

Wireless Physical Layer Security: Towards Practical Assumptions and Requirements

Biao He

June 2016

A Thesis Submitted for the Degree of
Doctor of Philosophy
of The Australian National University



Research School of Engineering
College of Engineering and Computer Science
The Australian National University

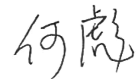
© Copyright by Biao He 2016

Declaration

The contents of this thesis are the results of original research and have not been submitted for a higher degree to any other university or institution.

Much of the work in this thesis has been published or has been submitted for publication as journal papers or conference proceedings.

The research work presented in this thesis has been performed jointly with Dr. Xiangyun Zhou (The Australian National University), Dr. Nan Yang (The Australian National University), Prof. Thushara D. Abhayapala (The Australian National University), Prof. Jinhong Yuan (The University of New South Wales), and Prof. A. Lee Swindlehurst (University of California, Irvine). The substantial majority of this work was my own.



Biao He
Research School of Engineering,
College of Engineering and Computer Science,
The Australian National University,
Canberra, ACT 2601,
Australia.

Acknowledgments

I would like to express my sincere gratitude to my principal supervisor Dr. Xiangyun Zhou for his guidance, support, and encouragement throughout my entire PhD journey. I could not imagine having a better advisor and mentor for my PhD study. I would also like to thank the chair of my supervision panel Dr. Salman Durrani for his valuable advice on my thesis.

My sincere thanks go to Dr. Nan Yang (The Australian National University), Prof. Thushara D. Abhayapala (The Australian National University), and Prof. A. Lee Swindlehurst (University of California, Irvine) for their constructive guidance and suggestion on some of the work produced during my PhD study. I would also like to thank Prof. Parastoo Sadeghi (The Australian National University) and Prof. Mark C. Reed (The University of New South Wales, Canberra) for their valuable career advice.

I would like to thank Prof. Jinhong Yuan from The University of New South Wales, Prof. Zhu Han from University of Houston, Prof. Lingyang Song from Peking University, and Prof. Zesong Fei from Beijing Institute of Technology for kindly welcoming me to visit their groups. The valuable discussion with Prof. Yuan led to part of the work presented in this thesis and the precious discussion with Prof. Han stimulated many interesting ideas in my work.

Thanks must go to The Australian National University for providing the PhD scholarship and a great environment supporting my research. It is my great pleasure to study in the Applied Signal Processing (ASP) group at the Research School of Engineering. I would like to thank all my friends at the ASP group who made my study here fun and enjoyable.

I would like to give my most sincere thanks to my parents for their continuous support in general. Last but not the least, I would like to give my special thanks to my partner Yimeng Jiang for her company, encouragement, and understanding.

Abstract

The current research on physical layer security is far from implementations in practical networks, arguably due to impractical assumptions in the literature and the limited applicability of physical layer security. Aiming to reduce the gap between theory and practice, this thesis focuses on wireless physical layer security towards practical assumptions and requirements.

In the first half of the thesis, we reduce the dependence of physical layer security on impractical assumptions. The secrecy enhancements and analysis based on impractical assumptions cannot lead to any true guarantee of secrecy in practical networks. The current study of physical layer security was often based on the idealized assumption of perfect channel knowledge on both legitimate users and eavesdroppers. We study the impact of channel estimation errors on secure transmission designs. We investigate the practical scenarios where both the transmitter and the receiver have imperfect channel state information (CSI). Our results show how the optimal transmission design and the achievable throughput vary with the amount of knowledge on the eavesdropper's channel. Apart from the assumption of perfect CSI, the analysis of physical layer security often ideally assumed the number of eavesdropper antennas to be known. We develop an innovative approach to study secure communication systems without knowing the number of eavesdropper antennas by introducing the concept of spatial constraint into physical layer security. That is, the eavesdropper is assumed to have a limited spatial region to place (possibly an infinite number of) antennas. We show that a non-zero secrecy rate is achievable with the help of a friendly jammer, even if the eavesdropper places an infinite number of antennas in its spatial region.

In the second half of the thesis, we improve the applicability of physical layer security. The current physical layer security techniques to achieve confidential broadcasting were limited to application in single-cell systems. The primary challenge to achieve confidential broadcasting in the multi-cell network is to deal with not only the inter-cell but also the intra-cell information leakage and interference. To tackle this challenge, we design linear precoders performing confidential broadcasting in multi-cell networks. We optimize the precoder designs to maximize the secrecy sum rate with based on the large-system analysis. Finally, we improve the applicability of physical layer security from a fundamental aspect. The analysis of physical layer security based on the existing secrecy metric was often not applicable in practical networks. We propose new metrics for evaluating the secrecy of transmissions over fading channels to address the practical limitations of using existing secrecy metrics for such evaluations. The first metric establishes a link between the concept of secrecy outage and the eavesdropper's ability to decode confidential messages. The second metric provides an error-probability-based se-

crecy metric which is often used for the practical implementation of secure wireless systems. The third metric characterizes how much or how fast the confidential information is leaked to the eavesdropper. We show that the proposed secrecy metrics enable one to appropriately design secure communication systems with different views on how secrecy is measured.

List of Publications

Journal Articles

- J1. **B. He** and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.
- J2. **B. He**, N. Yang, X. Zhou, and J. Yuan, "Base station cooperation for confidential broadcasting in multi-cell networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5287–5299, Oct. 2015.
- J3. **B. He**, X. Zhou, and T. D. Abhayapala, "Achieving secrecy without knowing the number of eavesdropper antennas," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7030–7043, Dec. 2015.
- J4. **B. He**, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," submitted to *IEEE Trans. Wireless Commun.*, Jan. 2016.
- J5. **B. He**, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Communications*, vol. 11, no. 3, pp. 11–19, Sept. 2013. (invited paper)
- J6. X. Xu, **B. He**, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016. (not included in the thesis)

Conference Papers

- C1. **B. He** and X. Zhou, "Impact of channel estimation error on secure transmission design," in *Proc. IEEE AusCTW*, Adelaide, SA, Jan. 2013, pp. 19–24.
- C2. **B. He** and X. Zhou, "New physical layer security measures for wireless transmissions over fading channels," in *Proc. IEEE GLOBECOM*, Austin, TX, Dec. 2014, pp. 722–727.
- C3. **B. He**, N. Yang, X. Zhou, and J. Yuan, "Confidential broadcasting via coordinated beamforming in two-cell networks," in *Proc. IEEE ICC*, London, UK, June 2015, pp. 7376–7382.

- C4. **B. He** and X. Zhou, “On the placement of RF energy harvesting node in wireless networks with secrecy considerations,” in *Proc. IEEE GLOBECOM Workshop*, Austin, TX, Dec. 2014, pp. 1355–1360. (not included in the thesis)
- C5. Y. Cai, X. Xu, **B. He**, W. Yang, and X. Zhou, “Protecting cognitive radio networks against Poisson distributed eavesdroppers,” in *Proc. IEEE ICC*, Kuala Lumpur, Malaysia, May 2016, pp. 4035–4041. (not included in the thesis)

Acronyms

AN	artificial noise
AWGN	additive white Gaussian noise
BD	block diagonalization
BS	base station
CBf	coordinated beamforming
CSI	channel state information
dB	decibel
i.i.d.	independent and identically distributed
MCP	multi-cell processing
MIMO	multi-input multi-output
MISO	multi-input single-output
MMSE	minimum mean square error
MRT	maximum ratio transmission
RCI	regularized channel inversion
RZF	regularized zero forcing
SINR	signal-to-interference-plus-noise ratio
SNR	signal-to-noise ratio
UCA	uniform circular array
ULA	uniform linear array
2D	two-dimensional
3D	three-dimensional

Notations

$ \cdot $	magnitude of an element
$ \mathbf{X} $	determinant of matrix \mathbf{X}
$\ \cdot\ $	Euclidean norm of a vector
\mathbf{I}_n	identity matrix with size $n \times n$
$(\cdot)^T$	transpose of a vector or a matrix
$(\cdot)^H$	conjugate transpose of a vector or a matrix
$\log_n(\cdot)$	logarithm to base n
$\ln(\cdot)$	natural logarithm
$\lceil \cdot \rceil$	ceiling operator
$\lfloor \cdot \rfloor$	floor operator
$\mathbb{E}\{\cdot\}$	expectation operator
$\mathbb{P}\{\cdot\}$	probability measure
$\text{Tr}(\cdot)$	trace of a matrix
$[x]^+$	$\max(x, 0)$
$\xrightarrow{a.s.}$	almost sure convergence
$\xrightarrow{i.p.}$	convergence in probability
$\mathcal{CN}(\mu, \sigma^2)$	circularly symmetric complex Gaussian distribution with mean μ and variance σ^2
$\max\{\cdot\}$	maximization
$\min\{\cdot\}$	minimization
$W_0\{\cdot\}$	the principal branch of the Lambert W function

Contents

Declaration	iii
Acknowledgments	v
Abstract	vii
List of Publications	ix
Acronyms	xi
Notations	xiii
1 Introduction	1
1.1 Fundamentals and Background	2
1.1.1 Information-Theoretic Secrecy and Wiretap Channel	2
1.1.2 Secrecy Metrics for Wireless Transmissions	4
1.1.2.1 Ergodic Secrecy Capacity	4
1.1.2.2 Secrecy Outage Probability	5
1.1.3 Signal Processing Secrecy Enhancements	6
1.1.3.1 Secure On-Off Transmission Scheme	6
1.1.3.2 Beamforming with AN	7
1.1.3.3 Linear Precoding for Confidential Broadcasting	9
1.2 Motivation and Challenges	10
1.2.1 Impractical Assumptions	10
1.2.2 Limited Applicability	11
1.3 Thesis Outline and Contributions	12
2 Secure On-Off Transmission Design with Channel Estimation Errors	19
2.1 Introduction	19
2.2 System Model	20
2.2.1 Channel Estimation	22
2.2.2 Channel Knowledge	23
2.2.3 Secure Encoding	24
2.3 On-Off Transmission Design	25

2.3.1	Scenario One	26
2.3.2	Scenario Two	29
2.3.3	Scenario Three	31
2.4	Joint Rate and On-Off Transmission Design	32
2.4.1	Non-Adaptive Rate Scheme	33
2.4.2	Adaptive Rate Scheme	35
2.5	Numerical Results	37
2.5.1	On-Off Transmission Design	37
2.5.2	Joint Rate and On-Off Transmission Design	40
2.6	Summary	42
3	Achieving Secrecy without Knowing the Number of Eavesdropper Antennas	45
3.1	Introduction	45
3.2	System Model	46
3.2.1	Wiretap-Channel System	47
3.2.2	Jammer-Assisted System	49
3.2.2.1	Case 1: Basic Jammer-Assisted System	49
3.2.2.2	Case 2: AN Jammer-Assisted System	50
3.3	Introducing Spatial Constraints into Secrecy Capacity Calculation	51
3.3.1	Secrecy Capacity of Wiretap-Channel System	52
3.3.2	Secrecy Capacity of Basic Jammer-Assisted System	53
3.3.3	Secrecy Capacity of AN Jammer-Assisted System	53
3.3.4	Secrecy Capacity with Legitimate CSI Available at Alice	54
3.3.5	Numerical Results	55
3.4	Worst-Case Analysis for Jammer-Assisted Systems	58
3.4.1	Wiretap-Channel System	58
3.4.2	Basic Jammer-Assisted System	59
3.4.2.1	Worst-Case Secrecy Capacity	59
3.4.2.2	Optimal Jamming Power	60
3.4.3	AN Jammer-Assisted System	61
3.4.4	Numerical Results	62
3.5	Summary	66
4	Base Station Cooperation for Confidential Broadcasting in Multi-Cell Networks	67
4.1	Introduction	67
4.2	Network Model	68
4.2.1	Confidential Broadcasting and Performance Metric	70
4.2.2	Multi-Cell Processing with RCI Precoder	71

4.2.3	Coordinated Beamforming with Generalized RCI Precoder	73
4.3	Secrecy Sum Rate in the Large-System Regime	75
4.3.1	Large-System Analysis	75
4.3.2	Numerical Results	76
4.4	Optimization of Secrecy Sum Rate	78
4.4.1	Optimal Regularization Parameter	78
4.4.1.1	α_{MCP}^* for MCP	79
4.4.1.2	α_{CBf}^* for CBf	79
4.4.1.3	Numerical Results	79
4.4.2	Power-Reduction Strategy	84
4.4.2.1	Power Reduction for MCP	85
4.4.2.2	Power Reduction for CBf	85
4.4.2.3	Numerical Results	86
4.5	Summary	87
5	New Secrecy Metrics for Wireless Transmission over Fading Channels	89
5.1	Introduction	89
5.2	Perfect Secrecy and Partial Secrecy	90
5.2.1	Perfect Secrecy	90
5.2.2	Partial Secrecy	91
5.3	New Secrecy Metrics for Wireless Transmissions	92
5.3.1	Fractional Equivocation for a Given Fading Realization	92
5.3.2	New Secrecy Metrics	93
5.3.2.1	Generalized Secrecy Outage Probability	93
5.3.2.2	Average Fractional Equivocation	93
5.3.2.3	Average Information Leakage Rate	94
5.4	Wireless Transmissions with Non-Adaptive Rate Wiretap Codes: An Example .	94
5.4.1	System Model	94
5.4.2	Secrecy Performance Evaluation	95
5.4.2.1	Generalized Secrecy Outage Probability	96
5.4.2.2	Average Fractional Equivocation	97
5.4.2.3	Average Information Leakage Rate	97
5.4.3	Numerical Results	97
5.5	Impact on System Designs	100
5.5.1	Problem Formulation	101
5.5.2	Feasibility of the Constraint	102
5.5.3	Optimal Rate Parameters	102
5.5.4	Numerical Results	103

5.6	Summary	106
6	Conclusions	109
6.1	Thesis Conclusions	109
6.2	Future Research Directions	110
A	Appendix A	111
A.1	Proof of Proposition 2.1	111
A.2	Proof of Proposition 2.2	112
A.3	Proof of Proposition 2.4	112
A.4	Proof of Proposition 2.5	113
B	Appendix B	115
B.1	Proof of Proposition 3.1	115
B.2	Proof of Theorem 3.1	117
B.3	Proof of Theorem 3.2	119
B.4	Proof of Proposition 3.2	120
C	Appendix C	123
C.1	Proof of Theorem 4.1	123
C.2	Proof of Theorem 4.2	125
D	Appendix D	129
D.1	Proof of Proposition 5.2	129
D.2	Proof of Proposition 5.3	129
D.3	Proof of Proposition 5.4	130
	Bibliography	133

List of Figures

1.1	Illustration of a wireless network with an eavesdropper.	2
1.2	Wiretap-channel model.	3
1.3	Illustration of beamforming with AN.	7
1.4	Illustration of confidential broadcasting in a single-cell network.	9
2.1	Scenario 1: Achievable throughput versus normalized pilot power for different average received data SNRs at Bob, $\alpha_b = 5$ dB, 10 dB, 15 dB, 20 dB. The other system parameters are $\delta = 0.1$, $\varphi = 0.05$, $\alpha_e = 0$ dB, $R_b = 2$, $R_s = 1$. . .	37
2.2	Scenario 2: Achievable throughput versus normalized pilot power for different average received data SNRs at Bob, $\alpha_b = 5$ dB, 10 dB, 15 dB, 20 dB. The other system parameters are $\delta = 0.1$, $\varphi = 0.05$, $\alpha_e = 0$ dB, $R_b = 2$, $R_s = 1$. . .	38
2.3	Achievable throughput versus secrecy constraint for different values of normalized pilot power, $\psi = 1, 5, \infty$. The other system parameters are $\alpha_b = 10$ dB, $\alpha_e = 0$ dB, $\delta = 0.1$, $R_b = 2$, $R_s = 1$	39
2.4	Non-adaptive rate scheme: feasible secrecy constraint versus feasible reliability constraint for different values of normalized pilot power, $\psi = 1, 5, \infty$. The other system parameters are $\mu_b = 9$, $\alpha_b = 10$ dB, $\alpha_e = 0$ dB.	40
2.5	Achievable throughput versus secrecy constraint for different values of normalized pilot power, $\psi = 1, 5$. The other system parameters are $\delta = 0.1$, $\alpha_b = 10$ dB, $\alpha_e = 0$ dB.	41
2.6	Achievable secrecy constraint versus normalized pilot power for different target throughput values, $\eta = 0.2, 0.5$. The other system parameters are $\delta = 0.1$, $\alpha_b = 10$ dB, $\alpha_e = 0$ dB.	42
3.1	2D model for the wiretap-channel system.	47
3.2	3D model for the wiretap-channel system.	48
3.3	2D model for the jammer-assisted system.	49
3.4	3D model for the jammer-assisted system.	50
3.5	Wiretap-channel system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.	55

3.6	Basic jammer-assisted system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively. . .	55
3.7	AN jammer-assisted system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively. . .	56
3.8	Secrecy capacity versus the number of eavesdropper antennas with $N_b = 35$. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.	57
3.9	The minimum number of Bob's antennas for achieving a non-zero worst-case secrecy capacity versus the radius of Eve's spatial constraint. The other system parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$ and $r_b = 2\lambda$	63
3.10	The worst-case secrecy capacity versus the radius of Eve's spatial constraint. The other system parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $r_b = 2\lambda$ and $N_b = N_{ob} = 37$	64
3.11	The worst-case secrecy capacity versus the jamming power. The other system parameters are $P_t = 20$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $r_b = 1.5\lambda$, $r_e = 1\lambda$ and $N_b = 30$	65
4.1	Illustration of a symmetric two-cell broadcast network, where each cell consists of one N -antenna BS and K single-antenna users.	68
4.2	The normalized rate difference versus the number of antennas at each BS for $\varepsilon = 0.5$, $\alpha = 0.2$, $\beta = 0.5$ and $\gamma = 10$ dB.	77
4.3	The normalized rate difference versus the cross-cell interference level for $N = 20$, $\alpha = 0.2$, $\beta = 0.5$ and $\gamma = 10$ dB.	78
4.4	The large-system secrecy rate per antenna versus the cross-cell interference level for different designs of the regularization parameter with $N = 20$, $\beta = 0.5$ and $\gamma = 10$ dB.	81
4.5	MCP: the large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $\beta = 0.8, 1, 1.2$, $N = 20$ and $\varepsilon = 0.5$	82
4.6	CBf: the large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $\beta = 0.4, 0.5, 0.6$, $N = 20$ and $\varepsilon = 0.5$	83
4.7	The large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $N = 20$ and $\varepsilon = 0.5$	84

4.8	MCP: the large-system secrecy rate per antenna versus the average transmit SNR per BS for the transmissions with and without power-reduction strategy. The other system parameters are $\beta = 1.2, 1.5, N = 20$ and $\varepsilon = 0.5$	86
4.9	CBf: the large-system secrecy rate per antenna versus the average transmit SNR per BS for the transmissions with and without power-reduction strategy. The other system parameters are $\beta = 0.6, 0.8, N = 20$ and $\varepsilon = 0.5$	87
5.1	Basic wiretap-channel system.	90
5.2	Generalized secrecy outage probability versus confidential information rate. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $R_b = 4$ and $\bar{\gamma}_e = 1$	98
5.3	Generalized secrecy outage probability versus average received SNR at Eve. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8$. The other parameters are $R_b = R_s = 4$	99
5.4	Average fractional equivocation (asymptotic lower bound on the decoding error probability at Eve) versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma}_e = 1, 2$. The other parameter is $R_b = 4$	100
5.5	Average information leakage rate versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma}_e = 1, 2$. The other parameter is $R_b = 4$	101
5.6	For different secrecy metrics: optimal confidential information rate versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.	104
5.7	For generalized secrecy outage probability: optimal confidential information rate versus minimum required throughput. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.	105
5.8	Secrecy outage probability versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.	106
5.9	Average fractional equivocation (asymptotic lower bound on the decoding error probability at Eve) versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.	107
5.10	Average information leakage rate versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.	108
B.1	Without jamming signals: C_i versus N_i . The other system parameters are $N_t = 100, r_i = 1\lambda, P_t = 10$ dB, $\alpha_i = 1, \sigma_i^2 = 1$	116

- B.2 With jamming signals: C_i versus N_i . The other system parameters are $N_t = N_j = 100, r_i = 1\lambda, P_t = 10$ dB, $P_j = 0$ dB $\alpha_i = 1, \beta_i = 1, \sigma_i^2 = 1$ 119

Introduction

Wireless communications is the transfer of information without the use of an electrical conductor or the “wire”. In the very beginning of the 20th century, the pioneering developments in radio communications by Guglielmo Marconi opened the way for modern wireless communications. Since then, wireless communications has developed into an important element of modern society, and wireless devices have become ubiquitous in everyday life with their great flexibility and mobility. The number of mobile-connected devices exceeded the world’s population in 2014, and is envisioned to reach 11.5 billion by 2019 [1]. Meanwhile, people become dependent on wireless devices to send an unprecedented amount of private and sensitive information, e.g., password, account information, personal identification, and credit card details. According to Javelin’s forecast [2], the total mobile online retail payments are expected to be \$217.4 billion by 2019. Consequently, wireless communication security has already become of critical importance to our society. Securing wireless communications is never easy. Unlike the wireline network which provides a nicely closed environment for the signal, the transmitter in a wireless network broadcasts the signal in an open medium. The unchangeable open nature of wireless channels allows not only the intended receiver but also unauthorized receiver to capture the signal from the transmitter. Therefore, how to secure wireless transmissions is an important but challenging issue.

Traditionally, cryptography algorithms are studied by computer scientists and engineers to provide computational security for wireless communications at the application layer. The computational security is conditioned on the limited computational capability of the adversary, such that the encryption is computationally infeasible to decrypt. With the rapid development of computational devices, the wireless security solely provided by cryptographic techniques is becoming vulnerable to attacks [3, 4, 5]. In recent years, a new paradigm has attracted considerable interests of wireless researchers due to its advantage of securing wireless communications at the physical layer [6, 7, 8, 9, 10]. This new paradigm termed physical layer security introduces a level of information-theoretic security by exploiting the characteristics of wireless channels, such as fading, interference, and noise. A major advantage of physical layer security is that the information-theoretic security is not constrained by the computational

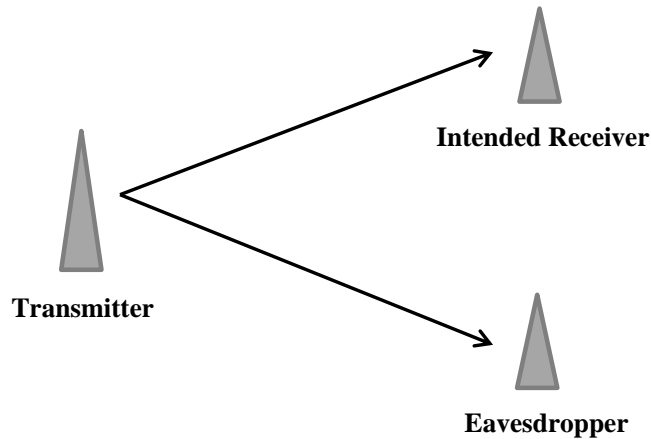


Figure 1.1: Illustration of a wireless network with an eavesdropper.

complexity [11], and hence the achieved level of security will not be compromised even if the adversary has a more powerful computational device. Another major advantage of physical layer security is that it can be used as a good complement to the current cryptographic techniques for increasing the overall wireless communication security. Physical layer security protects the communication phase while cryptography protects the data processing after the communication phase, i.e., they work in different domains and provide two separate layers of protection.

The remainder of this chapter is organized as follows. Section 1.1 introduces the fundamentals and background of physical layer security in wireless communications. Section 1.2 clarifies the motivation and challenges of the thesis. Finally, Section 1.3 gives the outline and highlights the contributions of the thesis.

1.1 Fundamentals and Background

To show the basic problem of the study on physical layer security, Figure 1.1 illustrates a typical example of a three-node wireless network. The transmitter sends confidential information to an intended receiver in the presence of an eavesdropper. The received signals at the intended receiver and the eavesdropper are usually different due to the different wireless channels from the transmitter to the intended receiver and the eavesdropper. Physical layer security exploits the characteristics of the channels to protect the data transmission from the transmitter to the intended receiver against the eavesdropper.

1.1.1 Information-Theoretic Secrecy and Wiretap Channel

Shannon [12] first introduced the notion of information-theoretic secrecy, which does not rely on the assumption on the computational ability of the eavesdropper. Perfect secrecy requires

that the amount of information leakage to the eavesdropper vanishes. It guarantees that the eavesdropper's optimal attack is to guess the message at random, and hence the eavesdropper's decoding error probability, P_e , asymptotically goes to 1. In the seminal work [13], Wyner introduced the wiretap-channel system, and addressed the tradeoff between the information rate to the intended receiver and the level of ignorance at the eavesdropper.

The basic wiretap-channel model is shown as Figure 1.2. Alice wants to send confidential information M to Bob in the presence of an eavesdropper, Eve. The confidential information, M , is encoded into a n -vector X^n . The received vectors at Bob and Eve are denoted by Y^n and Z^n , respectively. The entropy of the source information and the residual uncertainty for the message at the eavesdropper are denoted by $H(M)$ and $H(M | Z^n)$, respectively. The channel between Alice and Bob is named as the intended receiver's channel or the main channel. The channel between Alice and Eve is named as the eavesdropper's channel. Wyner also outlined the wiretap code [13] for confidential message transmissions. There are two rate parameters, namely, the codeword transmission rate, $R_b = H(X^n)/n$, and the confidential information rate, $R_s = H(M)/n$. The positive rate difference $R_e = R_b - R_s$ is the cost to provide secrecy against the eavesdropper. A length n wiretap code is constructed by generating 2^{nR_b} codewords $x^n(w, v)$ of length n , where $w = 1, 2, \dots, 2^{nR_s}$ and $v = 1, 2, \dots, 2^{n(R_b - R_s)}$. For each message index w , we randomly select v from $\{1, 2, \dots, 2^{n(R_b - R_s)}\}$ with uniform probability and transmit the codeword $x^n(w, v)$.

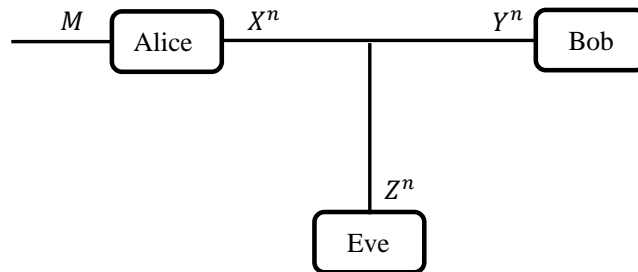


Figure 1.2: Wiretap-channel model.

Perfect secrecy means that the amount of information leakage to the eavesdropper vanishes, and guarantees that the eavesdropper's optimal attack is to guess the message at random. From Shannon's definition, perfect secrecy requires the statistical independence between the original message and Eve's observation, which is given by

$$H(M | Z^n) = H(M) \quad \text{or, equivalently,} \quad I(M, Z^n) = 0. \quad (1.1)$$

Since Shannon's definition of perfect secrecy is not convenient to be used for further analysis, current research often investigates the strong secrecy or weak secrecy [14]. Strong secrecy

requires asymptotic statistical independence of the message and Eve's observation as the code-word length goes to infinity, i.e., $\lim_{n \rightarrow \infty} I(M, Z^n) = 0$. Weak secrecy requires that the rate of information leaked to the eavesdropper vanishes, i.e., $\lim_{n \rightarrow \infty} \frac{1}{n} I(M, Z^n) = 0$. In this thesis, we use the term "perfect secrecy" to refer to not only Shannon's perfect secrecy but also the strong secrecy and the weak secrecy.

1.1.2 Secrecy Metrics for Wireless Transmissions

Wyner [13] defined the secrecy capacity as the maximum rate at which the message can be reliably transmitted to the intended receiver without being eavesdropped. The secrecy capacity of the Gaussian wiretap channel is given by [15],

$$C_s = [C_b - C_e]^+, \quad (1.2)$$

where $C_b = \log_2(1 + \gamma_b)$ and $C_e = \log_2(1 + \gamma_e)$ denote the intended receiver's channel capacity and eavesdropper's channel capacity, respectively, γ_b and γ_e denote the signal-to-noise ratios (SNRs) of the intended receiver's channel and the eavesdropper's channel, respectively. Note that a positive secrecy capacity is achievable only when the intended receiver's channel is better than the eavesdropper's channel.

To evaluate the secrecy performance of wireless transmissions over fading channels, the ergodic secrecy capacity and the secrecy outage probability are often adopted as secrecy metrics.

1.1.2.1 Ergodic Secrecy Capacity

Ergodic secrecy capacity applies to delay tolerant systems in which the encoded messages are assumed to span sufficient channel realizations so that the ergodic features of the channel are captured. Ergodic secrecy capacity reveals the capacity limit under the constraint of perfect secrecy. Typical examples of delay tolerant applications are document transmission and e-mail, both of which belong in the category of non-real-time data traffic.

Gopala *et al.* [16] derived the ergodic secrecy capacity for both the case of full channel state information (CSI) and the case with only the CSI of main channel. The secrecy capacity for one realization of the fading channels is given by (1.2). Taking average of the secrecy capacity over all fading realizations, we obtain the ergodic secrecy capacity with full CSI as

$$\bar{C}_s^{(f)} = \int_0^\infty \int_{\gamma_e}^\infty (\log_2(1 + \gamma_b) - \log_2(1 + \gamma_e)) f(\gamma_b) f(\gamma_e) d\gamma_b d\gamma_e, \quad (1.3)$$

where $f(\gamma_b)$ and $f(\gamma_e)$ are the distribution functions of γ_b and γ_e , respectively. With the full CSI on both channels, the transmitter can make sure that the transmission happens only when $\gamma_b > \gamma_e$. For the case with only the CSI of main channel available, the ergodic secrecy capacity

is given by

$$\bar{C}_s^{(b)} = \int_0^\infty \int_0^\infty [\log_2(1 + \gamma_b) - \log_2(1 + \gamma_e)]^+ f(\gamma_b)f(\gamma_e)d\gamma_b d\gamma_e. \quad (1.4)$$

Gopala *et al.* [16] also outlined a variable-rate transmission scheme to show the achievability of the ergodic secrecy capacity with only the CSI of main channel. During a coherence interval with the received SNR at the intended receiver, γ_b , the transmitter transmits codewords at a rate of $\log_2(1 + \gamma_b)$. This variable-rate scheme relies on the assumption of large coherence intervals and ensures that when $\gamma_b < \gamma_e$, the mutual information between the source and the eavesdropper is upper-bounded by $\log_2(1 + \gamma_b)$. When $\gamma_b \geq \gamma_e$, this mutual information is equal to $\log_2(1 + \gamma_e)$. Averaged over all fading states, the achievable secrecy rate is given as (1.4). The secure message is hidden across different fading states.

1.1.2.2 Secrecy Outage Probability

As mentioned before, the ergodic secrecy capacity applies to delay-tolerant systems which allow for the use of an ergodic version of fading channels. For the systems with stringent delay constraints, the perfect secrecy cannot always be achieved, and the ergodic secrecy capacity is inappropriate to characterize the performance limits of such systems. The secrecy outage probability, which measures the secrecy performance by probabilistic formulations, is more appropriate in such systems.

Parada and Blahut [17] analyzed the wireless systems over quasi-static fading channels with neither intended receiver nor eavesdropper's CSI available at the transmitter. They provided an alternative definition of the outage probability. According to this definition, the secure communication can be guaranteed for the fraction of time when the intended receiver's channel is stronger than the eavesdropper's channel. Barros and Rodrigues [18] provided the first detailed characterization of the secrecy outage capacity where the outage probability, p_{out} , is characterized by the probability that a given target rate, R_s , is greater than the difference between main channel capacity, C_b , and eavesdropper's channel capacity, C_e . The secrecy outage probability is given by

$$p_{\text{out}} = \mathbb{P}(C_b - C_e < R_s). \quad (1.5)$$

It was showed that the fading alone can guarantee the physical layer security, even when the eavesdropper has a better average SNR than the intended receiver.

The definition of secrecy outage probability in (1.5) captures the probability of failing to have a reliable and secure transmission. Reliability and secrecy are not differentiated, because an outage occurs whenever the transmission is either unreliable or not perfectly secure. Zhou *et al.* [19] presented an alternative secrecy outage formulation to directly measure the probability that a transmitted message is not perfectly secure. The alternative secrecy outage probability

is given by

$$p_{\text{so}} = \mathbb{P}(C_e > R_b - R_s \mid \text{message transmission}), \quad (1.6)$$

where R_b and R_s are the rate of transmitted codeword and the rate of the confidential information in the wire-tap code, respectively. The outage probability is conditioned on a message actually being transmitted. The definition of secrecy outage probability in (1.6) takes into account the system design parameters, such as the rate of transmitted codewords and the condition under which message transmissions take place.

1.1.3 Signal Processing Secrecy Enhancements

In the following, we introduce some important signal processing techniques for enhancing the secrecy performance of wireless communications. They are the secure on-off transmission scheme for single-antenna wiretap systems, the beamforming with artificial noise (AN) for multi-antenna wiretap systems, and the linear precoding for broadcast networks with confidential information.

1.1.3.1 Secure On-Off Transmission Scheme

The principle of secure on-off transmissions can be roughly described as follows. The transmitter does not always transmit information, and decides whether or not to transmit according to the knowledge of CSI. The transmission takes place only when the instantaneous CSI fulfills the requirements related to some given thresholds, e.g., SNR thresholds. Otherwise, the transmitter suspends the transmission.

Gopala *et al.* [16] proposed a low-complexity, on-off power allocation strategy according to the instantaneous CSI on the intended receiver's channel, which approaches optimal performance for asymptotically high average SNR. Zhou *et al.* [19] designed two on-off transmission schemes, each of which guarantees a certain level of secrecy whilst maximizing the throughput. With the statistics of eavesdropper's channel information, the first scheme requires the instantaneous CSI feedback from the intended receiver to the transmitter, and the second scheme requires only the one-bit feedback from the intended receiver. Rezki *et al.* [20] investigated the scenario where the transmitter has the imperfect CSI of the intended receiver and the statistical CSI of the eavesdropper. A simple on-off transmission scheme was proposed and the achievable secrecy rate with the Gaussian input was derived. Furthermore, the on-off transmission scheme has also been adopted to study the wireless systems with multiple eavesdroppers in, e.g., [21, 22, 23].

1.1.3.2 Beamforming with AN

The work by Hero [24] is arguably the first to consider secret communication in a multi-antenna transmission system, and sparked significant efforts to this problem [25]. For multi-antenna systems, beamforming with AN is one of the most widely-used techniques to secure the data transmission. The AN injection strategy was first proposed by Negi and Goel [26, 27]. In addition to transmitting information signals, the transmitter allocates a part of transmit power for broadcasting AN that confuses the eavesdropper. Specifically, the produced AN lies in the null space of the intended receiver's channel, and the information signal is transmitted in the range space of the intended receiver's channel. The AN technique relies on the knowledge of instantaneous CSI on the intended receiver's channel, but does not require the knowledge of instantaneous CSI of the eavesdropper's channel. An illustration of the beamforming with AN is depicted in Figure 1.3. Goel and Negi [27] also described the use of AN in relay net-

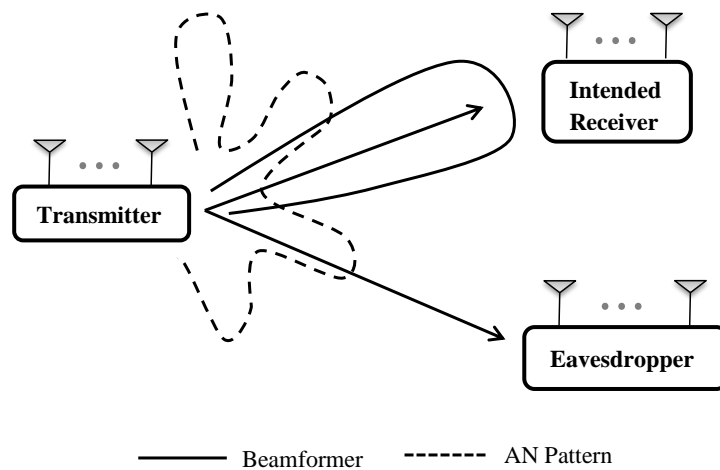


Figure 1.3: Illustration of beamforming with AN.

works. Secure communications assisted by relay nodes is often regarded as a natural extension of secure communications in multi-antenna networks. A virtual beam towards the legitimate receiver can be built by the collaboratively work among relay nodes, which is similar to the secure transmission in a multi-antenna system. However, unlike the multi-antenna transmission, the transmitter cannot directly control the relays. Specifically, the injection of AN in relay networks can be achieved by a 2-phase transmission protocol. In the first phase, the transmitter and the intended receiver both transmit independent AN signals to the relays. Different linear combinations of these two signals are received by the relays and the eavesdropper. In the second phase, the relays replay a weighted version of the received signal, using a publicly available sequence of weights. Meanwhile, the transmitter transmits the confidential information, along with a weighted version of the AN transmitted in the first stage. With the knowledge

of the AN component due to the intended receiver, the intended receiver is able to cancel off the AN and get the confidential information.

Based on Negi and Goel's work, the beamforming with AN was further investigated and optimized. The optimal power allocation between the information signal and the AN was studied in [28, 29, 30]. It was found that the equal power allocation results in nearly the same secrecy rate as if power are optimally allocated for the case of non-colluding eavesdroppers. For the case of colluding eavesdroppers, it was found that more power should be allocated to transmitting AN as the number of eavesdroppers increases. Huang and Swindlehurst [31] obtained the robust transmit covariance matrices for the worst-case secrecy rate maximization under both individual and global power constraints. They investigated both cases of the direct transmission and the cooperative jamming with a helper. Gerbracht *et al.* [32] characterized the optimal single-stream beamforming with the use of AN to minimize the outage probability. It was pointed out that the solution converges to the maximum ratio transmission (MRT) for the case with no instantaneous CSI of the eavesdropper, and the optimal beamforming vector converges to the generalized eigenvector solution with the growing level of CSI. For the case where even the statistical CSI of the eavesdropper is unknown, Swindlehurst and Mukherjee [33, 34] proposed a modified water-filling algorithm which balances the required transmit power with the number of spatial dimensions available for jamming the eavesdropper. As described in the modified water-filling algorithm, the transmitter first allocates enough power to meet a target performance criterion, e.g., SNR or rate, at the receiver, and then uses the remaining power to broadcast AN. In [35], the authors applied a similar algorithm to investigate the multiuser downlink channels.

Furthermore, some studies evaluated the impact of imperfect CSI of the intended receiver on the performance of beamforming with AN. When the CSI of the intended receiver is imperfect, the AN leaks into the intended receiver's channel, due to the fact that the AN is designed according to the estimated instantaneous CSI rather than the actual instantaneous CSI. As a result, the AN interferes with the intended user. Taylor *et al.* [36] showed the impact of channel estimation errors on an eigenvector-based jamming technique. Their results illustrated that the ergodic secrecy rate provided by the jamming technique decreases rapidly as the channel estimation error increases. Mukherjee and Swindlehurst [37] also pointed out that the secrecy provided by the beamforming is quite sensitive to imprecise channel estimates, they proposed a robust beamforming scheme for multi-input multi-output (MIMO) secure transmission systems with imperfect CSI of the intended receiver. Adapting the secrecy beamforming scheme, Liu *et al.* [38] investigated the joint design of training and data transmission signals for wiretap channels. The ergodic secrecy rate for systems with imperfect channel estimations at both the intended receiver and the eavesdropper was derived. Based on the derived ergodic secrecy rate, the optimal tradeoff between the power used for training and data signals was found as well.

1.1.3.3 Linear Precoding for Confidential Broadcasting

Apart from the studies on wiretap channels, another branch of research focuses on the physical layer security in broadcast networks, and aims at achieving confidential broadcasting. Different from the wiretap channel, confidential broadcasting requires multiple messages to be securely broadcasted to multiple users in the network. Each of the multiple messages is intended for one of the users but needs to be kept secret from the other users. An illustration of confidential broadcasting in a single-cell network is depicted in Figure 1.4.

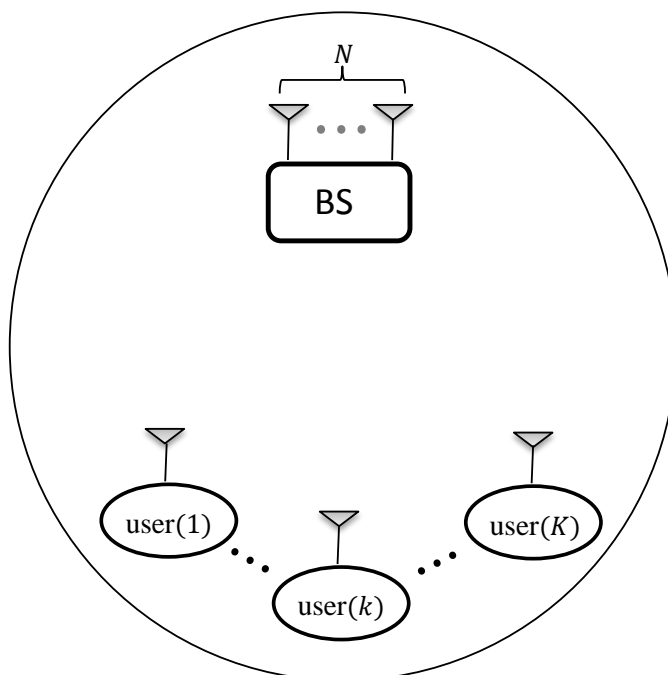


Figure 1.4: Illustration of confidential broadcasting in a single-cell network.

The secrecy capacity of the two-user multi-antenna broadcast network was examined in [39, 40]. The confidential broadcasting in the multi-user network where a base station (BS) serves an arbitrary number of receivers *in a single cell* was studied in [41, 42, 43, 44, 45]. A linear precoder at the BS to perform confidential broadcasting for single-antenna receivers was designed in [41]. It was shown that the linear precoding can control the amount of information leakage and interference among the users in the broadcast network. Thus although suboptimal, the linear precoder achieves secrecy with low-complexity implementation. The secrecy sum rate achieved by the linear precoder was thoroughly analyzed in [43]. The impact of channel correlation at the transmitter on the secrecy sum rate achieved by the same precoder was examined in [44]. Considering multi-antenna receivers, the authors of [45] designed the linear

precoder to perform confidential broadcasting and addressed unequal distances from the BS to the users.

1.2 Motivation and Challenges

Despite a significant amount of work that has been conducted from the theoretical perspective, physical layer security is still far from actual implementations in practical networks, arguably due to the impractical assumptions and the limited applicability.

1.2.1 Impractical Assumptions

As mentioned before, physical layer security is achieved by exploiting the characteristics of wireless channels, such as fading, interference, and noise. Consequently, the level of information-theoretic security provided by physical layer security techniques highly depends on the knowledge of wireless channels which includes the knowledge about both the intended receiver and the eavesdropper. Unfortunately, the assumption on the available knowledge is not generally practical in many of existing literatures.

For instance, some existing articles assumed that the perfect CSI of the channels to the intended receiver and the eavesdropper is available. Usually, the CSI is obtained at the receiver by channel estimation during pilot transmission. Then, a feedback link (if available) is used to send the CSI to the transmitter. In practice, an external eavesdropper naturally does not cooperate with the transmitter to send CSI feedback, and hence, it is very difficult for the transmitter to obtain the CSI of the eavesdropper. Although the intended receiver may cooperate to send CSI feedback, reliable uplink channels for the feedback cannot always be guaranteed. This leads to an increasing amount of recent work focusing on the scenario where the transmitter does not have perfect CSI of the channel to the intended receiver and/or the eavesdropper, e.g., [31, 37, 46, 47, 48].

On the other hand, most existing studies still assumed that the intended receiver has perfect CSI. Clearly, the assumption of perfect CSI available at the receiver is not very practical, since the channel estimation at the receiver generally is not error-free. In principle, the channel estimation error exists at both the intended receiver and the eavesdropper. Assuming perfect estimation at the eavesdropper is relatively reasonable from the secure transmission design point of view, since it is often difficult or impossible for the transmitter to know the accuracy of the eavesdropper's channel estimate. Assuming perfect CSI at the eavesdropper can be regarded as a worst-case scenario for the analysis. However, the assumption of perfect CSI at the intended receiver is difficult to justify from the practical perspective.

Apart from the assumption of perfect CSI knowledge at the receiver, another idealized assumption is often adopted in the existing literature on physical layer security. That is, the

number of eavesdropper antennas or an upper bound on the number of eavesdropper antennas is assumed to be known at the legitimate side, e.g., [27, 28, 37, 49, 50, 51, 52, 53]. If the number of eavesdropper antennas is unknown, we have to assume that the eavesdropper has an infinite number of antennas as a worst-case consideration, and then the secrecy rate would always go to zero intuitively. To the best of our knowledge, no existing literature has studied the scenario where the number of eavesdropper antennas is totally unknown. In practice, an external eavesdropper naturally does not inform the legitimate side about the number of antennas to expose its ability. As a weak justification, the upper bound on the number of eavesdropper antennas could be estimated from the eavesdropper's device size. However, such a weak justification, probably valid in the past, can no longer hold with the current development of large-scale antenna array technologies which allow a fast growing number of antennas be placed within a limited space. Thus, how to characterize the performance of physical layer security without knowing the number of eavesdropper antennas is a challenging but important problem.

1.2.2 Limited Applicability

As the traditional approach to securing wireless communications, cryptographic techniques have been well studied and designed for different systems subject to practical secrecy requirements. In contrast, the existing research on physical layer security is applicable only to simplified systems with information-theoretic secrecy requirements. In other words, the existing analysis on physical layer security is not generally applicable to practical wireless systems with practical secrecy requirements.

We can see that the existing analysis on physical layer security is not generally applicable for practical wireless systems by taking an example of the research on broadcast network with confidential information. While the confidential broadcasting in a single isolated cell has been elaborately studied, the solution to confidentially broadcasting messages in *multi-cell* networks has not been addressed in the literature. In other words, the existing analysis on physical layer security for achieving confidential broadcasting is applicable only for the networks with a single isolated cell, but is not applicable for practical wireless networks with multiple cells not far away from each other. The primary challenge to achieve confidential broadcasting in the multi-cell network is to deal with the inter-cell information leakage and interference, besides the intra-cell information leakage and interference. Thus, the techniques achieving single-cell confidential broadcasting in existing research cannot be applied to achieving multi-cell confidential broadcasting.

We now explain why the existing research on wireless physical layer security is not generally applicable for systems with practical secrecy requirements. The reason is due to the fundamental limitations on the secrecy metrics that adopted by the existing studies. As intro-

duced in Section 1.1.2, the secrecy performance of wireless transmissions over fading channels is often measured by the ergodic secrecy capacity or the secrecy outage probability. Unfortunately, these two secrecy measures are not (closely) related to the secrecy requirements in practice, and do not bear the same significance from a cryptographic perspective. In particular, the current definition of secrecy outage probability has two major limitations in evaluating the secrecy performance of wireless systems. First, the secrecy outage probability does not give any insight into the eavesdropper's ability to decode the confidential messages. The eavesdropper's decodability is an intuitive measure of security in real-world communication systems when classical information-theoretic secrecy is not always achievable, and error-probability-based secrecy metrics are often adopted to quantify secrecy performance in the literature, e.g., [54, 55, 56, 57]. A general secrecy requirement for the eavesdropper's decoding error probability, P_e , can be given as $P_e \geq \vartheta$, where $0 < \vartheta \leq 1$ denotes the minimum acceptable value of P_e . In contrast, classical secrecy outage probability reflects only an extremely stringent requirement on P_e for $\vartheta \rightarrow 1$, i.e., requiring $\vartheta \rightarrow 1$, since classical information-theoretic secrecy guarantees $P_e \rightarrow 1$. Second, the amount of information leakage to the eavesdropper cannot be characterized. When classical information-theoretic secrecy is not achievable, some information will be leaked to the eavesdropper. Different secure transmission designs that lead to the same secrecy outage probability may actually result in very different amounts of information leakage. Consequently, it is important to know how much or how fast the confidential information is leaked to the eavesdropper to obtain a finer view of the secrecy performance. However, the classical outage-based approach is not able to evaluate the amount of information leakage when a secrecy outage occurs.

1.3 Thesis Outline and Contributions

The objective of the thesis is to make contributions for bridging the gap between theory and practice in physical layer security. To reduce the dependence of physical layer security on impractical assumptions, we study the on-off transmission design with the consideration of channel estimation errors in Chapter 2, and provide an innovative solution to the challenging problem of achieving secrecy without knowing the number of eavesdropper antennas in Chapter 3. To make the analysis on physical layer security more applicable in practical networks, we develop an effective solution to tackle the challenge of confidential broadcasting in multi-cell networks in Chapter 4, and propose new secrecy measures for wireless systems over fading channels in Chapter 5. The contributions of each chapter are emphasized as follows.

Chapter 2 – Secure On-Off Transmission Design with Channel Estimation Errors

Chapter 2 studies the impact of channel estimation errors on the secure on-off transmission design. As introduced in Section 1.1.3.1, the secure on-off transmission scheme [16, 19] is an important secrecy enhancement for improving the secrecy performance of single-antenna wireless systems. The main contributions of this chapter are summarized as follows:

- We consider quasi-static slow fading channels and use the secrecy outage probability to study the secure transmission design with channel estimation errors at the receiver side. This is different from the previous works considering the impact of imperfect channel estimations on physical layer security, which all used the ergodic secrecy rate as the performance measure.
- We develop throughput-maximizing secure on-off transmission schemes with fixed encoding rates for different scenarios distinguished on whether or not there is channel estimation error at the eavesdropper, and whether or not the transmitter has the estimated channel quality fed back from the eavesdropper. Our analytical and numerical results show how the optimal design and the achievable throughput vary with the change in the channel knowledge assumptions.
- For systems in which the encoding rates are controllable parameters to design, we jointly optimize the encoding rates and the on-off transmission thresholds to maximize the throughput of secure transmissions. Both non-adaptive and adaptive rate transmissions are considered. Note that none of the previous works on physical layer security considering the channel estimation error has explicitly involved the rate parameters as part of the design problem.
- We also analyze how the training (pilot) power affects the achievable throughput of secure transmissions, since the accuracy of the channel estimation depends on the pilot power. One interesting finding is that, in the scenario where both the intended receiver and the eavesdropper obtain imperfect channel estimates, increasing the pilot power for more accurate channel estimation can harm the throughput of the secure transmission even if the pilot power is obtained for free.

The results in this chapter have been presented in the following publications which are listed again for ease of reference:

- J1. **B. He** and X. Zhou, “Secure on-off transmission design with channel estimation errors,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.
- C1. **B. He** and X. Zhou, “Impact of channel estimation error on secure transmission design,” in *Proc. IEEE AusCTW*, Adelaide, SA, Jan. 2013, pp. 19–24.

Chapter 3 – Achieving Secrecy without Knowing the Number of Eavesdropper Antennas

In Chapter 3, we provide an innovative solution to the challenging problem of how to achieve secrecy without the impractical assumption of knowing the number of eavesdropper antennas. Specifically, we introduce the concept of spatial constraint into physical layer security. Here the spatial constraint means the limited size of the spatial region for placing antennas at the communication node. In practice, knowing the eavesdropper's spatial constraint for placing antennas is much easier than knowing the exact number of the eavesdropper antennas. For example, we may know the size of the eavesdropper's device, but it is difficult to know how many antennas are installed on the device. Also, we may know that the eavesdropper hides in a room, but it is difficult to know how many antennas are placed inside the room.

The primary contributions of this chapter are summarized as follows.

- We introduce spatial constraints into physical layer security. To this end, we propose a framework to study physical layer security in multi-antenna systems with spatial constraints at the receiver side (both the intended receiver and the eavesdropper). We derive the secrecy capacity, and analyze the impact of spatial constraints on the secrecy capacity.
- For the first time, our proposed framework allows one to analyze physical layer security without the knowledge of the number of eavesdropper antennas. It relaxes the requirement on the knowledge of eavesdropper from knowing the number of antennas to knowing the spatial constraint. We show that a non-zero secrecy capacity is achievable even if the eavesdropper is assumed to have an infinite number of antennas. This is easily achieved by applying the basic friendly-jamming technique where the jammer sends random noise signals.
- We further study the impact of jamming power on the secrecy capacity of the spatially-constrained jammer-assisted systems. For the basic jammer-assisted system, we find that the secrecy capacity does not monotonically increase with the jamming power, and we obtain the closed-form solution of the optimal jamming power that maximizes the secrecy capacity. The optimality of the obtained solution is confirmed by the numerical result.

The results in this chapter have been presented in the following publications which are listed again for ease of reference:

- J3. **B. He**, X. Zhou, and T. D. Abhayapala, "Achieving secrecy without knowing the number of eavesdropper antennas," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7030–7043, Dec. 2015.

Chapter 4 – Base Station Cooperation for Confidential Broadcasting in Multi-Cell Networks

In Chapter 4, we build up an effective solution to tackle the challenge of confidential broadcasting in multi-cell networks. In the network, BS cooperation [58] is taken into consideration such that the BSs can share control signals, CSI and/or messages to cooperatively serve users in multiple cells. With BS cooperation, we specifically consider the confidential broadcasting in a symmetric two-cell network where there are K single-antenna users and one N -antenna BS in each cell. The two BSs cooperatively broadcast confidential information to the users. We focus on two different forms of cooperation at the BSs: i) multi-cell processing (MCP) and ii) coordinated beamforming (CBf). In the MCP, the BSs fully cooperate such that they share their CSI and messages to transmit. Alternatively, in the CBf the BSs “partially” cooperate. As such, they do not share their messages to transmit but allow users to feed back the CSI to the cross-cell BS.

The primary contributions of this chapter are summarized as follows.

- We design a linear precoder as per the principles of regularized channel inversion (RCI) [59] to perform confidential broadcasting in the multi-cell network with the MCP.¹ We also design a linear precoder as per the principles of generalized RCI [60] to perform confidential broadcasting in the multi-cell network with the CBf. In each precoder, the precoding matrix is designed to trade off the intended received signal, the intra- and inter-cell information leakage, and the intra- and inter-cell interference via a regularization parameter.
- We derive new channel-independent expressions for the secrecy sum rate achieved by the designed linear precoders for both the MCP and the CBf in the large-system regime. In this regime, we consider $K, N \rightarrow \infty$ and keep the ratio $\beta = K/N$ constant. The large-system expressions do not depend on the channel realizations, and thus eliminate the computational burden of performance evaluation incurred by Monte Carlo simulations. Notably, numerical results confirm that our large-system expressions are accurate even for finite K and N .
- We optimize the secrecy performance of confidential broadcasting in the multi-cell network based on our large-system expressions. We first determine the optimal regularization parameters of the RCI and the generalized RCI precoders in order to maximize the secrecy sum rate for the MCP and the CBf, respectively. We then design power-reduction linear precoders in order to significantly increase the secrecy sum rate at high transmit SNRs when the network load is high. To do this, we propose power-reduction strategies for the MCP when $\beta > 1$ and the CBf when $\beta > 0.5$. These strategies effectively prevent

¹The RCI is also sometimes called as regularized zero forcing (RZF) in some literatures.

the the secrecy sum rate from decreasing at high transmit SNRs which is caused by the RCI precoder when $\beta > 1$ and the generalized RCI precoder when $\beta > 0.5$.

The results in this chapter have been presented in the following publications which are listed again for ease of reference:

- J2. **B. He**, N. Yang, X. Zhou, and J. Yuan, "Base station cooperation for confidential broadcasting in multi-cell networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5287–5299, Oct. 2015.
- C3. **B. He**, N. Yang, X. Zhou, and J. Yuan, "Confidential broadcasting via coordinated beamforming in two-cell networks," in *Proc. IEEE ICC*, London, UK, June 2015, pp. 7376–7382.

Chapter 5 – New Secrecy Measures for Wireless Transmissions over Fading Channels

In Chapter 5, we propose three new secrecy metrics for wireless transmissions focusing on quasi-static fading channels, motivated by the limitations of the secrecy outage probability in evaluating practical networks. We evaluate the secrecy performance of an example wireless system with fixed-rate wiretap codes to illustrate the use of the proposed secrecy metrics, and show that the proposed secrecy metrics can jointly give a more comprehensive and in-depth understanding of the secrecy performance of wireless transmission over fading channels. We find that the newly proposed secrecy metrics lead to very different optimal design parameters that optimize the secrecy performance of the system, compared with the optimal design minimizing the current secrecy outage probability. Applying the optimal design that minimizes the secrecy outage probability can result in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper and/or a low information leakage rate. The primary contributions of this chapter, i.e., the three new secrecy metrics, are summarized as follows.

- Extended from the current definition of secrecy outage, a generalized formulation of secrecy outage probability is proposed. The generalized secrecy outage probability takes into account the level of secrecy measured by equivocation, and hence establishes a link between the existing concept of secrecy outage and the decodability of messages at the eavesdropper.
- An asymptotic lower bound on the eavesdropper's decoding error probability is proposed. This proposed metric provides a *direct* error-probability-based secrecy metric that is typically used for the practical implementation of actual secure wireless systems over fading channels.

-
- A metric evaluating the average information leakage rate is proposed. This proposed secrecy metric gives an answer to the important question of how fast or how much the confidential information is leaked to the eavesdropper when perfect secrecy is not achieved.

The results in this chapter have been presented in the following publications which are listed again for ease of reference:

- J4. **B. He**, X. Zhou, and A. L. Swindlehurst, “On secrecy metrics for physical layer security over quasi-static fading channels,” submitted to *IEEE Trans. Wireless Commun.*, Jan. 2016.
- C2. **B. He** and X. Zhou, “New physical layer security measures for wireless transmissions over fading channels,” in *Proc. IEEE GLOBECOM*, Austin, TX, Dec. 2014, pp. 722–727.

Secure On-Off Transmission Design with Channel Estimation Errors

2.1 Introduction

One of the key features in providing physical layer security is that the CSI of both the legitimate receiver and the eavesdropper often needs to be known by the transmitter to enable secure encoding and advanced signaling. However, the assumption of perfectly knowing the CSI is almost impossible in practice. This chapter aims to reduce the dependence of physical layer security on the impractical assumption of perfect CSI. Specifically, we study the impact of channel estimation errors on secure on-off transmissions designs.

In recent years, increasing attention has been paid to the impact of the uncertainty in the CSI of both legitimate receiver and eavesdropper's channels at the transmitter, e.g., [31, 37, 46, 47, 48]. Usually, the CSI is obtained at the receiver by channel estimation during pilot transmission [61]. Then, a feedback link (if available) is used to send the CSI to the transmitter. Hence, the accuracy of the channel estimation at the receiver affects the quality of CSI at the transmitter. In the literature of physical layer security, most existing studies assumed that the legitimate receiver has perfect channel estimation. Clearly, this assumption is not practical, since the channel estimation problem usually is not error-free. Previous studies on the physical layer security considering the imperfect channel estimation at the receiver side can be found in [28, 36, 38], where [28, 36] considered the channel estimation error at the legitimate receiver and [38] considered the channel estimation error at both the legitimate receiver and the eavesdropper. Specifically, Taylor *et al.* presented the impact of the legitimate receiver's channel estimation error on the performance of an eigenvector-based jamming technique in [36]. Their research showed that the ergodic secrecy rate provided by the jamming technique decreases rapidly as the channel estimation error increases. Zhou and McKay analyzed the optimal power allocation of the AN for the secure transmission considering the impact of imperfect CSI at the legitimate receiver in [28]. They found that it is wise to create more AN by compromising on the transmit power of information-bearing signals when the CSI

is imperfectly obtained. Liu *et al.* [38] adopted the secrecy beamforming scheme to investigate the joint design of training and data transmission signals for wiretap channels. They derived the ergodic secrecy rate for practical systems with imperfect channel estimations at both the legitimate receiver and the eavesdropper, and found the optimal tradeoff between the energy used for training and data signals based on the achievable ergodic secrecy rate.

The aforementioned works in [28, 36, 38] all used the ergodic secrecy rate to characterize the performance limits of systems. The ergodic secrecy rate is an appropriate secrecy metric for systems in which the encoded messages span sufficient channel realizations to capture the ergodic features of the fading channel [16]. In addition, the works in [28, 36, 38] implicitly assumed variable-rate transmission strategies where the encoding rates are adaptively chosen according to the instantaneous channel gains. The system achieving the ergodic secrecy rate has the implicit assumption of the variable-rate transmission, which is very different from traditional ergodic fading scenarios without the secrecy consideration. A detailed explanation can be found in [16]. In practice, communication systems sometimes prefer non-adaptive rate transmission to reduce complexity and applications like video streams in multimedia often require fixed encoding rates. Thus, variable-rate transmission strategies are not always feasible.

The remainder of this chapter is organized as follows. Section 2.2 gives the system model and the assumptions on channel knowledge. Section 2.3 analyzes the secure on-off transmission design for systems with fixed encoding rates. Section 2.4 develops two joint rate and on-off transmission designs depending on whether the encoding rates are non-adaptive or adaptive.¹ Numerical results and the summary of this chapter are given in Sections 2.5 and 2.6, respectively.

2.2 System Model

We consider a three-node wireless network in which a transmitter, Alice, wants to send confidential information to an intended user, Bob, in the presence of an eavesdropper, Eve. Alice, Bob and Eve are assumed to have a single antenna each. Both Bob and Eve are mobile users served by the BS, Alice. In order to secure the transmission to Bob against Eve, Alice tracks the channel qualities of both mobile stations by asking them to feed back their estimated instantaneous channel qualities through error-free feedback links. Note that only the channel quality, which is a real number as opposed to the complex channel coefficient, is required to feed back to Alice.

The main assumptions on the system model made in this chapter are listed as follows.

- (a) We assume quasi-static fading channels and adopt the block fading model [62], where

¹The system with non-adaptive rates in Section 2.4 is different from the system with fixed rates in Section 2.3. The fixed rates indicate that the encoding rates are given and cannot be chosen freely, while the non-adaptive rates indicate that the encoding rates can be chosen in the design process but are constant for all message transmissions.

the channel gains remain constant over a block of symbols (i.e., the transmission of one message) and change independently from one block to the next.

- (b) The block-wise transmission is adopted. At the start of each block, pilot symbols are transmitted to enable channel estimation at the receiver. Then, both Bob and Eve estimate their channels and feed the estimated channel qualities back to Alice. Finally, the data symbols are transmitted.
- (c) We assume that the transmission power of the pilot symbol can be different from the transmission power of the data symbol.
- (d) We assume that the duration of a block is sufficiently long. For simplicity, the time spent on training and feedback is negligible compared with the data transmission time.
- (e) We assume that the average SNRs at both Bob and Eve, without the consideration of channel estimation errors, are known at Alice.

The data symbol transmitted by Alice is denoted by d . The transmission power of the data symbol is normalized so that $\mathbb{E}\{|d|^2\} = 1$. The pilot symbol is denoted by t . The ratio of pilot power to data power is denoted by

$$\psi = \frac{\mathbb{E}\{|t|^2\}}{\mathbb{E}\{|d|^2\}} = \mathbb{E}\{|t|^2\}. \quad (2.1)$$

Since $\mathbb{E}\{|d|^2\} = 1$, we call ψ as the normalized pilot power (normalized by data power). The received symbols at Bob and Eve are given by

$$y_b = \sqrt{\alpha_b} h_b x + n_b \quad (2.2)$$

and

$$y_e = \sqrt{\alpha_e} h_e x + n_e, \quad (2.3)$$

respectively, where $h_b \sim \mathcal{CN}(0,1)$ and $h_e \sim \mathcal{CN}(0,1)$ denote the normalized channel gain from Alice to Bob and the normalized channel gain from Alice to Eve, respectively. We assume that h_b and h_e are independent. This assumption is reasonable for rich-scattering environment where Bob and Eve are not very close to each other. The additive white Gaussian noise (AWGN) at Bob is denoted by $n_b \sim \mathcal{CN}(0,1)$ and the AWGN at Eve is denoted by $n_e \sim \mathcal{CN}(0,1)$. The transmitted signal x can be a data symbol, d , or a pilot symbol, t . We further assume that the data power is normalized to unity, i.e., $\mathbb{E}\{|x|^2\} = 1$. The average (data) SNRs at Bob and Eve without the consideration of channel estimation errors are denoted by α_b and α_e , respectively. In fact, α_b and α_e indicate the overall channel conditions between the transmitter and the receivers. For example, $\alpha_b > \alpha_e$ may indicate that the distance between Alice and Bob is smaller than the distance between Alice and Eve.

2.2.1 Channel Estimation

We assume that Bob's channel is estimated by the minimum mean square error (MMSE) estimator during pilot transmission. The estimation of Bob's channel gain and the estimation error are denoted by \hat{h}_b and \tilde{h}_b , respectively. Thus,

$$h_b = \hat{h}_b + \tilde{h}_b, \quad (2.4)$$

where \hat{h}_b and \tilde{h}_b are assumed to have zero-mean complex Gaussian distributions. The assumption of Gaussian distributed channel estimation error arises from the use of MMSE estimator for channel estimation in the Bayesian linear model [63], e.g., the pilot-symbol-aided channel estimation [64]. More specifically, since the channel coefficient, h_b , has a complex Gaussian distribution and the received signal, y_b , is a linear function of the channel coefficient, the linear MMSE estimation becomes the optimal MMSE estimation. Thus, by using a linear estimator, the estimated channel coefficient and the estimation error are zero-mean complex Gaussian distributed. In fact, $|\hat{h}_b|$ is what Bob feeds back to Alice as the estimated instantaneous channel quality. The orthogonality principle implies $E\{|h_b|^2\} = E\{|\hat{h}_b|^2\} + E\{|\tilde{h}_b|^2\}$. According to [65], the variance of channel estimation error is given by

$$\varsigma_b = E\{|\tilde{h}_b|^2\} = \frac{1}{1 + \psi\alpha_b T_t}, \quad (2.5)$$

where T_t is the length of pilot transmission. We assumed that $T_t = 1$. Hence the effect of channel training is solely characterized by the normalized pilot power, ψ . For convenience, we let $\hat{\gamma}_b = \alpha_b |\hat{h}_b|^2$ and $\tilde{\gamma}_b = \alpha_b |\tilde{h}_b|^2$, each having an exponential distribution given by

$$f_{\hat{\gamma}_b}(\hat{\gamma}_b) = \frac{1}{\alpha_b(1 - \varsigma_b)} \exp\left(-\frac{\hat{\gamma}_b}{\alpha_b(1 - \varsigma_b)}\right), \quad \hat{\gamma}_b > 0, \quad (2.6)$$

$$f_{\tilde{\gamma}_b}(\tilde{\gamma}_b) = \frac{1}{\alpha_b \varsigma_b} \exp\left(-\frac{\tilde{\gamma}_b}{\alpha_b \varsigma_b}\right), \quad \tilde{\gamma}_b > 0. \quad (2.7)$$

Bob uses the estimated channel gain for data detection, and the actual instantaneous SNR at Bob can be written as [66]

$$\gamma_b = \frac{\alpha_b |\hat{h}_b|^2}{\alpha_b |\tilde{h}_b|^2 + 1} = \frac{\hat{\gamma}_b}{\tilde{\gamma}_b + 1}. \quad (2.8)$$

We assume that Eve's channel is also estimated by the MMSE estimator. The estimation of Eve's channel gain and the estimation error are denoted by \hat{h}_e and \tilde{h}_e , respectively. Thus,

$$h_e = \hat{h}_e + \tilde{h}_e. \quad (2.9)$$

Under the assumption of MMSE estimator for channel estimation in the Bayesian linear model, \hat{h}_e and \tilde{h}_e have zero-mean complex Gaussian distributions. In fact, $|\hat{h}_e|$ is what Eve is required

to feed back to Alice as the estimated instantaneous channel quality. The orthogonality principle implies $E\{|h_e|^2\} = E\{|\hat{h}_e|^2\} + E\{|\tilde{h}_e|^2\}$. In addition, the variance of channel estimation error is given by

$$\zeta_e = E\{|\tilde{h}_e|^2\} = \frac{1}{1 + \psi \alpha_e T_t}, \quad (2.10)$$

where we assume that $T_t = 1$. Similarly, we let $\hat{\gamma}_e = \alpha_e |\hat{h}_e|^2$ and $\tilde{\gamma}_e = \alpha_e |\tilde{h}_e|^2$, each having an exponential distribution given by

$$f_{\hat{\gamma}_e}(\hat{\gamma}_e) = \frac{1}{\alpha_e(1 - \zeta_e)} \exp\left(-\frac{\hat{\gamma}_e}{\alpha_e(1 - \zeta_e)}\right), \quad \hat{\gamma}_e > 0, \quad (2.11)$$

$$f_{\tilde{\gamma}_e}(\tilde{\gamma}_e) = \frac{1}{\alpha_e \zeta_e} \exp\left(-\frac{\tilde{\gamma}_e}{\alpha_e \zeta_e}\right), \quad \tilde{\gamma}_e > 0. \quad (2.12)$$

With the MMSE channel estimation, the actual instantaneous SNR for data detection at Eve can be written as

$$\gamma_e = \frac{\alpha_e |\hat{h}_e|^2}{\alpha_e |\tilde{h}_e|^2 + 1} = \frac{\hat{\gamma}_e}{\tilde{\gamma}_e + 1}. \quad (2.13)$$

It is worth mentioning that in principle Eve is able to further improve the channel estimation by performing joint channel and data detection, while Alice has no mechanism to tell if this is the case. As a robust approach for achieving secrecy, Alice may assume the worst case scenario where Eve perfectly knows her own channel. Then, the actual instantaneous SNR at Eve is $\gamma_e = \alpha_e |h_e|^2$, which has an exponential distribution given by

$$f_{\gamma_e}(\gamma_e) = \frac{1}{\alpha_e} \exp\left(-\frac{\gamma_e}{\alpha_e}\right), \quad \gamma_e > 0. \quad (2.14)$$

2.2.2 Channel Knowledge

As mentioned before, Alice asks both Bob and Eve to feed back their estimated instantaneous channel qualities after the pilot transmission phase. Since Bob is the intended user, we simply assume that Alice has and trusts the feedback from Bob with the knowledge of $\hat{\gamma}_b = \alpha_b |\hat{h}_b|^2$ as Bob's estimated instantaneous SNR. The actual instantaneous SNR at Bob is given in (2.8). However, Eve is an eavesdropper, and may not cooperate with Alice. Hence, Alice may not obtain or trust the feedback information from Eve. We specifically investigate the following three scenarios with different assumptions on the channel knowledge:

- Scenario 1: Alice has and trusts the feedback from Eve, knowing $\hat{\gamma}_e = \alpha_e |\hat{h}_e|^2$ as the estimate of the instantaneous SNR at Eve. Eve uses the MMSE channel estimate \hat{h}_e for data detection, and hence the actual instantaneous SNR at Eve is given in (2.13).
- Scenario 2: Alice has and trusts the feedback from Eve, knowing $\hat{\gamma}_e = \alpha_e |\hat{h}_e|^2$ as the

estimate of the instantaneous SNR at Eve. Eve is assumed to perfectly know her own channel, and the actual instantaneous SNR at Eve is $\gamma_e = \alpha_e |h_e|^2$.

- Scenario 3: Alice does not have or trust Eve's feedback, and hence has no knowledge about Eve's instantaneous channel. However, the statistics of Eve's channel, i.e., α_e , is still assumed to be known at Alice. Eve perfectly knows her own channel, and the actual instantaneous SNR at Eve is $\gamma_e = \alpha_e |h_e|^2$.

In fact, the three scenarios above can also be interpreted as follows. Scenario 1 represents the case where Eve is exactly identical to other mobile users. Scenario 2 generally represents the case where Alice has partial information about Eve's channel gain, while allowing Eve to have perfect knowledge on her own channel. Scenario 3 is valid for the case where Alice has no feedback from Eve. This scenario is perhaps the most practical one with current communication protocols where the channel feedback is only obtained from the intended receiver. Scenario 3 is also a robust approach for secrecy that allows Eve to have malicious behaviors, e.g., feeding wrong information back to Alice.

We note that Scenario 2 is the least-practical amongst the three scenarios. It is worth highlighting the value of studying Scenario 2 in this chapter. From the legitimate users' perspectives, Scenario 1 represents the most desirable case, where Alice has the feedback from Eve and Eve has imperfect CSI. In contrast, Scenario 3 represents the worst case, where Alice has no feedback from Eve and Eve has perfect CSI. There are two different CSI assumptions between these two scenarios, one on the feedback from Eve to Alice and the other on the CSI knowledge at Eve. From theoretical point of view, it is meaningful to evaluate the impact of changing one of the CSI assumptions on the secure transmission design. To this end, Scenario 2 is introduced as it differs from Scenario 1 or 3 in only one CSI assumption. The study of Scenario 2 enables us to compare the secure transmissions with different CSI assumptions changing in step. Specifically, we can learn the effect of the having different CSI qualities at Eve by comparing Scenarios 1 and 2. We can find the impact of the availability of CSI feedback at Alice by comparing Scenarios 2 and 3.

2.2.3 Secure Encoding

We consider the widely-adopted wiretap code [13] as introduced in Section 1.1.1 for the message transmissions. The two rate parameters are the codeword transmission rate, R_b , and the confidential information rate, R_s . The positive rate difference $R_e = R_b - R_s$ is the cost to provide secrecy against the eavesdropper. From [13] [67, Theorem 1] [68, Definition 2], perfect secrecy cannot be achieved when $R_e < C_e$, where C_e denotes Eve's channel capacity, $C_e = \log_2(1 + \gamma_e)$. Also, Bob is unable to decode the received codewords correctly when $R_b > C_b$, where C_b denotes Bob's channel capacity, $C_b = \log_2(1 + \gamma_b)$. Thus, given a pair of the rate choices, R_b

and R_s , the secrecy outage probability [19], p_{so} , and the connection outage probability, p_{co} , are given as

$$p_{\text{so}} = \mathbb{P}(C_e > R_b - R_s \mid \text{message transmission}), \quad (2.15)$$

$$p_{\text{co}} = \mathbb{P}(C_b < R_b \mid \text{message transmission}). \quad (2.16)$$

Note that both outage probabilities are conditioned on the message transmission. The secrecy level and the reliability level of a transmission scheme can then be measured by the secrecy outage probability and the connection outage probability, respectively.

2.3 On-Off Transmission Design

In the following, we consider each of the three scenarios described in Section 2.2 and show how to design transmission schemes with good throughput performance, whilst satisfying the secrecy and reliability constraints. In particular, we consider the on-off transmission scheme: Alice decides whether or not to transmit according to the information about Bob and Eve's estimated instantaneous SNRs, i.e., transmission takes place when the estimated instantaneous SNR at Bob, $\hat{\gamma}_b$, is greater than a certain threshold, μ_b , and the estimated instantaneous SNR at Eve, $\hat{\gamma}_e$, is less than another threshold, μ_e , while transmission is suspended when $\hat{\gamma}_b \leq \mu_b$ or $\hat{\gamma}_e \geq \mu_e$. Since the secrecy and reliability performances are related to different channels, which can be seen from (2.15) and (2.16), it is reasonable to set two separate SNR thresholds on Bob's channel and Eve's channel, respectively. In the scenario where Alice does not have or trust the feedback from Eve, there is no on-off SNR threshold on Eve's channel, μ_e , or equivalently $\mu_e = \infty$.

We assume that the encoding rates have already been designed such that both the codeword transmission rate, R_b , and the confidential information rate, R_s , are fixed. The design problem is to maximize the throughput, η , subject to two constraints, one on the secrecy performance and the other on the reliability performance, which can be written as

$$\max_{\mu_b, \mu_e} \quad \eta = p_{\text{tx}} (1 - p_{\text{co}}) R_s, \quad (2.17)$$

$$\text{s.t.} \quad p_{\text{so}} \leq \varphi, p_{\text{co}} \leq \delta, \quad (2.18)$$

where p_{tx} denotes the probability of transmission due to the on-off transmission scheme, $\varphi \in [0, 1]$ and $\delta \in [0, 1]$ represent the secrecy and reliability requirements. The maximum acceptable secrecy outage probability is φ , and the maximum acceptable connection outage probability is δ . The controllable parameters to design are the two on-off SNR thresholds, μ_b and μ_e .

Note that the overhead of pilot and feedback is not considered for calculating the throughput in (2.17), since we assume a sufficiently long block length for simplicity. If the pilot

transmission and feedback time is considered, we can simply introduce a new parameter, say ϖ , to represent the ratio of pilot transmission and feedback time to data transmission time. Then, the throughput can be calculated by taking this ratio, ϖ , into account, i.e., (2.17) will change to $\eta = \frac{1}{1+\varpi} p_{\text{tx}} (1 - p_{\text{co}}) R_s$.

In what follows, we consider the transmission design in the three different scenarios described in Section 2.2. For each scenario, the transmission probability, the connection outage probability and the secrecy outage probability are derived firstly. Then, the feasibility of secrecy and reliability constraints is discussed. Here the feasibility of constraints means that the constraints can be satisfied whilst achieving a positive information rate. Finally, the solution of the optimization problem is given as a proposition.

2.3.1 Scenario One

Derivations of p_{tx} , p_{co} and p_{so} : Since Bob's estimated instantaneous SNR is independent with Eve's estimated instantaneous SNR, the probability of transmission in Scenario 1 is given as

$$\begin{aligned} p_{\text{tx}} &= \mathbb{P}(\hat{\gamma}_b > \mu_b) \mathbb{P}(\hat{\gamma}_e < \mu_e) \\ &= \exp\left(-\frac{\mu_b}{\alpha_b(1-\zeta_b)}\right) \left(1 - \exp\left(-\frac{\mu_e}{\alpha_e(1-\zeta_e)}\right)\right). \end{aligned} \quad (2.19)$$

Since $\gamma_b \leq \hat{\gamma}_b$ according to (2.8) and Bob can decode the message without error only when $C_b \geq R_b$, it is wise to choose the value of μ_b satisfying

$$\log_2(1 + \mu_b) \geq R_b \Rightarrow \mu_b \geq 2^{R_b} - 1. \quad (2.20)$$

Then, the connection outage probability in Scenario 1 is given by

$$\begin{aligned} p_{\text{co}} &= \mathbb{P}(\log_2(1 + \gamma_b) < R_b \mid \hat{\gamma}_b > \mu_b) \\ &= \mathbb{P}\left(\log_2\left(1 + \frac{\hat{\gamma}_b}{\tilde{\gamma}_b + 1}\right) < R_b \mid \hat{\gamma}_b > \mu_b\right) \\ &= \frac{\mathbb{P}(\mu_b < \hat{\gamma}_b < (2^{R_b} - 1)(\tilde{\gamma}_b + 1))}{\mathbb{P}(\hat{\gamma}_b > \mu_b)} \\ &= \exp\left(\frac{\mu_b}{\alpha_b(1-\zeta_b)}\right) \int_{\frac{\mu_b}{2^{R_b}-1}-1}^{\infty} \left(\int_{\mu_b}^{(2^{R_b}-1)(\tilde{\gamma}_b+1)} f_{\hat{\gamma}_b}(\hat{\gamma}_b) d\hat{\gamma}_b\right) f_{\tilde{\gamma}_b}(\tilde{\gamma}_b) d\tilde{\gamma}_b \\ &= \frac{\zeta_b(2^{R_b}-1)}{1+\zeta_b(2^{R_b}-2)} \exp\left(\frac{1}{\alpha_b\zeta_b} \left(1 - \frac{\mu_b}{2^{R_b}-1}\right)\right). \end{aligned} \quad (2.21)$$

The secrecy outage probability in Scenario 1 is given by

$$\begin{aligned}
p_{\text{so}} &= \mathbb{P}(C_e > R_b - R_s \mid \hat{\gamma}_e < \mu_e) \\
&= \mathbb{P}\left(\log_2\left(1 + \frac{\hat{\gamma}_e}{\tilde{\gamma}_e + 1}\right) > R_b - R_s \mid \hat{\gamma}_e < \mu_e\right) \\
&= \frac{\mathbb{P}\left((2^{R_b - R_s} - 1)(\tilde{\gamma}_e + 1) < \hat{\gamma}_e < \mu_e\right)}{\mathbb{P}(\hat{\gamma}_e < \mu_e)}. \tag{2.22}
\end{aligned}$$

If $\mu_e \leq 2^{R_b - R_s} - 1$, we get $p_{\text{so}} = 0$. If $\mu_e > 2^{R_b - R_s} - 1$, we have

$$\begin{aligned}
p_{\text{so}} &= \frac{\int_0^{\frac{\mu_e}{2^{R_b - R_s} - 1} - 1} \left(\int_{(2^{R_b - R_s} - 1)(\tilde{\gamma}_e + 1)}^{\mu_e} f_{\hat{\gamma}_e}(\hat{\gamma}_e) d\hat{\gamma}_e \right) f_{\tilde{\gamma}_e}(\tilde{\gamma}_e) d\tilde{\gamma}_e}{1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)} \\
&= \frac{\frac{1 - \zeta_e}{1 + \zeta_e(2^{R_b - R_s} - 2)} \exp\left(-\frac{2^{R_b - R_s} - 1}{\alpha_e(1 - \zeta_e)}\right) - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)}{1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)} \\
&\quad + \frac{\frac{\zeta_e(2^{R_b - R_s} - 1)}{1 + \zeta_e(2^{R_b - R_s} - 2)} \exp\left(\frac{1}{\alpha_e} \left(\frac{1}{\zeta_e} - \frac{\mu_e}{1 - \zeta_e} - \frac{\mu_e}{\zeta_e(2^{R_b - R_s} - 1)} \right)\right)}{1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)}. \tag{2.23}
\end{aligned}$$

From (2.21), we find that the value of the on-off SNR threshold on Bob's channel needs to be very large such that μ_b goes to infinity, if the reliability constraint is very stringent such that p_{co} is required to go to zero. When μ_b goes to infinity, the throughput η will approach zero. Thus, it is interesting to investigate the behaviors of η and p_{co} for the limiting case where μ_b goes to infinity. From (2.17), (2.19) and (2.21), we see that both η and p_{co} are exponential functions of μ_b as μ_b goes to infinity. Then, the slopes of η and p_{co} with respect to μ_b go to zero as μ_b goes to infinity.

From (2.22) and (2.23), we find that the secrecy outage probability is directly influenced by the value of μ_e but not related to μ_b . If $\mu_e \leq 2^{R_b - R_s} - 1$, perfect secrecy is achievable in Scenario 1. Since $\hat{\gamma}_e \geq \gamma_e$ in Scenario 1, the estimate of Eve's instantaneous SNR is an upper bound of the actual Eve's instantaneous SNR. Hence, Alice can make sure that $C_e < R_b - R_s$ by having $\mu_e \leq 2^{R_b - R_s} - 1$. According to (2.23), we also find that the secrecy outage probability increases as μ_e increases if $\mu_e > 2^{R_b - R_s} - 1$.

Feasibility of Constraints: From (2.21), we find that p_{co} is a decreasing function of μ_b and

$$\lim_{\mu_b \rightarrow +\infty} p_{\text{co}} = 0. \tag{2.24}$$

Thus, the feasible range of the reliability constraint in Scenario 1 is given by

$$0 < \delta \leq 1. \tag{2.25}$$

According to (2.22), p_{so} is an increasing function of μ_e and $p_{\text{so}} = 0$ as long as $\mu_e \leq 2^{R_b - R_s} - 1$. Thus, the feasible range of the secrecy constraint in Scenario 1 is given by

$$0 \leq \varphi \leq 1. \quad (2.26)$$

Hence, any required reliability and secrecy constraints are feasible by appropriately adjusting the on-off thresholds. It is noted that perfect secrecy, i.e., $\varphi = 0$, can be achieved.

The following proposition summarizes the solution to the design problem in Scenario 1, where the optimal μ_b is expressed in a closed form and the optimal μ_e is obtained by numerically solving an equation.

Proposition 2.1. The optimal parameters of the throughput-maximizing transmission scheme in Scenario 1 are given as follows:

$$\mu_b = \begin{cases} 2^{R_b} - 1, & \text{if } R_b \leq \log_2 \left(1 + \frac{(1-\zeta_b)\delta}{\zeta_b(1-\delta)} \right) \\ (2^{R_b} - 1) \left(1 - \alpha_b \zeta_b \ln \left(\delta \frac{1+\zeta_b(2^{R_b}-2)}{\zeta_b(2^{R_b}-1)} \right) \right), & \text{otherwise,} \end{cases} \quad (2.27)$$

$$\mu_e = \begin{cases} +\infty, & \text{if } \frac{1-\zeta_e}{1+\zeta_e(2^{R_b-R_s}-2)} \exp \left(-\frac{2^{R_b-R_s}-1}{\alpha_e(1-\zeta_e)} \right) \leq \varphi \\ F_1, & \text{otherwise,} \end{cases} \quad (2.28)$$

where F_1 is the solution of μ_e to the equation

$$\varphi = \frac{\frac{1-\zeta_e}{1+\zeta_e(2^{R_b-R_s}-2)} \exp \left(-\frac{2^{R_b-R_s}-1}{\alpha_e(1-\zeta_e)} \right) - \exp \left(-\frac{\mu_e}{\alpha_e(1-\zeta_e)} \right)}{1 - \exp \left(-\frac{\mu_e}{\alpha_e(1-\zeta_e)} \right)} + \frac{\frac{\zeta_e(2^{R_b-R_s}-1)}{1+\zeta_e(2^{R_b-R_s}-2)} \exp \left(\frac{1}{\alpha_e} \left(\frac{1}{\zeta_e} - \frac{\mu_e}{1-\zeta_e} - \frac{\mu_e}{\zeta_e(2^{R_b-R_s}-1)} \right) \right)}{1 - \exp \left(-\frac{\mu_e}{\alpha_e(1-\zeta_e)} \right)}. \quad (2.29)$$

Proof: See Appendix A.1. ■

Remark 2.1. In this scenario, if the transmitter increases the pilot power, the estimation errors at both the legitimate receiver and the eavesdropper will reduce. Thus, the selection of normalized pilot power, ψ , will create an interesting tradeoff between reducing the estimation errors at the legitimate receiver and reducing the estimation errors at the eavesdropper. Here, we briefly discuss the method to calculate the optimal ψ as follows, instead of providing a detailed analysis. First, we need to find the expressions of optimal μ_b and μ_e in terms of ψ by substituting (2.5) and (2.10) into (2.27) and (2.28), respectively. Then, p_{tx} and p_{co} can be expressed as functions of ψ . Finally, the optimal ψ is the solution to the optimization problem

of

$$\max_{\psi} \quad \eta = p_{\text{tx}}(\psi) (1 - p_{\text{co}}(\psi)) R_s, \quad (2.30)$$

$$s.t. \quad \psi > 0. \quad (2.31)$$

Due to the complicated expressions for the optimal μ_b and μ_e , the closed-form expression for the optimal ψ is mathematically intractable. But this problem can be solved numerically.

2.3.2 Scenario Two

Derivations of p_{tx} , p_{co} and p_{so} : The derivations of the probability of transmission and the connection outage probability in Scenario 2 are the same as (2.19) and (2.21) in Scenario 1, respectively. The secrecy outage probability in Scenario 2 is given by

$$\begin{aligned} p_{\text{so}} &= \mathbb{P}(C_e > R_b - R_s \mid \hat{\gamma}_e < \mu_e) \\ &= \mathbb{P}(\log_2(1 + \gamma_e) > R_b - R_s \mid \hat{\gamma}_e < \mu_e) \\ &= \frac{\mathbb{P}(\gamma_e > 2^{R_b - R_s} - 1, \hat{\gamma}_e < \mu_e)}{\mathbb{P}(\hat{\gamma}_e < \mu_e)} \\ &= \frac{\int_0^{\mu_e} \left(\int_{2^{R_b - R_s} - 1}^{\infty} f_{\gamma_e | \hat{\gamma}_e}(\gamma_e | \hat{\gamma}_e) d\gamma_e \right) f_{\hat{\gamma}_e}(\hat{\gamma}_e) d\hat{\gamma}_e}{1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)}. \end{aligned} \quad (2.32)$$

According to the definitions of γ_e and $\hat{\gamma}_e$ in Scenario 2, γ_e conditioned on its estimate, $\hat{\gamma}_e$, follows a non-central chi-square distribution with two degrees of freedom. Applying the cumulative distribution function of the non-central chi-square distribution, we have

$$\int_{2^{R_b - R_s} - 1}^{\infty} f_{\gamma_e | \hat{\gamma}_e}(\gamma_e | \hat{\gamma}_e) d\gamma_e = Q_1 \left(\sqrt{\frac{2\hat{\gamma}_e}{\alpha_e \zeta_e}}, \sqrt{\frac{2^{R_b - R_s} - 1}{\alpha_e \zeta_e}} \right), \quad (2.33)$$

where $Q_x(a, b)$ represents the Marcum Q-function [69]. Thus, the secrecy outage probability in Scenario 2 can be rewritten as

$$\begin{aligned} p_{\text{so}} &= \frac{\int_0^{\mu_e} Q_1 \left(\sqrt{\frac{2\hat{\gamma}_e}{\alpha_e \zeta_e}}, \sqrt{\frac{2^{R_b - R_s} - 1}{\alpha_e \zeta_e}} \right) f_{\hat{\gamma}_e}(\hat{\gamma}_e) d\hat{\gamma}_e}{1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)} \\ &= \frac{\int_0^{\mu_e} \exp\left(-\frac{\hat{\gamma}_e}{\alpha_e(1 - \zeta_e)}\right) Q_1 \left(\sqrt{\frac{2\hat{\gamma}_e}{\alpha_e \zeta_e}}, \sqrt{\frac{2^{R_b - R_s} - 1}{\alpha_e \zeta_e}} \right) d\hat{\gamma}_e}{\alpha_e(1 - \zeta_e) \left(1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right) \right)}. \end{aligned} \quad (2.34)$$

Feasibility of Constraints: Since the connection outage probability does not change from Scenario 1 to Scenario 2, the feasible range of the reliability constraint in Scenario 2 is identical

to (2.25) in Scenario 1. Since p_{so} is an increasing function of μ_e and

$$\begin{aligned}
\lim_{\mu_e \rightarrow 0} p_{\text{so}} &= \mathbb{P}(C_e > R_b - R_s \mid \hat{\gamma}_e = 0) \\
&= \mathbb{P}(\log_2(1 + \gamma_e) > R_b - R_s \mid \hat{\gamma}_e = 0) \\
&= \int_{2^{R_b - R_s} - 1}^{\infty} f_{\gamma_e \mid \hat{\gamma}_e = 0}(\gamma_e \mid \hat{\gamma}_e = 0) d\gamma_e \\
&= Q_1\left(0, \sqrt{\frac{2^{R_b - R_s + 1} - 2}{\alpha_e \zeta_e}}\right). \tag{2.35}
\end{aligned}$$

Thus, the feasible range of the secrecy constraint is given as

$$Q_1\left(0, \sqrt{\frac{2^{R_b - R_s + 1} - 2}{\alpha_e \zeta_e}}\right) < \varphi \leq 1. \tag{2.36}$$

Thus, any required reliability constraint is feasible, while the secrecy constraint is feasible only when (2.36) is satisfied.

The following proposition summarizes the solution to the design problem in Scenario 2, where the optimal μ_b is expressed in a closed form and the optimal μ_e is obtained by numerically solving an equation.

Proposition 2.2. The optimal parameters of the throughput-maximizing transmission scheme in Scenario 2 are given as follows:

$$\mu_b = \begin{cases} 2^{R_b} - 1, & \text{if } R_b \leq \log_2\left(1 + \frac{(1 - \zeta_b)\delta}{\zeta_b(1 - \delta)}\right) \\ (2^{R_b} - 1) \left(1 - \alpha_b \zeta_b \ln\left(\delta \frac{1 + \zeta_b(2^{R_b} - 2)}{\zeta_b(2^{R_b} - 1)}\right)\right), & \text{otherwise,} \end{cases} \tag{2.37}$$

$$\mu_e = \begin{cases} +\infty, & \text{if } \exp\left(-\frac{2^{R_b - R_s} - 1}{\alpha_e}\right) \leq \varphi \\ F_2, & \text{otherwise,} \end{cases} \tag{2.38}$$

where F_2 is the solution of μ_e to the equation

$$\varphi = \frac{\int_0^{\mu_e} \exp\left(-\frac{\hat{\gamma}_e}{\alpha_e(1 - \zeta_e)}\right) Q_1\left(\sqrt{\frac{2\hat{\gamma}_e}{\alpha_e \zeta_e}}, \sqrt{\frac{2^{R_b - R_s + 1} - 2}{\alpha_e \zeta_e}}\right) d\hat{\gamma}_e}{\alpha_e(1 - \zeta_e) \left(1 - \exp\left(-\frac{\mu_e}{\alpha_e(1 - \zeta_e)}\right)\right)}. \tag{2.39}$$

Proof: See Appendix A.2. ■

Remark 2.2. In this scenario, when the secrecy constraint is very stringent such that p_{so} converges to its limit in (2.35), the value of the on-off SNR threshold on Eve's channel needs to be very small such that μ_e goes to zero. However, if μ_e goes to zero, we have the throughput η goes to zero. Thus, it is interesting to investigate the behavior of η for the limiting case where μ_e goes to zero or equivalently p_{so} converges to its limit. From (2.17) and (2.19), we

can rewrite η as

$$\eta(\mu_e) = A(1 - \exp(-B\mu_e)), \quad (2.40)$$

where $A = \exp\left(-\frac{\mu_b}{\alpha_b(1-\zeta_b)}\right)(1-p_{\text{co}})R_s$ and $B = \frac{1}{\alpha_e(1-\zeta_e)}$. The Taylor expansion of the above function around $\mu_e = 0$ is given by

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{\eta^{(n)}(0)\mu_e^n}{n!} &= A \left(1 - \sum_{n=0}^{\infty} (-1)^n \frac{B^n \mu_e^n}{n!} \right) \\ &= A(1 - (1 - B\mu_e + O(\mu_e^2))) \\ &= AB\mu_e - O(\mu_e^2), \end{aligned} \quad (2.41)$$

where $O(\cdot)$ denotes the less-significant terms, and expresses the error. Thus, the most-significant term of $\eta(\mu_e)$ around $\mu_e = 0$ is

$$AB\mu_e = \frac{(1-p_{\text{co}})R_s}{\alpha_e(1-\zeta_e)} \exp\left(-\frac{\mu_b}{\alpha_b(1-\zeta_b)}\right) \mu_e, \quad (2.42)$$

and the slope of $\eta(\mu_e)$, as μ_e goes to zero, can be approximated as

$$\frac{(1-p_{\text{co}})R_s}{\alpha_e(1-\zeta_e)} \exp\left(-\frac{\mu_b}{\alpha_b(1-\zeta_b)}\right). \quad (2.43)$$

Besides, according to (2.38) in Proposition 2.2, $\mu_e = \infty$ when

$$\exp\left(-\frac{2^{R_b-R_s}-1}{\alpha_e}\right) \leq \varphi \leq 1. \quad (2.44)$$

This indicates that Alice can ignore the feedback from Eve to design the system parameters when the secrecy constraint satisfies (2.44). Therefore, the design problem in Scenario 2 is identical to the design problem in Scenario 3 when the secrecy constraint satisfies (2.44).

2.3.3 Scenario Three

In Scenario 3, Alice does not have or trust the feedback from Eve. Thus, Alice decides whether or not to transmit according to the information about Bob's estimated instantaneous SNR. Then, the on-off SNR threshold on Eve's channel, μ_e , does not exist, and there is only one parameter to design, i.e., μ_b .

Derivations of p_{tx} , p_{co} and p_{so} : The probability of transmission in Scenario 3 is given as

$$p_{\text{tx}} = \mathbb{P}(\hat{\gamma}_b > \mu_b) = \exp\left(-\frac{\mu_b}{\alpha_b(1-\zeta_b)}\right). \quad (2.45)$$

The derivation of the connection outage probability in Scenario 3 is identical to (2.21) in Scenarios 1 and 2. The secrecy outage probability in Scenario 3 is given by

$$p_{\text{so}} = \mathbb{P}(C_e > R_b - R_s) = \exp\left(-\frac{2^{R_b - R_s} - 1}{\alpha_e}\right). \quad (2.46)$$

Note that the secrecy outage probability in Scenario 3 is a constant value and uncontrollable. Thus, the secrecy constraint is either always achievable or always unachievable no matter what the value of the design parameter is.

Feasibility of Constraints: Since the connection outage probability remains the same in Scenarios 1, 2 and 3, the feasible range of the reliability constraint in Scenario 3 is identical to (2.25) in Scenarios 1 and 2. Since the secrecy outage probability in Scenario 3 is not controllable, the feasible range of the secrecy constraint in Scenario 3 is given by

$$\exp\left(-\frac{2^{R_b - R_s} - 1}{\alpha_e}\right) \leq \varphi \leq 1. \quad (2.47)$$

Thus, any required reliability constraint is feasible, while the secrecy constraint is feasible only when (2.47) is satisfied. Note that the lower bound of the feasible secrecy constraint in this scenario is the same as (2.44) in the analysis for Scenario 2. This is because the design problems in Scenarios 2 and 3 are the same when (2.44) is satisfied.

The following proposition summarizes the solution to the design problem in Scenario 3.

Proposition 2.3. The optimal parameter of the throughput-maximizing transmission scheme in Scenario 3 is given in (2.27).

Remark 2.3. Comparing the optimal solutions to the design problems in the three different scenarios, we can find that the three scenarios have the same optimal solution of μ_b but different optimal solutions of μ_e . This is because that we have the same assumption on the channel knowledge of the legitimate link but different assumptions on the channel knowledge of the eavesdropper's link in different scenarios. Besides, it is noted that the secrecy performance of systems in Scenario 3 cannot be controlled by the design parameters for the fixed rate transmission scheme. In order to control the secrecy performance of systems in Scenario 3, a detailed analysis on the joint rate and on-off transmission design for systems in Scenario 3 is provided in Section 2.4.

2.4 Joint Rate and On-Off Transmission Design

As analyzed in Section 2.3, the secrecy performance of the systems in Scenario 3 is uncontrollable if we design only the on-off transmission parameters, i.e, the on-off thresholds. In order to control the secrecy performance, we re-study the design problem in Scenario 3 considering

the joint rate and on-off transmission design. Unlike the on-off transmission design in Section 2.3 where the encoding rates, R_b and R_s , are fixed, we now allow more degrees of freedom such that R_b and R_s can be optimally chosen.

The design problem is to maximize the throughput η subject to two constraints, one on the secrecy performance and the other on the reliability performance. In Scenario 3, Alice decides whether or not to transmit according to the estimated instantaneous SNR at Bob, $\hat{\gamma}_b$. The design problem can be written as

$$\max_{\mu_b, R_b, R_s} \eta, \quad (2.48)$$

$$\text{s.t.} \quad p_{\text{so}} \leq \varphi, p_{\text{co}} \leq \delta. \quad (2.49)$$

The parameters to design are the codeword transmission rate, R_b , the confidential information rate, R_s , and the on-off SNR threshold on Bob's channel, μ_b . In the following, two different transmission schemes are derived, according to whether the encoding rates are non-adaptive or adaptive.

2.4.1 Non-Adaptive Rate Scheme

We first consider the non-adaptive rate scheme where the codeword transmission rate, R_b , and the confidential information rate, R_s , are both constant over time. The throughput for the non-adaptive rate scheme is given by

$$\eta = p_{\text{tx}}(1 - p_{\text{co}})R_s. \quad (2.50)$$

Derivations of p_{tx} , p_{co} and p_{so} : The probability of transmission is given in (2.45). The connection outage probability is given in (2.21). The secrecy outage probability is given in (2.46). Note that we can control the secrecy performance by designing R_b and R_s .

Feasibility of Constraints: Since p_{so} is independent of μ_b , the choice of μ_b does not affect p_{so} . Also, from (2.24), we can set μ_b sufficiently large to achieve any arbitrarily small p_{co} . Thus, the feasible range of the reliability constraint in the non-adaptive rate scheme is identical to (2.25). According to (2.46), p_{so} is a decreasing function of $R_b - R_s$ and

$$\lim_{R_b - R_s \rightarrow +\infty} p_{\text{so}} = 0. \quad (2.51)$$

Thus, the feasible range of the secrecy constraint in the non-adaptive rate scheme is given by

$$0 < \varphi \leq 1. \quad (2.52)$$

Note that any required reliability and secrecy constraints are feasible by appropriately choosing R_b and R_s .

In Section 2.3, p_{so} and p_{co} are independently controlled by different design parameters. However, in this Section, the choices of encoding rates affect both the connection outage probability and the secrecy outage probability. In other words, with the encoding rates controllable, p_{so} and p_{co} are related by the rate parameters. For example, from the derivations of connection and secrecy outage probabilities, a smaller R_b allows us to achieve a smaller connection outage probability but may increase the secrecy outage probability. This enables a trade-off between the feasible reliability constraint and the feasible secrecy constraint. To illustrate such a trade-off, we analyze the feasible constraints for the system with a given on-off threshold, μ_b . To satisfy $R_s > 0$ and $p_{so} \leq \varphi$, we have $2^{R_b} - 1 > \alpha_e \ln(\varphi^{-1})$. Also, from (2.20) and $p_{co} \leq \delta$, we have $2^{R_b} - 1 \leq \min\{\mu_b, F_4(\mu_b, \delta)\}$ where $F_4(\mu_b, \delta)$ is the positive solution of x to the equation

$$\mu_b = x \left(1 - \alpha_b \zeta_b \ln \left(\delta \frac{\zeta_b^x + 1 - \zeta_b}{\zeta_b^x} \right) \right). \quad (2.53)$$

Thus, for any chosen value of μ_b , the feasible constraints for having secure communication with positive confidential information rate must satisfy

$$\exp \left(- \frac{\min\{\mu_b, F_4(\mu_b, \delta)\}}{\alpha_e} \right) < \varphi. \quad (2.54)$$

From (2.53), it is easy to see that $F_4(\mu_b, \delta)$ is an increasing function of δ . Thus, according to (2.54), the minimum feasible value of φ increases with the decrease of δ . In other words, if we set a stricter reliability constraint, the feasible secrecy constraint becomes loose. Note that when the reliability constraint is sufficiently loose, $F_4(\mu_b, \delta)$ becomes always greater than μ_b , and (2.54) changes to

$$\exp \left(- \frac{\mu_b}{\alpha_e} \right) < \varphi. \quad (2.55)$$

The following proposition summarizes the solution to the design problem for the non-adaptive rate scheme, where each of the optimal μ_b and the optimal R_s is expressed as a closed-form function of R_b and the optimal R_b is obtained by numerically solving an optimization problem.

Proposition 2.4. The optimal parameters of the throughput-maximizing transmission scheme with non-adaptive rates are given as follows:

$$\mu_b = \begin{cases} 2^{R_b} - 1, & \text{if } R_b \leq \log_2 \left(1 + \frac{(1-\zeta_b)\delta}{\zeta_b(1-\delta)} \right), \\ (2^{R_b} - 1) \left(1 - \alpha_b \zeta_b \ln \left(\delta \frac{1+\zeta_b(2^{R_b}-2)}{\zeta_b(2^{R_b}-1)} \right) \right), & \text{otherwise,} \end{cases} \quad (2.56)$$

$$R_s = R_b - k, \quad \text{where } k = \log_2 \left(1 + \alpha_e \ln(\varphi^{-1}) \right), \quad (2.57)$$

R_b is obtained by solving the problem given as

$$\max_{R_b} (R_b - k) \exp\left(-\frac{\mu_b}{\alpha_b(1 - \zeta_b)}\right) \cdot \left(1 - \frac{\zeta_b(2^{R_b} - 1)}{1 + \zeta_b(2^{R_b} - 2)} \exp\left(\frac{1}{\alpha_b \zeta_b} \left(1 - \frac{\mu_b}{2^{R_b} - 1}\right)\right)\right), \quad (2.58)$$

$$\text{s.t.} \quad k < R_b < \max\left\{\log_2\left(1 + \frac{(1 - \zeta_b)\delta}{\zeta_b(1 - \delta)}\right), k + \frac{1}{\ln 2} W_0\left(2^{-k} \alpha_b(1 - \zeta_b)\right)\right\}, \quad (2.59)$$

where $W_0(\cdot)$ denotes the principal branch of the Lambert W function and μ_b is a function of R_b whose expression is formulated as (2.56).

Proof: See Appendix A.3. ■

2.4.2 Adaptive Rate Scheme

Now, we consider the scenario where the codeword transmission rate, R_b , and the confidential information rate, R_s , can be adaptively chosen according to the estimated Bob's instantaneous SNR. Since the confidential information rate, R_s , is adaptively chosen according to the instantaneous $\hat{\gamma}_b$, the throughput for the adaptive rate scheme is given by

$$\eta = \int_{\mu_b}^{\infty} (1 - p_{\text{co}}) R_s f_{\hat{\gamma}_b}(\hat{\gamma}_b) d\hat{\gamma}_b. \quad (2.60)$$

The lower limit of the integral in (2.60) is equal to μ_b , since the transmission takes place only when $\hat{\gamma}_b > \mu_b$ due to the on-off transmission scheme.

Then, we consider the design problem of finding the values of R_b, R_s and μ_b that maximize the throughput. Since R_b and R_s can be adaptively chosen according to any given $\hat{\gamma}_b$, we treat this design as a two-step optimization problem given by

Step 1: For any given $\hat{\gamma}_b$ ($\hat{\gamma}_b > \mu_b$), solve

$$\max_{R_b, R_s} (1 - p_{\text{co}}) R_s, \quad (2.61)$$

$$\text{s.t.} \quad p_{\text{so}} \leq \varphi, p_{\text{co}} \leq \delta. \quad (2.62)$$

Step 2: Choose the best μ_b to maximize the overall throughput averaged over $\hat{\gamma}_b$.

Note that the optimal R_b and R_s are obtained in Step 1 for a given value of $\hat{\gamma}_b$. Thus, the following calculations of connection and secrecy outage probabilities are conditioned on a given $\hat{\gamma}_b$.

Derivations of p_{co} and p_{so} : Since $\gamma_b \leq \hat{\gamma}_b$ and Bob can decode the message without error only when $C_b \geq R_b$, it is wise to choose the value of R_b satisfying $R_b \leq \log_2(1 + \hat{\gamma}_b)$. Then, for

any given $\hat{\gamma}_b$, the connection outage probability can be computed as

$$\begin{aligned}
p_{\text{co}} &= \mathbb{P}(\log_2(1 + \gamma_b) < R_b \mid \hat{\gamma}_b) \\
&= \mathbb{P}\left(\log_2\left(1 + \frac{\hat{\gamma}_b}{\tilde{\gamma}_b + 1}\right) < R_b \mid \hat{\gamma}_b\right) \\
&= \mathbb{P}\left(\tilde{\gamma}_b > \frac{\hat{\gamma}_b}{2^{R_b} - 1} - 1 \mid \hat{\gamma}_b\right) \\
&= \exp\left(-\frac{1}{\alpha_b \zeta_b} \left(\frac{\hat{\gamma}_b}{2^{R_b} - 1} - 1\right)\right). \tag{2.63}
\end{aligned}$$

The secrecy outage probability for the adaptive rate scheme is the same as that for the non-adaptive rate scheme, i.e., (2.46).

Feasibility of Constraints: According to (2.63), we have

$$\hat{\gamma}_b \rightarrow \infty \Rightarrow p_{\text{co}} \rightarrow 0. \tag{2.64}$$

Since p_{so} is independent of μ_b , the choice of μ_b does not affect p_{so} . We can set μ_b sufficiently large such that transmission happens only when $\hat{\gamma}_b$ is sufficiently large to achieve any arbitrarily small p_{co} . Thus, the feasible range of the reliability constraint is the same as (2.25). For the same reason as described in the non-adaptive rate scheme, the feasible range of the secrecy constraint is identical to (2.52). Therefore, any required reliability and secrecy constraints are feasible by appropriately choosing R_b and R_s .

The following proposition summarizes the solution to the design problem for the adaptive rate scheme, where the optimal μ_b is given by a closed-form solution, the optimal R_s is expressed as a closed-form function of R_b and the optimal R_b is obtained by numerically solving an optimization problem.

Proposition 2.5. The optimal parameters of the throughput-maximizing transmission scheme with adaptive rates are given as follows:

$$\mu_b = (1 + \alpha_b \zeta_b \ln \delta^{-1}) \alpha_e \ln(\varphi^{-1}), \tag{2.65}$$

$$R_s = R_b - k, \quad \text{where } k = \log_2\left(1 + \alpha_e \ln(\varphi^{-1})\right), \tag{2.66}$$

R_b is obtained by solving the problem given by

$$\max_{R_b} \quad (R_b - k) \left(1 - \exp\left(-\frac{1}{\alpha_b \zeta_b} \left(1 - \frac{\hat{\gamma}_b}{2^{R_b} - 1}\right)\right)\right), \tag{2.67}$$

$$\text{s.t.} \quad k < R_b \leq \log_2\left(1 + \frac{\hat{\gamma}_b}{1 + \alpha_b \zeta_b \ln \delta^{-1}}\right). \tag{2.68}$$

Proof: See Appendix A.4. ■

Remark 2.4. From Proposition 2.5, one can further obtain that the optimal R_b is equal to either the upper bound of R_b , i.e., $R_b = \log_2 \left(1 + \frac{\hat{\gamma}_b}{1 + \alpha_b \zeta_b \ln \delta^{-1}} \right)$, or the solution of R_b to the equation

$$\frac{dI(R_b)}{dR_b} = 0 \quad (2.69)$$

where $I(R_b) = (R_b - k) \left(1 - \exp \left(\frac{1}{\alpha_b \zeta_b} \left(1 - \frac{\hat{\gamma}_b}{2^{R_b - 1}} \right) \right) \right)$. Note that when $\zeta_b = 0$, Proposition 2.5 implies that $R_b = \log_2(1 + \gamma_b)$. This is consistent with the optimal solution of R_b in the absence of the estimation error, where the optimal codeword rate matches the capacity of Bob's channel.

2.5 Numerical Results

2.5.1 On-Off Transmission Design

In this subsection, we present the numerical results for the on-off transmission designs in the three different scenarios. The transmission rates are fixed to $R_b = 2$ and $R_s = 1$.

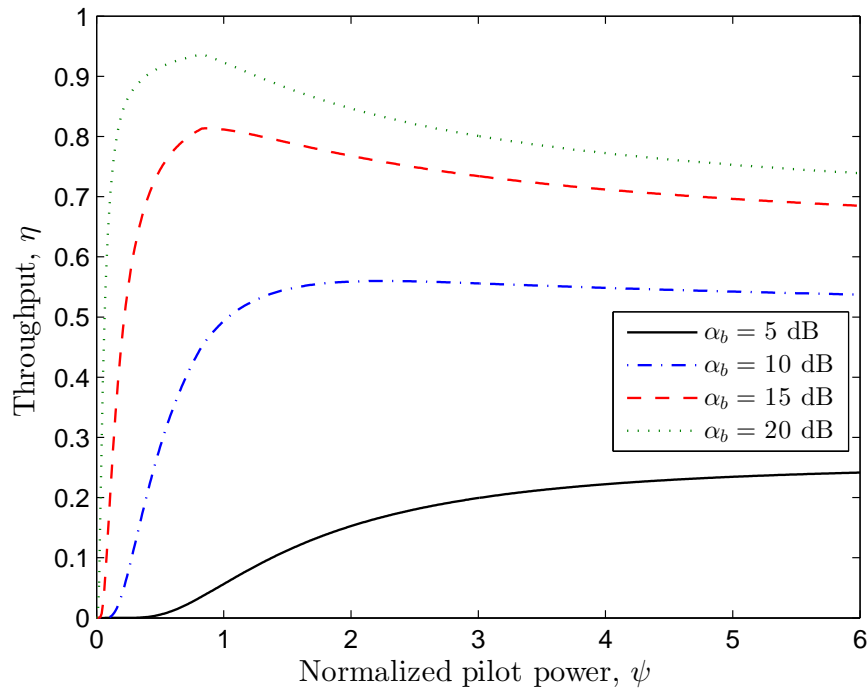


Figure 2.1: Scenario 1: Achievable throughput versus normalized pilot power for different average received data SNRs at Bob, $\alpha_b = 5$ dB, 10 dB, 15 dB, 20 dB. The other system parameters are $\delta = 0.1$, $\varphi = 0.05$, $\alpha_e = 0$ dB, $R_b = 2$, $R_s = 1$.

We first illustrate the impact of pilot power on the achievable throughput of the confidential information. Figures 2.1 and 2.2 plot η versus ψ for Scenarios 1 and 2, respectively. As shown

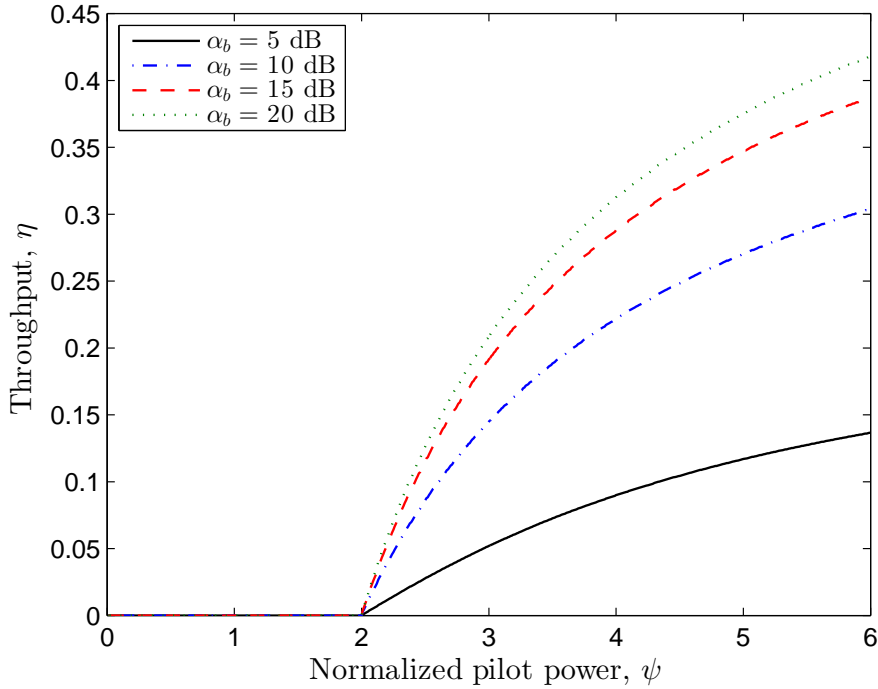


Figure 2.2: Scenario 2: Achievable throughput versus normalized pilot power for different average received data SNRs at Bob, $\alpha_b = 5$ dB, 10 dB, 15 dB, 20 dB. The other system parameters are $\delta = 0.1$, $\varphi = 0.05$, $\alpha_e = 0$ dB, $R_b = 2$, $R_s = 1$.

in Figure 2.1, the throughput does not always increase with the increase of normalized pilot power. As the curves of $\alpha_b = 10$ decibel (dB), 15 dB, 20 dB present, the throughput increases fast to a peak when the normalized pilot power increases to the optimal value ($\psi = 2.28$ for $\alpha_b = 10$ dB, $\psi = 0.87$ for $\alpha_b = 15$ dB, $\psi = 0.83$ for $\alpha_b = 20$ dB). After achieving the peak value, the throughput decreases with the increase of the normalized pilot power. This interesting observation is explained as follows. In Scenario 1, both Bob and Eve estimate their channels via the pilot transmission and feed the channel estimates back to Alice. Increasing pilot power not only enhances the legitimate users' knowledge about the channels, which has a positive effect on the secure transmission, but also increases the accuracy of channel estimation at the eavesdropper, which incurs a negative effect on the secure transmission. Before the normalized pilot power reaches the optimal value, obtaining a good channel knowledge at the legitimate users is more important than keeping the eavesdropper's channel estimation inaccurate. After the pilot power reaches the optimal value, the disadvantage incurred by further increasing pilot power overcomes the benefit. This observation suggests that when both Bob and Eve have imperfect channel estimation dependent on the training process, it is not always good to have more training power to get more accurate channel estimation. In addition, we

note that the pilot power achieving the peak of throughput increases as α_b decreases, since the importance of enhancing the legitimate users' knowledge increases as Bob's channel condition becomes worse. When the condition of Bob's channel does not have a clear advantage against Eve's channel, the benefit of enhancing the legitimate users' knowledge about the channels always overcomes the disadvantage of increasing the accuracy of channel estimation at the eavesdropper. Thus, we note in the figure that the throughput increases with the pilot power all the time, when $\alpha_b = 5$ dB.

On the other hand, from Figure 2.2 we find that the achievable throughput is always a non-decreasing function of the normalized pilot power for Scenario 2. This is because we assume that the channel estimation errors exist at only Bob but not Eve for Scenario 2. The increase of training power improves only the legitimate users' knowledge about the channels, but has no influence on the eavesdropper's knowledge about her own channel. Thus, it is always good to have more training power to increase the throughput in this scenario.

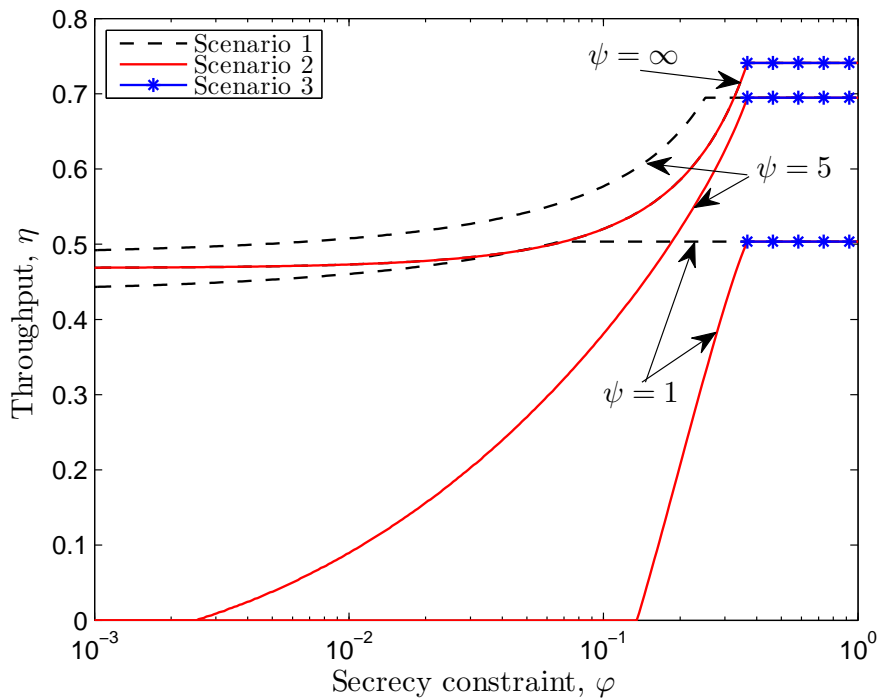


Figure 2.3: Achievable throughput versus secrecy constraint for different values of normalized pilot power, $\psi = 1, 5, \infty$. The other system parameters are $\alpha_b = 10$ dB, $\alpha_e = 0$ dB, $\delta = 0.1$, $R_b = 2$, $R_s = 1$.

We then compare the achievable throughput in Scenarios 1, 2 and 3 subject to different secrecy constraints. Figure 2.3 plots η versus ϕ . There are three groups of curves representing the networks with three different values of the normalized pilot power ψ . As shown in the figure, Scenario 1 can always achieve a positive throughput for any given secrecy constraint.

This is because Alice and Eve have the same amount of knowledge about the eavesdropper's channel in Scenario 1, and Alice in fact knows the upper bound of the actual instantaneous SNR at Eve ($\hat{\gamma}_e \geq \gamma_e$). On the other hand, Scenarios 2 and 3 can obtain a positive throughput only when the secrecy constraints are in the feasible ranges as formulated in (2.36) and (2.47), respectively. In addition, we find that the throughput of each network in Scenario 3 is a step function of the secrecy constraint (the throughput is equal to either zero or a positive constant value). This is due to the fact that the controllable parameter is not related to the secrecy performance for Scenario 3. In addition, we note that the three scenarios can achieve the same throughput, when the secrecy constraint is sufficiently loose satisfying (2.44) or (2.47). Besides, we find that the throughput difference between Scenarios 1 and 2 decreases as the normalized pilot power increases for a given secrecy constraint. Scenarios 1 and 2 can achieve the same throughput when the channel is perfectly estimated, i.e., $\psi = \infty$.

2.5.2 Joint Rate and On-Off Transmission Design

In this subsection, we show the numerical results for the joint rate and on-off transmission design for Scenario 3 with $\alpha_b = 10$ dB and $\alpha_e = 0$ dB.

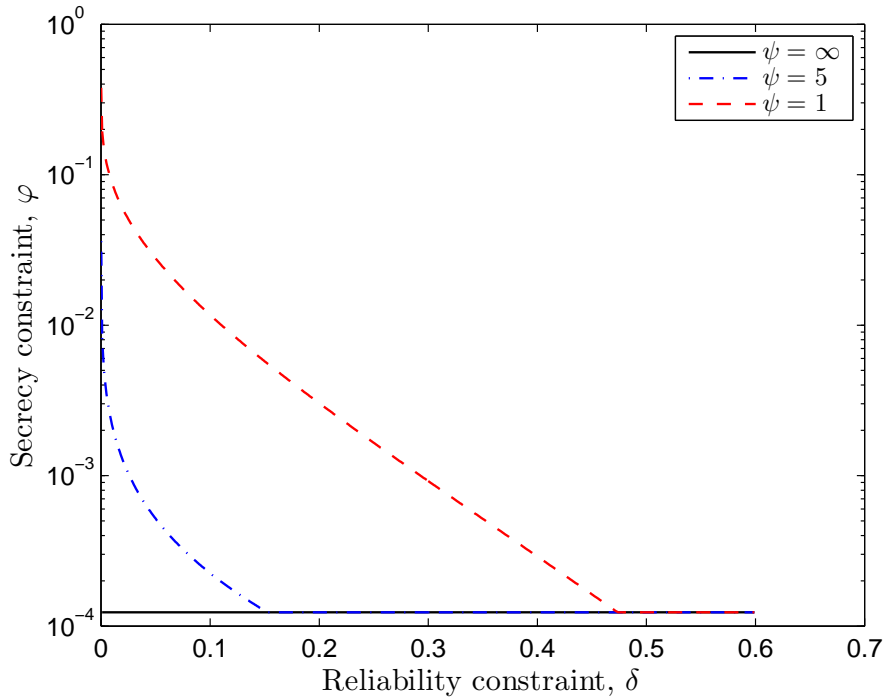


Figure 2.4: Non-adaptive rate scheme: feasible secrecy constraint versus feasible reliability constraint for different values of normalized pilot power, $\psi = 1, 5, \infty$. The other system parameters are $\mu_b = 9$, $\alpha_b = 10$ dB, $\alpha_e = 0$ dB.

We first present the trade-off between the feasible reliability constraint and the feasible secrecy constraint for the non-adaptive rate scheme. Figure 2.4 plots φ versus δ with a given on-off threshold of $\mu_b = 9$. For each network, the feasible constraints lie in the region above the corresponding curve. As depicted in the figure, the feasible φ decreases as δ increases, and there exists a lower bound on the feasible φ . According to the analytical result, the lower bound on the feasible φ is related to the on-off SNR threshold as given in (2.55).

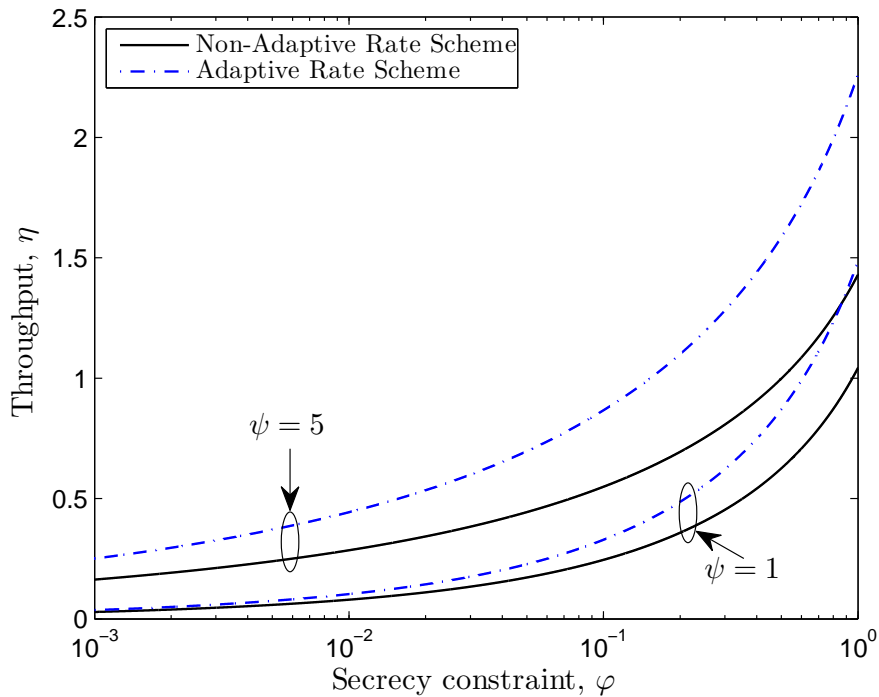


Figure 2.5: Achievable throughput versus secrecy constraint for different values of normalized pilot power, $\psi = 1, 5$. The other system parameters are $\delta = 0.1$, $\alpha_b = 10$ dB, $\alpha_e = 0$ dB.

We then compare the achievable throughput by the non-adaptive and adaptive rate schemes. Figure 2.5 plots η versus ψ with the reliability constraint fixed to $\delta = 0.1$. As shown in the figure, the achievable throughput increases as the normalized pilot power increases. We note that adaptively changing the encoding rates significantly improves the achievable throughput compared with the non-adaptive rate scheme. In addition, the joint rate and on-off transmission design significantly improves the achievable throughput, compared with the on-off transmission design with fixed rates in Section 2.3, For example, the on-off transmission design with fixed $R_b = 2$ and $R_s = 1$ cannot achieve a positive throughput value subject to a large range of secrecy constraints, as shown in Figure 2.3, while the joint rate and on-off transmission design can always achieve a positive throughput value subject to any secrecy constraint.

Finally, we look into the impact of pilot power on the achievable secrecy level of networks.

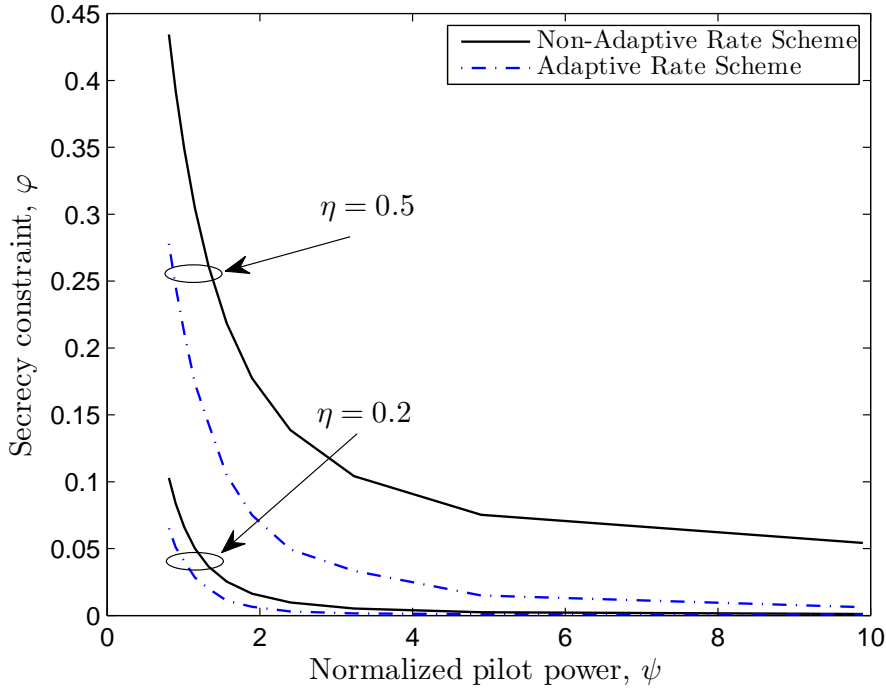


Figure 2.6: Achievable secrecy constraint versus normalized pilot power for different target throughput values, $\eta = 0.2, 0.5$. The other system parameters are $\delta = 0.1$, $\alpha_b = 10$ dB, $\alpha_e = 0$ dB.

Figure 2.6 plots φ versus ψ with different target throughput values. By observing the slopes of curves, we find that the improvement of increasing the pilot power on the achievable secrecy level is significant when the normalized pilot power is small. However, further increasing the pilot power can obtain very little benefit when the pilot power has already become large.

2.6 Summary

In this chapter, we presented a comprehensive study of secure transmission design in quasi-static slow fading channels with channel estimation errors. For systems with fixed encoding rates, throughput-maximizing on-off transmission schemes were proposed for scenarios with different assumptions on the channel knowledge. For systems with encoding rates controllable, we derived both non-adaptive and adaptive rate transmission schemes which jointly optimize the rate parameters and the on-off thresholds. The analytical and numerical results illustrated how the optimal design and the achievable throughput vary with the change in the channel knowledge assumptions. In addition, we found that increasing the pilot power for more accurate channel estimation sometimes can harm the system performance. When both the legitimate receiver and the eavesdropper estimate their channels via the pilot transmission,

increasing pilot power decreases the channel estimation errors at both the legitimate receiver and the eavesdropper. As the pilot power increases, the overall throughput increases at the beginning but can decrease after achieving the peak value.

Achieving Secrecy without Knowing the Number of Eavesdropper Antennas

3.1 Introduction

Chapter 2 studied the secure transmission design for single-antenna systems with the practical assumption of imperfect CSI. In recent years, the fast development of MIMO techniques has triggered a considerable amount of attention on physical layer security in multi-antenna systems, where the transmitter, the receiver and/or the eavesdropper are equipped with multiple antennas. For example, the secrecy capacity of the multi-antenna system was analyzed in [49, 50, 51] and signal processing techniques with multiple antennas for improving the secrecy performance were proposed in [27, 28, 37, 52, 53]. Apart from the assumption of perfect CSI, current research on physical layer security in multi-antenna systems is often based on another idealized assumption, i.e., knowing the number of eavesdropper antennas or setting an upper bound on the number of eavesdropper antennas. Knowing the number of eavesdropper antennas is impractical in most of actual systems, since an external eavesdropper naturally does not inform the legitimate side about the number of antennas to expose its ability. Estimating an upper bound on the number of antennas according the device size is also almost impossible, since the current development of large-scale antenna array technologies allows a fast growing number of antennas to place within a limited space.

In this chapter, we provide an innovative solution to the important problem of how to characterize the performance of physical layer security without knowing the number of eavesdropper antennas problem. To this end, we introduce the concept of spatial constraint into physical layer security. We focus on the effects of spatial constraints at the receiver side. Specifically, we consider the scenario where the transmitter has a large number of antennas without spatial constraint while both the intended receiver and the eavesdropper have spatial constraints to place the receive antennas. This is a valid assumption given less geometrical size restriction

for the BS to place a large number of transmit antennas, while the size of receiving device in the downlink is often relatively small [70]. Importantly, the number of receive antennas at the eavesdropper may not be known. We consider a simple and practical CSI assumption that the instantaneous CSI is known at the receiver end (the intended receiver and the eavesdropper) but not at the transmitter. Under these assumptions and considerations, we derive the secrecy capacity of the spatially-constrained multi-antenna system, and study the potential benefits brought by two widely-adopted friendly-jamming techniques. The two friendly-jamming techniques studied are the basic jamming technique and the AN jamming technique: the former degrades both the intended receiver and the eavesdropper's channels, while the latter degrades only the eavesdropper's channel but does not affect the intended receiver's channel. We find that a non-zero secrecy capacity is achievable for the spatially-constrained system with the help of friendly-jamming signals, even if the number of eavesdropper antennas is unknown and considered to be infinity as a worst case.

The remainder of this chapter is organized as follows. Section 3.2 describes system models for studying physical layer security with spatial constraints at the receiver side. In Section 3.3, we first give the secrecy capacity of the proposed systems with the knowledge of the number of eavesdropper antennas. The important case of not knowing the number of eavesdropper antennas is studied in Section 3.4, where the eavesdropper's receiver is assumed to be noise free and allowed to have infinitely many antennas for the worst-case consideration. Finally, Section 3.5 summarizes the chapter.

3.2 System Model

In this chapter, we study physical layer security in multi-antenna systems with spatial constraints at the receiver side. We assume that all communication nodes are equipped with multiple antennas and there exist spatial constraints at both the intended receiver and the eavesdropper. That is, the intended receiver and the eavesdropper have limited sizes of spatial regions for placing the receive antennas. To focus on the impact of spatial constraints at the receiver side, we adopt the following two assumptions as briefly mentioned in Section 3.1. Firstly, we assume that there is no spatial constraint at the transmitter side for placing transmit antennas. Secondly, we assume that the transmitter has a large number of transmit antennas, and hence the capacity of the channel from the transmitter to the receiver is mainly restricted by the receiver side. Note that the number of antennas at the BS is often predicted to be in the hundreds for the next generation wireless systems [71, 72]. These two assumptions were often adopted in the literature investigating the impact of spatial constraints at the receiver side on multi-antenna systems without secrecy considerations, e.g., [70, 73, 74, 75] studying the channel capacity and [76, 77, 78, 79] studying the spatial degrees of freedom. We specifically investigate two different secure communication systems, which are the wiretap-channel sys-

tem and the jammer-assisted system. For the jammer-assisted system, we further consider two different cases depending on the adopted jamming technique, namely basic jammer-assisted system and AN jammer-assisted system. The details of the system models are given in the following subsections.

3.2.1 Wiretap-Channel System

The wiretap-channel system consists of a transmitter, an intended receiver and an eavesdropper, with N_t, N_b and N_e antennas, respectively. The transmitter, Alice, sends confidential messages to the intended receiver, Bob, in the presence of the eavesdropper, Eve. The receive antennas at Bob and Eve are both spatially constrained. Alice is assumed to be a BS with a large number of antennas ($N_t \rightarrow \infty$) without a spatial constraint. For the two-dimensional (2D) analysis, Bob and Eve are assumed to be spatially constrained by circular apertures with radii r_b and r_e , respectively. For the three-dimensional (3D) analysis, Bob and Eve are assumed to be spatially constrained by spherical apertures with radii r_b and r_e , respectively. The 2D and 3D models for the wiretap-channel system are depicted in Figures 3.1 and 3.2, respectively.

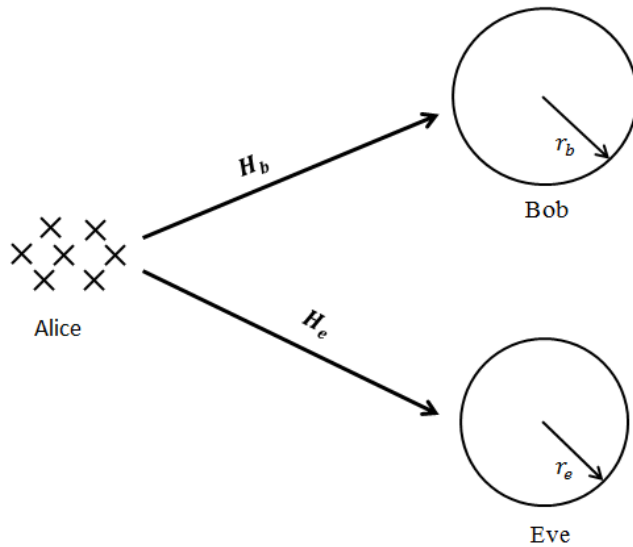


Figure 3.1: 2D model for the wiretap-channel system.

The received signal vector at Bob or Eve is given by

$$\mathbf{y}_i = \sqrt{\alpha_i} \mathbf{H}_i \mathbf{x} + \mathbf{n}_i, \quad i = b \text{ or } e, \quad (3.1)$$

where the subscripts b and e denote the parameters for Bob and Eve, respectively, \mathbf{x} denotes the transmitted signal vector from Alice with an average power of P_t , i.e., $\mathbb{E} \{ \mathbf{x}^H \mathbf{x} \} = P_t$. In addition, $\mathbf{n}_i \sim \mathcal{CN}(\mathbf{0}, \sigma_i^2 \mathbf{I})$ denotes the AWGN vector at Bob or Eve, $\mathbf{H}_i = [\mathbf{h}_{i1} \mathbf{h}_{i2} \cdots \mathbf{h}_{iN_t}]$ denotes

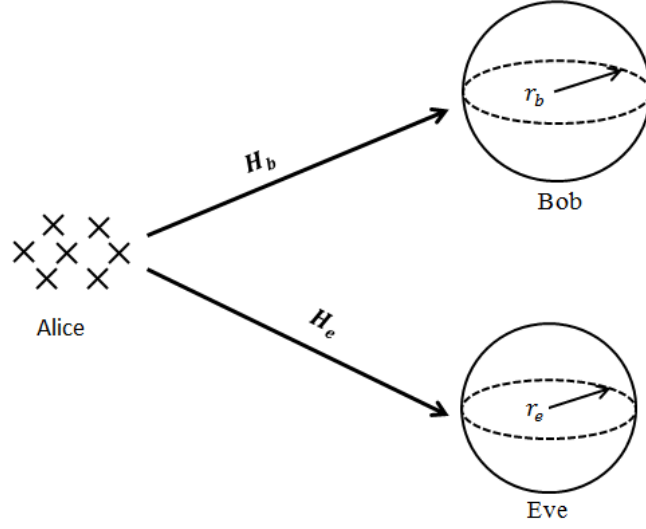


Figure 3.2: 3D model for the wiretap-channel system.

the $N_i \times N_i$ normalized channel matrix from Alice to Bob or Eve with \mathbf{h}_{ik} ($k \in \{1, 2, \dots, N_i\}$) representing the $N_i \times 1$ complex zero-mean Gaussian vector of the channel gains corresponding to the k th transmit antenna at Alice. Moreover, α_i denotes the average channel gain from Alice to Bob or Eve, which is often determined by the distance between the transmitter and the receiver. Besides, we assume that Bob and Eve perfectly know their CSI, while Alice does not know either Bob or Eve's instantaneous CSI.

The correlation matrix at the receiver is defined as

$$\mathbf{R}_i = \mathbb{E} \{ \mathbf{h}_i \mathbf{h}_i^H \}, \quad (3.2)$$

where the expectation is over all transmit antennas and channel realizations. We can also write

$$\mathbf{R}_i = \begin{bmatrix} \rho_{i,11} & \rho_{i,12} & \dots & \rho_{i,1N_i} \\ \rho_{i,21} & \rho_{i,22} & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{i,N_i1} & \dots & \dots & \rho_{i,N_iN_i} \end{bmatrix}, \quad (3.3)$$

with elements $\rho_{i,kk'}$ corresponding to the spatial correlation between two sensors k and k' at the receiver. The spatial correlation between sensors is mainly determined by the distance between the sensors. The spatial correlation increases as the distance between sensors decreases. Within a fixed space, the distance between the antennas decreases as the number of antennas increases, and hence, the spatial correlation increases as the number of antennas increases.

3.2.2 Jammer-Assisted System

The jammer-assisted system consists of a transmitter, a helper, an intended receiver and an eavesdropper, with N_t, N_j, N_b and N_e antennas, respectively. With the aid of the helper, Helen, the transmitter, Alice, sends confidential messages to the intended receiver, Bob, in the presence of the eavesdropper, Eve. Helen helps Alice by broadcasting friendly jamming signals. The receive antennas at Bob and Eve are both spatially constrained. Alice and Helen are assumed to be BSs with a large number of transmit antennas ($N_t, N_j \rightarrow \infty$) without the spatial constraint. The detailed assumptions of the spatial constraints on Bob and Eve are the same as those given in Section 3.2.1. The 2D and 3D models of the jammer-assisted system are depicted in Figures 3.3 and 3.4, respectively.

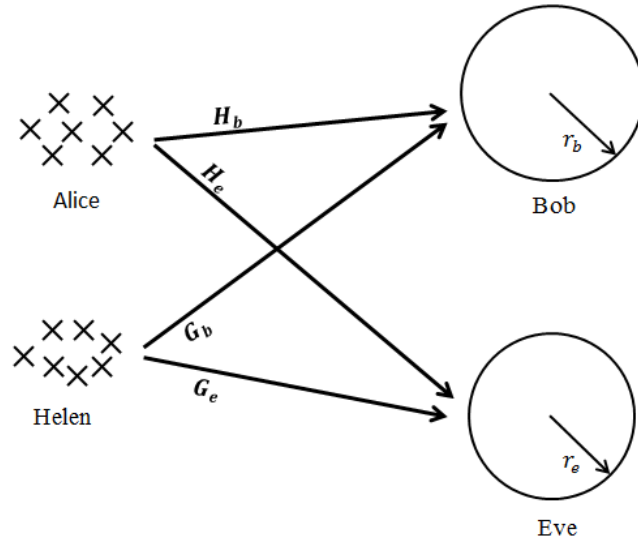


Figure 3.3: 2D model for the jammer-assisted system.

We assume that Bob and Eve perfectly know their CSI, and Alice does not know either Bob or Eve's instantaneous CSI. We further assume that Helen does not know Eve's instantaneous CSI, since the passive eavesdropper does not feed back the CSI to the helper. Moreover, for Helen's knowledge about Bob's channel, we consider two different cases in order to study two widely-adopted friendly-jamming techniques, as will be detailed next.

3.2.2.1 Case 1: Basic Jammer-Assisted System

In the first case, we assume that Helen does not know Bob's instantaneous CSI. This happens when there is no reliable uplink channel from Bob to Helen for CSI feedback. In this case, Helen broadcasts basic jamming signals that degrade both Bob and Eve's channels.

The received signal vector at Bob or Eve is given by

$$\mathbf{y}_i = \sqrt{\alpha_i} \mathbf{H}_i \mathbf{x} + \sqrt{\beta_i} \mathbf{G}_i \mathbf{w}_1 + \mathbf{n}_i, \quad i = b \text{ or } e, \quad (3.4)$$

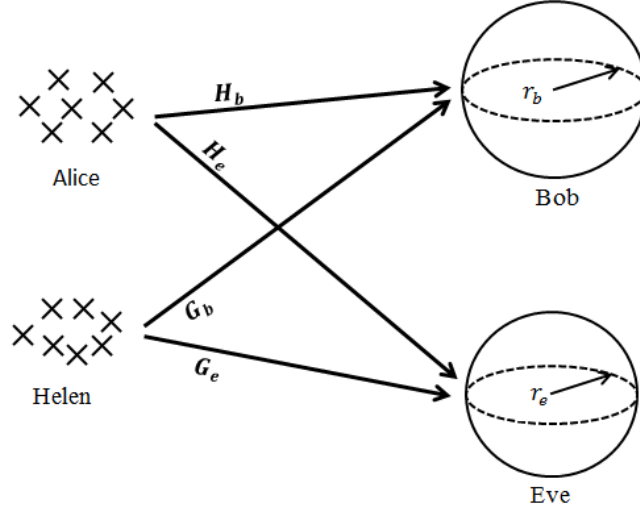


Figure 3.4: 3D model for the jammer-assisted system.

where \mathbf{x} , α_i , \mathbf{H}_i , \mathbf{n}_i and the subscripts b, e follow (3.1). In addition, \mathbf{w}_1 denotes the basic jamming signal vector transmitted from Helen with an average power of P_j , i.e., $\mathbb{E}\{\mathbf{w}_1^H \mathbf{w}_1\} = P_j$, and $\mathbf{G}_i = [\mathbf{g}_{i1} \mathbf{g}_{i2} \cdots \mathbf{g}_{iN_j}]$ denotes the normalized channel matrix from Helen to Bob or Eve with \mathbf{g}_{ik} ($k \in \{1, 2, \dots, N_j\}$) representing the $N_i \times 1$ complex zero-mean Gaussian vector of the channel gains corresponding to the k th transmit antenna at Helen. Moreover, β_i denotes the average channel gain from Helen to Bob or Eve.

3.2.2.2 Case 2: AN Jammer-Assisted System

In the second case, we assume that Helen perfectly knows the instantaneous CSI from herself to Bob. This happens when there exists a reliable uplink channel from Bob to Helen for CSI feedback. In such a case, Helen broadcasts AN jamming signals that degrade Eve's channel but do not affect Bob's channel. The AN jamming technique was proposed in [27], which is often applied in secure communication networks where the jammer has the CSI to the intended receiver. Specifically, the AN jamming signal vector from Helen, denoted by \mathbf{w}_2 , is chosen to lie in the null space of the channel to the intended receiver, \mathbf{G}_b . That is $\mathbf{G}_b \mathbf{w}_2 = \mathbf{0}$. In particular, \mathbf{w}_2 can be constructed by

$$\mathbf{w}_2 = \mathbf{Z}\mathbf{v}, \quad (3.5)$$

where \mathbf{v} is an independent and identically distributed (i.i.d.) complex Gaussian random variable vector, the $N_j \times (N_j - N_b)$ matrix \mathbf{Z} denotes the orthonormal basis of the null space of \mathbf{G}_b with $\mathbf{Z}^H \mathbf{Z} = \mathbf{I}$.

With the AN jamming signals, the received signal vectors at Bob and Eve are given by

$$\mathbf{y}_b = \sqrt{\alpha_b} \mathbf{H}_b \mathbf{x} + \sqrt{\beta_b} \mathbf{G}_b \mathbf{w}_2 + \mathbf{n}_b = \sqrt{\alpha_b} \mathbf{H}_b \mathbf{x} + \mathbf{n}_b \quad (3.6)$$

and

$$\mathbf{y}_e = \sqrt{\alpha_e} \mathbf{H}_e \mathbf{x} + \sqrt{\beta_e} \mathbf{G}_e \mathbf{w}_2 + \mathbf{n}_e = \sqrt{\alpha_e} \mathbf{H}_e \mathbf{x} + \sqrt{\beta_e} \mathbf{G}_e \mathbf{Z} \mathbf{v} + \mathbf{n}_e, \quad (3.7)$$

respectively, where, once again, $\mathbf{x}, \alpha_b, \alpha_e, \mathbf{H}_b, \mathbf{H}_e, \mathbf{n}_b, \mathbf{n}_e$ follow (3.1) and $\beta_b, \beta_e, \mathbf{G}_b, \mathbf{G}_e$ follow (3.4). Besides, the average transmit power at Helen is still given by P_j , i.e., $\mathbb{E} \{ \mathbf{w}_2^H \mathbf{w}_2 \} = P_j$.

Remark 3.1. We highlight that the analysis for the AN jammer-assisted system is mainly motivated by its importance from the theoretical point of view. The basic jamming and the AN jamming are the two most widely-studied physical-layer techniques to improve the secrecy performance of multi-antenna systems. In this chapter, we study the wireless physical layer security with spatial constraints at the receiver side. It is of significant importance to investigate the benefits brought by both of the jamming techniques in the spatially-constrained systems. The AN jamming technique is often studied in the scenario where both Alice and Helen have the legitimate CSI in the literature. The legitimate CSI available at Alice enables not only the injection of AN jamming signals but also the transmit beamforming, and the secrecy capacity will go to infinity under the assumption of infinitely large number of transmit antennas. This will be shown later in Section 3.3. In order to investigate the capacity improvement solely brought by AN jamming, we assume that Alice does not know the instantaneous CSI to Bob, but Helen knows the instantaneous CSI to Bob. Besides, the practical value of the AN jammer-assisted system studied in this chapter can be seen from the following scenario as an example: We can consider that Alice is a BS owned by company A to serve a mobile user, Bob. Helen is another BS owned by company B. Due to particular reasons, e.g., location or surrounding environment, the CSI feedback link from Bob to Alice is bad, while the CSI feedback link from Bob to Helen is good. Then, Alice asks Helen to help the secrecy transmission by broadcasting AN jamming signals. For the secrecy concern, company A does not intend to share the confidential information with company B, and hence Alice does not share the messages to transmit with Helen.

3.3 Introducing Spatial Constraints into Secrecy Capacity Calculation

In this section, we derive the secrecy capacity of the systems with spatial constraints at the receiver side as described in Section 3.2. The secrecy capacity characterizes the maximum rate at which messages can be reliably transmitted to Bob while Eve obtains zero information. It is mathematically defined by [15]

$$C_s = [C_b - C_e]^+, \quad (3.8)$$

where C_b and C_e denote Bob and Eve's channel capacities, respectively.

For the multi-antenna systems with spatial constraint at the receiver, the channel capacity is limited by the rank and the eigenvalues of the spatial correlation matrix at the receiver. As the number of antennas increases in a fixed space, the correlation between antennas increases. The increase in spatial correlation will limit the number of significant eigenvalues of the spatial correlation matrix. As more antennas are placed in the fixed space, they will be highly correlated with other antennas. As a result, the growth of channel capacity with respect to the number of receive antennas reduces from linear to logarithmic. The number of receive antennas at which the capacity scaling is reduced to logarithmic is approximated by the saturation number of receive antennas. The saturation number of receive antennas is given by [70, Chapters 3.3]

$$N_{0i} = \begin{cases} 2 \lceil \pi e r_i / \lambda \rceil + 1, & \text{for 2D analysis} \\ (\lceil \pi e r_i / \lambda \rceil + 1)^2, & \text{for 3D analysis,} \end{cases} \quad (3.9)$$

where λ denotes the wavelength, e denotes Euler's number, and subscript i denotes the parameters for Bob or Eve. As pointed out in [70], the growth of channel capacity (C_b or C_e) with respect to the number of *optimally-placed* receive antennas (N_b or N_e) reduces from linear to logarithmic when the number of receive antennas increases beyond the saturation number (N_{0b} or N_{0e}). Note that similar "saturation" effects on the growth of channel capacity with respect to the number of antennas at the spatially-constrained receiver have also been pointed out in, e.g., [80, 81, 82, 83].

It is worth mentioning that the capacity results in this chapter are approximations based on (3.9) and the assumption of infinitely large number of transmit antennas. The accuracy of the approximations are verified in Appendices. In the rest of the chapter, we simply refer to the approximated capacity result as the capacity.

3.3.1 Secrecy Capacity of Wiretap-Channel System

Proposition 3.1. The secrecy capacity of the wiretap-channel system with spatial constraints at the receiver side is given by $C_s = [C_b - C_e]^+$ where

$$C_b = \begin{cases} N_b \log_2 \left(1 + \frac{\alpha_b P_t}{\sigma_b^2} \right), & \text{if } N_b \leq N_{0b} \\ N_{0b} \log_2 \left(1 + \frac{N_b}{N_{0b}} \frac{\alpha_b P_t}{\sigma_b^2} \right), & \text{if } N_b > N_{0b}, \end{cases} \quad (3.10)$$

$$C_e = \begin{cases} N_e \log_2 \left(1 + \frac{\alpha_e P_t}{\sigma_e^2} \right), & \text{if } N_e \leq N_{0e} \\ N_{0e} \log_2 \left(1 + \frac{N_e}{N_{0e}} \frac{\alpha_e P_t}{\sigma_e^2} \right), & \text{if } N_e > N_{0e}. \end{cases} \quad (3.11)$$

Proof: The capacities of the channels to the spatially-constrained Bob and Eve follow easily from [70, Chapters 2 and 3]. The details are given in Appendix B.1. ■

Proposition 3.1 gives the secrecy capacity of the wiretap-channel system taking spatial constraints at the receiver side into account. From Proposition 3.1, we note that the growth of

secrecy capacity with N_b reduces from linear to logarithmic once N_b reaches N_{0b} . Also, the decrease of secrecy capacity with N_e reduces from linear to logarithmic once N_e reaches N_{0e} . Differently, the secrecy capacity without spatial constraint always increases linearly with N_b and decreases linearly with N_e . This verifies that the secrecy performances of the networks with and without spatial considerations are different.

3.3.2 Secrecy Capacity of Basic Jammer-Assisted System

Theorem 3.1. The secrecy capacity of the basic jammer-assisted system with spatial constraints at the receiver side is given by $C_s = [C_b - C_e]^+$ where

$$C_b = \begin{cases} N_b \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j + \sigma_b^2} \right), & \text{if } N_b \leq N_{0b} \\ N_{0b} \log_2 \left(1 + \frac{\frac{N_b}{N_{0b}} \alpha_b P_t}{\beta_b P_j + \sigma_b^2} \right), & \text{if } N_b > N_{0b}, \end{cases} \quad (3.12)$$

$$C_e = \begin{cases} N_e \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j + \sigma_e^2} \right), & \text{if } N_e \leq N_{0e} \\ N_{0e} \log_2 \left(1 + \frac{\frac{N_e}{N_{0e}} \alpha_e P_t}{\beta_e P_j + \sigma_e^2} \right), & \text{if } N_e > N_{0e}. \end{cases} \quad (3.13)$$

Proof: See Appendix B.2. ■

Theorem 3.1 gives the secrecy capacity of the basic jammer-assisted system taking spatial constraints at the receiver side into account. Similar to the result for the wiretap channel, we note that the secrecy capacity grows in linear with N_b when $N_b \leq N_{0b}$. Also, the secrecy capacity decreases in linear with N_e when $N_e \leq N_{0e}$. However, as N_i increases beyond N_{0i} , the change of secrecy capacity with respect to N_i becomes slower and slower. The secrecy capacity approaches an upper bound as $N_b \rightarrow \infty$, and a possible non-zero lower bound as $N_e \rightarrow \infty$, since

$$\lim_{N_b \rightarrow \infty} C_b = N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j} \right) \quad (3.14)$$

and

$$\lim_{N_e \rightarrow \infty} C_e = N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right). \quad (3.15)$$

3.3.3 Secrecy Capacity of AN Jammer-Assisted System

Theorem 3.2. The secrecy capacity of the AN jammer-assisted system with spatial constraints at the receiver side is given by $C_s = [C_b - C_e]^+$ where

$$C_b = \begin{cases} N_b \log_2 \left(1 + \frac{\alpha_b P_t}{\sigma_b^2} \right), & \text{if } N_b \leq N_{0b} \\ N_{0b} \log_2 \left(1 + \frac{\frac{N_b}{N_{0b}} \alpha_b P_t}{\sigma_b^2} \right), & \text{if } N_b > N_{0b}, \end{cases} \quad (3.16)$$

$$C_e = \begin{cases} N_e \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j + \sigma_e^2} \right), & \text{if } N_e \leq N_{0e} \\ N_{0e} \log_2 \left(1 + \frac{\frac{N_e}{N_{0e}} \alpha_e P_t}{\beta_e P_j + \sigma_e^2} \right), & \text{if } N_e > N_{0e}. \end{cases} \quad (3.17)$$

Proof: The capacity of Bob's channel is the same as that for the wiretap-channel system, since the AN jamming signals do not affect Bob's channel. We then derive the capacity of Eve's channel subject to the AN jamming signals. The details are given in Appendix B.3. ■

Theorem 3.2 gives the secrecy capacity of the AN jammer-assisted system taking spatial constraints at the receiver side into account. We note that the growth of secrecy capacity with N_b reduces from linear to logarithmic once N_b reaches N_{0b} . The decrease of secrecy capacity with N_e is in linear when $N_e \leq N_{0e}$, and becomes slower and slower when $N_e > N_{0e}$. The secrecy capacity approaches a (possible) non-zero lower bound as $N_e \rightarrow \infty$.

3.3.4 Secrecy Capacity with Legitimate CSI Available at Alice

We consider a simple and practical CSI assumption that the instantaneous CSI of Bob is not available at Alice. In fact, it is also possible in practice that Bob's CSI is available at Alice. In this subsection, we provide the analysis on the secrecy capacity of the scenario where both Alice and Helen have Bob's CSI. Note that for the scenario without the friendly jammer, Alice can use a portion of the transmit antennas for sending information signals and the rest for broadcasting AN jamming signals. Under the assumption of $N_t \rightarrow \infty$, the scenario without the jammer Helen can be regarded as the scenario having both Helen and Alice at the same location.

When Bob's CSI is available at Alice, Alice can design the transmit signals accordingly to enhance Bob's channel capacity. Alice can wisely allocate the transmit power by performing transmit beamforming based on \mathbf{H}_b , such that more power is allocated to the antennas having a good channel condition and less power is allocated to the antennas having a bad channel condition. Then, the received signal power at Bob would increase, and Bob's channel capacity would increase. At the same time, Helen can still transmit the AN jamming signals that degrade Eve's channel but do not affect Bob's channel. An infinitely large rate at Bob can be achieved by adopting a simple single-stream beamforming at Alice, under the assumption that the transmitter has an infinitely large number of antennas without the spatial constraint, while Eve does not benefit from the transmit beamforming. Hence, the secrecy capacity is equal to infinity in such a scenario with Bob's CSI available at Alice. It is worth mentioning that the secrecy capacity would be finite in a practical system with spatial constraints at both the transmitter side and the receiver side, due to the finite degrees of freedom in the spatially-constraint channel. The derivation of secrecy capacity in systems with spatial constraints at both the transmitter side and the receiver side is non-trivial and beyond the scope of the work in this chapter.

3.3.5 Numerical Results

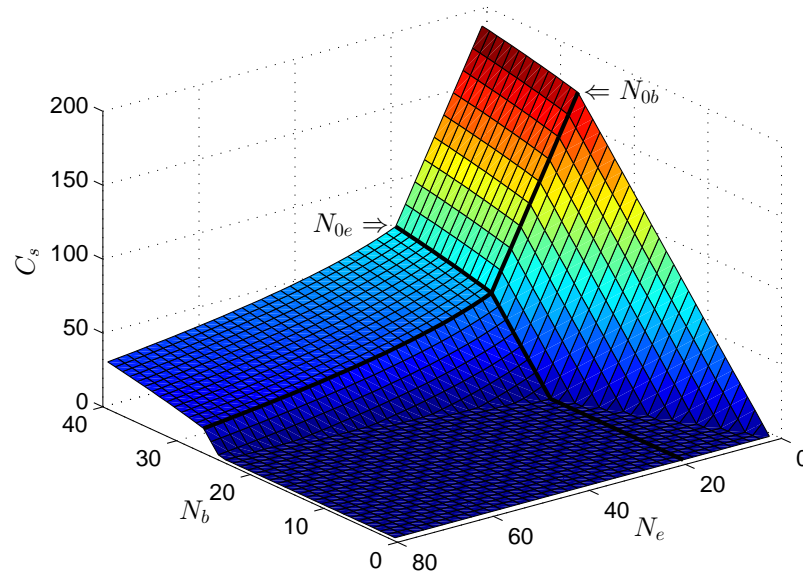


Figure 3.5: Wiretap-channel system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

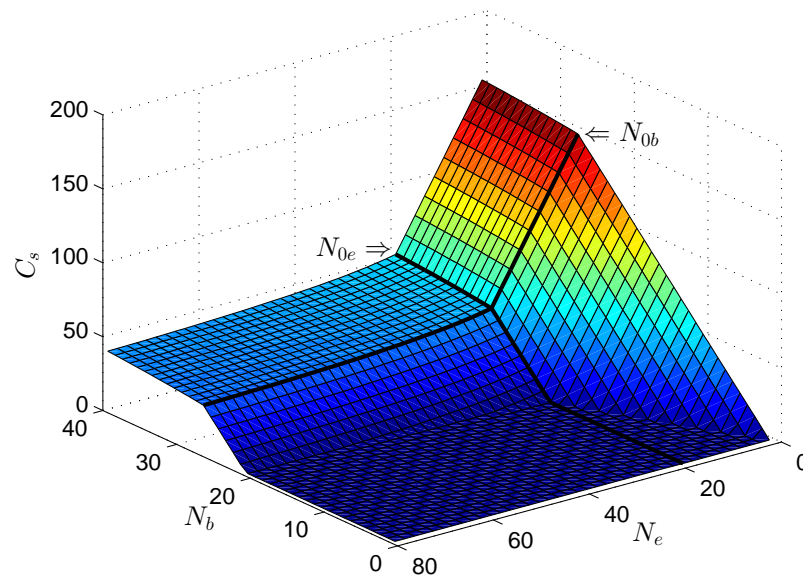


Figure 3.6: Basic jammer-assisted system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

In this subsection, we demonstrate the secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas for different systems. Specifically, the network parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $\sigma_e^2 = 1$, $r_b = 1.5\lambda$ and $r_e = 1\lambda$. We adopt the 2D analysis to characterize the spatial constraints at the receiver side. That is, Bob and Eve are assumed to be spatially constrained by circular apertures. According to (3.9), the saturation numbers of receive antennas for Bob and Eve are $N_{0b} = 2 \lceil \pi r_b / \lambda \rceil + 1 = 27$ and $N_{0e} = 2 \lceil \pi r_e / \lambda \rceil + 1 = 19$, respectively.

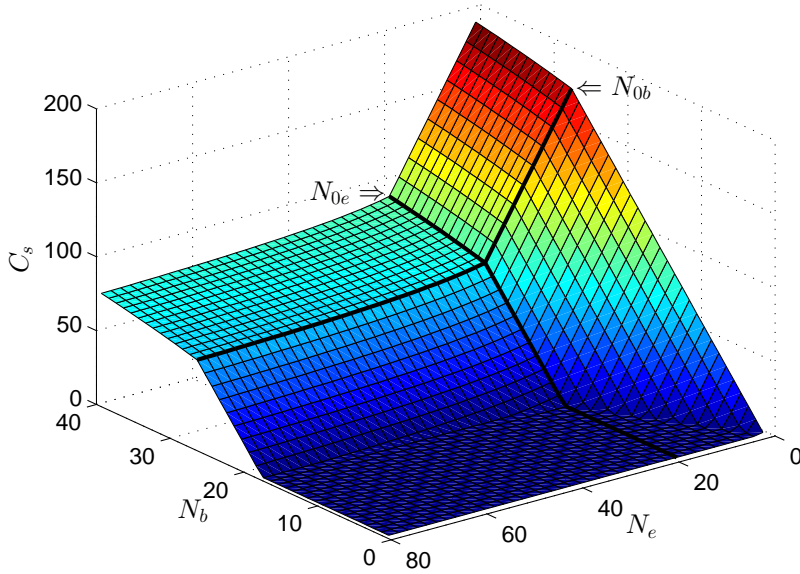


Figure 3.7: AN jammer-assisted system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

Figures 3.5, 3.6 and 3.7 plot C_s versus N_b and N_e for the wiretap-channel system, the basic jammer-assisted system and the AN jammer-assisted system, respectively. As shown in the figures, C_s increases with N_b and decreases with N_e . The increase of C_s with N_b slows down once $N_b > N_{0b}$ due to the effect of spatial constraint at Bob. Similarly, the decrease of C_s with N_e slows down once $N_e > N_{0e}$ due to the effect of spatial constraint at Eve. Besides, we note that the achieved secrecy capacities for different systems are different.

To make a clear comparison between the achieved secrecy capacities for different systems, we present Figure 3.8 plotting C_s versus N_e with a given value of $N_b = 35$. Note that the results for the basic jammer-assisted system are obtained with the optimal jamming power (≤ 0 dB) instead of having the fixed $P_j = 0$ dB. As shown in the figure, the secrecy capacity of the wiretap-channel system decreases fast as the number of Eve's antennas increases. We find that the secrecy capacity of the wiretap-channel system goes to zero as the number of

Eve's antennas continues to increase. Comparing the wiretap-channel system and the basic jammer-assisted system, we note that introducing the basic jamming signals effectively slows down the decrease of C_s when $N_e > N_{0e}$. Thus, the basic jammer-assisted system achieves a higher secrecy capacity compared with the wiretap-channel system when the number of Eve's antennas is large. In addition, as analyzed in Section 3.3.2, the secrecy capacity of the basic jammer-assisted system can approach a non-zero lower bound as $N_e \rightarrow \infty$. Besides, we observe from the figure that the secrecy capacity achieved by the basic jammer-assisted system is equal to that achieved by the wiretap-channel system when N_e is small, since it is wise to have $P_j = 0$ when N_e is small. Comparing the wiretap-channel system and the AN jammer-assisted system, we find that the AN jammer-assisted system always obtains a higher secrecy capacity than that of the wiretap-channel system. This is because the AN jamming signals degrade Eve's channel only, but do not affect Bob's channel. However, we should note that broadcasting the AN jamming signals requires the helper to know the instantaneous CSI of the intended receiver, which is not always possible in practice.

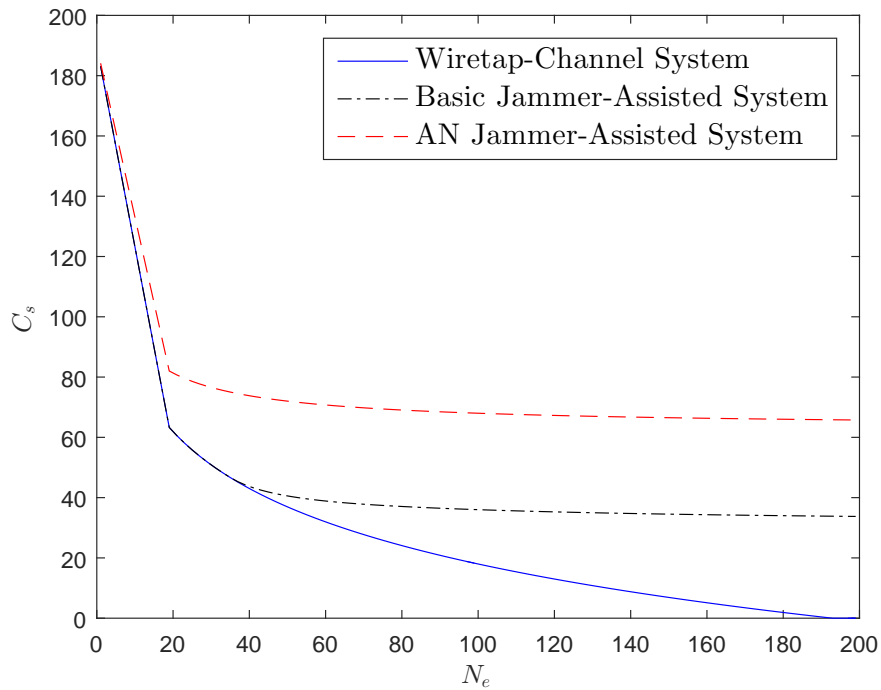


Figure 3.8: Secrecy capacity versus the number of eavesdropper antennas with $N_b = 35$. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

For the numerical results in this section, the transmit power and the jammer power are fixed to be 20 dB and 0 dB, respectively. In fact, increasing P_t always enhances the secrecy capacity for all three systems, as long as the secrecy capacity is non-zero. The effect of P_j on

the secrecy capacity is complicated and will be detailed in Section 3.4.

3.4 Worst-Case Analysis for Jammer-Assisted Systems

The previous section provides the basic analysis on the secure communication systems with spatial constraints at the receiver side. However, to evaluate the system performance by the capacity results given in Proposition 3.1, Theorems 3.1 and 3.2, we require very good knowledge on Eve, including N_e and σ_e^2 . In practice, it is desirable to be able to investigate the secrecy performance of a system without the knowledge of N_e and σ_e^2 . To this end, we consider a “worst-case eavesdropper” (from the legitimate users’ perspective) as in this section.

For such a worst-case eavesdropper, we assume that the number of receive antennas at the eavesdropper approaches infinity and the noise variance at the eavesdropper approaches zero, i.e., $N_e \rightarrow \infty$ and $\sigma_e^2 \rightarrow 0$. Then, the secrecy capacity with the worst-case consideration is given by

$$C_s^w = \lim_{N_e \rightarrow \infty, \sigma_e^2 \rightarrow 0} C_s, \quad (3.18)$$

where C_s is the secrecy capacity of systems with perfect knowledge of N_e and σ_e^2 , i.e., the secrecy capacity derived in the previous section. In addition, we refer to C_s^w as the worst-case secrecy capacity.

The worst-case scenario is motivated by the fact that the eavesdropper’s ability is difficult to be known or controlled by the legitimate side. As such, in the design of secure communications, we assume the worst-case scenario where the eavesdropper can deploy infinite number of antennas with arbitrarily small noise variance. If we assume that the eavesdropper has a given number of antennas, the designed secure communications would be vulnerable to eavesdropping caused by a larger number of antennas at the eavesdropper in practice. Therefore, the weaker assumption of knowing a finite number of antennas at the eavesdropper cannot lead to the true guarantee of security, and thus it is of critical significance to take into consideration the worst-case scenario with infinite number of eavesdropper antennas.

3.4.1 Wiretap-Channel System

Based on Proposition 3.1 and (3.18), the worst-case secrecy capacity of the wiretap-channel system is given by

$$C_s^w = 0. \quad (3.19)$$

We note that a non-zero worst-case secrecy capacity is not achievable under any condition for the wiretap-channel system, because the capacity of Eve’s channel always goes to infinity with $N_e \rightarrow \infty$ or $\sigma_e^2 \rightarrow 0$.

3.4.2 Basic Jammer-Assisted System

3.4.2.1 Worst-Case Secrecy Capacity

Based on Theorem 3.1 and (3.18), the worst-case secrecy capacity of the basic jammer-assisted system is given by

$$C_s^w = \begin{cases} \left[N_b \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j + \sigma_b^2} \right) - N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right) \right]^+, & \text{if } N_b \leq N_{0b} \\ \left[N_{0b} \log_2 \left(1 + \frac{\frac{N_b}{N_{0b}} \alpha_b P_t}{\beta_b P_j + \sigma_b^2} \right) - N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right) \right]^+, & \text{if } N_b > N_{0b}. \end{cases} \quad (3.20)$$

From (3.20), we note that a non-zero worst-case secrecy capacity sometimes is achievable for the basic jammer-assisted system depending on the system parameters, such as transmit power, average channel gains, the spatial constraint at Bob and the number of antennas at Bob. This result shows for the first time that a non-zero secrecy rate can be achieved even if the eavesdropper's receiver itself is noise free and allowed to have infinitely many antennas. Moreover, this is achieved by simply asking a friendly-jamming node to send random jamming signals.

To further study the condition for having a non-zero worst-case secrecy capacity, we consider the scenario where the number of antennas at Bob, N_b , is controllable and the other system parameters¹, i.e., $N_{0b}, N_{0e}, \alpha_b, \beta_b, \alpha_e, \beta_e, P_t$ and P_j , are fixed. From (3.20), we find that a non-zero worst-case secrecy capacity is always achievable by having "enough" receive antennas at Bob when $N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j} \right) > N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right)$. However, the secrecy capacity is always equal to zero when

$$N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j} \right) \leq N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right), \quad (3.21)$$

because $C_b < N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j} \right)$ always holds for any finite value of N_b . In addition, when $N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j} \right) > N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right)$, we can further derive the minimum N_b to ensure a non-zero worst-case secrecy capacity as

$$N_{b,\min} = \begin{cases} \left\lceil \frac{N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right)}{\log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j + \sigma_b^2} \right)} \right\rceil + 1, & \text{if } N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b P_j} \right) \geq N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right) \\ \left\lceil \frac{N_{0b} \alpha_b^2 \left(\left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right)^{N_{0b}} - 1 \right)}{\alpha_b P_t + \beta_b P_j - \hat{\alpha}_b P_j \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right)^{N_{0b}}} \right\rceil + 1, & \text{otherwise.} \end{cases} \quad (3.22)$$

¹Here the other system parameters depend on the spatial constraint, the location of communication node and the transmit power.

3.4.2.2 Optimal Jamming Power

From (3.20), we note that the worst-case secrecy capacity is not a monotonically increasing function of the jamming power. This is because the increase of P_j degrades not only Eve's channel but also Bob's channel, and there arises a tradeoff between maintaining the capacity of Bob's channel and decreasing the capacity of Eve's channel. In the following, we determine the optimal jamming power that maximizes the worst-case secrecy capacity, i.e., $P_j^* = \arg \max_{P_j} C_s^w$.

Proposition 3.2. The optimal jamming power that maximizes the worst-case secrecy capacity of the basic jammer-assisted system is given by

$$P_j^* = \begin{cases} x_1, & \text{if } N_b \leq N_{0b} \text{ and } f_1(x_1) > 0 \text{ with } x_1 \text{ is real and positive} \\ x_2, & \text{if } N_b \leq N_{0b} \text{ and } f_1(x_2) > 0 \text{ with } x_2 \text{ is real and positive} \\ x_3, & \text{if } N_b > N_{0b} \text{ and } f_2(x_3) > 0 \text{ with } x_3 \text{ is real and positive} \\ x_4, & \text{if } N_b > N_{0b} \text{ and } f_2(x_4) > 0 \text{ with } x_4 \text{ is real and positive} \\ \text{not applicable,} & \text{otherwise,} \end{cases} \quad (3.23)$$

where

$$f_1(x) = N_b \log_2 \left(1 + \frac{\alpha_b P_t}{\beta_b x + \sigma_b^2} \right) - N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e x} \right),$$

$$f_2(x) = N_{0b} \log_2 \left(1 + \frac{\frac{N_b}{N_{0b}} \alpha_b P_t}{\frac{N_b}{N_{0b}} \beta_b x + \sigma_b^2} \right) - N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e x} \right),$$

$$x_1 = \frac{2N_{0e} \alpha_e \sigma_b^2 - P_t \alpha_b \alpha_e (N_b - N_{0e})}{2(N_b \alpha_b \beta_e - N_{0e} \alpha_e \beta_b)} + \frac{\sqrt{\alpha_b^2 \alpha_e^2 \beta_b^2 P_t^2 (N_b - N_{0e})^2 + 4N_b N_{0e} \alpha_b \alpha_e \beta_b \sigma_b^2 (P_t \alpha_b \beta_e - P_t \alpha_e \beta_b + \beta_e \sigma_b^2)}}{2\beta_b (N_b \alpha_b \beta_e - N_{0e} \alpha_e \beta_b)},$$

$$x_2 = \frac{2N_{0e} \alpha_e \sigma_b^2 - P_t \alpha_b \alpha_e (N_b - N_{0e})}{2(N_b \alpha_b \beta_e - N_{0e} \alpha_e \beta_b)} - \frac{\sqrt{\alpha_b^2 \alpha_e^2 \beta_b^2 P_t^2 (N_b - N_{0e})^2 + 4N_b N_{0e} \alpha_b \alpha_e \beta_b \sigma_b^2 (P_t \alpha_b \beta_e - P_t \alpha_e \beta_b + \beta_e \sigma_b^2)}}{2\beta_b (N_b \alpha_b \beta_e - N_{0e} \alpha_e \beta_b)},$$

$$\begin{aligned}
x_3 &= \frac{2N_{0e}N_{0b}\alpha_e\sigma_b^2 - N_bP_t\alpha_b\alpha_e(N_{0b} - N_{0e})}{2N_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)} \\
&\quad + \frac{\sqrt{\alpha_b^2\alpha_e^2\beta_b^2P_t^2N_b^2(N_{0b} - N_{0e})^2 + 4N_{0b}^2N_{0e}\alpha_b\alpha_e\beta_b\sigma_b^2(N_bP_t\alpha_b\beta_e - N_bP_t\alpha_e\beta_b + N_{0b}\beta_e\sigma_b^2)}}{2N_b\beta_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)}, \\
x_4 &= \frac{2N_{0e}N_{0b}\alpha_e\sigma_b^2 - N_bP_t\alpha_b\alpha_e(N_{0b} - N_{0e})}{2N_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)} \\
&\quad - \frac{\sqrt{\alpha_b^2\alpha_e^2\beta_b^2P_t^2N_b^2(N_{0b} - N_{0e})^2 + 4N_{0b}^2N_{0e}\alpha_b\alpha_e\beta_b\sigma_b^2(N_bP_t\alpha_b\beta_e - N_bP_t\alpha_e\beta_b + N_{0b}\beta_e\sigma_b^2)}}{2N_b\beta_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)}.
\end{aligned}$$

Proof: See Appendix B.4. ■

Remark 3.2. Proposition 3.2 provides the optimal jamming power that maximizes the worst-case secrecy capacity of the basic jammer-assisted system. If there is no power constraint at the jammer, we can simply set the jamming power as P_j^* to achieve the best secrecy performance. If there exists a power constraint at the jammer, say $P_j \leq P_{j,\max}$, we should first check the feasibility of achieving the non-zero worst-case secrecy capacity, and then set the jamming power as $\min(P_j^*, P_{j,\max})$ if the non-zero worst-case secrecy capacity is achievable.

3.4.3 AN Jammer-Assisted System

Based on Theorem 3.2 and (3.18), the worst-case secrecy capacity of the AN jammer-assisted system is given by

$$C_s^w = \begin{cases} \left[N_b \log_2 \left(1 + \frac{\alpha_b P_t}{\sigma_b^2} \right) - N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right) \right]^+, & \text{if } N_b \leq N_{0b} \\ \left[N_{0b} \log_2 \left(1 + \frac{N_b}{N_{0b}} \frac{\alpha_b P_t}{\sigma_b^2} \right) - N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j} \right) \right]^+, & \text{if } N_b > N_{0b}. \end{cases} \quad (3.24)$$

Similar to the case of basic jammer-assisted system, we note that a non-zero worst-case secrecy capacity sometimes is achievable for the AN jammer-assisted system, depending on the system parameters, such as transmit power, average channel gains, the spatial constraint at Bob and the number of antennas at Bob. Consider the scenario where the number of antennas at Bob, N_b , is controllable and the other system parameters, i.e., $N_{0b}, N_{0e}, \alpha_b, \beta_b, \alpha_e, \beta_e, P_t$ and P_j , are fixed. From (3.24), we find that a non-zero worst-case secrecy capacity is always achievable by having “enough” receive antennas at Bob, and the minimum N_b to ensure a non-zero worst-case

secrecy capacity is given by

$$N_{b,\min} = \begin{cases} \left\lceil \frac{N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j}\right)}{\log_2 \left(1 + \frac{\alpha_b P_t}{\sigma_b^2}\right)} \right\rceil + 1, & \text{if } N_{0b} \log_2 \left(1 + \frac{\alpha_b P_t}{\sigma_b^2}\right) \geq N_{0e} \log_2 \left(1 + \frac{\alpha_e P_t}{\beta_e P_j}\right) \\ \left\lceil \frac{N_{0b} \alpha_b^2}{\beta_b P_t} \left(\left(1 + \frac{\beta_e P_t}{\beta_b P_j}\right)^{\frac{N_{0e}}{N_{0b}}} - 1 \right) \right\rceil + 1, & \text{otherwise.} \end{cases} \quad (3.25)$$

In terms of the optimal jammer power that maximizes the worst-case secrecy capacity, it is wise to have P_j as large as possible, since the increase of P_j only degrades the capacity of Eve's channel but does not affect the capacity of Bob's channel. Mathematically, we give the following proof for that the worst-case secrecy capacity of the AN jammer-assisted system is a monotonically increasing function of the jamming power.

Proof: We first rewrite (3.24) as

$$C_s^w = \begin{cases} [f_1(P_j)]^+, & \text{if } N_b \leq N_{0b} \\ [f_2(P_j)]^+, & \text{if } N_b > N_{0b}. \end{cases} \quad (3.26)$$

Then, we find that

$$\frac{\partial f_1(P_j)}{\partial P_j} = \frac{\partial f_2(P_j)}{\partial P_j} = \frac{N_{0e} P_t \alpha_e}{\left(1 + \frac{\alpha_e P_t}{\beta_e P_j}\right) \ln 2 \beta_e P_j^2} > 0 \quad (3.27)$$

always holds for any positive value of P_j . Thus, the secrecy capacity of the AN jammer-assisted system is a monotonically increasing function of the jamming power. ■

3.4.4 Numerical Results

In this subsection, we present the numerical results based on the worst-case analysis. Since the worst-case secrecy capacity of the wiretap-channel system is always equal to zero, we do not present the numerical results for the wiretap-channel system in this subsection but focus on the basic jammer-assisted system and the AN jammer-assisted system. Besides, we still adopt the 2D analysis to characterize the spatial constraints at the receiver side, such that Bob and Eve are spatially constrained by circular apertures.

We first compare the minimum numbers of Bob's antennas to achieve a non-zero worst-case secrecy capacity of the basic jammer-assisted system and the AN jammer-assisted system. Figure 3.9 plots $N_{b,\min}$ versus r_e based on (3.22) and (3.25). As shown in the figure, $N_{b,\min}$ increases with r_e for both systems, which indicates that we need more antennas at Bob to ensure a non-zero worst-case secrecy capacity as the radius of Eve's spatial constraint increases. In addition, we note that the increase of $N_{b,\min}$ with respect to r_e is slow when r_e is small, but it becomes fast when r_e is large. Such an observation is more clear for the basic jammer-

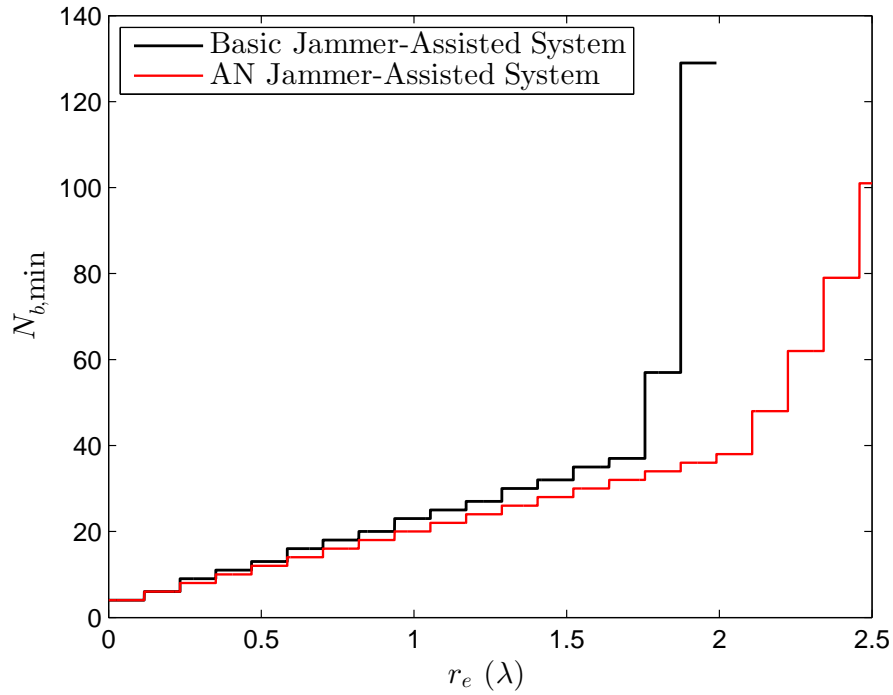


Figure 3.9: The minimum number of Bob's antennas for achieving a non-zero worst-case secrecy capacity versus the radius of Eve's spatial constraint. The other system parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$ and $r_b = 2\lambda$.

assisted system compared with that for the AN jammer-assisted system. Hence, the cost of antennas at Bob to ensure a non-zero worst-case secrecy capacity is very large when the radius of Eve's spatial constraint is large, especially for the basic jammer-assisted system. When r_e is very large, i.e., $r_e > r_b = 2\lambda$ in the figure, the basic jammer-assisted system cannot achieve a non-zero worst-case secrecy capacity no matter how many antennas are equipped at Bob. The condition under which the basic jammer-assisted system always cannot achieve the non-zero worst-case secrecy capacity is given by (3.21). In contrast, the AN jammer-assisted system can always ensure a non-zero worst-case secrecy capacity by increasing the number of Bob's antennas, as long as Eve has a finite spatial constraint.

It is worth pointing out that the minimum number of receive antennas to ensure a non-zero worst-case secrecy capacity is determined by not only the spatial constraint at the eavesdropper but also many other system parameters, such as the spatial constraint at the legitimate receiver, transmit power, jamming power, average channel gains and the noise variance at the receiver. Thus, the result in Figure 3.9 can be only regarded as an example to illustrate the required values of $N_{b,\min}$ for different values of r_e . The required $N_{b,\min}$ is not necessary to be extremely large for a very large value of r_e . For example, the required $N_{b,\min}$ is equal to 116 for $r_e = 10\lambda$

in an AN jammer-assisted system with $r_b = 8\lambda$, $\alpha_b = 10$, $\alpha_e = 10$, $\beta_b = 10$ and $\beta_e = 10$.

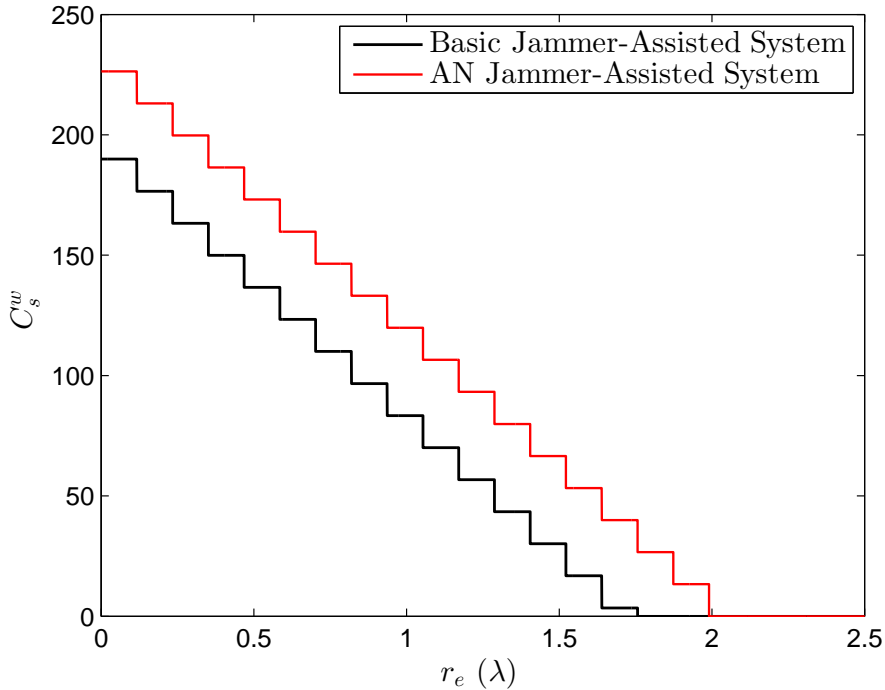


Figure 3.10: The worst-case secrecy capacity versus the radius of Eve's spatial constraint. The other system parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $r_b = 2\lambda$ and $N_b = N_{0b} = 37$.

Now, we depict the worst-case secrecy capacity for different spatial constraints at Eve. Figure 3.10 plots C_s^w versus r_e for the basic jammer-assisted system and the AN jammer-assisted system according to (3.20) and (3.24), respectively. The number of Bob's antennas is chosen equal to the saturation number of receive antennas at Bob, i.e., $N_b = N_{0b} = 37$. As the figure shows, C_s^w decreases with r_e for both systems. Comparing the two curves, we note that the worst-case secrecy capacity of the basic jammer-assisted system is always smaller than that for the AN jammer-assisted system. In addition, the difference of C_s^w between the two systems keeps the same for different values of r_e . This can be explained as follows. The basic jamming signals and the AN jamming signals have the same effect on Eve's channel while different effects on Bob's channel. Hence, the difference of C_s^w between the two systems is actually due to the difference of the capacity of Bob's channel subject to different jamming techniques, and it is not related to Eve's channel condition or spatial constraint. Therefore, the difference of C_s^w between the two curves in the figure keeps the same for different values of r_e .

Finally, we illustrate the impact of jamming power on the worst-case secrecy capacity. Figure 3.11 plots C_s^w versus P_j for both the basic jammer-assisted system and the AN jammer-

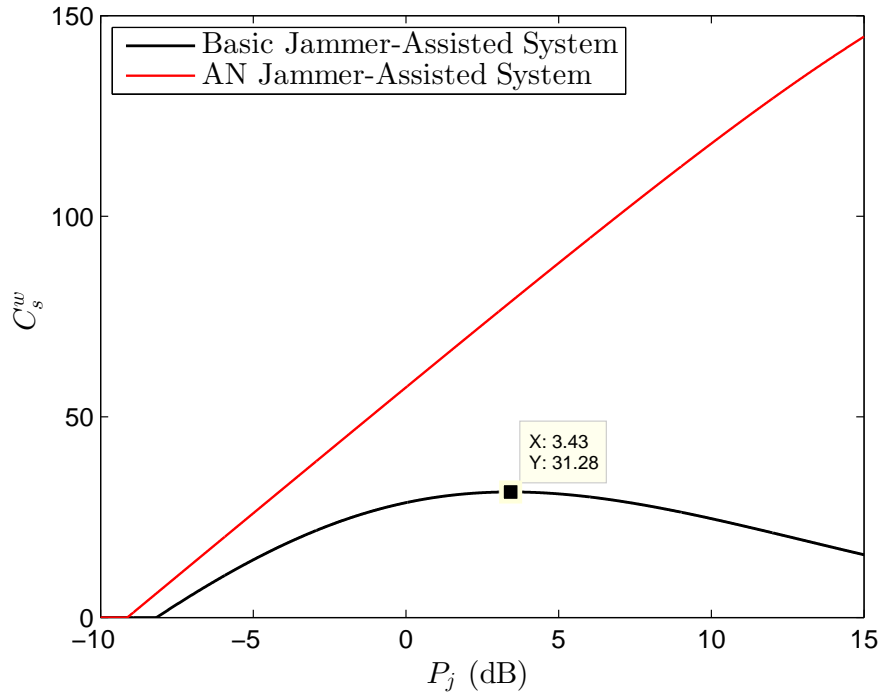


Figure 3.11: The worst-case secrecy capacity versus the jamming power. The other system parameters are $P_t = 20$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $r_b = 1.5\lambda$, $r_e = 1\lambda$ and $N_b = 30$.

assisted system. As shown in the figure, the value of C_s^w for the basic jammer-assisted system increases with P_j when P_j is small, but it decreases with P_j when P_j goes large. There exists an optimal value of P_j that maximizes C_s^w for the basic jammer-assisted system, i.e., $P_j = 3.43$ dB in the figure. By using the analytical results given in Proposition 3.2, we also obtain that P_j^* for the given scenario is equal to 3.43 dB. This verifies the optimality of P_j^* obtained in our analytical results. In contrast, the value of C_s^w for the AN jammer-assisted system always increases with P_j , which is also consistent with our analytical results. Moreover, comparing the basic jammer-assisted system and the AN jammer-assisted system, we note that the difference of C_s^w between the two curves increases with P_j all the time.

It is worth mentioning that the numerical results in this chapter are all based on the 2D analysis. If we adopt the 3D analysis rather than the 2D analysis, the saturation numbers of the antennas would increase given a same radius of the spatial constraint. The increase of the saturation number further affects other results shown in this chapter. Especially, we have to place more antennas at Bob (a larger $N_{b,\min}$) to ensure the non-zero secrecy capacity if we consider the 3D model rather than the 2D model.

3.5 Summary

In this chapter, we introduced the spatial constraint into physical layer security for multi-antenna systems, which provides an approach to study the secrecy capacity without knowing the number of eavesdropper antennas. We considered basic secure communication systems with spatial constraints at the receiver side. Specifically, we studied the wiretap-channel system, the basic jammer-assisted system and the AN jammer-assisted system, and derived the expressions for secrecy capacity of each system. We found that a non-zero worst-case secrecy capacity is achievable with the assist of jamming signals, even if the eavesdropper is equipped with infinite number of antennas. Moreover, the optimal jamming power that maximizes the worst-case secrecy capacity was obtained. We highlight that the major contribution of this chapter is to address the practically important problem of how to study secure communications without knowing the number of eavesdropper antennas, and hope the work in this chapter can be a good inspiration for future researchers to design novel physical layer techniques to efficiently secure wireless communications without the information of eavesdropper antennas.

Base Station Cooperation for Confidential Broadcasting in Multi-Cell Networks

4.1 Introduction

The previous two chapters studied the physical layer security with practical assumptions in order to enhance the practicality of physical layer security. In the following two chapters, we aim to improve the applicability of physical layer security in practical networks.

Apart from the wiretap-channel systems, there exists another branch of research focusing on the physical layer security in multi-antenna broadcast networks, and aiming at achieving confidential broadcasting. Confidential broadcasting requires multiple messages to be securely broadcasted to multiple users in the network, and each message is intended for one user but needs to keep secret from the other users. We note that the solution to confidentially broadcasting messages in multi-cell networks has not been addressed in the literature, although the confidential broadcasting in a single isolated cell has been elaborately studied in, e.g., [41, 43, 44, 45]. In multi-cell networks, the control of inter-cell information leakage and interference becomes very important, besides the intra-cell information leakage and interference. This makes the current techniques achieving confidential broadcasting in single-cell networks not applicable to multi-cell networks.

In this chapter, we provide an effective solution to tackle the challenging problem of multi-cell confidential broadcasting. To this end, we design linear precoders at BSs that achieve confidential broadcasting in the multi-cell network. Two forms of cooperation at the BSs, i.e., the MCP and the CBf, are taken into consideration such that the BSs can share control signals, CSI and/or messages to cooperatively serve users in multiple cells. In the MCP, the BSs fully cooperate such that they share their CSI and messages to transmit. Alternatively, in the CBf the BSs “partially” cooperate. As such, they do not share their messages to transmit but allow users to feed back the CSI to the cross-cell BS. In practice, the MCP is appropriate for the

networks where high-capacity backhaul links are established to enable the sharing of CSI and messages between BSs, while the CBF is suitable for the networks where such high-capacity backhaul links are not available.

The remainder of this chapter is organized as follows. Section 4.2 introduces the network model, describes the designed precoders, and formulates the achievable secrecy sum rate for the MCP and the CBF. Section 4.3 derives the large-system expressions for the secrecy sum rates for both forms of BS cooperation. Section 4.4 details the optimization of network performance. Finally, the summary of this chapter is given in Section 4.5.

4.2 Network Model

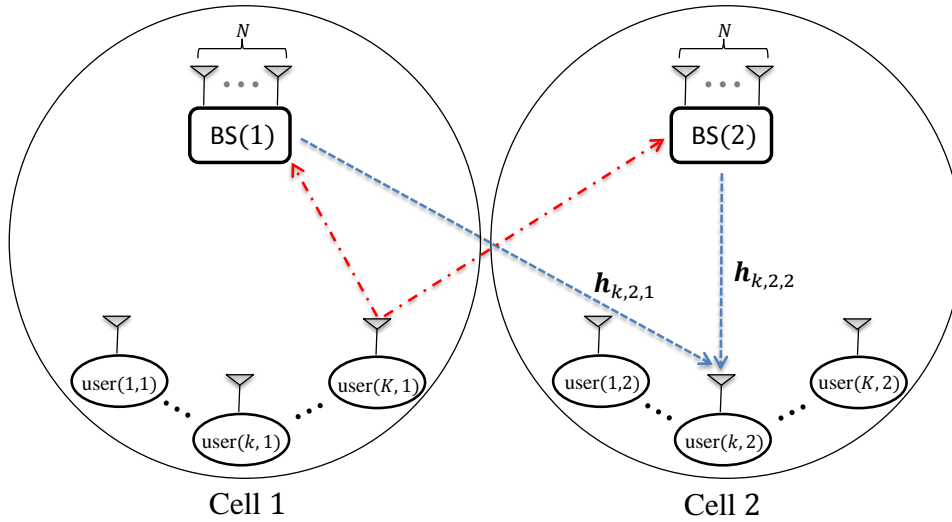


Figure 4.1: Illustration of a symmetric two-cell broadcast network, where each cell consists of one N -antenna BS and K single-antenna users.

We consider a symmetric two-cell broadcast network, as depicted in Figure 4.1. In each cell, there are K single-antenna users and one N -antenna BS. The two BSs cooperate to serve the users in two cells. For this network, we consider two forms of BS cooperation in this chapter, i.e., the MCP and the CBF, the practicality of which are presented in Section 4.1. For the sake of brevity, we denote BS (i) and user (k, j) as the BS in cell i and the user k in cell j , respectively, where $i \in \{1, 2\}$, $j \in \{1, 2\}$ and $k \in \{1, 2, \dots, K\}$. Moreover, we adopt the following notations to represent the channel coefficients in the two-cell broadcast network:

1. The channel vector from BS (i) to user (k, j) is denoted by the *row* vector $\mathbf{h}_{k,j,i}$.
2. The $2K \times N$ channel matrix from BS (i) to all the users in both cells is denoted by $\mathbf{H}_i = [\mathbf{h}_{1,1,i}^H, \mathbf{h}_{2,1,i}^H \cdots \mathbf{h}_{K,1,i}^H, \mathbf{h}_{1,2,i}^H, \mathbf{h}_{2,2,i}^H \cdots \mathbf{h}_{K,2,i}^H]^H$.

3. The channel vector from both BSs to user (k, j) is denoted by $\mathbf{h}_{k,j} = [\mathbf{h}_{k,j,1} \ \mathbf{h}_{k,j,2}]$.
4. The $2K \times 2N$ channel matrix from both BSs to all the users in both cells is denoted by $\mathbf{H} = [\mathbf{h}_{1,1}^H \ \mathbf{h}_{2,1}^H \ \cdots \ \mathbf{h}_{K,1}^H \ \mathbf{h}_{1,2}^H \ \mathbf{h}_{2,2}^H \ \cdots \ \mathbf{h}_{K,2}^H]^H$.
5. The channel vector between a user and the same-cell BS is denoted by $\mathbf{h}_{k,j,j}$.
6. The channel vector between a user and the cross-cell BS is denoted by $\mathbf{h}_{k,j,\bar{j}}$ where $\bar{j} = 1$ if $j = 2$ and $\bar{j} = 2$ if $j = 1$.

We assume that the antennas at the BSs and the users are sufficiently spaced apart such that all links between the transmit and receive antennas are uncorrelated. We also assume that the data are transmitted over the block fading channel where the coherence time of the channel is larger than the symbol interval. In addition, we consider a homogenous scenario where all users in the same cell to a BS have the same average power. This is a widely-adopted consideration for multi-user networks where the users in the same cell are located at the same distance away from the BS. A practical example of this scenario is that the users in the same cell are close together, e.g., in an office building, but far from the BS. Then, the channels between a user and the same-cell BS are modeled as i.i.d. complex Gaussian variables with zero mean and unit variance, i.e., $\mathbf{h}_{k,j,j} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$, whereas the channels between a user and the cross-cell BS are modeled as i.i.d. complex Gaussian variables with zero mean and variance ε , i.e., $\mathbf{h}_{k,j,\bar{j}} \sim \mathcal{CN}(\mathbf{0}, \varepsilon \mathbf{I}_N)$. Here, $0 < \varepsilon \leq 1$ represents the cross-cell interference level, which characterizes the severity of interference between two cells [60, 84]. In addition, we assume that each user (k, j) perfectly knows $\mathbf{h}_{k,j}$ and feeds back $\mathbf{h}_{k,j,j}$ to the same-cell BS and $\mathbf{h}_{k,j,\bar{j}}$ to the cross-cell BS through corresponding uplink channels. Finally, we assume that the BSs perfectly recover the CSI from feedback information. We note that this chapter adopts the assumption of perfect CSI at the BS. If channel estimation errors exist, the achievable secrecy rates of the proposed schemes would become worse. As such, the achievable secrecy rates derived in this chapter can be treated as an upper bound on the achievable secrecy rates for the network with channel estimation errors.

Given the aforementioned assumptions and notations, the received signal at user (k, j) is given by

$$y_{k,j} = \mathbf{h}_{k,j,1} \mathbf{x}_1 + \mathbf{h}_{k,j,2} \mathbf{x}_2 + n_{k,j}, \quad (4.1)$$

where $\mathbf{x}_i \in \mathbb{C}^{N \times 1}$, $i \in \{1, 2\}$ is the transmitted data from BS (i) and $n_{k,j} \sim \mathcal{CN}(0, \sigma_d^2)$ is the AWGN at user (k, j) . We clarify that \mathbf{x}_i consists of the linearly precoded symbols for the users to be served. We also clarify that the generation of \mathbf{x}_i depends on the form of BS cooperation considered, as will be detailed in Sections 4.2.2 and 4.2.3. The vector equation of received signals at all users is given by

$$\mathbf{y} = \mathbf{H}_1 \mathbf{x}_1 + \mathbf{H}_2 \mathbf{x}_2 + \mathbf{n}, \quad (4.2)$$

where $\mathbf{y} = [y_{1,1} \ y_{2,1} \ \cdots \ y_{K,1} \ y_{1,2} \ y_{2,2} \ \cdots \ y_{K,2}]^T$ and $\mathbf{n} = [n_{1,1} \ n_{2,1} \ \cdots \ n_{K,1} \ n_{1,2} \ n_{2,2} \ \cdots \ n_{K,2}]^T$.

4.2.1 Confidential Broadcasting and Performance Metric

The aim of this chapter is to design linear precoders to achieve confidential broadcasting in the two-cell broadcast network. To meet the requirement of confidential broadcasting, the message for each user (k, j) needs to be securely transmitted such that the unintended users obtain zero information. We consider a worst-case scenario in the two-cell network. In such a scenario, we assume that for the message to each user (k, j) , all remaining $2K - 1$ users in both cells act as eavesdroppers, and they jointly eavesdrop on the message in a collaborative manner. The cooperating eavesdroppers decode their own signals and share them with each other. It follows that the cooperating eavesdroppers are able to perform interference cancellation, leaving only the signal for the intended user. The alliance of $2K - 1$ cooperating eavesdroppers is equivalent to a single eavesdropper with $2K - 1$ distributed receive antennas, which is denoted by the eavesdropper (\tilde{k}, \tilde{j}) . The consideration of the worst-case scenario is motivated by the fact that the malicious behaviors of the potential eavesdroppers in the network are not fully controllable or predictable at the BSs. As a result, the weaker assumption of non-colluding eavesdroppers (or equivalently, eavesdroppers are interfered by each other) cannot lead to any true guarantee of security. Furthermore, we clarify that intentionally sharing the received messages by potential eavesdroppers does not disobey the rule of confidential broadcasting. This is due to the fact that confidential broadcasting requires the BSs to securely transmit messages to each user, but does not control the users' behaviors after receiving messages. Due to the aforementioned necessity, we highlight that the consideration of the worst-case scenario is widely adopted in designing confidential broadcasting networks, e.g., [41, 43, 44, 45].

The secrecy performance in the two-cell broadcast network is measured by the secrecy sum rate, denoted by R_s . It is mathematically formulated as

$$R_s = \sum_{j=1}^2 \sum_{k=1}^K R_{kj}, \quad (4.3)$$

where R_{kj} is the secrecy rate for the message to user (k, j) . According to the principles of physically layer security, R_{kj} is given by

$$R_{kj} = \left[\log_2 (1 + \text{SINR}_{k,j}) - \log_2 (1 + \text{SINR}_{\tilde{k},\tilde{j}}) \right]^+, \quad (4.4)$$

where $\text{SINR}_{k,j}$ and $\text{SINR}_{\tilde{k},\tilde{j}}$ denote the signal-to-interference-plus-noise ratios (SINRs) at the intended user (k, j) and the eavesdropper (\tilde{k}, \tilde{j}) , respectively.

Note that we assume that the eavesdroppers' CSI is available at the transmitter in this chapter, which is different from the CSI assumptions in the previous two chapters. This is because

that we study the scenario where potential eavesdroppers are users served by the transmitter in this chapter, while in the the previous two chapters we consider the scenarios where the eavesdropper(s) are external and not served by the transmitter.

4.2.2 Multi-Cell Processing with RCI Precoder

In the MCP, the two BSs fully cooperate to serve the users in the two cells based on the mutually shared CSI and messages to transmit. We note that the two-cell broadcast network with the MCP may appear to be similar to a single-cell broadcast network with $2N$ transmit antennas and $2K$ single-antenna users. However, it is worth mentioning that the design of transmission schemes and the corresponding analysis for confidential broadcasting in the MCP, which take the cross-cell interference level ε into consideration, are fundamentally different from those for confidential broadcasting in a single cell, e.g., [43]. As mentioned before, the cross-cell interference level, ε , characterizes the severity of interference between two cells. For the single-cell network considered in [43], the average SNRs for all channels between the BS and the users are assumed to be the same. This implies that all channels are identically distributed. Different from [43], for considered the MCP, the average SNRs of the same-cell channels are different from the average SNRs of the cross-cell channels. For example, if the average SNRs of the same-cell channels are equal to 1, the average SNRs of the cross-cell channels are equal to ε , where $0 < \varepsilon \leq 1$. This implies that all channels are non-identically distributed. Therefore, the large-system analysis of the secrecy sum rate in [43] cannot be directly applied in the MCP, and new large-system analysis needs to be conducted to address the non-identically distributed channel coefficients. We find that when $\varepsilon = 1$, the MCP reduces to the single-cell network, which shows that the result in [43] is a special case of the result for the MCP.

We next detail the precoder design for the MCP. In our design, the RCI precoder [59] is adopted at BSs to achieve confidential broadcasting. As a linear precoder, the RCI precoder has a low signal-processing complexity and the ability of controlling the information leakage as well as the interference amongst the users [43, 45]. As per the rules of the RCI precoder, the precoding vector for the message to user (k, j) is given by

$$\mathbf{w}_{k,j} = c (\mathbf{H}^H \mathbf{H} + \alpha \mathbf{I}_{2N})^{-1} \mathbf{h}_{k,j}^H, \quad (4.5)$$

where c is a scaling factor to ensure the power constraint at BSs and α is a real non-negative regularization parameter. Notably, the regularization parameter α achieves a tradeoff between the signal power at the intended receiver and the amount of information leakage as well as interference amongst users. Using $\mathbf{w}_{k,j}$, the transmitted data vector $\mathbf{x} = [\mathbf{x}_1; \mathbf{x}_2]$ is written as

$$\mathbf{x} = \sum_{j=1}^2 \sum_{k=1}^K \mathbf{w}_{k,j} s_{k,j}, \quad (4.6)$$

where $s_{k,j}$ denotes the message to be transmitted to user (k, j) . We assume that the messages for different users are independent and impose a unit average power constraint on $s_{k,j}$ such that $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_{2K}$ with $\mathbf{s} = [\mathbf{s}_1; \mathbf{s}_2]$ and $\mathbf{s}_j = [s_{1,j} \ s_{2,j} \ \dots \ s_{K,j}]^T$. We also assume that the BSs are subject to an average sum-power constraint such that $\mathbb{E}\{\|\mathbf{x}\|^2\} = P_t$. Accordingly, the scaling factor c is determined by

$$c^2 = \frac{P_t}{\text{Tr}\left((\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-2}\mathbf{H}^H\mathbf{H}\right)}. \quad (4.7)$$

Based on (4.5) and (4.6), the received signal at the intended user (k, j) is written as

$$\begin{aligned} y_{k,j} &= \mathbf{c}\mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{H}^H\mathbf{s} + n_{k,j} \\ &= \mathbf{c}\mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H s_{k,j} + \mathbf{c}\mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{s}_{\tilde{k},\tilde{j}} + n_{k,j}, \end{aligned} \quad (4.8)$$

where $\mathbf{H}_{\tilde{k},\tilde{j}}$ and $\mathbf{s}_{\tilde{k},\tilde{j}}$ are obtained from \mathbf{H} and \mathbf{s} by removing the row corresponding to user (k, j) , respectively. Moreover, the received signal vector at the eavesdropper (\tilde{k}, \tilde{j}) is written as

$$\mathbf{y}_{\tilde{k},\tilde{j}} = c\mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H s_{k,j} + \mathbf{n}_{\tilde{k},\tilde{j}}, \quad (4.9)$$

where $\mathbf{y}_{\tilde{k},\tilde{j}}$ and $\mathbf{n}_{\tilde{k},\tilde{j}}$ are obtained from \mathbf{y} and \mathbf{n} by removing the row corresponding to user (k, j) , respectively. Based on (4.8) and (4.9), the SINRs for the message $s_{k,j}$ at the intended user (k, j) and the eavesdropper (\tilde{k}, \tilde{j}) are given by

$$\text{SINR}_{k,j} = \frac{c^2 \left| \mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H \right|^2}{c^2\psi + \sigma_d^2} \quad (4.10)$$

and

$$\text{SINR}_{\tilde{k},\tilde{j}} = \frac{c^2 \left| \mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H \right|^2}{\sigma_d^2}, \quad (4.11)$$

respectively, where

$$\psi = \mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}. \quad (4.12)$$

As such, the secrecy sum rate achieved by the RCI precoder for the MCP is obtained as

$$R_{s,\text{MCP}} = \sum_{j=1}^2 \sum_{k=1}^K \left[\log_2 \left(\frac{1 + \frac{c^2 \left| \mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H \right|^2}{c^2 \mathbf{h}_{k,j}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H + \sigma_d^2}}{1 + \frac{c^2 \left| \mathbf{H}_{\tilde{k},\tilde{j}}(\mathbf{H}^H\mathbf{H} + \alpha\mathbf{I}_{2N})^{-1}\mathbf{h}_{k,j}^H \right|^2}{\sigma_d^2}} \right) \right]^+. \quad (4.13)$$

4.2.3 Coordinated Beamforming with Generalized RCI Precoder

In the CBf, the two BSs partially cooperate based on the CSI from all users. Since the BSs do not know the messages for the cross-cell users, they only transmit data for the users in their own cells. Also, the two BSs cooperate to control the information leakage in both cells. Furthermore, they cooperate to control the interference power amongst the users in both cells (or equivalently, the received signal power at unintended users) by properly designing the precoder and wisely choosing the regularization parameter α [60, 85].

We now detail the precoder design for the CBf. In this design, we consider the generalized RCI precoder [60] at BSs to achieve confidential broadcasting. Note that the generalized RCI precoder has never been investigated as a method to achieve confidential broadcasting. Moreover, the principle of the generalized RCI precoder is different from that of the RCI precoder. We clarify that the primary benefit of using the generalized RCI precoder for the CBf is that each BS in this precoder controls the interference and information leakage amongst the users not only in the same cell but also in the cross cell. If we adopt the RCI precoder in the CBf, as we do in the MCP, each BS transmits data and controls the interference and information leakage amongst the users only in the same cell. As per the rules of the generalized RCI precoder, the precoding vector for the message to user (k, j) is given by

$$\begin{aligned} \mathbf{w}_{k,j} &= c_j \hat{\mathbf{w}}_{k,j} \\ &= c_j \left(\sum_{(l,m) \neq (k,j)} \mathbf{h}_{l,m,j}^H \mathbf{h}_{l,m,j} + \alpha \mathbf{I}_N \right)^{-1} \mathbf{h}_{k,j,j}^H, \end{aligned} \quad (4.14)$$

where c_j is the scaling factor to ensure the power constraint at BS (j) and α is the real non-negative regularization parameter achieving the tradeoff between the signal power at the intended receiver and the amount of information leakage as well as interference amongst users. The transmitted data vector at the BS (j) is written as

$$\mathbf{x}_j = \sum_{k=1}^K \mathbf{w}_{k,j} s_{k,j}, \quad (4.15)$$

where $s_{k,j}$ denotes the message to be transmitted to user (k, j) with the same property as that in the MCP. From (4.14) and (4.15), we find that BS (j) only requires the CSI from itself to users, $\mathbf{h}_{k,i,j}$, to construct the precoding matrix. That is, BS (j) does not need the CSI from the other BS (\bar{j}) to users, $\mathbf{h}_{k,i,\bar{j}}$, for the precoding matrix construction. Different from the average sum-power constraint for two BSs in the MCP, we consider in the CBf that each BS is subject to an average power constraint, such that $\mathbb{E} \{ \|\mathbf{x}_j\|^2 \} = P_j$. Then the total power constraint for two BSs is given by $P_t = P_1 + P_2$. Here we assume the same average power constraint at both

BSs, i.e., $P_1 = P_2 = P = P_t/2$. Hence, the scaling factor c_j in (4.14) is determined by

$$c_j^2 = \frac{P_j}{\sum_{k=1}^K \|\hat{\mathbf{w}}_{k,j}\|^2}. \quad (4.16)$$

Based on (4.14) and (4.15), the received signal at the intended user (k, j) is written as

$$y_{k,j} = \mathbf{h}_{k,j,j} \mathbf{w}_{k,j} s_{k,j} + \sum_{(k',j') \neq (k,j)} \mathbf{h}_{k,j,j'} \mathbf{w}_{k',j'} s_{k',j'} + n_{k,j}. \quad (4.17)$$

Moreover, the received signal vector at the eavesdropper (\tilde{k}, \tilde{j}) is written as

$$\mathbf{y}_{\tilde{k},\tilde{j}} = \mathbf{H}_{\tilde{k},\tilde{j},j} \mathbf{w}_{k,j} s_{k,j} + \mathbf{n}_{\tilde{k},\tilde{j}}. \quad (4.18)$$

where $\mathbf{H}_{\tilde{k},\tilde{j},j}$ and $\mathbf{n}_{\tilde{k},\tilde{j}}$ are obtained from \mathbf{H}_j and \mathbf{n} by removing the row corresponding to user (k, j) , respectively. Based on (4.17) and (4.18), the SINRs for the message $s_{k,j}$ at the intended user (k, j) and the eavesdropper (\tilde{k}, \tilde{j}) are given by

$$\text{SINR}_{k,j} = \frac{c_j^2 |\mathbf{h}_{k,j,j} \hat{\mathbf{w}}_{k,j}|^2}{\sum_{(k',j') \neq (k,j)} c_{j'}^2 |\mathbf{h}_{k,j,j'} \hat{\mathbf{w}}_{k',j'}|^2 + \sigma_d^2} \quad (4.19)$$

and

$$\text{SINR}_{\tilde{k},\tilde{j}} = \frac{\sum_{(k',j') \neq (k,j)} c_j^2 |\mathbf{h}_{k',j',j} \hat{\mathbf{w}}_{k,j}|^2}{\sigma_d^2}, \quad (4.20)$$

respectively. Aided by (4.19) and (4.20), the secrecy sum rate achieved by the generalized RCI precoder for the CBF is obtained as

$$R_{s,\text{CBf}} = \sum_{j=1}^2 \sum_{k=1}^K \left[\log_2 \left(\frac{1 + \frac{c_j^2 |\mathbf{h}_{k,j,j} \hat{\mathbf{w}}_{k,j}|^2}{\sum_{(k',j') \neq (k,j)} c_{j'}^2 |\mathbf{h}_{k,j,j'} \hat{\mathbf{w}}_{k',j'}|^2 + \sigma_d^2}}{1 + \frac{c_j^2 |\mathbf{h}_{k',j',j} \hat{\mathbf{w}}_{k,j}|^2}{\sigma_d^2}} \right) \right]^+. \quad (4.21)$$

It is evident that the secrecy sum rates in (4.13) and (4.21) depend on the realization of each channel, $\mathbf{h}_{k,j,i}$. Based on them, we can only evaluate the secrecy performance by time-consuming numerical simulations. This motivates us to seek channel-independent expressions that reduce the complexity of performance evaluations. Therefore, in the next section we resort to the large-system analysis to explicitly characterize the secrecy sum rate of confidential broadcasting in the two-cell broadcast network.

4.3 Secrecy Sum Rate in the Large-System Regime

In this section, we derive channel-independent expressions for the secrecy sum rate of the two-cell broadcast network in the large-system regime. In such a regime, both the number of users in each cell, K , and the number of transmit antennas at each BS, N , approach infinity with a fixed ratio, $\beta = K/N$. Besides, we denote $\gamma = P_t / (2\sigma_d^2) = P / \sigma_d^2$ as the average *transmit* SNR at *each* BS. As will be shown later in numerical simulations, the analytical result in the large-system regime can accurately approximate the secrecy sum rate of the network even with finite K and N .

4.3.1 Large-System Analysis

In the large-system analysis for the symmetric two-cell network with $K, N \rightarrow \infty$, the secrecy rate for all messages $s_{k,j}$ converge to the same non-random function. This function does not depend on the realization of each channel $\mathbf{h}_{k,j,i}$. Thus, the secrecy sum rate is analytically approximated by

$$R_s^\infty = 2K (R_{k,j}^\infty) = 2K \left[\log_2 \frac{1 + \text{SINR}_{k,j}^\infty}{1 + \text{SINR}_{\tilde{k},\tilde{j}}^\infty} \right]^+, \quad (4.22)$$

where $R_{k,j}^\infty$ denotes the large-system secrecy rate for each user, $\text{SINR}_{k,j}^\infty$ and $\text{SINR}_{\tilde{k},\tilde{j}}^\infty$ denote the large-system approximations of the SINRs at the intended user and the eavesdropper, respectively.

In the following Theorem 4.1 and Theorem 4.2, we present the large-system secrecy sum rate achieved by the RCI precoder for the MCP and the large-system secrecy sum rate achieved by the generalized RCI precoder for the Cbf, respectively.

Theorem 4.1. In the large-system regime, the secrecy sum rate achieved by the RCI precoder for the MCP converges in probability to a deterministic quantity given by

$$R_{s,\text{MCP}}^\infty = \begin{cases} 2K \left[\log_2 \left(\frac{1 + (1+\varepsilon)\gamma g(\beta, \rho_M) \frac{1 + \frac{\rho_M}{\beta}(1+g(\beta, \rho_M))^2}{(1+\varepsilon)\gamma + (1+g(\beta, \rho_M))^2}}{1 + \frac{(1+\varepsilon)\gamma}{(1+g(\beta, \rho_M))^2}} \right) \right]^+, & \text{if } \alpha \neq 0 \\ 2K \log_2 \left(1 + \frac{(1-\beta)(1+\varepsilon)\gamma}{\beta} \right), & \text{if } \alpha = 0 \text{ and } \beta \leq 1 \\ 2K \left[\log_2 \left(\frac{\beta^3(\beta + (\beta-1)(1+\varepsilon)\gamma)}{(\beta^2 + (\beta-1)^2(1+\varepsilon)\gamma^2)} \right) \right]^+, & \text{if } \alpha = 0 \text{ and } \beta > 1. \end{cases} \quad (4.23)$$

where $\rho_M = (1 + \varepsilon)^{-1} \alpha / N$ and $g(\beta, \rho_M)$ is the solution of x to $x = \left(\rho_M + \frac{\beta}{1+x} \right)^{-1}$.

Proof: See Appendix C.1. ■

Theorem 4.2. In the large-system regime, the secrecy sum rate achieved by the generalized

RCI precoder for the CBf converges almost surely to a deterministic quantity given by

$$R_{s,\text{CBf}}^\infty = \begin{cases} 2K \left[\log_2 \left(\frac{1 + \frac{\frac{\Lambda}{\beta} \left(\rho_C + \frac{\beta\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{\beta}{(1+\Lambda)^2} \right)}{\frac{1}{\gamma} + \frac{\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{1}{(1+\Lambda)^2}}}{1 + \gamma \left(\frac{\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{1}{(1+\Lambda)^2} \right)} \right) \right]^+, & \text{if } \alpha \neq 0 \\ 2K \log_2 \left(1 + \frac{(1-2\beta)\gamma}{\beta} \right), & \text{if } \alpha = 0 \text{ and } \beta \leq 0.5 \\ 2K \left[\log_2 \left(\frac{1 + \frac{\frac{\Lambda_0}{\beta} \left(\frac{\beta\varepsilon}{(1+\varepsilon\Lambda_0)^2} + \frac{\beta}{(1+\Lambda_0)^2} \right)}{\frac{1}{\gamma} + \frac{\varepsilon}{(1+\varepsilon\Lambda_0)^2} + \frac{1}{(1+\Lambda_0)^2}}}{1 + \gamma \left(\frac{\varepsilon}{(1+\varepsilon\Lambda_0)^2} + \frac{1}{(1+\Lambda_0)^2} \right)} \right) \right]^+, & \text{if } \alpha = 0 \text{ and } \beta > 0.5. \end{cases} \quad (4.24)$$

where $\rho_C = \alpha/N$, Λ is the solution of x to $x = \left(\rho_C + \frac{\beta\varepsilon}{1+\varepsilon x} + \frac{\beta}{1+x} \right)^{-1}$ and Λ_0 is the solution of x to $x = \left(\frac{\beta\varepsilon}{1+\varepsilon x} + \frac{\beta}{1+x} \right)^{-1}$.

Proof: See Appendix C.2. ■

We provide several remarks about the large-system secrecy sum rates derived in Theorems 4.1 and 4.2, as follows:

Remark 4.1. Theorems 4.1 and 4.2 provide closed-form and channel-independent expressions for the large-system secrecy sum rates for the MCP and the CBf, respectively. We highlight that these expressions eliminate the computational burden of performance evaluation incurred by Monte Carlo simulations. Notably, these expressions allow us to evaluate and optimize the secrecy performance efficiently. The comparison of the optimal achievable secrecy performance between the MCP and the CBf will be conducted in Section 4.4.1.

Remark 4.2. The results for both the MCP and the CBf contain the parameter ε , such that they characterize the impact of the cross-cell interference level on the secrecy sum rate. This demonstrates that the analysis of confidential broadcasting in multi-cell networks is fundamentally different from that in single-cell networks which did not consider ε , e.g., [43].

Remark 4.3. We note that the result in Theorem 4.1 with $\varepsilon = 1$ reduces to the result for the single-cell confidential broadcasting given in [43], which demonstrates the generality of our analysis. This is due to the fact that the confidential broadcasting in a single cell with one $2N$ -antenna BS and $2K$ single-antenna users is equivalent to a special case of the confidential broadcasting in the MCP.

4.3.2 Numerical Results

In this subsection, we examine the accuracy of the large-system results by comparing the large-system secrecy sum rate, R_s^∞ , with the average secrecy sum rate of networks with finite K and

$N, \mathbb{E}\{R_s\}$. To this end, we introduce the normalized rate difference defined by

$$\Delta R_s = \frac{|\mathbb{E}\{R_s\} - R_s^\infty|}{\mathbb{E}\{R_s\}}, \quad (4.25)$$

which quantifies the rate difference between R_s^∞ and $\mathbb{E}\{R_s\}$ for finite K and N .

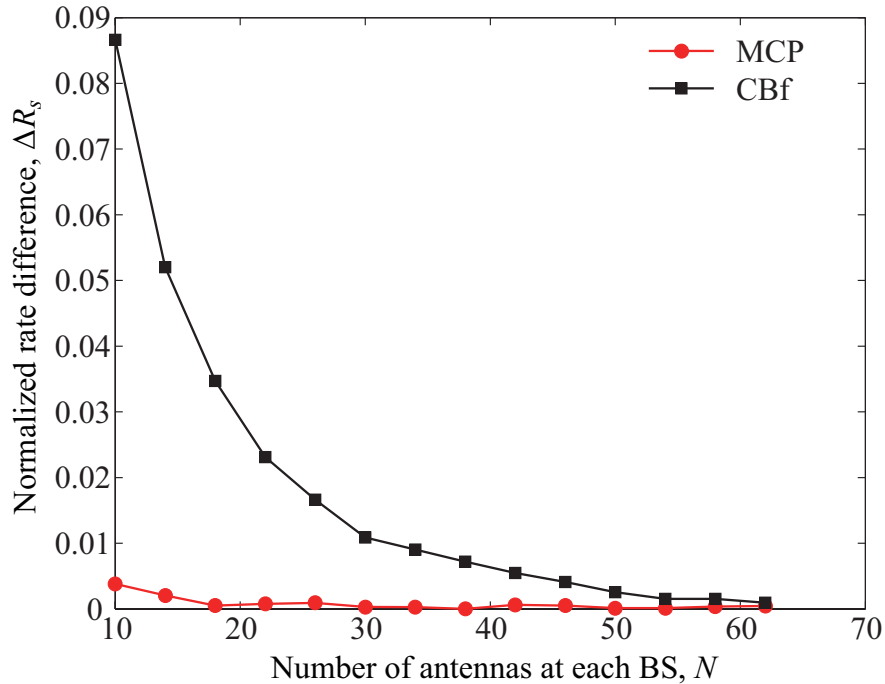


Figure 4.2: The normalized rate difference versus the number of antennas at each BS for $\varepsilon = 0.5$, $\alpha = 0.2$, $\beta = 0.5$ and $\gamma = 10$ dB.

We first demonstrate the accuracy of the large-system approximation over the size of network. Figure 4.2 plots ΔR_s versus N for the MCP and the CBf. As depicted in the figure, ΔR_s decreases as N increases. This indicates that the large-system approximation becomes more accurate as the size of network increases. Moreover, we find that the rate difference for the MCP is very small across the whole range of N , which indicates that $R_{s,\text{MCP}}^\infty$ in (4.23) is a very accurate approximation. Furthermore, we find that the rate difference for the CBf is a bit higher than that for the MCP for small N , but decreases rapidly when N grows large. Notably, the rate differences for both the MCP and the CBf are extremely small for large N , e.g., $\Delta R_s < 1\%$ for $N \geq 40$.

We then confirm the accuracy of the large-system approximation over the entire range of ε . Figure 4.3 plots ΔR_s versus ε for the MCP and the CBf. In this figure, we consider the network with $N = 20$. We find that the highest rate difference for the MCP is lower than 3×10^{-3} and the highest rate difference for the CBf is approximately 4×10^{-2} . As such, our large-system approximations provide reasonable accuracy across the entire range of ε .

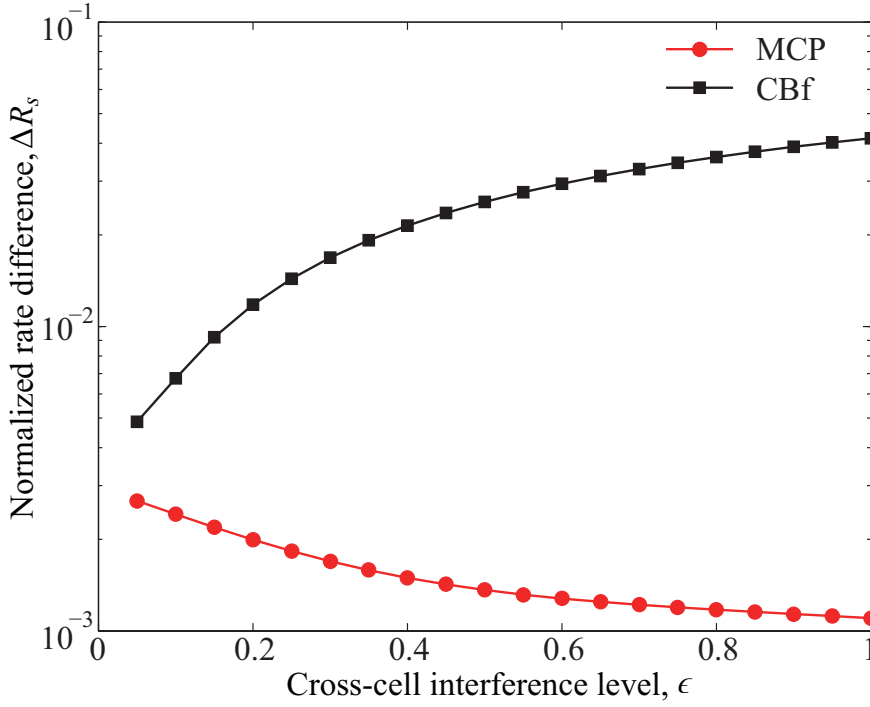


Figure 4.3: The normalized rate difference versus the cross-cell interference level for $N = 20$, $\alpha = 0.2$, $\beta = 0.5$ and $\gamma = 10$ dB.

4.4 Optimization of Secrecy Sum Rate

In this section, we maximize the large-system secrecy sum rate for the MCP and the CBf based on the derived channel-independent large-system approximations. We first determine the optimal regularization parameter that maximizes the large-system secrecy sum rate. Moreover, we propose power-reduction strategies to maintain the maximum large-system secrecy sum rate when an increasing transmit SNR cannot sustain a growing large-system secrecy sum rate for a high network load.

4.4.1 Optimal Regularization Parameter

In this subsection, we seek the optimal α which maximizes the secrecy sum rate in the large-system regime. We note that the regularization parameter in the linear precoding matrix, α , plays a pivotal role in determining the network performance. This is due to its ability of handling the trade-off between the signal power at the intended receiver and the amount of information leakage as well as interference amongst users. We denote $\alpha_{\text{MCP}}^* = \arg \max_{\alpha} R_{s,\text{MCP}}^{\infty}$ and $\alpha_{\text{CBf}}^* = \arg \max_{\alpha} R_{s,\text{CBf}}^{\infty}$ as the optimal regularization parameters for the MCP and the CBf, respectively.

4.4.1.1 α_{MCP}^* for MCP

We now determine α_{MCP}^* . By taking the first order derivative of $R_{s,\text{MCP}}^\infty$ in (4.23) with respect to α , we find that there are two possibilities for the sign of $\partial R_{s,\text{MCP}}^\infty / \partial \alpha$ when $\alpha \geq 0$: 1) $\partial R_{s,\text{MCP}}^\infty / \partial \alpha$ is always negative or 2) $\partial R_{s,\text{MCP}}^\infty / \partial \alpha$ is positive for small α and becomes negative as α increases. This implies that the optimal value of α that maximizes $R_{s,\text{MCP}}^\infty$ is equal to either zero or a unique positive value. Then we obtain the value of α_{MCP}^* by seeking the solution of α to $\partial R_{s,\text{MCP}}^\infty / \partial \alpha = 0$. After performing a series of complicated algebraic manipulations, we obtain α_{MCP}^* as

$$\alpha_{\text{MCP}}^* = \left[\frac{\beta^2 - \phi_1^2 - (\beta + \phi_1) \sqrt{\beta^2 + \beta \phi_2 + \phi_1^2} + 3\phi_3}{\frac{3\gamma}{N} (\beta + \phi_2)} \right]^+, \quad (4.26)$$

where $\phi_1 = (1 + \varepsilon)(\beta - 1)\gamma$, $\phi_2 = (1 + \varepsilon)(\beta + 2)\gamma$ and $\phi_3 = (1 + \varepsilon)\beta\gamma$. The optimality of α_{MCP}^* will be verified in Section 4.4.1.3.

4.4.1.2 α_{CBf}^* for CBf

We note that the closed-form expression for α_{CBf}^* is mathematically intractable. As such, we present Algorithm 4.1 to numerically determine α_{CBf}^* . By taking the first order derivative of $R_{s,\text{CBf}}^\infty$ in (4.24) with respect to α , we find that there are two possibilities for the sign of $\partial R_{s,\text{CBf}}^\infty / \partial \alpha$ when $\alpha \geq 0$: 1) $\partial R_{s,\text{CBf}}^\infty / \partial \alpha$ is positive for small α and becomes negative as α increases or 2) $\partial R_{s,\text{CBf}}^\infty / \partial \alpha$ is always negative. This implies that, from the theoretical perspective, the optimal value of α that maximizes $R_{s,\text{CBf}}^\infty$ is a unique positive value or approaches zero. Therefore, the value of α_{CBf}^* can be obtained by numerically searching the value of α that satisfies $\partial R_{s,\text{CBf}}^\infty / \partial \alpha = 0$, with the aid of Algorithm 4.1.

4.4.1.3 Numerical Results

In the following numerical results, we verify the optimality of the determined α_{MCP}^* and α_{CBf}^* . Figure 4.4 plots the large-system secrecy rate per transmit antenna, $R_s^\infty / (2N)$, versus ε . Specifically, we compare the performances for two different designs of α : 1) the optimal α that maximizes the large-system secrecy sum rate, i.e., α_{MCP}^* given by (4.26) for the MCP or α_{CBf}^* obtained by Algorithm 4.1 for the CBf and 2) the optimal α that maximizes the large-system sum rate without secrecy considerations given by [84], i.e., $\tilde{\alpha}_{\text{MCP}}^*$ for the MCP or $\tilde{\alpha}_{\text{CBf}}^*$ for the CBf. We find that the performance achieved by α_{MCP}^* or α_{CBf}^* is always better than that achieved by $\tilde{\alpha}_{\text{MCP}}^*$ or $\tilde{\alpha}_{\text{CBf}}^*$. We note that the difference between the performances achieved by α_{MCP}^* and $\tilde{\alpha}_{\text{MCP}}^*$ is not as obvious as that for the CBf. This is due to the values of network parameters (i.e., β and γ) chosen in the figure. Actually, the advantage of using α_{MCP}^* against $\tilde{\alpha}_{\text{MCP}}^*$ can be very obvious as well if some other network parameters are considered, e.g., $\beta = 1$.

Algorithm 4.1 Numerical Search for α_{CBf}^*

```

1: Input:  $f(x) = \frac{\partial R_{s,\text{CBf}}^\infty}{\partial \alpha}(\alpha = x)$ ;           17:   Update the upper bound by
   Acceptable error  $d$  (e.g.,  $d =$             $\alpha_u = \alpha_u \times 10^{-1}$ ;
    $10^{-10}$ );
   Initial search point  $\alpha_p$  (e.g.,  $\alpha_p =$ 
   1);
2: Output:  $\alpha_{\text{CBf}}^*$  that satisfies  $|f(\alpha_{\text{CBf}}^*)| \leq$  18:   end while
    $d$ ;
3: Initialize iteration counters:  $c = 0$ ;
4: if  $|f(\alpha_p)| \leq d$  then
5:   return  $\alpha_{\text{CBf}}^* = \alpha_p$ ; {The value of  $\alpha_{\text{CBf}}^*$ 
   is obtained.}
6: end if
7: if  $f(\alpha_p) > 0$  then
8:   Initialize the lower bound of  $\alpha_{\text{CBf}}^*$  by
    $\alpha_l = \alpha_p$ ;
9:   while  $f(\alpha_l + 2^c) > 0$  do
10:    Update the lower bound by  $\alpha_l =$ 
    $\alpha_l + 2^c$ ;
11:    Exponentially increase the one-side
   search step  $2^c$  by  $c = c + 1$ ;
12:   end while
13:   Set the upper bound of  $\alpha_{\text{CBf}}^*$  by  $\alpha_u =$ 
    $\alpha_l + 2^c$ ;
14: else
15:   Initialize the upper bound of  $\alpha_{\text{CBf}}^*$  by
    $\alpha_u = \alpha_p$ ;
16:   while  $f(\alpha_u \times 10^{-1}) < 0$  do
   17:     Update the upper bound by
    $\alpha_u = \alpha_u \times 10^{-1}$ ;
   18:   end while
   19:   Set the lower bound of  $\alpha_{\text{CBf}}^*$  by
    $\alpha_l = \alpha_u \times 10^{-1}$ ;
   20: end if
   21: if  $|f(\alpha_l)| \leq d$  then
   22:   return  $\alpha_{\text{CBf}}^* = \alpha_l$ ; {The value of  $\alpha_{\text{CBf}}^*$ 
   is obtained.}
   23: end if
   24: if  $|f(\alpha_u)| \leq d$  then
   25:   return  $\alpha_{\text{CBf}}^* = \alpha_u$ ; {The value of  $\alpha_{\text{CBf}}^*$ 
   is obtained.}
   26: end if
   27: Initialize the mid-point  $\alpha_m = (\alpha_l +$ 
    $\alpha_u)/2$ ;
   28: while  $|f(\alpha_m)| > d$  do
   29:   if  $f(\alpha_m) > 0$  then
   30:      $\alpha_l = \alpha_m$ ;  $\alpha_u = \alpha_u$ ;
   31:   else
   32:      $\alpha_l = \alpha_l$ ;  $\alpha_u = \alpha_m$ ;
   33:   end if
   34:    $\alpha_m = (\alpha_l + \alpha_u)/2$ ;
   35: end while
   36: return  $\alpha_{\text{CBf}}^* = \alpha_m$ ; {The value of  $\alpha_{\text{CBf}}^*$ 
   is obtained.}

```

These observations indicate that the optimal values of α without secrecy considerations given by [84] are no longer optimal for the networks with secrecy considerations.

Comparing the results for the MCP and the CBf, it is evident that the secrecy rate for the MCP is in general higher than that for the CBf. This is due to the fact that the BSs in the MCP share messages to transmit while the BSs in the CBf do not. Note that such an advantage of secrecy rate necessitates the high-capacity backhaul links in the MCP. Moreover, we find that the secrecy rate for the MCP increases with ε . In contrast, the secrecy rate for the CBf decreases with ε . This observation can be explained as follows. The value of ε determines the average channel gain from the cross-cell BS to the users. In particular, a higher ε increases the power of the received signals from the cross-cell BS. In the MCP where BSs share messages to transmit, a higher ε increases the received signal power at the intended user, although the interference power at the intended user and the received signal power at the eavesdropper

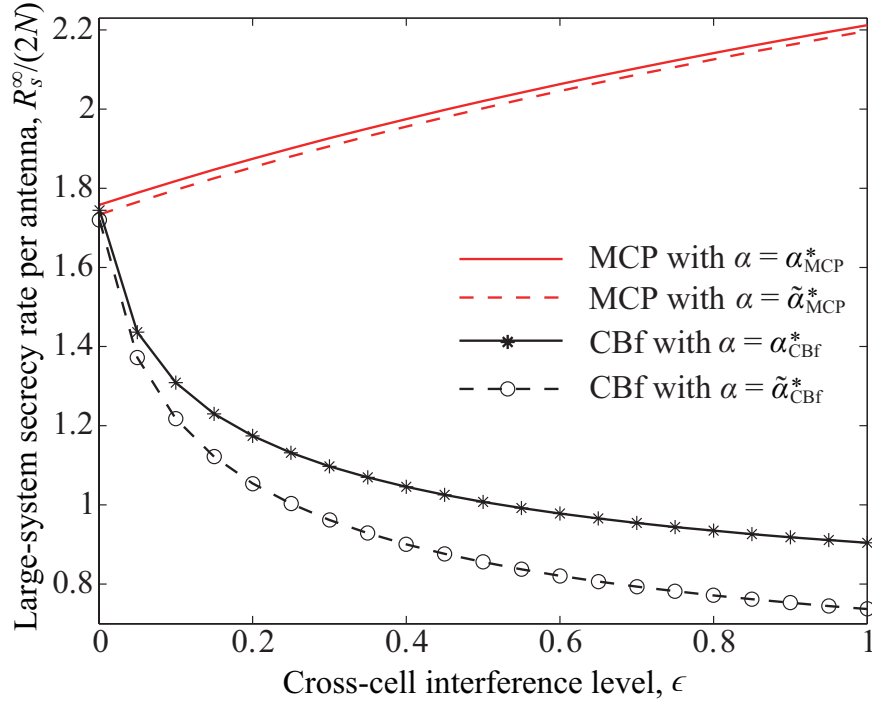


Figure 4.4: The large-system secrecy rate per antenna versus the cross-cell interference level for different designs of the regularization parameter with $N = 20$, $\beta = 0.5$ and $\gamma = 10$ dB.

increase as well. Thus, the secrecy rate for the MCP can increase as ϵ increases. On the other hand, the BSs cannot share messages to transmit in the CBf. As such, a higher ϵ only increases the interference power at the intended user and the received signal power at the eavesdropper, but does not increase the received signal power at the intended receiver. It follows that the secrecy rate for the CBf always decreases as ϵ increases.

We next demonstrate the optimality of the determined α_{MCP}^* and α_{CBf}^* over the average transmit SNR per BS, γ , and examine the impact of γ on the large-system secrecy sum rate. Figures 4.5 and 4.6 plot $R_s^\infty / (2N)$ versus γ for the MCP and the CBf, respectively. We compare the performance achieved by the obtained optimal α with the performance achieved by an arbitrarily chosen α , i.e., $\alpha = 0.2$, in the figures. As shown in both figures, the secrecy rate achieved by the optimal regularization parameter is always higher than that achieved by $\alpha = 0.2$ for both the MCP and the CBf, which confirms the optimality of α_{MCP}^* and α_{CBf}^* . Besides, we note that the secrecy rate achieved by $\alpha = 0.2$ always reduces to zero when γ grows large. This can be explained based on (4.23) and (4.24), i.e.,

$$\lim_{\gamma \rightarrow \infty} R_{s,MCP}^\infty = \lim_{\gamma \rightarrow \infty} R_{s,CBf}^\infty = 0, \text{ if } \alpha \neq 0. \quad (4.27)$$

Differently, the secrecy rate achieved by the optimal regularization parameter may not reduce

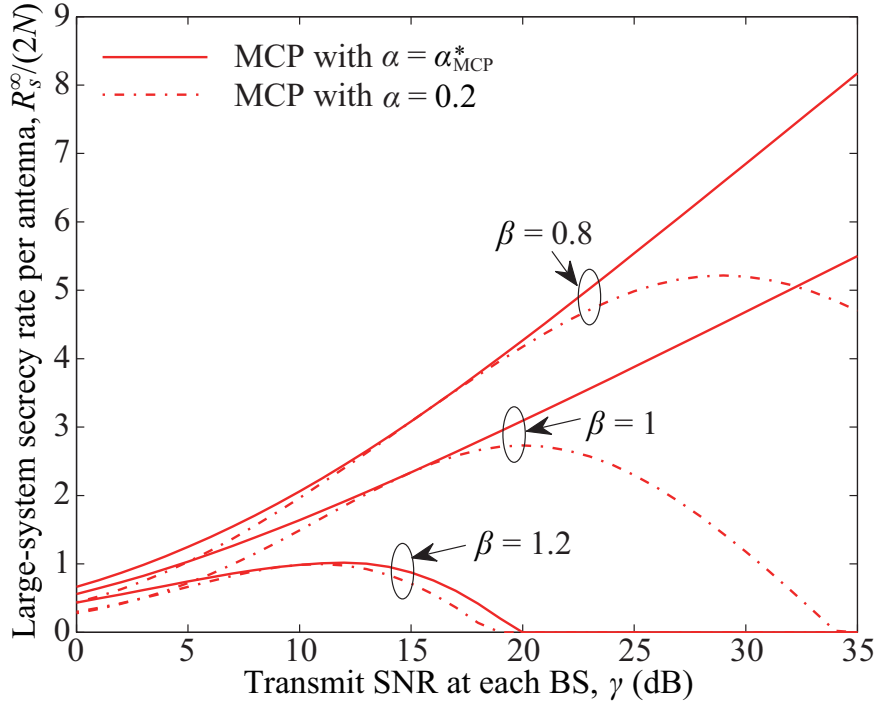


Figure 4.5: MCP: the large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $\beta = 0.8, 1, 1.2$, $N = 20$ and $\varepsilon = 0.5$.

to zero when γ is high. For the MCP, Figure 4.5 shows that the secrecy rate achieved by $\alpha = \alpha_{MCP}^*$ monotonically increases with γ if $\beta \leq 1$, but goes to zero at high transmit SNRs if $\beta > 1$. For the CBf, Figure 4.6 shows that the secrecy rate achieved by $\alpha = \alpha_{CBf}^*$ monotonically increases with γ if $\beta \leq 0.5$, but goes to zero at high transmit SNRs if $\beta > 0.5$. These observations reveal that the increase in γ benefits the secrecy performance achieved by the optimal α , when the network load is low. We now analytically explain these observations as follows. From the analytical results, we find that the optimal regularization parameter goes to zero as γ increases for both the MCP and the CBf. When $\alpha \rightarrow 0$, we find from (4.23) that $\lim_{\alpha \rightarrow 0} R_{s,MCP}^\infty$ monotonically increases with γ if $\beta \leq 1$, while $\lim_{\alpha \rightarrow 0} R_{s,MCP}^\infty$ approaches to zero at high transmit SNRs if $\beta > 1$. Similarly, it is found from (4.24) that $\lim_{\alpha \rightarrow 0} R_{s,CBf}^\infty$ monotonically increases with γ if $\beta \leq 0.5$, while $\lim_{\alpha \rightarrow 0} R_{s,CBf}^\infty$ goes to zero at high transmit SNRs if $\beta > 0.5$.

Finally, we demonstrate the advantage of the proposed precoders relative to the channel inversion precoder in the two-cell network. The channel inversion precoder (also called as zero-forcing precoder) is a well-known linear precoder that can eliminate the interference amongst users in the multi-user multi-input single-output (MISO) broadcasting network where the number of users is less than or equal to the number of transmit antennas at the BS, i.e., $\beta \leq 1$ for the MCP or $\beta \leq 0.5$ for the CBf. In addition, the well-known block-diagonalization (BD)

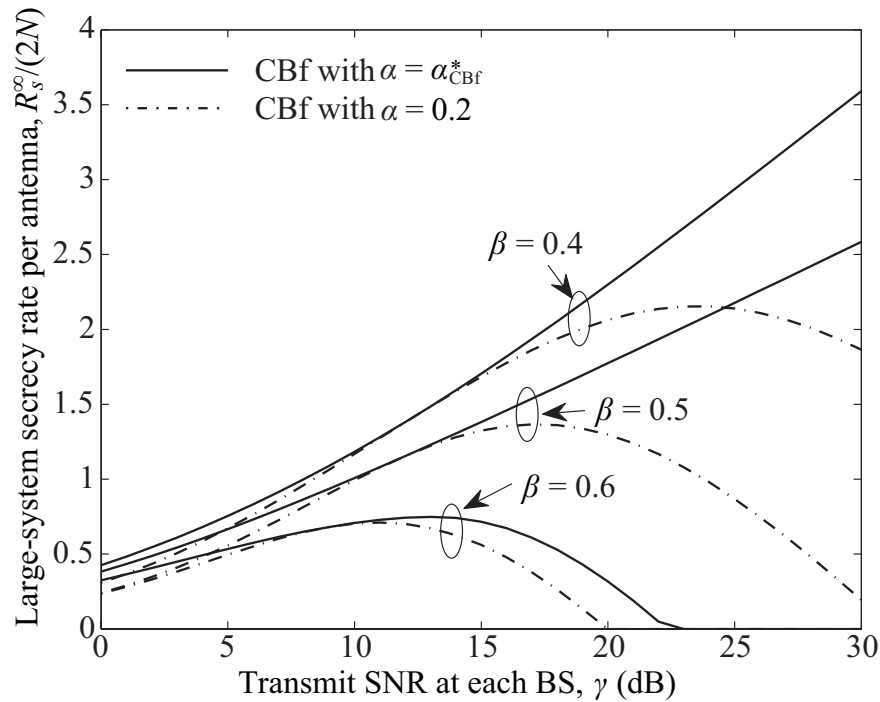


Figure 4.6: CBf: the large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $\beta = 0.4, 0.5, 0.6$, $N = 20$ and $\varepsilon = 0.5$.

precoder is a generalization of the channel inversion precoder to the scenario where multiple antennas are equipped at each user [86, 87, 88]. Figure 4.7 plots $R_s^\infty / (2N)$ versus γ for the proposed precoders and the channel inversion precoder. The proposed precoders include the RCI precoder with $\alpha = \alpha_{MCP}^*$ for the MCP and the generalized RCI precoder with $\alpha = \alpha_{CBf}^*$ for the CBf. For the MCP, the RCI precoder with $\alpha = 0$ reduces to the channel inversion precoder considered for comparison. For the CBf, the generalized RCI precoder with $\alpha = 0$ is considered for comparison, since the conventional channel inversion precoder cannot achieve confidential broadcasting in the CBf. Note that the regularized RCI with $\alpha = 0$ can eliminate the interference amongst users, which has the same effects as the channel inversion precoder in the single-cell network or the MCP. It is evident from the figure that the proposed precoders outperform the channel inversion precoder for both the MCP and the CBf. We find that the proposed precoders exhibit a profound performance gain over the channel inversion precoder in the regime of low transmit SNR. We also find that this performance gain decreases when the transmit SNR increases. This can be explained by the fact that the optimal regularization parameter approaches zero when the transmit SNR grows large. Besides, it is worth mentioning that the channel inversion precoder achieves confidential broadcasting only when the number of users is less than or equal to the number of transmit antennas at the BS, i.e., $\beta \leq 1$ for the MCP or $\beta \leq 0.5$ for the CBf. Differently, the proposed precoders can achieve confidential

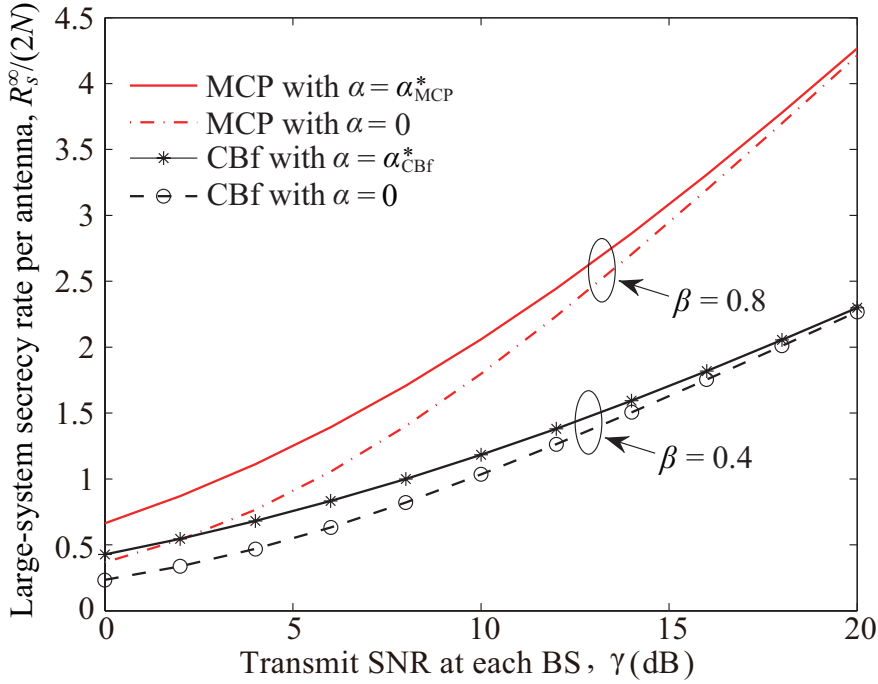


Figure 4.7: The large-system secrecy rate per antenna versus the average transmit SNR per BS for different designs of the regularization parameter with $N = 20$ and $\varepsilon = 0.5$.

broadcasting even if $\beta > 1$ for the MCP or $\beta > 0.5$ for the CBf.

4.4.2 Power-Reduction Strategy

We find from Figures 4.5 and 4.6 that the large-system secrecy sum rate achieved by the optimal regularization parameter, denoted by $R_s^{\infty*}$, does not monotonically increase with γ when the network load is high. Specifically, $R_s^{\infty*}$ decreases as γ increases at high transmit SNRs when $\beta > 1$ for the MCP or $\beta > 0.5$ for the CBf. Hence, we propose power-reduction strategies to compensate for the secrecy sum rate loss at high transmit SNRs for a high network load. We highlight that although the principle of the power reduction strategy in our work is similar to that in [43], the prominent challenge of designing our power reduction strategy is to determine the optimal transmit SNR that maximizes the secrecy sum rate using our newly derived expressions for the secrecy sum rate. As such, the design of the power reduction strategy in this chapter is different from that in [43]. To this end, we first obtain the optimal transmit SNR that maximizes the large-system secrecy sum rate for each of the MCP and the CBf.

4.4.2.1 Power Reduction for MCP

For the MCP, we focus on the network with $\beta > 1$, since $R_{s,\text{MCP}}^{\infty*}$ does not monotonically increase with γ when $\beta > 1$. We first derive the optimal transmit SNR, γ_{MCP}^* , that maximizes the large-system secrecy sum rate achieved by α_{MCP}^* , i.e., $\gamma_{\text{MCP}}^* = \arg \max_{\gamma} R_{s,\text{MCP}}^{\infty*}$. By taking the first-order derivative of $R_{s,\text{MCP}}^{\infty*}$ with respect to γ and equating it to zero, we obtain γ_{MCP}^* as

$$\gamma_{\text{MCP}}^* = \frac{\beta(2-\beta)}{(1+\varepsilon)(\beta-1)^2}. \quad (4.28)$$

Based on (4.28), we propose the power-reduction strategy to reduce the total transmit power such that the maximum large-system secrecy sum rate is maintained. The precoding vector with the power-reduction strategy is given by

$$\mathbf{w}_{\text{PR}} = \begin{cases} \sqrt{\frac{\gamma_{\text{MCP}}^*}{\gamma}} \mathbf{w}^* & \beta > 1 \text{ and } \gamma > \gamma_{\text{MCP}}^*, \\ \mathbf{w} & \text{otherwise,} \end{cases} \quad (4.29)$$

where \mathbf{w} is the original RCI precoding vector given in (4.5) with $\alpha = \alpha_{\text{MCP}}^*$ and \mathbf{w}^* is the original RCI precoding vector with $\alpha = \alpha_{\text{MCP}}^*$ at $\gamma = \gamma_{\text{MCP}}^*$. We highlight that $\sqrt{\gamma_{\text{MCP}}^*/\gamma}$ is the power-reduction coefficient for the MCP, which is adopted when $\beta > 1$ and $\gamma > \gamma_{\text{MCP}}^*$. As such, we refer to the RCI precoder using \mathbf{w}_{PR} in (4.29) as the RCI-PR precoder. Note that the reduced transmit SNR by adopting the RCI-PR precoder becomes

$$\gamma_{\text{MCP}}^{\text{PR}} = \begin{cases} \gamma_{\text{MCP}}^*, & \beta > 1 \text{ and } \gamma > \gamma_{\text{MCP}}^* \\ \gamma, & \text{otherwise.} \end{cases} \quad (4.30)$$

4.4.2.2 Power Reduction for CBf

For the CBf, we focus on the network with $\beta > 0.5$, since $R_{s,\text{CBf}}^{\infty*}$ does not monotonically increase with γ when $\beta > 0.5$. We first determine the optimal transmit SNR, γ_{CBf}^* , that maximizes the large-system secrecy sum rate achieved by α_{CBf}^* , i.e., $\gamma_{\text{CBf}}^* = \arg \max_{\gamma} R_{s,\text{CBf}}^{\infty*}$. Since the closed-form expression for γ_{CBf}^* cannot be derived, we obtain γ_{CBf}^* through numerical search. Using γ_{CBf}^* , we propose the power-reduction strategy to reduce the total transmit power and maintain the maximum large-system secrecy sum rate. The precoding vector with the power-reduction strategy is given by

$$\mathbf{w}_{\text{PR}} = \begin{cases} \sqrt{\frac{\gamma_{\text{CBf}}^*}{\gamma}} \mathbf{w}^* & \beta > 0.5 \text{ and } \gamma > \gamma_{\text{CBf}}^*, \\ \mathbf{w} & \text{otherwise,} \end{cases} \quad (4.31)$$

where \mathbf{w} is the original generalized RCI precoding vector given in (4.14) with $\alpha = \alpha_{\text{CBf}}^*$ and \mathbf{w}^* is the original generalized RCI precoding vector with $\alpha = \alpha_{\text{CBf}}^*$ at $\gamma = \gamma_{\text{CBf}}^*$. We highlight

that $\sqrt{\gamma_{\text{CBf}}^*/\gamma}$ is the power-reduction coefficient for the CBf, which is adopted when $\beta > 0.5$ and $\gamma > \gamma_{\text{CBf}}^*$. Therefore, we refer to the generalized RCI precoder using \mathbf{w}_{PR} in (4.31) as the generalized RCI-PR precoder. Notably, the reduced transmit SNR by adopting the generalized RCI-PR precoder becomes

$$\gamma_{\text{CBf}}^{\text{PR}} = \begin{cases} \gamma_{\text{CBf}}^*, & \beta > 0.5 \text{ and } \gamma > \gamma_{\text{CBf}}^* \\ \gamma, & \text{otherwise.} \end{cases} \quad (4.32)$$

4.4.2.3 Numerical Results

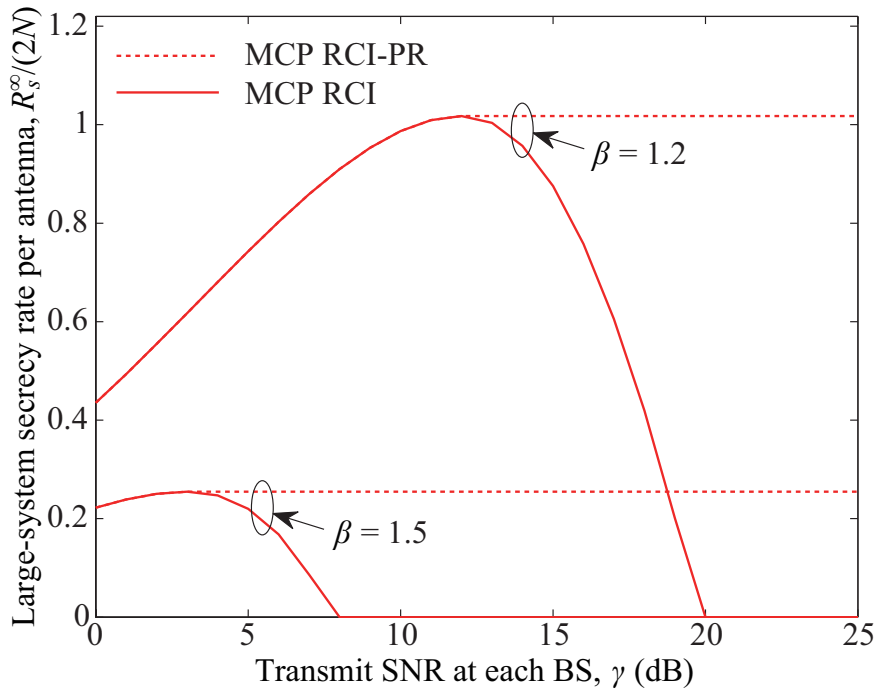


Figure 4.8: MCP: the large-system secrecy rate per antenna versus the average transmit SNR per BS for the transmissions with and without power-reduction strategy. The other system parameters are $\beta = 1.2, 1.5, N = 20$ and $\varepsilon = 0.5$.

Figures 4.8 and 4.9 demonstrate the performance improvement offered by the proposed power-reduction strategy for the MCP and the CBf, respectively. Figure 4.8 plots $R_s^\infty / (2N)$ versus γ for the MCP, where the curve of MCP RCI-PR is for the proposed power-reduction strategy and the curve of MCP RCI is for the RCI precoding with $\alpha = \alpha_{\text{MCP}}^*$. Figure 4.9 plots $R_s^\infty / (2N)$ versus γ for the CBf, where the curve of CBf Generalized RCI-PR is for the proposed power-reduction strategy and the curve of CBf Generalized RCI is for the generalized RCI precoding with $\alpha = \alpha_{\text{CBf}}^*$. We clarify that the actual transmit SNR of the RCI-PR precoder in Figure 4.8 is γ_{MCP}^* when $\gamma > \gamma_{\text{MCP}}^*$, as indicated by (4.30), and the actual transmit SNR of the generalized RCI-PR precoder in Figure 4.9 is γ_{CBf}^* when $\gamma > \gamma_{\text{CBf}}^*$, as indicated by (4.32). As

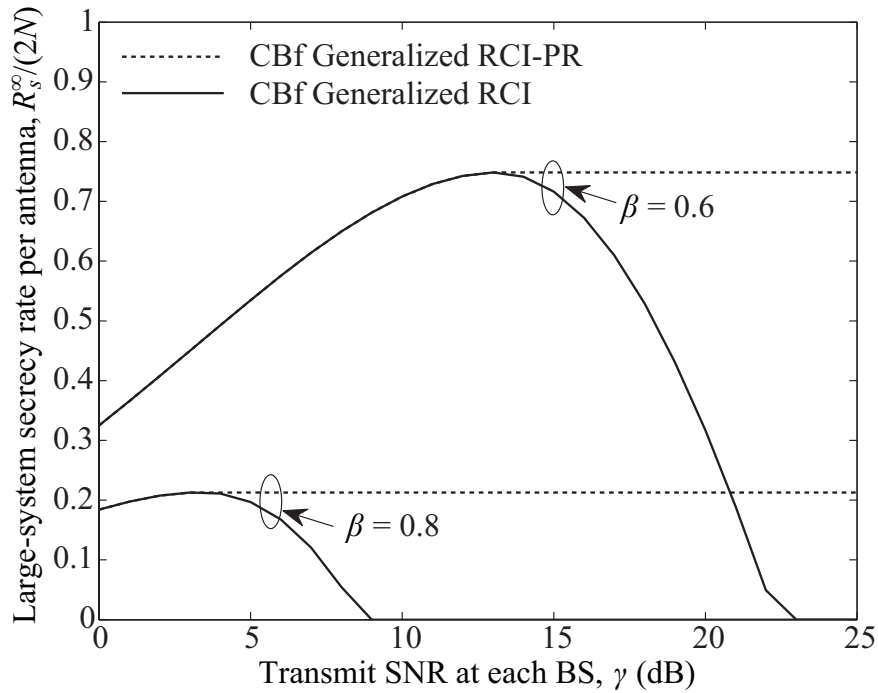


Figure 4.9: CBf: the large-system secrecy rate per antenna versus the average transmit SNR per BS for the transmissions with and without power-reduction strategy. The other system parameters are $\beta = 0.6, 0.8, N = 20$ and $\varepsilon = 0.5$.

shown in both figures, the proposed power-reduction strategies efficiently prevent the secrecy rate from decreasing at high transmit SNRs. Particularly, the power-reduction strategy allows the secrecy rate at high transmit SNRs to be equal to the maximum secrecy rate achieved at the optimal transmit SNR. It is worth nothing that the improvement in the secrecy rate at high transmit SNRs is achieved by using a lower transmit power compared with the transmission without the power-reduction strategy.

4.5 Summary

In this chapter, we designed the RCI precoder and the generalized RCI precoder for the MCP and the CBf, respectively, to achieve confidential broadcasting in a two-cell broadcast network. For each form of BS cooperation, we derived accurate large-system expressions for the secrecy sum rate achieved by the linear precoder. Based on these expressions, we determined α_{MCP}^* and α_{CBf}^* which are the optimal regularization parameters maximizing the large-system secrecy sum rate for the MCP and the CBf, respectively. Furthermore, we proposed the RCI-PR precoder for the MCP and the generalized RCI-PR precoder for the CBf, which can significantly increase the secrecy sum rate at high transmit SNRs by power-reduction strategies. Using numerical results, we demonstrated the accuracy of our large-system expressions, the optimality

of α_{MCP}^* and α_{CBf}^* , and the secrecy sum rate improvement provided by the RCI-PR and the generalized RCI-PR precoders. Notably, our analytical and numerical results allow us to examine the impact of the cross-cell interference level on the secrecy sum rate.

New Secrecy Metrics for Wireless Transmission over Fading Channels

5.1 Introduction

In Chapter 4, we improved the applicability of confidential broadcasting by taking into account the effects of multi-cell networks. As mentioned earlier in Section 1.2.2, there exists a fundamental reason that limits the applicability of physical layer security for systems with practical secrecy requirements. That is, the current definition of secrecy outage probability has two major limitations in evaluating the secrecy performance of wireless systems: a) the secrecy outage probability does not give any insight into the eavesdropper's decodability of confidential messages; b) the amount of information leakage to the eavesdropper cannot be characterized.

Motivated by the limitations of the secrecy outage probability, we propose new secrecy metrics for wireless transmissions focusing on quasi-static fading channels in this chapter. Different from the secrecy outage probability based on the concept of perfect secrecy, our proposed secrecy metrics are based on another regime of interest in physical layer security, namely the partial secrecy regime. The partial secrecy of a system is often investigated by the equivocation reflecting the level at which the eavesdropper is confused. The exploration on equivocation can be found as early as Wyner's pioneering work for the wiretap channel [13]. Similarly, Csiszár and Körner [89] used the normalized equivocation to quantify the partial secrecy for the broadcast channel with confidential information. Importantly, the equivocation is closely related to the decoding error probability [13, 90, 91]. Therefore, evaluating the secrecy performance on the basis of equivocation can reflect the decodability of confidential messages at the eavesdropper.

It is worth mentioning that the work in this chapter is solely motivated by the limitations of the current secrecy outage probability from a more practical point of view. Our proposed new secrecy metrics based on the concept of partial secrecy do not imply that the secrecy metrics based on the perfect secrecy is inappropriate from the information-theoretic perspective.

We acknowledge the importance of requiring perfect secrecy for the research on information-theoretic security. Meanwhile, we notice the large gap between the requirement of information-theoretic security and the condition of practical secrecy. We hope that the newly proposed secrecy metrics can make contributions to bridge the gap between theory and practice in physical layer security.

The remainder of the chapter is organized as follows. Section 5.2 gives the preliminary on perfect secrecy and partial secrecy. Section 5.3 introduces the three new secrecy metrics for wireless transmissions over fading channels. Section 5.4 illustrates the use of newly proposed secrecy metrics by evaluating the secrecy performance of an example wireless system with non-adaptive rate wiretap codes. Section 5.5 demonstrates the impact of new secrecy metrics on the system design. Finally, Section 5.6 summarizes the chapter.

5.2 Perfect Secrecy and Partial Secrecy

Recall the basic wiretap-channel system as shown in Figure 5.1. A transmitter, Alice, sends confidential information, M , to an intended receiver, Bob, in the presence of an eavesdropper, Eve. The source is stationary and ergodic. The confidential information, M , is encoded into a n -vector X^n . The received vectors at Bob and Eve are denoted by Y^n and Z^n , respectively. The entropy of the source information and the residual uncertainty for the message at the eavesdropper are denoted by $H(M)$ and $H(M | Z^n)$, respectively.

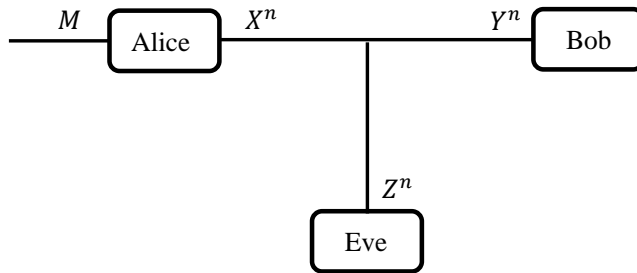


Figure 5.1: Basic wiretap-channel system.

5.2.1 Perfect Secrecy

Perfect secrecy means that the amount of information leakage to the eavesdropper vanishes, and guarantees that the eavesdropper's optimal attack is to guess the message at random. From Shannon's definition, perfect secrecy requires

$$H(M | Z^n) = H(M) \quad \text{or, equivalently,} \quad I(M; Z^n) = 0. \quad (5.1)$$

The requirement of no information leakage to Eve in fact is equivalent to guaranteeing the highest possible decoding error probability at Eve. As explained in [9, Remark 3.1], consider that messages are uniformly taken from a size K set $[1, 2, \dots, K]$, and Eve minimizes her decoding error probability P_e by performing maximum-likelihood decoding. The condition of no information leakage ensures that Eve can only guess the original message, and the probability of error under maximum-likelihood decoding is $P_e = \frac{K-1}{K}$. Therefore, from the decodability point of view, perfect secrecy is equivalent to guaranteeing $P_e \geq \frac{K-1}{K}$. Furthermore, when the entropy of the message is very large that $K \rightarrow \infty$, perfect secrecy actually guarantees that P_e asymptotically goes to 1,

$$\lim_{K \rightarrow \infty} P_e \geq \lim_{K \rightarrow \infty} \frac{K-1}{K} = 1. \quad (5.2)$$

In practice, the secrecy requirement on the decodability of messages at Eve can be generally written as $P_e \geq \vartheta$ for some ϑ . Depending on the applications, the value of ϑ ranges from 0 to 1, which falls outside the perfect secrecy regime.

5.2.2 Partial Secrecy

The partial secrecy is often investigated by the equivocation that indicates the level at which Eve is confused. We specifically consider the fractional equivocation, which is defined as [15]

$$\Delta = \frac{H(M | Z^n)}{H(M)}. \quad (5.3)$$

Note that evaluating security on the basis of equivocation is related to the conventional requirement on the decodability of messages at Eve [13]. Although there is no one-to-one relation between the equivocation and the error probability, the tight lower and upper bounds of the decoding error probability can be derived from the equivocation [90, 91].

When studying secrecy, we particularly want to ensure that the decoding error probability at eavesdropper is larger than a certain level. Thus, it is desirable to have the decoding error probability at Eve lower bounded by the equivocation. Still consider the general case where messages are uniformly taken from a size K set $[1, 2, \dots, K]$, which achieves the maximal entropy over an alphabet of size K . Then, the entropy of the message is given by $H(M) = \log_2(K)$. From Fano's inequality [90, Chapter 2.10], we have

$$H(M | Z^n) \leq h(P_e) + P_e \log_2(K), \quad (5.4)$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$, $0 \leq x \leq 1$. This inequality can be weakened to

$$P_e \geq \frac{H(M | Z^n) - 1}{\log_2(K)} = \Delta - \frac{1}{\log_2(K)}. \quad (5.5)$$

When the entropy of the message is very large that $K \rightarrow \infty$, we can further derive (5.5) as

$$\lim_{K \rightarrow \infty} P_e \geq \Delta - \lim_{K \rightarrow \infty} \frac{1}{\log_2(K)} = \Delta. \quad (5.6)$$

Thus, P_e is asymptotically lower bounded by Δ .

5.3 New Secrecy Metrics for Wireless Transmissions

Still consider the basic wiretap-channel system. We now assume that the messages are transmitted over quasi-static fading channels. Bob and Eve perfectly know their own CSI. Eve's instantaneous CSI is not available at the legitimate side. For wireless transmissions in such a system, perfect secrecy is not always achievable, and the secrecy outage probability is commonly used to measure the secrecy performance. From the perfect secrecy perspective, the current definition of secrecy outage probability treats the failure of achieving *perfect secrecy* as the case of secrecy outage. Thus, the secrecy outage probability is applicable only for the system which has an extremely stringent requirement on Eve's decoding error probability, $\vartheta \rightarrow 1$, but cannot handle the general requirement on Eve's decoding error probability, $0 < \vartheta \leq 1$. In addition, the outage-based secrecy metric cannot evaluate how fast or how much the confidential information is leaked to Eve.

Different from the current secrecy outage probability, we study the secrecy performance of wireless communications from the partial secrecy perspective. For wireless transmissions over fading channels, the fractional equivocation, Δ , is a random variable due to the fading properties of the channel. Thus, we start from the derivation of Δ for a given fading realization. The distribution of Δ can be obtained according to the distribution of channel gains. After that, three new secrecy metrics are proposed based on the distribution of Δ .

5.3.1 Fractional Equivocation for a Given Fading Realization

A given fading realization of the wireless channel is equivalent to the (non-degraded) Gaussian wiretap channel[92]. The value of the fractional equivocation for the Gaussian wiretap channel actually depends on the coding and transmission strategies, and there is no such a general expression applicable for all scenarios. However, an upper bound on Δ can be easily derived following closely from [15, Theorem 1] and [92, Corollary 2]. The maximum achievable fractional equivocation for a given fading realization of the wireless channel is given by

$$\Delta \leq \begin{cases} 1, & \text{if } C_e \leq C_b - R \\ (C_b - C_e)/R, & \text{if } C_b - R < C_e < C_b \\ 0, & \text{if } C_b \leq C_e, \end{cases} \quad (5.7)$$

where C_b and C_e denote Bob and Eve's channel capacities, respectively, $R = \frac{H(M)}{n}$ denotes the secrecy rate for transmission.

5.3.2 New Secrecy Metrics

From (5.7), we note that the value of Δ for a given fading realization is determined by the instantaneous channel gains and the transmission rate. Taking into account the fading properties of wireless channels, we can derive the distribution of Δ according to the distribution of the channel gains and the transmission rate. Then, we investigate the distribution of Δ from three aspects to propose three secrecy metrics.

5.3.2.1 Generalized Secrecy Outage Probability

Extending the current definition of secrecy outage probability, we propose a generalized definition of secrecy outage probability, given by

$$p_{\text{out}} = \mathbb{P}(\Delta < \theta), \quad (5.8)$$

where $\mathbb{P}(\cdot)$ denotes the probability measure and $0 < \theta \leq 1$ denotes the minimum acceptable value of the fractional equivocation.

Since the fractional equivocation is related to the decoding error probability, the generalized secrecy outage probability is applicable for systems with different levels of secrecy requirements in terms of Eve's decodability of confidential messages (by choosing different values of θ). The current secrecy outage probability is defined as $\mathbb{P}(\Delta < 1)$, and hence is a special case of the newly proposed secrecy outage probability (by setting $\theta = 1$). In the rest of the chapter, we refer to perfect secrecy outage probability as the current definition of secrecy outage probability.

Apart from the discussion above, another way to understand the generalized secrecy outage probability can be described as follows. From (5.3), the information leakage ratio to Eve can be written as $\frac{I(M; Z^n)}{H(M)} = 1 - \Delta$. The information leakage ratio tells the percentage of transmitted confidential information leaked to the eavesdropper. Then, the generalized secrecy outage probability, $p_{\text{out}} = \mathbb{P}(\Delta < \theta) = \mathbb{P}(1 - \Delta > 1 - \theta)$, actually characterizes the probability that the information leakage ratio is larger than a certain value, $1 - \theta$.

5.3.2.2 Average Fractional Equivocation

Taking average of the fractional equivocation from its distribution, we can derive the (long-term) average value of the fractional equivocation, given by

$$\bar{\Delta} = \mathbb{E}\{\Delta\}, \quad (5.9)$$

where $\mathbb{E}\{\cdot\}$ denotes the expectation operation. As discussed earlier in (5.6), Eve's decoding error probability for a given fading realization is asymptotically lower bounded by the fractional equivocation. Thus, the average fractional equivocation, $\bar{\Delta}$, actually gives an asymptotic lower bound on the overall decoding error probability at Eve, i.e., $P_e \geq \bar{\Delta}$.

5.3.2.3 Average Information Leakage Rate

With the knowledge of message transmission rate $R = \frac{H(M)}{n}$, we can further derive the average information leakage rate, given by

$$\begin{aligned} R_L &= \mathbb{E} \left\{ \frac{I(M; Z^n)}{n} \right\} \\ &= \mathbb{E} \left\{ \frac{I(M; Z^n)}{H(M)} \cdot \frac{H(M)}{n} \right\} \\ &= \mathbb{E} \{ (1 - \Delta) R \}. \end{aligned} \quad (5.10)$$

The average information leakage rate tells how fast the information is leaked to the eavesdropper. Note that the transmission rate R cannot be simply taken out of the expectation in (5.10), since R can be a variable parameter (e.g., adaptive rate transmission) and its distribution may be correlated with the distribution of Δ . However, when the non-adaptive rate transmission scheme is adopted, (5.10) can be simplified as

$$R_L = \mathbb{E} \{ (1 - \Delta) R \} = (1 - \bar{\Delta}) R. \quad (5.11)$$

Remark 5.1. The proposed secrecy metrics in this section, i.e., (5.8), (5.9) and (5.10), are general and can be applied to evaluate the performance of any coding and transmission strategy in any system model (e.g., signal-antenna or multi-antenna systems). A specific scenario is studied as an example in the next section, wherein the expressions for the proposed secrecy metrics are further derived in terms of transmission rates and channel statistics.

5.4 Wireless Transmissions with Non-Adaptive Rate Wiretap Codes: An Example

5.4.1 System Model

We consider the system where a transmitter, Alice, wants to send confidential information to an intended receiver, Bob, in the presence of an eavesdropper, Eve, over quasi-static Rayleigh fading channels. Alice, Bob and Eve are assumed to have a single antenna each. The instant-

neous channel capacities at Bob and Eve are given by

$$C_b = \log_2(1 + \gamma_b) \quad (5.12)$$

and

$$C_e = \log_2(1 + \gamma_e), \quad (5.13)$$

respectively, where γ_b and γ_e denote the instantaneous received SNRs at Bob and Eve, respectively. The instantaneous received SNRs at Bob and Eve have exponential distributions, given by

$$f_{\gamma_b}(\gamma_b) = \frac{1}{\bar{\gamma}_b} \exp\left(-\frac{\gamma_b}{\bar{\gamma}_b}\right) \quad (5.14)$$

and

$$f_{\gamma_e}(\gamma_e) = \frac{1}{\bar{\gamma}_e} \exp\left(-\frac{\gamma_e}{\bar{\gamma}_e}\right), \quad (5.15)$$

respectively, where $\bar{\gamma}_b$ and $\bar{\gamma}_e$ denote the average received SNRs at Bob and Eve, respectively.

We consider the widely-adopted wiretap code [13] as introduced in Section 1.1.1 for the message transmissions. The two rate parameters are the codeword transmission rate, R_b , and the confidential information rate, R_s . We further consider the non-adaptive rate transmission, where the transmission rates, i.e., R_b and R_s , are fixed over time.

Bob and Eve perfectly know their own channels. Hence, C_b and C_e are known at Bob and Eve, respectively. Alice has the statistical knowledge on Bob and Eve's channels, but does not know either Bob or Eve's instantaneous CSI. We further assume that Bob provides a one-bit feedback about his channel quality to Alice in order to avoid unnecessary transmissions [19, 93]. The one-bit feedback enables an on-off transmission scheme to guarantee that the transmission takes place only when $R_b \leq C_b$. In addition, the on-off transmission scheme incurs a probability of transmission, given by

$$\begin{aligned} p_{\text{tx}} &= \mathbb{P}(R_b \leq C_b) \\ &= \mathbb{P}(R_b \leq \log_2(1 + \gamma_b)) \\ &= \exp\left(-\frac{2^{R_b} - 1}{\bar{\gamma}_b}\right). \end{aligned} \quad (5.16)$$

5.4.2 Secrecy Performance Evaluation

To characterize the secrecy performance of wireless transmissions over the fading channel, we start from the investigation on a given fading realization of the channel.

Proposition 5.1. For a given fading realization of the wireless channel, the achievable frac-

tional equivocation for the wiretap code of $R_b \leq C_b$ and $R_s \leq R_b$ is given by

$$\Delta = \begin{cases} 1, & \text{if } C_e \leq R_b - R_s \\ (R_b - C_e)/R_s, & \text{if } R_b - R_s < C_e < R_b \\ 0, & \text{if } R_b \leq C_e. \end{cases} \quad (5.17)$$

Proof: The proof follows closely from [92, Corollary 2] and the steps in [15, Section III] while having $\frac{H(X^n)}{n} = R_b$. ■

From (5.13), we can further derive (5.17) as

$$\Delta = \begin{cases} 1, & \text{if } \gamma_e \leq 2^{R_b - R_s} - 1 \\ \frac{R_b - \log_2(1 + \gamma_e)}{R_s}, & \text{if } 2^{R_b - R_s} - 1 < \gamma_e < 2^{R_b} - 1 \\ 0, & \text{if } 2^{R_b} - 1 \leq \gamma_e. \end{cases} \quad (5.18)$$

Now, we are ready to evaluate the secrecy performance of wireless transmissions over fading channels from the distribution of Δ , which can be derived according to the distribution of γ_e given in (5.15).

5.4.2.1 Generalized Secrecy Outage Probability

The generalized secrecy outage probability is given by

$$\begin{aligned} p_{\text{out}} &= \mathbb{P}(\Delta < \theta) \\ &= \mathbb{P}(2^{R_b} - 1 \leq \gamma_e) + \mathbb{P}(2^{R_b - R_s} - 1 < \gamma_e < 2^{R_b} - 1) \\ &\quad \cdot \mathbb{P}\left(\frac{R_b - \log_2(1 + \gamma_e)}{R_s} < \theta \mid 2^{R_b - R_s} - 1 < \gamma_e < 2^{R_b} - 1\right) \\ &= \exp\left(-\frac{2^{R_b - \theta R_s} - 1}{\bar{\gamma}_e}\right), \end{aligned} \quad (5.19)$$

where $0 < \theta \leq 1$.

For the extreme case of $\theta = 1$, we have

$$p_{\text{out}}(\theta = 1) = \exp\left(-\frac{2^{R_b - R_s} - 1}{\bar{\gamma}_e}\right). \quad (5.20)$$

We note that (5.20) is exactly the same as [19, Eq. (8)], which gives the perfect secrecy outage probability of wireless transmissions with non-adaptive rate wiretap codes.

5.4.2.2 Average Fractional Equivocation

The average fractional equivocation is given by

$$\begin{aligned}
 \bar{\Delta} &= \mathbb{E}\{\Delta\} \\
 &= \int_0^{2^{R_b-R_s}-1} f_{\gamma_e}(\gamma_e) d\gamma_e + \int_{2^{R_b-R_s}-1}^{2^{R_b}-1} \left(\frac{R_b - \log_2(1 + \gamma_e)}{R_s} \right) f_{\gamma_e}(\gamma_e) d\gamma_e \\
 &= 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right) \right), \tag{5.21}
 \end{aligned}$$

where $\text{Ei}(x) = \int_{-\infty}^x e^t/t dt$ denotes the exponential integral function. As mentioned before, the average fractional equivocation actually gives an asymptotic lower bound on eavesdropper's decoding error probability.

5.4.2.3 Average Information Leakage Rate

Since the non-adaptive rate transmission scheme is adopted, the average information leakage rate can be derived from (5.11), given by

$$\begin{aligned}
 R_L &= (1 - \bar{\Delta})R_s \\
 &= \frac{1}{\ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right) \right), \tag{5.22}
 \end{aligned}$$

which captures how fast on average the information is leaked to Eve. Note that the derivation of R_L in (5.22) is without the probability of transmission p_{tx} , which indicates that R_L actually characterizes how fast on average that the information is leaked to the eavesdropper when message transmission happens.

5.4.3 Numerical Results

We first compare the generalized secrecy outage probabilities subject to different requirements on the fractional equivocation. Figure 5.2 plots p_{out} versus R_s with different values of θ . Note that $\theta = 1$ represents the case of requiring perfect secrecy. As shown in the figure, for different levels of secrecy requirements in terms of the fractional equivocation or the decodability of messages at Eve, the transmission has different secrecy outage performances. We find that the difference in the generalized secrecy outage probabilities increases as the confidential information rate increases.

We then present an example to illustrate that the generalized secrecy outage probability sometimes reveal more information about the secrecy performance of wireless transmissions compared with the perfect secrecy outage probability. Figure 5.3 plots p_{out} versus $\bar{\gamma}_e$. The perfect secrecy outage probability ($\theta = 1$) and the newly proposed generalized secrecy outage

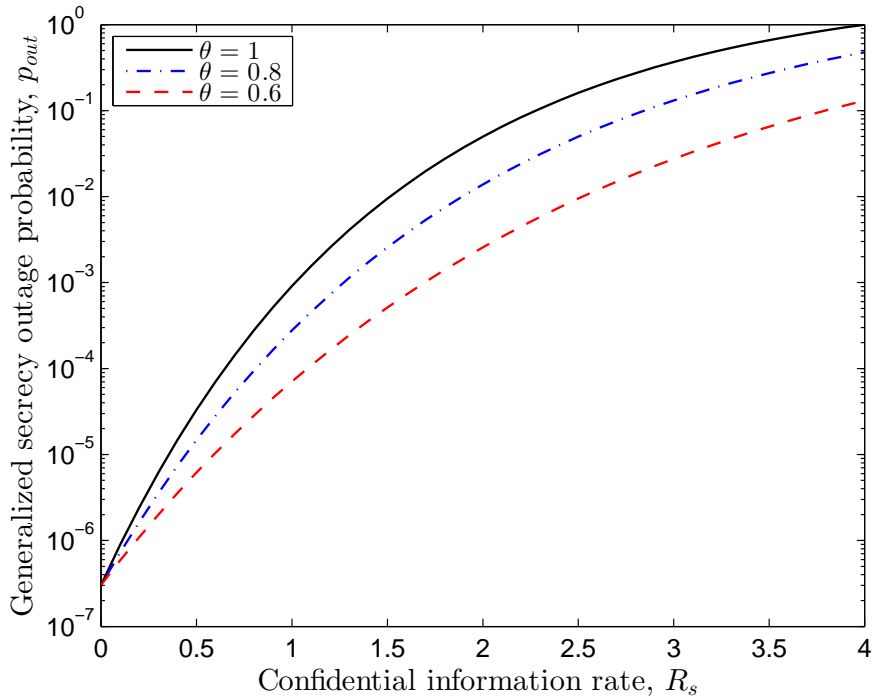


Figure 5.2: Generalized secrecy outage probability versus confidential information rate. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $R_b = 4$ and $\tilde{\gamma}_e = 1$.

probability with $\theta = 0.8$ are compared. We consider an extreme case that the confidential information rate is set to be the same as the total codeword rate, $R_b = R_s$. This is equivalent to using an ordinary code instead of the wiretap code for transmission. As shown in the figure, the secrecy performance measured by the perfect secrecy outage probability is not related to Eve's channel condition, since the perfect secrecy outage probability is always equal to 1. However, we know that the decodability of messages at the receiver is related to the channel condition. Intuitively, with the increase of average received SNR at Eve, the probability of error at Eve should decrease, and the secrecy performance should become worse. Therefore, we see that the secrecy performance of wireless transmissions cannot always be properly characterized by the perfect secrecy outage probability. In contrast, the generalized secrecy outage probability ($\theta = 0.8$) increases with the improvement of Eve's channel condition, which properly captures the change of secrecy performance. By this specific example of the transmission with an ordinary code, we show that the generalized secrecy outage probability is able to reveal some information about the secrecy performance of wireless transmissions that cannot be captured by the perfect secrecy outage probability.

Now, we present the secrecy performance of wireless transmissions measured by the aver-

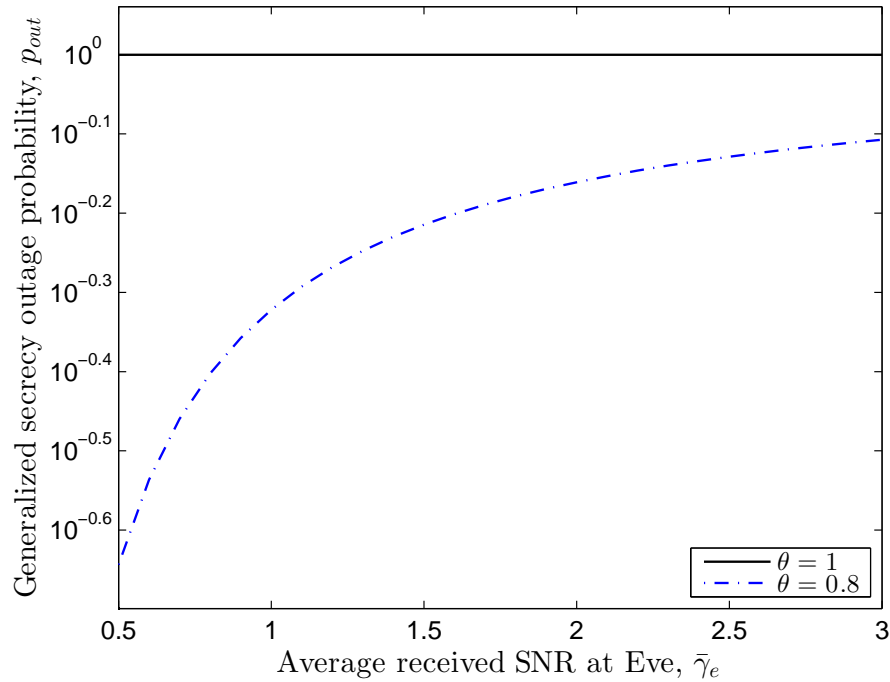


Figure 5.3: Generalized secrecy outage probability versus average received SNR at Eve. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8$. The other parameters are $R_b = R_s = 4$.

age fractional equivocation, which gives an asymptotic lower bound on Eve's decoding error probability. Figure 5.4 plots $\bar{\Delta}$ versus R_s . As shown in the figure, the average fractional equivocation decreases as the confidential information rate increases and/or the average received SNR at Eve increases. Besides, we note that even when an ordinary code is used instead of the wiretap code, i.e., $R_b = R_s = 4$, Eve still suffers from a relatively high decoding error probability, e.g., $P_e > 0.78$ for $\bar{\gamma}_e = 1$. This observation indicates that the wireless channel itself can provide a certain level of secrecy for the transmission.

Finally, we illustrate the secrecy performance of wireless transmissions measured by the average information leakage rate. Figure 5.5 plots R_L versus R_s . As the figure shows, the average information leakage rate increases as the confidential information rate increases and/or the average received SNR at Eve increases. We note that R_L does not reach R_s even when R_s goes to $R_b = 4$. This implies that the information is not all leaked to the eavesdropper even when we use an ordinary code instead of the wiretap code for transmission. This observation once again confirms that the wireless channel itself can provide a certain level of secrecy for the transmission.

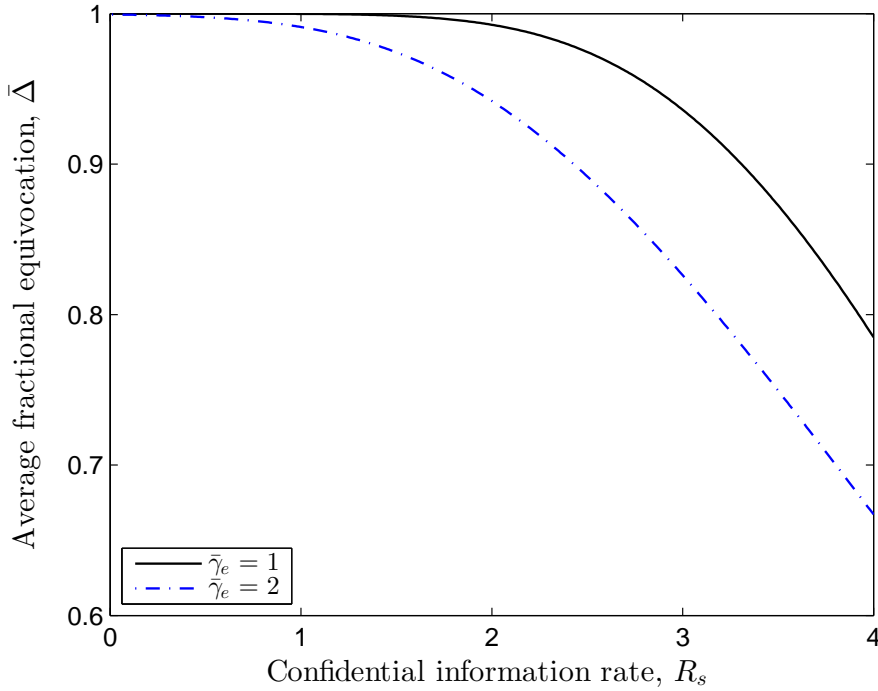


Figure 5.4: Average fractional equivocation (asymptotic lower bound on the decoding error probability at Eve) versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\tilde{\gamma}_e = 1, 2$. The other parameter is $R_b = 4$.

5.5 Impact on System Designs

In this section, we examine the significance of the newly proposed secrecy metrics from the perspective of a system designer, by checking the answers to the following questions:

- Q1) Do the newly proposed secrecy metrics lead to very different optimal design parameters that optimize the secrecy performance of the system, compared with the optimal design parameters minimizing the perfect secrecy outage probability?
- Q2) Does applying the optimal transmission design based on the perfect secrecy outage probability result in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper or a low information leakage rate?

If the answers to both questions are yes, we can confirm that the existing transmission designs based on the perfect secrecy outage probability are inappropriate for actual systems requiring a low decodability at the eavesdropper or a low information leakage rate. This further implies that the newly proposed secrecy metrics have their own significance for the system designers, since the new secrecy metrics enable appropriate transmission designs for systems with different secrecy requirements.

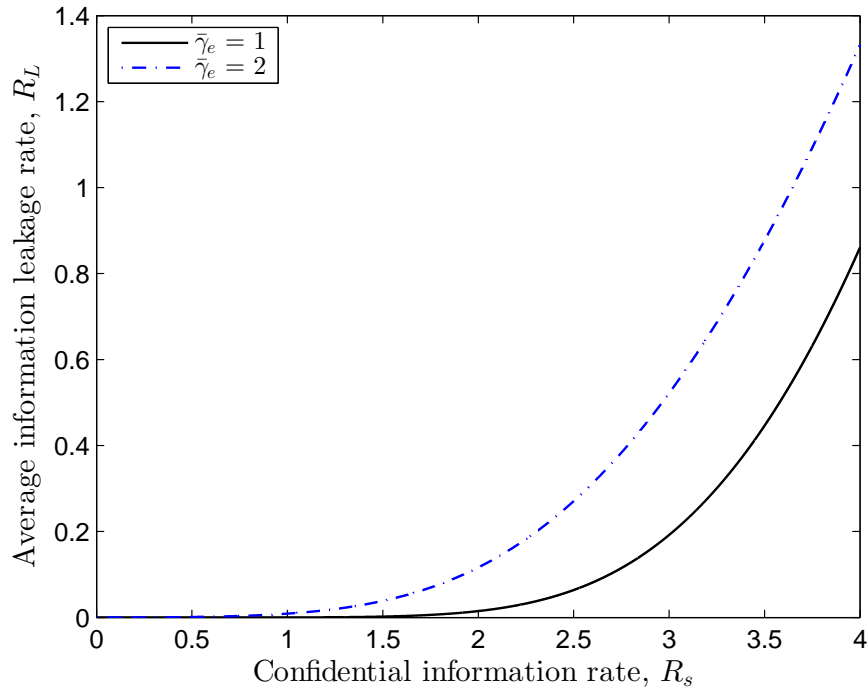


Figure 5.5: Average information leakage rate versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma}_e = 1, 2$. The other parameter is $R_b = 4$.

5.5.1 Problem Formulation

We still consider the system with non-adaptive rate wiretap codes described in the previous section. We optimize the secrecy performance of the wireless system subject to a throughput constraint $\eta > \Gamma$, where η denotes the throughput of confidential message transmission and Γ denotes its minimum required value. The controllable parameters to design are the wiretap code rates R_b and R_s . Taking into account the probability of transmission given in (5.16), the throughput of confidential message transmission is given by

$$\eta = p_{\text{tx}} R_s = \exp\left(-\frac{2^{R_b} - 1}{\bar{\gamma}_b}\right) R_s. \quad (5.23)$$

We specifically formulate three problems for the systems with different secrecy metrics, which are given as follows:

Problem 1: Minimize the generalized secrecy outage probability

$$\min_{R_b, R_s} p_{\text{out}} = \exp\left(-\frac{2^{R_b - \theta R_s} - 1}{\bar{\gamma}_e}\right), \quad (5.24)$$

$$\text{s.t.} \quad \eta \geq \Gamma, R_b \geq R_s > 0. \quad (5.25)$$

Problem 2: Maximize the average fractional equivocation

$$\max_{R_b, R_s} \quad \bar{\Delta} = 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right) \right), \quad (5.26)$$

$$\text{s.t.} \quad \eta \geq \Gamma, R_b \geq R_s > 0. \quad (5.27)$$

Problem 3: Minimize the average information leakage rate

$$\min_{R_b, R_s} \quad R_L = \frac{1}{\ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right) \right), \quad (5.28)$$

$$\text{s.t.} \quad \eta \geq \Gamma, R_b \geq R_s > 0. \quad (5.29)$$

5.5.2 Feasibility of the Constraint

The required throughput constraint is not feasible when Γ is larger than the maximum achievable throughput for $R_b \geq R_s > 0$. We find that the three problems have the same feasible constraint region, which is given by the following proposition.

Proposition 5.2. The feasible range of the throughput constraint is given by

$$0 \leq \Gamma \leq \frac{W_0(\bar{\gamma}_b)}{\ln 2} \exp\left(-\frac{2^{\frac{W_0(\bar{\gamma}_b)}{\ln 2}} - 1}{\bar{\gamma}_b}\right), \quad (5.30)$$

where $W_0(\cdot)$ denotes the principal branch of the Lambert W function.

Proof: See Appendix D.1. ■

5.5.3 Optimal Rate Parameters

We denote $R_{s,\min}$ and $R_{s,\max}$ as the solutions of x to $\exp\left(-\frac{2^x-1}{\bar{\gamma}_b}\right)x = \Gamma$ with $R_{s,\min} < R_{s,\max}$. The optimal solutions to Problems 1, 2 and 3 are summarized in Propositions 5.3, 5.4 and 5.5, respectively, as follows.

Proposition 5.3. The optimal rate parameters minimizing the generalized secrecy outage probability are given as follows:

$$R_{b1}^* = \log_2 \left(1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_{s1}^*} \right) \quad (5.31)$$

and

$$R_{s1}^* = \begin{cases} R_{s,\min}, & \text{if } R_{s,\min} > R_{so} \\ R_{so}, & \text{if } R_{s,\min} \leq R_{so} \leq R_{s,\max} \\ R_{s,\max}, & \text{if } R_{s,\max} < R_{so}, \end{cases} \quad (5.32)$$

where R_{s0} is the solution of x to

$$\theta = \frac{\bar{\gamma}_b}{x \ln(2) (\bar{\gamma}_b \ln(1 - \frac{\Gamma}{x}))}. \quad (5.33)$$

Proof: See Appendix D.2. ■

Proposition 5.4. The optimal rate parameters maximizing the average fractional equivocation are given as follows:

$$R_{b2}^* = \log_2 \left(1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_{s2}^*} \right) \quad (5.34)$$

and R_{s2}^* is obtained by numerically solving the problem given as

$$\min_x \frac{1}{x} \left(\text{Ei} \left(-\frac{1 - \bar{\gamma}_b \ln \frac{\Gamma}{x}}{\bar{\gamma}_e} \right) - \text{Ei} \left(-\frac{1 - \bar{\gamma}_b \ln \frac{\Gamma}{x}}{\bar{\gamma}_e 2^x} \right) \right), \quad (5.35)$$

$$\text{s.t.} \quad R_{s,\min} \leq x \leq R_{s,\max}. \quad (5.36)$$

Proof: See Appendix D.3. ■

Proposition 5.5. The optimal rate parameters minimizing the average information leakage rate are given as follows:

$$R_{b3}^* = \log_2 \left(1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_{s3}^*} \right) \quad (5.37)$$

and R_{s3}^* is obtained by numerically solving the problem given as

$$\min_x \text{Ei} \left(-\frac{1 - \bar{\gamma}_b \ln \frac{\Gamma}{x}}{\bar{\gamma}_e} \right) - \text{Ei} \left(-\frac{1 - \bar{\gamma}_b \ln \frac{\Gamma}{x}}{\bar{\gamma}_e 2^x} \right), \quad (5.38)$$

$$\text{s.t.} \quad R_{s,\min} \leq x \leq R_{s,\max}. \quad (5.39)$$

Proof: The proof follows closely from the proof of Proposition 5.4, i.e., Appendix D.3. ■

Remark 5.2. The numerical optimization problems for obtaining R_{s2}^* and R_{s3}^* in Propositions 5.4 and 5.5 can be easily solved by either the simple brute-force search or techniques like the golden section search [94].

5.5.4 Numerical Results

In this subsection, we present the numerical results for the wireless system with $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB to demonstrate the impact of new secrecy metrics on the transmission designs. The feasible range of the throughput constrain is $0 \leq \Gamma \leq 1.569$, which is obtained by Proposition 5.2.

We first compare the optimal transmission rates that optimize the secrecy performance of the system measured by different secrecy metrics. Figure 5.6 plots the optimal confidential

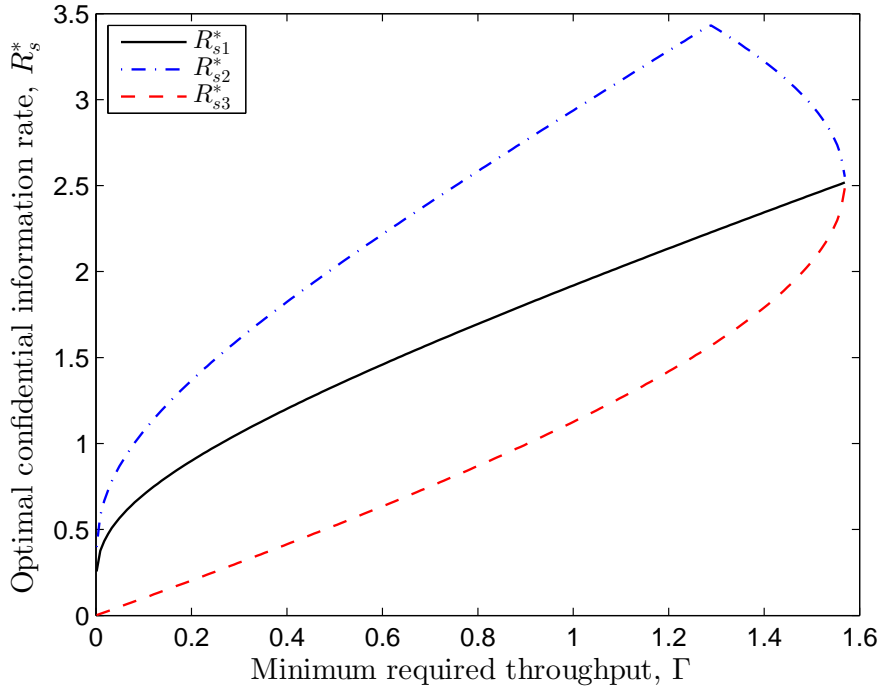


Figure 5.6: For different secrecy metrics: optimal confidential information rate versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.

information rate R_s^* versus the throughput constraint Γ . The values of R_{s1}^* , R_{s2}^* and R_{s3}^* are obtained by Propositions 5.3, 5.4 and 5.5, respectively. The optimal codeword transmission rate R_b^* is not presented in the figure. This is because the optimal codeword transmission rate is equal to $R_b^* = \log_2 \left(1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_s^*} \right)$ for all of the three problems, and the differences between R_{b1}^* , R_{b2}^* and R_{b3}^* are determined by the differences between R_{s1}^* , R_{s2}^* and R_{s3}^* . As depicted in the figure, the values of R_{s1}^* , R_{s2}^* and R_{s3}^* are clearly different to each other. We note that $R_{s1}^* = R_{s2}^* = R_{s3}^*$ if and only if the throughput constraint is very stringent, under which condition the transmission rates are totally determined by the throughput constraint. The observations above show the fact that the optimal transmission designs are very different when we use different secrecy metrics to evaluate the secrecy performance.

We just compared the optimal transmission rates that optimize the secrecy performance of the system measured by different secrecy metrics. Now, we focus on the optimal transmission rates that minimize the generalized secrecy outage probabilities subject to different requirements on the fractional equivocation. Figure 5.7 plots R_{s1}^* versus Γ with different values of θ . As shown in the figure, the optimal transmission rates minimizing the secrecy outage probability are different if the required values of θ are different. We find that the optimal confidential information rate R_{s1}^* increases as the level of required fractional equivocation θ

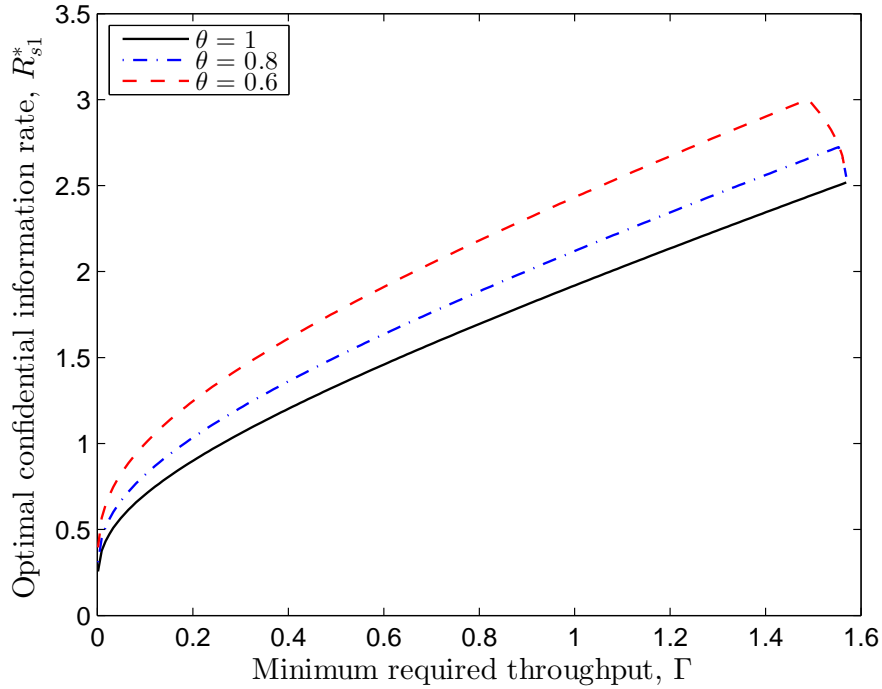


Figure 5.7: For generalized secrecy outage probability: optimal confidential information rate versus minimum required throughput. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.

decreases. The observations from Figures 5.6 and 5.7 confirm that the answer to Q1 is yes, the newly proposed secrecy metrics lead to very different optimal design parameters that optimize the secrecy performance of the system.

In the following, we check the answer to the second question listed at the beginning of this section by Figures 5.8, 5.9 and 5.10. From the analytical results, we have obtained three different solutions of the optimal design parameters: (R_{b1}^*, R_{s1}^*) is optimal for minimizing the generalized secrecy outage probability; (R_{b2}^*, R_{s2}^*) is optimal for maximizing the average fractional equivocation; (R_{b3}^*, R_{s3}^*) is optimal for minimizing the average information leakage rate. We collectively consider all three design solutions and study their performance in all three secrecy metrics. Specifically, Figure 5.8 plots p_{out} achieved by different transmission designs; Figure 5.9 plots $\bar{\Delta}$ achieved by different transmission designs; Figure 5.10 plots R_L achieved by different transmission designs. As shown in the figures, the transmission with R_{b1}^* and R_{s1}^* minimizes the secrecy outage probability, but will lead to a considerable secrecy loss if the practical secrecy requirement is to ensure a high fractional equivocation (decoding error probability at Eve) or a low information leakage rate. Similarly, the transmission with R_{b2}^* and R_{s2}^* maximizes the average fractional equivocation, but will incur a considerable secrecy loss if the

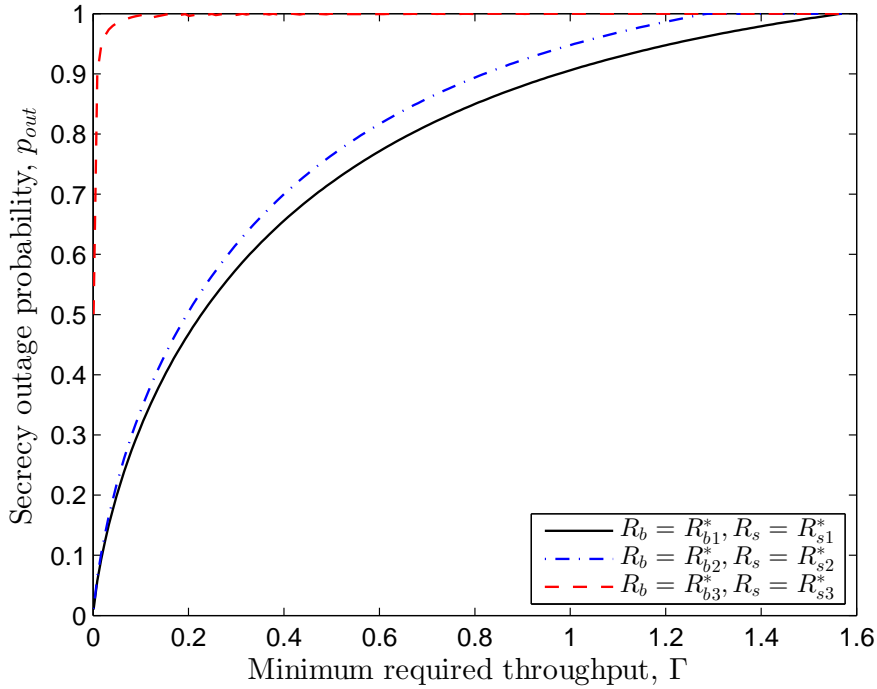


Figure 5.8: Secrecy outage probability versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.

practical secrecy requirement is to have a low secrecy outage probability or a low information leakage rate. The transmission with R_{b3}^* and R_{s3}^* minimizes the average information leakage rate, but will incur a large secrecy loss if the practical secrecy requirement is to maintain a low secrecy outage probability or a high fractional equivocation. The observations from Figures 5.8, 5.9 and 5.10 show that it is important to appropriately design the system with its preferred secrecy metric. It is also confirmed that the answer to Q2 is yes, applying the transmission design based on the perfect secrecy outage probability can result in a large secrecy loss if the actual system requires a low decodability at the eavesdropper or a low information leakage rate.

5.6 Summary

To address the limitation of the perfect secrecy outage probability from a practical point of view, in this chapter we proposed three new secrecy metrics for physical layer security over quasi-static fading channels. Specifically, the generalized secrecy outage probability establishes a link between the existing concept of secrecy outage and the decodability of messages at the eavesdropper. The asymptotic lower bound on the eavesdropper's decoding error proba-

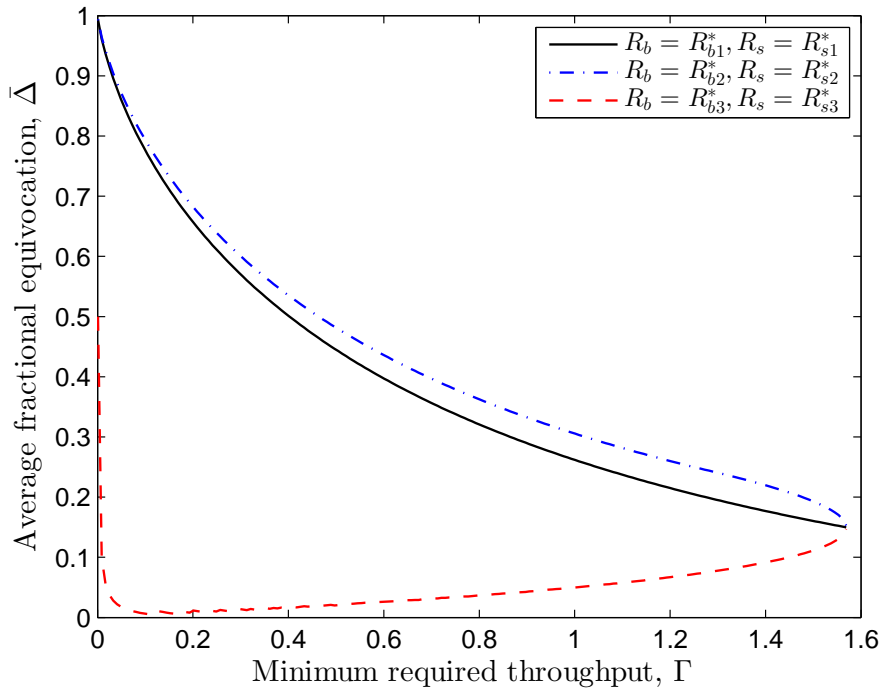


Figure 5.9: Average fractional equivocation (asymptotic lower bound on the decoding error probability at Eve) versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.

bility provides a direct error-probability-based secrecy metric. The average information leakage rate characterizes how fast the confidential information is leaked to the eavesdropper when perfect secrecy is not achieved. We evaluated the secrecy performance of an example wireless system with non-adaptive rate wiretap codes by the proposed secrecy metrics. We showed that the new secrecy metrics give a more comprehensive understanding of physical layer security over fading channels. We also found that the new secrecy metrics can give insights on the secrecy performance of wireless transmissions that sometimes cannot be captured by the perfect secrecy outage probability. Furthermore, we examined the significance of the newly proposed secrecy metrics from the perspective of a system designer. We found that applying the optimal transmission design minimizing the perfect secrecy outage probability can result in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper or a low information leakage rate. The new secrecy metrics enable appropriate transmission designs for systems with different secrecy requirements.

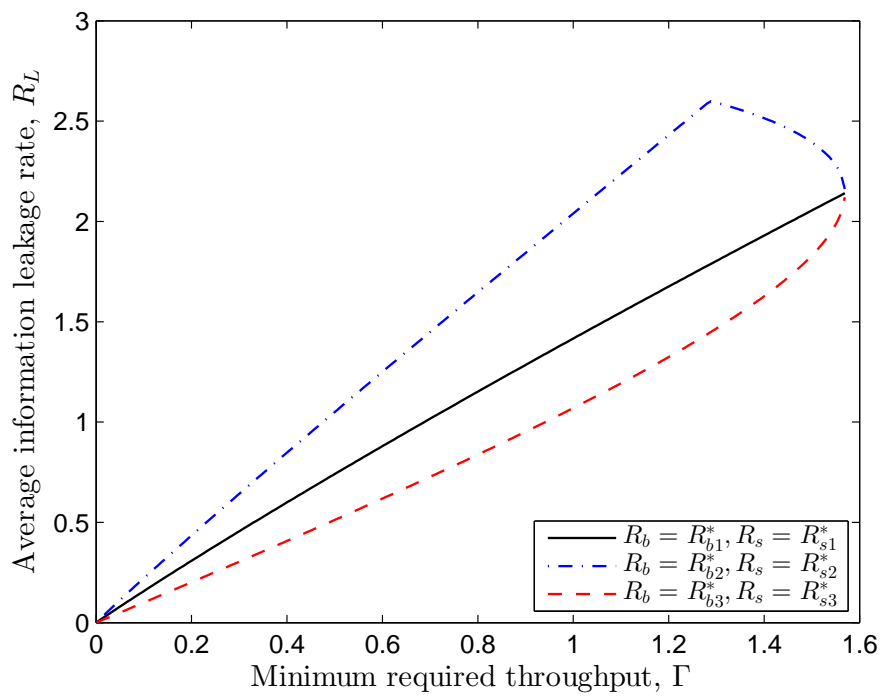


Figure 5.10: Average information leakage rate versus minimum required throughput. The other parameters are $\theta = 1$, $\bar{\gamma}_b = 10$ dB and $\bar{\gamma}_e = 10$ dB.

Conclusions

In this chapter, we first summarize the general conclusions drawn from the thesis, and then outline some future research directions.

6.1 Thesis Conclusions

Motivated by the large gap between theory and practice in wireless physical layer security, this thesis has studied the wireless physical layer security towards practical assumptions and requirements.

In the first half of the thesis, we reduced the dependence of physical layer security on impractical assumptions. We first studied the secure transmission designs with the consideration of channel estimation errors, against the impractical assumption of perfect CSI. We presented a comprehensive study of secure on-off transmission design with different transmission schemes, i.e., the fixed rate transmission, the non-adaptive rate transmission, and the adaptive rate transmission. Our results illustrated how the optimal design and the achievable system performance vary with the change in the channel knowledge assumptions. We then introduced the spatial constraint into physical layer security, which provides an innovative approach to study the multi-antenna secure networks without the impractical assumption of knowing the number of eavesdropper antennas. With the spatial constraints at the receiver side, we investigated the wiretap-channel system, the basic jammer-assisted system, and the AN jammer-assisted system. We found that a non-zero secrecy capacity is achievable with the assist of jamming signals, even if the eavesdropper is equipped with infinite number of antennas.

In the second half of the thesis, we improved the applicability of the study on physical layer security. Firstly, we designed linear precoders to achieve confidential broadcasting in a two-cell broadcast network, while the current confidential broadcasting is applicable only in single-cell networks. We considered two forms of BS cooperation, i.e., the MCP and the CBf. For each form of BS cooperation, we proposed an appropriate linear precoder to efficiently achieve the confidential broadcasting. We conducted the large-system analysis, and optimized the precoder designs based on the large-system results. Secondly, we proposed new secrecy

metrics for physical layer security over fading channels. This is motivated by the limitations of the perfect secrecy outage probability on evaluating wireless systems with practical requirements. The newly proposed secrecy metrics can give insights on the secrecy performance of wireless transmissions that sometimes cannot be captured by the perfect secrecy outage probability. Our results showed that the new secrecy metrics enable appropriate transmission designs for systems with practical secrecy requirements.

6.2 Future Research Directions

In this section, we point out some possible future research directions that arise from the work presented in this thesis.

Secure communications with spatial constraints at the transmitter and the receiver:

As a first step of studying the effects of spatial constraints on physical layer security, Chapter 3 considered a simple scenario with spatial constraints at the receiver side only. A natural future work is to extend the study by investigating the effects of spatial constraints at both the transmitter and the receiver sides. To this end, a limited number of transmit antennas with the spatial constraint at the transmitter should be considered [95]. However, it is worth mentioning that the extension is non-trivial, since the secrecy capacity would depend on instantaneous channel realizations even if the number of transmit antennas goes to infinity.

Stochastic geometry in broadcast networks with confidential information: Chapter 4 assumed a simple homogenous scenario where the users in the same cell are located at the same distance away from the BS. In practical networks, the users are more likely to spatially randomly distributed in the network with different distances to the BS. To characterize the randomness of user locations, we can adopt the stochastic geometry approach [96] for modeling the user locations, since it allows us to appropriately study the probabilistic network behaviors and corresponding performance metrics [97, 98, 99, 100]. In fact, the spatial modeling of user locations using stochastic geometry approach has already been adopted in the research of physical layer security, e.g., [101, 102, 103], while it has never been considered in the study of confidential broadcasting.

Analysis and design of physical layer security based on the new secrecy metrics: In Chapter 5, we proposed new secrecy metrics for wireless transmission over fading channels. A natural future research direction is to adopt the proposed secrecy metrics to analyze physical layer security in wireless systems. Also, it is interesting to develop efficient secure transmission designs or secrecy enhancements based on the proposed secrecy metrics, according to the secrecy requirements on practical wireless networks.

Appendix A

A.1 Proof of Proposition 2.1

We first derive the optimal μ_b in Scenario 1. One can find that $\mu_b = 2^{R_b} - 1$ is the only solution of μ_b to the equation

$$\frac{\partial \eta(\mu_b, \mu_e)}{\partial \mu_b} = 0 \quad (\text{A.1})$$

and

$$\frac{\partial^2 \eta(2^{R_b} - 1, \mu_e)}{\partial \mu_b^2} < 0. \quad (\text{A.2})$$

Thus, if we ignore the possible bound of μ_b , the optimal μ_b is equal to $2^{R_b} - 1$. However, to satisfy the reliability constraint, $p_{\text{co}} \leq \delta$, there exists a possible lower bound of μ_b given by

$$\mu_b \geq (2^{R_b} - 1) \left(1 - \alpha_b \zeta_b \ln \left(\delta \frac{1 + \zeta_b(2^{R_b} - 2)}{\zeta_b(2^{R_b} - 1)} \right) \right). \quad (\text{A.3})$$

Considering the lower bound, the optimal μ_b in Scenario 1 is formulated as (2.27) in Proposition 2.1.

Then, we derive the optimal μ_e in Scenario 1. Since p_{tx} is an increasing function of μ_e and p_{co} is independent of μ_e , it is optimal to maximize μ_e while satisfying the security constraint $p_{\text{so}} \leq \varphi$. From the definition of p_{so} , one can find that p_{so} is an increasing function of μ_e . Thus, there is only one or no solution of μ_e to the equation

$$p_{\text{so}}(\mu_e) = \varphi, \quad (\text{A.4})$$

where the expression of p_{so} is given as (2.23). When

$$\Pr(C_e > R_b - R_s) \leq \varphi \Leftrightarrow \frac{1 - \zeta_e}{1 + \zeta_e(2^{R_b - R_s} - 2)} \exp \left(-\frac{2^{R_b - R_s} - 1}{\alpha_e(1 - \zeta_e)} \right) \leq \varphi, \quad (\text{A.5})$$

there is no solution of μ_e to (A.4), which means that there is no need to set an on-off SNR threshold on $\hat{\gamma}_e$ for the system (the required security constraint is always achievable) or equiv-

alently $\mu_e = \infty$. Otherwise, there exists one and only one solution of μ_e to (A.4), which is the optimal value of μ_e to the maximization problem. The optimal μ_e in Scenario 1 can be numerically solved as given in (2.28). This completes the proof of Proposition 2.1.

A.2 Proof of Proposition 2.2

The optimal μ_b in Scenario 2 is the same as that in Scenario 1 and the proof of it is identical to the corresponding part in the proof of Proposition 2.1. Now, we derive the optimal μ_e in Scenario 2. Since p_{tx} is an increasing function of μ_e and p_{co} is independent of μ_e , it is optimal to maximize μ_e while satisfying the security constraint $p_{\text{so}} \leq \varphi$. From the definition of p_{so} , one can find that p_{so} is an increasing function of μ_e . Thus, there is only one or no solution of μ_e to the equation

$$p_{\text{so}}(\mu_e) = \varphi, \quad (\text{A.6})$$

where the expression of p_{so} is given as (2.34). When

$$\Pr(C_e > R_b - R_s) \leq \varphi \Leftrightarrow \exp\left(-\frac{2^{R_b - R_s} - 1}{\alpha_e}\right) \leq \varphi, \quad (\text{A.7})$$

there is no solution of μ_e to (A.6), which means that there is no need to set an on-off SNR threshold on $\hat{\gamma}_e$ for the system (the required security constraint is always achievable) or equivalently $\mu_e = \infty$. Otherwise, there exists one and only one solution of μ_e to (A.6), which is the optimal value of μ_e to the maximization problem. The optimal μ_e in Scenario 2 can be numerically solved as given in (2.38). This completes the proof of Proposition 2.2.

A.3 Proof of Proposition 2.4

The proof of the optimal μ_b for the non-adaptive scheme is identical to the proof of optimal μ_b in Section 2.3. Now, we prove the optimal R_s for any chosen R_b as follows. Since p_{tx} and p_{co} are independent of R_s , it is optimal to maximize R_s . Thus, we obtain the optimal R_s while satisfying $p_{\text{so}} \leq \varphi$ as (2.57) in Proposition 2.4. Then, we prove the optimal R_b . Since $R_s > 0$, we have $R_b > k$. It is easy to prove that when

$$R_b \geq \max\left\{\log_2\left(1 + \frac{(1 - \zeta_b)\delta}{\zeta_b(1 - \delta)}\right), k + \frac{1}{\ln 2}W_0\left(2^{-k}\alpha_b(1 - \zeta_b)\right)\right\}, \quad (\text{A.8})$$

the value of η is a decreasing function of R_b , i.e.,

$$\frac{\partial \eta(\mu_b, R_b)}{\partial R_b} < 0. \quad (\text{A.9})$$

Therefore, the optimal R_b can be obtained by solving the optimization problem given in Proposition 2.4. This completes to proof of Proposition 2.4.

A.4 Proof of Proposition 2.5

The proof of the optimal R_s for the adaptive rate scheme is identical to the corresponding part in the proof of Proposition 2.4. Now, we derive the optimal R_b . To satisfy $R_s > 0$ and $p_{co} \leq \delta$, we obtain the lower and upper bounds of R_b given by $R_b > k$ and $R_b \leq \log_2 \left(1 + \frac{\hat{\gamma}_b}{1 + \alpha_b \zeta_b \ln \delta^{-1}} \right)$. Thus, the optimal R_b can be obtained by solving the optimization problem given in Proposition 2.5. Then, we derive the optimal μ_b . To derive the optimal, μ_b , we start from looking for the range of $\hat{\gamma}_b$ in which it is possible to have secure communication with positive confidential information rate while satisfying both constraints. Let the lower bound of R_b be less than the upper bound of R_b , we can find the feasible range of $\hat{\gamma}_b$ as

$$\log_2 (1 + \alpha_e \ln (\varphi^{-1})) < \log_2 \left(1 + \frac{\hat{\gamma}_b}{1 + \alpha_b \zeta_b \ln \delta^{-1}} \right) \Leftrightarrow \hat{\gamma}_b > (1 + \alpha_b \zeta_b \ln \delta^{-1}) \alpha_e \ln (\varphi^{-1}). \quad (\text{A.10})$$

Therefore, the optimal μ_b is equal to the lower bound of the feasible $\hat{\gamma}_b$, given by (2.65). This completes to proof of Proposition 2.5.

Appendix B

B.1 Proof of Proposition 3.1

The capacity of Bob or Eve's channel can be written as

$$C_i = \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i \mathbf{H}_i \mathbf{Q}_x \mathbf{H}_i^H}{\sigma_i^2} \right|, \quad (\text{B.1})$$

where \mathbf{Q}_x denotes the covariance matrix of \mathbf{x} , i.e., $\mathbf{Q}_x = \mathbb{E} \{ \mathbf{x} \mathbf{x}^H \}$. Since Alice has no instantaneous CSI of Bob and there is sufficient space at Alice for independent transmit antenna allocation, the best transmission strategy is to have the transmit signal vector composed of statistically independent equal power components, each with a Gaussian distribution. Then, the covariance matrix of \mathbf{x} is equal to $\mathbf{Q}_x = \frac{P_t}{N_t} \mathbf{I}_{N_t}$, and the channel capacity becomes to

$$C_i = \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i P_t}{\sigma_i^2 N_t} \mathbf{H}_i \mathbf{H}_i^H \right|, \quad (\text{B.2})$$

where

$$\mathbf{H}_i \mathbf{H}_i^H = \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H. \quad (\text{B.3})$$

Considering a large number of transmit antennas ($N_t \rightarrow \infty$) and sufficient space for placing transmit antennas (independent \mathbf{h}_{it}), the correlation matrix at the receiver in (3.2) becomes to

$$\mathbf{R}_i \rightarrow \frac{1}{N_t} \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H. \quad (\text{B.4})$$

Note that there is no expectation over channel realizations in (B.4), since $\frac{1}{N_t} \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H = \mathbb{E} \left\{ \frac{1}{N_t} \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H \right\}$ when $N_t \rightarrow \infty$. Then, the channel capacity with a large number of sufficiently separated transmit antennas is approximated by

$$C_i \approx \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i P_t}{\sigma_i^2} \mathbf{R}_i \right|. \quad (\text{B.5})$$

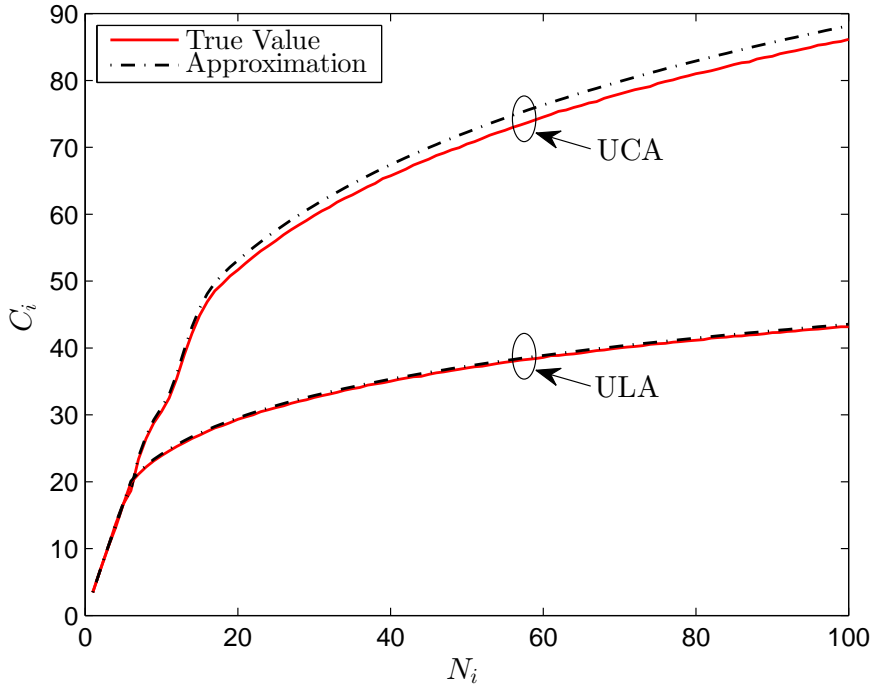


Figure B.1: Without jamming signals: C_i versus N_i . The other system parameters are $N_t = 100$, $r_i = 1\lambda$, $P_t = 10$ dB, $\alpha_i = 1$, $\sigma_i^2 = 1$.

We highlight that the approximation by (B.5) provides good accuracy even if the number of transmit antennas is finite. To examine the accuracy of the approximation by (B.5), we compare the true value of C_i obtained by (B.2) and the approximation obtain by (B.5) for given receive antenna array configurations. The simulation result is presented by Figure B.1. The number of transmit antennas is set as a large but finite number, $N_t = 100$. The number of receive antennas is in the range of $1 \leq N_i \leq N_t = 100$. We consider two different antenna array configurations, which are the uniform linear array (ULA) and the uniform circular array (UCA), in a fixed circular aperture at the receiver with $r_i = 1\lambda$. Since the number of transmit antennas is set as a finitely large number but not infinity, the capacity result by (B.2) would depend on the instantaneous channel realization. Thus, the “true value” in Figure B.1 is the average value of C_i obtained by (B.2) over different channel realizations. It is evident from Figure B.1 that the difference between the true value and the approximation is very small for the whole range of N_i , which indicates that the approximation by (B.5) provides good accuracy even if the transmitter has a finite number of antennas.

For the receiver with N_i optimally-placed antennas in a fixed aperture region, the channel

capacity in (B.5) can be further approximated by [70, Chapter 3],

$$C_i \approx \begin{cases} N_i \log\left(1 + \frac{\alpha_i P_i}{\sigma_i^2}\right), & \text{if } N_i \leq N_{0i} \\ N_{0i} \log\left(1 + \frac{N_i}{N_{0i}} \frac{\alpha_i P_i}{\sigma_i^2}\right), & \text{if } N_i > N_{0i}, \end{cases} \quad (\text{B.6})$$

where the expression of N_{0i} for a 2D circular aperture or a 3D spherical aperture is given by (3.9). The C_i in (B.6) is derived with the approximation that $J_m\left(\frac{2\pi}{\lambda} r_i\right) \rightarrow 0$ for $m \geq \lceil \pi e r_i / \lambda \rceil + 1$, where $J_m(\cdot)$ denotes the Bessel function of order m . Such an approximation is shown to be very accurate in [70].

Finally, substituting (B.6) into (3.8) completes the proof of Proposition 3.1.

B.2 Proof of Theorem 3.1

The capacity of Bob or Eve's channel subject to the basic jamming signals is written as [104, Section 3.1]

$$C_i = \log \left| \mathbf{I}_{N_i} + \alpha_i \mathbf{H}_i \mathbf{Q}_x \mathbf{H}_i^H (\beta_i \mathbf{G}_i \mathbf{Q}_w \mathbf{G}_i^H + \sigma_i^2 \mathbf{I}_{N_i})^{-1} \right|, \quad (\text{B.7})$$

where \mathbf{Q}_x and \mathbf{Q}_w denote the covariance matrices of \mathbf{x} and \mathbf{w}_1 , respectively, i.e., $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$ and $\mathbf{Q}_w = \mathbb{E}\{\mathbf{w}_1\mathbf{w}_1^H\}$. Since neither Alice nor Helen has the instantaneous CSI to Bob or Eve, the equal power allocation at the transmit antennas is adopted at both Alice and Helen, and the covariance matrices of \mathbf{x} and \mathbf{w}_1 are equal to $\mathbf{Q}_x = \frac{P_i}{N_i} \mathbf{I}_{N_i}$ and $\mathbf{Q}_w = \frac{P_j}{N_j} \mathbf{I}_{N_j}$, respectively. Then, the channel capacity becomes to

$$C_i = \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i P_i}{N_i} \mathbf{H}_i \mathbf{H}_i^H \left(\frac{\beta_i P_j}{N_j} \mathbf{G}_i \mathbf{G}_i^H + \sigma_i^2 \mathbf{I}_{N_i} \right)^{-1} \right|. \quad (\text{B.8})$$

Considering the large number of transmit antennas ($N_t \rightarrow \infty, N_j \rightarrow \infty$) and sufficient space for placing transmit antennas (independent \mathbf{h}_{it} and independent \mathbf{g}_{it}), we have

$$\frac{1}{N_t} \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H = \frac{1}{N_j} \sum_{t=1}^{N_j} \mathbf{g}_{it} \mathbf{g}_{it}^H = \mathbf{R}_i, \quad (\text{B.9})$$

where \mathbf{R}_i is the correlation matrix at the receiver side. Note that \mathbf{R}_i is determined by the receive antenna correlations.

Therefore, the channel capacity can be approximated by

$$\begin{aligned}
C_i &\approx \log \left| \mathbf{I}_{N_i} + \alpha_i P_t \mathbf{R}_i (\beta_i P_j \mathbf{R}_i + \sigma_i^2 \mathbf{I}_{N_i})^{-1} \right| \\
&= \log \left| (\alpha_i P_t \mathbf{R}_i + \beta_i P_j \mathbf{R}_i + \sigma_i^2 \mathbf{I}_{N_i}) (\beta_i P_j \mathbf{R}_i + \sigma_i^2 \mathbf{I}_{N_i})^{-1} \right| \\
&= \log \left| \left(\mathbf{I}_{N_i} + \left(\frac{\alpha_i P_t}{\sigma_i^2} + \frac{\beta_i P_j}{\sigma_i^2} \right) \mathbf{R}_i \right) \left(\mathbf{I}_{N_i} + \frac{\beta_i P_j}{\sigma_i^2} \mathbf{R}_i \right)^{-1} \right| \\
&= \log \left| \mathbf{I}_{N_i} + \left(\frac{\alpha_i P_t}{\sigma_i^2} + \frac{\beta_i P_j}{\sigma_i^2} \right) \mathbf{R}_i \right| - \log \left| \mathbf{I}_{N_i} + \frac{\beta_i P_j}{\sigma_i^2} \mathbf{R}_i \right|. \tag{B.10}
\end{aligned}$$

We highlight that the approximation by (B.10) provides good accuracy even if the number of transmit antennas and the number of jamming antennas are finite. To examine the accuracy of the approximation by (B.10), we compare the true value of C_i obtained by (B.8) and the approximation obtain by (B.10) for given receive antenna array configurations. The simulation result is presented by Figure B.2. The number of transmit antennas and the number of jamming antennas are set as $N_t = N_j = 100$. The number of receive antennas is in the range of $1 \leq N_i \leq N_t = N_j = 100$. We still consider two different antenna array configurations, i.e., the ULA and the UCA, in a fixed circular aperture at the receiver with $r_i = 1\lambda$. It is evident from Figure B.2 that the difference between the true value and the approximation is very small for the whole range of N_i . This confirms that the approximation by (B.10) provides good accuracy even if the transmitter and the jammer have finite numbers of antennas.

For the receiver with N_i optimally-placed antennas in a fixed aperture region, the channel capacity in (B.10) can be further approximated by

$$\begin{aligned}
C_i &\approx \begin{cases} N_i \log \left(1 + \frac{\alpha_i P_t}{\sigma_i^2} + \frac{\beta_i P_j}{\sigma_i^2} \right) - N_i \log \left(1 + \frac{\beta_i P_j}{\sigma_i^2} \right), & \text{if } N_i \leq N_{0i} \\ N_{0i} \log \left(1 + \frac{N_i}{N_{0i}} \left(\frac{\alpha_i P_t}{\sigma_i^2} + \frac{\beta_i P_j}{\sigma_i^2} \right) \right) - N_{0i} \log \left(1 + \frac{N_i}{N_{0i}} \frac{\beta_i P_j}{\sigma_i^2} \right), & \text{if } N_i > N_{0i} \end{cases} \\
&= \begin{cases} N_i \log \left(1 + \frac{\alpha_i P_t}{\beta_i P_j + \sigma_i^2} \right), & \text{if } N_i \leq N_{0i} \\ N_{0i} \log \left(1 + \frac{\frac{N_i}{N_{0i}} \alpha_i P_t}{\frac{N_i}{N_{0i}} \beta_i P_j + \sigma_i^2} \right), & \text{if } N_i > N_{0i}. \end{cases} \tag{B.11}
\end{aligned}$$

Still, the C_i in (B.11) is derived with the approximation that $J_m \left(\frac{2\pi}{\lambda} r_i \right) \rightarrow 0$ for $m \geq \lceil \pi e r_i / \lambda \rceil + 1$.

Finally, substituting (B.11) into (3.8) completes the proof of Theorem 3.1.

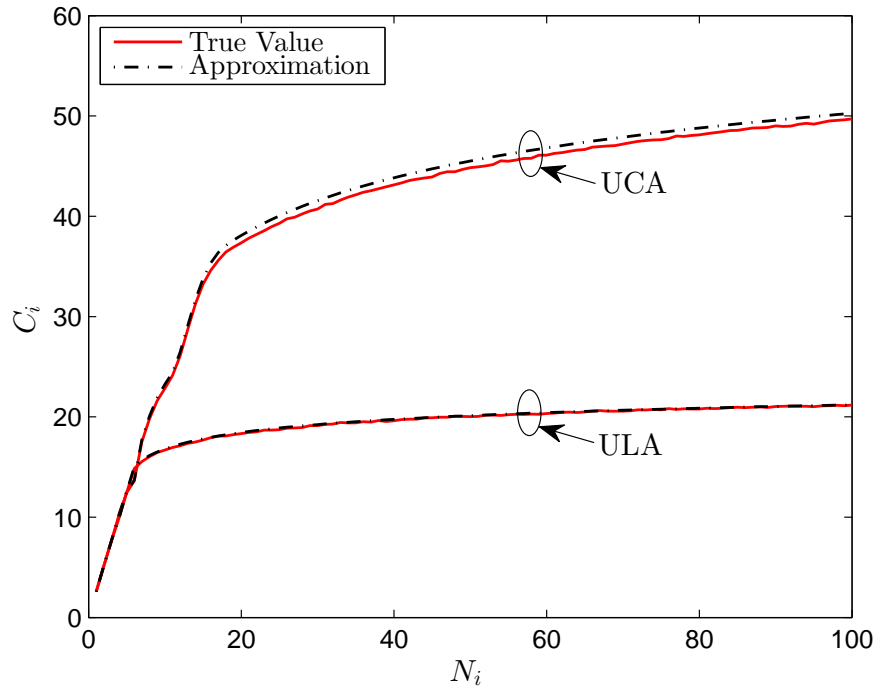


Figure B.2: With jamming signals: C_i versus N_i . The other system parameters are $N_t = N_j = 100$, $r_i = 1\lambda$, $P_t = 10$ dB, $P_j = 0$ dB, $\alpha_i = 1$, $\beta_i = 1$, $\sigma_i^2 = 1$.

B.3 Proof of Theorem 3.2

Since the AN jamming signals do not degrade Bob's channel, we derive the capacity of Bob's channel directly from (B.6), which is given by

$$C_b \approx \begin{cases} N_b \log\left(1 + \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{if } N_b \leq N_{0b} \\ N_{0b} \log\left(1 + \frac{N_b}{N_{0b}} \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{if } N_b > N_{0b}. \end{cases} \quad (\text{B.12})$$

Now, we derive the capacity of Eve's channel subject to the AN jamming signals. The received signal vector at Eve is written as

$$\mathbf{y}_e = \sqrt{\alpha_e} \mathbf{H}_e \mathbf{x} + \sqrt{\beta_e} \mathbf{K} \mathbf{v} + \mathbf{n}_e, \quad (\text{B.13})$$

where $\mathbf{K} = \mathbf{G}_e \mathbf{Z}$ represents the equivalent channel for the vector \mathbf{v} to Eve. Due to the orthonormality of \mathbf{Z} , the $N_e \times (N_j - N_b)$ matrix \mathbf{K} has circularly symmetric i.i.d. complex Gaussian distributed elements. Then, the capacity of Eve's channel is written as

$$C_e = \log \left| \mathbf{I}_{N_e} + \alpha_e \mathbf{H}_e \mathbf{Q}_x \mathbf{H}_e^H (\beta_e \mathbf{K} \mathbf{Q}_v \mathbf{K}^H + \sigma_e^2 \mathbf{I}_{N_e})^{-1} \right|, \quad (\text{B.14})$$

where \mathbf{Q}_x and \mathbf{Q}_v denote the covariance matrices of \mathbf{x} and \mathbf{v} , respectively, i.e., $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$ and $\mathbf{Q}_v = \mathbb{E}\{\mathbf{v}\mathbf{v}^H\}$. With the equal power allocation at Alice, we have $\mathbf{Q}_x = \frac{P_t}{N_t} \mathbf{I}_{N_t}$. Also, since \mathbf{v} is chosen as i.i.d. complex Gaussian random variables, we have $\mathbf{Q}_v = \frac{P_j}{N_j - N_b} \mathbf{I}_{N_j - N_b}$. Then, the capacity of Eve's channel becomes to

$$C_e = \log \left| \mathbf{I}_{N_e} + \alpha_e P_t \mathbf{R}_e \left(\frac{\beta_e P_j}{N_j - N_b} \mathbf{K}\mathbf{K}^H + \sigma_e^2 \mathbf{I}_{N_e} \right)^{-1} \right|, \quad (\text{B.15})$$

where \mathbf{R}_e is the correlation matrix at Eve, and is determined by the receive antenna correlations at Eve. Define $\mathbf{K} = [\mathbf{k}_1 \cdots \mathbf{k}_i \cdots \mathbf{k}_{N_j - N_b}]$, $\mathbf{Z} = [\mathbf{z}_1 \cdots \mathbf{z}_i \cdots \mathbf{z}_{N_j - N_b}]$, and hence $\mathbf{k}_i = \mathbf{H}_e \mathbf{z}_i$.

If we can prove that \mathbf{k}_i are independent, the correlation matrix would converge to $\mathbf{R} \rightarrow \frac{1}{N_j - N_b} \mathbf{K}\mathbf{K}^H$ as $(N_j - N_b) \rightarrow \infty$, and the capacity of Eve's channel could be written as

$$C_e = \log \left| \mathbf{I}_{N_e} + \alpha_e P_t \mathbf{R}_e (\beta_e P_j \mathbf{R}_e + \sigma_e^2 \mathbf{I}_{N_e})^{-1} \right|. \quad (\text{B.16})$$

Having (B.16), we can derive the channel capacity of spatially-constrained Eve which is the same as (B.11).

Therefore, in the following, we need only to prove that \mathbf{k}_i are independent to complete the proof of Theorem 3.2. For any \mathbf{k}_m and \mathbf{k}_n where $m \neq n$, we have

$$[\mathbf{k}_m - \mathbb{E}\{\mathbf{k}_m\}]^H [\mathbf{k}_n - \mathbb{E}\{\mathbf{k}_n\}] = \mathbf{z}_m^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{z}_n \stackrel{(a)}{=} \mathbf{z}_m^H \mathbf{z}_n \stackrel{(b)}{=} 0, \quad (\text{B.17})$$

where (a) is because of the independence between transmit antennas and (b) is because of the orthogonality of \mathbf{Z} . Thus, \mathbf{k}_i are pairwise uncorrelated. In addition, multivariate normality and no correlation implies independence. Multivariate normality and pairwise independence implies mutual independence. Since \mathbf{k}_i are multivariate normally distributed, \mathbf{k}_i are mutually independent. This completes the proof of Theorem 3.2.

B.4 Proof of Proposition 3.2

We first rewrite (3.20) as

$$C_s^w = \begin{cases} [f_1(x = P_j)]^+, & \text{if } N_b \leq N_{0b} \\ [f_2(x = P_j)]^+, & \text{if } N_b > N_{0b}. \end{cases} \quad (\text{B.18})$$

If $N_b \leq N_{0b}$, we can obtain two possible stationary points of $f_1(x)$, i.e., x_1 and x_2 , by taking the derivative of $f_1(x)$ with respect to x and equating it to zero. If C_s^w is not always equal to zero, P_j^* should exist and be equal to one of the stationary points, since $\lim_{x \rightarrow 0} f(x) \rightarrow -\infty$ and $\lim_{x \rightarrow \infty} f(x) \rightarrow 0$. Then, we determine P_j^* by examining the values of x_1 and x_2 . When neither x_1 nor x_2 is real and positive, it is not applicable to determine the optimal value of P_j , because

the stationary point for $f_1(x)$ does not exist, and C_s^w is always equal to zero for any value of P_j . Similarly, if $N_b > N_{0b}$, we can obtain two possible stationary points of $f_2(x)$, i.e., x_3 and x_4 , by taking the derivative of $f_2(x)$ with respect to x and equating it to zero. Then, we determine P_j^* by examining the values of x_3 and x_4 . When neither x_3 nor x_4 is real and positive, it is not applicable to determine the optimal value of P_j , because C_s^w is always equal to zero for any value of P_j . This completes the proof of Proposition 3.2.

Appendix C

C.1 Proof of Theorem 4.1

We first derive the large-system approximations of the SINRs for message $s_{k,j}$ at the intended receiver and the eavesdropper. Based on the approximations, we then obtain the large-system secrecy sum rate using (4.22).

We recall that the following equality holds:

$$(\mathbf{H}^H \mathbf{H} + \alpha \mathbf{I}_{2N})^{-1} = \left(\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} + \mathbf{h}_{k,j}^H \mathbf{h}_{k,j} + \alpha \mathbf{I}_{2N} \right)^{-1}. \quad (\text{C.1})$$

By applying the matrix inversion lemma, we obtain

$$\begin{aligned} (\mathbf{H}^H \mathbf{H} + \alpha \mathbf{I}_{2N})^{-1} &= \left(\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} + \alpha \mathbf{I}_{2N} \right)^{-1} \\ &\quad - \frac{\left(\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} + \alpha \mathbf{I}_{2N} \right)^{-1} \mathbf{h}_{k,j}^H \mathbf{h}_{k,j} \left(\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} + \alpha \mathbf{I}_{2N} \right)^{-1}}{1 + \mathbf{h}_{k,j} \left(\mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} + \alpha \mathbf{I}_{2N} \right)^{-1} \mathbf{h}_{k,j}^H}. \end{aligned} \quad (\text{C.2})$$

Then let us define

$$\mathbf{Z}_{k,j} = \mathbf{O}_{k,j} - \frac{\mathbf{O}_{k,j} \left(\frac{1}{N} \mathbf{h}_{k,j}^H \mathbf{h}_{k,j} \right) \mathbf{O}_{k,j}}{1 + \frac{1}{N} \mathbf{h}_{k,j} \mathbf{O}_{k,j} \mathbf{h}_{k,j}^H}, \quad (\text{C.3})$$

where

$$\mathbf{O}_{k,j} = \left(\frac{1}{N} \mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} + \frac{\alpha}{N} \mathbf{I}_{2N} \right)^{-1}. \quad (\text{C.4})$$

This allows us to rewrite (C.2) as

$$(\mathbf{H}^H \mathbf{H} + \alpha \mathbf{I}_{2N})^{-1} = \frac{1}{N} \mathbf{Z}_{k,j}. \quad (\text{C.5})$$

Moreover, we rewrite (4.10) and (4.11), respectively, as

$$\text{SINR}_{k,j} = \frac{c^2 \left| \frac{A_{k,j}}{1+A_{k,j}} \right|^2}{c^2 B_{k,j} + \sigma_d^2}, \quad (\text{C.6})$$

$$\text{SINR}_{\tilde{k},\tilde{j}} = \frac{c^2 B_{k,j}}{\sigma_d^2}, \quad (\text{C.7})$$

where

$$A_{k,j} = \frac{1}{N} \mathbf{h}_{k,j} \mathbf{O}_{k,j} \mathbf{h}_{k,j}^H, \quad (\text{C.8})$$

and

$$B_{k,j} = \frac{1}{N} \mathbf{h}_{k,j} \mathbf{Z}_{k,j} \left(\frac{1}{N} \mathbf{H}_{\tilde{k},\tilde{j}}^H \mathbf{H}_{\tilde{k},\tilde{j}} \right) \mathbf{Z}_{k,j} \mathbf{h}_{k,j}^H. \quad (\text{C.9})$$

Aided by [84], we obtain

$$A_{k,j} \xrightarrow{i.p.} g(\beta, \rho_M), \quad (\text{C.10})$$

$$B_{k,j} \xrightarrow{i.p.} \frac{1}{(1 + g(\beta, \rho_M))^2} \left(g(\beta, \rho_M) + \rho_M \frac{\partial g(\beta, \rho_M)}{\partial \rho_M} \right), \quad (\text{C.11})$$

and

$$c^2 \xrightarrow{a.s.} \frac{\frac{1}{2}(1 + \varepsilon) P_t}{g(\beta, \rho_M) + \rho_M \frac{\partial g(\beta, \rho_M)}{\partial \rho_M}}, \quad (\text{C.12})$$

where $\rho_M = (1 + \varepsilon)^{-1} \alpha / N$ and $g(\beta, \rho_M)$ is the solution of x to $x = \left(\rho_M + \frac{\beta}{1+x} \right)^{-1}$. In addition, we find that

$$g(\beta, \rho_M) + \rho_M \frac{\partial g(\beta, \rho_M)}{\partial \rho_M} = \frac{\beta g(\beta, \rho_M)}{\beta + \rho_M (1 + g(\beta, \rho_M))^2}. \quad (\text{C.13})$$

Therefore, substituting (C.10), (C.11) and (C.12) into (C.6), we derive the large-system approximate SINR at the intended user as

$$\text{SINR}_{k,j}^\infty = (1 + \varepsilon) \gamma g(\beta, \rho_M) \frac{1 + \frac{\rho_M}{\beta} (1 + g(\beta, \rho_M))^2}{(1 + \varepsilon) \gamma + (1 + g(\beta, \rho_M))^2}. \quad (\text{C.14})$$

Also, substituting (C.11) and (C.12) into (C.7), we derive the large-system approximate SINR at the eavesdropper as

$$\text{SINR}_{\tilde{k},\tilde{j}}^\infty = \frac{(1 + \varepsilon) \gamma}{(1 + g(\beta, \rho_M))^2}. \quad (\text{C.15})$$

Finally, by substituting (C.14) and (C.15) into (4.22), we obtain $R_{s,\text{MCP}}^\infty$ for $\alpha \neq 0$ in (4.23). If $\alpha = 0$, we derive the desired result in (4.23) by calculating $R_{s,\text{MCP}}^\infty(\alpha = 0) = \lim_{\alpha \rightarrow 0} R_{s,\text{MCP}}^\infty$. This completes the proof of Theorem 4.1.

C.2 Proof of Theorem 4.2

We first derive the large-system approximations of the SINRs for message $s_{k,j}$ at the intended receiver and the eavesdropper, based on which we obtain the large-system secrecy sum rate with the aid of (4.22).

Let us define

$$\mathbf{A}_j = \left(\rho_C + \frac{1}{N} \sum_{m=1}^2 \sum_{l=1}^K \mathbf{h}_{l,m,j}^H \mathbf{h}_{l,m,j} \right)^{-1} \quad (\text{C.16})$$

and

$$\mathbf{A}_{kj} = \left(\rho_C + \frac{1}{N} \sum_{(l,m) \neq (k,j)} \mathbf{h}_{l,m,j}^H \mathbf{h}_{l,m,j} \right)^{-1}, \quad (\text{C.17})$$

where $\rho_C = \alpha/N$. Due to the consideration of $P_1 = P_2 = P$, we have $c_j = c_{j'} = c$ in (4.19) and (4.20). Then, (4.19) and (4.20) can be, respectively, rewritten as

$$\text{SINR}_{k,j} = \frac{c^2 \left| \frac{1}{N} \mathbf{h}_{k,j,j} \mathbf{A}_{kj} \mathbf{h}_{k,j,j}^H \right|^2}{\sum_{(k',j') \neq (k,j)} \frac{c^2}{N} \theta_{k,j} + \sigma_d^2}, \quad (\text{C.18})$$

and

$$\text{SINR}_{\tilde{k},\tilde{j}} = \frac{\sum_{(k',j') \neq (k,j)} \frac{c^2}{N} \theta_{\tilde{k},\tilde{j}}}{\sigma_d^2}, \quad (\text{C.19})$$

where $\theta_{k,j} = \mathbf{h}_{k,j,j'} \mathbf{A}_{k',j',j'} \mathbf{h}_{k',j',j'}^H \mathbf{h}_{k',j',j'} \mathbf{A}_{k',j',j'} \mathbf{h}_{k,j,j}^H$, $\theta_{\tilde{k},\tilde{j}} = \mathbf{h}_{k',j',j} \mathbf{A}_{kj} \mathbf{h}_{k,j,j}^H \mathbf{h}_{k,j,j} \mathbf{A}_{kj} \mathbf{h}_{k',j',j}^H$, and

$$c^2 = \frac{P}{\sum_{k=1}^K \|\hat{\mathbf{w}}_{k,j}\|^2} = \frac{P}{\sum_{k=1}^K \frac{1}{N^2} \mathbf{h}_{k,j,j} \mathbf{A}_{kj}^2 \mathbf{h}_{k,j,j}^H}. \quad (\text{C.20})$$

According to [84], we have

$$\max_{j=1,2,k \leq K} \left| \frac{1}{N} \mathbf{h}_{k,j,j} \mathbf{A}_{kj} \mathbf{h}_{k,j,j}^H - \frac{1}{N} \text{Tr}(\mathbf{A}_j) \right| \xrightarrow{a.s.} 0, \quad (\text{C.21})$$

$$\max_{j=1,2,k \leq K} \left| \frac{1}{N^2} \mathbf{h}_{k,j,j} \mathbf{A}_{kj}^2 \mathbf{h}_{k,j,j}^H - \frac{1}{N} \text{Tr}(\mathbf{A}_j^2) \right| \xrightarrow{a.s.} 0, \quad (\text{C.22})$$

$$\max_{j,j'=1,2, k,k' \leq K, (k,j) \neq (k',j')} \left| \frac{1}{N} \theta_{k,j} - \vartheta_{j'} \right| \xrightarrow{a.s.} 0, \quad (\text{C.23})$$

$$\max_{j,j'=1,2, k,k' \leq K, (k,j) \neq (k',j')} \left| \frac{1}{N} \theta_{\tilde{k},\tilde{j}} - \vartheta_j \right| \xrightarrow{a.s.} 0, \quad (\text{C.24})$$

where $\vartheta_{j'} = \frac{\frac{\text{Tr}(\mathbf{A}_{j'}^2)}{N}}{\left(1 + \frac{\text{Tr}(\mathbf{A}_{j'})}{N}\right)^2}$, $\vartheta_j = \frac{\frac{\text{Tr}(\mathbf{A}_j^2)}{N}}{\left(1 + \frac{\text{Tr}(\mathbf{A}_j)}{N}\right)^2}$, and

$$\omega_{jj'} = \begin{cases} 1 & \text{if } j = j', \\ \varepsilon & \text{if } j \neq j'. \end{cases} \quad (\text{C.25})$$

In addition, we find that

$$\frac{\text{Tr}(\mathbf{A}_j)}{N} = \frac{\text{Tr}(\mathbf{A}_{j'})}{N} \xrightarrow{a.s.} \Lambda, \quad (\text{C.26})$$

$$\frac{\text{Tr}(\mathbf{A}_j^2)}{N} = \frac{\text{Tr}(\mathbf{A}_{j'}^2)}{N} \xrightarrow{a.s.} -\frac{\partial \Lambda}{\partial \rho_C}, \quad (\text{C.27})$$

where Λ is the solution of x to

$$x = \frac{1}{\rho_C + \frac{\beta}{1+x} + \frac{\beta\varepsilon}{1+\varepsilon x}}. \quad (\text{C.28})$$

Therefore, we obtain the following approximations as

$$|\mathbf{h}_{k,j,j} \hat{\mathbf{w}}_{k,j}|^2 \xrightarrow{a.s.} \Lambda^2, \quad (\text{C.29})$$

$$\sum_{(k',j') \neq (k,j)} |\mathbf{h}_{k,j,j'} \hat{\mathbf{w}}_{k',j'}|^2 \xrightarrow{a.s.} -\left(\frac{\beta\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{\beta}{(1+\Lambda)^2}\right) \frac{\partial \Lambda}{\partial \rho_C}, \quad (\text{C.30})$$

$$\sum_{(k',j') \neq (k,j)} |\mathbf{h}_{k',j',j} \hat{\mathbf{w}}_{k,j}|^2 \xrightarrow{a.s.} -\left(\frac{\beta\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{\beta}{(1+\Lambda)^2}\right) \frac{\partial \Lambda}{\partial \rho_C}, \quad (\text{C.31})$$

and

$$c^2 \xrightarrow{a.s.} -\frac{P}{\beta \frac{\partial \Lambda}{\partial \rho_C}}, \quad (\text{C.32})$$

with

$$-\frac{\partial \Lambda}{\partial \rho_C} = \frac{\Lambda}{\rho_C + \frac{\beta\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{\beta}{(1+\Lambda)^2}}. \quad (\text{C.33})$$

Substituting (C.29), (C.30) and (C.32) into (C.18), we derive large-system approximate SINR at the intended user as

$$\text{SINR}_{k,j}^\infty = \frac{\frac{\Lambda}{\beta} \left(\rho_C + \frac{\beta\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{\beta}{(1+\Lambda)^2} \right)}{\frac{1}{\gamma} + \frac{\varepsilon}{(1+\varepsilon\Lambda)^2} + \frac{1}{(1+\Lambda)^2}}. \quad (\text{C.34})$$

Also, substituting (C.31) and (C.32) into (C.19), we derive large-system approximate

SINR at the eavesdropper as

$$\text{SINR}_{\tilde{k},\tilde{j}}^{\infty} = \gamma \left(\frac{\varepsilon}{(1 + \varepsilon\Lambda)^2} + \frac{1}{(1 + \Lambda)^2} \right), \quad (\text{C.35})$$

Finally, by substituting (C.34) and (C.35) into (4.22), we obtain $R_{s,\text{CBf}}^{\infty}$ for $\alpha \neq 0$ in (4.24). If $\alpha = 0$, we derive the desired result in (4.24) by calculating $R_{s,\text{CBf}}^{\infty}(\alpha = 0) = \lim_{\alpha \rightarrow 0} R_{s,\text{CBf}}^{\infty}$. This completes the proof of Theorem 4.2.

Appendix D

D.1 Proof of Proposition 5.2

To determine the maximum achievable secrecy throughput, we need first obtain the optimal rate parameters that maximize the secrecy throughput. The problem is formulated by

$$\begin{aligned} \max_{R_b, R_s} \quad & \eta = \exp\left(-\frac{2^{R_b} - 1}{\tilde{\gamma}_b}\right) R_s, & (D.1) \\ \text{s.t.} \quad & R_b \geq R_s > 0. & (D.2) \end{aligned}$$

Given any R_s , we find that $\partial\eta/\partial R_b$ is always less than 0. Hence given any R_s , it is wise to have the minimum R_b , i.e., $R_b = R_s$, for maximizing η . Then, the problem changes to

$$\begin{aligned} \max_{R_s} \quad & \eta(R_b = R_s) = \exp\left(-\frac{2^{R_s} - 1}{\tilde{\gamma}_b}\right) R_s, & (D.3) \\ \text{s.t.} \quad & R_s > 0. & (D.4) \end{aligned}$$

Taking the first order derivative of $\eta(R_b = R_s)$ with respect to R_s , we have

$$\frac{\partial\eta(R_b = R_s)}{\partial R_s} = \exp\left(-\frac{2^{R_s} - 1}{\tilde{\gamma}_b}\right) \left(1 - \frac{2^{R_s} R_s \ln 2}{\tilde{\gamma}_b}\right) \quad (D.5)$$

By solving for R_s in $\frac{\partial\eta(R_b = R_s)}{\partial R_s} = 0$, we obtain the optimal value of R_s that maximizes η , which is given by

$$R_s^\circ = \frac{W_0(\tilde{\gamma}_b)}{\ln 2}. \quad (D.6)$$

Finally, substituting $R_s = R_s^\circ$ into (D.3) completes the proof of Proposition 5.2.

D.2 Proof of Proposition 5.3

As analyzed in Appendix D.1, given any R_s , it is wise to have the minimum R_b , i.e., $R_b = R_s$, for maximizing η . Hence, we can obtain the feasible range of R_s for satisfying the throughput

constraint by solving R_s to the equation $\eta(R_b = R_s) = \Gamma$. The feasible range is given by $R_{s,\min} \leq R_s \leq R_{s,\max}$.

From $p_{\text{out}} = \exp\left(-\frac{2^{R_b - \theta R_s} - 1}{\bar{\gamma}_e}\right)$, we find that minimizing p_{out} is equivalent to maximizing

$$O_1 = R_b - \theta R_s. \quad (\text{D.7})$$

To minimize O_1 in (D.7), it is wise to have the maximum R_b while satisfying the throughput constraint, for any given R_s . From $\eta = \exp\left(-\frac{2^{R_b} - 1}{\bar{\gamma}_b}\right) R_s \geq \Gamma$, we have

$$R_b \leq \log_2 \left(1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_s} \right). \quad (\text{D.8})$$

Hence, we obtain R_{b1}^* as (5.31). Then, we can rewrite the optimization problem as

$$\max_{R_s} \quad \log_2 \left(1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_s} \right) - \theta R_s, \quad (\text{D.9})$$

$$\text{s.t.} \quad R_{s,\min} \leq R_s \leq R_{s,\max}. \quad (\text{D.10})$$

Finally, by solving for R_s in the equation $\frac{\partial O}{\partial R_s} = 0$ and considering the feasible range of R_s , we obtain R_{s1}^* as (5.32). This completes the proof of Proposition 5.3.

D.3 Proof of Proposition 5.4

The feasible range of R_s for satisfying the throughput constraint is given as $R_{s,\min} \leq R_s \leq R_{s,\max}$.

From $\bar{\Delta} = 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{2^{R_b - R_s}}{\bar{\gamma}_e}\right) \right)$, we find that maximizing $\bar{\Delta}$ is equivalent to minimizing

$$O_2 = \frac{1}{R_s} \left(\text{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{2^{R_b - R_s}}{\bar{\gamma}_e}\right) \right). \quad (\text{D.11})$$

Given any R_s , we have

$$\frac{\partial O_2}{\partial R_b} = \frac{\ln(2)}{R_s} \left(\exp\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \exp\left(-\frac{2^{R_b - R_s}}{\bar{\gamma}_e}\right) \right) < 0. \quad (\text{D.12})$$

Hence given any R_s , it is wise to have the maximum R_b while satisfying the throughput constraint to minimize O_2 in (D.11). Hence, we obtain R_{b2}^* as (5.34). Then, we rewrite the optimization problem as

$$\min_{R_s} \quad \frac{1}{R_s} \left(\text{Ei}\left(-\frac{1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_s}}{\bar{\gamma}_e}\right) - \text{Ei}\left(-\frac{1 - \bar{\gamma}_b \ln \frac{\Gamma}{R_s}}{\bar{\gamma}_e 2^{R_s}}\right) \right), \quad (\text{D.13})$$

$$\text{s.t.} \quad R_{s,\min} \leq R_s \leq R_{s,\max}. \quad (\text{D.14})$$

We find that the closed-form solution of R_{s2}^* is mathematically intractable. We can obtain R_{s2}^* by numerically solving the problem above. This completes the proof of Proposition 5.4.

Bibliography

- [1] Cisco, “Cisco visual networking index: global mobile data traffic forecast update, 2014–2019,” *Inc. White Paper*, Feb. 2015. (cited on page 1)
- [2] M. Monahan and D. V. Dyke, “Mobile online retail payments forecast 2015,” *Javelin Strategy and Research, Report*, July 2015. (cited on page 1)
- [3] B. Schneier, “Cryptographic design vulnerabilities,” *IEEE Computer*, vol. 31, no. 9, pp. 26–33, Sept. 1998. (cited on page 1)
- [4] G. Kapoor and S. Piramithu, “Vulnerabilities in some recently proposed rfid ownership transfer protocols,” *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 260–262, Mar. 2010. (cited on page 1)
- [5] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, “Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures,” *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012. (cited on page 1)
- [6] Y. Liang, H. V. Poor, and S. Shamai, “Information theoretic security,” *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4-5, pp. 355–580, 2008. (cited on page 1)
- [7] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, Norwell, 2009. (cited on page 1)
- [8] E. Jorswieck, A. Wolf, and S. Gerbracht, *Secrecy on the Physical Layer in Wireless Networks*. Telecommunications, In-Tech Publishers, 2010. (cited on page 1)
- [9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011. (cited on pages 1 and 91)
- [10] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013. (cited on page 1)
- [11] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008. (cited on page 2)
- [12] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949. (cited on page 2)

- [13] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975. (cited on pages 3, 4, 24, 89, 91, and 95)
- [14] I. Csiszár, "Almost independence and secrecy capacity," *Prob. Inf. Trans.*, vol. 32, no. 1, pp. 40–47, Jan. 1996. (cited on page 3)
- [15] 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. (cited on pages 4, 51, 91, 92, and 96)
- [16] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008. (cited on pages 4, 5, 6, 13, and 20)
- [17] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE ISIT*, Adelaide, SA, Sept. 2005, pp. 2152–2155. (cited on page 5)
- [18] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, WA, July 2006, pp. 356–360. (cited on page 5)
- [19] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011. (cited on pages 5, 6, 13, 25, 95, and 96)
- [20] Z. Rezk, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, Nov. 2011, pp. 952–957. (cited on page 6)
- [21] 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. (cited on page 6)
- [22] 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. (cited on page 6)
- [23] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proc. IEEE ICC*, June 2014, pp. 987–992. (cited on page 6)
- [24] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003. (cited on page 7)

-
- [25] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014. (cited on page 7)
- [26] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC*, vol. 3, Dallas, TX, Sept. 2005, pp. 1906–1910. (cited on page 7)
- [27] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008. (cited on pages 7, 11, 45, and 50)
- [28] 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. (cited on pages 8, 11, 19, 20, and 45)
- [29] 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. (cited on page 8)
- [30] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013. (cited on page 8)
- [31] 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. (cited on pages 8, 10, and 19)
- [32] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012. (cited on page 8)
- [33] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440. (cited on page 8)
- [34] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE SPAWC Workshop*, Perugia, Italy, June 2009, pp. 344–348. (cited on page 8)
- [35] —, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Allerton Conf. Commun., Control Computing*, Monticello, IL, Oct. 2009, pp. 1134–1140. (cited on page 8)
- [36] J. M. Taylor, M. Hempel, H. Sharif, S. Ma, and Y. Yang, "Impact of channel estimation errors on effectiveness of eigenvector-based jamming for physical layer security in

- wireless networks,” in *Proc. IEEE CAMAD Workshop*, Kyoto, Japan, June 2011, pp. 122–126. (cited on pages 8, 19, and 20)
- [37] A. Mukherjee and A. L. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011. (cited on pages 8, 10, 11, 19, and 45)
- [38] T.-Y. Liu, S.-C. Lin, T.-H. Chang, and Y.-W. P. Hong, “How much training is enough for secrecy beamforming with artificial noise,” in *Proc. IEEE ICC*, Ottawa, ON, June 2012, pp. 4782–4787. (cited on pages 8, 19, and 20)
- [39] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “Multiple-input multiple-output Gaussian broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sept. 2010. (cited on page 9)
- [40] D. A. A. Fakoorian and A. L. Swindlehurst, “MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sept. 2011. (cited on page 9)
- [41] 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. (cited on pages 9, 67, and 70)
- [42] G. Geraci, J. Yuan, and I. B. Collings, “Large system analysis of the secrecy sum-rates with regularized channel inversion precoding,” in *Proc. IEEE WCNC*, Apr. 2012, pp. 533–537. (cited on page 9)
- [43] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, “Large system analysis of linear precoding in MISO broadcast channels with confidential messages,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sept. 2013. (cited on pages 9, 67, 70, 71, 76, and 84)
- [44] G. Geraci, A. Y. Al-Nahari, J. Yuan, and I. B. Collings, “Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation,” *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1164–1167, June 2013. (cited on pages 9, 67, and 70)
- [45] N. Yang, G. Geraci, J. Yuan, and R. Malaney, “Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks,” *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, July 2014. (cited on pages 9, 67, 70, and 71)
- [46] D. W. K. Ng, E. S. Lo, and R. Schober, “Resource allocation for secure OFDMA networks with imperfect CSIT,” in *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011, pp. 1–6. (cited on pages 10 and 19)

-
- [47] 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. (cited on pages 10 and 19)
- [48] 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. (cited on pages 10 and 19)
- [49] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010. (cited on pages 11 and 45)
- [50] —, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010. (cited on pages 11 and 45)
- [51] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011. (cited on pages 11 and 45)
- [52] 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. (cited on pages 11 and 45)
- [53] 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. (cited on pages 11 and 45)
- [54] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. J. Kwak, “LDPC codes for the Gaussian wiretap channel,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sept. 2011. (cited on page 12)
- [55] M. Baldi, M. Bianchi, and F. Chiaraluce, “Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, June 2012. (cited on page 12)
- [56] K. Guan, P. J. Winzer, A. M. Tulino, and E. Soljanin, “An error probability approach for quantifying physical layer security of MIMO-SDM systems,” in *Proc. Eur. Conf. Opt. Commun.*, Sept. 2014, pp. 1–3. (cited on page 12)
- [57] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, “Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel,” in *Proc. IEEE ICC Workshops*, June 2015, pp. 446–451. (cited on page 12)

- [58] D. Gesbert, S. Hanly, H. Huang, S. S. Shitz, O. Simeone, and W. Yu, "Multi-cell MIMO cooperative networks: A new look at interference," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 9, pp. 1380–1408, Dec. 2010. (cited on page 15)
- [59] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication—Part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005. (cited on pages 15 and 71)
- [60] R. Zakhour and S. Hanly, "Base station cooperation on the downlink: Large system analysis," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2079–2106, Apr. 2012. (cited on pages 15, 69, and 73)
- [61] X. Zhou, P. Sadeghi, T. A. Lamacchia, and S. Durrani, "Design guidelines for training-based MIMO systems with feedback," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 4014–4026, Oct. 2009. (cited on page 19)
- [62] L. H. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 2, pp. 359–378, May 1994. (cited on page 20)
- [63] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ: PTR Prentice Hall, 1993. (cited on page 22)
- [64] J. K. Cavers, "An analysis of pilot symbol assisted modulation for Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 40, no. 4, pp. 686–693, Nov. 1991. (cited on page 22)
- [65] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003. (cited on page 22)
- [66] A. Vakili, M. Sharif, and B. Hassibi, "The effect of channel estimation error on the throughput of broadcast channels," in *Proc. IEEE ICASSP*, vol. 4, Toulouse, France, May 2006. (cited on page 22)
- [67] A. Thangaraj, S. Doherty, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007. (cited on page 24)
- [68] X. Tang, R. Liu, Sapsojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1590, Apr. 2009. (cited on page 24)

-
- [69] J. I. Marcum, *Table of Q Functions*. U.S. Air Force Project RAND Research Memorandum M-339, ASTIA Document AD 1165451, Rand Corporation, Santa Monica, CA, 1950. (cited on page 29)
- [70] T. S. Pollock, “On limits of multi-antenna wireless communications in spatially selective channels,” Ph.D. dissertation, The Australian National University, Australia, July 2003. [Online]. Available: <http://hdl.handle.net/1885/47999> (cited on pages 46, 52, and 117)
- [71] E. G. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, “Massive MIMO for next generation wireless systems,” *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014. (cited on page 46)
- [72] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, “What will 5G be?” *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, June 2014. (cited on page 46)
- [73] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, “Introducing space into MIMO capacity calculations,” *J. Telecommun. Syst.*, vol. 24, no. 2, pp. 415–436, Oct. 2003. (cited on page 46)
- [74] T. D. Abhayapala, R. A. Kennedy, and J. T. Y. Ho, “On capacity of multi-antenna wireless channels: Effects of antenna separation and spatial correlation,” in *Proc. IEEE AusCTW*, Canberra, Australia, Feb. 2002, pp. 4–5. (cited on page 46)
- [75] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, “Introducing ‘space’ into space-time MIMO capacity calculations: A new closed form upper bound,” in *Proc. ICT*, vol. 2, Feb. 2003, pp. 1536–1541. (cited on page 46)
- [76] R. A. Kennedy, P. Sadeghi, T. D. Abhayapala, and H. M. Jones, “Intrinsic limits of dimensionality and richness in random multipath fields,” *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 2542–2556, June 2007. (cited on page 46)
- [77] F. Bashar and T. D. Abhayapala, “Degrees of freedom of band limited signals measured over space,” in *Proc. ISCIT*, Oct. 2012, pp. 735–740. (cited on page 46)
- [78] F. Bashar, S. M. A. Salehin, and T. D. Abhayapala, “Analysis of degrees of freedom of wideband random multipath fields observed over time and space windows,” in *Proc. IEEE Workshop SSP*, June 2014, pp. 45–48. (cited on page 46)
- [79] —, “Band limited signals observed over finite spatial and temporal windows: An upper bound to signal degrees of freedom,” submitted to *IEEE Trans. Signal Process.*, 2014. [Online]. Available: <http://arxiv.org/abs/1405.2163> (cited on page 46)

- [80] D. Gesbert, T. Ekman, and N. Christophersen, "Capacity limits of dense palm-sized MIMO arrays," in *Proc. IEEE GLOBECOM*, vol. 2, Nov. 2002, pp. 1187–1191. (cited on page 52)
- [81] L. Hanlen and M. Fu, "Capacity of MIMO wireless systems with spatially correlated receive elements," in *Proc. WITSP*, Wollongong, Australia, Dec. 2002, pp. 1–6. (cited on page 52)
- [82] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, "Antenna saturation effects on MIMO capacity," in *Proc. IEEE ICC*, vol. 4, May 2003, pp. 2301–2305. (cited on page 52)
- [83] Y. Wu and Z. Nie, "On the MIMO channel capacity saturation for spatially constrained receive region," *J. Systems Engineering Electronics*, vol. 18, no. 3, pp. 437–442, Sept. 2007. (cited on page 52)
- [84] R. Muharar, R. Zakhour, and J. Evans, "Base station cooperation with feedback optimization: A large system analysis," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3620–3644, June 2014. (cited on pages 69, 79, 80, 124, and 125)
- [85] H. Dahrouj and W. Yu, "Coordinated beamforming for the multicell multi-antenna wireless system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1748–1759, May 2010. (cited on page 73)
- [86] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for down-link spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004. (cited on page 83)
- [87] H. Sung, S.-R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489–3499, Nov. 2009. (cited on page 83)
- [88] Z. Shen, R. Chen, J. G. Andrews, R. W. Heath, and B. L. Evans, "Low complexity user selection algorithms for multiuser MIMO systems with block diagonalization," *IEEE Trans. Signal Process.*, vol. 54, no. 9, pp. 3658–3663, Sept. 2006. (cited on page 83)
- [89] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978. (cited on page 89)
- [90] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley, 2006. (cited on pages 89 and 91)
- [91] M. Feder and N. Merhav, "Relations between entropy and error probability," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 259–266, Jan. 1994. (cited on pages 89 and 91)

-
- [92] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008. (cited on pages 92 and 96)
- [93] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013. (cited on page 95)
- [94] J. Kiefer, "Sequential minimax search for a maximum," *Proc. Amer. Math. Soc.*, vol. 4, no. 3, pp. 502–506, 1953. (cited on page 103)
- [95] X. Zhou, P. Sadeghi, T. A. Lamahewa, and S. Durrani, "Optimizing antenna configuration for MIMO systems with imperfect channel estimation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1177–1181, Mar. 2009. (cited on page 110)
- [96] M. Haenggi, J. 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, Sept. 2012. (cited on page 110)
- [97] F. Baccelli, B. Blaszczyzyn, and P. Miihlethaler, "Stochastic analysis of spatial and opportunistic ALOHA," *IEEE J. Select. Areas Commun.*, vol. 27, no. 7, pp. 1105–1119, Sept. 2009. (cited on page 110)
- [98] S. Weber and J. G. Andrews, *Transmission Capacity of Wireless Networks*, 1st ed. Now Publishers Inc., 2012. (cited on page 110)
- [99] S. Srinivasa and M. Haenggi, "Distance distributions in finite uniformly random networks: Theory and applications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010. (cited on page 110)
- [100] Z. Khalid and S. Durrani, "Distance distributions in regular polygons," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2363–2368, June 2013. (cited on page 110)
- [101] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012. (cited on page 110)
- [102] O. O. Koyluoglu, C. E. Koksall, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 3000–3015, May. 2012. (cited on page 110)
- [103] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013. (cited on page 110)

- [104] A. Bayesteh, M. Ansari, and A. K. Khandani, “Effect of jamming on the capacity of MIMO channels,” in *Proc. Allerton*, Oct. 2004, pp. 401–410. (cited on page 117)