b}{\phi_b^2} \lambda_b e^{-\lambda_b \bar{\gamma}_b}, \quad (\text{B.4})$$

$$\frac{\partial p_{so}}{\partial \phi_b} = \frac{M\chi^{M-1}(1-\chi)\zeta_e\bar{\gamma}_e}{\phi_b^2}, \quad (\text{B.5})$$

$$\frac{\partial^2 p_{to}}{\partial \phi_b^2} = \frac{\lambda_b^N \varepsilon_b^{N-1}}{(N-1)!} \frac{\zeta_b}{\phi_b^3} e^{-\lambda_b \bar{\gamma}_b} (t+2), \quad (\text{B.6})$$

and

$$\frac{\partial^2 p_{so}}{\partial \phi_b^2} = \frac{M\chi^{M-2}}{e^{\beta\bar{\gamma}_e}} \left[-\frac{(M-1)\zeta_e^2 \bar{\gamma}_e^2}{\phi_b^4 e^{\beta\bar{\gamma}_e}} + \chi \left(\frac{\zeta_e^2 \varepsilon_e^2}{\phi_b^4} - \frac{2\zeta_e \bar{\gamma}_e}{\phi_b^3} \right) \right]. \quad (\text{B.7})$$

Thus, when $\frac{\partial T}{\partial \phi_b} = 0$, from (B.1), we have

$$(1-p_{to}) \frac{\partial p_{so}}{\partial \phi_b} = -(1-p_{so}) \frac{\partial p_{to}}{\partial \phi_b}. \quad (\text{B.8})$$

Substituting (4.16), (4.17), (B.4), and (B.5) into (B.8), and after some mathematical manipulations, we have

$$\sum_{n=0}^{N-1} \frac{(\lambda_b \bar{\gamma}_b)^n}{n!} = \frac{\chi}{M(1-\chi)\bar{\gamma}_e} \frac{\lambda_b^N \bar{\gamma}_b^{N-1} \zeta}{(N-1)!}. \quad (\text{B.9})$$

Applying (B.6), (B.7), and (B.9) in (B.2), it yields

$$\frac{\partial^2 T}{\partial \phi_b^2} = R_s \frac{\lambda_b^N \bar{\gamma}_b^{N-1}}{(N-1)!} \frac{\zeta}{\phi_b^4} \chi^{M-1} e^{-\lambda_b \bar{\gamma}_b} f(\phi_b), \quad (\text{B.10})$$

where

$$f(\phi_b) = -(Me^{-\beta\bar{\gamma}_e} + 1)\bar{\gamma}_e - \chi t\phi_b < -\bar{\gamma}_e - \chi t\phi_b < -\chi(\bar{\gamma}_e + t\phi_b). \quad (\text{B.11})$$

To show the sign of $\frac{\partial^2 T}{\partial \phi_b^2}$, we need to determine the sign of $f(\phi_b)$. Define $g(\lambda_b)$ as follows

$$g(\lambda_b) = \frac{\chi}{M(1-\chi)\bar{\gamma}_e} \frac{\lambda_b^N \bar{\gamma}_b^{N-1} \zeta}{(N-1)!} - \sum_{n=0}^{N-1} \frac{(\lambda_b \bar{\gamma}_b)^n}{n!}. \quad (\text{B.12})$$

Denoting the root of (B.9) as λ_0 , we observe that λ_0 is the root of (B.12). By using the exponentially increasing property of the exponential function, we can infer that $\frac{\partial g(\lambda_b)}{\partial \lambda_b} > 0$, when $\lambda_b = \lambda_0$. After some mathematical manipulations, we can obtain

$$\left. \frac{\partial g(\lambda_b)}{\partial \lambda_b} \right|_{\lambda_b=\lambda_0} = \frac{(\lambda_b \bar{\gamma}_b)^{N-1}}{(N-1)!} \left[\frac{\chi(\bar{\gamma}_e \lambda_b P + t)}{MP \bar{\gamma}_e (1 - \chi)} + \frac{\lambda_b}{M} + \bar{\gamma}_b \right]. \quad (\text{B.13})$$

The first term within the square bracket must be an increasing function w.r.t. λ_b . By taking the derivative w.r.t. it, we have

$$\frac{\chi [\bar{\gamma}_e P(\bar{\gamma}_e \lambda_b P + t) + (\bar{\gamma}_e P - \bar{\gamma}_b)]}{M \bar{\gamma}_e P (1 - \chi)} + \frac{\bar{\gamma}_e \lambda_b P + t}{M} > 0. \quad (\text{B.14})$$

Thus, we can conclude that $\bar{\gamma}_e \lambda_b P + N - \lambda_b \bar{\gamma}_b > 0$ must hold, i.e., $f(\phi_b) < 0$ will always be correct.

By using the result of Lemma 4.3, we can conclude that the EST is a quasi-concave function w.r.t. ϕ_b . Following that, the global optimal ϕ_b that maximizes the EST can be found numerically, which lies either on the critical point or the boundary. The critical point can be obtained by setting the first derivative to zero, i.e., the root of (B.9). When $N \rightarrow \infty$, we also have $p_{to} \rightarrow 0$, and (B.9) becomes

$$(\lambda_b \bar{\gamma}_b)^{N-1} \chi \zeta_b \lambda_b e^{-\lambda_b \bar{\gamma}_b} - M(N-1)! \bar{\gamma}_e (1 - \chi) = 0. \quad (\text{B.15})$$

Solving the above equation, we obtain ϕ_b^o .

B.2 Proof of Theorem 4.2

The proof can be classified into two different cases:

Case I: when $1 - \phi_u \geq \phi_b^o$, from (4.29) we have $\phi_b^* = \phi_b^o$. Substitute ϕ_b^* into (4.21), we can obtain $\phi_u^* = \phi_b^o \eta$ when $\tau \geq \tau_0^o$, and $\phi_u^* = 1 - \frac{1 - \phi_b^o}{N-1}$, otherwise. Since $1 - \phi_u \geq \phi_b^o$ must hold, we have $\phi_b^o \leq \frac{1}{\eta+1}$.

Case II: when $1 - \phi_u < \phi_b^o$, we have $\phi_b^* = 1 - \phi_u$. Substitute ϕ_b^* into (4.21), we

can obtain $\phi_u^* = \frac{\eta}{\eta+1}$, when $\tau \geq \tau'$, and $\phi_u^* = 0$, otherwise, where τ' is obtained by letting $\phi_{u,\min} = \frac{\phi_u}{N-1}$. Since $1 - \phi_u < \phi_b^o$, $\phi_b^o > \frac{1}{\eta+1}$.

Combining the above results, we can obtain Theorem 4.2.

B.3 Proof of Theorem 4.3

The first and second derivatives of T are given by

$$\frac{\partial T}{\partial R_s} = (1 - p_{to})(1 - p_{so}) - R_s(1 - p_{to})\frac{\partial p_{so}}{\partial R_s}, \quad (\text{B.16})$$

and

$$\frac{\partial^2 T}{\partial R_s^2} = -(1 - p_{to}) \left(2\frac{\partial p_{so}}{\partial R_s} - R_s \frac{\partial^2 p_{so}}{\partial R_s^2} \right), \quad (\text{B.17})$$

respectively, where

$$\frac{\partial p_{so}}{\partial R_s} = \ln 2 M \beta \bar{\gamma}_e (\bar{\gamma}_e + 1) \chi^{M-1} (1 - \chi). \quad (\text{B.18})$$

When $\frac{\partial T}{\partial R_s} = 0$, we have

$$(1 - p_{so}) = R_s \frac{\partial p_{so}}{\partial R_s}. \quad (\text{B.19})$$

Substituting (4.17) and (B.18) into (B.19), yields

$$\chi = \ln 2 (1 - \chi) R_s M \beta (\bar{\gamma}_e + 1). \quad (\text{B.20})$$

Then the second term of (B.17) becomes

$$2\frac{\partial p_{so}}{\partial R_s} - R_s \frac{\partial^2 p_{so}}{\partial R_s^2} = \ln 2 M \beta (\bar{\gamma}_e + 1) \chi^{M-2} (1 - \chi) f(R_s), \quad (\text{B.21})$$

where

$$\begin{aligned} f(R_s) &= [2\chi + \ln 2R_s (\beta(\bar{\gamma}_e + 1)(Me^{-\beta\bar{\gamma}_e} - 1) + \chi)] \\ &> 2\chi - \ln 2\chi R_s (\beta(\bar{\gamma}_e + 1) - 1). \end{aligned} \quad (\text{B.22})$$

From (B.20), we have

$$R_s = \frac{e^{\beta\bar{\gamma}_e} - 1}{\ln 2M\beta(\bar{\gamma}_e + 1)}. \quad (\text{B.23})$$

By taking the derivative of the right-hand term w.r.t. R_s , we yield $\frac{e^{\beta\bar{\gamma}_e}(\beta(\bar{\gamma}_e+1)-1)}{M\beta(\bar{\gamma}_e+1)} > 0$. Hence, we can conclude that $\beta(\bar{\gamma}_e + 1) - 1 < 0$. Thus, $f(R_s) > 0$, $\partial^2 T / \partial R_s^2 < 0$. By using the result of Lemma 4.3, we can conclude that the EST is a quasi-concave function of R_s . Then the optimal value can be determined by comparing the EST achieved at the critical point and the boundary point, where the critical point can be obtained by solving (B.20).

Appendix C

Proofs of Theorems and Propositions in Chapter 5

C.1 Proof of Theorem 5.1

Define $X_i = \phi P \left[\left| \mathbf{h}_{i,0}^T \mathbf{w}_i \right|^2 + \xi \left\| \mathbf{h}_{i,0}^T \mathbf{G}_i \right\|^2 \right]$, since $\mathbf{w}_i$ and $\mathbf{h}_{i,0}$ are independent of each other, $\left| \mathbf{h}_{i,0}^T \mathbf{w}_i \right|^2 \sim \text{Exp}(1)$, $\left\| \mathbf{h}_{i,0}^T \mathbf{G}_i \right\|^2 \sim \text{Gamma}(N-1, 1)$. Then the PDF of X_i can be derived as [35]

$$f_{X_i}(x) = \begin{cases} \frac{x^{N-1}}{(N-1)!(\phi P)^N} e^{-\frac{x}{\phi P}}, & \text{if } \xi = 1, \\ \frac{(1-\xi)^{1-N}}{\phi P(N-2)!} e^{-\frac{x}{\phi P}} \gamma \left(N-1, \frac{(1-\xi)x}{\xi \phi P} \right), & \text{otherwise.} \end{cases} \quad (\text{C.1})$$

The Laplace transform of I_B can be expressed as

$$\begin{aligned} \mathcal{L}_{I_B}(s) &= \mathbb{E}_{I_B} \left[\exp \left(-s \sum_{i \in \Phi_b^a} X_i r_{i,0}^{-\alpha} \right) \right] \\ &= \mathbb{E}_{\Phi_b^a} \left[\prod_{i \in \Phi_b^a} \mathbb{E}_{X_i} [\exp(-s X_i r_{i,0}^{-\alpha})] \right] \\ &\stackrel{(a)}{=} \exp \left(- \int_{\mathbb{R}^2} (1 - \chi) \Lambda(dr) \right) \\ &= \exp \left(-2\pi \lambda_b p_a \int_{r_{0,0}}^{\infty} (1 - \chi) r dr \right), \end{aligned} \quad (\text{C.2})$$

where (a) follows from the probability generating functional (PGFL) over PPP and $\chi = \int_0^\infty e^{-sxr^{-\alpha}} f_{X_i}(x) dx$ is the Laplace transform of X_i . By using [1, eq. (8.352.1)], we have

$$\chi = \begin{cases} (1 + wr^{-\alpha})^{-N}, & \text{if } \xi = 1, \\ \frac{(1-\xi)^{1-N}}{1+wr^{-\alpha}} - \sum_{n=0}^{N-2} \frac{\xi(1-\xi)^{n+1-N}}{(1+\xi wr^{-\alpha})^{n+1}}, & \text{otherwise,} \end{cases} \quad (\text{C.3})$$

where $w = \phi Ps$. Hence, we have

$$\mathcal{L}_{I_B}(s) = \exp \left(-2\pi\lambda_b p_a \left(\underbrace{\int_0^\infty (1-\chi)rdr}_{\tau_1} - \underbrace{\int_0^{r_0} (1-\chi)rdr}_{\tau_2} \right) \right). \quad (\text{C.4})$$

By using eq. (8) in [33], τ_1 can be derived as

$$\tau_1 = \begin{cases} w^\delta \kappa_{N+1}, & \text{if } \xi = 1, \\ \frac{w^\delta \kappa_2}{(1-\xi)^{N-1}} - \sum_{n=0}^{N-2} \frac{w^\delta \xi^{1+\delta} \kappa_{n+2}}{(1-\xi)^{N-n-1}}, & \text{otherwise.} \end{cases} \quad (\text{C.5})$$

When $\xi = 1$, by using [1, eq. (3.194.2)], we have

$$\tau_2 = r_0^2 \left[1 - \frac{\delta \varphi_0(N, wr_{0,0}^{-\alpha})}{(N+\delta)(wr_{0,0}^{-\alpha})^N} \right]. \quad (\text{C.6})$$

Similarly, when $\xi \neq 1$, we have

$$\tau_2 = r_{0,0}^2 \left[1 - \frac{\delta \varphi_0(1, wr_{0,0}^{-\alpha})}{(1+\delta)(1-\xi)^{N-1} wr_{0,0}^{-\alpha}} + \sum_{n=0}^{N-2} \frac{\delta \xi \varphi_0(n+1, \xi wr_{0,0}^{-\alpha})}{(n+1+\delta)(1-\xi)^{N-1-n} (\xi wr_{0,0}^{-\alpha})^{n+1}} \right]. \quad (\text{C.7})$$

Substituting the above results into (C.4), we have

$$\mathcal{L}_{I_B} \left(\frac{\bar{\gamma} r_{0,0}^\alpha}{\phi P} \right) = \exp \left(-\pi \lambda_b p_a k_0 r_{0,0}^2 \right), \quad (\text{C.8})$$

where k_0 is given by (5.10). By using the Leibniz formula, the p -th derivative of $\mathcal{L}_{I_B}(s)$ can be expressed in a recursive form given by

$$\begin{aligned} \mathcal{L}_{I_B}^{(p)}(s) = & \pi \lambda_b p_a \sum_{i=0}^{p-1} \binom{p-1}{i} \frac{(-1)^{p-i}}{(1-\xi)^{N-1}} \mathcal{L}_{I_B}^{(i)}(s) \int_{r_{0,0}^2}^{\infty} \left[\frac{(p-i)! (\phi P r^{-\frac{\alpha}{2}})^{p-i}}{(1+wr^{-\frac{\alpha}{2}})^{p-i+1}} \right. \\ & \left. - \sum_{n=0}^{N-2} \frac{\xi(n+p-i)!}{n!(1-\xi)^{-n}} \frac{(\xi \phi P r^{-\frac{\alpha}{2}})^{p-i}}{(1+\xi w r^{-\frac{\alpha}{2}})^{n+p-i+1}} \right] dr. \end{aligned} \quad (\text{C.9})$$

Let $x_p = (-1)^p s^p / p! \mathcal{L}_{I_B}^{(p)}(s)$ and use the variable transformation $r^{-\frac{\alpha}{2}} \rightarrow v$ we have

$$\begin{aligned} x_p = & \frac{\pi \lambda_b p_a \delta}{(1-\xi)^{N-1}} \sum_{i=0}^{p-1} \frac{p-i}{p} w^{p-i} \int_0^{r_{0,0}^{-\frac{\alpha}{2}}} \left[\frac{v^{p-i-\delta-1}}{(1+wv)^{p-i+1}} \right. \\ & \left. - \sum_{n=0}^{N-2} \binom{n+p-i}{n} (1-\xi)^n \frac{\xi^{p-i+1} v^{p-i-\delta-1}}{(1+\xi w v)^{n+p-i+1}} \right] dv x_i. \end{aligned} \quad (\text{C.10})$$

After some algebraic manipulations, we have

$$x_p = \pi \lambda_b p_a r_{0,0}^2 \sum_{i=0}^{p-1} \frac{p-i}{p} k_{p-i} x_i, \quad (\text{C.11})$$

where k_i is given by (5.12). Similar to the proof in [154], we can obtain Theorem 5.1.

C.2 Proof of Proposition 5.2

From Lemma 5.2, we know that when N approaches infinity, $\gamma_{u_0}^\infty = \frac{\phi P N r_{0,0}^{-\alpha}}{I_B^\infty}$. Following that, the asymptotic connection outage probability can be rewritten as

$$p_{to}^\infty = \mathbb{P}(\phi P N < \bar{\gamma} I_B^\infty r_{0,0}^\alpha) = \int_{\frac{\phi P N}{\bar{\gamma} r_{0,0}^\alpha}}^{\infty} f_{I_B^\infty}(x) dx, \quad (\text{C.12})$$

where

$$I_B^\infty = \sum_{i \in \Phi_b^a} \phi P \left[|\mathbf{h}_{i,0}^T \mathbf{w}_i|^2 + \xi(N-1) \right] r_{i,0}^{-\alpha}. \quad (\text{C.13})$$

Note that $f_{I_B^\infty}(x)$ is the inverse Laplace transform of $\mathcal{L}_{I_B^\infty}(s)$. Since the inverse Laplace transform is nontrivial to obtain, we adopt the log-normal approximations to approximate $f_{I_B^\infty}(x)$ [37]. Hence, the PDF of I_B^∞ can be approximated by

$$f_{I_B^\infty}(x) \approx \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2}\right), \quad (\text{C.14})$$

where μ and σ^2 given by (5.19) are the mean and variance of I_B^∞ , which can be derived by applying the Campbell's theorem. A similar proof can be found in [37]. Thus,

$$p_{to}^\infty = \int_0^\infty \bar{F}_{I_B^\infty}\left(\frac{\phi PN}{\bar{\gamma} r_0^\alpha}\right) f_{r_0}(r_0) dr_0. \quad (\text{C.15})$$

C.3 Proof of Theorem 5.2

Define $\gamma_{0,e_l} = \phi P \left[|\mathbf{g}_{0,e_l}^T \mathbf{w}_0|^2 - \bar{\gamma}_e \xi \|\mathbf{g}_{0,e_l}^T \mathbf{G}_0\|^2 \right]$, then the CDF of γ_{0,e_l} can be derived as

$$F_{\gamma_{0,e_l}}(x) = 1 - (1 + \bar{\gamma}_e \xi)^{1-N} e^{-\frac{x}{\phi P}}. \quad (\text{C.16})$$

Thus, for the k th Eve, we have

$$\begin{aligned} \mathbb{P}(\gamma_{e_l} < \bar{\gamma}_e) &= \mathbb{E}_{\Phi_b} \left[\mathbb{P}(\gamma_{0,e_l} < \bar{\gamma}_e r_{0,e_l}^\alpha I_{B,e_l}) \right] \\ &= 1 - (1 + \bar{\gamma}_e \xi)^{1-N} \mathbb{E}_{\Phi_b^a} \left[\int_0^\infty e^{-\frac{\bar{\gamma}_e r_{0,e_l}^\alpha t}{\phi P}} f_{I_{B,e_l}}(t) dt \right] \\ &= 1 - (1 + \bar{\gamma}_e \xi)^{1-N} \mathcal{L}_{I_{B,e_l}}\left(\frac{\bar{\gamma}_e r_{0,e_l}^\alpha}{\phi P}\right). \end{aligned} \quad (\text{C.17})$$

Similar to the derivation of $\mathcal{L}_{I_B}(s)$ in Appendix C.1, we have

$$\mathcal{L}_{I_{B,e_l}}(s) = \exp(-\pi \lambda_b p_a \varpi (\phi P s)^\delta). \quad (\text{C.18})$$

Then the secrecy outage probability can be expressed as

$$\begin{aligned} p_{so} &= 1 - \exp \left(-2\pi\lambda_e (1 + \bar{\gamma}_e \xi)^{1-N} \int_0^\infty \exp(-\Theta r^2) r dr \right) \\ &= 1 - \exp \left(-\frac{\pi\lambda_e}{\Theta} (1 + \bar{\gamma}_e \xi)^{1-N} \right). \end{aligned} \quad (\text{C.19})$$

C.4 Proof of Proposition 5.3

When N approaches infinity, the SIR at the k th Eve can be rewritten as

$$\gamma_{e_l}^\infty = \frac{\phi P |\mathbf{g}_{0,e_l}^T \mathbf{w}_0|^2 r_{0,e_l}^{-\alpha}}{\xi \phi P (N-1) r_{0,e_l}^{-\alpha} + I_{B,e_l}^\infty}, \quad (\text{C.20})$$

where

$$I_{B,e_l}^\infty = \sum_{i \in \Phi_b^a \setminus \{0\}} \phi P W r_{i,e_l}^{-\alpha}, \quad (\text{C.21})$$

and $W = \left[|\mathbf{g}_{i,e_l}^T \mathbf{w}_i|^2 + (\phi^{-1} - 1) \right]$. By using the PGFL over PPP and swapping the order of expectation, we have [33]

$$\mathcal{L}_{I_{B,e_l}^\infty}(s) = \exp \left(-\pi\lambda_b p_a \Gamma(1 - \delta) (\phi P s)^\delta \mathbb{E}[W^\delta] \right), \quad (\text{C.22})$$

where

$$\mathbb{E}[W^\delta] = \int_0^\infty (x + (\phi^{-1} - 1))^\delta e^{-x} dx = \Gamma(1 + \delta, (\phi^{-1} - 1)) e^{(\phi^{-1} - 1)}. \quad (\text{C.23})$$

Denote $\gamma_{0,e_l}^\infty = \phi P \left[|\mathbf{g}_{0,e_l}^T \mathbf{w}_0|^2 - \bar{\gamma}_e \xi (N-1) \right]$, then the CDF of γ_{0,e_l}^∞ is given by

$$F_{\gamma_{0,e_l}^\infty}(x) = 1 - e^{-\bar{\gamma}_e (N-1) \xi} e^{-\frac{x}{\phi P}}. \quad (\text{C.24})$$

Following the procedures in Appendix C.3, we have

$$\mathbb{P}(\gamma_{e_l}^\infty < \bar{\gamma}_e) = 1 - e^{-\bar{\gamma}_e (N-1) \xi} \exp(-\Theta^\infty r_{0,e_l}^2). \quad (\text{C.25})$$

Hence, the asymptotic secrecy outage probability is given by

$$\begin{aligned} p_{so}^\infty &= 1 - \exp \left(-2\pi\lambda_e e^{-\bar{\gamma}_e(N-1)\xi} \int_0^\infty \exp(-\Theta^\infty r^2) r dr \right) \\ &= 1 - \exp \left(-\frac{\pi\lambda_e}{\Theta^\infty} e^{-\bar{\gamma}_e(N-1)\xi} \right). \end{aligned} \quad (\text{C.26})$$

C.5 Proof of Theorem 5.3

Using Jensen's inequality, the average secrecy rate can be lower bounded by

$$R \geq \{\mathbb{E}[R_u] - \mathbb{E}[R_e]\}^+ \triangleq R_L. \quad (\text{C.27})$$

Denote $\bar{X}_0 = |\mathbf{h}_{0,0}^T \mathbf{w}_0|^2$, and $\bar{X}_i = \frac{X_i}{\phi P} r_{i,0}^\alpha$. Based on the lemma in [162], the average data rate of can be calculated as

$$\begin{aligned} R_u(r_{0,0}) &= \mathbb{E}_{\Phi_b} \left[\log \left(1 + \frac{\bar{X}_0 r_{0,0}^{-\alpha}}{\sum_{i \in \Phi_b^a \setminus \{0\}} \bar{X}_i r_{i,0}^{-\alpha}} \right) \middle| r_{0,0} \right] \\ &= \int_0^\infty \frac{1 - \mathbb{E}[e^{-z\bar{X}_0}]}{z} \mathbb{E} \left[e^{-z \sum_{i \in \Phi_b \setminus \{0\}} \bar{X}_i r_{0,0}^\alpha r_{i,0}^{-\alpha}} \right] dz \\ &= \int_0^\infty \frac{1 - \mathbb{E}[e^{-z\bar{X}_0}]}{z} \mathbb{E} \left[\prod_{i \in \Phi_b \setminus \{0\}} \tilde{\chi} \right] dz \\ &= \int_0^\infty \frac{1 - \frac{1}{(1+z)^N}}{z} \exp \left(-2\pi\lambda_b p_a \int_{r_{0,0}}^\infty (1 - \tilde{\chi}) r dr \right) dz \\ &= \int_0^\infty \frac{1 - \frac{1}{(1+z)^N}}{z} \exp \left(-\pi\lambda_b p_a r_{0,0}^2 \Xi \right) dz, \end{aligned} \quad (\text{C.28})$$

where $\tilde{\chi}$ can be obtained by replacing w with $zr_{0,0}^\alpha$ in χ , $\Xi = z^\delta \int_{z^{-\delta}}^\infty \vartheta du$, and ϑ is given by

$$\vartheta = \begin{cases} 1 - (1 + u^{-\frac{\alpha}{2}})^{-N}, & \text{if } \xi = 1, \\ 1 - \frac{(1-\xi)^{1-N}}{1+u^{-\frac{\alpha}{2}}} + \sum_{n=0}^{N-2} \frac{\xi(1-\xi)^{n+1-N}}{(1+\xi u^{-\frac{\alpha}{2}})^{n+1}}, & \text{otherwise.} \end{cases} \quad (\text{C.29})$$

Following that, we have

$$\begin{aligned} R_u &= \mathbb{E}_{r_{0,0}} [R_u(r_{0,0})] = \int_0^\infty R_u(r) 2\pi \lambda_b r e^{-\pi \lambda_b r^2} dr \\ &= \int_0^\infty \frac{1 - (1+z)^{-N}}{z} \frac{1}{1 + p_a \Xi} dz. \end{aligned} \quad (\text{C.30})$$

Based on the asymptotic SOP in (5.31), the eavesdropped rate can be expressed as

$$R_e \approx \int_0^\infty \log(1+z) f_{\gamma_E}(z) dz = \int_0^\infty \frac{1 - F(z)}{1+z} dz, \quad (\text{C.31})$$

where $F(z)$ is given by (5.39).

C.6 Proof of Proposition 5.4

Due to the existence of guard zone, the interference from the active BSs will be much larger than that from the jammers, i.e., $\Theta_j \ll \Theta_b$ will always hold. Thus, the secrecy probability for the adaptive eavesdropping can be approximated by

$$p_{so}^A \approx \frac{\lambda_e}{\lambda_e + \Theta_b} (1 + \bar{\gamma}_e \xi)^{1-N} \leq \frac{\lambda_e}{\lambda_e + \Theta_b (1 + \bar{\gamma}_e \xi)^{N-1}}, \quad (\text{C.32})$$

where the equality holds when $\xi = 0$. Denote

$$x = \frac{\lambda_e (1 + \bar{\gamma}_e \xi)^{1-N}}{\Theta_b}, \quad (\text{C.33})$$

then $p_{st}^A < p_{st}^0$ is equivalent to $(x+1)e^{-x} > \theta$. Denote $f(x) = (x+1)e^{-x}$, when $f(x) = \theta$, we have

$$x_0 = -W_p(-\theta e^{-1}) - 1 \cup -W_m(-\theta e^{-1}) - 1, \quad (\text{C.34})$$

where $W_p(\cdot)$ and $W_m(\cdot)$ are the real-valued principle branch and other branch of Lambert W-function, respectively. Since $\theta < 1$, we reject the first branch and

$$x_0 = -W_m(-\theta e^{-1}) - 1. \quad (\text{C.35})$$

Since $f'(x) = -xe^{-x} < 0$, the solution of $p_{st}^A < p_{st}^0$ is $x < x_0$, which completes the proof.

Appendix D

Proofs of Propositions in Chapter 6

D.1 Derivation of Equation (6.32)

Similar to the proof in [167] and [166], we approximate the large-scale fading coefficients of interfering cells by their means. Thus,

$$\begin{aligned}
 \left| \bar{\mathbf{h}}_{00}^{(0)T} \mathbf{y}_{00}^{(0)} \right|^2 &\stackrel{(a)}{=} \frac{P_p (X_{00}^{(0)})^2}{(\Sigma_{00}^{(0)})^2} \left| \mathbf{y}_{00}^{(0)} \right|^4 \\
 &\stackrel{(b)}{\approx} \frac{P_p (X_{00}^{(0)})^2}{(\Sigma_{00}^{(0)})^2} \mathbb{E} \left| \mathbf{y}_{00}^{(0)} \right|^4 \\
 &\stackrel{(c)}{=} P_p (X_{00}^{(0)})^2 (N_\mu^2 + N_\mu),
 \end{aligned} \tag{D.1}$$

where (a) follows from (6.5), (b) follows from the fact that $\left| \mathbf{y}_{00}^{(0)} \right|^4 \rightarrow \mathbb{E} \left| \mathbf{y}_{00}^{(0)} \right|^4$ when $N_\mu \rightarrow \infty$, (c) follows from the fact that $\mathbb{E} \left| \mathbf{y}_{00}^{(0)} \right|^4 = (N_\mu^2 + N_\mu)(\Sigma_{00}^{(0)})^2$. For the interference term caused by channel estimation error, we have

$$\begin{aligned}
 \mathbb{E} \left| \hat{\mathbf{h}}_{00}^{(0)T} \mathbf{y}_{00}^{(0)} \right|^2 &= \frac{1}{N_\mu} \mathbb{E} \left| \hat{\mathbf{h}}_{00}^{(0)} \right|^2 \mathbb{E} \left| \mathbf{y}_{00}^{(0)} \right|^2 \\
 &= \frac{1}{N_\mu} N_\mu X_{00}^{(0)} \left(1 - \frac{P_p X_{00}^{(0)}}{\Sigma_{00}^{(0)}} \right) N_\mu \Sigma_{00}^{(0)} \\
 &= N_\mu X_{00}^{(0)} \Delta_0.
 \end{aligned} \tag{D.2}$$

Similarly, for the inter-user interference, we have

$$\sum_{k=1}^{K-1} \frac{|\mathbf{y}_{00}^{(0)}|^2}{|\mathbf{y}_{00}^{(k)}|^2} \mathbb{E} \left| \mathbf{h}_{00}^{(0)T} \mathbf{y}_{00}^{(k)} \right|^2 = \sum_{k=1}^{K-1} N_\mu X_{00}^{(0)} \Sigma_{00}^{(0)}. \quad (\text{D.3})$$

For the interference from other BSs, we have

$$\begin{aligned} \mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{y}_{ii}^{(k)} \right|^2 &= \mathbb{E} \left| P_p^{\frac{1}{2}} \sum_{j \in \Phi_\mu} \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ij}^{(k)} + P_e^{\frac{1}{2}} \sum_{l \in \Phi_e^{(k)}} \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ie}^{(l)} + \mathbf{h}_{i0}^{(0)T} \mathbf{n}_0^{(k)} \right|^2 \\ &\stackrel{(d)}{=} P_p \sum_{j \in \Phi_\mu} \mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ij}^{(k)} \right|^2 + P_e \sum_{l \in \Phi_e^{(k)}} \mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ie}^{(l)} \right|^2 + N_\mu X_{i0}^{(0)} \sigma^2, \end{aligned} \quad (\text{D.4})$$

where (d) holds due to the fact that $\mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ij}^{(0)}$ and $\mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ie}^{(l)}$ are uncorrelated zero-mean random variables. Note that when $k = j = 0$, we have

$$\mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ij}^{(k)} \right|^2 = \mathbb{E} \left| \mathbf{h}_{i0}^{(0)} \right|^4 = (N_\mu^2 + N_\mu) (X_{i0}^{(0)})^2, \quad (\text{D.5})$$

when $(k, j) \neq (0, 0)$, we have

$$\mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ij}^{(k)} \right|^2 = N_\mu X_{i0}^{(0)} X_{ij}^{(k)}. \quad (\text{D.6})$$

Similarly,

$$\mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{h}_{ie}^{(l)} \right|^2 = N_\mu X_{i0}^{(0)} X_{ie}^{(l)}. \quad (\text{D.7})$$

Note that when N_μ approaches infinity, $\left| \mathbf{h}_{i0}^{(0)T} \mathbf{V}_i \right|^2 \rightarrow (N - K) X_{i0}^{(0)}$, thus

$$\begin{aligned} &\sum_{k=0}^{K-1} \frac{1}{|\mathbf{y}_{ii}^{(k)}|^2} \mathbb{E} \left| \mathbf{h}_{i0}^{(0)T} \mathbf{y}_{ii}^{(k)} \right|^2 + K \xi \left| \mathbf{h}_{i0}^{(0)T} \mathbf{V}_i \right|^2 \\ &= P_p N_\mu \frac{(X_{i0}^{(0)})^2}{\Sigma_{ii}^{(0)}} + K X_{i0}^{(0)} + \xi K (N - K) X_{i0}^{(0)}, \end{aligned} \quad (\text{D.8})$$

By combining the above results, we can obtain (6.32).

D.2 Proof of Proposition 6.1

With the exclusion ball model and by using the Campbell's theorem [125], we have

$$\mathbb{E} \left[\sum_{j \in \Phi_\mu \setminus \{0\}} X_{ij}^{(0)} \right] = 2\pi\lambda_\mu c_\mu \int_{R_{eq}}^{\infty} x^{-\alpha_\mu} x dx = a_1. \quad (\text{D.9})$$

Similarly, for the Eves, we have $\mathbb{E} \left[\sum_{l \in \Phi_e^{(0)}} X_{0e}^{(l)} \right] = a_2$. Hence, we have $\bar{\Delta}_0 = \mathbb{E}\Delta_0 = P_p a_1 + P_e a_2 + \sigma^2$, $\mathbb{E}\Sigma_{00}^{(0)} = P_p \mathbb{E}X_{00}^{(0)} + \bar{\Delta}_0$. For the interference from nearby MBSs, by using the Campbell's theorem, we have

$$\mathbb{E} \left[\sum_{i \in \Phi_\mu \setminus 0} (X_{i0}^{(0)})^2 \right] = 2\pi\lambda_\mu c_\mu^2 \int_{R_0}^{\infty} x^{-2\alpha_\mu} x dx = a_3 R_0^{2-2\alpha_\mu} \quad (\text{D.10})$$

and

$$\mathbb{E} \left[\sum_{i \in \Phi_\mu \setminus 0} X_{i0}^{(0)} \right] = 2\pi\lambda_\mu c_\mu \int_{R_0}^{\infty} x^{-\alpha_\mu} x dx = a_4 R_0^{2-\alpha_\mu}. \quad (\text{D.11})$$

Combining the above results, we have $\mathbb{E}[\Sigma_{00}^{(0)} \Delta_1] = P_p N_\mu a_3 R_0^{2-2\alpha_\mu}$ and $\mathbb{E}[\Delta_2] = K a_4 R_0^{2-\alpha_\mu}$. Hence, the SINR can be rewritten as

$$\text{SINR}_0^\mu \approx \frac{A_0}{A_1 R_0^\alpha + A_2 R_0^2 + A_3 R_0^{2+\alpha_\mu} + A_4}. \quad (\text{D.12})$$

Then conditioning on R_0 , the coverage probability can be calculated by

$$\begin{aligned} & \mathbb{P}(\text{SINR}_0^\mu > T \mid R_0) \\ &= \mathbb{P} \left(1 > \frac{T(A_1 R_0^\alpha + A_2 R_0^2 + A_3 R_0^{2+\alpha_\mu}) + A_4}{A_0} \right) \\ &\stackrel{(e)}{\approx} \mathbb{P} \left(u > \frac{T(A_1 R_0^\alpha + A_2 R_0^2 + A_3 R_0^{2+\alpha_\mu}) + A_4}{A_0} \right) \\ &\stackrel{(f)}{=} \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} \exp \left(-\frac{nvTA_4}{A_0} \right) \exp \left(-\frac{nvT(A_1 R_0^\alpha + A_2 R_0^2 + A_3 R_0^{2+\alpha_\mu})}{A_0} \right), \end{aligned} \quad (\text{D.13})$$

where in (e), u is a normalized gamma random variable with shape parameter N and the approximation is due to the fact that a normalized gamma variable converges to identity when its shape parameter goes to infinity. Note that (f) follows from the Alzer's inequality. By de-conditioning on R_0 , we can directly obtain (6.33).

D.3 Proof of Proposition 6.3

Similar to the proof in Appendix D.2, we have

$$\left| \mathbf{g}_{0e}^{(l)T} \mathbf{y}_{00}^{(0)} \right|^2 = N_\mu X_{0e}^{(l)} \Sigma_{00}^{(0)} + \mathbb{1}(S_{e_l}) N_\mu^2 P_e (X_{0e}^{(l)})^2, \quad (\text{D.14})$$

where $\mathbb{1}(S_{e_l}) = 1$ when $e_l \in \Phi_e^{(0)}$, else $\mathbb{1}(S_{e_l}) = 0$. Note that since $\left| \mathbf{g}_{ie}^{(l)T} \mathbf{V}_i \right|^2 \xrightarrow{N_\mu \rightarrow \infty} (N - K) X_{ie}^{(l)}$, the SIR of the l th Eve in (6.50) can be expressed as

$$\text{SIR}_{e_l}^\mu = \frac{N_\mu X_{0e}^{(l)} \Sigma_{00}^{(0)} + \mathbb{1}(S_{e_l}) N_\mu^2 P_e (X_{0e}^{(l)})^2}{\xi K (N - K) \Sigma_{00}^{(0)} \sum_{i \in \Phi_\mu} X_{ie}^{(l)}}. \quad (\text{D.15})$$

Equation (D.15) can be further simplified as

$$\begin{aligned} \text{SIR}_{e_l}^\mu &= \frac{\mathbb{1}(S_{e_l}) N_\mu P_e c_\mu^2 (R_{0e}^{(l)})^{-2\alpha_\mu} + \bar{\Delta} c_\mu (R_{0e}^{(l)})^{-\alpha_\mu}}{\xi_0 K a_4 \bar{\Delta}} \\ &\leq \frac{B_2 (R_{0e}^{(l)})^{-2\alpha_\mu} + B_1 (R_{0e}^{(l)})^{-\alpha_\mu}}{B_0}. \end{aligned} \quad (\text{D.16})$$

Hence, for the l th Eve we have

$$\begin{aligned} \mathbb{P}(\text{SIR}_{e_l}^\mu > x) &= \mathbb{P}\left(1 > \frac{B_0 x}{B_1 (R_{0e}^{(l)})^{-\alpha_\mu} + B_2 (R_{0e}^{(l)})^{-2\alpha_\mu}}\right) \\ &= \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} \exp\left(-\frac{nv B_0 x}{B_1 (R_{0e}^{(l)})^{-\alpha_\mu} + B_2 (R_{0e}^{(l)})^{-2\alpha_\mu}}\right), \end{aligned} \quad (\text{D.17})$$

where the last equation is obtained by approximating the unit variable as a gamma variable with unit mean and shape parameter N and using the Alzer's inequality.

Following that, the secrecy probability can be expressed as

$$\begin{aligned}
 \mathbb{P}(\text{SIR}_E^\mu < T_e) &= \mathbb{P}\left(\max_{e_l \in \Phi_E} \text{SIR}_{e_l}^\mu < T_e\right) \\
 &= \mathbb{E}_{\Phi_E} \left[\prod_{e_l \in \Phi_E} \mathbb{P}(\text{SIR}_{e_l}^\mu < T_e) \right] \\
 &\stackrel{(g)}{\leq} \exp \left(-2\pi\lambda_E \int_0^\infty \sum_{n=1}^N (-1)^{n+1} e^{-\frac{nvT_e B_0}{B_1 R^{-\alpha\mu} + B_2 R^{-2\alpha\mu}}} R dR \right),
 \end{aligned} \tag{D.18}$$

where (g) follows from the probability generating functional (PGFL) over PPP, and the equality holds when $K = 1$, i.e., all the Eves share the same pilot with the typical user.

D.4 Proof of Proposition 6.4

Due to the zero side lobe of the SBS, $D_{BS} = G_{BS}$ when the beam of e_l is aligned with the transmit beam of SBS, otherwise $D_{BS} = 0$. We consider the two different cases separately:

Case 1: when the beams between the SBS and the typical user are successfully aligned, we denote the set of Eves whose AOA lie $\mathcal{R}_0$ as $\Phi_e^{(0)}$ with intensity $\frac{\theta_{BS}}{\pi} \lambda_E$.

$$\mathbb{P}(\text{SNR}_{E,SA}^m \leq T_e) \approx \mathbb{P}\left(\max_{l \in \Phi_e^{(0)}} X_{0e}^{(l)} \leq \frac{1}{\mu}\right) \stackrel{(h)}{=} e^{-\pi \frac{\theta_{BS}}{\pi} \lambda_E \Lambda(\mu)}, \tag{D.19}$$

where (h) is derived by using the CCDF of the path loss of the Eve, similar to Lemma 6.1.

Case 2: when the beams between the SBS and the typical user are unsuccessfully aligned, i.e., the transmit beam of SBS is aligned with one of the Eves, then we have

$$\mathbb{P}(\text{SNR}_{E,UA}^m \leq T_e) \approx \mathbb{P}\left(\max_{l \in \Phi_E} X_{0e}^{(l)} \leq \frac{1}{\mu}\right) = e^{-\pi \lambda_E \Lambda(\mu)}. \tag{D.20}$$

Thus,

$$p_{sec}^m = \mathbb{P}(\text{SINR}_{E,SA}^m < T_e \mid \text{SA})\mathbb{P}(\text{SA}) + \mathbb{P}(\text{SINR}_{E,UA}^m < T_e \mid \text{UA})\mathbb{P}(\text{UA}). \quad (\text{D.21})$$

By substituting (D.20) and (D.21), and the success probability in (6.40), we can obtain (6.54). This completes the proof.

Author's Publications

The following is a list of publications in refereed journals and conference proceedings produced during my Ph.D. candidature. In some cases, the journal papers contain partial material overlapping with the conference publications.

Journals:

1. **W. Wang**, K. C. Teh, S. Luo and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach," *IEEE Trans. Commun.*, Major Revision.
2. **W. Wang**, K. C. Teh, and K. H. Li, "On the impact of adaptive eavesdroppers in multi-antenna cellular networks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 269-279, Feb. 2018.
3. **W. Wang**, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470-1482, Jun. 2017.
4. **W. Wang**, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106-109, Feb. 2017.
5. **W. Wang**, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505 - 515, Mar. 2017.
6. **W. Wang**, K. C. Teh, and K. H. Li, "Relay selection for secure successive

AF relaying networks with untrusted nodes,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2466-2476, Nov. 2016.

7. **W. Wang**, K. C. Teh, and K. H. Li, “Generalized relay selection for improved security in cooperative DF relay networks,” *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 28-31, Feb. 2016.

Conference:

1. **W. Wang**, K. C. Teh, S. Luo, and K. H. Li, “Secure transmission in MI-SOME wiretap channels with half and full-duplex active eavesdroppers,” *IEEE Globecom*, Singapore, Dec., 2017.
2. **W. Wang**, K. C. Teh, and K. H. Li, “Interference exploitation for enhanced security in D2D spectrum sharing networks,” *IEEE ICC*, Paris, France, May, 2017.
3. **W. Wang**, K. C. Teh, and K. H. Li, “Securing cooperative AF relaying networks with untrustworthy relay nodes,” *IEEE Globecom*, Washington D.C., US, Dec., 2016.

Bibliography

- [1] I. Gradshteyn, I. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic Press, 2007.
- [2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, “What will 5G be?” *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, 2014.
- [3] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 2016.
- [4] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, “Five disruptive technology directions for 5G,” *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.
- [5] J. L. Massey, “An introduction to contemporary cryptology,” *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May. 1988.
- [6] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Wireless Commun.*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
- [7] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, “A key management scheme for wireless sensor networks using deployment knowledge,” in *Proc. IEEE Conference on Computer Communications (INFOCOM)*, Hong Kong, Mar. 2004, pp. 586–597.
- [8] W. Trappe, “The challenges facing physical layer security,” *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
- [9] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Comm. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.
- [10] A. Mukherjee, “Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints,” *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
- [11] N. Yang, L. Wang, G. Geraci, M. ElKashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

- [12] X. Chen, D. W. K. Ng, W. Gerstacker, and H.-H. Chen, “A survey on multiple-antenna techniques for physical layer security,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, Second quarter 2017.
- [13] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, Jan. 2017.
- [14] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
- [15] K. Ren, H. Su, and Q. Wang, “Secret key generation exploiting channel characteristics in wireless communications,” *IEEE Wireless Commun.*, vol. 18, no. 4, Aug. 2011.
- [16] Q. Wang, K. Xu, and K. Ren, “Cooperative secret key generation from phase estimation in narrowband fading channels,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.
- [17] K. Zeng, “Physical layer key generation in wireless networks: Challenges and opportunities,” *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
- [18] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, “Experimental study on key generation for physical layer security in wireless communications,” *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.
- [19] X. He and A. Yener, “Two-hop secure communication using an untrusted relay: A case for cooperative jamming,” in *Proc. IEEE Global Telecommunications Conference*. New Orleans, LO, USA: IEEE, 2008, pp. 1–5.
- [20] —, “Cooperation with an untrusted relay: A secrecy perspective,” *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
- [21] —, “Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay,” *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.
- [22] —, “End-to-end secure multi-hop communication with untrusted relays,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.
- [23] L. Sun, T. Zhang, L. Yubo, and N. Hao, “Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.
- [24] J.-B. Kim, J. Lim, and J. M. Cioffi, “Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3866–3876, Jul. 2015.
- [25] J. Li and A. P. Petropulu, “On ergodic secrecy rate for Gaussian MISO wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

-
- [26] V. U. Prabhu and M. R. 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.
 - [27] N. Li, X. Tao, and J. Xu, "Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 969–972, June 2014.
 - [28] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large system analysis of artificial noise assisted communication in the multiuser downlink: Ergodic secrecy sum-rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.
 - [29] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.
 - [30] N. Yang, M. ElKashlan, T. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. on Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.
 - [31] Z. Li, P. Mu, B. Wang, and X. Hu, "Optimal semi-adaptive transmission with artificial-noise-aided beamforming in MISO wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7021–7035, Sep. 2016.
 - [32] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.
 - [33] 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.
 - [34] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
 - [35] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.
 - [36] 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, Jun. 2013.
 - [37] 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, Jun. 2014.

- [38] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.
- [39] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2155–2163, Mar. 2016.
- [40] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.
- [41] L. Yang, J. Chen, H. Jiang, S. Vorobyov, and H. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 26–42, Jan. 2017.
- [42] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
- [43] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.
- [44] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.
- [45] L. J. Rodriguez, N. Tran, and T. Le-Ngoc, "Optimal power allocation schemes for the single AF relay and jammer wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3042–3056, May 2016.
- [46] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.
- [47] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.
- [48] 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.
- [49] E. Tekin, "The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming," in *Proc. IEEE Information Theory and Applications Workshop*. La Jolla, CA, USA: IEEE, Jan. 2007, pp. 404–413.
- [50] 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.

-
- [51] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
 - [52] 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.
 - [53] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
 - [54] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.
 - [55] W. Wang, K. C. Teh, and K. H. Li, "Generalized relay selection for improved security in cooperative DF relay networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 28–31, Feb. 2016.
 - [56] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
 - [57] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
 - [58] Y. Yang, Q. Li, W. K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.
 - [59] H.-M. Wang, "Joint cooperative beamforming jamming and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.
 - [60] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, Jul. 2012.
 - [61] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189–2203, Apr. 2014.
 - [62] 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.
 - [63] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

- [64] K. H. Park, T. Wang, and M. S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.
- [65] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal. Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.
- [66] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.
- [67] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.
- [68] H. Mikko, K. Dani, H. Timo, A.-R. Emilio, V. Sathya, R. Taneli, A. Lauri, I. Clemens, H. Katsuyuki, W. Risto, and V. Mikko, "Recent advances in antenna design and interference cancellation algorithms for in-band full duplex relays," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 91–101, May 2015.
- [69] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
- [70] O. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1075–1078, June 2014.
- [71] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525 – 528, Apr. 2015.
- [72] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure beamforming in MISO full-duplex two-way secure communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 408–414, Jan. 2016.
- [73] H. A. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. J. Smith, "Low-complexity end-to-end performance optimization in MIMO full-duplex relay systems," *IEEE Trans. Wirel. Commun.*, vol. 13, no. 2, pp. 913–927, Feb 2014.
- [74] L. Wang, M. El Kashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.
- [75] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of non-regenerative network with untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2703–2709, Jun. 2015.

-
- [76] 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.
- [77] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.
- [78] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [79] 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 Proces. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.
- [80] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [81] —, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [82] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.
- [83] 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.
- [84] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
- [85] 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.
- [86] 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.
- [87] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.
- [88] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

- [89] 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.
- [90] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
- [91] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2096–2099, 2013.
- [92] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.
- [93] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.
- [94] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
- [95] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, June 2013.
- [96] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.
- [97] 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.
- [98] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.
- [99] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.
- [100] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up mimo: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, 2013.

-
- [101] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
 - [102] 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, Sep. 2014.
 - [103] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.
 - [104] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.
 - [105] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.
 - [106] 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.
 - [107] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.
 - [108] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Secure transmission for relay wiretap channels in the presence of spatially random eavesdroppers," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, San Diego, USA, 2015, pp. 1–6.
 - [109] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.
 - [110] Y. Deng, L. Wang, M. ElKashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.
 - [111] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.
 - [112] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

- [113] 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.
- [114] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.
- [115] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *International Conference on Ad Hoc Networks*. Springer, 2013, pp. 146–161.
- [116] J. Y. Ryu, J. Lee, and T. Q. Quek, "Transmission strategy against opportunistic attack for MISO secure channels," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2304–2307, Nov. 2016.
- [117] L. Li, A. Petropulu, and Z. Chen, "MIMO secret communications against an active eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2387–2401, Oct. 2017.
- [118] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [119] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [120] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [121] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *IEEE International Symposium on Information Theory (ISIT), 2007*. IEEE, 2007, pp. 2471–2475.
- [122] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
- [123] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, 2014.
- [124] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Queensland, Australia, Aug. 2001, pp. 87–89.
- [125] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge University Press, 2012.
- [126] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjørungnes, *Game theory in wireless and communication networks: Theory, models, and applications*. Cambridge, U.K.: Cambridge University Press, 2012.

-
- [127] R. D. Yates, "A framework for uplink power control in cellular radio systems," *IEEE J. Sel. Areas Commun.*, vol. 13, no. 7, pp. 1341–1347, Sep. 1995.
 - [128] H. Elshaer, M. N. Kulkarni, F. Boccardi, J. G. Andrews, and M. Dohler, "Downlink and uplink cell association with traditional macrocells and millimeter wave small cells," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6244–6258, Sep. 2016.
 - [129] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.
 - [130] S. Singh, M. N. Kulkarni, A. Ghosh, and J. G. Andrews, "Tractable model for rate in self-backhauled millimeter wave cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2196–2211, Oct. 2015.
 - [131] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.
 - [132] M. Di Renzo, "Stochastic geometry modeling and analysis of multi-tier millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5038–5057, Sep. 2015.
 - [133] T. Bai, R. Vaze, and R. W. Heath, "Analysis of blockage effects on urban cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 5070–5083, Sep. 2014.
 - [134] A. Alkhateeb, O. El Ayach, G. Leus, and R. W. Heath, "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831–846, Oct. 2014.
 - [135] A. Alkhateeb, Y.-H. Nam, M. S. Rahman, J. Zhang, and R. W. Heath, "Initial beam association in millimeter wave cellular systems: Analysis and design insights," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2807–2821, May 2017.
 - [136] C. Liu, M. Li, S. V. Hanly, I. B. Collings, and P. Whiting, "Millimeter wave beam alignment: Large deviations analysis and design insights," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1619–1631, July 2017.
 - [137] S. H. Kim, T. V. K. Chaitanya, T. Le-Ngoc, and J. Kim, "Rate maximization based power allocation and relay selection with IRI consideration for two-path AF relaying," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6012–6027, Nov. 2015.
 - [138] C. Wang and H. M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.
 - [139] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

- [140] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.
- [141] I. Krikidis, H. Suraweera, P. J. Smith, C. Yuen *et al.*, "Full-duplex relay selection for amplify-and-forward cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4381–4393, Dec. 2012.
- [142] H.-C. Yang and M. S. Alouini, *Order Statistics in Wireless Communications: Diversity, Adaptation, and Scheduling in MIMO and OFDM Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
- [143] T. Van Nguyen and H. Shin, "Power allocation and achievable secrecy rates in MISOME wiretap channels," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1196–1198, Nov. 2011.
- [144] Q. Xiong, Y. Gong, Y. C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357–360, Aug. 2014.
- [145] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.
- [146] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
- [147] 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.
- [148] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.
- [149] G. Alefeld and J. McNamee, *Numerical Methods for Roots of Polynomials. Part I*. The Netherlands: Elsevier, 2010.
- [150] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications*. New York: Springer, 2011.
- [151] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [152] F. W. Olver, *NIST Handbook of Mathematical Functions*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
- [153] D. P. Bertsekas, *Nonlinear Programming*. Belmont, Massachusetts: Athena Scientific, 1999.

-
- [154] C. Li, J. Zhang, and K. B. Letaief, "Throughput and energy efficiency analysis of small cell networks with multi-antenna base stations," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2505–2517, May 2014.
 - [155] C. Li, J. Zhang, M. Haenggi, and K. B. Letaief, "User-centric intercell interference nulling for downlink small cell networks," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1419–1431, Apr. 2015.
 - [156] C. Li, J. Zhang, J. G. Andrews, and K. B. Letaief, "Success probability and area spectral efficiency in multiuser MIMO HetNets," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1544–1556, Apr. 2016.
 - [157] Z. Chen, L. Qiu, and X. Liang, "Area spectral efficiency analysis and energy consumption minimization in multi-antenna Poisson distributed networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4862–4874, Jul. 2016.
 - [158] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. ElKashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.
 - [159] C.-H. Liu and L.-C. Wang, "Optimal cell load and throughput in green small cell networks with generalized cell association," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1058–1072, May 2016.
 - [160] H. Alzer, "On some inequalities for the incomplete Gamma function," *Math. Comput.*, vol. 66, no. 218, pp. 771–778, Apr. 1997.
 - [161] F. Baccelli, B. Blaszczyzyn, and P. Muhlethaler, "An Aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.
 - [162] K. A. Hamdi, "A useful lemma for capacity analysis of fading interference channels," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 411–416, Feb. 2010.
 - [163] R. Steele and L. Hanzo, *Mobile Radio Communications: Second and Third Generation Cellular and WATM Systems*. Chichester, U.K.: John Wiley, 1999.
 - [164] R. Lucchetti, F. Mignanego, and G. Pieri, "Existence theorems of equilibrium points in Stackelberg," *Optimization*, vol. 18, no. 6, pp. 857–866, 1987.
 - [165] S. Singh, X. Zhang, and J. G. Andrews, "Joint rate and SINR coverage analysis for decoupled uplink-downlink biased cell associations in HetNets," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5360–5373, Oct. 2015.
 - [166] Q. Zhang, H. H. Yang, T. Q. S. Quek, and J. Lee, "Heterogeneous cellular networks with LoS and NLoS transmissions-The role of massive MIMO and small cells," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 7996–8010, Dec. 2017.
 - [167] T. Bai and R. W. Heath, "Analyzing uplink SINR and rate in massive MIMO systems using stochastic geometry," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4592–4606, Nov. 2016.

- [168] E. Björnson, L. Sanguinetti, and M. Kountouris, “Deploying dense networks for maximal energy efficiency: Small cells meet massive MIMO,” *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 832–847, Apr. 2016.
- [169] T. S. 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.
- [170] R. B. Waterhouse, D. Novak, A. Nirmalathas, and C. Lim, “Broadband printed sectorized coverage antennas for millimeter-wave wireless applications,” *IEEE Trans. Antennas Propag.*, vol. 50, no. 1, pp. 12–16, Jan. 2002.
- [171] Y. Li, J. G. Andrews, F. Baccelli, T. D. Novlan, and J. C. Zhang, “Design and analysis of initial access in millimeter wave cellular networks,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6409 – 6425, Oct. 2017.
- [172] T. Bai and R. W. Heath, “Analysis of beam sweep channel estimation in MmWave massive MIMO networks,” in *proc. IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Washington, DC, USA, Dec 2016, pp. 615–619.
- [173] W. Wang, K. C. Teh, and K. H. Li, “Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels,” *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505–515, Mar. 2017.
- [174] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, “Secure transmissions in millimeter wave systems,” *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.
- [175] W. Wang, K. C. Teh, and K. Li, “Artificial noise aided physical layer security in multi-antenna small-cell networks,” *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.
- [176] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, “Jamming-resistant receivers for the massive MIMO uplink,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.
- [177] T. Lv, H. Gao, and S. Yang, “Secrecy transmit beamforming for heterogeneous networks,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.
- [178] H. H. Yang, G. Geraci, T. Q. Quek, and J. G. Andrews, “Cell-edge-aware precoding for downlink massive MIMO cellular networks,” *IEEE Trans. Signal Process.*, vol. 65, no. 13, pp. 3344–3358, Jul.
- [179] T. X. Tran and K. C. Teh, “Spectral and energy efficiency analysis for SLNR precoding in massive MIMO systems with imperfect CSI,” *IEEE Trans. Wireless Commun.*, to appear.