Transmit Optimization Techniques for Physical Layer Security

Zheng Chu

Newcastle University

Newcastle upon Tyne, U.K.

A thesis submitted for the degree of

Doctor of Philosophy

July 2016

To my loving parents and relatives.

Acknowledgements

I would like to express my gratitude to my supervisor Prof. Zhiguo Ding for his first two-year support and interest in my research. I am grateful to him for providing me with great motivation, enthusiasm, technical insight and encouragement. I am extremely thankful to Dr. Kanapathippillai Cumanan for providing me with technical insight to study convex optimization which finally led to some good publications during my PhD study. Also, I would like to thank my two supervisors Dr. Martin Johnston and Dr. Stephane Le Goff for their valuable and continuous support and encouragement, and excellent contributing suggestion on my publications regardless of their busy schedule.

In addition, I am very grateful to my collaborators, Hong Xing and Zhengyu Zhu to their valuable discussions for my research. I am also grateful to all my friends in Communications, Sensors, Signal and Information Processing (ComS^{2}IP) Group for providing a stable environment. Very special and deep thanks go to Zhen Mei, Yuaiyi Zhao, Weichen Xiang, Yang Sun and Jamal Ahmed Hussein for being such a great friend always ready to listen and help me. I also want to thank my friends from China and UK. Finally, I am at loss to find suitable words that express my gratefulness for my parents and relatives for their continuous support, encouragement throughout my PhD.

Abstract

Over the last several decades, reliable communication has received considerable attention in the area of dynamic network configurations and distributed processing techniques. Traditional secure communications mainly considered transmission cryptography, which has been developed in the network layer. However, the nature of wireless transmission introduces various challenges of key distribution and management in establishing secure communication links. Physical layer security has been recently recognized as a promising new design paradigm to provide security in wireless networks in addition to existing conventional cryptographic methods, where the physical layer dynamics of fading channels are exploited to establish secure wireless links. On the other hand, with the ever-increasing demand of wireless access users, multi-antenna transmission has been considered as one of effective approaches to improve the capacity of wireless networks. Multi-antenna transmission applied in physical layer security has extracted more and more attentions by exploiting additional degrees of freedom and diversity gains.

In this thesis, different multi-antenna transmit optimization techniques are developed for physical layer secure transmission. The secrecy rate optimization problems (i.e., power minimization and secrecy rate maximization) are formulated to guarantee the optimal power allocation. First, transmit optimization for multiple-input single-output (MISO) secrecy channels are developed to design secure transmit beamformer that minimize the transmit power to achieve a target secrecy rate. Besides, the associated robust scheme with the secrecy rate outage probability constraint are presented with statistical channel uncertainty, where the outage probability constraint requires that the achieved secrecy rate exceeds certain thresholds with a specific probability. Second, multi-antenna cooperative jammer (CJ) is presented to provide jamming ser-

vices that introduces extra interference to assist a multiple-input multiple-output (MIMO) secure transmission. Transmit optimization for this CJ-aided MIMO secrecy channel is designed to achieve an optimal power allocation. Moreover, secure transmission is achieved when the CJ introduces charges for its jamming service based on the amount of the interference caused to the eavesdropper, where the *Stackelberg* game is proposed to handle, and the *Stackelberg* equilibrium is analytically derived. Finally, transmit optimization for MISO secure simultaneous wireless information and power transfer (SWIPT) is investigated, where secure transmit beamformer is designed with/without the help of artificial noise (AN) to maximize the achieved secrecy rate such that satisfy the transmit power budget and the energy harvesting (EH) constraint. The performance of all proposed schemes are validated by MATLAB simulation results.

Contents

List of Figures

List of Tables

Nomenclature

Symbols

$(\cdot)^*$	Complex Conjugate
$(\cdot)^{-1}$	Inverse
$(\cdot)^H$	Hermitian Transpose
$(\cdot)^T$	Transpose
$[x]^+$	$\max\{x, 0\}$
$\Im\{\cdot\}$	Imaginary Part
$\lambda_{\max}(\cdot)$	Maximum Eigenvalue
$\mathbb{E}\{\cdot\}$	Statistical Expectation
$\mathbf{A} \succeq \mathbf{0}$	$\mathbf{A}$ is a Positive Semidefinite Matrix
$\mathbf{I}$	Identity Matrix
$\mathcal{L}(\cdot)$	Lagrange Dual Function
$\mid \mathbf{A} \mid$	Determinant of $\mathbf{A}$
$\otimes$	Kronecker Products
$\|\cdot\|_F$	Frobenius Norm
$\|\cdot\|_2$	Euclidean Norm
$\Re\{\cdot\}$	Real Part
$\mathrm{Tr}(\cdot)$	Trace Operator
$\mathrm{Vec}(\mathbf{A})$	Vectorization of $\mathbf{A}$

$v_{\max}(\cdot)$	Maximum Eigenvalue

Acronyms/Abbreviations

1D	One-dimensional Search
2D	Two-dimensional Search
5G	Fifth-generation
AF	Amplify-and-Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BS	Base Station
CB	Cooperative Beamforming
CDF	Cumulative Density Function
CJ	Cooperative Jammer
CR	Cognitive Radio
CSI	Channel State Information
D2D	Device-to-Device
DF	Decode-and-Forward
DoF	Degrees of Freedom
EE	Energy Efficiency
ER	Energy Receiver
GP	Geometric Programming
GPS	Global Positioning System
GSVD	Generalized Singular Value Decomposition
IR	Information Receiver
KKT	Karush-Kuhn-Tucker

LHS	Left Hand Side
LMI	Linear Matrix Inequality
LP	Linear Programming
MAC	Medium Access Control
MIMO	Multiple-input Multiple-ouput
NOMA	Non-Orthogonal Multiple Access
OFDMA	Orthogonal Frequency-Division Multiple Access
PDF	Probability Density Function
PHY	Physical Layer
PSD	Positive Semidefinite
QCQP	Quadratically Constrained Quadratic Programming
QoS	Quality of Service
QP	Quadratic Programming
RF	Radio-Frequency
RHS	Right Hand Side
SCA	Successive Convex Approximation
SDP	Semidefinite Programming
SE	Spectral Efficiency
SEE	Secure Energy Efficiency
SI	Self-Interference
SISO	Single-input Single-output
SNR	Signal-to-Noise Ratio
SOC	Second-Order Cone
SOCP	Second-Order Cone Programming

SSE	Secure Spectral Efficiency
SVD	Singular Value Decomposition
SWIPT	Simultaneous Wireless Information Power Transfer
WSN	Wireless Sensor Network

Chapter 1

Introduction

Wireless communication techniques have experienced an explosive growth in the communication industry, capturing more and more attention in terms of research [1, 2]. As such, there are various state-of-the-art applications such as wireless sensor network (WSN), WIFI, global positioning system (GPS), remote surveillance system, smart grids, etc., which are emerging from theoretical research ideas through to commercialisation. The exponential progress of these applications has driven the development of wireless electronic devices, such as mobile phones, laptop computers, etc., which promise a bright future for wireless networks. An increasing number of wireless customers has resulted into huge demands for the limited spectrum resources available, such that wireless services are becoming overloaded. In order to meet with these ever-increasing demands, some novel techniques and approaches need to be developed for future wireless communication networks.

There are three criteria that are associated with such demands: quality of service (QoS), energy efficiency (EE) and security, which have been widely considered as the main driving forces for the evolutions of wireless communication networks. Traditionally, these requirements can be satisfied by increasing the transmission bandwidth and the transmit power. However, frequency reuse becomes a novel approach to serve an increasing number of users within the availability of extreme scarce radio spectrum. Hence, it will not be always a good solution to increase transmit power as it will increase the co-channel interference power. In addition, power saving in cellular networks not only alleviates financial burden to service providers, but also reduces the emission of the greenhouse gases effectively. Therefore, a better system design that fully exploits the limited spectral resource is essential.

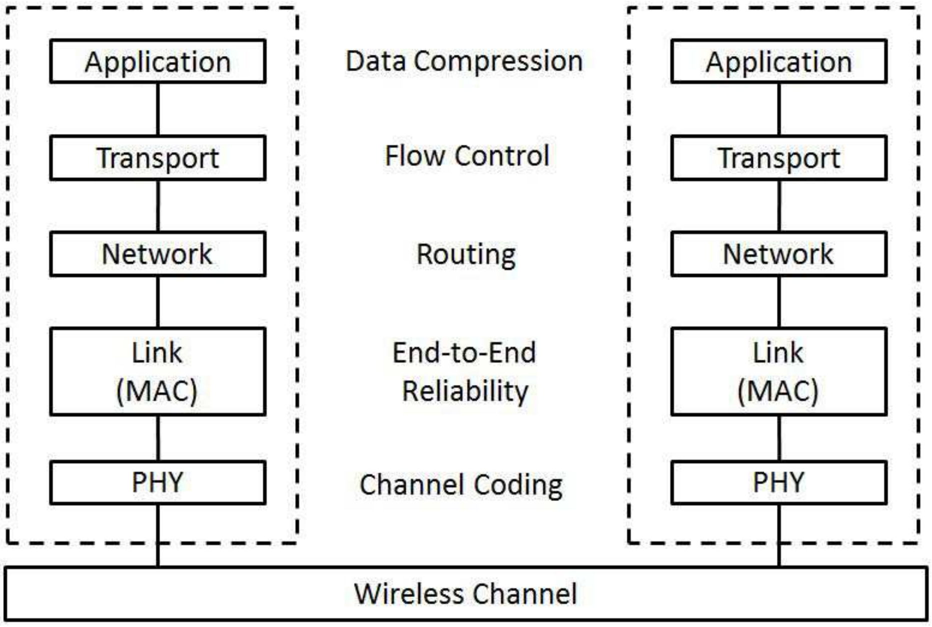

Figure 1.1: Layer protocol

1.1 Wireless Security Motivations

Security, as one of the most important criteria in wireless networks, plays a very significant role in wireless communications, ensuring that some important messages are confidential enough to prevent eavesdropping from unauthorized users. There are three main reasons leading to the security issues: First of all, wireless channels are vulnerable to channel jamming, so that an eavesdropper can easily jam and prevent legitimate users from accessing the network. This threat is more difficult to counter as it aims at disrupting traffic and not intercepting information. Secondly, an active attacker can obtain illegal access to the important network resources and bypass secure infrastructures (i.e., firewalls) without the authentication mechanisms. Finally, eavesdropping can be performed without advanced technological devices due to the open nature of wireless channels [3]. In principle, even legitimate users in wireless networks could be considered as potential eavesdroppers [3]. Based on the aforementioned security issues, solutions can be adopted in different layers. Fig. 1.1 shows the different layer protocols taken into consideration in wireless communications and their functions. Channel coding and spread-spectrum modulation techniques are implemented at the Physical (PHY) layer, and guarantee that all the upper layers operate in an error-free environment as well as mitigate channel jamming, respectively. In addition, admission control is tackled at the Medium Access Control (MAC) layer, where authentication mechanisms are implemented to prevent illegal

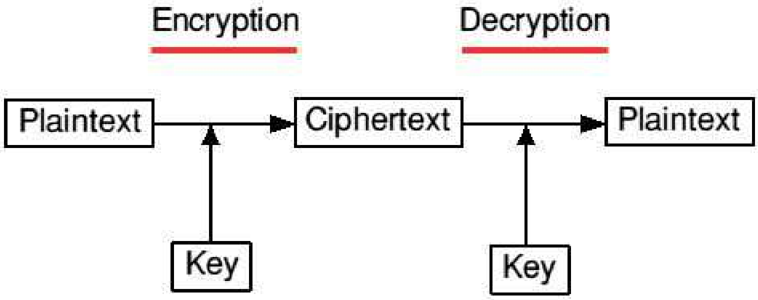

Figure 1.2: Encryption diagram

access and message encryption is implemented at the Application layer [3].

Traditionally, confidential processing is usually achieved in the network layer of wireless networking, like the widely adopted cryptography [4]. Fig. 1.2 shows a conventional and simple cryptographic method that is generally implemented by encrypting the plain message by employing private encryption keys available to the legitimate user who employs these keys to decrypt this message. It is assumed that these keys are computationally intractable for the adversary to decrypt if these encryption keys are not available by the adversary. However, the existing cryptographic methods cannot handle these scenarios due to high computer computational capabilities and cracking of encryption algorithms. Additionally, variety of challenges are introduced in terms of key distribution and management to establish secure communication links with the nature of wireless transmission [5].

Based on these above challenges, there exists the question of how to solve the security problem of the eavesdropping at the PHY layer. Unlike cryptography that the difference is ignored between the received signals at different receivers, physical layer security is considered by exploiting the difference in the properties of physical channels to achieve unconditional security. As such, physical layer security is usually performed by information theory principle, which is currently widely considered as a stronger notion than computational security. The explosive growth of wireless applications, coupled with information privacy will indicate a bright future for physical layer security.

However, with the ever-increasing demand of wireless access users, multi-antenna transmission has been considered as one of effective approaches to improve the capacity of wireless networks [6–9]. Multi-antenna transmission techniques can be applied in physical layer security to bring more degrees of freedom (DoF) and diversity gains. Moreover, low complexity transceiver will be designed by employing convex optimization techniques with and without global channel state information (CSI). How to achieve the secure communications to satisfy spectral and energy efficiency in multi-antenna transmission has been a hot research topic in wireless communication. In this thesis, novel algorithms for the optimal resource allocation for multi-antenna transceiver will be designed to realize spectral efficient, energy efficient, and secure communication networks by utilizing mathematical optimization techniques and game theory.

1.2 Literature Review

In recent years, physical layer security has paid significant attention in establishing reliable wireless links to prevent eavesdropping from illegal customers [10, 11]. Traditionally, secure communications are realized through traditional cryptographic methods performed in the network layer. However, with the nature of wireless transmission, various challenges are introduced in terms of key distribution and management [12]. Physical layer security technique provides a fundamentally different paradigm, compared to conventional cryptographic approaches, in which secrecy capacity is achieved by exploiting the physical layer properties of wireless communication system [13]. The concept of physical layer security was originally proposed by initially defining wiretap channels in [14], and has recently been recognized as a promising technique to establish secure data transmission between legitimate transceivers, which has been developed based on information theory principle [5,12,15,16]. Recently, secret communication for multi-antenna secrecy channels has attracted the research community due to the advantage of having additional DoF and diversity gains, and the achieved secrecy rates are constrained by the information rates achieved by the eavesdroppers [17, 18].

Several approaches and algorithms have been introduced to improve the secrecy rates, which consists of cooperative beamforming (CB), artificial noise (AN), cooperative jamming (CJ), and device-to-device (D2D) transmission, etc. [11, 19–32]. Convex optimization techniques have often been employed to design the optimal transmit beamformer by solving the secrecy rate optimization problems (i.e., power minimization and secrecy rate maximization) [19]. Relays and jamming nodes are introduced in the secure network, which have the capability to improve performance at the legitimate receiver, preventing the eavesdroppers from intercepting the desired messages intended for the legitimate receivers [23, 33–37]. Moreover, secrecy rate maximization algorithm has been proposed for multiple-input multiple-output (MIMO) wiretap channel, which provides the necessary sufficient conditions based on the optimal input covariance matrix [38], whereas in [39] a full-rank optimal input covariance matrix solution was presented to achieve the secrecy capacity of the MIMO Gaussian wiretap channel. CB requires relays to forward the signal from the source to the legitimate user based on the assumption that the direct transmission is not available. The optimal power allocation in the context of a decode-and-forward (DF) scheme has been proposed to maximize the sum secrecy rate [20], whereas in [21] the relay relies on an amplify-and-forward (AF) scheme in a MIMO system, where the source and relay beamformer have been jointly designed to maximize the achieved secrecy rate in the cooperative scheme. For MIMO relay networks, the optimal power allocation has been derived by exploiting the generalized singular value decomposition (GSVD)-based secure relaying scheme [22]. AN is also a well-known technique, which introduces the interference to eavesdroppers by embedding noise in the desired transmission signal [28, 29]. In [28], an *isotropic* AN scheme has been designed using an orthogonal projection approach, whereas the spatially selective AN algorithm is investigated to jointly design transmit beamformer and AN covariance matrix to interfere the eavesdroppers in [29]. CJ is another technique that can be applied to improve physical layer security [23–26]. For the single-antenna case, the secrecy rate has been maximized by employing a one-dimensional (1D) search algorithm [23]. In [24], first-order Taylor series expansion has been applied to approximate the secrecy capacity for MIMO secrecy channel with a multi-antenna CJ, which reformulate the non-convex secrecy rate optimization framework to a convex one, whereas the stochastic geometry approach is appropriate to the networks where the jammers and the eavesdroppers are deployed randomly [27]. Moreover, game theory is a promising mathematical tool for decision making and resource allocation in secure communications [40, 41].

In general, the CSI is assumed to be perfectly available at the transmitter between the transmitter and the legitimate receiver as well as the eavesdropper. However, it is not possible that this assumption is always valid with channel estimation and quantization errors. Without having the CSI at the legitimate transmitter, it is more challenging for the transmitter to perform optimization. To circumvent these issues of imperfection, robust optimization techniques have been considered to incorporate the channel uncertainty [19, 34, 42–48]. The robust optimization approaches have been applied in physical layer security based on the worst-case scheme [19,48,49]. The bridge has been built between wiretap channel and cognitive radio (CR) channel incorporating norm-bounded channel uncertainty [49]. In [19], the robust transmit covariance matrix has been designed for MISO secrecy channels with multiple multi-antenna eavesdroppers, and the robust optimization problem can be relaxed as semidefinite programming (SDP) by exploiting *S-Procedure*. In [48], a conservative approximation approach at low SNRs has been proposed for MIMO secrecy channel, whereas AN-assisted robust techniques has been developed in [29,47]. In [34], a robust CJ scheme has been proposed for secure channels based on the worst-case scheme. In addition to the robust secrecy rate optimization, the outage robust secrecy rate optimization schemes with only statistical knowledge of channel uncertainty have been considered in [32, 50]. The robust outage secrecy rate optimization for MIMO secrecy channel has been investigated in [32], where a *Bernstein-type* inequality based Taylor approximation was presented to handle the nonconvex outage secrecy rate constraint, while in [50], the outage probability minimization problem of a secrecy channel has been developed to satisfy a target secrecy rate with the assumption that the only distribution of the eavesdropper's channel error is available at the legitimate transmitter.

Energy harvesting is employed in fifth-generation (5G) wireless communication networks to circumvent the issue of energy limitations in mobile devices and improve the energy efficiency of these networks by extracting energy from the external natural environment (e.g., solar power, wind energy, etc.) [51, 52].

Traditionally, energy is directly harvested from external sources without exploiting the resources of the communication network itself. However, when the natural environment is not able to provide stable energy, wireless mobile receivers have to find an alternative energy source in the communication network. This source can be the information-carrying radio-frequency (RF) signal radiated by the fixed transmitters (base stations, hot spots, etc.) [53–55]. In this case, the role of the transmitter is not only to send the signal to the mobile receivers, but also transfer power that can be used to charge these receivers' batteries. Simultaneous wireless information and power transfer (SWIPT) is a promising paradigm to provide power for communication devices to mitigate the energy scarcity and extend the lifetime of wireless networks [53, 54].

Recently, secure communication in SWIPT has been investigated in [56–63]. In [56], the authors have considered a MISO secure SWIPT system. Two optimization problems: 1) secrecy rate maximization of information receiver (IR) with individual harvested energy constraints of energy receivers (ERs), 2) energy harvesting maximization with a secrecy rate constraint for the IR, have been developed to guarantee a reliable information transmission to the IR and the target harvested energy simultaneously transferred to the ERs are satisfied by optimally designing the beamformer vectors and the power allocation at the legitimate transmitter. In [58], the authors first addressed the secure communication system with SWIPT when two types of eavesdroppers (i.e., passive eavesdroppers and potential eavesdroppers) coexist. A total transmit power minimization problem was formulated to jointly optimize the transmit beamforming, AN and energy beamforming, achieving secure communications with a target amount of harvested power by incorporating channel uncertainties of the idle receivers (potential eavesdroppers). While [59] considered a multiuser MISO SWIPT system with multi-antenna energy harvesting receivers (potential eavesdroppers) only, where an energy harvesting maximization problem is proposed to guarantee secure communications. In addition, the authors have shown that there always exists a rank-one optimal transmit covariance solution and proposed one efficient algorithm to construct an equivalent rank-one optimal solution [56, 59]. However, in [56, 59], the CSI is assumed to be available, or only the CSI of the potential eavesdropper is unavailable at the transmitter [57,58], for which there are practical difficulties to obtain the CSI of the link between the transmitter and the users. Furthermore, robust secure transmission for a MISO SWIPT system have been proposed without AN [60] and with AN [61], respectively, by incorporating the channel uncertainties of all channels. In [60–62], semidefinite programming (SDP) relaxation has been studied to solve the secrecy rate maximization problem, however, the suboptimal solution has been proposed to guarantee the solution of the relaxed problem is rank-one [60], whereas in [61, 62], the authors have shown the optimal solution of the relaxed problem is rank-two, which is not exact to the optimal condition for the SDP relaxation. In [63], a two-step algorithm with conic reformulation is proposed to circumvent the rank-one solution in the MISO secure SWIPT system, while a novel SDP relaxation is investigated to guarantee that the relaxed problem yields rank-one solution in the AN-aided MISO secure SWIPT system. The optimal resource allocation in the AN-aided secure Orthogonal Frequency-Division

Multiple Access (OFDMA) systems with SWIPT was investigated in [64], where the weighted sum secrecy rate maximization problem of the IRs subject to minimum harvested power requirements of individual ERs, and a new frequency-domain AN-aided OFDMA-based SWIPT to facilitate both secrecy information transmission and energy transfer to IRs and ERs, respectively.

1.3 Main Contributions and Thesis Outline

1.3.1 Main Contributions

In this section, the main contributions in this thesis are presented, where different transmit optimization techniques are investigated to improve physical layer security. Secrecy rate optimization problems (i.e. power minimization and secrecy rate maximization) are formulated to design the secure transmit beamformer, achieving the optimal power allocation by mathematical optimization techniques and game theory.

Chapter 4 investigates the transmit optimization for MISO secure channels with multiple multi-antenna eavesdroppers. First, second-order cone programming (SOCP) reformulation is proposed to relax the power minimization problem. Additionally, a closed-form solution is derived for a special case with single multi-antenna eavesdropper by exploiting Karush-Kuhn-Tucker (KKT) conditions. Besides, the robust schemes with secrecy rate outage probability constraint are considered incorporating statistical channel uncertainty, where the outage probability constraint requires that the achieved secrecy rate exceeds certain thresholds with high probability such that naturally ensure the desired robustness. Due to nonconvex problem, a two-step algorithm with two conservative reformulations is proposed to reformulate it into a convex optimization framework. An initial proof shows the solution to each reformulated problem returns rank-one, which, therefore, guarantees that its solution is also optimal to the original problem.

Chapter 5 studies CJ-aided transmit optimization for MIMO wiretap channel, where a multi-antenna CJ is introduced to provide jamming service to introduce the extra interference to the eavesdropper. Both transmit covariance matrices of the legitimate transmitter and the CJ are designed, alternatively, to obtain the optimal power allocation for the secrecy rate optimization problems, where first-order Taylor approximation is considered to handle the nonconvex secrecy rate constraint. The robust scheme is formulated by incorporating norm-bounded channel uncertainty. By exploiting linear matrix transformation, it can be reformulated as convex optimization framework by employing SDP relaxation. Moreover, game theory based secure transmit optimization is developed when a private CJ is employed which charges for its jamming service according to the amount of interference caused to the eavesdropper. This scheme is modelled as a *Stackelberg* game, where the private CJ and the legitimate transmitter are the leader and follower of the game, respectively, and both of them are to maximize their own revenue functions. For the proposed game, *Stackelberg* equilibrium is analytically derived in terms of closed-form solutions.

Chapter 6 investigates transmit optimization for secure MISO SWIPT system. First, secure transmit beamformer are designed to maximize the achieved secrecy rate, subjecting to the transmit power and the EH constraint. A two-step algorithm with conic reformulation is considered to handle the nonconvex secrecy rate constraint, and first-order Taylor approximation is employed to linearize the EH constraint. In addition, AN-aided transmit optimization is considered to further improve the achieved secrecy rate. Secure transmit beamformer and AN are jointly designed. SDP relaxation based two-level optimization and successive convex approximation (SCA) are proposed to relax the secrecy rate maximization problem. Besides, it is shown that the relaxed problem yields a rank-one solution, which, therefore, guarantees that its solution is also optimal to the original problem.

1.3.2 Thesis Outline

Chapter 1 outlines the motivations of this thesis and literature review. Chapter 2 provides preliminaries. Chapter 3 introduces some basic concepts of convex optimization techniques. Some generic convex problems will be given. Additionally, the dual principle is provided by the Lagrange dual function, with KKT conditions. Chapter 4 investigates transmit optimization for MISO secure channel with multiple multi-antenna eavesdroppers. Chapter 5 investigates transmit optimization for CJ-aided MIMO secrecy channel, where a multi-antenna CJ is considered to provide the jamming service to improve secure communication. Chapter 6 investigates transmit optimization for secure MISO SWIPT system. Chapter 7 draws the conclusions, and summarizes future works.

1.4 Publications Lists

The novelty of this thesis is based on the following publications:

1.4.1 Journal Publications

1. **Z. Chu**, Z. Zhu, M. Johnston, and S. Le goff, "Simultaneous Wireless Information Power Transfer for MISO Secrecy Channel," *to appear in IEEE Trans. Vehicular Technol.*, 2015.

2. **Z. Chu**, H. Xing, M. Johnston, and S. Le Goff, "Secrecy Rate Optimizations for a MISO Secrecy Channel with Multiple multi-antenna Eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283-297, Jan. 2016.

3. **Z. Chu**, M. Johnston, and S. Le Goff, "SWIPT for Wireless Cooperative Networks," *Electron. Lett.,* vol. 51 no. 6, pp. 536-538, Mar. 2015.

4. **Z. Chu**, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Robust Outage Secrecy Rate Optimizations for a MIMO Secrecy Channel," *IEEE Wireless Commun. Lett.,* vol. 4, no. 1, pp. 86-89, Feb. 2015.

5. **Z. Chu**, K. Cumanan, M. Xu, and Z. Ding, "Robust Secrecy Rate Optimizations for Multiuser Multiple-Input Single-Output Channel with Device-to-Device Communications," *IET Commun.,* vol. 9, no. 3, pp. 396-403, Feb. 2015.

6. **Z. Chu**, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy Rate Optimizations for a MIMO Secrecy Channel with a Cooperative Jammer," *IEEE Trans. Vehicular Technol.,* vol. 64, no. 5, pp. 1833-1847, May 2015.

1.4.2 Conference Publications

1. **Z. Chu**, M. Johnston, and S. Le Goff, "Alternating Optimization for MIMO Secrecy Channel with a Cooperative Jammer," *in Proc. Vehicular Technology Conference (VTC-Spring)*, Glasgow, 2015.

2. **Z. Chu**, M. Johnston, and S. Le Goff, "Robust Beamforming Techniques for MISO Secrecy Communication with a Cooperative Jammer," *in Proc. Vehicular Technology Conference (VTC-Spring)*, Glasgow, 2015.

3. H. Xing, **Z. Chu**, Z. Ding, and A. Nallanathan, "Harvest-and-Jam:Improving Security for Wireless Energy Harvesting Cooperative Networks," *in Proc. IEEE GLOBECOM*, pp. 3145-3150, Dec. 2014.

4. Y. Yuan, **Z. Chu**, Z. Ding, K. Cumanan, and M. Johnston, "Joint Relay Beamforming and Power Splitting Ratio Optimization in a Multi-Antenna Relay Network," *in Proc. IEEE Wireless Communications and Signal Processing (WCSP),*, pp. 1-5, Oct. 2014.

5. **Z. Chu**, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy Rate Optimizations for a MIMO Secrecy Channel Based on Stackelberg Game," *in Proc. 22th European Signal Processing Conference (EUSIPCO)*, pp. 126-130, Sept. 2014.

Chapter 2

Preliminaries

This chapter outlines fundamental concepts and results of multi-antenna transmission and information-theoretical security techniques. First, multi-antenna wireless communications is studied, which includes multiple-input multiple-output (MIMO) wireless communications and beamforming techniques. Then the basic information-theoretical concepts are introduced briefly, which takes a three-node *wiretap channel* as an example. Unlike traditional approaches, which handle security at the network layer, physical layer security aims at developing effective secure communication schemes exploiting the properties of the physical layer, which plays a significant role in improving security performance from information-theoretical aspects. Finally, the information-theoretical security for multiple-antenna case will be investigated.

2.1 Multiple-Antenna Wireless Communications

Multiple-antenna transmission has been widely employed to improve the capacity of wireless networks, which has been investigated in [7, 8]. Both transmitter and receiver are equipped with multiple antennas in wireless systems, popularly known as MIMO, has been more attractive than single-input single-output (SISO) over the past decades with its powerful performance enhancing system capacity [9]. MIMO technology provides a new paradigm in wireless communication system design, which offers variety of advantages to satisfy the challenges posed by both the impairments in the wireless channel and resource constraints [9].

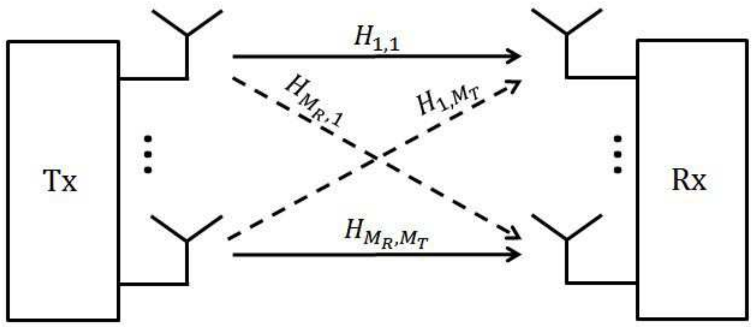

Figure 2.1: MIMO channel

2.1.1 MIMO Channel and Signal Model

In this section, the property of the MIMO channel is investigated to guarantee communication algorithms can be designed efficiently. Fig. 2.1 shows a MIMO system equipped with M_T transmit antennas and M_R receive antennas, it is assumed to be frequency-flat fading channel, the MIMO channel at a given time period is expressed as an $M_R \times M_T$ matrix

$$\mathbf{H} = \begin{bmatrix} H_{1,1} & \cdots & H_{1,M_T} \\ \vdots & \ddots & \vdots \\ H_{M_R,1} & \cdots & H_{M_R,M_T} \end{bmatrix}, \tag{2.1}$$

where $H_{m,n}$ denotes SISO channel gain between the m-th receive and n-th transmit antenna pair. In a frequency-flat fading MIMO channel, general MIMO received signal is expressed as

$$\mathbf{y} = \sqrt{\frac{P}{M_T}}\mathbf{H}\mathbf{x} + \mathbf{n}, \tag{2.2}$$

where $\mathbf{y} \in \mathbb{C}^{M_R \times 1}$ represents the received signal vector, $\mathbf{x} \in \mathbb{C}^{M_T \times 1}$ denotes the transmitted signal vector, $\mathbf{n} \in \mathbb{C}^{M_R \times 1}$ is additive white complex Gaussian noise with $\mathbb{E}\{\mathbf{n}\mathbf{n}^H\} = \sigma^2\mathbf{I}$, and P denotes the total average transmit power. The total transmit power during a symbol period can be written as the transmit covariance matrix $\mathbf{R} = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$ with $\mathrm{Tr}(\mathbf{R}) = P$. The signal-to-noise ratio (SNR) per receiver antenna can be denoted by $\rho = P/\sigma^2$.

2.2 Capacity Limits of of Wireless System

2.2.1 Mutual Information and Shannon Capacity

In this section, the backgrounds on Shannon capacity and mutual information will be introduced, and these ideas are applied to the single-user additive white Gaussian noise (AWGN) channel. The channel capacity was first proposed by Claude Shannon in the late 1940s, based on mutual information through the Shannon capacity limits [65]. The channel capacity, C, is the maximum rate at which secure communication can be guaranteed without any constraints on the transceiver complexity. It is shown by Shannon that for any rate $R < C$, there exist rate R channel codes with arbitrarily small symbol error probabilities. Thus, for any given rate $R < C$ and any desired non-zero probability of error P_e, there exists a rate R code to satisfy P_e. However, such channel codes may have a very long block length, and the encoding and decoding are extremely complicated. In the following, the precise mathematical definition of channel capacity will be given.

2.2.2 Mathematical Definition of Capacity

Shannon's initial work has shown that the channel capacity has been defined as the maximum rate to realize reliable communication. It can be simply described in terms of the mutual information between channel input and channel output. The simple channel model is composed of a random input X, a random output Y, and a probabilistic relationship between X and Y that is generally characterized by the conditional probability of Y given X ($f(y|x)$). The mutual information of a single-user channel can be defined as follows

$$I(X;Y) = \int_{S_x,S_y} f(x,y) \log \left(\frac{f(x,y)}{f(x)f(y)} \right) dxdy, \tag{2.3}$$

where the integral of S_x, S_y denotes the random variables X and Y, respectively, and $f(x)$, $f(x)$, and $f(x,y)$ denote the probability distribution function (PDF) of these random variables. The log function is generally with respect to base 2. Mutual information can be modified by the differential entropy of the channel output and conditional output as $I(X;Y) = h(Y) - h(Y|X)$, where $h(Y) = -\int_{S_y} \log f(y)dy$, and $h(Y|X) = -\int_{S_x,S_y} \log f(y|x)dxdy$. Shannon have shown that the channel capacity is equivalent to the mutual information maximization

$$C = \max_{f(x)} I(X;Y) = \int_{S_x,S_y} f(x,y) \log\left(\frac{f(x,y)}{f(x)f(y)}\right). \tag{2.4}$$

In this thesis, the time-invariant AWGN channel is considered, thus, the channel capacity can be expressed with bandwidth B and received SNR γ based on the assumption that $f(x)$ follows the Gaussian distribution as

$$C = B\log(1+\gamma) \text{ bps}. \tag{2.5}$$

2.3 Multi-Antenna Beamforming Techniques

In this section, we introduce a signal spatial filtering technique, also known as beamforming (beamformer), which can be achieved by combining elements from different phased angles. Beamforming is employed at the transmitter and receiver sides to achieve spatial selectivity. In addition, it can improve the transmit/receive gain.

2.3.1 MIMO Beamforming Design

In this subsection, the beamforming technique applied in MIMO system is studied, where the transmit and receive beamformers are designed jointly in most of existing works [66–68]. Either the data rate and/or the diversity performance is increased by employing multiple antennas. Also, multiplexing performance can be achieved by decomposing MIMO channel matrix into variety of independent sub-channels to realize different data streams transmission independently. It has the potential to increase the data rate up to a factor, same as the rank of the MIMO channel matrix, compared to the single-antenna system [1]. Consider a point-to-point MIMO system, in which the transmitter and the receiver consists of N_T and N_R transmit and receive antennas, respectively. The received signal can be expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{2.6}$$

where $\mathbf{y} = [y_1, ..., y_{N_R}]^T$, and y_{n_r} $(n_r = 1, ..., N_R)$ is the received signal at n_r-th receive antenna. $\mathbf{H} \in \mathbb{C}^{N_R \times N_T}$ denotes the MIMO channel matrix, and $h_{i,j}$ is the channel coefficients between the i-th transmit antenna and j-th receive antenna.

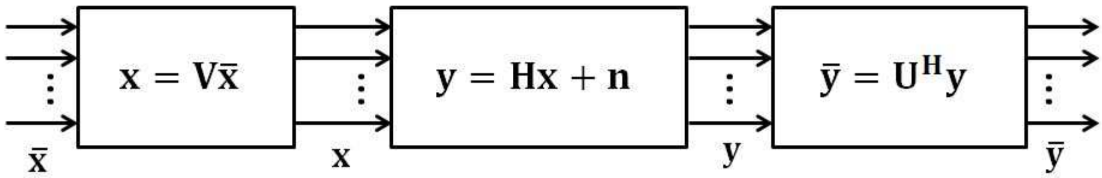

Figure 2.2: Transmit precoding and receiver shaping

$\mathbf{x} \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{n} \in \mathbb{C}^{N_R \times 1}$ are the transmitted signal vector and the noise vector, respectively. Assuming that the channel matrix $\mathbf{H}$ is available to both the transmitter and the receiver. The MIMO channel matrix is decomposed by the singular value decomposition (SVD) as [69]

$$\mathbf{H} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H, \tag{2.7}$$

where $\mathbf{U} \in \mathbb{C}^{N_R \times N_R}$, $\mathbf{V} \in \mathbb{C}^{N_T \times N_T}$ are unitary matrices, and $\boldsymbol{\Sigma} \in \mathbb{C}^{N_R \times N_T}$ is a diagonal matrix with the singular values δ_i of $\mathbf{H}$. N is the number of nonzero singular values, which is also known as the rank of $\mathbf{H}$. The singular value satisfies $\delta_i = \sqrt{\lambda_i}$, where λ_i denotes the i-th eigenvalue of $\mathbf{H}\mathbf{H}^H$. These sub-channels are achieved using linear transformation of the input signal and the output signal through transmit precoding and receive shaping. In transmit precoding, the symbol stream can be precoded as

$$\mathbf{x} = \mathbf{V}\bar{\mathbf{x}}, \tag{2.8}$$

where $\bar{\mathbf{x}}$ is the transmitted signal stream. While the received signal can be modified as

$$\bar{\mathbf{y}} = \mathbf{U}^H\mathbf{y}. \tag{2.9}$$

Fig. 2.2 shows that both transmit precoding and receiver shaping decompose the MIMO channel into N number of independent SISO channels as shown in Fig. 2.3, and the received signal can be expressed as

$$\bar{\mathbf{y}} \; = \mathbf{U}^H(\mathbf{H}\mathbf{x} + \mathbf{n}) = \mathbf{U}^H\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H\mathbf{V}\bar{\mathbf{x}} + \mathbf{U}^H\mathbf{n} = \boldsymbol{\Sigma}\bar{\mathbf{x}} + \bar{\mathbf{n}}, \tag{2.10}$$

where $\bar{\mathbf{n}} = \mathbf{U}^H\mathbf{n}$. Hence, this MIMO achieves up to N times data rate of an asso-

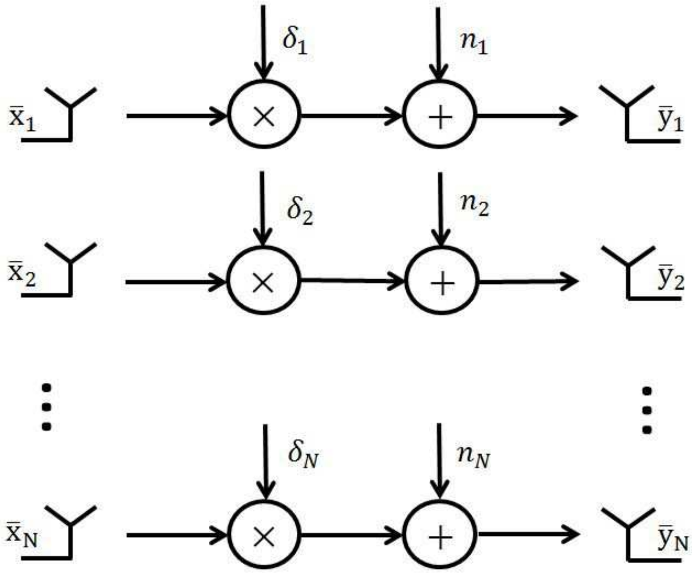

Figure 2.3: Parallel decomposition of the MIMO channel

ciated SISO channel. Each channel performance depends on δ_i. Thus, the transmit precoding and receiver shaping matrices also known as transmit and receiver beamformers. Provided that the MIMO channel matrix is known to the transmitter and the receiver, the channel capacity of this MIMO system is equivalent to the sum of capacities of each independent parallel channels.

$$C = \max_{p_i} \sum_{i=1}^{N} B \log\left(1 + \frac{\delta_i^2 p_i}{\sigma^2}\right), \; s.t. \sum_{i=1}^{N} p_i \leq P, p_i \geq 0, \tag{2.11}$$

where P and p_i are the total transmit power and power allocated to the i-th independent channel, respectively. B, δ_i and σ^2 are the bandwidth, the i-th independent channel coefficients and the noise power, respectively. By exploiting Karush-Kuhn-Tucker (KKT) conditions [70], the following relations hold:

$$\alpha_i \geq 0, \tag{2.12a}$$

$$\alpha_i p_i = 0, \tag{2.12b}$$

$$\left(\frac{B}{1 + \frac{\delta_i^2 p_i}{\sigma^2}}\right)\frac{\delta_i^2}{\sigma^2} + \alpha_i = \beta, \tag{2.12c}$$

where α_i and β are the dual multipliers of i-th individual power and total power constraints, respectively. From complementary slackness as in (2.12b) and (2.12c),

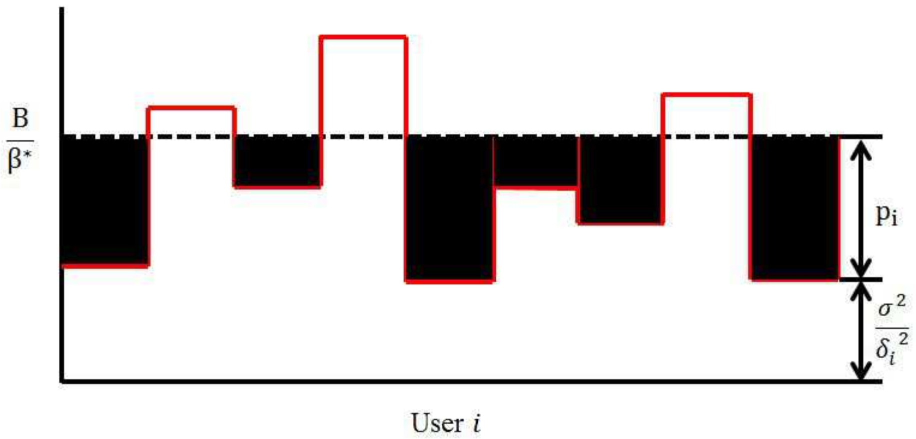

Figure 2.4: Water-filling power allocations.

the optimal power allocation is written in terms of closed-form solution as

$$p_i^* = \begin{cases} \left[\frac{B}{\beta} - \frac{\sigma^2}{\delta_i^2}\right]^+, \ \alpha_i = 0, \\ 0, \ \alpha_i \neq 0. \end{cases} \tag{2.13}$$

In addition, the optimal value of β is given by (2.14),

$$\sum_{i=1}^{N} \max\left\{0, \left(\frac{B}{\beta} - \frac{\sigma^2}{\delta_i^2}\right)\right\} = P, \tag{2.14}$$

which is known as the water-filling solution shown in Fig. 2.4, in which the water-level is equal to $\frac{B}{\beta^*}$. The parameter β^* is the optimal value of β, which can be obtained by solving the equation (2.14).

2.4 Information-theoretical Security

Information-theoretical security is a new paradigm that potentially strengthen the security of existing systems by introducing a level of information theory principle. This has been widely considered as a stronger notion than computational security [3, 5, 12, 17, 71].

2.4.1 Information-Theoretical Security

Information-theoretical security, mainly focuses on the secure transmission analysis based on the information theory principles [72], where this principle was first pro-

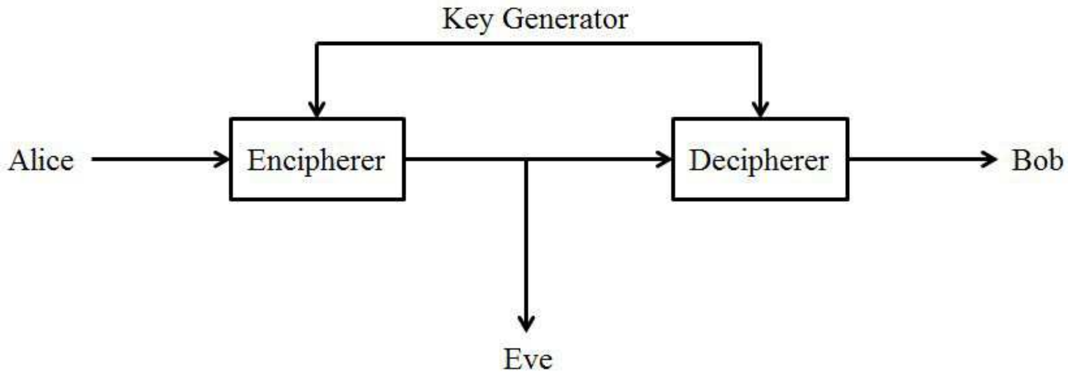

Figure 2.5: Shannon secrecy model

posed in communication theory, which introduced a Shannon secrecy model shown in Fig. 2.5. In this secrecy model, it consists of the legitimate transmitter (i.e., Alice), the legitimate user (i.e., Bob) and the eavesdropper (i.e., Eve). Eve can access to the insecure channel and eavesdrops the same messages to Bob by achieving the cryptogram C, where C is a function of the plaintext M and a secret key K, generated by key generator and shared by Alice and Bob. According to Shannon's definition, this system is perfect if the following equality holds

$$I(M;C) = 0,$$

which implies Eve has no knowledge of M with knowing C [3].

However, Shannon's secrecy system model leads to the fact that it is assumed that the channel from Alice to Eve has the same capacity as the channel from Alice to Bob, since Eve can access to the cryptogram perfectly. Therefore, the key is employed to guarantee perfect secrecy transmission is to modify Shannons model such that the Eve cannot achieve the same information as Bob.

Based on this motivation, a novel secrecy system, named *wiretap channel*, was initially proposed in [14], and then further developed in [73]. Fig. 2.6 shows a simple wiretap channel, where Alice transmits the confidential message to Bob, whereas Eve can access to the messages received by the legitimate receiver. In [73], a broadcast channel with confidential messages is described (c.f. Fig. 2.7), where Alice communicates with Bob via a *discrete broadcast channel* explained by a discrete input alphabet $\mathcal{X}$, two discrete output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, and a probability transition function $p_{YZ|X}(y, z|x)$. It is assumed that this channel is memoryless,

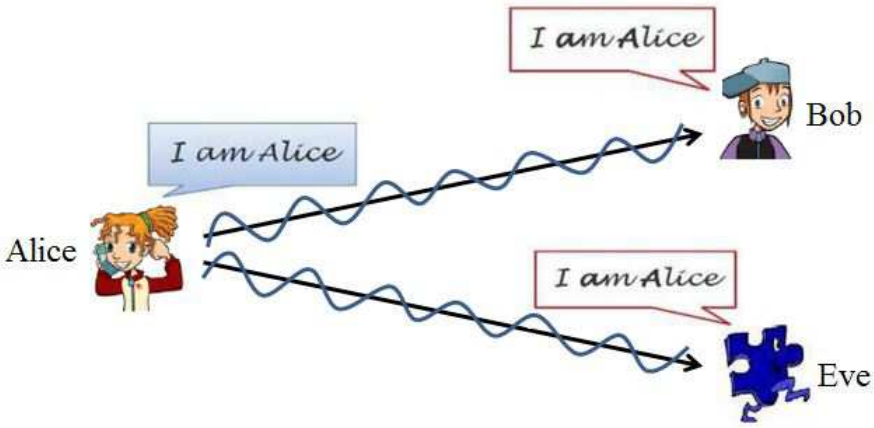

Figure 2.6: Simple wiretap channel

thus, the transition probability of a sequence of n symbols is expressed as

$$p(\mathbf{y}^n, \mathbf{z}^n|\mathbf{x}^n) = \prod_{i=1}^{n} p_{YZ|X}(y_i, z_i|x_i) \tag{2.15}$$

Alice sends a common message S_0 to both Bob and Eve as well as a private message S_M to Bob only.

Definition *A* $(2^{nR_0}, 2^{nR_M}, n)$ *code for the broadcast channel with confidential messages consists of the following statements:*

- *Two message sets* $\mathcal{S}_0 = \{1, 2, ..., 2^{nR_0}\}$ *and* $\mathcal{S}_M = \{1, 2, ..., 2^{nR_M}\}$.
- *An encoding function* $f_n : \mathcal{S}_0 \times \mathcal{S}_M \to \mathcal{X}^n$*, which maps each message pair* $(s_0, s_M) \in \mathcal{S}_0 \times \mathcal{S}_M$ *to a codeword* $\boldsymbol{x}^n \in \mathcal{X}^n$.
- *Two decoding functions* $g_n : \mathcal{Y}^n \to \mathcal{S}_0 \times \mathcal{S}_M$ *and* $h_n : \mathcal{Z}^n \to \mathcal{S}_0$*, which map an observation* $\boldsymbol{y}_n$ *to a message pair* $(\hat{s}_0, \hat{s}_M)$ *and an observation* $\boldsymbol{z}^n$ *to a message* $\tilde{s}_0$.

The confidential message S_M with respect to the eavesdropper is measured by *equivocation rate*:

$$\frac{1}{n} H(S_M|Z^n) \tag{2.16}$$

The rate set (R_0, R_M, R_E) is achieved rate for the broadcast channel with confidential

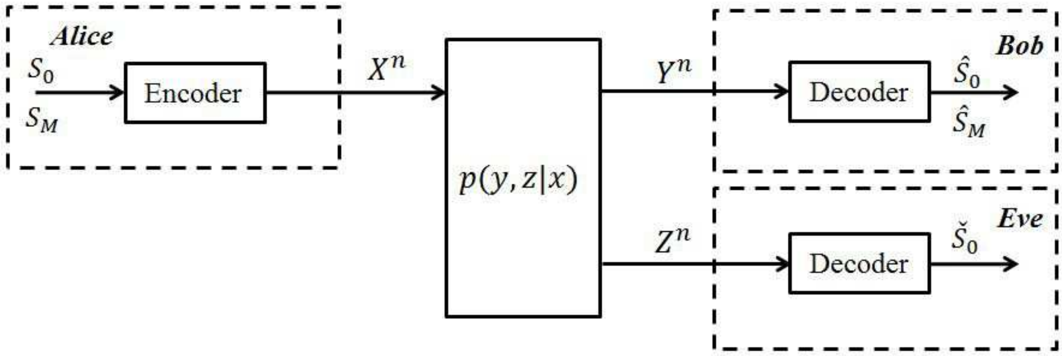

Figure 2.7: Broadcast wiretap channel with confidential message

message, if and only if, for any $\epsilon > 0$, there exists a $(2^{nR_0}, 2^{nR_M}, n)$ code such that

$$P[g_n(\mathbf{Y}^n) \neq (S_0, S_M) \text{ or } h_n(\mathbf{Z}^n \neq S_0)] < \epsilon,$$
$$\frac{1}{n}H(S_M|\mathbf{Z}^n) \geq R_E - \epsilon.$$

The above two inequalities represent reliability and secrecy conditions, which are not a *priori* obvious that both conditions are satisfied simultaneously. In addition, the trade-off between reliability and secrecy can be characterized exactly as shown in the following *theorem*.

Theorem 2.1 *[73, Theorem 1] The closed convex set of achievable rates (R_0, R_M, R_E) is given as follows:*

$$\mathcal{C} = \cup_{U \to V \to X \to YZ} \begin{cases} 0 \leq R_E \leq R_M, \\ R_E \leq I(V;Y|U) - I(V;Z|U), \\ R_0 + R_M \leq I(V;Y|U) + \min(I(U;Y), I(U;Z)), \\ 0 \leq R_0 \leq \min(I(U;Y), I(U;Z)). \end{cases} \tag{2.17}$$

From the above *theorem*, it is easy to define a metric characterization of the information-theoretical security for a channel, *secrecy capacity* of a broadcast channel with confidential messages, which can be defined as the upper bound of all rates R_M such that $(0, R_M, R_M)$ is achievable. This metric explains the usual channel capacity, which only considers reliable communications without secrecy constraints. Hence, the following *corollary* is considered:

Corollary 2.1 *[73, Corollary 2] In a broadcast channel with confidential messages,*

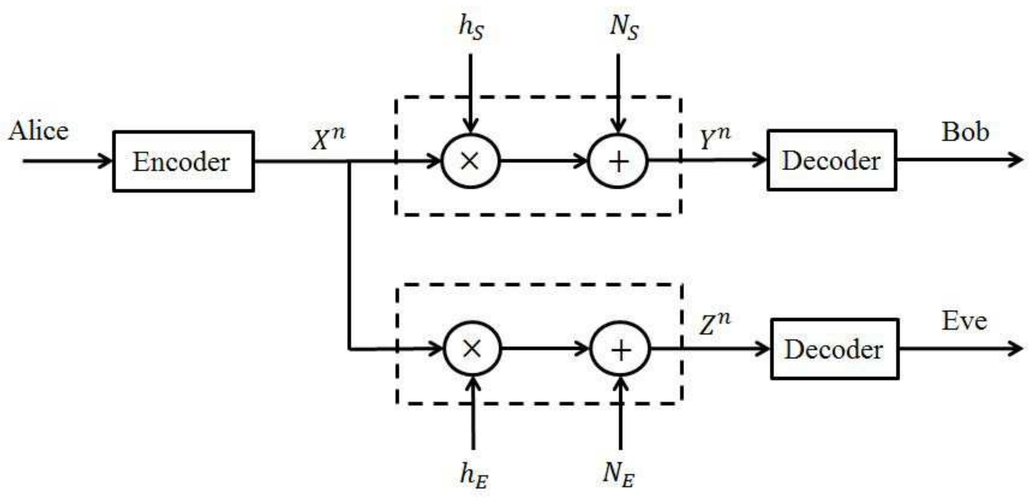

Figure 2.8: Gaussian wiretap channel

the secrecy capacity can be written as

$$C = \max_{V \to X \to YZ} [I(V;Y) - I(V;Z)]. \tag{2.18}$$

The secrecy capacity can be computed by the *Corollary* 2.1 for any discrete memoryless channel, and it can also be applied in continuous memoryless channels. The secrecy capacity is dependent on the channel transition probability only through the marginal probabilities $p_{Y|X}(y|x)$ and $p_{Z|X}(z|x)$. However, it employs the maximization to meet a Markov chain condition, which is not practical [3].

2.4.2 Gaussian Wiretap Channel

In this subsection, a simple, practical and useful wiretap channel is considered, *Gaussian wiretap channel*, which is described in Fig. 2.8. From this figure, it is assumed that both main and eavesdropping channels are additive white Gaussian noise (AWGN) channels with channel gains h_S and h_E, respectively, whereas the noise powers of these Gaussian noises N_S and N_E are denoted by σ_S^2 and σ_E^2, respectively. In addition, assuming that the messages transmitted over the channels are subject to the average transmit power constraint

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}(X_i) \leq P. \tag{2.19}$$

Based on these assumptions, the following *theorem* can be given:

Theorem 2.2 *[12, 71, 74] The secrecy capacity of the Gaussian wiretap channel is written as*

$$C = \left[\log\left(1 + \frac{h_S P}{\sigma_S^2}\right) - \log\left(1 + \frac{h_E P}{\sigma_E^2}\right) \right]^+. \tag{2.20}$$

Theorem 2.2 confirms that there exists a coding scheme guaranteeing information-theoretic security, if the legitimate receiver outperforms that of the eavesdropper in terms of SNR, and the maximum secrecy rate is the difference between the main channel capacity and the eavesdropping channel capacity.

2.5 Secure Communications for Multiple-Antenna Transceiver

In this section, secure communications for multiple-antenna cases are studied, where the transceivers (i.e., transmitter, receiver or/and eavesdropper) are equipped with multiple antenna. Multi-antenna secure communications have been widely focused in some existing works [17, 18, 48, 75, 76].

2.5.1 Transmit Optimization for MIMO Wiretap Channel

In this subsection, transmit optimization for MIMO wiretap channel is investigated [48], where a legitimate transmitter establishes a secure communication link with a legitimate user for data transmission with a multi-antenna eavesdropper. Assuming that the legitimate transmitter and the legitimate user consists of N_T transmit and N_R receive antennas, respectively, whereas the eavesdropper is equipped with N_E receive antennas. The channel coefficients between the legitimate transmitter and the legitimate receiver as well as the eavesdropper are represented by $\mathbf{H}_s \in \mathbb{C}^{N_T \times N_R}$ and $\mathbf{H}_e \in \mathbb{C}^{N_T \times N_E}$, respectively. The maximum transmit power available at the legitimate transmitter is denoted by P. The received signal at the legitimate user is written as

$$\mathbf{y}_s = \mathbf{H}_s^H \mathbf{x} + \mathbf{n}_s, \ \mathbf{y}_e = \mathbf{H}_s^H \mathbf{x} + \mathbf{n}_e, \tag{2.21}$$

where $\mathbf{x} \in \mathbb{C}^{N_T \times 1}$ denotes the desired signal intended to the legitimate receiver. The transmit covariance matrix is defined as $\mathbf{Q}_s = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$. The noises, $\mathbf{n}_s$ and $\mathbf{n}_e$, are set to be zero-mean circularly symmetric Gaussian random variables with covariances $\sigma_s^2\mathbf{I} \in \mathbb{C}^{N_R \times N_R}$ and $\sigma_e^2\mathbf{I} \in \mathbb{C}^{N_E \times N_E}$, respectively. The achievable transmission rate to the legitimate user and the eavesdropper can be expressed, respectively, as [7]

$$R_s = \log\left|\mathbf{I} + \frac{1}{\sigma_s^2}\mathbf{H}_s^H\mathbf{Q}_s\mathbf{H}_s\right|,\; R_e = \log\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e^H\mathbf{Q}_s\mathbf{H}_e\right| \tag{2.22}$$

Thus, the achieved secrecy rate at the legitimate receiver is written as [18]

$$R = [R_s - R_e]^+, \tag{2.23}$$

where $[x]^+$ represents $\max\{x, 0\}$. Two secrecy rate optimization problems: a) power minimization b) secrecy rate maximization are formulated as follows:

1. Power minimization:

$$\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \mathrm{Tr}(\mathbf{Q}_s), \quad s.t. \ R \geq \bar{R}. \tag{2.24}$$

2. Secrecy rate maximization:

$$\max_{\mathbf{Q}_s \succeq \mathbf{0}} \ R, \quad s.t. \ \mathrm{Tr}(\mathbf{Q}_s) \leq P. \tag{2.25}$$

Both above problems are not convex in terms of transmit covariance matrix $\mathbf{Q}_s$, and cannot be solved directly. However, this secrecy rate can be linearized based on Taylor approximation such that both problems can be recast as the convex ones. In this optimization framework, it is first assumed that global channel state information (CSI) are perfectly available at the transmitter. This assumption has been widely used in recent work [19, 76, 77]. Thus, the secrecy rate can be approximated at any transmit covariance $\tilde{\mathbf{Q}}_s$ as follows:

$$\begin{aligned} R \simeq\; & \log\left|\mathbf{I} + \frac{1}{\sigma_s^2}\mathbf{H}_s^H\mathbf{Q}_s\mathbf{H}_s\right| - \log\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e^H\tilde{\mathbf{Q}}_s\mathbf{H}_e\right| - \mathrm{Tr}\left[\frac{1}{\sigma_e^2}\left(\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e^H\tilde{\mathbf{Q}}_s\mathbf{H}_e\right)^{-1}\mathbf{H}_e^H\mathbf{Q}_s\mathbf{H}_e\right] \\ & + \mathrm{Tr}\left[\frac{1}{\sigma_e^2}\left(\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e^H\tilde{\mathbf{Q}}_s\mathbf{H}_e\right)^{-1}\mathbf{H}_e^H\tilde{\mathbf{Q}}_s\mathbf{H}_e\right] \triangleq \tilde{R}, \end{aligned} \tag{2.26}$$

It can be easily observed that $\tilde{R}$ is a concave function in terms of $\mathbf{Q}_s$. Based on this approximation, the power minimization problem in (2.24) is modified as

$$\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \mathrm{Tr}(\mathbf{Q}_s), \quad s.t. \ \tilde{R} \geq \bar{R}. \tag{2.27}$$

In order to solve the problem in (2.27), the following Lagrange dual problem is written:

$$\max_{\lambda \geq 0} \min_{\mathbf{Q}_s \succeq \mathbf{0}} \left[\mathrm{Tr}(\mathbf{Q}_s) + \lambda(\bar{R} - \tilde{R}) \right], \tag{2.28}$$

where λ is the dual multiplier associated with the secrecy rate constraint. It is easily shown that the strong duality holds [48], since (2.27) is convex and satisfies Slaters condition such that the duality gap between (2.27) and (2.28) is zero. Thus, (2.27) can be handled by finding the optimal solution of the dual problem and updating the Lagrangian multiplier based on subgradient method [78].

To satisfy the particular achieved secrecy rate, the transmitter will be required a certain amount of transmission power. In general, the maximum available transmit power is limited, which leads to the power minimization problem might turn out to be infeasible. In general, the target secrecy rate needs to be decreased such that achieves the secrecy rate to satisfy the transmit power budget. In such cases, the same design will be repeated with a lower target secrecy rate, which is quite difficult to predict in advance. To circumvent this issue, a more attractive problem formulation is secrecy rate maximization shown in (2.25), where transmit optimization to maximize the achieved secrecy rate to meet with the transmit power constraint. It is always possible that this secrecy rate maximization problem can yield a feasible solution regardless of the maximum available transmission power or the channel conditions. The secrecy rate maximization problem (2.25) can be solved in a similar approach to the power minimization problem (2.24).

2.5.2 Robust Secrecy Rate Optimization

In the previous subsection, the secrecy rate optimization problems has been solved based on the assumption that the transmitter has the perfect CSI of the legitimate user and the eavesdropper. However, it is not possible that this assumption is always valid due to the channel estimation and quantization errors. Therefore, robust secrecy rate optimization techniques are proposed by incorporating channel uncertainty, which can be relaxed as semidefinite programming (SDP) at low SNR regime [48]. The imperfect CSI was modelled as the deterministic models [48,79–82], and the statistical models [32,83]. Based on deterministic channel uncertainty models, *S-Procedure* is employed to remove the impact of the channel error by reformulating the nonconvex secrecy rate constraint into the linear matrix inequality (LMI), whereas the robust outage secrecy rate optimization can be solved by using *Bernstein-type* inequality to tackle the outage probability constraint based on statistical channel uncertainty models.

Chapter 3

Convex Optimization Theory

The utilization of optimization approaches plays a significant role in signal processing and wireless communication [70, 84–86]. An increasing number of problems in signal processing and communications can be appropriately modelled as constrained optimization frameworks, which are either naturally convex or can be reformulated into convex forms by applying some mathematical optimization techniques. Once one problem has been reformulated into convex form, it can be efficiently solved by employing interior-point methods [70, 87]. Convex optimization techniques have brought many conveniences of practical interest in numerical analyses, since a local optimality is also the global optimum for the convex problems and they are solved in terms of polynomial time complexity. In addition, the optimal solution of a convex problem can be verified by employing Karush-Kuhn-Tucker (KKT) conditions and duality gaps. Also, the existing MATLAB software and toolboxes (i.e., SeDuMi [88], Yamip [89], and CVX [90]) are used to solve convex problems that make convex optimization techniques more attractive or applicable in many engineering applications. However, most of problems are generally not convex, which cannot be solved directly. Therefore, how to recognize the problems which can be handled using convex optimization and how to formulate the problem into a convex form are the key steps in the application of convex optimization techniques. In this section, the fundamentals of convex optimization techniques will be introduced.

3.1 Convex Set

A set $\mathcal{S}$ is convex if it can be written as

$$\theta y_1 + (1-\theta) y_2 \in \mathcal{S}, \ \forall \theta \in [0 \ 1], \text{ and } y_1, y_2 \in \mathcal{S}. \tag{3.1}$$

A set can be defined as a convex set if all the points of a line segment are in the same set, which is constructed by connecting any two points of this line segment by a straight line. Every affine set is also convex, since it contains the entire line between any two distinct points in it, and therefore also the line segment between the points [70].

3.2 Convex Cone

A set $\mathcal{S}$ is defined as a *cone*, or *nonnegative homogeneous*, if for every $y \in \mathcal{S}$ and $\alpha \geq 0$, $\alpha y \in \mathcal{S}$ holds. A set $\mathcal{S}$ is a convex cone if it is convex and a cone, and the following inequality holds for any y_1, $y_2 \in \mathcal{S}$ and θ_1, $\theta_2 \geq 0$

$$\theta_1 y_1 + \theta_2 y_2 \in \mathcal{S}. \tag{3.2}$$

Convex cones lead to various forms in some applications, in which the most common convex cones are given as

1. Nonnegative orthant $\mathbb{R}^n_+$.
2. Second-order cone (SOC): $\mathcal{S} = \{(y, x) | \|x\| \leq y\}$.
3. Positive semidefinite cone: $\mathcal{S} = \{\mathbf{Y} | \mathbf{Y}$ is symmctric and $X \succeq \mathbf{0}\}$.

3.3 Convex Function

A function $f(x) : \mathbb{R}^n \to \mathbb{R}$ is convex if $\text{dom} f(x)$ is a convex set and for all x_1, $x_2 \in \text{dom} f(x)$, the following inequality holds:

$$f(\theta x_1 + (1-\theta) x_2) \leq \theta f(x_1) + (1-\theta) f(x_2), \ \forall \theta \in [0 \ 1]. \tag{3.3}$$

In other words, $f(x)$ is less than or equal to the value of the linear function agreeing with $f(x)$ at the end points for any line segment in dom$f(x)$. The function $f(x)$ is concave if $-f(x)$ is convex. If $f(x)$ is continuously differentiable, the convexity of $f(x)$ is equivalent to

$$f(y) \geq f(x) + \nabla f(x)(y - x) \tag{3.4}$$

In addition, if $f(x)$ is twice continuously differentiable, then the convexity of $f(x)$ can be given by showing its Hessian matrix is a positive semidefinite (PSD),

$$\nabla^2 f(x) \succeq \mathbf{0}, \quad \forall x \in \mathbb{R}^n. \tag{3.5}$$

Therefore, for instance, a linear function is always convex, while a quadratic function $f(x) = x^H \mathbf{A} x + \mathbf{b} x + c$ is convex if and only if $\mathbf{A} \succeq \mathbf{0}$.

3.4 Convex Optimization Problems

A standard convex optimization problem can be written as the following form

$$\begin{aligned} \min \quad & f_0(x), \\ s.t. \quad & f_i(x) \leq 0, i = 1, ..., m, \\ & h_i(x) = 0, i = 1, ..., p, \end{aligned} \tag{3.6}$$

where $x \in \mathbb{R}^n$ is the *optimization variable*, the functions $f_0, ..., f_m : \mathbb{R}^n \to \mathbb{R}$ are convex functions, and the functions $h_1, ..., h_p$ are linear functions. In addition, $f_i(x) \leq 0$, $i = 1, ..., m$, are defined as the *inequality constraints*, and $h_i(x) = 0$, $i = 1, ..., p$, are defined as the *equality constraints*. If there are no constraints, then the problem can be known as an unconstrained problem. The domain to (3.6) is the set of points, for which the objective function and the constraints are defined as

$$\mathcal{D} = \bigcap_{i=0}^{m} \text{dom} f_i \cap \bigcap_{i=1}^{p} \text{dom} h_i \tag{3.7}$$

If a point $x \in \mathcal{D}$ is feasible, then it satisfies all the constraints $f_i(x) \leq 0$, $i = 1, ..., m$ and $h_i(x) = 0$, $i = 1, ..., p$. The optimal solution to (3.6) can be achieved at the optimal point x^* to guarantee the following inequality holds

$$f_0(x^*) \leq f_0(x), \ \forall x \in \mathcal{D}. \tag{3.8}$$

In the following, general forms of the canonical optimization problem formulations will be given.

3.4.1 Linear Programming

A convex optimization problem can be known as a linear programming (LP), when the objective and all constraint functions are affine (linear). A general LP can be written as

$$\begin{aligned} \min_{\mathbf{x}} \quad & \mathbf{c}^T\mathbf{x} + d, \\ s.t. \quad & \mathbf{G}\mathbf{x} \preceq \mathbf{h}, \\ & \mathbf{A}\mathbf{x} = \mathbf{b}, \end{aligned} \tag{3.9}$$

where $\mathbf{G} \in \mathbb{R}^{m\times n}$ and $\mathbf{A} \in \mathbb{R}^{p\times n}$.

3.4.2 Quadratic Programming

A convex optimization problem can be called quadratic programming (QP) when the objective function is quadratic (convex) and the constraint functions are affine. A QP is written as follows:

$$\begin{aligned} \min_{\mathbf{x}} \quad & \mathbf{x}^T\mathbf{P}\mathbf{x} + \mathbf{q}^T\mathbf{x} + r, \\ s.t. \quad & \mathbf{G}\mathbf{x} \preceq \mathbf{h}, \\ & \mathbf{A}\mathbf{x} = \mathbf{b}, \end{aligned} \tag{3.10}$$

where $\mathbf{P} \in \mathbb{S}_+^n$, $\mathbf{G} \in \mathbb{R}^{m\times n}$, and $\mathbf{A} \in \mathbb{R}^{p\times n}$. In QP, a convex quadratic function is minimized over a polyhedron. LP is a special case of QP with $\mathbf{P} = 0$ in (3.10).

3.4.3 Quadratically Constrained Quadratic Programming

A convex optimization problem is known as a quadratically constrained quadratic programming (QCQP), when both objective and all constraint functions are quadratic, which can be expressed as follows:

$$\begin{aligned}
\min_{\mathbf{x}} \quad & \mathbf{x}^T \mathbf{P}_0 \mathbf{x} + \mathbf{q}_0^T \mathbf{x} + r_0, \\
s.t. \quad & \mathbf{x}^T \mathbf{P}_i \mathbf{x} + \mathbf{q}_i^T \mathbf{x} + r_i \leq 0, \ i = 1, ..., m, \\
& \mathbf{A}\mathbf{x} = \mathbf{b},
\end{aligned} \tag{3.11}$$

where $\mathbf{P}_i \in \mathbb{S}_+^n, i = 0, ..., m$. In a QCQP, a quadratic convex function is minimized over a feasible region that is the intersection of ellipsoids with $\mathbf{P}_i \succ \mathbf{0}$. It is easily observed that LP is also a special case of QCQP with $\mathbf{P}_i = \mathbf{0}$.

3.4.4 Second-Order Cone Programming

A convex optimization problem is Second-order cone programming (SOCP), in which its standard form can be defined as

$$\begin{aligned}
\min_{\mathbf{x}} \quad & \mathbf{f}^T \mathbf{x}, \\
s.t. \quad & \|\mathbf{A}_i \mathbf{x} + \mathbf{b}_i\|_2 \leq \mathbf{c}_i^T \mathbf{x} + d_i, i = 1, ..., m, \\
& \mathbf{F}\mathbf{x} = \mathbf{g},
\end{aligned} \tag{3.12}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the optimization variable, $\mathbf{A}_i \in \mathbb{R}^{n_i \times n}$, and $\mathbf{F} \in \mathbb{R}^{p \times n}$. The constraint $\|\mathbf{A}\mathbf{x} + \mathbf{b}\|_2 \leq \mathbf{c}^T \mathbf{x} + d$, where $\mathbf{A} \in \mathbb{R}^{k \times n}$, is called as *second-order cone constraint*, since it is the same as requiring the affine function $(\mathbf{A}x + \mathbf{b}, \mathbf{c}^T \mathbf{x} + d)$ to lie in the second-order cone in $\mathbb{R}^{k+1}$. The SOCP (3.12) is equivalent to a QCQP (which is achieved by squaring each constraints). Similarly, if $\mathbf{A}_i = 0$, $i = 1, ..., m$, then the SOCP (3.12) reduces to a (general) LP. SOCP is, however, more general than QCQP and LP.

3.4.5 Semidefinite Programming

The conic form problem is called a semidefinite programming (SDP), when K is $\mathbb{S}_+^k$, the cone of positive semidefinite $k \times k$ matrices, and can be expressed as

$$\begin{aligned}
\min_{\mathbf{x}} \quad & \mathbf{c}^T \mathbf{x}, \\
s.t. \quad & \mathbf{x}_1 \mathbf{F}_1 + \mathbf{x}_2 \mathbf{F}_2 + ... + \mathbf{x}_n \mathbf{F}_n + \mathbf{G} \preceq \mathbf{0}, \\
& \mathbf{A}\mathbf{x} = \mathbf{b},
\end{aligned} \tag{3.13}$$

where $\mathbf{G}$, $\mathbf{F}_1, ..., \mathbf{F}_n \in \mathbb{S}^k$, and $\mathbf{A} \in \mathbb{R}^{p \times n}$. The inequality here is called linear matrix inequality (LMI). If the matrices G, $\mathbf{F}_1, ..., \mathbf{F}_n$ are all diagonal, then the LMI in (3.13) is equivalent to a set of n linear inequalities, and the SDP (3.13) reduces to LP.

3.4.6 Duality and KKT Conditions

In this subsection, the Lagrange duality is introduced, which is to take (3.6) into account by combining the objective function with a weighted sum of the constraint functions. The Lagrange dual problem $\mathcal{L} : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}$ for the problem (3.6) can be written as

$$\mathcal{L}(x, \lambda, \nu) = f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x), \tag{3.14}$$

where $\lambda_i \geq 0$, and $\nu_i \geq 0$ are the Lagrange dual multipliers associated with the i-th inequality $f_i(x) \leq 0$ and equality $h_i(x) = 0$ constraints, respectively. The objective function $f_0(x)$ in (3.6) is termed the primal objective and the optimization variable x is called the primal variable. Lagrange dual multipliers λ and ν associated with the problem (3.14) are also known as the dual variables. The Lagrange dual objective or the Lagrange dual function $g : \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}$ is defined as the minimum value of the Lagrange dual function over x for $\lambda \in \mathbb{R}^m$, $\nu \in \mathbb{R}^p$:

$$g(x, \lambda, \nu) = \inf_{x \in \mathcal{D}} \mathcal{L}(x, \lambda, \nu) \tag{3.15}$$

The Lagrange dual function is always concave regardless of whether the original problem is convex or not, since the dual function is the pointwise infimum of a series of affine functions of (λ, ν). The dual function $g(\lambda, \nu)$ yields a lower bound on the optimal value $f_0(x^*)$ to (3.6). For any $\lambda \succeq \mathbf{0}$ and any ν,

$$g(\lambda, \nu) \leq f_0(x^*), \tag{3.16}$$

For any feasible set (x, λ, ν), the following inequality holds

$$\begin{aligned} f_0(x) &\geq f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x) \\ &\geq \inf_{y \in \mathcal{D}} \left(f_0(y) + \sum_{i=1}^{m} \lambda_i f_i(y) + \sum_{i=1}^{p} \nu_i h_i(y) \right) \\ &\geq g(\lambda, \nu), \end{aligned} \tag{3.17}$$

Duality gap is the difference between the primal objective $f_0(x)$ and the dual objective $g(\lambda, \nu)$. When the inequality (3.16) holds with strict inequality, then it is called a weak duality. If the inequality (3.16) is satisfied with equality, it holds strong duality between the primal problem and the dual problem. To achieve the best lower bound of the original problem, the following dual problem can be solved:

$$\begin{aligned} \max_{\lambda, \nu} \quad & g(\lambda, \nu), \\ s.t. \quad & \lambda \geq 0, \end{aligned} \tag{3.18}$$

The Lagrange dual problem is always a convex problem, since the objective function in (3.18), which is always a concave function, is maximized with convex constraints. This always holds regardless of the nature of the primal problem (3.6). The following conditions are known as KKT conditions, which confirm the optimality of the solutions

1. Primal constraints: $f_i(x) \leq 0$, $i = 1, ..., m$; $h_i(x) = 0$, $i = 1, ..., p$.

2. Dual constraints: $\lambda \succeq \mathbf{0}$.

3. Complementary slackness: $\lambda_i f_i(x) = 0$, $i = 1, ..., m$.

4. Gradient of Lagrange dual function with respect to x:

$$\nabla f_0(x) + \sum_{i=1}^{m} \lambda_i \nabla f_i(x) + \sum_{i=1}^{p} \nu_i \nabla h_i(x) = 0. \tag{3.19}$$

For general optimization, the above KKT conditions are necessary conditions for optimality, but not sufficient conditions. For any optimization problem, if strong duality holds, then the KKT conditions can be satisfied, but not vice versa. However, for convex optimization problems, if the KKT conditions hold, then the strong duality holds between the primal problem and the dual problem, both of which are optimal [70].

3.5 Summary

In this chapter, variety of general convex optimization problems have been studied briefly. These problems can be effectively solved by using interior-point methods. The concepts of Lagrange duality and KKT conditions have also been investigated. However, this thesis mainly focus on SOCP and SDP to solve the optimization problems in physical layer security. More details can be found in [70, 85, 87, 91, 92] about these convex optimization problem formulations, applications of convex optimization, complexity analysis and interior-point methods.

Chapter 4

Transmit Optimization for MISO Secure Communications

This chapter studies transmit optimization for a multiple-input-single-output (MISO) secrecy channel with multiple multi-antenna eavesdroppers. For this chapter, the main contributions are given as follows:

- *Power Minimization*: Power minimization problem is investigated based on global channel state information (CSI), where a second-order cone programming (SOCP) based reformulation is proposed to design the transmit beamformer to minimize the transmit power while satisfying the secrecy rate. In addition, a closed-form solution for single eavesdropper case is derived based on Karush-Kuhn-Tucker (KKT) conditions.

- *Robust Outage Secrecy Rate Optimizations*: Robust outage secrecy rate optimization techniques are presented incorporating statistical channel uncertainty, where the outage probability constraint requires that the achieved secrecy rate exceeds certain thresholds with a specific probability. Due to nonconvex problem, a two-step algorithm with two conservative reformulations (i.e., *Bernstein-type* inequality and *S-Procedure*) is proposed to reformulate it into a convex optimization framework. It is proved that the solution to each reformulated problem returns rank-one, which, therefore, guarantees that its solution is also optimal to the original problem.

4.1 System Model

A MISO secure channel is considered in this section, where a legitimate transmitter establishes a confidential communications link to a legitimate receiver with K multi-antenna eavesdroppers. It is assumed that the legitimate transmitter consists of N_T transmit antennas, whereas the legitimate receiver and the k-th eavesdropper are equipped with single and $N_{E,k}$ receive antennas, respectively. The channel coefficients at the legitimate user and the k-th eavesdropper are denoted by $\mathbf{h}_s \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{H}_{e,k} \in \mathbb{C}^{N_T \times N_{E,k}}$, respectively. The received signal at the legitimate receiver and the k-th eavesdropper can be written as

$$y_s = \mathbf{h}_s^H \mathbf{x} + \mathrm{n}_s, \; \mathbf{y}_{e,k} = \mathbf{H}_{e,k}^H \mathbf{x} + \mathbf{n}_{e,k}, \; k = 1, ..., K,$$

where $\mathbf{x} \in \mathbb{C}^{N_T \times 1}$ is the signal vector intended to the legitimate user. In addition, n_s and $\mathbf{n}_{e,k}$ are zero-mean additive white Gaussian noises with noise variance σ_s^2 and the covariance matrix $\sigma_{e,k}^2 \mathbf{I}$, respectively. The transmit covariance matrix is defined as $\mathbf{Q}_s = \mathbb{E}\left\{\mathbf{x}\mathbf{x}^H\right\}$. The achieved secrecy rate at the legitimate receiver overheard by the k-th eavesdropper is defined as

$$R_{s,k} = \left[\log(1 + \frac{1}{\sigma_s^2}\mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log\left|\mathbf{I} + \frac{1}{\sigma_{e,k}^2}\mathbf{H}_{e,k}^H \mathbf{Q}_s \mathbf{H}_{e,k}\right|\right]^+, \; \forall k. \tag{4.1}$$

4.2 Power Minimization

In this section, transmit optimization for the power minimization problem subject to the minimum secrecy rate constraint is considered based on the global CSI, which can be written as

$$\min_{\mathbf{Q}_s \succeq \mathbf{0}} \mathrm{Tr}\left(\mathbf{Q}_s\right), \quad s.t. \; \min_k R_{s,k} \geq R, \quad \forall k, \tag{4.2}$$

where R is the predefined secrecy rate of the legitimate user. The problem (4.2) is not convex due to the nonconvex secrecy rate constraint, which, thus, is relaxed by the following matrix inequality [19, 93]:

$$|\mathbf{I} + \mathbf{A}| \geq 1 + \mathrm{Tr}(\mathbf{A}), \tag{4.3}$$

where the equality holds if and only if rank($\mathbf{A}$) = 1. If $\mathbf{Q}_s$ is rank-one, the relaxed problem is equivalent to the original problem (4.2), which can be written as

$$\begin{aligned}
&\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \mathrm{Tr}\,(\mathbf{Q}_s) \\
&s.t. \ 1+\frac{1}{\sigma_s^2}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s \geq 2^R\left[1+\mathrm{Tr}\left(\frac{1}{\sigma_{e,k}^2}\mathbf{H}_{e,k}^H\mathbf{Q}_s\mathbf{H}_{e,k}\right)\right], \quad \forall k, \\
&\quad\ \ \mathrm{rank}(\mathbf{Q}_s) \leq 1.
\end{aligned} \tag{4.4}$$

Problem (4.4) is a standard semidefinite programming (SDP) by ignoring the non-convex rank-one constraint, and its optimal solution has been shown to be rank-one [19]. Hence, it is easily verified that the optimal solution to (4.4) is also optimal to the original problem (4.2), which confirms the tightness of this relaxation. Accordingly, the following *theorem* holds:

Theorem 4.1 *Due to the rank-one solution to* (4.4)*,* $\mathbf{Q}_s$ *can be decomposed as* $\mathbf{Q}_s = \mathbf{w}\mathbf{w}^H$*, thus, the problem* (4.4) *can be formulated into a SOCP as follows:*

$$\begin{aligned}
\min_{\mathbf{w}} \quad & \|\mathbf{w}\|_2 \\
s.t. \quad & \begin{bmatrix} \frac{1}{\sigma_s}\mathbf{h}_s^H\mathbf{w} \\ \frac{2^{\frac{R}{2}}}{\sigma_{e,k}}\mathbf{H}_{e,k}^H\mathbf{w} \\ \left(2^R-1\right)^{\frac{1}{2}} \end{bmatrix} \succeq_K 0, \quad \forall k.
\end{aligned} \tag{4.5}$$

Proof Please refer to Section 4.6.1. ■

The problem (4.5) is convex, which can be solved by the interior-point methods [70]. Now, a special scenario is considered by using the following *proposition*:

Proposition 4.1 *For a single eavesdropper scenario, the optimal solution can be derived as*

$$\mathbf{w}^* = \sqrt{p^*}\mathbf{v}^*, \ \ \mathbf{v}^* = \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|_2}, \ \ p^* = \lambda^*(2^R-1), \ \ \lambda^* = \frac{1}{\lambda_{max}(\frac{1}{\sigma_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\sigma_e^2}\mathbf{H}_e\mathbf{H}_e^H)}, \tag{4.6}$$

where $\mathbf{v}_1 = v_{max}(\frac{1}{\sigma_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\sigma_e^2}\mathbf{H}_e\mathbf{H}_e^H)$.

Proof Please refer to Section 4.6.2. ■

4.3 Robust Outage Secrecy Rate Optimization

In the previous section, the power minimization problem has been solved based on the assumption that the perfect CSI of the legitimate user and the eavesdroppers can be available at the legitimate transmitter. However, it is not always possible that the perfect CSI might be available at the legitimate transmitter due to channel estimation and quantization errors. Robust secrecy rate optimization has been proposed incorporating channel uncertainty based on the worst case secrecy rate in [19, 29, 48], where the channel errors were modelled as norm bound. However, it is not possible that the legitimate transmitter always obtains these error bound accurately. Therefore, in this section, both robust outage secrecy rate optimization problems (i.e., robust power minimization and robust outage secrecy rate maximization) with outage probability secrecy rate constraint are presented.

4.3.1 Problem Formulation

In this subsection, two robust outage secrecy rate optimization problems (i.e., robust power minimization and robust outage secrecy rate maximization) with outage probability secrecy rate constraint are formulated, which are written as

$$\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \mathrm{Tr}(\mathbf{Q}_s), \quad s.t.\ \Pr\left\{ \min_k R_{s,k} \geq R \right\} \geq 1-\rho, \ \forall k, \tag{4.7a}$$

and

$$\max_{\mathbf{Q}_s \succeq \mathbf{0}} \ R, \quad s.t.\ \Pr\left\{ \min_k R_{s,k} \geq R \right\} \geq 1-\rho, \ \forall k, \ \mathrm{Tr}(\mathbf{Q}_s) \leq P, \tag{4.7b}$$

The problems (4.7) can be reformulated as

$$\min_{\mathbf{Q}_s \succeq \mathbf{0}} \quad \mathrm{Tr}(\mathbf{Q}_s),$$

$$s.t.\ \Pr\left\{ \log(1+\frac{1}{\sigma_s^2}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s) - \log\left|\mathbf{I}+\frac{1}{\sigma_{e,k}^2}\mathbf{H}_{e,k}^H\mathbf{Q}_s\mathbf{H}_{e,k}\right| \geq R \right\} \geq 1-\rho, \ \forall k, \tag{4.8a}$$

and

$$\max_{\mathbf{Q}_s \succeq \mathbf{0}} \ R, \quad s.t. \ \ \mathrm{Tr}(\mathbf{Q}_s) \leq P,$$
$$\Pr\left\{ \log(1 + \frac{1}{\sigma_s^2}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s) - \log\left|\mathbf{I} + \frac{1}{\sigma_{e,k}^2}\mathbf{H}_{e,k}^H\mathbf{Q}_s\mathbf{H}_{e,k}\right| \geq R\right\} \geq 1-\rho, \ \forall k, \quad (4.8b)$$

where $\rho \in (0,1]$ is the maximum allowable secrecy outage probability for the eavesdroppers, and P is the maximum available transmit power.

Remark For robust power minimization problem, the legitimate transmitter requires a certain amount of transmit power to satisfy the target secrecy rate within the required outage probability. However, due to insufficient transmit power or extremely worse channel conditions of the main channel than the eavesdroppers, the robust power minimization problem (4.8a) with outage probability secrecy rate constraint might turn out to be infeasible. To circumvent this infeasibility issue, the robust outage secrecy rate maximization problem (4.8b) is considered with outage probability secrecy rate and transmit power constraints. Similar statement has been found in [48]. Under the transmit power constraint, what the maximum secrecy rate R is that can be achieved subject to the (secrecy) outage probability less than 100 ρ % (i.e., 100 ρ %-secrecy outage capacity) [12,94]. In order to solve (4.8b), a two-stage algorithm is proposed. In the first stage, for any given R that makes (4.8a) feasible, the minimized transmit power is achieved by solving it. It is easily observed that the optimum value of R in (4.8b) monotonically increases with the transmit power (i.e., $\mathrm{Tr}(\mathbf{Q}_s)$). In the second stage, R is updated via a bisection search [70,95]. Hence, without loss of generality, the remaining part of this chapter only focuses on (4.8a), which can be reformulated as a convex optimization framework by employing *Bernstein-type* inequality or *S-Procedure*, though it is non-convex.

4.3.2 Channel Uncertainty Models

In this section, two statistical channel uncertainty models are specifically modelled.

- *Partial Channel Uncertainty Model*: Here, it is assumed that the legitimate transmitter has the perfect CSI of the legitimate user, and imperfect CSI of the eavesdropper. Accordingly, the channel uncertainty model is given

$$\mathbf{H}_{e,k} = \bar{\mathbf{H}}_{e,k} + \mathbf{E}_{e,k},\ \forall k,$$

where $\bar{\mathbf{H}}_{e,k} \in \mathbb{C}^{N_T \times N_{E,k}}$ is the estimated CSI of the k-th eavesdropper, and $\mathrm{vec}(\mathbf{E}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k})$ are the statistical information of channel error at the k-th eavesdropper, $\mathbf{R}_{e,k}$ is a positive semidefinite (PSD) matrix ($\succeq \mathbf{0}$).

- *Full Channel Uncertainty Model*: In this case, the imperfect CSI at the legitimate receiver and the eavesdroppers is available at the legitimate transmitter. The actual channels at the legitimate receiver and the k-th eavesdropper can be modelled respectively as

$$\mathbf{h}_s = \bar{\mathbf{h}}_s + \mathbf{e}_s,\ \mathbf{H}_{e,k} = \bar{\mathbf{H}}_{e,k} + \mathbf{E}_{e,k}, \forall k,$$

where $\bar{\mathbf{h}}_s \in \mathbb{C}^{N_T \times 1}$, $\bar{\mathbf{H}}_{e,k} \in \mathbb{C}^{N_T \times N_{E,k}}$ are the estimated CSI, and $\mathbf{e}_s \sim \mathcal{CN}(0, \mathbf{R}_s)$, $\mathrm{vec}(\mathbf{E}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k})$ are the statistical information of channel error at the legitimate user and the k-th eavesdropper, respectively. In addition, $\mathbf{R}_s$ and $\mathbf{R}_{e,k}$ are PSD matrices (i.e., $\mathbf{R}_s \succeq \mathbf{0}$, $\mathbf{R}_{e,k} \succeq \mathbf{0}$).

4.3.3 Robust Power Minimization Based on Partial Channel Uncertainty

In this subsection, the robust power minimization problem (4.8a) is considered based on the assumption of imperfect CSI only for the eavesdroppers, where two conservative reformulations (i.e., *Bernstein-type* inequality and *S-Procedure*) are employed to make the outage probability secrecy rate constraint tractable. This robust optimization problem can be expressed as

$$\begin{aligned} &\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \mathrm{Tr}(\mathbf{Q}_s) \\ &s.t.\ \Pr\left\{ \log(1 + \frac{1}{\sigma_s^2}\mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log\left|\mathbf{I} + \frac{1}{\sigma_{e,k}^2}\mathbf{H}_{e,k}^H \mathbf{Q}_s \mathbf{H}_{e,k}\right| \geq R \right\} \geq 1 - \rho, \\ &\quad \mathbf{H}_{e,k} = \bar{\mathbf{H}}_{e,k} + \mathbf{E}_{e,k},\ \mathrm{vec}(\mathbf{E}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k}),\ \forall k. \end{aligned} \tag{4.9}$$

The above problem is not convex in terms of the outage probability secrecy rate constraint. By considering the inequality in (4.3), the outage probability secrecy rate constraint is relaxed as

$$\Pr\bigg\{\mathrm{Tr}(\mathbf{H}_{e,k}^H\mathbf{Q}_s\mathbf{H}_{e,k}) \leq \frac{\sigma_{e,k}^2}{2^R}(1+\frac{1}{\sigma_s^2}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s) - \sigma_{e,k}^2\bigg\} \geq 1-\rho,\ \forall k. \tag{4.10}$$

The left hand side (LHS) to (4.10) cannot be reformulated in terms of a closed-form solution. Thus, the reformulation for this outage probability constraint is considered. From the following matrix identities,

$$\mathrm{Vec}(\mathbf{AXB}) = (\mathbf{B}^T \otimes \mathbf{A})\mathrm{Vec}(\mathbf{X}), \tag{4.11a}$$

$$\mathrm{Tr}(\mathbf{A}^T\mathbf{B}) = \mathrm{Vec}(\mathbf{A})^T\mathrm{Vec}(\mathbf{B}), \tag{4.11b}$$

$$(\mathbf{A}\otimes\mathbf{B})^T = \mathbf{A}^T \otimes \mathbf{B}^T. \tag{4.11c}$$

The constraint (4.10) is written as

$$\Pr\bigg\{\mathbf{e}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{e}_{e,k} + 2\Re\{\mathbf{e}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\} + \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k} \leq c_k\bigg\} \geq 1-\rho,\ \forall k, \tag{4.12}$$

where $c_k = \frac{\sigma_{e,k}^2}{2^R}(1+\frac{1}{\sigma_s^2}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s) - \sigma_{e,k}^2$, $\bar{\mathbf{h}}_{e,k} = \mathrm{vec}(\bar{\mathbf{H}}_{e,k})$ and $\mathbf{e}_{e,k} = \mathrm{vec}(\mathbf{E}_{e,k})$. Since $\mathbf{e}_{e,k} \sim \mathcal{CN}(0,\mathbf{R}_{e,k})$, the following transformation is given

$$\mathbf{e}_{e,k} = \mathbf{R}_{e,k}^{\frac{1}{2}}\mathbf{v}_{e,k}, \tag{4.13}$$

where $\mathbf{v}_{e,k} \sim \mathcal{CN}(0,\mathbf{I})$. Thus, the constraint (4.12) can be equivalently reformulated as

$$\begin{aligned}\Pr\bigg\{\mathbf{v}_{e,k}^H\Big[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\Big]\mathbf{v}_{e,k} + 2\Re\Big(\mathbf{v}_{e,k}^H[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}]\Big)\\ + [c_k - \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}] \geq 0\bigg\} \geq 1-\rho,\ \forall k.\end{aligned} \tag{4.14}$$

4.3.3.1 Bernstein-Type Inequality

In order to make the outage probability constraint (4.14) more tractable, the *Bernstein-type* inequality is applied and shown in the following *lemma*.

Lemma 4.1 *[96]: For any* $(\mathbf{A},\mathbf{u},c)$*, where* $\mathbf{A}\in\mathbb{C}^{N\times N}$ *is a complex hermitian* *matrix,* $\mathbf{u} \in \mathbb{C}^{N\times 1}$, $\mathbf{x} \sim \mathcal{CN}(0, \mathbf{I}_N)$ *and* $\rho \in (0, 1]$, *the following inequalities hold:*

$$Pr\{\mathbf{x}^H\mathbf{A}\mathbf{x} + 2\Re[\mathbf{x}^H\mathbf{u}] + c \geq 0\} \geq 1 - \rho, \tag{4.15}$$

$$\Leftarrow \begin{cases} Tr(\mathbf{A}) - \sqrt{-2\ln(\rho)}w + \ln(\rho)y + c \geq 0 \\ \left\| \begin{bmatrix} vec(\mathbf{A}) \\ \sqrt{2}\mathbf{u} \end{bmatrix} \right\| \leq w \\ y\mathbf{I}_N + \mathbf{A} \succeq \mathbf{0} \end{cases} \tag{4.16}$$

where w *and* y *are slack variables. The equalities* (4.16) *are jointly convex in terms of* $\mathbf{A}$, w *and* y.

Based on *Lemma* 4.1, the constraint (4.14) can be reformulated as

$$\begin{aligned} &\mathrm{Tr}\left[\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\right] + \sqrt{-2\ln(\rho)}w_k - \ln(\rho)y_k - \frac{\sigma_{e,k}^2}{2^R\sigma_s^2}\mathrm{Tr}[\mathbf{h}_s\mathbf{h}_s^H\mathbf{Q}_s] \\ &\qquad + \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k} \leq \sigma_{e,k}^2(\frac{1}{2^R} - 1), &\text{(4.17a)} \\ &\left\| \begin{bmatrix} \mathrm{vec}(\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}) \\ \sqrt{2}(\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}) \end{bmatrix} \right\|_2 \leq w_k, &\text{(4.17b)} \\ &y_k\mathbf{I} - \mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}} \succeq \mathbf{0}, y_k \geq 0, \ \forall k. &\text{(4.17c)} \end{aligned}$$

According to (4.17), the robust power minimization (4.9) can be equivalently written as

$$\min_{\mathbf{Q}_s} \ \ \mathrm{Tr}(\mathbf{Q}_s), \ \ s.t. \ \ (4.17), \ \ \mathbf{Q}_s \succeq \mathbf{0}. \tag{4.18}$$

The problem (4.18) is convex and can be solved efficiently by using the interior-point method [90]. In order to guarantee the optimal solution $\mathbf{Q}_s$ to problem (4.18) is also optimal to problem (4.9), the following *theorem* is provided to characterize the rank-one property of the solution $\mathbf{Q}_s$.

Theorem 4.2 *Provided that the problem in* (4.9) *is feasible, the problem* (4.18) *returns a rank-one solution based on a restricted* (4.17b).

Proof Please refer to Section 4.6.3. ■

4.3.3.2 S-Procedure

In this subsection, another conservative reformulation based on *S-Procedure* is considered to handle the outage probability secrecy rate constraint. First, the following *lemma* is considered to set the channel uncertainty regions for (4.14).

Lemma 4.2 *[83]: Provided a set* $\mathcal{S} \subset \mathbb{C}^{N\times 1}$ *with* $Pr\{\mathbf{v} \in \mathcal{S}\} \geq 1-\rho$ *such that* $\forall \mathbf{v} \in \mathcal{S}, \mathbf{v}^H\mathbf{A}\mathbf{v} + 2\Re\{\mathbf{v}^H\mathbf{u}\} + c \geq 0$, *then*

$$Pr\{\mathbf{v}^H\mathbf{A}\mathbf{v} + 2\Re\{\mathbf{v}^H\mathbf{u}\} + c \geq 0\} \geq 1-\rho \tag{4.19}$$

From *Lemma* 4.2, given the following deterministic quadratic constraint

$$\begin{aligned}\mathbf{v}_{e,k}^H[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}]\mathbf{v}_{e,k} + \ & 2\Re\{\mathbf{v}_{e,k}^H[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}]\} \\ &+ (c_k - \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}) \geq 0, \forall k,\end{aligned} \tag{4.20}$$

such that $\mathbf{v}_{e,k}$ belongs to the following set

$$\mathcal{S} = \{\mathbf{v}_{e,k}|\Pr(\mathbf{v}_{e,k}^H\mathbf{v}_{e,k} \leq \gamma_{e,k}^2) \geq 1-\rho\}, \forall k. \tag{4.21}$$

Since $\mathbf{v}_{e,k} \sim \mathcal{CN}(0, \mathbf{I}_{N_{E,k}N_T})$, it can be easily shown that $\|\mathbf{v}_e\|^2$ is a *Chi-square* random variable with degrees of freedom (DoF) $2N_{E,k}N_T$. The probability of the event (4.20) with the channel uncertainty regions in (4.21) is $1-\rho$, thus, the channel uncertainty regions always hold for $\gamma_{e,k} = \sqrt{\frac{F^{-1}(1-\rho)}{2}}$, where $F^{-1}(a)$ represents the inverse cumulative distribution function (CDF) of the *Chi-square* random variable at a. Thus, the outage probability secrecy rate constraint (4.14) is equivalently modified as

$$\begin{cases}\mathbf{v}_{e,k}^H[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}]\mathbf{v}_{e,k} + 2\Re\{\mathbf{v}_{e,k}^H[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}]\} \\ \qquad +(c_k - \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}) \geq 0, \\ -\mathbf{v}_{e,k}^H\mathbf{v}_{e,k} + \gamma_{e,k}^2 \geq 0.\end{cases} \tag{4.22}$$

In order to handle (4.22), the following *lemma* is given

Lemma 4.3 (S-Procedure) *[97]: Let* $f_k(\mathbf{x}), k = 1, 2,$ *be defined as*

$$f_k(\mathbf{x}) = \mathbf{x}^H\mathbf{A}_k\mathbf{x} + 2\Re\left\{\mathbf{b}_k^H\mathbf{x}\right\} + c_k, \tag{4.23}$$

where $\mathbf{A}_k = \mathbf{A}_k^H \in \mathbb{C}^{n\times n}$, $\mathbf{b}_k \in \mathbb{C}^{n\times 1}$ *and* $c_k \in \mathbb{R}$. *The implication* $f_1(\mathbf{x}) \geq 0 \Longrightarrow f_2(\mathbf{x}) \geq 0$ *holds if and only if there exists* $\mu \geq 0$ *such that*

$$\begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{bmatrix} - \mu \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{bmatrix} \succeq \mathbf{0}, \tag{4.24}$$

provided there exists a point $\tilde{\mathbf{x}}$ *with* $f_1(\tilde{\mathbf{x}}) > 0$.

By exploiting *S-Procedure* in *Lemma* 4.3, the problem (4.9) can be reformulated as

$$\begin{aligned} &\min_{\mathbf{Q}_s,\lambda_k} \ \mathrm{Tr}(\mathbf{Q}_s) \quad s.t. \ \begin{bmatrix} \lambda_k\mathbf{I} - [\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}] & -\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k} \\ -\bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}} & t_k - \lambda_k\gamma_{e,k}^2 \end{bmatrix} \succeq \mathbf{0}, \\ &\qquad \mathbf{Q}_s \succeq \mathbf{0}, \lambda_k \geq 0, \ \forall k, \end{aligned} \tag{4.25}$$

where $t_k = (\frac{1}{2^R} - 1)\sigma_{e,k}^2 + \frac{\sigma_{e,k}^2}{2^R\sigma_s^2}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s - \mathbf{h}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{h}_{e,k}$. The relaxed problem (4.25) is a standard SDP, and is solved efficiently by using convex optimization software [90]. Besides, it can be shown that the optimal solution to (4.25) is also optimal to (4.9) by using the following *theorem*:

Theorem 4.3 *Provided that the problem* (4.9) *is feasible, the relaxed problem* (4.25) *always yield a rank-one solution.*

Proof Please refer to Section 4.6.4. ■

4.3.4 Robust Power Minimization Based on Full Channel Uncertainty Model

In the previous section, the robust power minimization problem based on the partial statistical channel uncertainty model has been investigated. Now, a more challenging channel uncertainty model is studied with the imperfect CSI of the legitimate receiver as well as the eavesdroppers. Comparing with the previous channel uncertainty model, it is more difficult to handle the outage probability constraint, since the channel estimation errors of both the legitimate receiver and the eavesdroppers are considered. Accordingly, the problem (4.8a) is written as

$$\begin{aligned}
&\min_{\mathbf{Q}_s \succeq \mathbf{0}} \operatorname{Tr}(\mathbf{Q}_s), \quad s.t. \ \Pr\bigg\{ \log\bigg(1 + \frac{1}{\sigma_s^2}(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{Q}_s (\bar{\mathbf{h}}_s + \mathbf{e}_s)\bigg) \\
&\qquad - \log\bigg|\mathbf{I} + \frac{1}{\sigma_{e,k}^2}(\bar{\mathbf{H}}_{e,k} + \mathbf{E}_{e,k})^H \mathbf{Q}_s (\bar{\mathbf{H}}_{e,k} + \mathbf{E}_{e,k})\bigg| \geq R\bigg\} \geq 1 - \rho, \\
&\qquad \mathbf{e}_s \sim \mathcal{CN}(0, \mathbf{R}_s), \ \operatorname{vec}(\mathbf{E}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k}), \ \forall k. \qquad (4.26)
\end{aligned}$$

Based on the full channel uncertainty model, (4.26) will be also solved by exploiting *Bernstein-type* inequality and *S-Procedure* to make the outage probability secrecy rate constraint tractable.

4.3.4.1 Bernstein-Type Inequality

In this subsection, the *Bernstein-Type* inequality is employed to tackle the outage probability secrecy rate constraint in (4.26), which is written by exploiting the matrix inequalities (4.3) and (4.11) as

$$\begin{aligned}
&\Pr\bigg\{\frac{1}{\sigma_s^2}\Big[\mathbf{e}_s^H \mathbf{Q}_s \mathbf{e}_s + 2\Re\{\mathbf{e}_s^H \mathbf{Q}_s \bar{\mathbf{h}}_s\} + \bar{\mathbf{h}}_s^H \mathbf{Q}_s \bar{\mathbf{h}}_s\Big] - \frac{2^R}{\sigma_{e,k}^2}\Big[\mathbf{e}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{e}_{e,k} \\
&\qquad + 2\Re\{\mathbf{e}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \bar{\mathbf{h}}_{e,k}\} + \bar{\mathbf{h}}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \bar{\mathbf{h}}_{e,k}\Big] \geq 2^R - 1\bigg\} \geq 1 - \rho, \ \forall k. \qquad (4.27)
\end{aligned}$$

The above constraint is rewritten in terms of matrix form as

$$\begin{aligned}
&\Pr\bigg\{[\mathbf{e}_s^H, \mathbf{e}_{e,k}^H]\begin{bmatrix} \frac{1}{\sigma_s^2}\mathbf{Q}_s & \mathbf{0} \\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}(\mathbf{I} \otimes \mathbf{Q}_s) \end{bmatrix}[\mathbf{e}_s^H, \mathbf{e}_{e,k}^H]^H \\
&+ 2\Re\bigg\{[\mathbf{e}_s^H, \mathbf{e}_{e,k}^H]\begin{bmatrix} \frac{1}{\sigma_s^2}\mathbf{Q}_s & \mathbf{0} \\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}(\mathbf{I} \otimes \mathbf{Q}_s) \end{bmatrix}[\bar{\mathbf{h}}_s^H, \bar{\mathbf{h}}_{e,k}^H]^H\bigg\} \\
&+ [\bar{\mathbf{h}}_s^H, \bar{\mathbf{h}}_{e,k}^H]\begin{bmatrix} \frac{1}{\sigma_s^2}\mathbf{Q}_s & \mathbf{0} \\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}(\mathbf{I} \otimes \mathbf{Q}_s) \end{bmatrix}[\bar{\mathbf{h}}_s^H, \bar{\mathbf{h}}_{e,k}^H]^H \geq 2^R - 1\bigg\} \geq 1 - \rho, \ \forall k. \qquad (4.28)
\end{aligned}$$

In order to handle the above outage probability constraint by the *Bernstein-type* inequality as described in Section 4.3.3.1, the CSI errors of the legitimate receiver and the eavesdropper are written as $\mathbf{e}_s = \mathbf{R}_s^{\frac{1}{2}}\mathbf{v}_s$, and $\mathbf{e}_{e,k} = \mathbf{R}_{e,k}^{\frac{1}{2}}\mathbf{v}_{e,k}$, respectively, where $\mathbf{v}_s \sim \mathcal{CN}(0, \mathbf{I}_{N_T})$ and $\mathbf{v}_{e,k} \sim \mathcal{CN}(0, \mathbf{I}_{N_T N_{e,k}})$, and set $\mathbf{v}_k = [\mathbf{v}_s^H, \mathbf{v}_{e,k}^H]^H$, $\forall k$.

Thus, this outage probability constraint can be reformulated as

$$\Pr\left\{\mathbf{v}_k^H\mathbf{A}_k\mathbf{v}_k + 2\Re\{\mathbf{v}_k^H\mathbf{u}_k\} + \mathrm{c}_k \geq 0\right\} \geq 1-\rho,\ \forall k, \tag{4.29}$$

where

$$\begin{aligned}
\mathbf{A}_k &= \begin{bmatrix} \frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}} & \mathbf{0} \\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}} \end{bmatrix},\\
\mathbf{u}_k &= \begin{bmatrix} \frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s & \mathbf{0} \\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s) \end{bmatrix}[\bar{\mathbf{h}}_s^H\ \bar{\mathbf{h}}_{e,k}^H]^H,\\
\mathrm{c}_k &= [\bar{\mathbf{h}}_s^H\ \bar{\mathbf{h}}_{e,k}^H]\begin{bmatrix} \frac{1}{\sigma_s^2}\mathbf{Q}_s & \mathbf{0} \\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}(\mathbf{I}\otimes\mathbf{Q}_s) \end{bmatrix}[\bar{\mathbf{h}}_s^H\ \bar{\mathbf{h}}_{e,k}^H]^H + 1 - 2^R.
\end{aligned}$$

By applying *Lemma* 4.1, the constraint (4.29) is expressed as

$$\mathrm{Tr}(\mathbf{A}_k) - \sqrt{-2\ln(\rho)}w_k + \ln(\rho)y_k + \mathrm{c}_k \geq 0, \tag{4.30a}$$

$$\left\|\begin{bmatrix} \mathrm{vec}(\mathbf{A}_k) \\ \sqrt{2}\mathbf{u}_k \end{bmatrix}\right\|_2 \leq w_k, \tag{4.30b}$$

$$y_k\mathbf{I} + \mathbf{A}_k \succeq \mathbf{0}, y_k \geq 0, \forall k. \tag{4.30c}$$

Thus, replacing the constraints (4.27) with (4.30), the problem (4.26) is reformulated as

$$\min_{\mathbf{Q}_s\succeq\mathbf{0}} \ \mathrm{Tr}(\mathbf{Q}_s), \quad s.t. \ (4.30),\ \forall k. \tag{4.31}$$

The problem (4.31) is convex, which can be solved by using interior-point methods. With more complex structure of the problem (4.31), it is more challenging to directly prove a rank-one solution of $\mathbf{Q}_s$. However, the following *theorem* is provided to guarantee a rank-one solution to (4.31).

Theorem 4.4 *Provided that the problem in* (4.26) *is feasible, the reformulated problem* (4.31) *yields a rank-one solution subject to a restricted* (4.30b).

Proof Please refer to Section 4.6.5. ■

4.3.4.2 S-Procedure

In this subsection, *S-Procedure* based reformulation is considered, where the problem (4.26) is expressed as

$$\begin{aligned}
&\min_{\mathbf{Q}_s \succeq \mathbf{0}} \quad \mathrm{Tr}(\mathbf{Q}_s) \\
&s.t.\ \Pr\Bigg\{\frac{1}{\sigma_s^2}(\bar{\mathbf{h}}_s^H\mathbf{Q}_s\bar{\mathbf{h}}_s + 2\Re\{\mathbf{e}_s^H\mathbf{Q}_s\bar{\mathbf{h}}_s\} + \mathbf{e}_s^H\mathbf{Q}_s\mathbf{e}_s) - \frac{2^R}{\sigma_{e,k}^2}[\bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k} \\
&\quad + 2\Re\{\mathbf{e}_{e,k}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\} + \mathbf{e}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{e}_{e,k}] \geq 2^R - 1\Bigg\} \geq 1-\rho,\ \forall k. \qquad (4.32)
\end{aligned}$$

In order to tackle the outage probability constraint (4.32), $\mathbf{e}_s = \mathbf{R}_s^{\frac{1}{2}}\mathbf{v}_s$ and $\mathbf{e}_{e,k} = \mathbf{R}_{e,k}^{\frac{1}{2}}\mathbf{v}_{e,k}$ are considered, respectively, where $\mathbf{v}_s \sim \mathcal{CN}(0, \mathbf{I}_{N_T})$ and $\mathbf{v}_{e,k} \sim \mathcal{CN}(0, \mathbf{I}_{N_T N_{E,k}})$, and thus (4.32) is reformulated as

$$\begin{aligned}
&\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \mathrm{Tr}(\mathbf{Q}_s) \\
&s.t.\ \Pr\Bigg\{\frac{1}{\sigma_s^2}(\mathbf{v}_s^H\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}}\mathbf{v}_s + 2\Re\{\mathbf{v}_s^H\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\bar{\mathbf{h}}_s\} + \bar{\mathbf{h}}_s^H\mathbf{Q}_s\bar{\mathbf{h}}_s) - \frac{2^R}{\sigma_{e,k}^2}[\mathbf{v}_{e,k}^H\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\mathbf{v}_{e,k} \\
&\quad + 2\Re\{\mathbf{v}_{e,k}^H\mathbf{R}_s^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\} + \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}] \geq 2^R - 1\Bigg\} \geq 1-\rho,\ \forall k. \qquad (4.33)
\end{aligned}$$

From [98], the channel uncertainty regions are equivalently defined as follows:

$$\Rightarrow \mathbb{R}_s = \{\mathbf{v}_s : \mathbf{v}_s^H\mathbf{v}_s \leq \gamma_s^2\},\ \mathbb{R}_{e,k} = \{\mathbf{v}_{e,k} : \mathbf{v}_{e,k}^H\mathbf{v}_{e,k} \leq \gamma_{e,k}^2\}, \qquad (4.34)$$

where $\gamma_s = \sqrt{\frac{F_s^{-1}(1-\rho)}{2}}$ and $\gamma_{e,k} = \sqrt{\frac{F_e^{-1}(1-\rho)}{2}}$; F_s^{-1} and F_e^{-1} are the inverse cumulative density function (CDF) of the *Chi-squared* distributed variables with DoF $2N_T$ and $2N_TN_{E,k}$, respectively. Thus, the following problem is given

$$\begin{aligned}
&\min_{\mathbf{Q}_s \succeq \mathbf{0}} \mathrm{Tr}(\mathbf{Q}_s) \\
&s.t.\ \frac{1}{\sigma_s^2}(\mathbf{v}_s^H\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}}\mathbf{v}_s + 2\Re\{\mathbf{v}_s^H\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\bar{\mathbf{h}}_s\} + \bar{\mathbf{h}}_s^H\mathbf{Q}_s\bar{\mathbf{h}}_s) - \frac{2^R}{\sigma_{e,k}^2}[\mathbf{v}_{e,k}^H\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\mathbf{v}_{e,k} \\
&\quad + 2\Re\{\mathbf{v}_{e,k}^H\mathbf{R}_s^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\} + \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}] \geq 2^R - 1, \\
&\quad \mathbf{v}_s^H\mathbf{v}_s \leq \gamma_s^2,\ \mathbf{v}_{e,k}^H\mathbf{v}_{e,k} \leq \gamma_{e,k}^2,\ \forall k. \qquad (4.35)
\end{aligned}$$

Here, a worst-case optimization framework is considered to reformulate (4.35), which can be developed as

$$\min_{\mathbf{Q}_s\succeq\mathbf{0},t_s\geq 0,t_{e,k}\geq 0} \mathrm{Tr}(\mathbf{Q}_s), \quad s.t. \ t_s - t_{e,k} \geq 2^R - 1,$$
$$\frac{1}{\sigma_s^2}(\mathbf{v}_s^H\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}}\mathbf{v}_s + 2\Re\{\mathbf{v}_s^H\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\bar{\mathbf{h}}_s\} + \bar{\mathbf{h}}_s^H\mathbf{Q}_s\bar{\mathbf{h}}_s) \geq t_s,$$
$$\frac{2^R}{\sigma_{e,k}^2}[\mathbf{v}_{e,k}^H\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\mathbf{v}_{e,k} + 2\Re\{\mathbf{v}_{e,k}^H\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\} + \bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}] \leq t_{e,k},$$
$$\mathbf{v}_s^H\mathbf{v}_s \leq \gamma_s^2, \quad \mathbf{v}_{e,k}^H\mathbf{v}_{e,k} \leq \gamma_{e,k}^2, \ \forall k, \tag{4.36}$$

where $t_s > 0$ and $t_{e,k} > 0$ are slack variables for the achieved rate of the legitimate receiver and the k-th eavesdropper, respectively. By exploiting *S-Procedure* in *Lemma* 4.3, the problem (4.36) is reformulated as

$$\min_{\mathbf{Q}_s\succeq\mathbf{0}} \mathrm{Tr}(\mathbf{Q}_s)$$
$$s.t. \ t_s - t_{e,k} \geq 2^R - 1, \tag{4.37a}$$
$$\mathbf{T}_s = \begin{bmatrix} \mu_s\mathbf{I} + \frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}} & \frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\bar{\mathbf{h}}_s \\ \frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s^H\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}} & \frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s^H\mathbf{Q}_s\bar{\mathbf{h}}_s - t_s - \mu_s\gamma_s^2, \end{bmatrix} \succeq \mathbf{0}, \tag{4.37b}$$
$$\mathbf{T}_{e,k} = \begin{bmatrix} \mu_k\mathbf{I} - \frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}} & -\frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k} \\ -\frac{2^R}{\sigma_{e,k}^2}\bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}} & t_{e,k} - \frac{2^R}{\sigma_{e,k}^2}\bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k} - \mu_{e,k}\gamma_{e,k}^2 \end{bmatrix} \succeq \mathbf{0}, \tag{4.37c}$$
$$\mu_s \geq 0, \mu_{e,k} \geq 0, \ \forall k. \tag{4.37d}$$

The problem (4.37) is a SDP, which can be solved efficiently by interior-point method, and the following *theorem* is given to confirm that (4.37) returns a rank-one solution

Theorem 4.5 *The optimal solution to problem* (4.37) *can be proven to be rank-one provided that problem* (4.26) *is feasible.*

Proof Please refer to Section 4.6.6.

4.4 Simulation Results

Simulation results are provided to validate the theoretical results to the proposed schemes in this section. To evaluate the performance of the proposed schemes, the system consists of one multi-antenna legitimate transmitter, one single-antenna legitimate receiver and three multi-antenna eavesdroppers. Additionally, the legitimate transmitter is equipped with five antennas (i.e., $N_T = 5$), whereas each eavesdropper consists of three antennas (i.e., $N_{E,k} = 3$, $\forall k$). The maximum available transmit power is assumed to be 10 dB unless specified. All channel coefficients are generated using zero-mean circularly symmetric independent and identically distributed (i.i.d) complex Gaussian random variables, and the noise powers at the legitimate user and the eavesdroppers are set to be one (i.e., $\sigma_s^2 = \sigma_{e,k}^2 = 1$). The outage probability is set to be $\rho = 0.05$.

4.4.1 Power Minimization

First, simulation results are given to confirm the closed-form solution derived in (4.6), where the power minimization problem is formulated as a SOCP. The transmit power is achieved by solving the SOCP, the SDP and closed-form expression for five different random channels as shown in Table 4.1, where the target secrecy rate is set to be 2 bps/Hz. From this table, it can be observed that the results of these three schemes are the same, which confirms the closed-form solution and the SOCP.

Channels	Closed-form	Convex optimization	
		SOCP	SDP in [19]
Channel 1	1.8081	1.8081	1.8081
Channel 2	1.4943	1.4943	1.4943
Channel 3	1.1292	1.1292	1.1292
Channel 4	0.6896	0.6896	0.6896
Channel 5	1.6659	1.6659	1.6659

Table 4.1: The transmit power for three schemes.

4.4.2 Robust Outage Secrecy Rate Optimization with Partial Channel Uncertainties

In this subsection, the performance of the proposed robust outage secrecy rate optimization is evaluated by exploiting channel uncertainty of the eavesdroppers. Here, the k-th eavesdropper's CSI error covariance matrix is assumed to be $\mathbf{R}_{e,k} = \varepsilon_{e,k}^2\mathbf{I}$, where $\varepsilon_{e,k}^2$ denotes the channel error variance of the k-th eavesdropper. The channel error variance is set to be $\varepsilon_{e,k}^2 = 0.01$ or 0.04 unless specified.

Fig. 4.1 shows the CDF versus the achieved secrecy rate, where the target secrecy rate is set to be 1 bps/Hz. It is observed from this result that the *Bernstein-type* inequality scheme can satisfy the outage probability secrecy rate constraint within the required probability, whereas the *S-Procedure* scheme has a small proportion of the achieved secrecy rates that cannot satisfy the outage constraint within the required probability, since approximately 10 % of the achieved secrecy rates are below the predefined secrecy rate. Fig. 4.2 represents the achieved secrecy rate with different

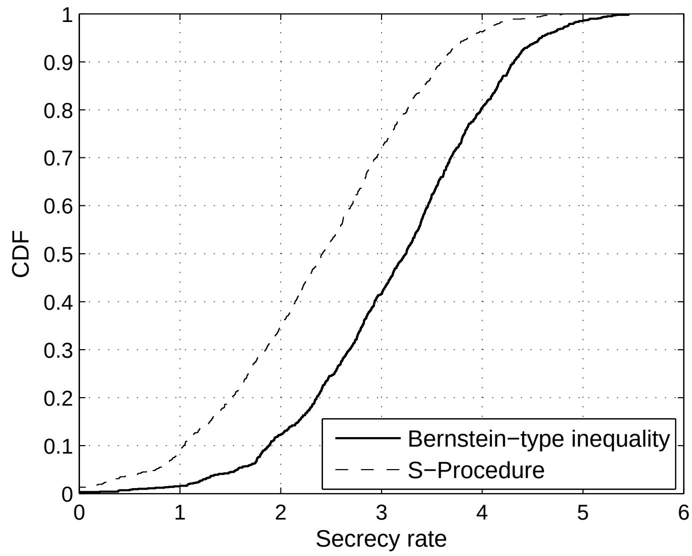

Figure 4.1: The CDF of secrecy rate with partial channel uncertainties.

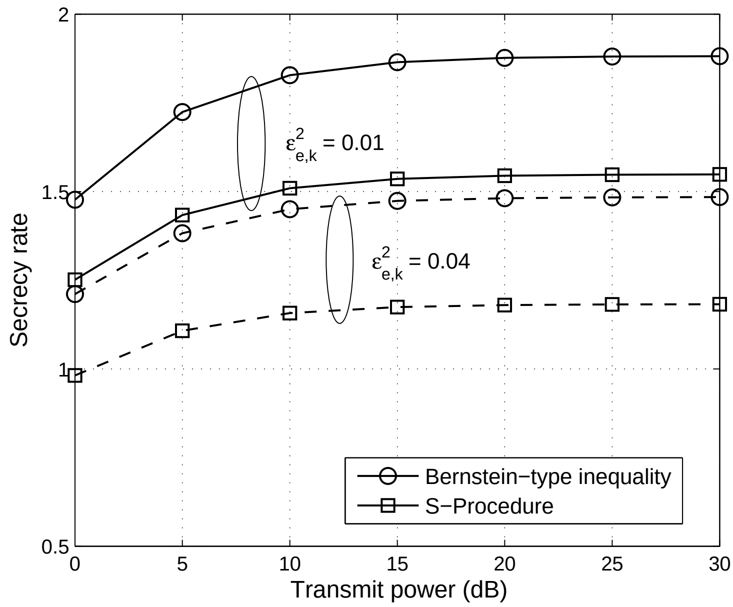

Figure 4.2: The secrecy rate with different transmit powers based on partial channel uncertainties.

transmit powers, where the achieved secrecy rate increases with the transmit power, and the *Bernstein-type* inequality scheme outperforms *S-Procedure* scheme in terms of the achieved secrecy rate. The achieved secrecy rate with different error variances

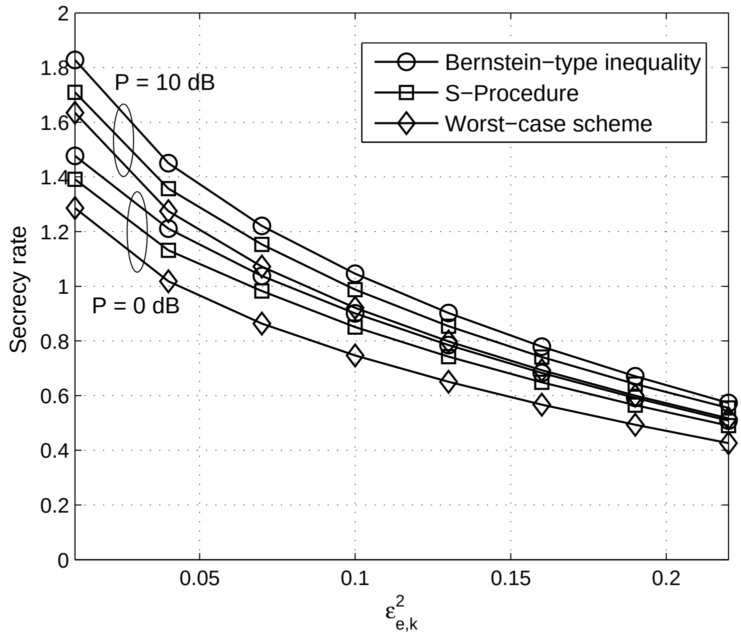

Figure 4.3: The secrecy rate with different error variances based on partial channel uncertainties.

(i.e., $\varepsilon_{e,k}^2$) is shown in Fig. 4.3. As seen in this result, the achieved secrecy rates of both robust proposed schemes and the worst-case scheme decrease with increasing error variance. Additionally, compared with the worst-case scheme shown in [19], both robust proposed scheme outperform the worst-case scheme, and *Bernstein-type* inequality scheme outperforms *S-Procedure* scheme.

4.4.3 Robust Outage Secrecy Rate Optimization with Full Channel Uncertainties

Next, simulation results are provided to evaluate the achieved secrecy rate performance based on the full channel uncertainty model, where the imperfect CSI of both the legitimate user and the eavesdroppers is available at the legitimate transmitter. The CSI error covariance matrices of the legitimate user and the eavesdropper are assumed to be $\mathbf{R}_s = \varepsilon_s^2\mathbf{I}$, $\mathbf{R}_{e,k} = \varepsilon_{e,k}^2\mathbf{I}$, where ε_s^2 and $\varepsilon_{e,k}^2$ represent the channel error variances of the legitimate user and the k-th eavesdropper, respectively. Here, it is assumed that the channel error variances as $\varepsilon_s^2 = \varepsilon_{e,k}^2 = 0.01$, 0.04 or 0.1.

The CDF versus the achieved secrecy rate is shown in Fig. 4.4, where the target secrecy rate is assumed to be 1 bps/Hz, and the *Bernstein-type* inequality scheme

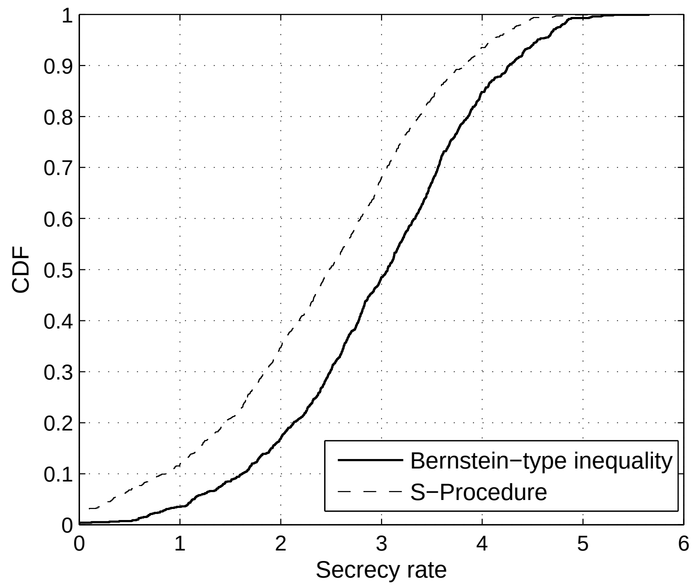

Figure 4.4: The CDF of secrecy rate with full channel uncertainties.

can satisfy the outage probability secrecy rate constraint since the approximately 5 % of the achieved secrecy rates are below the target secrecy rate. However, the *S-Procedure* scheme has approximately 10 % of the achieved secrecy rates that cannot satisfy the outage probability secrecy rate constraint, which is under the predefined secrecy rate. Fig. 4.5 shows the achieved secrecy rate with different transmit

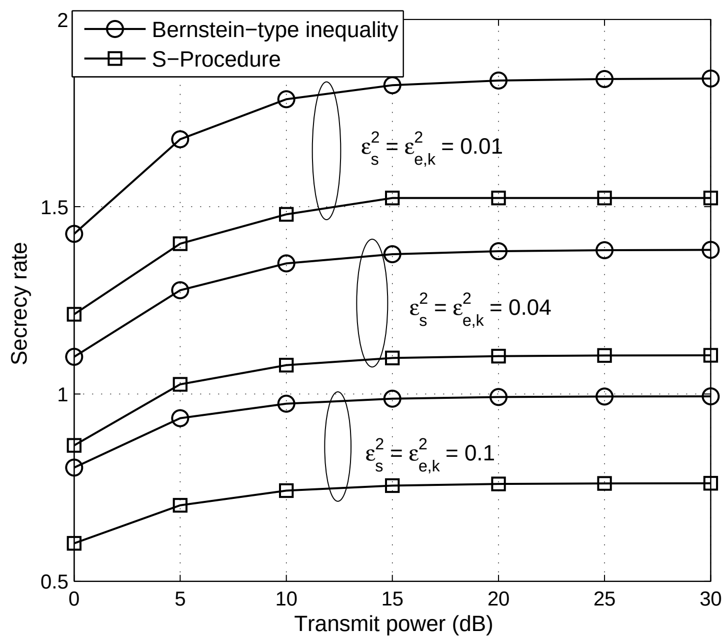

Figure 4.5: The secrecy rate with different transmit powers based on full channel uncertainties.

powers, where the achieved secrecy rate increases with transmit power, and the

Bernstein-type inequality scheme outperforms *S-Procedure* scheme. The achieved secrecy rate with different error variances is shown in Fig. 4.6. As seen in this result, the achieved secrecy rate of both proposed schemes and the worst-case scheme decrease with error variance. In addition, the *Bernstein-type* inequality scheme outperforms the *S-Procedure* scheme and the worst-case scheme. Besides, the achieved

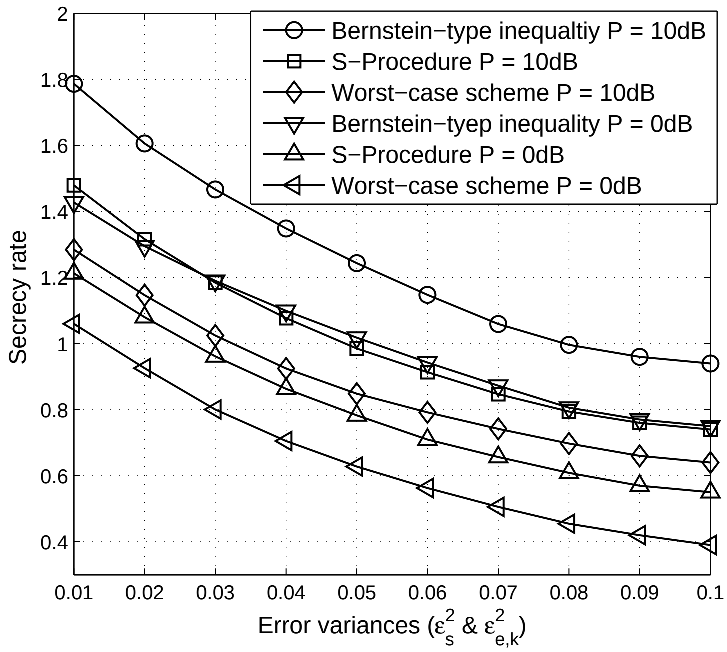

Figure 4.6: The secrecy rate with different error variances based on full channel uncertainties.

secrecy rate versus the number of the eavesdroppers (i.e., K) is plotted in Fig. 4.7. From this result, the achieved secrecy rate gets decreased as more eavesdroppers are present. Also, *Bernstein-type* inequality scheme outperforms the *S-Procedure* scheme in terms of the achieved secrecy rate.

4.5 Summary

In this chapter, different transmit optimization techniques for MISO secrecy channel has been studied. First, the power minimization was formulated into a SOCP framework for the case of a single legitimate user and multiple eavesdroppers, and a closed-form solution was derived for the case of only single eavesdropper. Additionally, robust outage secrecy rate optimization problems with outage probability secrecy rate constraint have been presented incorporating two statistical channel uncertainty models. The robust outage secrecy rate optimization problems were

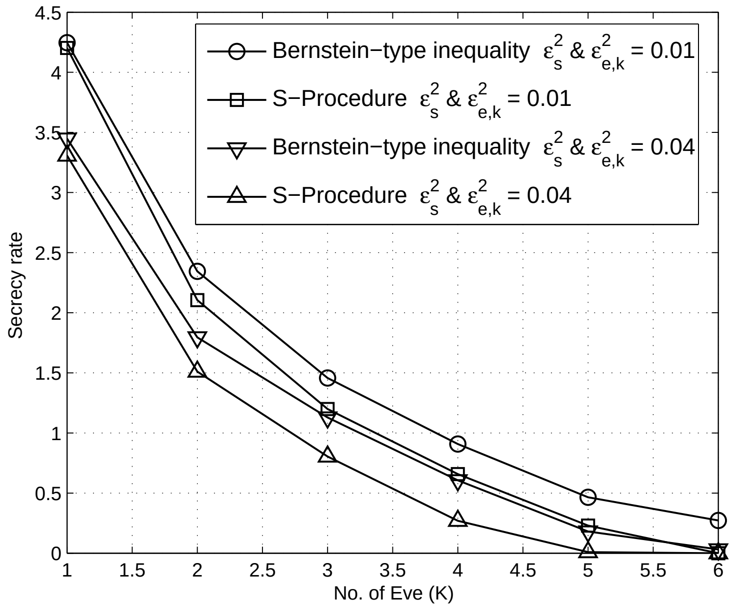

Figure 4.7: The secrecy rate with different numbers of the eavesdropper based on full channel uncertainties.

not convex in terms of the outage probability constraint. In order to make it tractable, a two-step algorithm with both conservative approximation approaches (i.e., *Bernstein-type* inequality and *S-Procedure*) was proposed to handle the outage probability constraint. An initial proof shows the solution to each reformulated problem returns rank-one, which, therefore, guarantees that its solution is also optimal to the original problem. Simulation results have been provided to confirm the performance of the proposed schemes.

4.6 Appendix

4.6.1 Proof of Theorem 4.1

First, due to the rank-one solution of the problem (4.4), it can be written with $\mathbf{Q}_s = \mathbf{w}\mathbf{w}^H$ as

$$\min_{\mathbf{w}} \ \|\mathbf{w}\|_2^2$$
$$s.t. \ \frac{1 + \frac{1}{\sigma_s^2}\mathbf{w}^H\mathbf{h}_s\mathbf{h}_s^H\mathbf{w}}{1 + \frac{1}{\sigma_{e,k}^2}\mathbf{w}^H\mathbf{H}_{e,k}\mathbf{H}_{e,k}^H\mathbf{w}} \geq 2^R, \forall k. \tag{4.38}$$

Then, the above problem can be written as

$$\begin{aligned} &\min_{\mathbf{w}} \ \|\mathbf{w}\|_2^2 \\ &s.t. \ \frac{2^R}{\sigma_{e,k}^2}\|\mathbf{H}_{e,k}^H\mathbf{w}\|^2 + (2^R-1) \le \frac{1}{\sigma_s^2}|\mathbf{h}_s^H\mathbf{w}|^2, \forall k. \end{aligned} \tag{4.39}$$

From the following inequality relation

$$\begin{bmatrix} x \\ \mathbf{y} \end{bmatrix} \succeq_K \mathbf{0}, \Leftrightarrow \|\mathbf{y}\|_2 \le x. \tag{4.40}$$

The problem (4.2) is reformulated as a SOCP as defined in (4.5). This completes the proof of *Theorem* 4.1. ■

4.6.2 Proof of Proposition 4.1

First, let $\mathbf{w} = \sqrt{p}\mathbf{v}$, the problem (4.38) for only one eavesdropper can be written as

$$\min_{p,\mathbf{v}} \ p\mathbf{v}^H\mathbf{v}, \ s.t. \ \frac{\mathbf{v}^H(\mathbf{I} + \frac{p}{\sigma_s^2}\mathbf{h}_s\mathbf{h}_s^H)\mathbf{v}}{\mathbf{v}^H(\mathbf{I} + \frac{p}{\sigma_e^2}\mathbf{H}_e\mathbf{H}_e^H)\mathbf{v}} \ge 2^R, \ \mathbf{v}^H\mathbf{v} = 1, p \ge 0. \tag{4.41}$$

In order to solve the above problem, the Lagrange dual function to (4.38) is considered, which can be written as,

$$\begin{aligned} L(\mathbf{w},\lambda) &= \mathbf{w}^H\mathbf{w} + \lambda 2^R(1 + \frac{1}{\sigma_e^2}\mathbf{w}^H\mathbf{H}_e\mathbf{H}_e^H\mathbf{w}) - \lambda(1 + \frac{1}{\sigma_s^2}\mathbf{w}^H\mathbf{h}_s\mathbf{h}_s^H\mathbf{w}) \\ &= \mathbf{w}^H\left(\mathbf{I} + \frac{1}{\sigma_e^2}\lambda 2^R\mathbf{H}_e\mathbf{H}_e^H - \frac{1}{\sigma_s^2}\lambda\mathbf{h}_s\mathbf{h}_s^H\right)\mathbf{w} + \lambda\left(2^R - 1\right), \end{aligned} \tag{4.42}$$

where $\lambda \ge 0$ is dual multiplier with the secrecy rate constraint. The corresponding dual problem is defined as follows:

$$\max_{\lambda} \lambda\left(2^R - 1\right), \quad s.t. \ \mathbf{Z} \triangleq \mathbf{I} + \frac{1}{\sigma_e^2}\lambda 2^R\mathbf{H}_e\mathbf{H}_e^H - \frac{1}{\sigma_s^2}\lambda\mathbf{h}_s\mathbf{h}_s^H \succeq \mathbf{0}, \ \lambda \ge 0. \tag{4.43}$$

In order to show the strong duality between the problem (4.38) and its dual problem, its Hessian matrix is derived as

$$\nabla_{\mathbf{w}\mathbf{w}^H} = \mathbf{I} + \frac{1}{\sigma_e^2}\lambda 2^R\mathbf{H}_e\mathbf{H}_e^H - \frac{1}{\sigma_s^2}\lambda\mathbf{h}_s\mathbf{h}_s^H. \tag{4.44}$$

The strong duality holds between the primal problem and its dual problem provided the Hessian is a PSD matrix [99]. This will be satisfied provided that the problem (4.38) is feasible, which implies that the strong duality holds between (4.38) and (4.43). Thus, the optimal λ^* is derived as

$$\lambda^* = \frac{1}{\lambda_{max}(\frac{1}{\sigma_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\sigma_e^2}\mathbf{H}_e\mathbf{H}_e^H)}. \tag{4.45}$$

Note that the above equality can be obtained based on the fact $\mathrm{Tr}(\mathbf{A}) \geq \lambda_{\max}(A)$. Thus, the minimum power can be derived as

$$p^* = \lambda^*(2^R - 1). \tag{4.46}$$

In addition, the optimal $\mathbf{w}$ lies in the null space of $\mathbf{Z}$, thus

$$\mathbf{v}_1 = \upsilon_{max}(\frac{1}{\sigma_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\sigma_e^2}\mathbf{H}_e\mathbf{H}_e^H), \quad \mathbf{v} = \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|_2}. \tag{4.47}$$

This completes the proof of *Proposition* 4.1. ■

4.6.3 Proof of Theorem 4.2

In order to show the rank-one solution to the problem (4.18), the SOCP constraint (4.17b) can be restrictedly given by

$$\begin{aligned}
&\sqrt{\|\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\|_F^2 + 2\|\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\|^2} \leq \sqrt{\|\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\|_F^2(\|\mathbf{R}_{e,k}^{\frac{1}{2}}\|_F^2 + 2\|\bar{\mathbf{h}}_{e,k}\|^2)} \\
&\leq \sqrt{\mathrm{Tr}[(\mathbf{I}\otimes\mathbf{Q}_s)(\mathbf{I}\otimes\mathbf{Q}_s)^H]}\sqrt{\mathrm{Tr}^2(\mathbf{R}_{e,k}) + 2\mathrm{Tr}(\mathbf{R}_{e,k})\|\bar{\mathbf{h}}_{e,k}\|^2} \leq w_k, \\
&\Rightarrow \mathrm{Tr}[(\mathbf{I}\otimes\mathbf{Q}_s)(\mathbf{I}\otimes\mathbf{Q}_s)^H]l_k^2 \leq w_k^2,
\end{aligned} \tag{4.48}$$

where $l_k = \sqrt{\mathrm{Tr}^2(\mathbf{R}_{e,k}) + 2\mathrm{Tr}(\mathbf{R}_{e,k})\|\bar{\mathbf{h}}_{e,k}\|^2}$. By exploiting $\mathrm{Tr}[(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D})] = \mathrm{Tr}(\mathbf{AB}\otimes\mathbf{CD})$, $\mathrm{Tr}(\mathbf{A}\otimes\mathbf{B}) = \mathrm{Tr}(\mathbf{A})\mathrm{Tr}(\mathbf{B})$ and $(\mathbf{A}\otimes\mathbf{B})^T = \mathbf{A}^T\otimes\mathbf{B}^T$, the following relations hold:

$$l_k^2 N_{E,k} \mathrm{Tr}(\mathbf{Q}_s \mathbf{Q}_s^H) \leq w_k^2, \ \Rightarrow \lambda_{max}(\mathbf{Q}_s \mathbf{Q}_s^H) \leq \mathrm{Tr}(\mathbf{Q}_s \mathbf{Q}_s^H) \leq \frac{w_k^2}{l_k^2 N_{E,k}},$$
$$\Rightarrow \mathbf{Q}_s \mathbf{Q}_s^H \preceq t_k^2 \mathbf{I}, \ \Rightarrow \mathbf{S}_k = \begin{bmatrix} t_k \mathbf{I} & \mathbf{Q}_s \\ \mathbf{Q}_s^H & t_k \mathbf{I} \end{bmatrix} \succeq \mathbf{0}, \tag{4.49}$$

where $t_k^2 = \frac{w_k^2}{l_k^2 N_{E,k}}$. Thus, the constraint (4.49) can be rewritten as the following linear matrix inequality (LMI)

$$\begin{cases} \begin{bmatrix} t_k \mathbf{I} & \mathbf{0} \\ \mathbf{0}^H & t_k \mathbf{I} \end{bmatrix} \succeq \begin{bmatrix} \mathbf{I} \\ \mathbf{0} \end{bmatrix} \mathbf{Q}_s \begin{bmatrix} \mathbf{0} & -\mathbf{I} \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ -\mathbf{I} \end{bmatrix} \mathbf{Q}_s^H \begin{bmatrix} \mathbf{I} & \mathbf{0} \end{bmatrix}, \\ \|\mathbf{Q}_s\| \leq t_k. \end{cases} \tag{4.50}$$

In order to further reformulate the above LMI, the following *lemma* is considered:

Lemma 4.4 *(Nemirovski lemma) [100]: For a given set of matrices* $\mathbf{A} = \mathbf{A}^H$, $\mathbf{B}$ *and* $\mathbf{C}$*, the following LMI is satisfied:*

$$\mathbf{A} \succeq \mathbf{BXC} + \mathbf{C}^H \mathbf{X}^H \mathbf{B}, \|\mathbf{X}\| \leq t, \tag{4.51}$$

if and only if there exists non-negative real numbers a *such that*

$$\begin{bmatrix} \mathbf{A} - a\mathbf{C}^H \mathbf{C} & -t\mathbf{B}^H \\ -t\mathbf{B} & a\mathbf{I} \end{bmatrix} \succeq 0. \tag{4.52}$$

By applying *Lemma* 4.4 to the LMI in (4.50),

$$\mathbf{S}_k = \begin{bmatrix} \begin{bmatrix} t_k \mathbf{I} & \mathbf{0} \\ \mathbf{0} & t_k \mathbf{I} \end{bmatrix} - a_1 \begin{bmatrix} \mathbf{0} \\ -\mathbf{I} \end{bmatrix} \begin{bmatrix} \mathbf{0} & -\mathbf{I} \end{bmatrix} & -t_k \begin{bmatrix} \mathbf{I} \\ \mathbf{0} \end{bmatrix} \\ -t_k \begin{bmatrix} \mathbf{I} & \mathbf{0} \end{bmatrix} & a_1 \mathbf{I} \end{bmatrix} \succeq \mathbf{0}. \tag{4.53}$$

From (4.53), it is claimed that constraint (4.49) can be equivalently rewritten without $\mathbf{Q}_s$. In order to prove rank-one of the power minimization problem, the Lagrangian dual function of (4.18) is given in (4.54),

$$
\begin{aligned}
L(\mathbf{Q}_s, \mathbf{Z}, \lambda_k, \mathbf{C}_k) &= \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{Q}_s) + \sum_{k=1}^{K} \lambda_k \Big[\mathrm{Tr}[(\mathbf{R}_{e,k} + \bar{\mathbf{h}}_{e,k}\bar{\mathbf{h}}_{e,k}^H)(\mathbf{I} \otimes \mathbf{Q}_s)] \\
&- \frac{\sigma_{e,k}^2}{2^R \sigma_s^2} \mathrm{Tr}(\mathbf{h}_s \mathbf{h}_s^H \mathbf{Q}_s) + \sqrt{-2\ln(\rho)} w_k - \ln(\rho) y_k - \sigma_{e,k}^2 (\frac{1}{2^R} - 1) \Big] \\
&- \sum_{k=1}^{K} \mathrm{Tr}\Big[\mathbf{C}_k \Big(y_k \mathbf{I} - \mathbf{R}_{e,k}^{\frac{1}{2}} (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{R}_{e,k}^{\frac{1}{2}} \Big) \Big] \\
&= \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{Q}_s) + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \lambda_k \mathrm{Tr}(\mathbf{H}_k^{(n,n)} \mathbf{Q}_s) - \sum_{k=1}^{K} \frac{\lambda_k \sigma_{e,k}^2}{2^R \sigma_s^2} \mathrm{Tr}(\mathbf{h}_s \mathbf{h}_s^H \mathbf{Q}_s) \\
&\quad + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathrm{Tr}[\mathbf{T}_{e,k}^{(n,n)} \mathbf{Q}_s]. \qquad (4.54)
\end{aligned}
$$

where $\mathbf{Z}$, λ_k and $\mathbf{C}_k$ are dual variables associated with $\mathbf{Q}_s$, (4.17a) and (4.17c), respectively. In addition, $\mathbf{H}_k^{(n,n)} \in \mathbb{H}_+^{N_T \times N_T}$ and $\mathbf{T}_{e,k}^{(n,n)} \in \mathbb{H}_+^{N_T \times N_T}$ are block submatrices of $\mathbf{R}_{e,k} + \bar{\mathbf{h}}_{e,k}\bar{\mathbf{h}}_{e,k}^H$ and $\mathbf{R}_{e,k}^{\frac{1}{2}} \mathbf{C}_k \mathbf{R}_{e,k}^{\frac{1}{2}}$, respectively, which are expressed specifically as follows:

$$
\mathbf{R}_{e,k} + \bar{\mathbf{h}}_{e,k}\bar{\mathbf{h}}_{e,k}^H = \begin{bmatrix} \mathbf{H}_k^{(1,1)} & \cdots & \mathbf{H}_k^{(1,N_{E,k})} \\ \vdots & \ddots & \vdots \\ \mathbf{H}_k^{(N_{E,k},1)} & \cdots & \mathbf{H}_k^{(N_{E,k},N_{E,k})} \end{bmatrix} \qquad (4.55)
$$

and

$$
\mathbf{R}_{e,k}^{\frac{1}{2}} \mathbf{C}_k \mathbf{R}_{e,k}^{\frac{1}{2}} = \begin{bmatrix} \mathbf{T}_{e,k}^{(1,1)} & \cdots & \mathbf{T}_{e,k}^{(1,N_{E,k})} \\ \vdots & \ddots & \vdots \\ \mathbf{T}_{e,k}^{(N_{E,k},1)} & \cdots & \mathbf{T}_{e,k}^{(N_{E,k},N_{E,k})} \end{bmatrix} \qquad (4.56)
$$

The following KKT conditions related to the proof are considered

$$
\frac{\partial \mathcal{L}}{\partial \mathbf{Q}_s} = 0, \qquad (4.57a)
$$

$$
\mathbf{Z}\mathbf{Q}_s = \mathbf{0}, \qquad (4.57b)
$$

$$
\mathbf{Q}_s \succeq \mathbf{0},\ \mathbf{Z} \succeq \mathbf{0},\ \lambda_k \geq 0,\ \mathbf{C}_k \succeq \mathbf{0}, \forall k. \qquad (4.57c)
$$

According to the KKT condition in (4.57a),

$$\mathbf{I}-\mathbf{Z}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\lambda_k\mathbf{H}_k^{(n,n)}-t\mathbf{h}_s\mathbf{h}_s^H+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{T}_{e,k}^{(n,n)}=\mathbf{0}, \tag{4.58}$$

where $t=\sum_{k=1}^{K}\frac{\lambda_k\sigma_{e,k}^2}{2^R\sigma_s^2}$. Postmultiplying the two sides of (4.58) by $\mathbf{Q}_s$, and based on (4.57b), the following equality holds

$$\left(\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\lambda_k\mathbf{H}_k^{(n,n)}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{T}_{e,k}^{(n,n)}\right)\mathbf{Q}_s=t\mathbf{h}_s\mathbf{h}_s^H\mathbf{Q}_s, \tag{4.59}$$

From (4.59), it is claimed that there is at least one λ_k, $\forall k$ such that $\lambda_k>0$, which is shown by contradiction. If all $\lambda_k=0$ for $\forall k$, then $t=0\Rightarrow\Big(\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{T}_{e,k}^{(n,n)}\Big)\mathbf{Q}_s=\mathbf{0}$ (c.f. (4.59)) such that $\mathbf{Q}_s=\mathbf{0}$ due to $\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{T}_{e,k}^{(n,n)}\succ\mathbf{0}$, which implies that the legitimate transmitter does not send any information to the legitimate receiver. Thus, there exists at least one $\lambda_k>0$ such that $t>0$ holds. According to (4.59), the following relation of rank holds:

$$\begin{aligned}\operatorname{rank}(\mathbf{Q}_s)&=\operatorname{rank}\left[\left(\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\lambda_k\mathbf{H}_k^{(n,n)}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{T}_{e,k}^{(n,n)}\right)\mathbf{Q}_s\right]\\&=\operatorname{rank}(t\mathbf{h}_s\mathbf{h}_s^H\mathbf{Q}_s)\le\min\{\operatorname{rank}(t\mathbf{h}_s\mathbf{h}_s^H),\operatorname{rank}(\mathbf{Q}_s)\}\le 1.\end{aligned} \tag{4.60}$$

This completes the proof of *Theorem* 4.2. ■

4.6.4 Proof of Theorem 4.3

In order to show the rank-one solution to (4.25), the first step is to write the dual function of (4.25) as follows:

$$L(\mathbf{Q}_s,\mathbf{Z},\mathbf{Y}_k)=\operatorname{Tr}(\mathbf{Q}_s)-\operatorname{Tr}(\mathbf{Z}\mathbf{Q}_s)-\sum_{k=1}^{K}\operatorname{Tr}(\mathbf{Y}_k\mathbf{A}_k), \tag{4.61}$$

where

$$\mathbf{A}_k=\begin{bmatrix}\lambda_k\mathbf{I}+[-\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}] & -\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\bar{\mathbf{h}}_{e,k}\\ -\bar{\mathbf{h}}_{e,k}^H(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}} & t_k-\lambda_k\gamma_{e,k}^2\end{bmatrix},$$

in addition, $\mathbf{Z}$ and $\mathbf{Y}_k$ are the dual variables associated with $\mathbf{Q}_s$ and $\mathbf{A}_k$, respectively. Then, $\mathbf{A}_k$ is rewritten for the convenience of notations.

$$\mathbf{A}_k = \begin{bmatrix} \lambda_k \mathbf{I} & \mathbf{0} \\ \mathbf{0} & (\frac{1}{2^R}-1)\sigma_{e,k}^2 - \lambda_k \gamma_{e,k}^2 \end{bmatrix} + \frac{\sigma_{e,k}^2}{2^R \sigma_s^2} \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix}^H \mathbf{Q}_s \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix}$$
$$- \begin{bmatrix} \mathbf{R}_{e,k}^{\frac{1}{2}} & \bar{\mathbf{h}}_{e,k} \end{bmatrix}^H (\mathbf{I} \otimes \mathbf{Q}_s) \begin{bmatrix} \mathbf{R}_{e,k}^{\frac{1}{2}} & \bar{\mathbf{h}}_{e,k} \end{bmatrix}. \quad (4.62)$$

From (4.62), the Lagrangian dual function can be rewritten as (4.63),

$$L(\mathbf{Q}_s, \mathbf{Z}, \mathbf{Y}_k) = \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{Q}_s) + \sum_{k=1}^{K} \mathrm{Tr}\left(\mathbf{Y}_k \left[\mathbf{R}_{e,k}^{\frac{1}{2}} \ \bar{\mathbf{h}}_{e,k} \right]^H (\mathbf{I} \otimes \mathbf{Q}_s) \left[\mathbf{R}_{e,k}^{\frac{1}{2}} \ \bar{\mathbf{h}}_{e,k} \right] \right)$$
$$- \sum_{k=1}^{K} \mathrm{Tr}\left(\mathbf{Y}_k \begin{bmatrix} \lambda_k \mathbf{I} & \mathbf{0} \\ \mathbf{0} & (\frac{1}{2^R}-1)\sigma_{e,k}^2 - \lambda_k \gamma_{e,k}^2 \end{bmatrix} \right) - \sum_{k=1}^{K} \frac{\sigma_{e,k}^2}{2^R \sigma_s^2} \mathrm{Tr}\left(\mathbf{Y}_k \left[\mathbf{0} \ \mathbf{h}_s \right]^H \mathbf{Q}_s \left[\mathbf{0} \ \mathbf{h}_s \right] \right)$$
$$= \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{Q}_s) + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathrm{Tr}\left(\mathbf{S}_k^{(n,n)} \mathbf{Q}_s \right) - \sum_{k=1}^{K} \mathrm{Tr}\left(\mathbf{Y}_k \begin{bmatrix} \lambda_k \mathbf{I} & \mathbf{0} \\ \mathbf{0} & (\frac{1}{2^R}-1)\sigma_{e,k}^2 - \lambda_k \gamma_{e,k}^2 \end{bmatrix} \right)$$
$$- \sum_{k=1}^{K} \frac{\sigma_{e,k}^2}{2^R \sigma_s^2} \mathrm{Tr}\left(\mathbf{Y}_k \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix}^H \mathbf{Q}_s \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix} \right), \quad (4.63)$$

where $\mathbf{S}_k^{(n,n)} \in \mathbb{H}_+^{N_T}$ is a submatrix of $\left[\mathbf{R}_{e,k}^{\frac{1}{2}} \ \bar{\mathbf{h}}_{e,k} \right] \mathbf{Y}_k \left[\mathbf{R}_{e,k}^{\frac{1}{2}} \ \bar{\mathbf{h}}_{e,k} \right]^H$ similar to Appendix III. Next, the following KKT conditions is employed,

$$\frac{\partial L}{\partial \mathbf{Q}_s} = \mathbf{I} - \mathbf{Z} - \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix} \mathbf{T} \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix}^H + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{S}_k^{(n,n)} = \mathbf{0},$$
$$\Rightarrow \mathbf{I} - \mathbf{Z} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{S}_k^{(n,n)} = \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix} \mathbf{T} \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix}^H, \quad (4.64)$$

where $\mathbf{T} = \sum_{k=1}^{K} \frac{\sigma_{e,k}^2}{2^R \sigma_s^2} \mathbf{Y}_k$. Multiplying $\mathbf{Q}_s$ by the two sides of (4.64),

$$\left(\mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{S}_k^{(n,n)} \right) \mathbf{Q}_s = \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix} \mathbf{T} \begin{bmatrix} \mathbf{0} & \mathbf{h}_s \end{bmatrix}^H \mathbf{Q}_s, \quad (4.65)$$

From the above equality, it is shown that $\mathbf{T} \neq \mathbf{0}$ by contradiction. If $\mathbf{T} = \mathbf{0}$, then $\left(\mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{S}_k^{(n,n)} \right) \mathbf{Q}_s = \mathbf{0}$. such that $\mathbf{Q}_s = \mathbf{0}$ due to $\mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{S}_k^{(n,n)} \succ \mathbf{0}$, which violates $\mathbf{Q}_s \neq \mathbf{0}$ due to $R > 0$. Thus, it is claimed that $\mathbf{T} \succ \mathbf{0}$, and the rank-one relations hold:

$$\begin{aligned}\operatorname{rank}(\mathbf{Q}_s) &= \operatorname{rank}\Bigg(\Bigg(\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{S}_k^{(n,n)}\Bigg)\mathbf{Q}_s\Bigg) = \operatorname{rank}\Bigg(\begin{bmatrix}\mathbf{0} & \mathbf{h}_s\end{bmatrix}\mathbf{T}\begin{bmatrix}\mathbf{0} & \mathbf{h}_s\end{bmatrix}^H\mathbf{Q}_s\Bigg)\\ &\leq \operatorname{rank}(\begin{bmatrix}\mathbf{0} & \mathbf{h}_s\end{bmatrix}) \leq 1, \end{aligned} \tag{4.66}$$

This completes the proof of *Theorem* 4.3. ■

4.6.5 Proof of Theorem 4.4

In order to prove the rank-one solution to (4.31), first, transform this problem into the following form

$$\begin{aligned} &\min_{\mathbf{Q}_s} \operatorname{Tr}(\mathbf{Q}_s)\\ s.t.\ &\frac{1}{\sigma_s^2}[\operatorname{Tr}(\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H\mathbf{Q}_s)+\operatorname{Tr}(\mathbf{R}_s\mathbf{Q}_s)]-\frac{2^R}{\sigma_{e,k}^2}\operatorname{Tr}[(\bar{\mathbf{h}}_{e,k}\bar{\mathbf{h}}_{e,k}^H+\mathbf{R}_{e,k})(\mathbf{I}\otimes\mathbf{Q}_s)]+a_k\geq 0,\\ &\begin{bmatrix} w_k\mathbf{I} & \mathbf{f}_k \\ \mathbf{f}_k^H & w_k\end{bmatrix}\succeq\mathbf{0},\quad y_k\mathbf{I}_{N_T}+\frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}}\succeq\mathbf{0}, \qquad (4.67\text{a})\\ &y_k\mathbf{I}_{N_TN_{E,k}}-\frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\succeq\mathbf{0}, \qquad (4.67\text{b})\end{aligned}$$

where $a_k = 1-2^R-\sqrt{-2\ln\rho}w_k+\ln\rho y_k$, and

$$\mathbf{f}_k = \begin{bmatrix} \operatorname{vec}\left(\begin{bmatrix}\frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s\mathbf{R}_s^{\frac{1}{2}} & \mathbf{0}\\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\mathbf{R}_{e,k}^{\frac{1}{2}}\end{bmatrix}\right)\\ \sqrt{2}\begin{bmatrix}\frac{1}{\sigma_s^2}\mathbf{R}_s^{\frac{1}{2}}\mathbf{Q}_s & \mathbf{0}\\ \mathbf{0} & -\frac{2^R}{\sigma_{e,k}^2}\mathbf{R}_{e,k}^{\frac{1}{2}}(\mathbf{I}\otimes\mathbf{Q}_s)\end{bmatrix}\begin{bmatrix}\bar{\mathbf{h}}_s^H & \bar{\mathbf{h}}_{e,k}^H\end{bmatrix}\end{bmatrix}. \tag{4.68}$$

The first constraints in (4.67a) can also be restrictedly modified by using the similar approach as shown in the proof of *Theorem* 4.2, whilst the Hermitian matrix in the second constraint is evidently positive definite as a result of its structure. Then, the

Lagrange dual function to (4.67) is written

$$\mathcal{L}(\mathbf{Q}_s, \mathbf{Z}, \lambda_k, \mathbf{B}_k, \mathbf{C}_k) = \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{Q}_s) - \sum_{k=1}^{K} \lambda_k \Bigg(\frac{1}{\sigma_s^2}[\mathrm{Tr}(\bar{\mathbf{h}}_s \bar{\mathbf{h}}_s^H \mathbf{Q}_s) + \mathrm{Tr}(\mathbf{R}_s \mathbf{Q}_s)]$$
$$- \frac{2^R}{\sigma_{e,k}^2} \mathrm{Tr}[(\bar{\mathbf{h}}_{e,k}\bar{\mathbf{h}}_{e,k}^H + \mathbf{R}_{e,k})(\mathbf{I} \otimes \mathbf{Q}_s)] + a_k \Bigg) - \sum_{k=1}^{K} \mathrm{Tr}\Bigg[\mathbf{C}_k \Bigg(y_k \mathbf{I}_{N_T N_{E,k}}$$
$$- \frac{2^R}{\sigma_{e,k}^2} \mathbf{R}_{e,k}^{\frac{1}{2}} (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{R}_{e,k}^{\frac{1}{2}} \Bigg) \Bigg], \tag{4.69}$$

According to the relevant KKT condition,

$$\frac{\partial \mathcal{L}}{\partial \mathbf{Q}_s} = \mathbf{I} - \sum_{k=1}^{K} \frac{\lambda_k}{\sigma_s^2} \bar{\mathbf{h}}_s \bar{\mathbf{h}}_s^H - \sum_{k=1}^{K} \frac{\lambda_k}{\sigma_s^2} \mathbf{R}_s + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \frac{\lambda_k 2^R}{\sigma_{e,k}^2} \mathbf{H}_k^{(n,n)} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \frac{2^R}{\sigma_{e,k}^2} \mathbf{R}_k^{(n,n)} - \mathbf{Z} = 0, \tag{4.70}$$

where $\mathbf{H}_k^{(n,n)} \in \mathbb{H}_+^{N_T}$ is a block submatrix of $\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H + \mathbf{R}_{e,k}$, and $\mathbf{R}_k^{(n,n)} \in \mathbb{H}_+^{N_T}$ is a block submatrix of $\mathbf{R}_{e,k}^{\frac{1}{2}} \mathbf{C}_k \mathbf{R}_{e,k}^{\frac{1}{2}}$. Then, setting

$$\mathbf{T} = \mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \frac{2^R}{\sigma_{e,k}^2} \left(\lambda_k \mathbf{H}_k^{(n,n)} + \mathbf{R}_k^{(n,n)} \right) - \left(\sum_{k=1}^{K} \frac{\lambda_k}{\sigma_s^2} \right) \mathbf{R}_s, \tag{4.71}$$

the following equality holds:

$$\mathbf{Z} = \mathbf{T} - \left(\sum_{k=1}^{K} \frac{\lambda_k}{\sigma_s^2} \right) \bar{\mathbf{h}}_s \bar{\mathbf{h}}_s^H. \tag{4.72}$$

From (4.71), it is easily verified that $\mathbf{T} \succ \mathbf{0}$ when $\lambda_k = 0$. Thus, only the case of $\lambda_k > 0$ is considered. By setting $v = \sum_{k=1}^{K} \frac{\lambda_k}{\sigma_s^2} > 0$, one can easily observe that $\mathbf{T} \succeq \mathbf{0}$ and $\mathrm{rank}(v\mathbf{h}_s\mathbf{h}_s^H) = 1$ from (4.72). Let $\mathrm{rank}(\mathbf{T}) = r_{\mathbf{T}}$, the following assumption is considered:

if $\mathbf{T} \succ \mathbf{0}$, then this implies $r_{\mathbf{T}} = N_T$, according to [101, Lemma 5], $\mathrm{rank}(\mathbf{Z}) \geq N_T - 1$. It is claimed that $\mathrm{rank}(\mathbf{Z}) \neq N_T$ due to $\mathbf{Q}_s \neq \mathbf{0}$. Thus, $\mathrm{rank}(\mathbf{Z}) = N_T - 1$ only when $\mathrm{rank}(\mathbf{Q}_s) = 1$ due to the KKT condition $\mathbf{Z}\mathbf{Q}_s = \mathbf{0}$. Therefore, the remaining part is to show that $\mathbf{T} \succ \mathbf{0}$. By exploiting [101, Appendix D], it is concluded that $\mathbf{T} \succ \mathbf{0}$ such that $\mathrm{rank}(\mathbf{Q}_s) = 1$.

This completes the proof of *Theorem* 4.4. ■

4.6.6 Proof of Theorem 4.5

In order to show the rank-one solution of the problem in (4.37), $\mathbf{T}_s$ and $\mathbf{T}_{e,k}$ can be modified as follows:

$$\mathbf{T}_s = \boldsymbol{\Xi}_s + \mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s, \tag{4.73a}$$

$$\mathbf{T}_{e,k} = \boldsymbol{\Xi}_{e,k} - \mathbf{V}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{V}_{e,k}, \tag{4.73b}$$

where

$$\boldsymbol{\Xi}_s = \begin{bmatrix} \mu_s \mathbf{I} & \mathbf{0} \\ \mathbf{0} & -t_s - \mu_s \gamma_s^2, \end{bmatrix}, \mathbf{V}_s = \frac{1}{\sigma_s} \begin{bmatrix} \mathbf{R}_s^{\frac{1}{2}} & \bar{\mathbf{h}}_s \end{bmatrix},$$

$$\boldsymbol{\Xi}_{e,k} = \begin{bmatrix} \mu_k \mathbf{I} & \mathbf{0} \\ \mathbf{0} & t_{e,k} - \mu_{e,k} \gamma_{e,k}^2 \end{bmatrix}, \mathbf{V}_{e,k} = \frac{2^{\frac{R}{2}}}{\sigma_{e,k}} \begin{bmatrix} \mathbf{R}_{e,k}^{\frac{1}{2}} & \bar{\mathbf{h}}_{e,k} \end{bmatrix}.$$

Then, the Lagrange dual function to problem (4.37) is written by replacing (4.37b) and (4.37c) with (4.73a) and (4.73b), respectively,

$$\mathcal{L}(\mathbf{Q}_s, \mathbf{Z}, \mathbf{A}_s, \mathbf{A}_{e,k}, \nu_k, \lambda_s, \lambda_{e,k}) = \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Q}_s \mathbf{Z}) - \mathrm{Tr}(\mathbf{T}_s \mathbf{A}_s) - \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{T}_{e,k} \mathbf{A}_{e,k})$$
$$- \sum_{k=1}^{K} \nu_k (t_s - t_{e,k} - 2^R + 1) - \lambda_s \mu_s - \sum_{k=1}^{K} \lambda_{e,k} \mu_{e,k}, \tag{4.74}$$

where $\mathbf{Z}$, $\mathbf{A}_s$, $\mathbf{A}_{e,k}$, ν_k, λ_s and $\lambda_{e,k}$ are dual variables associated with $\mathbf{Q}_s$, $\mathbf{T}_s$, $\mathbf{T}_{e,k}$, μ_s, $\mu_{e,k}$, and (4.37a), respectively. The relevant KKT conditions are considered as follows:

$$\frac{\partial \mathcal{L}}{\partial \mathbf{Q}_s} = \mathbf{0}, \tag{4.75a}$$

$$\mathbf{Q_s Z} = \mathbf{0}, \tag{4.75b}$$

$$\mathbf{T}_s \mathbf{A}_s = \mathbf{0}, \tag{4.75c}$$

$$\mathbf{A}_s \succeq \mathbf{0}, \mathbf{A}_{e,k} \succeq \mathbf{0}, \mathbf{Q}_s \succeq \mathbf{0}, \lambda_s \geq 0. \tag{4.75d}$$

From (4.75a),

$$\frac{\partial \mathcal{L}}{\partial \mathbf{Q}_s} = \mathbf{I} - \mathbf{Z} - \mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^H + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{S}_{e,k}^{(n,n)} = 0, \tag{4.76}$$

where $\mathbf{S}_{e,k}^{(n,n)} \in \mathbb{H}_+^{N_T}$ is a block submatrix of $\mathbf{V}_{e,k}\mathbf{A}_{e,k}\mathbf{V}_{e,k}^H$.

$$\mathbf{V}_{e,k}\mathbf{A}_{e,k}\mathbf{V}_{e,k}^H = \begin{bmatrix} \mathbf{S}_{e,k}^{(1,1)} & \cdots & \mathbf{S}_{e,k}^{(1,N_{E,k})} \\ \vdots & \ddots & \vdots \\ \mathbf{S}_{e,k}^{(N_{E,k},1)} & \cdots & \mathbf{S}_{e,k}^{(N_{E,k},N_{E,k})} \end{bmatrix}. \tag{4.77}$$

By premultiplying $\mathbf{Q}_s$ by both sides of (4.76),

$$\mathbf{Q}_s\left(\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{S}_{e,k}^{(n,n)}\right) = \mathbf{Q}_s\mathbf{V}_s\mathbf{A}_s\mathbf{V}_s^H \tag{4.78}$$

From the above equality, one can observe the following rank relations,

$$\text{rank}(\mathbf{Q}_s) = \text{rank}\left[\mathbf{Q}_s\left(\mathbf{I}+\sum_{k=1}^{K}\sum_{n=1}^{N_{E,k}}\mathbf{S}_{e,k}^{(n,n)}\right)\right] = \text{rank}\left(\mathbf{Q}_s\mathbf{V}_s\mathbf{A}_s\mathbf{V}_s^H\right). \tag{4.79}$$

In order to prove $\text{rank}(\mathbf{Q}_s) \leq 1$, it will be shown that $\text{rank}(\mathbf{Q}_s\mathbf{V}_s\mathbf{A}_s\mathbf{V}_s^H) \leq 1$ holds. Due to (4.75c), we postmultiply $\mathbf{V}_s^H$ by the two sides of this KKT condition,

$$\boldsymbol{\Xi}_s\mathbf{A}_s\mathbf{V}_s^H+\mathbf{V}_s^H\mathbf{Q}_s\mathbf{V}_s\mathbf{A}_s\mathbf{V}_s^H=\mathbf{0}. \tag{4.80}$$

As a result of the following equalities,

$$\begin{aligned} \frac{1}{\sigma_s}\begin{bmatrix}\mathbf{R}_s^{\frac{1}{2}} & \mathbf{0}\end{bmatrix}\boldsymbol{\Xi}_s &= \mu_s\left(\mathbf{V}_s-\frac{1}{\sigma_s}\begin{bmatrix}\mathbf{0} & \bar{\mathbf{h}}_s\end{bmatrix}\right), \\ \frac{1}{\sigma_s}\begin{bmatrix}\mathbf{R}_s^{\frac{1}{2}} & \mathbf{0}\end{bmatrix}\mathbf{V}_s^H &= \frac{1}{\sigma_s^2}\mathbf{R}_s. \end{aligned}$$

By premultiplying both sides of (4.80) by $\frac{1}{\sigma_s}\begin{bmatrix}\mathbf{R}_s^{\frac{1}{2}} & \mathbf{0}\end{bmatrix}$,

$$\begin{aligned} &\mu_s\left(\mathbf{V}_s-\frac{1}{\sigma_s}\begin{bmatrix}\mathbf{0} & \bar{\mathbf{h}}_s\end{bmatrix}\right)\mathbf{A}_s\mathbf{V}_s^H+\frac{1}{\sigma_s^2}\mathbf{R}_s\mathbf{Q}_s\mathbf{V}_s\mathbf{A}_s\mathbf{V}_s^H=\mathbf{0}, \\ \Rightarrow &\left(\mu_s\mathbf{I}+\frac{1}{\sigma_s^2}\mathbf{R}_s\mathbf{Q}_s\right)\mathbf{V}_s\mathbf{A}_s\mathbf{V}_s^H=\frac{\mu_s}{\sigma_s}\begin{bmatrix}\mathbf{0} & \bar{\mathbf{h}}_s\end{bmatrix}\mathbf{A}_s\mathbf{V}_s^H. \end{aligned} \tag{4.81}$$

Now, the following two scenarios for the equality (4.81) are provided. First, the scenario when $\mu_s = 0$ is discussed. From (4.73a),

$$\mathbf{T}_s = \begin{bmatrix}\mathbf{0} & \mathbf{0} \\ \mathbf{0} & -t_s\end{bmatrix}+\mathbf{V}_s^H\mathbf{Q}_s\mathbf{V}_s. \tag{4.82}$$

Assuming that $\text{rank}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s) = r_s$, it thus straightforwardly follows from (4.82) that

$$\text{rank}(\mathbf{T}_s) \geq \text{rank}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s) - \text{rank} \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & t_s \end{bmatrix} = r_s - 1,$$
$$\Rightarrow \text{rank}(\text{null}(\mathbf{T}_s)) \leq N_T + 1 - (r_s - 1). \quad (4.83)$$

Assuming that there exists at least one ξ that lies in the null space of $\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s$ such that $\mathbf{Q}_s^{\frac{1}{2}} \mathbf{V}_s \xi = \mathbf{0}$. This assumption holds true, since $\text{null}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s)$ is non-empty, due to $\text{rank}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s) < (N_T + 1)$. Pre-multiply ξ^H and postmultiply ξ on both sides of (4.82),

$$\xi^H \mathbf{T}_s \xi = \xi^H \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -t_s \end{bmatrix} \xi \geq 0. \quad (4.84)$$

It is easily verified that $\xi^H \mathbf{T}_s \xi = 0$ due to $t_s > 0$ and therefore,

$$\forall \xi \in \text{null}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s) \Rightarrow \xi \in \text{null}(\mathbf{T}_s),$$
$$\Rightarrow \text{null}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s) \subseteq \text{null}(\mathbf{T}_s). \quad (4.85)$$

According to (4.85),

$$\text{rank}(\text{null}(\mathbf{V}_s^H \mathbf{Q}_s \mathbf{V}_s)) \leq \text{rank}(\text{null}(\mathbf{T}_s)),$$
$$\Rightarrow \text{rank}(\text{null}(\mathbf{T}_s)) \geq N_T + 1 - r_s. \quad (4.86)$$

Combining (4.83) with (4.86),

$$N_T + 1 - r_s \leq \text{rank}(\text{null}(\mathbf{T}_s)) \leq N_T + 1 - (r_s - 1). \quad (4.87)$$

Since $\mathbf{T}_s \mathbf{A}_s = \mathbf{0}$,

$$N_T + 1 - r_s \leq \text{rank}(\mathbf{A}_s) \leq N_T + 1 - (r_s - 1). \quad (4.88)$$

Accordingly, $\mathbf{A}_s$ is of the following structure:

$$\mathbf{A}_s = \sum_{i=1}^{N_T+1-r_s} \alpha_i \xi_i \xi_i^H + \beta \eta \eta^H, \ (\alpha_i > 0, \forall i, \ \beta \geq 0). \tag{4.89}$$

If $\beta = 0$, then

$$\mathbf{Q}_s \mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^H = \mathbf{Q}_s^{\frac{1}{2}} \mathbf{Q}_s^{\frac{1}{2}} \mathbf{V}_s \left(\sum_{i=1}^{N_T+1-r_s} \alpha_i \xi_i \xi_i^H \right) \mathbf{V}_s^H = \mathbf{Q}_s^{\frac{1}{2}} \sum_{i=1}^{N_T+1-r_s} \alpha_i \left(\mathbf{Q}_s^{\frac{1}{2}} \mathbf{V}_s \xi_i \xi_i^H \mathbf{V}_s^H \right) = \mathbf{0}. \tag{4.90}$$

Together with (4.79), $\text{rank}(\mathbf{Q}_s) = 0$ holds, which contradicts to the optimality of the problem (4.8a). Therefore, $\beta > 0$ and

$$\begin{aligned} \mathbf{Q}_s \mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^H &= \mathbf{Q}_s^{\frac{1}{2}} \mathbf{Q}_s^{\frac{1}{2}} \mathbf{V}_s^H \left(\sum_{i=1}^{N_T+1-r_s} \alpha_i \xi_i \xi_i^H + \beta \eta \eta^H \right) \mathbf{V}_s = \mathbf{Q}_s^{\frac{1}{2}} \left(\mathbf{0} + \beta \mathbf{Q}_s^{\frac{1}{2}} \mathbf{V}_s \eta \eta^H \mathbf{V}_s^H \right) \\ &= \beta \mathbf{Q}_s \mathbf{V}_s \eta \eta^H \mathbf{V}_s^H. \end{aligned} \tag{4.91}$$

One can easily observe from (4.91) that $\text{rank}(\mathbf{Q}_s \mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^H) \leq \text{rank}(\eta \eta^H) = 1$. Moreover, the case of $\mu_s > 0$ is provided, since $\mu_s \mathbf{I} + \frac{1}{\sigma_s^2} \mathbf{R}_s \mathbf{Q}_s$ is of full-rank, according to (4.81),

$$\begin{aligned} \text{rank}(\mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^H) &= \text{rank} \left[\frac{\mu_s}{\sigma_s} \left(\mu_s \mathbf{I} + \frac{1}{\sigma_s^2} \mathbf{R}_s \mathbf{Q}_s \right)^{-1} \left[\begin{array}{cc} \mathbf{0} & \bar{\mathbf{h}}_s \end{array} \right] \mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^H \right] \\ &\leq \text{rank} \left(\left[\begin{array}{cc} \mathbf{0} & \bar{\mathbf{h}}_s \end{array} \right] \right) \leq 1, \Rightarrow \text{rank}(\mathbf{Q}_s \mathbf{V}_s \mathbf{A}_s \mathbf{V}_s^{\mathbf{H}}) \leq 1, \end{aligned} \tag{4.92}$$

which completes the proof of *Theorem* 4.5. ■

Chapter 5

Transmit Optimization for MIMO Secure Communications with Cooperative Jammer

In this chapter, transmit optimization for multiple-input multiple-output (MIMO) secrecy channel is investigated to solve the secrecy rate optimization problems (i.e., power minimization and secrecy rate maximization), where a multi-antenna cooperative jammer (CJ) is employed to enhance secret communication in the presence of a multi-antenna eavesdropper. For this secrecy network, the main contributions are presented as follows:

1. *Secrecy rate optimization*: First, two secrecy optimization problems, namely, power minimization and secrecy rate maximization are considered based on the assumption that the legitimate transmitter perfectly knows the channel state information (CSI) of the legitimate receiver and the eavesdropper. Both optimization problems are not jointly convex due to the transmit covariance matrices of the transmitter and the CJ. To circumvent the non-convexity issues, the transmit covariance matrices of the legitimate transmitter and the CJ are designed alternatively. For a given transmit covariance matrix at the CJ, the secrecy rate optimization problems are reformulated into convex ones by a first-order Taylor approximation. Then, an iterative algorithm to solve both approximated problems is proposed based on dual problem and subgradient method.

2. *Robust secrecy rate optimization*: In the previous optimization problems, it is

assumed that the transmitters have the perfect CSI of the eavesdropper channel. However, it is generally difficult that the perfect CSI is available at the transmitter due to lack of cooperation between the legitimate transmitters and the eavesdropper as well as the channel estimation errors. In order to incorporate the imperfect eavesdropper CSI, robust optimization techniques based on the worst-case secrecy rates is considered. An alternative optimization algorithm is proposed, where the transmit covariance matrices of the legitimate transmitter and the CJ are optimally designed, alternatively. It is shown that the robust secrecy rate maximization problem can be reformulated into a semidefinite programming (SDP) by exploiting the *S-Procedure*.

3. *Secrecy Rate Maximization based on Game Theory*: Finally, the secrecy rate maximization problem is considered based on game theory, where the jammer is considered as a private CJ who introduces charges for its jamming service based on the amount of the interference caused to the eavesdropper. Moreover, the legitimate transmitter 'pays' for this jamming service to improve the achieved secrecy rate. This secrecy rate maximization problem is formulated as a *Stackelberg* game, where the private CJ and the transmitter are modelled as the leader and follower of the game, respectively, both of them try to maximize their own revenues. For the proposed game, a *Stakelberg* equilibrium is analytically derived where both the transmitter and the private CJ come to an agreement on the interference requirement at the eavesdropper and the interference price.

5.1 System Model

In this chapter, a MIMO wiretap channel is considered as shown in Fig. 5.1, where a multi-antenna transmitter establishes secure communication with a multi-antenna receiver in the presence of a multi-antenna eavesdropper, and a multi-antenna CJ assists the secured communication between the legitimate terminals by providing its jamming service to interfere the eavesdropper. It is assumed that the transmitter and the CJ consist of with N_T and N_J transmit antennas, respectively, whereas the legitimate receiver and the eavesdropper is equipped with M_R and M_E receive antennas, respectively. The channel coefficients between the legitimate transmitter

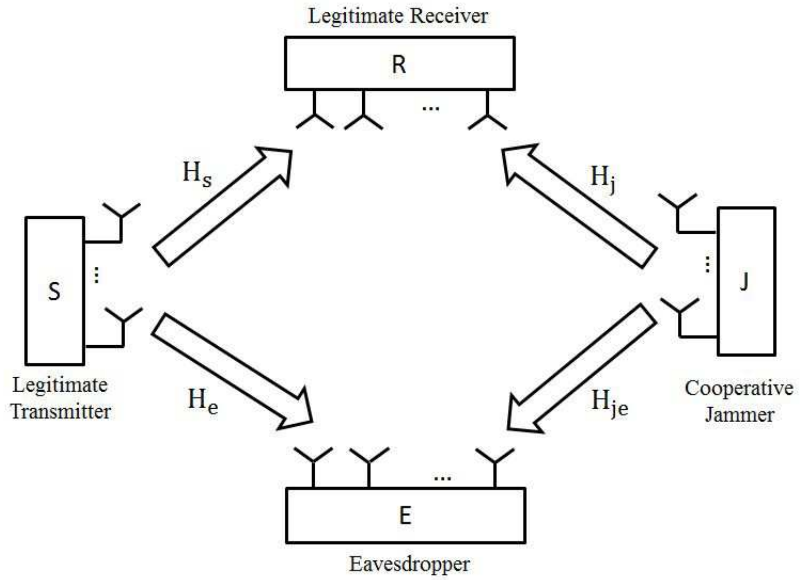

Figure 5.1: A MIMO secrecy channel with a CJ in the presence of a multi-antenna eavesdropper

and the legitimate receiver as well as the eavesdropper are denoted by $\mathbf{H}_s \in \mathbb{C}^{\mathrm{M}_R \times \mathrm{N}_T}$ and $\mathbf{H}_e \in \mathbb{C}^{\mathrm{M}_E \times \mathrm{N}_T}$, respectively. On the other hand, $\mathbf{H}_j \in \mathbb{C}^{\mathrm{M}_R \times \mathrm{N}_J}$ and $\mathbf{H}_{je} \in \mathbb{C}^{\mathrm{M}_E \times \mathrm{N}_J}$ represent the channel coefficients between the CJ and the legitimate receiver as well as the eavesdropper, respectively. The received signals at the legitimate receiver and the eavesdropper are written as

$$\mathbf{y}_r = \mathbf{H}_s\mathbf{x}_1 + \mathbf{H}_j\mathbf{x}_2 + \mathbf{n}_r, \quad \mathbf{y}_e = \mathbf{H}_e\mathbf{x}_1 + \mathbf{H}_{je}\mathbf{x}_2 + \mathbf{n}_e, \tag{5.1}$$

where $\mathbf{x}_1 \in \mathbb{C}^{N_T \times 1}$ is the signal vector intended for the legitimate user, whereas $\mathbf{x}_2 \in \mathbb{C}^{N_J \times 1}$ represents the jamming signal vector. $\mathbf{n}_r \in \mathbb{C}^{M_R \times 1}$ and $\mathbf{n}_e \in \mathbb{C}^{M_E \times 1}$ are the noise vectors at the legitimate receiver and the eavesdropper, and assumed to be zero-mean circularly symmetric Gaussian random variables with covariance matrices $\sigma_r^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$, respectively. The transmit covariance matrices of the transmitter and the CJ are defined as $\mathbf{Q}_1 = \mathbb{E}\left\{\mathbf{x}_1\mathbf{x}_1^H\right\}$ and $\mathbf{Q}_2 = \mathbb{E}\left\{\mathbf{x}_2\mathbf{x}_2^H\right\}$. Thus, the achieved secrecy rate is written as [18]:

$$\begin{aligned} R_{sr} = [\mathcal{I}_r - \mathcal{I}_e]^+ = \Bigg[& \log \frac{\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|}{\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|} \\ & - \log \frac{\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right|}{\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right|}\Bigg]^+, \end{aligned} \tag{5.2}$$

where $\mathcal{I}_r$ and $\mathcal{I}_e$ are the mutual information of the legitimate receiver and the eavesdropper, whereas $\mathbf{Q}_1(\succeq \mathbf{0})$ and $\mathbf{Q}_2(\succeq \mathbf{0})$ are the transmit covariance matrices of the legitimate user and the CJ, respectively.

5.2 Secrecy Rate Optimizations

In this section, two secrecy rate optimization problems, namely, power minimization and secrecy rate maximization are formulated. The power minimization problem can be written as

$$\min_{\mathbf{Q}_1,\mathbf{Q}_2} \ \mathrm{Tr}(\mathbf{Q}_1)+\mathrm{Tr}(\mathbf{Q}_2), \quad s.t. \ R_{sr} \geq \bar{R}_{sr}, \mathbf{Q}_1 \succeq 0, \ \mathbf{Q}_2 \succeq 0, \tag{5.3}$$

where $\bar{\mathbf{R}}_{sr}$ is the required secrecy rate. Assume that the legitimate transmitter and the CJ have perfect CSI (i.e., $\mathbf{H}_e$ and $\mathbf{H}_{je}$) of the eavesdropper, which can be estimated through local oscillator power leakage from the eavesdropper receiver's RF frontend [102]. The power minimization problem (5.3) requires a certain amount of power to satisfy the predefined secrecy rate, however, it might turn out to be infeasible due to insufficient transmit power. To overcome this infeasibility issue, transmit optimization is developed to maximize the achieved secrecy rate with the transmit power constraint. Thus, this secrecy rate maximization problem is expressed as

$$\max_{\mathbf{Q}_1,\mathbf{Q}_2} \ R_{sr}, \quad s.t. \ \mathrm{Tr}(\mathbf{Q}_1) \leq P_1, \mathbf{Q}_1 \succeq 0, \mathrm{Tr}(\mathbf{Q}_2) \leq P_2, \mathbf{Q}_2 \succeq 0, \tag{5.4}$$

where P_1 and P_2 are the maximum available transmit power at the legitimate transmitter and the CJ, respectively. Unfortunately, both optimization problems are not jointly convex in terms of transmit covariance matrices $\mathbf{Q}_1$ and $\mathbf{Q}_2$, and cannot be solved directly. Therefore, each original problem can be divided into two subproblems and design the transmit covariance matrix of the legitimate transmitter (i.e., $\mathbf{Q}_1$) for a fixed jammer transmit covariance matrix (i.e., $\mathbf{Q}_2$). The legitimate transmit covariance matrix can be optimally designed by a first-order Taylor approximation, which will be discussed in the following section. On the other hand, the transmit covariance matrix of the CJ (i.e., $\mathbf{Q}_2$) can be optimally designed based on a null space scheme and CJ maximization method, which will be shown in the following.

5.2.1 Null Space Method

In this subsection, a null space scheme is considered, where the CJ transmit covariance matrix is designed to ensure that it lies in the null space of the channel between the CJ and the legitimate receiver (i.e., $\mathbf{H}_j$). Here, it is assumed that the number of antennas at the CJ is greater than that of the eavesdropper. Thus the null space vectors are expressed such that satisfy $\mathbf{H}_j\mathbf{U} = \mathbf{0}$ as

$$\mathbf{U} = \left(\mathbf{I} - \mathbf{H}_j^H(\mathbf{H}_j\mathbf{H}_j^H)^{-1}\mathbf{H}_j\right)\mathbf{H}_{je}\mathbf{D}_1, \tag{5.5}$$

where $\mathbf{D}_1$ is a diagonal matrix, which controls the power allocation, satisfying the total transmit power constraint at the CJ. Thus, the rate maximization between the CJ and the eavesdropper is written as

$$\max_{\mathbf{D}} \; \log|\mathbf{I} + \mathbf{V}|, \quad s.t.\ \mathrm{Tr}\left(\mathbf{P}\mathbf{H}_{je}^H\mathbf{D}\mathbf{H}_{je}\mathbf{P}^H\right) \leq P_2,\ \mathbf{D} \succeq 0, \tag{5.6}$$

where $\mathbf{D} = \mathbf{D}_1^2$, $\mathbf{V} = \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{P}\mathbf{H}_{je}^H\mathbf{D}\mathbf{H}_{je}\mathbf{P}^H\mathbf{H}_{je}^H$ and $\mathbf{P} = \mathbf{I} - \mathbf{H}_j^H(\mathbf{H}_j\mathbf{H}_j^H)^{-1}\mathbf{H}_j$. The problem in (5.6) is convex and easily solved by using interior-point methods [87]. Thus, the CJ transmit covariance matrix can be obtained $\mathbf{Q}_2 = \mathbf{U}\mathbf{U}^H$.

5.2.2 Maximizing Cooperative Jammer Rate

In order to introduce more interference to interfere the eavesdropper, the rate between the CJ and the eavesdropper is maximized while minimizing the interference to the legitimate receiver. Hence, the jammer transmit covariance matrix $\mathbf{Q}_2$ is optimally designed by maximizing the difference between the jammer-eavesdropper rate and the jammer-legitimate user rate with the CJ transmit power constraint. Thus, the optimization problem is formulated as

$$\begin{aligned} &\max_{\mathbf{Q}_2 \succeq 0} R_j \triangleq \log\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right| - \log\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|, \\ &\quad s.t.\ \mathrm{Tr}(\mathbf{Q}_2) \leq P_2, \mathbf{Q}_2 \succeq 0. \end{aligned} \tag{5.7}$$

The problem defined in (5.7) is not convex due to the non-convex objective function. Hence, the objective function is linearized by the first-order Taylor approximation

[48] at a given $\tilde{\mathbf{Q}}_2$ as

$$\begin{aligned}\max_{\mathbf{Q}_2} \tilde{R}_j \triangleq \log\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right| - \log\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\tilde{\mathbf{Q}}_2\mathbf{H}_j^H\right| \\ - \operatorname{Tr}\left[\frac{1}{\sigma_r^2}\left(\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\tilde{\mathbf{Q}}_2\mathbf{H}_j^H\right)^{-1}\mathbf{H}_j(\mathbf{Q}_2 - \tilde{\mathbf{Q}}_2)\mathbf{H}_j^H\right] \\ s.t.\ \operatorname{Tr}(\mathbf{Q}_2) \leq \mathbf{P}_2,\ \mathbf{Q}_2 \succeq 0. \qquad (5.8)\end{aligned}$$

The problem (5.8) is easily shown to be convex and hence $\mathbf{Q}_2$ can be obtained iteratively by solving (5.8). The proposed iterative algorithm for optimizing the CJ transmit covariance matrix $\mathbf{Q}_2$ is summarized in Table 5.1.

The approximated transmit covariance matrix $\tilde{\mathbf{Q}}_2$ can be updated at each iteration by $\mathbf{Q}_2^*$, which is obtained from the previous iteration. It is noted that $\mathbf{Q}_2$ is equal to $\mathbf{Q}_2^*$ at the convergence of the proposed algorithm, which confirms that the approximated rate $\tilde{R}_j$ is equal to the actual rate R_j.

Table 5.1: Cooperative jammer rate maximization algorithm

1. Initialize: $\tilde{\mathbf{Q}}_2 = \mathbf{0}$.
2. **Repeat**
   (a) Solve (5.8) to obtain $\mathbf{Q}_2^*$ for a given $\tilde{\mathbf{Q}}_2$.
   (b) Update $\tilde{\mathbf{Q}}_2 \leftarrow \mathbf{Q}_2^*$.
3. **Until** the required accuracy.

5.2.3 Power Minimization with Secrecy Rate Constraint

In the previous subsections, the CJ transmit covariance matrix $\mathbf{Q}_2^*$ has been designed by employing the null space method and the CJ rate maximization. Here, the transmit covariance matrix of the legitimate transmitter $\mathbf{Q}_1$ is optimally designed to minimize the transmit power such that it satisfies the achieved secrecy rate. This power minimization problem is formulated as

$$\min_{\mathbf{Q}_1\succeq 0} \operatorname{Tr}(\mathbf{Q}_1), \quad s.t.\ R_{sr} = \log \frac{\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2^*\mathbf{H}_j^H\right|}{\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2^*\mathbf{H}_j^H\right|} - \log \frac{\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right|}{\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right|} \geq \bar{R}_{sr}. \tag{5.9}$$

The problem (5.9) is not convex due to the non-convex secrecy rate constraint. As discussed before, this constraint can be linearized by the first-order Taylor approximation as

$$\begin{aligned} R_{sr} \approx{}& \log\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2^*\mathbf{H}_j^H\right| + \log\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right| \\ &- \log\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2^*\mathbf{H}_j^H\right| - \log\left|\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right| \\ &- \operatorname{Tr}\left[\frac{1}{\sigma_e^2}\left(\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right)^{-1}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H\right] \\ &+ \operatorname{Tr}\left[\frac{1}{\sigma_e^2}\left(\mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H + \frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right)^{-1}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right] \triangleq \tilde{R}_{sr}. \end{aligned} \tag{5.10}$$

The proof is similar to the proof to the problem (5.8). (5.10) is a concave function in terms of $\mathbf{Q}_1$, since the first log term is a concave function and other terms are either linear function or constant. Thus, the approximated problem is modified as

$$\min_{\mathbf{Q}_1\succeq 0} \operatorname{Tr}(\mathbf{Q}_1), \quad s.t.\ \mathbf{Q}_1 \succeq 0, \tilde{R}_{sr} \geq \bar{R}_{sr}. \tag{5.11}$$

One can observe that (5.11) is a convex problem, and can be solved by using interior-point methods. Now, the Lagrange dual problem to (5.11) is considered, which is written as

$$\max_{\lambda\geq 0} \min_{\mathbf{Q}_1\succeq 0} \ L(\mathbf{Q}_1, \lambda) = \operatorname{Tr}(\mathbf{Q}_1) + \lambda\left(\bar{R}_{sr} - \tilde{R}_{sr}\right), \tag{5.12}$$

where λ is the dual multiplier associated with the secrecy rate constraint. Since the problem (5.11) is convex, which satisfies Slater's condition, the duality gap between (5.11) and (5.12) is zero, and the optimal solution to this power minimization problem can be determined by updating the dual multiplier λ by using the subgradient method [78]. The solution to (5.11) is dependent on $\tilde{\mathbf{Q}}_1$, and two initializations are

Table 5.2: Power minimization algorithm

1. Initialize: λ and $\tilde{\mathbf{Q}}_1 = \mathbf{0}$ or $\tilde{\mathbf{Q}}_1 = \mathbf{Q}_{\mathrm{WF}}$.
2. **Iteration loop begin**
   (a) Solve the problem in (5.12) to obtain $\mathbf{Q}_1^*$ for a given λ.
   (b) Update λ based on the sub-gradient method.
3. **Until** the required accuracy.
4. **Iteration loop end**
5. Update $\tilde{\mathbf{Q}}_1 \leftarrow \mathbf{Q}_1^*$.
6. **Until** required accuracy.

considered: a) an all zero element matrix (i.e., $\tilde{\mathbf{Q}}_1 = 0$) and b) a water-filling solution (i.e., $\tilde{\mathbf{Q}}_1 = \tilde{\mathbf{Q}}_{\mathrm{WF}}$). Thus, an iterative algorithm is proposed to find the solution to (5.9), as shown in Table 5.2.

A question may arise with regard to the problem (5.11) on whether the predefined secrecy rate can be satisfied at the convergence of the algorithm. If $\tilde{\mathbf{Q}}_1$ and $\mathbf{Q}_1$ are equal, then the approximated rate ($\tilde{R}_{sr}$) at $\tilde{\mathbf{Q}}_1$ will be equal to the actual secrecy rate (R_{sr}), since the fifth and the sixth terms in the right hand side (RHS) of (5.10) cancel each other, as seen from Fig. 5.2 and Fig. 5.3. Hence, the predefined secrecy rate is satisfied when the algorithm converges.

5.2.4 Secrecy Rate Maximization with Transmit Power Constraint

In the previous section, transmit optimization was performed to minimize the transmit power with the secrecy rate constraint. However, the maximum available transmit power is generally limited such that the power minimization problem might be infeasible due to insufficient transmit power. In this section, the secrecy rate maximization problem is considered to avoid the infeasible issue, where $\mathbf{Q}_1$ can be optimally designed for a given $\mathbf{Q}_2^*$. This optimization problem is written as

$$\max_{\mathbf{Q}_1 \succeq 0} R_{sr}, \quad s.t.\ \mathrm{Tr}(\mathbf{Q}_1) \leq P_1, \quad \mathbf{Q}_1 \succeq 0. \tag{5.13}$$

The problem (5.13) is not convex due to non-convexity of the objective function. Hence, the problem (5.13) is modified with the approximated rate (5.10) as

$$\max_{\mathbf{Q}_1} \quad \tilde{R}_{sr}, \quad s.t. \; \mathrm{Tr}(\mathbf{Q}_1) \leq P_1, \quad \mathbf{Q}_1 \succeq 0. \tag{5.14}$$

The problem (5.14) is convex and can be solved directly. Now, the Lagrange dual method is considered to find the solution to (5.14). First, the dual function to (5.14) is written, similar to Section 5.2.3, as follows:

$$L\left(\mathbf{Q}_1, \lambda, \mathbf{Z}\right) = -\tilde{R}_{sr} + \lambda\left[\mathrm{Tr}(\mathbf{Q}_1) - P_1\right] - \mathrm{Tr}(\mathbf{Z}\mathbf{Q}_1) \tag{5.15}$$

and the corresponding Lagrange dual problem is expressed as

$$\min_{\lambda \geq 0} \quad \max_{\mathbf{Q}_1 \succeq 0} \left[\tilde{R}_{sr} - \lambda[\mathrm{Tr}(\mathbf{Q}_1) - P_1]\right], \tag{5.16}$$

where λ is the dual multiplier associated with the transmission power constraint. The dual problem (5.16) can be solved and the dual variable will be updated based on the subgradient method. The proposed iterative algorithm is similar to Table 5.2. It should be noted that $\tilde{\mathbf{Q}}_1$ is equal to $\mathbf{Q}_1$ when the iterative algorithm converges, which confirms that both the approximated secrecy rate and the achieved secrecy rate are the same.

5.3 Robust Secrecy Rate Optimization

In this section, robust secrecy rate optimization problems are considered for the same secrecy network incorporating channel uncertainty. It is assumed that imperfect CSI of the eavesdropper is available at legitimate transmitter. In the following subsections, the channel uncertainty will be modelled and the associated robust schemes will be presented incorporating the channel errors between the legitimate transmitter and the eavesdropper as well as the CJ and the eavesdropper.

5.3.1 Channel Uncertainty

The imperfect CSI can be modelled based on the deterministic channel model, where it is assumed that the true channels are centered at the mean of the channels [79].

Hence, the actual channels can be modelled as

$$\tilde{\mathbf{H}}_e = \mathbf{H}_e + \mathbf{E}_e, \quad \tilde{\mathbf{H}}_{je} = \mathbf{H}_{je} + \mathbf{E}_{je}, \tag{5.17}$$

where $\mathbf{H}_e$ and $\mathbf{H}_{je}$ represent the channel mean of the corresponding channels, and $\mathbf{E}_e$, and $\mathbf{E}_{je}$ are the corresponding channel errors. It is assumed that the channel means can be obtained at the transmitter by channel estimations. These errors are given by defining the bounds through ellipsoid model as [70]:

$$\varepsilon_1 = \{\mathbf{E}_e : \mathrm{Tr}(\mathbf{E}_e\mathbf{P}_e^{-1}\mathbf{E}_e^H) \leq \varepsilon_e^2\}, \ \varepsilon_2 = \{\mathbf{E}_{je} : \mathrm{Tr}(\mathbf{E}_{je}\mathbf{P}_{je}^{-1}\mathbf{E}_{je}^H) \leq \varepsilon_{je}^2\},$$

where $\mathbf{P}_e$ and $\mathbf{P}_{je}$ are known positive definite matrices, which are assumed to be identity matrices such that the channel errors are considered to be bounded by Fronbenius norms ($||\mathbf{E}_e||_F \leq \varepsilon_e$ and $||\mathbf{E}_{je}||_F \leq \varepsilon_{je}$). ε_e and ε_{je} denote the channel error bounds.

5.3.2 Robust Power Minimization

In this subsection, the robust power minimization problem is proposed optimally design transmit covariance matrices of the legitimate transmitter (i.e., $\mathbf{Q}_1$) and the CJ (i.e., $\mathbf{Q}_2$) incorporating the channel uncertainty shown in Section 5.3.1. This robust power minimization problem can be written as

$$\begin{aligned}
\min_{\mathbf{Q}_1 \succeq \mathbf{0}, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \mathrm{Tr}(\mathbf{Q}_1) + \mathrm{Tr}(\mathbf{Q}_2) \\
s.t. \log & \frac{\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|}{\left|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|} \\
& - \log \frac{\left|\mathbf{I} + \frac{1}{\sigma_e^2}\tilde{\mathbf{H}}_e\mathbf{Q}_1\tilde{\mathbf{H}}_e^H + \frac{1}{\sigma_e^2}\tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right|}{\left|\mathbf{I} + \frac{1}{\sigma_e^2}\tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right|} \geq \bar{R}_{sr}, \\
& \tilde{\mathbf{H}}_e = \mathbf{H}_e + \mathbf{E}_e, \ \tilde{\mathbf{H}}_{je} = \mathbf{H}_{je} + \mathbf{E}_{je}, \ ||\mathbf{E}_e||_F \leq \varepsilon_e, \ ||\mathbf{E}_{je}||_F \leq \varepsilon_{je}.
\end{aligned} \tag{5.18}$$

The problem (5.18) is not convex in terms of the secrecy rate constraint. In order to solve this problem, two sub-problems with $\mathbf{Q}_1$ (or $\mathbf{Q}_2$) only are considered, and an alternative optimization algorithm is presented to design $\mathbf{Q}_1$ ($\mathbf{Q}_2$) for a given $\mathbf{Q}_2$ ($\mathbf{Q}_1$), respectively, each of which is reformulated into a SDP by exploiting linear

Table 5.3: Alternative optimization algorithm

1. Initialize: $\mathbf{Q}_2 = \mathbf{0}$ or $\mathbf{Q}_2 = \mathbf{Q}_{\mathrm{WF}}$; $\tilde{\mathbf{Q}}_1 = \mathbf{Q}_{\mathrm{WF}}$ for approximation.
2. **Iteration loop begin**
   (a) Solve the robust power minimization problem in (5.19) to obtain $\tilde{\mathbf{Q}}_1^*$ for a given $\mathbf{Q}_2$.
   (b) $\mathbf{Q}_1 \leftarrow \tilde{\mathbf{Q}}_1^*$.
   (c) Solve the robust power minimization problem in (5.22) to obtain $\tilde{\mathbf{Q}}_2^*$ for a given $\mathbf{Q}_1$.
   (d) $\mathbf{Q}_2 \leftarrow \tilde{\mathbf{Q}}_2^*$.
3. **Until** the required accuracy.
4. **Iteration loop end**
5. Update $\mathbf{Q}_1^* \leftarrow \tilde{\mathbf{Q}}_1$, and $\mathbf{Q}_2^* \leftarrow \tilde{\mathbf{Q}}_2$.

matrix transformations.

First, $\mathbf{Q}_2$ is assumed to be given to optimally design $\mathbf{Q}_1$ by solving the robust power minimization problem (5.18). By exploiting the first-order Taylor approximation, (5.18) can be written by linearizing the nonconvex secrecy rate constraint as

$$\begin{aligned}
&\min_{\mathbf{Q}_1,\mu_1,t_2} \mathrm{Tr}(\mathbf{Q}_1)\\
&\quad s.t. \log\left|\mathbf{I}+\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H+\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right| - t_1 - \log\left|\mathbf{I}+\frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|\\
&\qquad\quad + \log\left|\mathbf{I}+\frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right| \geq \bar{R}_{sr},\\
&\quad \begin{bmatrix} \mu_1\mathbf{I}-\mathbf{B}_1 & -(\mathbf{Q}_1^T\otimes\mathbf{I})^T\mathbf{a}\\ -\mathbf{a}^H(\mathbf{Q}_1^T\otimes\mathbf{I})^* & -\mu\varepsilon_e^2-\alpha_1+\beta_1+t_1-\mathbf{h}_e^H\mathbf{B}_1\mathbf{h}_e \end{bmatrix} \succeq \mathbf{0},\\
&\quad \mathbf{Q}_1 \succeq \mathbf{0}, \mu_1 \geq 0, t_1 \geq 0,
\end{aligned} \tag{5.19}$$

where

$$
\begin{aligned}
\alpha_1 &= \log\left|\mathbf{I} + \mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H + \mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right|,\\
\beta_1 &= \mathrm{Tr}\left[\left(\mathbf{I} + \mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H + \mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right)^{-1}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right],\\
\mathbf{S}_1 &= \left(\mathbf{I} + \mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H + \mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right)^{-1},\\
\mathbf{B}_1 &= (\mathbf{Q}_1^T \otimes \mathbf{I})^T(\mathbf{I}\otimes\mathbf{S}_1), \mathbf{h}_e = \mathrm{vec}(\mathbf{H}_e), \quad \mathbf{a} = \mathrm{vec}(\mathbf{S}_1\mathbf{H}_e).
\end{aligned}
$$

Proof Please refer to Section 5.7.1. ■

Similarly, $\mathbf{Q}_2$ is optimized for a given $\mathbf{Q}_1$ by solving (5.18), which can be expressed as

$$
\begin{aligned}
&\min_{\mathbf{Q}_2,t_3,t_4} \mathrm{Tr}(\mathbf{Q}_2)\\
&\quad s.t. \log\left|\mathbf{I} + \mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H + \mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right| - \log\left|\mathbf{I} + \mathbf{H}_j\tilde{\mathbf{Q}}_2\mathbf{H}_j^H\right|\\
&\qquad + \mathrm{Tr}\left[\left(\mathbf{I} + \mathbf{H}_j\tilde{\mathbf{Q}}_2\mathbf{H}_j^H\right)^{-1}\mathbf{H}_j\tilde{\mathbf{Q}}_2\mathbf{H}_j^H\right] - \mathrm{Tr}\left[\left(\mathbf{I} + \mathbf{H}_j\tilde{\mathbf{Q}}_2\mathbf{H}_j^H\right)^{-1}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right]\\
&\qquad + \log(t_2) - t_3 \geq \bar{\mathrm{R}}_{sr}, && (5.20\text{a})\\
&\qquad \log\left|\mathbf{I} + \tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right| \geq \log(t_2), && (5.20\text{b})\\
&\qquad \alpha_2 - \beta_2 + \mathrm{Tr}\left[\mathbf{S}_2\tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right] \leq t_3, && (5.20\text{c})\\
&\qquad \mathbf{Q}_2 \succeq \mathbf{0}, \quad t_2 \geq 0, \quad t_3 \geq 0, && (5.20\text{d})
\end{aligned}
$$

where

$$
\begin{aligned}
\alpha_2 &= \log\left|\mathbf{I} + \mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + \mathbf{H}_{je}\tilde{\mathbf{Q}}_2\mathbf{H}_{je}^H\right|,\\
\beta_2 &= \mathrm{Tr}\left[\left(\mathbf{I} + \mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + \mathbf{H}_{je}\tilde{\mathbf{Q}}_2\mathbf{H}_{je}^H\right)^{-1}\mathbf{H}_{je}\tilde{\mathbf{Q}}_2\mathbf{H}_{je}^H\right],\\
\mathbf{S}_2 &= \left(\mathbf{I} + \mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + \mathbf{H}_{je}\tilde{\mathbf{Q}}_2\mathbf{H}_{je}^H\right)^{-1}.
\end{aligned}
$$

The constraints (5.20b) and (5.20c) can be converted into semidefinite constraints similar to (5.19) as

$$\begin{bmatrix} \lambda_1 \mathbf{I} + (\mathbf{Q}_2^T \otimes \mathbf{I}) & (\mathbf{Q}_2^T \otimes \mathbf{I})\mathbf{h}_{je} \\ \mathbf{h}_{je}^H (\mathbf{Q}_2^T \otimes \mathbf{I}) & -\lambda_1 \varepsilon_{je}^2 - t_2 + \mathbf{h}_{je}^H (\mathbf{Q}_2^T \otimes \mathbf{I})\mathbf{h}_{je} + 1 \end{bmatrix} \succeq \mathbf{0}, \tag{5.21a}$$

$$\begin{bmatrix} \lambda_2 \mathbf{I} - \mathbf{B}_2 & -(\mathbf{Q}_2^T \otimes \mathbf{I})^T \mathbf{a}_1 \\ -\mathbf{a}_1^H (\mathbf{Q}_2^T \otimes \mathbf{I})^* & -\lambda_2 \varepsilon_{je}^2 - \alpha_2 + \beta_2 + t_3 - \mathbf{h}_{je}^H \mathbf{B}_2 \mathbf{h}_{je} \end{bmatrix} \succeq \mathbf{0}, \tag{5.21b}$$

where $\mathbf{h}_{je} = \text{vec}(\mathbf{H}_{je})$, $\mathbf{a}_1 = \text{vec}(\mathbf{S}_2 \mathbf{H}_{je})$ and $\mathbf{B}_2 = (\mathbf{Q}_2^T \otimes \mathbf{I})^T (\mathbf{I} \otimes \mathbf{S}_2)$.

Proof Please refer to Section 5.7.2. ■

Hence, the problem (5.20) can be reformulated as

$$\begin{aligned} &\min_{\mathbf{Q}_2, \lambda_1, \lambda_2, t_2, t_3} \text{Tr}(\mathbf{Q}_2), \quad s.t. \ (5.20a), \ (5.21a), \ (5.21b), \ \mathbf{Q}_2 \succeq \mathbf{0}, \\ &\qquad\qquad \lambda_1 \geq 0, \lambda_2 \geq 0, t_2 \geq 0, t_3 \geq 0. \end{aligned} \tag{5.22}$$

Both (5.19) and (5.22) are convex problems, each of which can be solved to optimize $\mathbf{Q}_1$ (or $\mathbf{Q}_2$) by the proposed alternative optimization algorithm as shown in Table 5.3. The same alternative optimization approach can also be applied in the robust secrecy rate maximization problem, where the same linear matrix transformations can also be employed to reformulate this nonconvex problem.

5.4 Secrecy Rate Optimization Based on Game Theory

In the previous sections, secrecy rate optimization problems have been solved with the help of a multi-antenna CJ. However, it is not always possible to have our own CJ to improve the secure communications. Another option is to employ the private CJ by paying some charges for the jamming service. The private CJ charges for this jamming service with the amount of interference caused to the eavesdropper. Here, the main focus is to seek optimal power allocation at the private CJ which determines the cost needed to be paid by the legitimate transmitter. In this section, the private CJ is considered to have single antenna for convenience. In the case of multi-antenna at the CJ, the corresponding beamformer will be designed independently so that the multiple antennas scenario with a fixed beamformer can be formulated into the same problem as with single antenna.

5.4.1 Stackelberg Game

The achieved secrecy rate at the legitimate receiver is written with single antenna private CJ as

$$R_s = \log|\mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H| - \log\frac{\left|\mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + p_1\mathbf{g}\mathbf{g}^H)\right|}{|\mathbf{I} + \frac{1}{\sigma_e^2}p_1\mathbf{g}\mathbf{g}^H|}, \tag{5.23}$$

where $\mathbf{g}$ is the channel between the private CJ and the eavesdropper and p_1 is the power allocation at the private CJ. The private CJ aims to maximize its revenue by selling the interference to the legitimate transmitter. This private CJ revenue function is written as

$$U_j(p_1, \mu_0) = \mu_0 p_1\|\mathbf{g}\|_2^2, \tag{5.24}$$

where μ_0 is the unit interference price charged by the private CJ to cause the interference to the eavesdropper. According to the interference requirement at the eavesdropper, the interference price should be decided by the private CJ to maximize its revenue. The optimal price can be achieved by solving the following problem:
Problem (A):

$$\max_{\mu_0} \; U_j(p_1, \mu_0), \quad s.t. \; \mu_0 \geq 0. \tag{5.25}$$

In order to compensate for the interference charge from the private CJ, the legitimate transmitter pays the CJ service for maintaining secured communication. In addition, the legitimate transmitter should maximize its revenue by introducing the interference to improve the achieved secrecy rate at the legitimate user. Thus, the revenue function of the legitimate transmitter can be defined as

$$\begin{aligned} U_L(\mathbf{Q}_1, p_1) &= \lambda_0 R_s - \mu_0 p_1 \|\mathbf{g}\|_2^2 \\ &= \lambda_0 \Bigg(\log \left| \mathbf{I} + \frac{1}{\sigma_r^2} \mathbf{H}_s \mathbf{Q}_1 \mathbf{H}_s^H \right| - \log \left| \mathbf{I} + \frac{1}{\sigma_e^2} (\mathbf{H}_e \mathbf{Q}_1 \mathbf{H}_e^H + p_1 \mathbf{g}\mathbf{g}^H) \right| \Bigg) \\ &\quad + \lambda_0 \log |\mathbf{I} + \frac{1}{\sigma_e^2} p_1 \mathbf{g}\mathbf{g}^H| - \mu_0 p_1 \|\mathbf{g}\|_2^2, \end{aligned} \tag{5.26}$$

where λ_0 is the unit price for the secrecy rate. Hence, the legitimate transmitter should design the transmit covariance matrix and decide the interference requirement to maximize its revenue. This optimization problem is formulated as
Problem (B):

$$\max_{\mathbf{Q}_1, p_1} U_L(\mathbf{Q}_1, p_1), \quad s.t.\ \mathbf{Q}_1 \succeq \mathbf{0}, p_1 \geq \mathbf{0}. \tag{5.27}$$

Problem (A) and *Problem (B)* can form a *Stackelberg* game, where the private CJ (leader) announces the interference price, then the legitimate transmitter (follower) decides the amount of interference required at the eavesdropper. The solution of this game can be achieved by exploiting the *Stackelberg* equilibrium, where both the legitimate transmitter and the private CJ come to an agreement on the interference requirement and the interference price. The deviation of either the legitimate transmitter or the private CJ from the *Stackelberg* equilibrium will introduce a loss in their revenues.

5.4.2 Stackelberg Equilibrium

The *Stackelberg* equilibrium for the proposed game is defined as follows:
Stackelberg equilibrium: Let $\mathbf{Q}_1^*$ and p_1^* be the optimal solution for *Problem (B)*, whereas μ_0^* is the best price for *Problem (A)*. The solutions $\mathbf{Q}_1^*$, p_1^* and μ_0^* can be defined as the *Stackelberg* equilibrium if the following conditions hold for any set of $\mathbf{Q}_1$, p_1 and μ_0:

$$U_L(\mathbf{Q}_1^*, p_1^*, \mu_0^*) \geq U_L(\mathbf{Q}_1, p_1, \mu_0^*),\ U_j(\mathbf{Q}_1^*, p_1^*, \mu_0^*) \geq U_j(\mathbf{Q}_1^*, p_1^*, \mu_0).$$

5.4.3 Solution of Proposed Stackelberg Game

According to the definition of *Stackelberg* equilibrium shown in Section 5.4.2, the best responses of the follower (the legitimate transmitter) and the leader (the jammer) can be achieved by solving *Problem (B)* and *Problem (A)*, respectively. Since, the leader (private CJ) obtains the optimal interference requirement from the legitimate transmitter, the best response of the follower (the legitimate transmitter) should be derived first in terms of the interference price. For the proposed game, *Stackelberg* equilibrium can be derived by solving *Problem (B)* to obtain p_1^* for a given $\mathbf{Q}_1$, then the best interference price μ_0^* can be achieved by solving *Problem (A)*.

First, the interference requirement p_1 can be obtained for a given $\mathbf{Q}_1$ by solving *Problem (B)*, where the following *lemma* holds

Lemma 5.1 *The problem* (5.27) *for a given* $\mathbf{Q}_1$ *is a convex problem in terms of* p_1.

Proof Please refer to Section 5.7.3. ■

From *Lemma* 5.1, the optimal solution p_1^* satisfy the following Karush-Kuhn-Tucker (KKT) condition:

$$\frac{\partial U_L(\mathbf{Q}_1, p_1)}{\partial p_1} = 0,\ \lambda_0 \mathrm{Tr}[\mathbf{A}_1^{-1}\mathbf{g}\mathbf{g}^H - \mathbf{A}_2^{-1}\mathbf{g}\mathbf{g}^H] - \mu_0\|\mathbf{g}\|_2^2 = 0, \tag{5.28}$$

where

$$\mathbf{A}_1 = \left(\mathbf{I} + \frac{p_1}{\sigma_e^2}\mathbf{g}\mathbf{g}^H\right),\quad \mathbf{A}_2 = \mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + p_1\mathbf{g}\mathbf{g}^H).$$

From the KKT conditions in (5.28), the closed form solution of p_1 can be easily derived as follows:

$$p_1^* = \frac{-\frac{c_1+c_2}{\sigma_e^2} + \sqrt{\frac{(c_1-c_2)^2}{\sigma_e^4} + \frac{4\lambda_0 c_1 c_2 (c_1-c_2)}{\mu_0\|\mathbf{g}\|^2}}}{2\frac{c_1 c_2}{\sigma_e^4}}, \tag{5.29}$$

where $c_1 = \mathbf{g}^H\mathbf{g}$, $c_2 = \mathbf{g}^H\mathbf{A}^{-1}\mathbf{g}$ and $\mathbf{A} = \mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H$, and the proof is provided in Section 5.7.4. Then, the best response of the private CJ can be obtained for a given interference requirement (i.e., p_1) by solving the following problem:

$$\max_{\mu_0}\ U_j(p_1^*, \mu_0),\quad s.t.\ \mu_0 \geq 0. \tag{5.30}$$

Substituting (5.30) with (5.29), the optimal solution of μ_0 can be derived by the following *Lemma*:

Lemma 5.2 *The problem* (5.30) *for a fixed* $\mathbf{Q}_1$ *is a convex problem in terms of* μ_0*, and the optimal solution of* μ_0 *can be expressed as*

$$\mu_0^* = \frac{e}{x\|\mathbf{g}\|^2}, \tag{5.31}$$

where

$$\begin{aligned} x &= -\frac{\frac{d\|\mathbf{g}\|^2}{2a} - \frac{\frac{b^2\|\mathbf{g}\|^4}{4a^2} + \frac{b\|\mathbf{g}\|^2}{2a}\sqrt{\frac{(b^2-d)\|\mathbf{g}\|^4}{4a^2}}}{\frac{\|\mathbf{g}\|^2}{2a}}}{\frac{\|\mathbf{g}\|^2}{4a}} \\ &= -2(d - b^2 - b\sqrt{b^2-d}) \\ &= 2\sqrt{b^2-d}(\sqrt{b^2-d}+b), \end{aligned} \tag{5.32}$$

where $a = \frac{c_1 c_2}{\sigma_e^4}$, $b = \frac{c_1+c_2}{\sigma_e^2}$, $d = \frac{(c_1-c_2)^2}{\sigma_e^4}$ *and* $e = 4\lambda_0 c_1 c_2 (c_1 - c_2)$.

Proof Please refer to Section 5.7.4. ■

Hence, both revenue functions of the legitimate transmitter and the private CJ are concave in terms of p_1 and μ_0, respectively. This confirms that there exists a *Stackelberg* equilibrium (p_1^*, μ_0^*) for the proposed *Stackelberg* game. To achieve this *Stackelberg* equilibrium, first, the private CJ announces a relatively low interference price μ_0, for which the legitimate transmitter determines the optimal interference requirement at the eavesdropper. Then, the private CJ increases the interference price by a small amount provided its revenue function increases with the interference price. Otherwise, it will reduce the interference price by a small amount. This procedure will be carried out until the maximum private CJ revenue is achieved which is a *Stackelberg* equilibrium. It is noted that the deviation from this equilibrium will result in a loss to either the legitimate transmitter or the private CJ.

5.5 Simulation Results

Simulation results are provided to validate the proposed algorithms for the secrecy network as shown in Section 5.1. It is assumed that the legitimate transmitter and the CJ consist of four ($\mathrm{N}_T = \mathrm{N}_J = 4$) antennas whereas the legitimate receiver and the eavesdropper are equipped with three ($M_R = M_E = 3$) antennas. The maximum available transmit power at both the legitimate transmitter and the CJ is set to be 5 W. In the first set of simulations, the channel coefficients (i.e., $\mathbf{H}_s$, $\mathbf{H}_j$, $\mathbf{H}_e$ and $\mathbf{H}_{je}$) are assumed to be perfectly known at the transmitter. The noise covariance matrices at the legitimate receiver and the eavesdropper are set to be identity matrices.

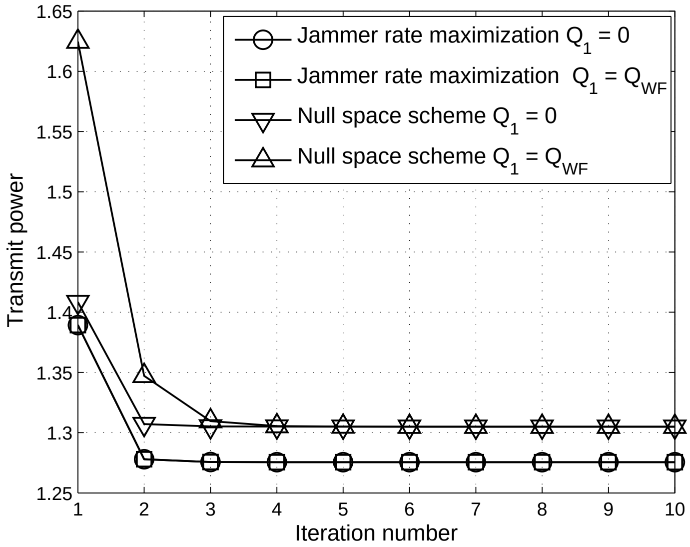

Figure 5.2: Convergence of the transmit power for power minimization.

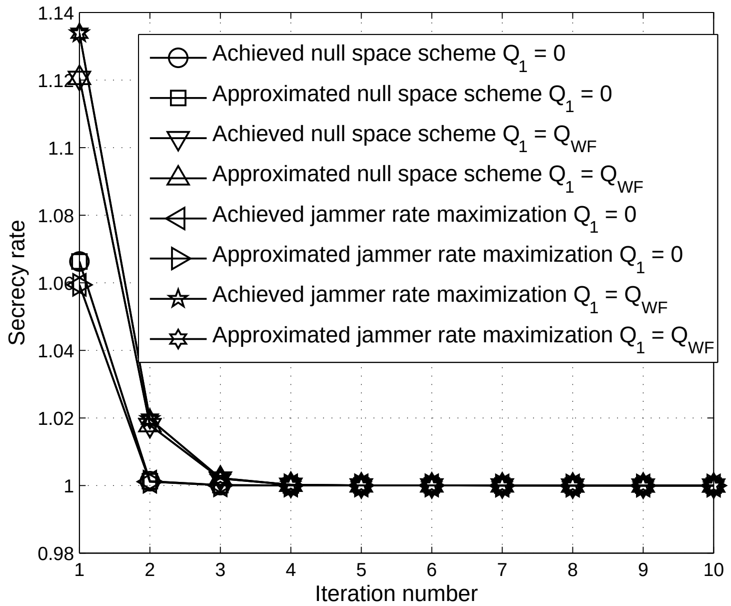

Figure 5.3: Convergence of the secrecy rate for power minimization.

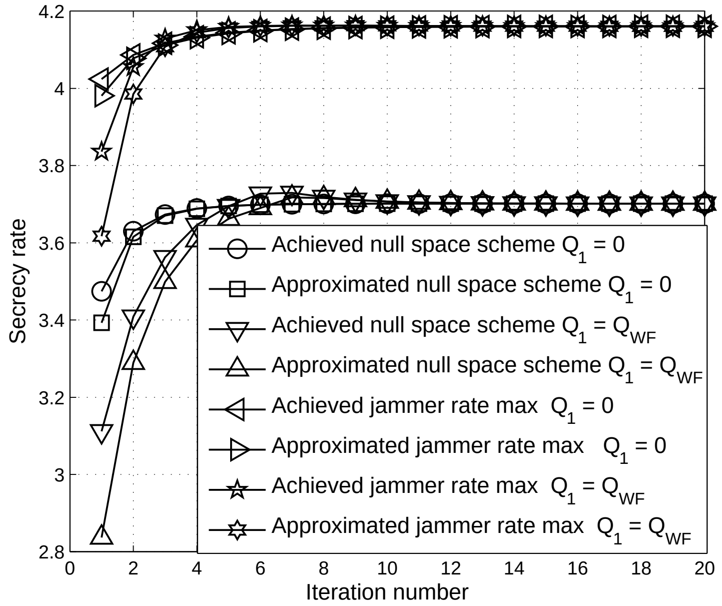

Figure 5.4: Convergence of the secrecy rate for secrecy rate maximization.

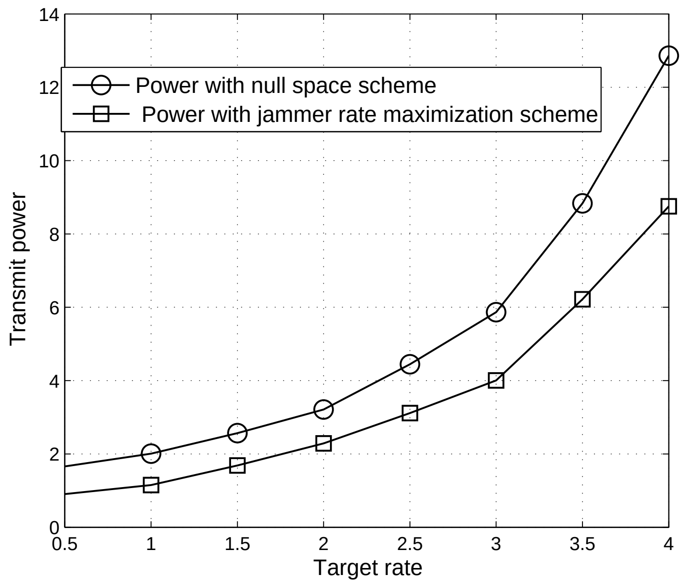

Figure 5.5: The transmit power with different target secrecy rates.

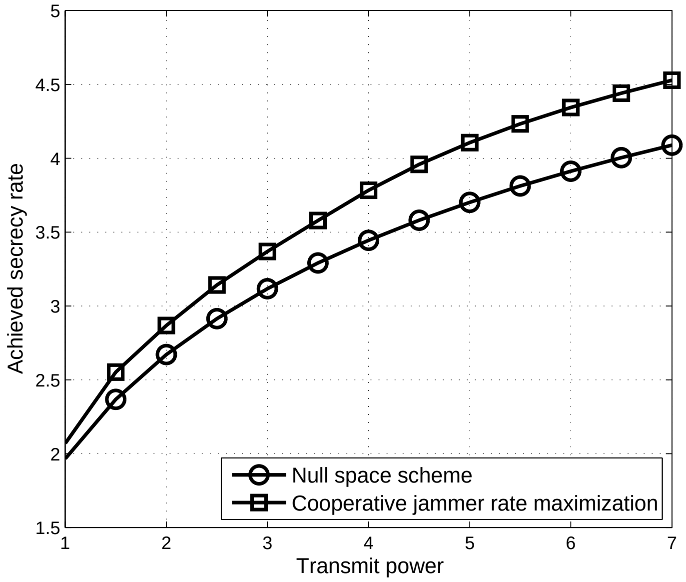

Figure 5.6: The secrecy rate with different transmit powers.

5.5.1 Secrecy Rate Optimizations with Perfect CSI

First, the convergence of the power minimization problem is evaluated, where the target secrecy rate is set to 1 bps/Hz. Fig. 5.2 and Fig. 5.3 show the convergence of the transmit power and secrecy rate for the power minimization problem based on the null space scheme and the CJ rate maximization with two initializations of $\tilde{\mathbf{Q}}_1$ (i.e., zero-element and water-filling). From both results, one can observe that both the transmit power and the secrecy rate decrease monotonically with every iteration, and the target secrecy rate can be satisfied when the proposed iterative algorithm converges. Next, the convergence of the secrecy rate maximization algorithm is shown in Fig. 5.4, where the result shows that the achieved secrecy rate and the approximated secrecy rate increase monotonically and are equal at the convergence of the proposed algorithm. In order to compare the performance of these two sub-problems (i.e., null space scheme and CJ rate maximization), Fig. 5.5 shows the variation of the transmit power with different target secrecy rates. From this result, the CJ rate maximization scheme consumes less power than the null space scheme for the same target secrecy rate. The difference between both schemes increases with the target secrecy rate. Additionally, Fig. 5.6 shows the achieved secrecy rates with different transmit powers for both schemes. As seen in Fig. 5.6, the CJ rate maximization scheme outperforms the null space scheme.

5.5.2 Robust Secrecy Rate Optimizations

In this subsection, the performance of the robust scheme is evaluated. The error bounds are assumed to be $\|\mathbf{E}_e\|^2 = 0.1$ and $\|\mathbf{E}_{je}\|^2 = 0.1$. First, Table 5.4 shows that the achieved secrecy rate of the robust power minimization, where the non-robust scheme can be achieved by solving the power minimization problem with perfect CSI. It is observed from Table 5.4 that the robust scheme outperforms the non-robust scheme, implying the non-robust secrecy rate does not satisfy the target secrecy rate, whereas the robust secrecy rate always satisfies the target rate. Also, the robust secrecy rate maximization problem with different channels is shown in Table 5.5, where the robust scheme outperforms the non-robust scheme in terms of the achieved secrecy rate. Fig. 5.7 and Fig. 5.8 show the achieved secrecy rates of the robust and non-robust schemes versus transmit power and error bound, respectively. From both results, it is observed that the performance of the robust secrecy rate maximization algorithm outperforms the non-robust scheme in terms of the achieved secrecy rate.

Random channels	Robust scheme	Non-robust scheme
Channel 1	1.1695	0.9848
Channel 2	1.1445	0.9753
Channel 3	1.1096	0.9966
Channel 4	1.1006	0.9875
Channel 5	1.1131	0.9682

Table 5.4: The comparison of achieved secrecy rates of robust and non-robust power minimization scheme with target rate $\bar{\mathrm{R}}_s = 1$ bps/Hz.

Random channels	Robust scheme	Non-robust scheme
Channel 1	2.4121	1.8112
Channel 2	3.8684	3.6255
Channel 3	2.3065	1.7519
Channel 4	3.0274	2.9007
Channel 5	1.3999	1.1407

Table 5.5: The comparison of achieved secrecy rates of robust and non-robust secrecy rate maximization scheme.

5.5.3 Secrecy Rate Optimization based on Game Theory

Finally, the *Stackelberg* equilibrium to the proposed *Stackelberg* game is evaluated. Fig. 5.9 depicts the revenue function of the legitimate transmitter with the inter-

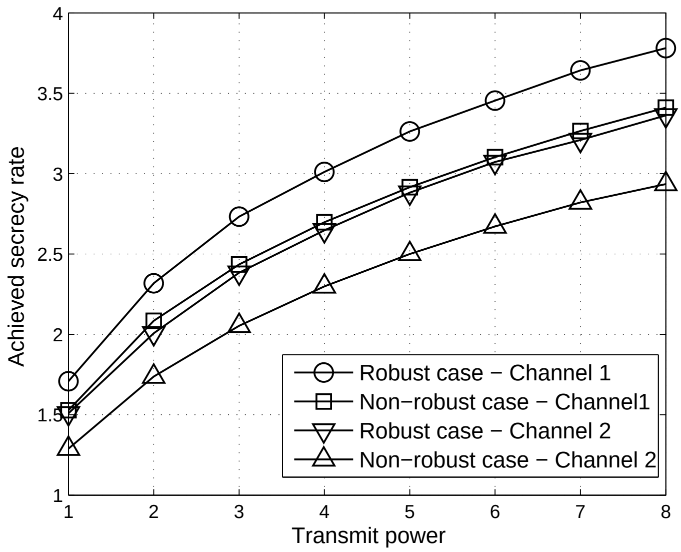

Figure 5.7: Achieved secrecy rate versus transmit power.

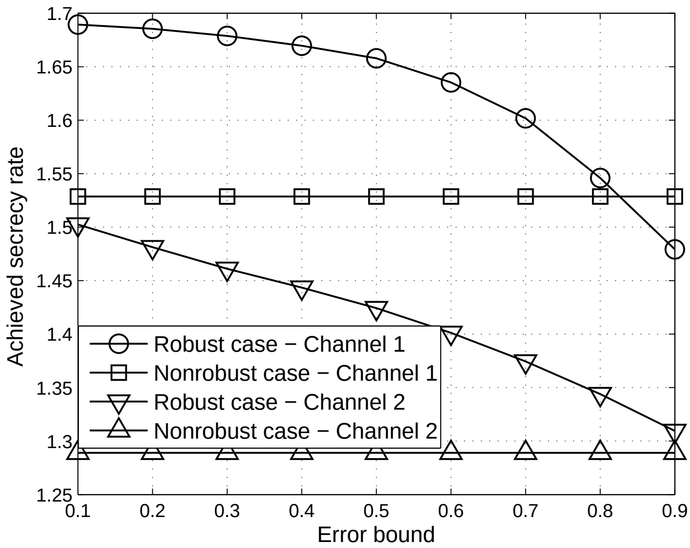

Figure 5.8: Achieved secrecy rate versus error bound.

ference requirement of p_1. From this result, it confirms that this revenue function is concave in terms of p_1, which validates the convexity of the legitimate transmitter revenue function. The closed-form solution of p_1^* in (5.29) is also verified by this result. Fig. 5.10 shows the revenue function of the private CJ with different interference prices (i.e., μ_0). As seen from Fig. 5.10, the private CJ revenue function is concave in terms of μ_0, which supports the convexity of the private CJ revenue function. The optimal μ_0 derived in (5.31) is validated by this result. Fig. 5.11 shows the optimal revenue function of the legitimate transmitter for a given μ_0^*, and then a corresponding optimal value p_1^* can be achieved, hence, (p_1^*, μ_0^*) defines the *Stackelberg* equilibrium as indicated in Fig. 5.11.

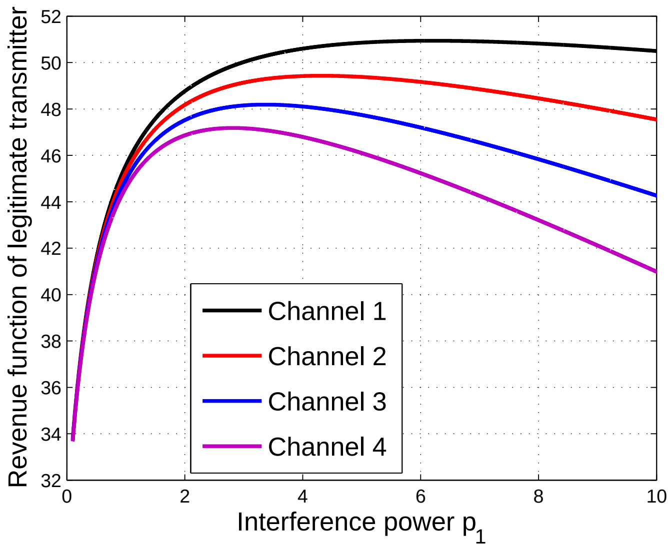

Figure 5.9: Revenue function of the legitimate transmitter.

5.6 Summary

In this chapter, transmit optimization for a MIMO secure channel with a multi-antenna CJ in the presence of a multi-antenna eavesdropper. Both secrecy rate optimization problems (power minimization and secrecy rate maximization) have been formulated. These original problems are not jointly convex due to the transmit covariance matrices of the transmitter and the CJ. To circumvent this issue, these original problems was divided into two sub-problems, where both transmit covariance matrices are optimally designed by the Taylor approximation, separately. In addition, an iterative algorithm to solve the reformulated problem is proposed based

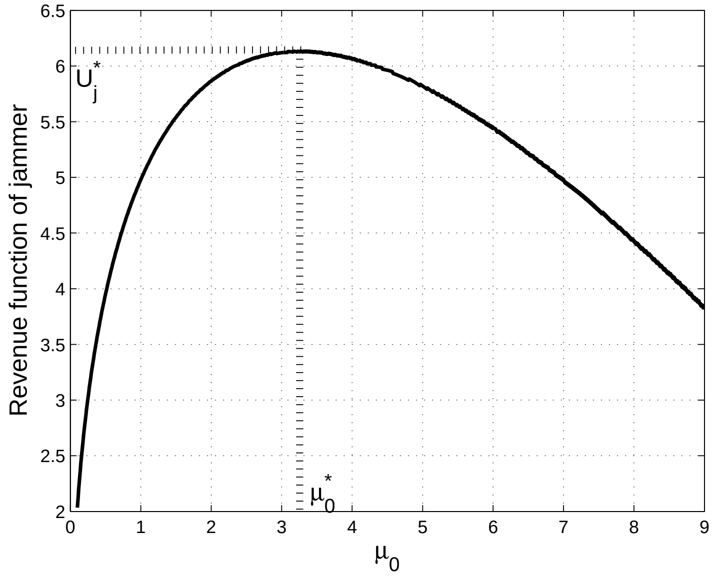

Figure 5.10: Revenue function of the private CJ.

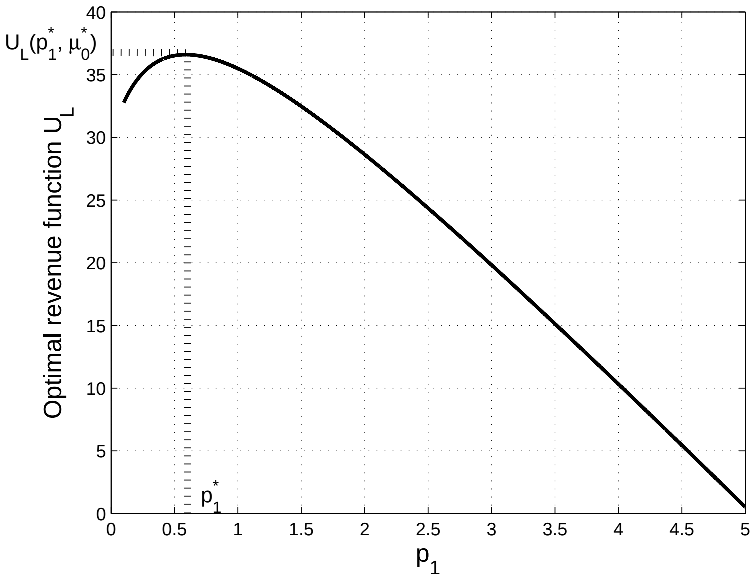

Figure 5.11: Optimal revenue function of the legitimate transmitter.

on dual problem and the subgradient method. Next, the robust secrecy rate optimizations have been studied incorporating the channel uncertainty associated with the eavesdropper. The robust optimization problem was developed by exploiting linear matrix transformation. Finally, secrecy rate maximization based on *Stackelber* game was proposed. This optimization problem was modelled as a *Stackelberg* game, and the corresponding equilibrium has been derived. Simulation results have been provided to demonstrate the benefits of the proposed algorithms.

5.7 Appendix

5.7.1 Proof of Problem (5.19)

Here, the proof for the problem (5.19) is provided, which can be represented using standard epigraph form as

$$\begin{aligned}
&\min_{\mathbf{Q}_1} \ \mathrm{Tr}(\mathbf{Q}_1),\\
&s.t. \ \log\left|\mathbf{I}+\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H+\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right| - t_1 - \log\left|\mathbf{I}+\frac{1}{\sigma_r^2}\mathbf{H}_j\mathbf{Q}_2\mathbf{H}_j^H\right|\\
&\qquad + \log\left|\mathbf{I}+\frac{1}{\sigma_e^2}\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right| \geq \bar{R}_{sr},\\
&\quad \alpha-\beta+\mathrm{Tr}[\mathbf{S}(\mathbf{H}_e+\mathbf{E}_e)\mathbf{Q}_1(\mathbf{H}_e+\mathbf{E}_e)^H] \leq t_1,\\
&\quad \mathbf{Q}_1 \succeq \mathbf{0}, t_1 \geq 0, \|\mathbf{E}_e\|_F^2 \leq \varepsilon_e^2,
\end{aligned} \tag{5.33}$$

where

$$\alpha = \log\left|\mathbf{I}+\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H+\mathbf{H}_{je}\mathbf{Q}_2^*\mathbf{H}_{je}^H\right|, \ \beta = \mathrm{Tr}\left[\left(\mathbf{I}+\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H+\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right)^{-1}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right],$$
$$\mathbf{S}_1 = \left(\mathbf{I}+\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H+\mathbf{H}_{je}\mathbf{Q}_2\mathbf{H}_{je}^H\right)^{-1}.$$

The above problem is not convex and it is difficult to derive the worst-case secrecy rate in terms of $\mathbf{E}_e$. The constraint (5.33) can be equivalently modified as

$$\begin{aligned}
&\alpha-\beta+\mathrm{Tr}[\mathbf{S}_1(\mathbf{H}_e+\mathbf{E}_e)\mathbf{Q}_1(\mathbf{H}_e+\mathbf{E}_e)^H] \leq t_1 \iff\\
&\quad \alpha-\beta+\mathbf{h}_e^H\mathbf{B}_1\mathbf{h}_e+2\Re[\mathbf{a}^H(\mathbf{Q}_1\otimes\mathbf{I})\mathbf{e}_e]+\mathbf{e}_e^H\mathbf{B}_1\mathbf{e}_e \leq t_1,
\end{aligned} \tag{5.34}$$

where

$$\mathbf{h}_e = \mathrm{vec}(\mathbf{H}_e), \quad \mathbf{e}_e = \mathrm{vec}(\mathbf{E}_e), \quad \mathbf{a} = \mathrm{vec}(\mathbf{S}_1\mathbf{H}_e), \quad \mathbf{B}_1 = (\mathbf{Q}_1^T \otimes \mathbf{I})^T(\mathbf{I} \otimes \mathbf{S}_1).$$

In addition, the constraint $\mathbf{e}_e^H\mathbf{e}_e \leq \varepsilon_e^2$ holds. In order to incorporate the channel uncertainties in the robust optimization framework (5.33), the following *lemma* is considered:

Lemma 5.3 *(S-Procedure) [97]: Let $f_k(\mathbf{x}), k = 1, 2,$ be defined as*

$$f_k(\mathbf{x}) = \mathbf{x}^H\mathbf{A}_k\mathbf{x} + 2\Re\left\{\mathbf{b}_k^H\mathbf{x}\right\} + c_k, \tag{5.35}$$

where $\mathbf{A}_k = \mathbf{A}_k^H \in \mathbb{C}^{n\times n}$, $\mathbf{b}_k \in \mathbb{C}^n$ and $c_k \in \mathbb{R}$. The implication $f_1(\mathbf{x}) \geq 0 \Longrightarrow f_2(\mathbf{x}) \geq 0$ holds if and only if there exists $\mu \geq 0$ such that

$$\begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{bmatrix} - \mu \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{bmatrix} \succeq \mathbf{0}, \tag{5.36}$$

provided there exists a point $\tilde{\mathbf{x}}$ with $f_1(\tilde{\mathbf{x}}) > 0$.

By exploiting *S-Procedure* shown in *Lemma* 5.3, the constraint in (5.34) can be written as

$$\begin{bmatrix} \mu_1\mathbf{I} - \mathbf{B}_1 & -(\mathbf{Q}_1^T \otimes \mathbf{I})^T\mathbf{a} \\ -\mathbf{a}^H(\mathbf{Q}_1^T \otimes \mathbf{I})^* & -\mu\varepsilon_e^2 - \alpha + \beta + t_1 - \mathbf{h}_e^H\mathbf{B}_1\mathbf{h}_e \end{bmatrix} \succeq \mathbf{0}. \tag{5.37}$$

This completes the proof. ■

5.7.2 Proof of Constraint (5.21)

Here, the proof for the reformulation of (5.20b) and (5.20c) is provided, first, the constraints (5.20b) and (5.20c) are written as follows:

$$\log\left|\mathbf{I} + \tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right| \geq \log(t_2), \tag{5.38a}$$

$$\alpha_2 - \beta_2 + \mathrm{Tr}\left[\mathbf{S}_2\tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right] \leq t_3. \tag{5.38b}$$

For (5.38a), the following matrix inequality is required

$$|\mathbf{I} + \mathbf{A}| \geq 1 + \mathrm{Tr}(\mathbf{A}), \tag{5.39}$$

Thus by employing the above inequality, the lower bound of the left hand side (LHS) of the constraint in (5.38a) can be obtained, and this constraint can be modified as

$$\begin{aligned} &\log\left|\mathbf{I} + \tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H\right| \geq \log(t_2) \Rightarrow \log[1 + \mathrm{Tr}(\tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H)] \geq \log(t_2), \\ &\Rightarrow \mathrm{Tr}(\tilde{\mathbf{H}}_{je}\mathbf{Q}_2\tilde{\mathbf{H}}_{je}^H) \geq t_2 - 1. \end{aligned} \tag{5.40}$$

Besides, from the following matrix identities:

$$\begin{gathered} \mathrm{Vec}(\mathbf{AXB}) = (\mathbf{B}^T \otimes \mathbf{A})\mathrm{Vec}(\mathbf{X}),\ \mathrm{Tr}(\mathbf{A}^T\mathbf{B}) = \mathrm{Vec}(\mathbf{A})^T\mathrm{Vec}(\mathbf{B}), \\ (\mathbf{A} \otimes \mathbf{B})^T = \mathbf{A}^T \otimes \mathbf{B}^T. \end{gathered}$$

The constraint in (5.40) can be expressed as,

$$\begin{aligned} &\mathbf{e}_{je}^H\mathbf{A}\mathbf{e}_{je} + 2\Re\left[\mathbf{a}_1^H\mathbf{A}\mathbf{e}_{je}\right] + \mathbf{h}_{je}^H\mathbf{A}\mathbf{h}_{je} - t_2 + 1 \geq 0, \\ &\mathbf{e}_{je}^H\mathbf{e}_{je} \leq \varepsilon_{je}^2, \end{aligned} \tag{5.41}$$

where $\mathbf{A} = \mathbf{Q}_2^T \otimes \mathbf{I}$, $\mathbf{h}_{je} = \mathrm{vec}(\mathbf{H}_{je})$, and $\mathbf{e}_{je} = \mathrm{vec}(\mathbf{E}_{je})$. Similarly, by exploiting *Lemma* 5.3, the constraint (5.38a) is reformulated into the following linear matrix inequality (LMI):

$$\begin{bmatrix} \lambda_1\mathbf{I} + (\mathbf{Q}_2^T \otimes \mathbf{I}) & (\mathbf{Q}_2^T \otimes \mathbf{I})\mathbf{h}_{je} \\ \mathbf{h}_{je}^H(\mathbf{Q}_2^T \otimes \mathbf{I}) & -\lambda_1\varepsilon_{je}^2 - t_2 + \mathbf{h}_{je}^H(\mathbf{Q}_2^T \otimes \mathbf{I})\mathbf{h}_{je} + 1 \end{bmatrix} \succeq \mathbf{0}. \tag{5.42}$$

Also, the constraint (5.38b) is reformulated into the following LMI:

$$\begin{bmatrix} \lambda_2\mathbf{I} - \mathbf{B}_2 & -(\mathbf{Q}_2^T \otimes \mathbf{I})^T\mathbf{a}_1 \\ -\mathbf{a}_1^H(\mathbf{Q}_2^T \otimes \mathbf{I})^* & -\lambda_2\varepsilon_{je}^2 - \alpha_2 + \beta_2 + t_3 - \mathbf{h}_{je}^H\mathbf{B}_2\mathbf{h}_{je} \end{bmatrix} \succeq \mathbf{0}, \tag{5.43}$$

where α_2, β_2, $\mathbf{S}_2$, $\mathbf{h}_{je}$, $\mathbf{a}_1$ and $\mathbf{B}_2$ are defined in (5.20) and (5.21). This completes the proof. ■

5.7.3 Proof of Lemma 5.1

The revenue function of the legitimate transmitter is

$$\begin{aligned} U_L(\mathbf{Q}_1, p_1) = \lambda_0 \Big(& \log |\mathbf{A}_0| - \log |\mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e \mathbf{Q}_1 \mathbf{H}_e^H + p_1 \mathbf{g}\mathbf{g}^H)| \Big) \\ & + \lambda_0 \log |\mathbf{I} + \frac{1}{\sigma_e^2} p_1 \mathbf{g}\mathbf{g}^H| - \mu_0 p_1 \|\mathbf{g}\|_2^2, \end{aligned} \tag{5.44}$$

where $\mathbf{A}_0 = \mathbf{I} + \frac{1}{\sigma_r^2}\mathbf{H}_s \mathbf{Q}_1 \mathbf{H}_s^H$. In order to show that the function (5.44) is convex with respect to p_1, its first derivative is considered as follows:

$$\begin{aligned} \frac{\partial \mathbf{U}_L(\mathbf{Q}_1, p_1)}{\partial p_1} = & -\lambda_0 \frac{\partial}{\partial p_1} (\log |\mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e \mathbf{Q}_1 \mathbf{H}_e^H + p_1 \mathbf{g}\mathbf{g}^H)|) \\ & + \lambda_0 \frac{\partial}{\partial p_1} (\log |\mathbf{I} + \frac{p_1}{\sigma_e^2} \mathbf{g}\mathbf{g}^H| - \mu_0 p_1 \|\mathbf{g}\|_2^2). \end{aligned} \tag{5.45}$$

In order to find the derivative of (5.45), the following matrix identities are required:

$$\partial \ln(\det \mathbf{X}) = \mathrm{Tr}[\mathbf{X}^{-1} \partial \mathbf{X}], \partial \ln(\det \mathbf{A}\mathbf{Z}^{-1}) = \mathrm{Tr}[\mathbf{Z}^{-1}\mathbf{A}\mathbf{Z}^{-1} \partial \mathbf{Z}].$$

For the term $\log \left| \mathbf{I} + \frac{p_1}{\sigma_e^2} \mathbf{g}\mathbf{g}^H \right|$:
First derivative:

$$\frac{\partial \log \left| \mathbf{I} + \frac{p_1}{\sigma_e^2} \mathbf{g}\mathbf{g}^H \right|}{\partial p_1} = \mathrm{Tr}\left[\left(\mathbf{I} + \frac{p_1}{\sigma_e^2} \mathbf{g}\mathbf{g}^H \right)^{-1} \frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2} \right]. \tag{5.46}$$

Second derivative:

$$\frac{\partial^2 \log \left| \mathbf{I} + \frac{p_1}{\sigma_e^2} \mathbf{g}\mathbf{g}^H \right|}{\partial^2 p_1} = -\mathrm{Tr}\left[\mathbf{A}_1^{-1} \frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2} \mathbf{A}_1^{-1} \frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2} \right]. \tag{5.47}$$

Similarly, for the term $\log \left| \mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e \mathbf{Q}_1 \mathbf{H}_e^H + p_1 \mathbf{g}\mathbf{g}^H) \right|$:
First derivative:

$$\frac{\partial \Big(\log \left| \mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e \mathbf{Q}_1 \mathbf{H}_e^H + p_1 \mathbf{g}\mathbf{g}^H) \right| \Big)}{\partial p_1} = \mathrm{Tr}\left[\left(\mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e \mathbf{Q}_1 \mathbf{H}_e^H + p_1 \mathbf{g}\mathbf{g}^H) \right)^{-1} \frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2} \right]. \tag{5.48}$$

Second derivative:

$$\frac{\partial^2\left(\log\left|\mathbf{I}+\frac{1}{\sigma_e^2}(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H+p_1\mathbf{g}\mathbf{g}^H)\right|\right)}{\partial^2 p_1}=-\mathrm{Tr}\left[\mathbf{A}_2^{-1}\frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2}\mathbf{A}_2^{-1}\frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2}\right]. \tag{5.49}$$

Thus

$$\frac{\partial^2\mathbf{U}_L(\mathbf{Q}_1,p_1)}{\partial^2 p_1}=\mathrm{Tr}\left[\mathbf{A}_2^{-1}\frac{\mathbf{g}_1\mathbf{g}_1^H}{\sigma_e^2}\mathbf{A}_2^{-1}\frac{\mathbf{g}_1\mathbf{g}_1^H}{\sigma_e^2}\right]-\mathrm{Tr}\left[\mathbf{A}_1^{-1}\frac{\mathbf{g}_1\mathbf{g}_1^H}{\sigma_e^2}\mathbf{A}_1^{-1}\frac{\mathbf{g}_1\mathbf{g}_1^H}{\sigma_e^2}\right], \tag{5.50}$$

where

$$\mathbf{A}_1=\mathbf{I}+\frac{1}{\sigma_e^2}p_1\mathbf{g}\mathbf{g}^H,\mathbf{A}_2=\mathbf{I}+\frac{1}{\sigma_e^2}\left(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H+p_1\mathbf{g}\mathbf{g}^H\right).$$

Since the eigenvalues of $\mathbf{A}_2^{-1}$ are smaller than that of $\mathbf{A}_1^{-1}$, the following holds:

$$\begin{aligned}
&\mathbf{A}_2^{-1}-\mathbf{A}_1^{-1}\leq 0,\quad \mathbf{g}^H(\mathbf{A}_2^{-1}-\mathbf{A}_1^{-1})\mathbf{g}\leq 0,\\
&\mathbf{g}^H\mathbf{A}_2^{-1}\mathbf{g}\mathbf{g}^H\mathbf{A}_2^{-1}\mathbf{g}\leq\mathbf{g}^H\mathbf{A}_1^{-1}\mathbf{g}\mathbf{g}^H\mathbf{A}_1^{-1}\mathbf{g},\\
&\mathrm{Tr}\left[\mathbf{A}_2^{-1}\frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2}\mathbf{A}_2^{-1}\frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2}\right]\leq\mathrm{Tr}\left[\mathbf{A}_1^{-1}\frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2}\mathbf{A}_1^{-1}\frac{\mathbf{g}\mathbf{g}^H}{\sigma_e^2}\right].
\end{aligned}$$

Hence, $\frac{\partial^2\mathbf{U}_L(\mathbf{Q}_1,p_1)}{\partial^2 p_1}\leq 0$, which proves that $\mathbf{U}_L(\mathbf{Q}_1,p_1)$ is a concave function in terms of p_1 for a fixed $\mathbf{Q}_1$. This completes the proof. ■

5.7.4 Proof of Lemma 5.2

The KKT condition in (5.28) is rewritten as

$$\lambda_0\mathrm{Tr}[\mathbf{A}_1^{-1}\mathbf{g}\mathbf{g}^H-\mathbf{A}_2^{-1}\mathbf{g}\mathbf{g}^H]-\mu_0\|\mathbf{g}\|_2^2=0, \tag{5.51}$$

where $\mathbf{A}_1$ and $\mathbf{A}_2$ have been defined after (5.28). From the following matrix identity,

$$(\mathbf{A}+\mathbf{b}\mathbf{c}^T)^{-1}=\mathbf{A}^{-1}-\frac{\mathbf{A}^{-1}\mathbf{b}\mathbf{c}^T\mathbf{A}^{-1}}{1+\mathbf{c}^T\mathbf{A}^{-1}\mathbf{b}}, \tag{5.52}$$

$\mathbf{A}_1^{-1}$ and $\mathbf{A}_2^{-1}$ in (5.51) can expressed as follows:

$$\mathbf{A}_1^{-1} = \mathbf{I} - \frac{\frac{p_1}{\sigma_e^2}\mathbf{g}\mathbf{g}^H}{1+\frac{p_1}{\sigma_e^2}\mathbf{g}^H\mathbf{g}}, \tag{5.53a}$$

$$\mathbf{A}_2^{-1} = \mathbf{A}^{-1} - \frac{\frac{p_1}{\sigma_e^2}\mathbf{A}^{-1}\mathbf{g}\mathbf{g}^H\mathbf{A}^{-1}}{1+\frac{p_1}{\sigma_e^2}\mathbf{g}^H\mathbf{A}^{-1}\mathbf{g}}, \tag{5.53b}$$

where $\mathbf{A} = \mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H$. Based on (5.53), the KKT condition in (5.51) can be equivalently modified as

$$\begin{aligned}
&\lambda_0\mathrm{Tr}(\mathbf{g}\mathbf{g}^H) - \lambda_0\frac{\frac{p_1}{\sigma_e^2}}{1+\frac{p_1}{\sigma_e^2}\mathbf{g}^H\mathbf{g}}\mathrm{Tr}(\mathbf{g}\mathbf{g}^H\mathbf{g}\mathbf{g}^H) - \lambda_0\mathrm{Tr}(\mathbf{A}^{-1}\mathbf{g}\mathbf{g}^H) \\
&\quad + \lambda_0\frac{\frac{p_1}{\sigma_e^2}}{1+\frac{p_1}{\sigma_e^2}\mathbf{g}^H\mathbf{A}^{-1}\mathbf{g}}\mathrm{Tr}(\mathbf{A}^{-1}\mathbf{g}\mathbf{g}^H\mathbf{A}^{-1}\mathbf{g}\mathbf{g}^H) - \mu_0\|\mathbf{g}\|^2 = 0.
\end{aligned} \tag{5.54}$$

Setting $c_1 = \mathbf{g}^H\mathbf{g}, c_2 = \mathbf{g}^H\mathbf{A}^{-1}\mathbf{g}$,

$$\frac{\lambda_0 c_1}{1+\frac{p_1}{\sigma_e^2}c_1} - \frac{\lambda_0 c_2}{1+\frac{p_1}{\sigma_e^2}c_2} - \mu_0\|\mathbf{g}\|^2 = 0, \tag{5.55}$$

$$\frac{c_1c_2}{\sigma_e^4}p_1^2 + \frac{c_1+c_2}{\sigma_e^2}p_1 + \left(1 - \frac{\lambda_0(c_1-c_2)}{\mu_0\|\mathbf{g}\|^2}\right) = 0, \tag{5.56}$$

It is easy to show that $\sqrt{(\frac{c_1+c_2}{\sigma_e^2})^2 - 4\frac{c_1c_2}{\sigma_e^4}\left[1-\frac{\lambda_0(c_1-c_2)}{\mu_0\|\mathbf{g}\|^2}\right]} \geq 0$ by showing $c_1 - c_2 \geq 0$, which holds if $\mathbf{g}^H(\mathbf{I}-\mathbf{A}^{-1})\mathbf{g} \geq 0$. Thus, $\mathbf{I}-\mathbf{A}^{-1} \succeq 0$ can be shown as follows:

$$\mathbf{I}-\mathbf{A}^{-1} \succeq 0, \Leftarrow \mathbf{I} \succeq \mathbf{A}^{-1} \Leftarrow \mathrm{Tr}(\mathbf{I}) \geq \mathrm{Tr}(\mathbf{A}^{-1}), \tag{5.57}$$

Since $\mathrm{Tr}(\mathbf{A}) = \sum_{i=1}^{N_E}\lambda_i$ and $\mathbf{A}$ is positive definite matrix, and $\lambda_i \geq 1$ represents the i-th eigenvalue of the matrix $\mathbf{A}$, the i-th eigenvalue of $\mathbf{A}^{-1}$ is $\frac{1}{\lambda_i} \leq 1$ holds if $\lambda_i \neq 0$ in terms of $\lambda_i \geq 1$, which implies $\mathrm{Tr}(\mathbf{A}^{-1}) \leq \mathrm{Tr}(\mathbf{I}) = \mathrm{M}_E$. Thus, $c_1 \geq c_2$ holds. From $p_1 \geq 0$, the optimal solution of p_1 can be derived as

$$p_1^* = \frac{-\frac{c_1+c_2}{\sigma_e^2} + \sqrt{\frac{(c_1+c_2)^2}{\sigma_e^4} + \frac{4\lambda_0c_1c_2(c_1-c_2)}{\mu_0\|\mathbf{g}\|^2}}}{2\frac{c_1c_2}{\sigma_e^4}}. \tag{5.58}$$

The revenue function of the jammer can be written in terms of μ_0 by substituting p_1^* as

$$U_j(p_1^*, \mu_0) = -\frac{b}{2a}\mu_0\|\mathbf{g}\|^2 + \frac{\|\mathbf{g}\|^2}{2a}\mu_0\left(d + \frac{4\lambda_0 c_1 c_2(c_1 - c_2)}{\mu_0\|\mathbf{g}\|^2}\right)^{\frac{1}{2}}, \tag{5.59}$$

where $a = \frac{c_1 c_2}{\sigma_e^4}$, $b = \frac{c_1+c_2}{\sigma_e^2}$ and $d = \frac{(c_1-c_2)^2}{\sigma_e^4}$. In order to prove the concavity of the jammer revenue function in terms of interference price, the second derivative of (5.59) is written with respect to μ_0 as follows:

$$\begin{aligned}\frac{\partial U_j}{\partial \mu_0} &= -\frac{b}{2a}\|\mathbf{g}\|^2 + \frac{\|\mathbf{g}\|^2}{2a}\left(d + \frac{4\lambda_0 c_1 c_2(c_1 - c_2)}{\mu_0\|\mathbf{g}\|^2}\right)^{\frac{1}{2}} \\ &+ \frac{\|\mathbf{g}\|^2}{4a}\left(d + \frac{4\lambda_0 c_1 c_2(c_1 - c_2)}{\mu_0\|\mathbf{g}\|^2}\right)^{-\frac{1}{2}}\left(-\frac{4\lambda_0 c_1 c_2(c_1 - c_2)}{\mu_0\|\mathbf{g}\|^2}\right),\end{aligned} \tag{5.60}$$

$$\frac{\partial^2 U_j}{\partial^2 \mu_0} = -\frac{\|\mathbf{g}\|^2}{4a}\left[-\frac{1}{2}\left(d + \frac{e}{\mu_0\|\mathbf{g}\|^2}\right)^{-\frac{3}{2}}\right]\left(-\frac{e}{\mu_0^2\|\mathbf{g}\|^2}\right)\left(\frac{e}{\|\mathbf{g}\|^2}\right) \leq 0, \tag{5.61}$$

where $e = 4\lambda_0 c_1 c_2(c_1 - c_2)$. Since, the second derivative is negative, Problem (A) is a convex problem in terms of μ_0. The optimal solution of μ_0 can be derived as follows:

$$\frac{\partial U_j}{\partial \mu_0} = 0, \Rightarrow \mu_0^* = \frac{e}{x\|\mathbf{g}\|^2}, \tag{5.62}$$

where

$$x = -\frac{\frac{d\|\mathbf{g}\|^2}{2a} - \frac{\frac{b^2\|\mathbf{g}\|^4}{4a^2} + \frac{b\|\mathbf{g}\|^2}{2a}\sqrt{\frac{(b^2-d)\|\mathbf{g}\|^4}{4a^2}}}{\frac{\|\mathbf{g}\|^2}{2a}}}{\frac{\|\mathbf{g}\|^2}{4a}} = 2\sqrt{b^2-d}(\sqrt{b^2-d}+b). \tag{5.63}$$

This completes the proof. ■

Chapter 6

Transmit Optimization for Secure MISO SWIPT System

This chapter investigates transmit optimization for a multiple-input single-output (MISO) secure simultaneous wireless information and power transfer (SWIPT) system, where transmit beamformer is designed to maximize the achieved secrecy rate while satisfying the transmit power budget and the energy harvesting (EH) constraint. In addition, artificial noise (AN) is employed to play two roles: intercept to the eavesdroppers and harvest power to the EH receivers. In this chapter, the main contributions are listed as follows:

1. *Transmit optimization for secrecy rate maximization*: First, transmit beamformer is designed for the secrecy rate maximization problem subject to the transmit power and energy harvesting (EH) constraints, where this optimization problem is not convex and cannot be solved directly. In order to circumvent this issue, a two-step method is considered, where the secrecy rate maximization problem is first decomposed into a sequence of power minimization problems for a given target secrecy rate, each of which can be reformulated as a convex optimization framework by using conic matrix transformations and first-order Taylor approximation. Then, this target secrecy rate is updated via bisection search. In addition, the associated robust schemes are investigated by incorporating channel uncertainty. The robust problem can be solved by exploiting conic matrix transformations.

2. *AN-aided transmit optimization for secrecy rate maximization*: Transmit beamformer and AN are jointly designed to maximize the achieved secrecy rate with

the transmit power and EH constraints. Due to nonconvex problem, first, the two-level approach is considered, where the inner level problem can be relaxed by semidefinite programming (SDP) relaxation, the outer level problem is a single-variable optimization problem, which is solved by using a one-dimensional (1D) search algorithm. Then, a successive convex approximation (SCA) based secrecy rate maximization problem is proposed. Moreover, the associated robust scheme incorporating channel uncertainty is solved by exploiting linear matrix transformation. Tightness analysis for each relaxation is provided to show the relaxed problem yields a rank-one solution.

6.1 System Model

In this section, a MISO secured SWIPT channel is considered, where it consists one multi-antenna legitimate transmitter, one legitimate user, K eavesdroppers and L energy harvesting (EH) receivers. It is assumed that the transmitter is equipped with N_T transmit antennas, whereas the legitimate user, the eavesdroppers and the EH receivers each have a single receive antenna. The channel coefficients between the legitimate transmitter and the legitimate user, the k-th eavesdropper as well as the l-th EH receiver are denoted by $\mathbf{h}_s \in \mathbb{C}^{N_T \times 1}$, $\mathbf{h}_{e,k} \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{h}_l \in \mathbb{C}^{N_T \times 1}$, respectively. The noise power at the legitimate user and the eavesdroppers are assumed to be σ_s^2 and σ_e^2. The received signal at the legitimate user and the k-th eavesdropper can be written as

$$y_s = \mathbf{h}_s^H \mathbf{w} s + n_s, \quad y_{e,k} = \mathbf{h}_{e,k}^H \mathbf{w} s + n_{e,k}, \;\; k = 1, ..., K,$$

where s and $\mathbf{w} \in \mathbb{C}^{N_T \times 1}$ are the desired signal for the legitimate user ($\mathbb{E}\{s^2\} = 1$) and the transmit beamformer at the legitimate transmitter, respectively. In addition, $n_s \sim \mathcal{CN}(0, \sigma_s^2)$ and $n_{e,k} \sim \mathcal{CN}(0, \sigma_e^2)$ represent the noise of the legitimate user and the k-th eavesdropper, respectively. Thus, the achieved secrecy rate at the legitimate user is expressed as follows:

$$R_s = \left[\log\left(1 + \frac{|\mathbf{h}_s^H \mathbf{w}|^2}{\sigma_s^2}\right) - \max_k \log\left(1 + \frac{|\mathbf{h}_{e,k}^H \mathbf{w}|^2}{\sigma_e^2}\right) \right]^+, \forall k. \tag{6.1}$$

The harvested energy at the l-th EH receiver is written as

$$E_l = \xi_l |\mathbf{h}_l^H \mathbf{w}|^2, \ \forall l, \tag{6.2}$$

where $\xi_l \in (0, 1]$ is the energy conversion efficiency of the energy transducers at the l-th EH receiver that accounts for the loss in the energy transducers for converting the harvested energy to electrical energy to be stored [101]. For convenience, it is assumed that $\xi_l = 1$, $\forall l$.

Remark This system model consists of L EH receivers, which harvest power carried by the RF signal without AN or with AN based on a reliable transmission scenario. These EH receivers sometimes play a " helper " role by employing the harvested power to introduce a jamming signal to confuse the eavesdroppers [103]. However, the efficiency of this harvest-and-jamming policy is dependant on the network topology [104]. In this chapter, the transmit beamformer without or with AN will be focused to maximize the achieved secrecy rate, satisfying the transmit power and the EH constraints.

6.2 Transmit Optimization for Secrecy Rate Maximization

In this section, secure transmit beamformer is designed for the secrecy rate maximization subject to the transmit power and the EH constraints. This optimization problem is written as follows:

$$\max_{\mathbf{w}} R_s, \ s.t. \ \|\mathbf{w}\|^2 \leq P, \ \min_{l} E_l \geq E, \ \forall k, l, \tag{6.3}$$

where P is the maximum available transmit power at the legitimate transmitter, and E denotes the target harvested energy of the EH receivers. The secrecy rate maximization problem (6.3) is not convex in terms of the nonconvex secrecy rate objective function and EH constraint, and cannot be solved directly. Unlike the existing work [60], where the SDP relaxation is considered to reformulate the secrecy rate maximization problem, however, it is challenging to yield a rank-one solution for the relaxed problem. In this section, a conic reformulation for the secrecy rate maximization problem is proposed to circumvent this issue. First, the problem (6.3)

Table 6.1: Bisection methods

1. Given lower and upper bound of the targeted secrecy rate $R_{\min}$ and $R_{\max}$, and a desired solution accuracy τ (very small value).
2. Setting $R = (R_{\min} + R_{\max})/2$.
3. **Iteration loop begin**
   (a) Solve the corresponding power minimization problem in (6.4) using the relaxation method to obtain the beamformer $\mathbf{w}$.
   (b) Compute the transmit power $\tilde{P} = \|\mathbf{w}\|^2$.
   (c) If $\tilde{P} \leq P$, then $R_{\min} = R$; otherwise, $R_{\max} = R$.
   (d) **Until** $R_{\max} - R_{\min} \leq \tau$, **break**.
4. **Iteration loop end**
5. R is the achieved secrecy rate of the secrecy rate maximization problem, and $\mathbf{w}$ is the corresponding optimal solution.

is decomposed into a sequence of power minimization problems for a target rate $R > 0$, each of which can be written as

$$\min_{\mathbf{w}} \ \|\mathbf{w}\|^2, \quad s.t. \ R_s \geq R, \ \min_{l} E_l \geq E, \ \forall k, l. \tag{6.4}$$

The optimal solution to (6.3) can be obtained by solving the corresponding power minimization problem (6.4) with different R, which is reformulated as a convex optimization framework by using conic matrix transformations. Then, bisection search is employed to update this target rate R by checking the feasibility of the power minimization problem [95]. Thus, this algorithm can be summarized in Table 6.1 to solve the secrecy rate maximization problem. In the following, the power minimization problem (6.4) will be solved.

6.2.1 Power Minimization

Now, the power minimization problem is considered based on the assumption that the transmitter has perfect channel state information (CSI) of the legitimate user, the eavesdroppers and the EH receivers. Thus, the problem (6.4) can be relaxed as

$$\begin{aligned}&\min_{\mathbf{w}} \|\mathbf{w}\|^2, \quad s.t.\ \log\left(1+\frac{|\mathbf{h}_s^H\mathbf{w}|^2}{\sigma_s^2}\right) - \log\left(1+\frac{|\mathbf{h}_{e,k}^H\mathbf{w}|^2}{\sigma_e^2}\right) \geq R,\ \forall k,\\ &|\mathbf{h}_l^H\mathbf{w}|^2 \geq E,\ \forall l.\end{aligned} \tag{6.5}$$

The above problem is not convex in terms of the non-convex secrecy rate and EH constraints. In order to circumvent the issue, the following *lemma* is required:

Lemma 6.1 *The problem in* (6.5) *is reformulated into the following form:*

$$\begin{aligned}&\min_{\mathbf{w},s_1} s_1, \quad s.t. \begin{bmatrix} s_1 \\ \mathbf{w}\end{bmatrix} \succeq_K \mathbf{0},\\ &\mathbf{S}_k = \begin{bmatrix} \frac{1}{\sigma_s}\mathbf{w}^H\mathbf{h}_s\mathbf{I} & \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\mathbf{h}_{e,k} \\ (2^R-1)^{\frac{1}{2}}\end{bmatrix} \\ \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\mathbf{h}_{e,k} \\ (2^R-1)^{\frac{1}{2}}\end{bmatrix}^H & \frac{1}{\sigma_s}\mathbf{w}^H\mathbf{h}_s \end{bmatrix} \succeq \mathbf{0},\ \forall k,\\ &x_l = \Re\{\mathbf{w}^H\mathbf{h}_l\},\ y_l = \Im\{\mathbf{w}^H\mathbf{h}_l\},\ \mathbf{u}_l = [x_l\ y_l],\\ &\|\mathbf{u}_l^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}_l^{(n)}(i)[\mathbf{u}_l(i) - \mathbf{u}_l^{(n)}(i)] \geq E,\ \forall l.\end{aligned} \tag{6.6}$$

Proof Please refer to Section 6.6.1. ■

In problem (6.6), the secrecy rate constraint is reformulated into linear matrix inequality (LMI), whereas the EH constraint is approximated by a first-order Taylor approximation, thus (6.6) is a convex problem for a given $\mathbf{u}_l$. An initialization value of the vector $\mathbf{u}_l$ is randomly generated and can be updated at each iteration. The algorithm converges when $\mathbf{u}_l^{(n+1)} = \mathbf{u}_l^{(n)}$ holds, and it is guaranteed to converge to a locally optimal solution (quite close to the globally optimal solution) [105, 106].

6.2.2 Robust Power Minimization

In the previous section, the power minimization problem has been solved based on the assumption that the legitimate transmitter has perfect CSI. However, it is not always possible to have perfect CSI due to the lack of cooperation as well as channel estimation and quantization errors. In this section, the robust power minimization problem is considered by incorporating norm-bounded channel uncertainty.

6.2.2.1 Channel Uncertainty

In this subsection, it is assumed that the CSI is not available at the legitimate transmitter. The channel uncertainty are modelled as

$$\begin{aligned}
\mathbf{h}_s &= \bar{\mathbf{h}}_s + \mathbf{e}_s, \\
\mathbf{h}_{e,k} &= \bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}, \ \forall k, \\
\mathbf{h}_l &= \bar{\mathbf{h}}_l + \mathbf{e}_l, \ \forall l,
\end{aligned}$$

where $\bar{\mathbf{h}}_s$, $\bar{\mathbf{h}}_{e,k}$ and $\bar{\mathbf{h}}_l$ denote the estimated channels of the legitimate user, the k-th eavesdropper and the l-th EH receiver, and $\mathbf{e}_s$, $\mathbf{e}_{e,k}$ and $\mathbf{e}_l$ represent the corresponding channel errors, which are assumed to be bounded as

$$\begin{aligned}
\|\mathbf{e}_s\|_2 &= \|\mathbf{h}_s - \bar{\mathbf{h}}_s\|_2 \leq \varepsilon_s, \text{for} \ \ \varepsilon_s \geq 0, , \\
\|\mathbf{e}_{e,k}\|_2 &= \|\mathbf{h}_{e,k} - \bar{\mathbf{h}}_{e,k}\|_2 \leq \varepsilon_{e,k}, \text{for} \ \ \varepsilon_{e,k} \geq 0, \ \forall k, \\
\|\mathbf{e}_l\|_2 &= \|\mathbf{h}_l - \bar{\mathbf{h}}_l\|_2 \leq \varepsilon_l, \text{for} \ \ \varepsilon_l \geq 0, \ \forall l,
\end{aligned}$$

where ε_s, $\varepsilon_{e,k}$ and ε_l represent the norm bound of the channel errors.

6.2.2.2 Robust Power Minimization

Now, the robust power minimization problem is written by incorporating the channel uncertainty as

$$\min_{\mathbf{w}} \ \|\mathbf{w}\|^2,$$

$$s.t. \ \min_{\mathbf{e}_s} \log\left(1 + \frac{|(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{w}|^2}{\sigma_s^2}\right) - \max_{\mathbf{e}_{e,k}} \log\left(1 + \frac{|(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H \mathbf{w}|^2}{\sigma_e^2}\right) \geq R, \ \forall k, \tag{6.7a}$$

$$\min_{\mathbf{e}_l} |(\bar{\mathbf{h}}_l + \mathbf{e}_l)^H \mathbf{w}|^2 \geq E, \ \forall l. \tag{6.7b}$$

The problem (6.7) is not convex due to (6.7a) and (6.7b), and cannot be solved directly. Thus, the following reformulation of the secrecy rate constraint (6.7a) as

$$\begin{cases} \frac{1}{\sigma_s}\left(\mathbf{w}^H\bar{\mathbf{h}}_s - \varepsilon_s\|\mathbf{w}\|\right) \geq \sqrt{t_2}, \\ \left[\begin{array}{cc} \frac{2^{\frac{R}{2}}}{\sigma_e}(\bar{\mathbf{h}}_{e,k}+\mathbf{e}_{e,k})^H\mathbf{w} & (2^R-1)^{\frac{1}{2}} \end{array}\right]\left[\begin{array}{c} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H(\bar{\mathbf{h}}_{e,k}+\mathbf{e}_{e,k}) \\ (2^R-1)^{\frac{1}{2}} \end{array}\right] \leq t_2, \end{cases} \tag{6.8}$$

The first constraint in (6.8) is modified based on a first-order Taylor approximation

$$\frac{1}{\sigma_s}\Re\{\mathbf{w}^H\bar{\mathbf{h}}_s\} - \frac{\varepsilon_s}{\sigma_s}\|\mathbf{w}\| \geq f^{(n)}(t_2), \tag{6.9}$$

where $f^{(n)}(t_2) = \sqrt{t_2^{(n)}} + \frac{1}{2\sqrt{t_2^{(n)}}}(t_2 - t_2^{(n)})$. The following *lemma* is considered to reformulate the second constraint in (6.8) ,

Lemma 6.2 *The second constraint in* (6.8) *can be reformulated as*

$$\bar{\mathbf{S}}_k = \left[\begin{array}{cc} \mathbf{S}_{k,1} - \lambda_k \left[\begin{array}{cc} \mathbf{0} & -1 \end{array}\right]\left[\begin{array}{c} \mathbf{0} \\ -1 \end{array}\right] & -\varepsilon_{e,k}\left[\begin{array}{c} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H \\ \mathbf{0} \\ \mathbf{0} \end{array}\right] \\ -\varepsilon_{e,k}\left[\begin{array}{ccc} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H & \mathbf{0} & \mathbf{0} \end{array}\right] & \lambda_k\mathbf{I} \end{array}\right] \succeq \mathbf{0}, \forall k. \tag{6.10}$$

where

$$\mathbf{S}_{k,1} = \left[\begin{array}{cc} f^{(n)}(t_2)\mathbf{I} & \left[\begin{array}{c} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\bar{\mathbf{h}}_{e,k} \\ (2^R-1)^{\frac{1}{2}} \end{array}\right] \\ \left[\begin{array}{c} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\bar{\mathbf{h}}_{e,k} \\ (2^R-1)^{\frac{1}{2}} \end{array}\right]^H & f^{(n)}(t_2) \end{array}\right]. \tag{6.11}$$

Proof Please refer to Section 6.6.2. ■

Thus, the robust power minimization problem can be written as

$$\begin{aligned}
&\min_{s_2,\mathbf{w},\lambda_k} \quad s_2, \quad s.t. \begin{bmatrix} s_2 \\ \mathbf{w} \end{bmatrix} \succeq_K \mathbf{0}, \\
&\bar{\mathbf{S}}_k(\lambda_k, f^{(n)}(t_2)) \succeq \mathbf{0}, \ \forall k, \\
&\frac{1}{\sigma_s}\mathbf{w}^H\bar{\mathbf{h}}_s - \frac{\varepsilon_s}{\sigma_s}\|\mathbf{w}\| \geq f^{(n)}(t_2), \\
&\Re\{\bar{\mathbf{h}}_l^H\mathbf{w}\} \geq E^{\frac{1}{2}} + \varepsilon_l\|\mathbf{w}\|_2, \ \Im\{\bar{\mathbf{h}}_l^H\mathbf{w}\} = 0, \ \forall l.
\end{aligned} \tag{6.12}$$

The above problem is convex for a given $t_2^{(n)}$ at each iteration. Thus, an initialization of t_2 is given to solve the problem in (6.12) by using interior-point method, which is updated iteratively. It is easily observed that t_2 is updated when $t_2^{(n+1)} = t_2^{(n)}$, which confirms that the algorithm converges.

6.3 AN-aided Transmit Optimization for Secrecy Rate Maximization

In the previous section, the secrecy rate maximization problem has been solved to optimize the secure transmit beamformer. In this section, AN-aided transmit optimization for secrecy rate maximization problem is investigated, where transmit beamformer and AN are jointly designed to maximize the achieved secrecy rate with the transmit power and the EH constraints.

6.3.1 Problem Formulation

The secrecy rate maximization problem is formulated subject to the transmit power and the minimum EH constraints, where the transmit signal can be written as $\mathbf{x} = \mathbf{w}s + \mathbf{v}$, and the secure transmit beamformer (i.e., $\mathbf{w}$) and AN (i.e., $\mathbf{v} \sim \mathcal{CN}(0, \mathbf{V})$) are jointly designed. This optimization problem can be formulated as

$$\begin{aligned}
&\max_{\mathbf{w},\mathbf{V}} \ \min_{k} R_s - R_{e,k}, \\
&\ s.t. \ \|\mathbf{w}\|^2 + \mathrm{Tr}(\mathbf{V}) \leq P, \ [\mathbf{w}\mathbf{w}^H]_{(i,i)} + [\mathbf{V}]_{(i,i)} \leq p_i, \ \forall i, \\
&\quad \min_{l} |\mathbf{h}_l^H\mathbf{w}|^2 + \mathbf{h}_l^H\mathbf{V}\mathbf{h}_l \geq E_l, \ \forall l, \ \mathbf{V} \succeq \mathbf{0},
\end{aligned} \tag{6.13}$$

where $[\mathbf{w}\mathbf{w}^H]_{(i,i)} + [\mathbf{V}]_{(i,i)}$ $(i = 1, ..., N_T)$ represents each antenna transmit power constraint, and the mutual information at the legitimate user and k-th eavesdropper can be written as

$$R_s = \log\left(1 + \frac{\mathbf{h}_s^H \mathbf{w}\mathbf{w}^H \mathbf{h}_s}{\mathbf{h}_s^H \mathbf{V}\mathbf{h}_s + \sigma_s^2}\right), \quad R_{e,k} = \log\left(1 + \frac{\mathbf{h}_{e,k}^H \mathbf{w}\mathbf{w}^H \mathbf{h}_{e,k}}{\mathbf{h}_{e,k}^H \mathbf{V}\mathbf{h}_{e,k} + \sigma_e^2}\right), \ \forall k.$$

The optimization problem (6.13) is not convex and cannot be solved directly. Thus, two reformulations are proposed to make this problem tractable. Unlike [61], where it has shown that the relaxed problem returns rank-two. In this section, a novel SDP relaxation for the secrecy rate maximization is investigated, which shows that the optimal solution returns rank-one to guarantee the optimal condition. First, the optimization problem (6.13) is written by defining $\mathbf{Q}_s = \mathbf{w}\mathbf{w}^H$ as

$$\begin{aligned}
\max_{\mathbf{Q}_s, \mathbf{V}} \ & \log\left(1 + \frac{\mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s}{\mathbf{h}_s^H \mathbf{V}\mathbf{h}_s + \sigma_s^2}\right) - \max_k \log\left(1 + \frac{\mathbf{h}_{e,k}^H \mathbf{Q}_s \mathbf{h}_{e,k}}{\mathbf{h}_{e,k}^H \mathbf{V}\mathbf{h}_{e,k} + \sigma_e^2}\right), \\
s.t. \ & \mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P, \quad \mathrm{Tr}[\mathbf{A}_i(\mathbf{Q}_s + \mathbf{V})] \leq p_i, \ \forall i, && (6.14a) \\
& \mathbf{h}_l^H(\mathbf{Q}_s + \mathbf{V})\mathbf{h}_l \geq E_l, \ \forall l, && (6.14b) \\
& \mathbf{Q}_s \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, && (6.14c) \\
& \mathrm{rank}(\mathbf{Q}_s) = 1,
\end{aligned}$$

where $\mathbf{A}_i = \mathbf{a}_i \mathbf{a}_i^H$ is the given antenna design parameters to adjust each antenna power budget, and $\mathbf{a}_i$ is a unit i-th vector (i.e., $[\mathbf{a}_i]_j = 1$ for $i = j$ and $[\mathbf{a}_i]_j = 0$ for $i \neq j$). The specific applications of each antenna power constraint have already been described in [29, 101].

6.3.2 Secrecy Rate Maximization

For the secrecy rate maximization problem (6.13), two reformulations to jointly optimize the transmit beamformer and AN, namely, two-level optimization and SCA are provided.

6.3.2.1 Two-Level Optimization

In this section, two-level optimization is considered to handle the secrecy rate maximization problem (6.14). First, this optimization can be written by introducing a slack variable t as

$$\begin{aligned}&\max_{\mathbf{Q}_s,\mathbf{V},t}\ R_s+\log(t),\\&\quad s.t.\ \log\left(1+\frac{\mathbf{h}_{e,k}^H\mathbf{Q}_s\mathbf{h}_{e,k}}{\mathbf{h}_{e,k}^H\mathbf{V}\mathbf{h}_{e,k}+\sigma_e^2}\right)\le\log(\frac{1}{t}),\ \forall k, &(6.15a)\\&\quad\quad (6.14a),\ (6.14b),\ (6.14c),\ \mathrm{rank}(\mathbf{Q}_s)=1. &(6.15b)\end{aligned}$$

The problem (6.15) is still not convex in terms of the constraint (6.15a), and cannot be solved directly. Then, this optimization problem can be formulated as a two-level optimization problem. The outer problem is a single-variable optimization problem of t, which can be written as

$$\max_{t}\ \log(1+f(t))+\log(t),\quad s.t.\ t_{\min}\le t\le 1, \tag{6.16}$$

where the lower bound $t_{\min}$ can be determined as

$$\begin{aligned}t&\ge\left(1+\frac{\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s}{\mathbf{h}_s^H\mathbf{V}\mathbf{h}_s+\sigma_s^2}\right)^{-1}\ge\left(1+\frac{\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s}{\sigma_s^2}\right)^{-1}\\&\ge\left(1+\frac{\lambda_{\max}(\mathbf{Q}_s)\|\mathbf{h}_s\|^2}{\sigma_s^2}\right)^{-1}\ge\left(1+\frac{\mathrm{Tr}(\mathbf{Q}_s)\|\mathbf{h}_s\|^2}{\sigma_s^2}\right)^{-1}\\&\ge\left(1+\frac{P\|\mathbf{h}_s\|^2}{\sigma_s^2}\right)^{-1}=t_{\min},\end{aligned} \tag{6.17}$$

which can be handled by using 1D search method. The inner problem can be recast for a given t as follows:

$$\begin{aligned}f(t)=&\max_{\mathbf{Q}_s,\mathbf{V}}\ \frac{\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s}{\mathbf{h}_s^H\mathbf{V}\mathbf{h}_s+\sigma_s^2},\\&s.t.\ (6.15a),\ (6.14a),\ (6.14b),\ (6.14c),\\&\quad\ \ \mathrm{rank}(\mathbf{Q}_s)=1.\end{aligned} \tag{6.18}$$

It is easily verified that the constraint in (6.15) can be reformulated as

$$\mathbf{h}_{e,k}^H\left[\mathbf{Q}_s-(\frac{1}{t}-1)\mathbf{V}\right]\mathbf{h}_{e,k}\le(\frac{1}{t}-1)\sigma_e^2. \tag{6.19}$$

Then, (6.18) can be recast for a given t as

$$f(t) = \max_{\mathbf{Q}_s, \mathbf{V}} \frac{\mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s}{\mathbf{h}_s^H \mathbf{V} \mathbf{h}_s + \sigma_s^2},$$
$$s.t.\ (6.19), (6.14a), (6.14b), (6.14c), \mathrm{rank}(\mathbf{Q}_s) = 1. \tag{6.20}$$

The problem (6.20) is a quasi-convex problem without the nonconvex rank-one constraint, thus the Charnes-Cooper transformation is employed to convert it into a convex problem by introducing δ so that the following relations hold:

$$\mathbf{Q}_s = \frac{\bar{\mathbf{Q}}_s}{\delta},\ \mathbf{V} = \frac{\bar{\mathbf{V}}}{\delta} \tag{6.21}$$

Thus, the problem (6.20) is relaxed as

$$\begin{aligned} f(t) = \max_{\bar{\mathbf{Q}}_s, \bar{\mathbf{V}}, \delta}\ & \mathbf{h}_s^H \bar{\mathbf{Q}}_s \mathbf{h}_s, \\ s.t.\ & \mathbf{h}_s^H \bar{\mathbf{V}} \mathbf{h}_s + \delta \sigma_b^2 = 1, \\ & \mathbf{h}_{e,k}^H \left[\bar{\mathbf{Q}}_s - (\frac{1}{t} - 1) \bar{\mathbf{V}} \right] \mathbf{h}_{e,k} \leq (\frac{1}{t} - 1) \delta \sigma_e^2, \\ & \mathrm{Tr}(\bar{\mathbf{Q}}_s + \bar{\mathbf{V}}) \leq \delta P,\ \mathrm{Tr}[\mathbf{A}_i (\bar{\mathbf{Q}}_s + \bar{\mathbf{V}})] \leq \delta p_i,\ \forall i, \\ & \mathbf{h}_l^H (\bar{\mathbf{Q}}_s + \bar{\mathbf{V}}) \mathbf{h}_l \geq \delta E_l,\ \forall l,\ \bar{\mathbf{Q}}_s \succeq \mathbf{0},\ \bar{\mathbf{V}} \succeq \mathbf{0}. \end{aligned} \tag{6.22}$$

The problem (6.22) is a convex problem, and can be solved efficiently by using interior-point method [70]. Thus, the optimal solution to (6.20) can be obtained through (6.21), once (6.22) has been solved.

6.3.2.2 Optimality Conditions for SDP Relaxation

In this subsection, the tightness of the SDP relaxation to (6.20) is investigated. It is assumed that $f(t)$ is the optimal value to (6.20), which can be achieved by solving (6.22), resulting in the following inequality,

$$\frac{\mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s}{\mathbf{h}_s^H \mathbf{V} \mathbf{h}_s + \sigma_s^2} \geq f(t) \Rightarrow \mathbf{h}_s^H [\mathbf{Q}_s - f(t) \mathbf{V}] \mathbf{h}_s \geq f(t) \sigma_s^2, \tag{6.23}$$

Thus, the following power minimization problem is considered

$$\begin{aligned}
&\min_{\mathbf{Q}_s, \mathbf{V}} \ \mathrm{Tr}(\mathbf{Q}_s) \\
&\ s.t. \ (6.23),\ (6.19),\ (6.14\text{a}),\ (6.14\text{b}),\ (6.14\text{c}).
\end{aligned} \tag{6.24}$$

It is easily verified that the feasible solution to (6.24) is the optimal solution of (6.20) due to the constraints (6.23), (6.14a), (6.14b), and (6.14c). Thus, the following *theorem* is provided to show that the problem (6.24) yields a rank-one solution.

Theorem 6.1 *Suppose the problem* (6.24) *is feasible, there always exists an optimal solution* ($\mathbf{Q}_s$, $\mathbf{V}$) *to* (6.24) *such that rank*($\mathbf{Q}_s$) = 1.

Proof Please refer to Section 6.6.3. ■

From *Theorem* 6.1, a tightness analysis has been provided such that the problem (6.20) yields a rank-one solution for all feasible t.

6.3.2.3 Successive Convex Approximation

In this section, SCA is proposed to jointly design secure transmit beamformer and AN. First, the problem (6.13) can be modified as

$$\min_{\mathbf{Q}_s, \mathbf{V}} \max_{k} \frac{\left(\sigma_e^2 + \mathrm{Tr}[\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H(\mathbf{Q}_s + \mathbf{V})]\right)\left(\sigma_s^2 + \mathrm{Tr}(\mathbf{h}_s\mathbf{h}_s^H\mathbf{V})\right)}{\left(\sigma_s^2 + \mathrm{Tr}[\mathbf{h}_s\mathbf{h}_s^H(\mathbf{Q}_s + \mathbf{V})]\right)\left(\sigma_e^2 + \mathrm{Tr}(\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H\mathbf{V})\right)}$$

$$s.t. \mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \le P, \ \ \mathrm{Tr}[\mathbf{A}_i(\mathbf{Q}_s + \mathbf{V})] \le p_i, \ \forall i, \tag{6.25a}$$

$$\mathbf{h}_l^H(\mathbf{Q}_s + \mathbf{V})\mathbf{h}_l \ge E_l, \ \forall l, \tag{6.25b}$$

$$\mathbf{Q}_s \succeq \mathbf{0}, \ \mathbf{V} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{Q}_s) = 1. \tag{6.25c}$$

Due to nonconvexity of the problem (6.25), the following exponential variables is introduced to equivalently convert the objective function

$$\begin{aligned}
e^{x_0} &= \sigma_s^2 + \mathrm{Tr}[\mathbf{h}_s\mathbf{h}_s^H(\mathbf{Q}_s + \mathbf{V})], \ e^{x_k} = \sigma_e^2 + \mathrm{Tr}(\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H\mathbf{V}), \\
e^{y_k} &= \sigma_e^2 + \mathrm{Tr}[\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H(\mathbf{Q}_s + \mathbf{V})], \ e^{y_0} = \sigma_s^2 + \mathrm{Tr}(\mathbf{h}_s\mathbf{h}_s^H\mathbf{V}).
\end{aligned} \tag{6.26}$$

Thus, (6.25) can be written by introducing a slack variable τ as

$$\min_{\mathbf{Q}_s,\mathbf{V},x_0,y_0,x_k,y_k} \tau \tag{6.27a}$$

$$s.t.\ e^{y_0-x_0+y_k-x_k} \leq \tau, \tag{6.27b}$$

$$\sigma_s^2 + \mathrm{Tr}[\mathbf{h}_s\mathbf{h}_s^H(\mathbf{Q}_s+\mathbf{V})] \geq e^{x_0}, \sigma_e^2 + \mathrm{Tr}(\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H\mathbf{V}) \geq e^{x_k}, \tag{6.27c}$$

$$\sigma_e^2 + \mathrm{Tr}[\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H(\mathbf{Q}_s+\mathbf{V})] \leq e^{y_k}, \sigma_s^2 + \mathrm{Tr}(\mathbf{h}_s\mathbf{h}_s^H\mathbf{V}) \leq e^{y_0}, \tag{6.27d}$$

$$(6.25a),\ (6.25b),\ (6.25c),\ \forall k,l,i. \tag{6.27e}$$

The above problem is not still convex in terms of the constraint (6.27d). Thus, the Taylor approximation (i.e., $a^{\hat{x}} + a^{\hat{x}} \ln a(x-\hat{x}) \leq a^x$) is employed to linearise (6.27d) as follows:

$$\sigma_e^2 + \mathrm{Tr}[\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H(\mathbf{Q}_s+\mathbf{V})] \leq e^{\hat{y}_k}(y_k - \hat{y}_k + 1), \tag{6.28a}$$

$$\sigma_s^2 + \mathrm{Tr}(\mathbf{h}_s\mathbf{h}_s^H\mathbf{V}) \leq e^{\hat{y}_0}(y_0 - \hat{y}_0 + 1), \tag{6.28b}$$

where $\hat{y}_0$ and $\hat{y}_k$ are approximated values such that $y_0 = \hat{y}_0$ and $y_k = \hat{y}_k$ when the approximations are tight. Thus, the secrecy rate maximization problem can be relaxed as

$$\begin{aligned} &\min_{\mathbf{Q}_s,\mathbf{V},x_0,y_0,x_k,y_k,\tau} \tau \\ &\quad s.t.\ (6.25a),\ (6.25b),\ (6.27b),\ (6.27c),\ (6.28),\ \forall k,l,i, \\ &\quad\quad \mathbf{Q}_s \succeq \mathbf{0},\ \mathbf{V} \succeq \mathbf{0},\ \mathrm{rank}(\mathbf{Q}_s) = 1. \end{aligned} \tag{6.29}$$

The problem (6.29) is convex without the nonconvex rank-one constraint for a given $(\hat{y}_0, \hat{y}_k)$, and can be solved by using an interior-point method. From SCA, the current optimal solution can be updated iteratively until the constraints (6.27c) and (6.27d) hold with equality, which implies (6.25) is optimally solved. This SCA algorithm is outlined in Table 6.2. The optimal solution obtained by the SCA algorithm at the n-th iteration is assumed to be $(\mathbf{Q}_s^*(n), \mathbf{V}^*(n), x_0^*(n), y_0^*(n), x_k^*(n), y_k^*(n), \tau^*(n))$, which can achieve a stable point when the SCA algorithm converges [107].

Now, the tightness analysis to (6.27) is considered. It is assumed that $(\mathbf{Q}_s^*, \mathbf{V}^*)$ are the optimal solutions to (6.25) that are obtained by solving (6.29) with the SCA algorithm, and the corresponding slack variables (i.e., $x_0^*, y_0^*, x_k^*, y_k^*, \tau^*$) can be

Table 6.2: SCA algorithm for the robust secrecy rate maximization problem (6.27).

1. Initialize $(\mathbf{Q}_s[0], \mathbf{V}[0])$ so that (6.27) is feasible, and given κ as the tolerance factor for stopping criterion.
2. **Iteration loop begin**:
   (a) Updating $(x_0[n], x_k[n], y_0[n], y_k[n])$ by (6.26).
   (b) Solving (6.29) with $(x_0[n], x_k[k], y_0[n], y_k[n])$ to obtain $(\mathbf{Q}_s[n], \mathbf{V}[n])$.
3. **Iteration loop end until stopping criterion** $|\tau(n+1) - \tau(n)| \leq \kappa$**.**

obtained by (6.26) and (6.27b), respectively. Thus, the following power minimization problem is required:

$$\begin{aligned}
&\min_{\mathbf{Q}_s, \mathbf{V}} \ \mathrm{Tr}(\mathbf{Q}_s) \\
&\ s.t. \ (6.25\text{a}), \ (6.25\text{b}), \ \mathbf{Q}_s \succeq \mathbf{0}, \ \mathbf{V} \succeq \mathbf{0}, \\
&\quad \sigma_s^2 + \mathrm{Tr}[\mathbf{h}_s \mathbf{h}_s^H (\mathbf{Q}_s + \mathbf{V})] \geq e^{x_0^*}, \ \sigma_e^2 + \mathrm{Tr}(\mathbf{h}_{e,k} \mathbf{h}_{e,k}^H \mathbf{V}) \geq e^{x_k^*}, \\
&\quad \sigma_e^2 + \mathrm{Tr}[\mathbf{h}_{e,k} \mathbf{h}_{e,k}^H (\mathbf{Q}_s + \mathbf{V})] \leq e^{y_k^*}, \ \sigma_s^2 + \mathrm{Tr}(\mathbf{h}_s \mathbf{h}_s^H \mathbf{V}) \leq e^{y_0^*}, \\
&\quad \forall k, l, i.
\end{aligned} \tag{6.30}$$

It is assumed that the optimal solutions to (6.30) can be denoted as $(\hat{\mathbf{Q}}_s, \hat{\mathbf{V}})$, which are the feasible solutions to (6.25) with the objective value $\hat{\tau}$ obtained by substituting $(\hat{\mathbf{Q}}_s, \hat{\mathbf{V}})$ into (6.25), and $\hat{\tau} \leq \tau^*$ holds, which implies $(\hat{\mathbf{Q}}_s, \hat{\mathbf{V}})$ is at least the same optimal solution $(\mathbf{Q}_s^*, \mathbf{V}^*)$ to (6.25). Thus, provided that the problem (6.30) is feasible for positive secrecy rates, (6.30) always yield a rank-one solution, and the proof is similar to that of *Theorem* 6.1.

6.3.3 Robust Secrecy Rate Maximization

In the previous subsection, the secrecy rate maximization problem has been solved based on global CSI, however, it is not always possible that the legitimate transmitter has perfect CSI due to lack of cooperation as well as the channel estimation and quantization errors. In this subsection, the robust secrecy rate maximization is considered to jointly optimize the transmit beamformer and AN by incorporating norm-bounded channel uncertainty shown in Section 6.2.2.1. In addition, per-antenna power constraints is considered, where the Hermitian positive semidefinite

(PSD) matrix $\mathbf{A}_i$ is not available at the legitimate transmitter, thus the true PSD matrix can be written as

$$\mathbf{A}_i = \bar{\mathbf{A}}_i + \boldsymbol{\Delta}_i, \ \|\boldsymbol{\Delta}_i\|_F \leq \epsilon_i, \ \forall i, \tag{6.31}$$

where $\bar{\mathbf{A}}_i \in \mathbb{H}_+^{N_T}$ is the estimated Hermitian PSD matrix, and $\boldsymbol{\Delta}_i$ is estimated error of the matrix $\bar{\mathbf{A}}_i$, which can be modelled as a spherical uncertainty with a norm bound ϵ_i [57].

6.3.3.1 Two-Level Optimization

In this subsection, two-level optimization shown in 6.3.2.1 is considered to solve the robust secrecy rate maximization, jointly designing secure transmit beamformer and AN by incorporating the channel uncertainty. Since the outer problem does not involve the channel uncertainty similar to Section 6.3.2.1, thus, in this subsection, the inner problem is the main work, which can be written as

$$\begin{aligned}
f(t) = \max_{\mathbf{Q}_s, \mathbf{V}} \ & \frac{(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{Q}_s (\bar{\mathbf{h}}_s + \mathbf{e}_s)}{(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{V} (\bar{\mathbf{h}}_s + \mathbf{e}_s) + \sigma_s^2}, \\
s.t. \ & (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H \left[\mathbf{Q}_s - \left(\frac{1}{t} - 1\right)\mathbf{V}\right](\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}) \leq (\frac{1}{t} - 1)\sigma_e^2, \\
& \mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P, \ \max_{\boldsymbol{\Delta}_i} \mathrm{Tr}[(\bar{\mathbf{A}}_i + \boldsymbol{\Delta}_i)(\mathbf{Q}_s + \mathbf{V})] \leq p_i, \\
& (\bar{\mathbf{h}}_l + \mathbf{e}_l)^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_l + \mathbf{e}_l) \geq E_l, \ \forall l, \\
& \mathbf{Q}_s \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{Q}_s) = 1.
\end{aligned} \tag{6.32}$$

Due to the nonconvexity of the problem (6.32), this robust secrecy rate maximization problem can be modified by exploiting *S-Procedure* as

$$f(t) = \max_{\mathbf{Q}_s, \mathbf{V}, \lambda_{e,k}, \alpha_l} \ \frac{(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{Q}_s (\bar{\mathbf{h}}_s + \mathbf{e}_s)}{(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{V} (\bar{\mathbf{h}}_s + \mathbf{e}_s) + \sigma_s^2},$$

$$s.t. \ \mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P, \ \mathrm{Tr}[\bar{\mathbf{A}}_i(\mathbf{Q}_s + \mathbf{V})] + \epsilon_i \|\mathbf{Q}_s + \mathbf{V}\|_F \leq p_i, \ \forall i, \tag{6.33a}$$

$$\begin{bmatrix} \lambda_{e,k}\mathbf{I} - [\mathbf{Q}_s - (\frac{1}{t} - 1)\mathbf{V}] & -[\mathbf{Q}_s - (\frac{1}{t} - 1)\mathbf{V}]\bar{\mathbf{h}}_{e,k} \\ -\bar{\mathbf{h}}_{e,k}^H[\mathbf{Q}_s - (\frac{1}{t} - 1)\mathbf{V}] & c_k \end{bmatrix} \succeq \mathbf{0}, \ \forall k, \tag{6.33b}$$

$$\begin{bmatrix} \alpha_l\mathbf{I} + (\mathbf{Q}_s + \mathbf{V}) & (\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_l \\ \bar{\mathbf{h}}_l^H(\mathbf{Q}_s + \mathbf{V}) & \bar{\mathbf{h}}_l^H(\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_l - E_l - \alpha_l\varepsilon_l^2 \end{bmatrix} \succeq \mathbf{0}, \ \forall l, \tag{6.33c}$$

$$\mathbf{Q}_s \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{Q}_s) = 1. \tag{6.33d}$$

where $c_k = -\bar{\mathbf{h}}_{e,k}^H[(\mathbf{Q}_s - \frac{1}{t} - 1)\mathbf{V}]\bar{\mathbf{h}}_{e,k} + (\frac{1}{t} - 1)\sigma_e^2 - \lambda_{e,k}\varepsilon_{e,k}^2$. Then, a slack variable τ is introduced to relax the objective function in (6.33). By exploiting *S-Procedure* and Charnes-Cooper transformation, this robust problem can be expressed as

$$\begin{aligned}
f(t) = &\max_{\bar{\mathbf{Q}}_s, \bar{\mathbf{V}}, \lambda_s, \mu_s, \lambda_{e,k}, \alpha_l, \delta, \tau} \quad \tau, \\
s.t. &\begin{bmatrix} \lambda_s \mathbf{I} + \bar{\mathbf{Q}}_s & \bar{\mathbf{Q}}_s \bar{\mathbf{h}}_s \\ \bar{\mathbf{h}}_s^H \bar{\mathbf{Q}}_s & \bar{\mathbf{h}}_s^H \bar{\mathbf{Q}}_s \bar{\mathbf{h}}_s - \tau - \lambda_s \varepsilon_s^2 \end{bmatrix} \succeq \mathbf{0}, \\
&\begin{bmatrix} \mu_s \mathbf{I} - \bar{\mathbf{V}} & -\bar{\mathbf{V}} \bar{\mathbf{h}}_s \\ -\bar{\mathbf{h}}_s^H \bar{\mathbf{V}} & -\bar{\mathbf{h}}_s^H \bar{\mathbf{V}} \bar{\mathbf{h}}_s - \delta \sigma_s^2 + 1 - \mu_s \varepsilon_s^2 \end{bmatrix} \succeq \mathbf{0}, \\
&\begin{bmatrix} \lambda_{e,k} \mathbf{I} - [\bar{\mathbf{Q}}_s - (\frac{1}{t} - 1)\bar{\mathbf{V}}] & -[\bar{\mathbf{Q}}_s - (\frac{1}{t} - 1)\bar{\mathbf{V}}]\bar{\mathbf{h}}_{e,k} \\ -\bar{\mathbf{h}}_{e,k}^H [\bar{\mathbf{Q}}_s - (\frac{1}{t} - 1)\bar{\mathbf{V}}] & \bar{c}_k \end{bmatrix} \succeq \mathbf{0}, \\
&\begin{bmatrix} \alpha_l \mathbf{I} + (\bar{\mathbf{Q}}_s + \bar{\mathbf{V}}) & (\bar{\mathbf{Q}}_s + \bar{\mathbf{V}})\bar{\mathbf{h}}_l \\ \bar{\mathbf{h}}_l^H (\bar{\mathbf{Q}}_s + \bar{\mathbf{V}}) & \bar{\mathbf{h}}_l^H (\bar{\mathbf{Q}}_s + \bar{\mathbf{V}})\bar{\mathbf{h}}_l - \delta E_l - \alpha_l \varepsilon_l^2 \end{bmatrix} \succeq \mathbf{0}, \\
&\mathrm{Tr}[\bar{\mathbf{A}}_i(\bar{\mathbf{Q}}_s + \bar{\mathbf{V}})] + \epsilon_i \|\bar{\mathbf{Q}}_s + \bar{\mathbf{V}}\|_F \leq \delta p_i, \forall i, \\
&\mathrm{Tr}(\bar{\mathbf{Q}}_s + \bar{\mathbf{V}}) \leq \delta P, \bar{\mathbf{Q}}_s \succeq \mathbf{0}, \tilde{\mathbf{V}} \succeq \mathbf{0}, t \geq 0.
\end{aligned} \tag{6.34}$$

where $\bar{c}_k = -\bar{\mathbf{h}}_{e,k}^H[\bar{\mathbf{Q}}_s - (\frac{1}{t} - 1)\bar{\mathbf{V}}]\bar{\mathbf{h}}_{e,k} + \delta(\frac{1}{t} - 1)\sigma_e^2 - \lambda_{e,k}\varepsilon_{e,k}^2$. Without the nonconvex rank constraint, (6.34) is convex, and can be solved by using interior-point method. By solving the problem (6.34), the optimal value $f(t)^*$ can be written as

$$\begin{aligned}
&\frac{(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{Q}_s (\bar{\mathbf{h}}_s + \mathbf{e}_s)}{(\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{V} (\bar{\mathbf{h}}_s + \mathbf{e}_s) + \sigma_s^2} \geq f(t)^*, \\
&\Rightarrow (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H [\mathbf{Q}_s - f(t)^* \mathbf{V}] (\bar{\mathbf{h}}_s + \mathbf{e}_s) \geq f(t)^* \sigma_s^2.
\end{aligned} \tag{6.35}$$

Thus, the associated power minimization problem is considered as

$$\min_{\mathbf{Q}_s, \mathbf{V}, \alpha_l, \beta_s, \lambda_{e,k}} \quad \mathrm{Tr}(\mathbf{Q}_s),$$

$$s.t. \ (6.33\text{a}) - (6.33\text{c}), \tag{6.36a}$$

$$\begin{bmatrix} \beta_s \mathbf{I} + [\mathbf{Q}_s - f(t)^* \mathbf{V}] & [\mathbf{Q}_s - f(t)^* \mathbf{V}]\bar{\mathbf{h}}_s \\ \bar{\mathbf{h}}_s^H [\mathbf{Q}_s - f(t)^* \mathbf{V}] & d_s \end{bmatrix} \succeq \mathbf{0}, \tag{6.36b}$$

where $d_s = \bar{\mathbf{h}}_s^H[\mathbf{Q}_s - f(t)^*\mathbf{V}]\bar{\mathbf{h}}_s - f(t)^*\sigma_s^2 - \beta_s\varepsilon_s^2$. (6.36b) is achieved by employing *S-Procedure*. It is easily verified that the feasible solution to (6.36) is optimal for

(6.33), which is derived from (6.36a) and (6.36b). Thus, the following theorem holds to show that the optimal solution to (6.33) is rank-one:

Theorem 6.2 *Provided that* (6.36) *is feasible, there always exists an optimal solution to* (6.36) *such that rank*$(\mathbf{Q}_s) \leq 1$.

Proof Please refer to Section 6.6.4. ■

6.3.3.2 Successive Convex Approximation

Now, the SCA reformulation is considered to solve the robust secrecy rate maximization problem to jointly optimize secure transmit beamformer and AN by incorporating channel uncertainty. This robust optimization problem is written as

$$\min_{\mathbf{Q}_s, \mathbf{V}} \max_{k} \frac{t_{e,k} r_s}{t_s r_{e,k}} \tag{6.37a}$$

$$s.t.\ \mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P,\ \mathrm{Tr}[(\bar{\mathbf{A}}_i + \boldsymbol{\Delta}_i)(\mathbf{Q}_s + \mathbf{V})] \leq p_i, \forall i, \tag{6.37b}$$

$$(\bar{\mathbf{h}}_l + \mathbf{e}_l)^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_l + \mathbf{e}_l) \geq E_l,\ \forall l, \tag{6.37c}$$

$$\mathbf{Q}_s \succeq \mathbf{0},\ \mathbf{V} \succeq \mathbf{0},\ \mathrm{rank}(\mathbf{Q}_s) = 1. \tag{6.37d}$$

where $t_{e,k} = \sigma_e^2 + (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})$, $r_s = \sigma_s^2 + (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{V}(\bar{\mathbf{h}}_s + \mathbf{e}_s)$, $t_s = \sigma_s^2 + (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_s + \mathbf{e}_s)$ and $r_{e,k} = \sigma_e^2 + (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H \mathbf{V}(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})$. The above problem is convex in terms of (6.37a) and (6.37c). Firs, the exponential variables are introduced to modified (6.37a) as

$$e^{x_0} \leq \sigma_s^2 + \min_{\mathbf{e}_s} (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_s + \mathbf{e}_s), \tag{6.38a}$$

$$e^{x_k} \leq \sigma_e^2 + \min_{\mathbf{e}_{e,k}} (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H \mathbf{V}(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}), \tag{6.38b}$$

$$e^{y_k} \geq \sigma_e^2 + \max_{\mathbf{e}_{e,k}} (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}), \tag{6.38c}$$

$$e^{y_0} \geq \sigma_s^2 + \max_{\mathbf{e}_s} (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{V}(\bar{\mathbf{h}}_s + \mathbf{e}_s), \tag{6.38d}$$

By employing the slack variables (i.e., τ, u_s, $u_{e,k}$, v_s, and $v_{e,k}$) for (6.37a), (6.38a), (6.38b), (6.38c), and (6.38d), respectively, (6.37) can be reformulated as

$$\begin{aligned}
&\min_{\Omega} \ \tau, \\
&s.t. \ e^{y_0+y_k-x_0-x_k} \leq \tau, \ (6.37\text{b}), \ (6.37\text{c}), \ (6.37\text{d}), \\
&\quad e^{x_0} \leq \sigma_s^2 + u_s, \ \min_{\mathbf{e}_s} (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H [\mathbf{Q}_s + \mathbf{V}](\bar{\mathbf{h}}_s + \mathbf{e}_s) \geq u_s, && (6.39\text{a}) \\
&\quad e^{x_k} \leq \sigma_e^2 + u_{e,k}, \ \min_{\mathbf{e}_{e,k}} (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H \mathbf{V} (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}) \geq u_{e,k}, && (6.39\text{b}) \\
&\quad e^{y_k} \geq \sigma_e^2 + v_{e,k}, \ \max_{\mathbf{e}_{e,k}} (\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H (\mathbf{Q}_s + \mathbf{V})(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}) \leq v_{e,k}, && (6.39\text{c}) \\
&\quad e^{y_0} \geq \sigma_s^2 + v_s, \ \max_{\mathbf{e}_s} (\bar{\mathbf{h}}_s + \mathbf{e}_s)^H \mathbf{V} (\bar{\mathbf{h}}_s + \mathbf{e}_s) \leq v_s, && (6.39\text{d}) \\
&\quad \{\mathbf{Q}_s, \mathbf{V}, \mathbf{e}_s, \mathbf{e}_{e,k}, x_0, y_0, x_k, y_k, u_s, u_{e,k}, v_s, v_{e,k}\} \in \Omega, \ \forall k, l, i. && (6.39\text{e})
\end{aligned}$$

By exploiting *S-Procedure* and the first-order Taylor approximation, the problem (6.39a) is written as

$$\begin{aligned}
&\min_{\Omega} \ \tau, \\
&s.t. \ e^{y_0+y_k-x_0-x_k} \leq \tau, \ e^{x_0} \leq \sigma_s^2 + u_s, \ e^{x_k} \leq \sigma_e^2 + u_{e,k}, && (6.40\text{a}) \\
&\quad e^{\bar{y}_k}(y_k - \bar{y}_k + 1) \geq \sigma_e^2 + v_{e,k}, \ e^{\bar{y}_0}(y_0 - \bar{y}_0 + 1) \geq \sigma_s^2 + v_s, && (6.40\text{b}) \\
&\quad \begin{bmatrix} \lambda_s \mathbf{I} + (\mathbf{Q}_s + \mathbf{V}) & (\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_s \\ \bar{\mathbf{h}}_s^H (\mathbf{Q}_s + \mathbf{V}) & \bar{\mathbf{h}}_s^H (\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_s - u_s - \lambda_s \varepsilon_s^2 \end{bmatrix} \succeq \mathbf{0}, && (6.40\text{c}) \\
&\quad \begin{bmatrix} \lambda_{e,k} \mathbf{I} + \mathbf{V} & \mathbf{V}\bar{\mathbf{h}}_{e,k} \\ \bar{\mathbf{h}}_{e,k}^H \mathbf{V} & \bar{\mathbf{h}}_{e,k}^H \mathbf{V} \bar{\mathbf{h}}_{e,k} - u_{e,k} - \lambda_{e,k} \varepsilon_{e,k}^2 \end{bmatrix} \succeq \mathbf{0}, && (6.40\text{d}) \\
&\quad \begin{bmatrix} \beta_{e,k} \mathbf{I} - (\mathbf{Q}_s + \mathbf{V}) & -(\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_{e,k} \\ -\bar{\mathbf{h}}_{e,k}^H (\mathbf{Q}_s + \mathbf{V}) & -\bar{\mathbf{h}}_{e,k}^H (\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_{e,k} + v_{e,k} - \beta_{e,k} \varepsilon_{e,k}^2 \end{bmatrix} \succeq \mathbf{0}, && (6.40\text{e}) \\
&\quad \begin{bmatrix} \beta_s \mathbf{I} - \mathbf{V} & -\mathbf{V}\bar{\mathbf{h}}_s \\ -\bar{\mathbf{h}}_s^H \mathbf{V} & -\bar{\mathbf{h}}_s^H \mathbf{V} \bar{\mathbf{h}}_s + v_s - \beta_s \varepsilon_s^2 \end{bmatrix} \succeq \mathbf{0}, && (6.40\text{f}) \\
&\quad \begin{bmatrix} \alpha_l \mathbf{I} + (\mathbf{Q}_s + \mathbf{V}) & (\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_l \\ \bar{\mathbf{h}}_l^H (\mathbf{Q}_s + \mathbf{V}) & \bar{\mathbf{h}}_l^H (\mathbf{Q}_s + \mathbf{V})\bar{\mathbf{h}}_l - E_l - \alpha_l \varepsilon_l^2 \end{bmatrix} \succeq \mathbf{0}, && (6.40\text{g}) \\
&\quad \mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P, \ \mathrm{Tr}[\bar{\mathbf{A}}_i(\mathbf{Q}_s + \mathbf{V})] + \epsilon_i \|\mathbf{Q}_s + \mathbf{V}\|_F \leq p_i, \\
&\quad \{\mathbf{Q}_s \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, x_0, y_0, x_k, y_k, u_s, u_{e,k}, v_s, v_{e,k}, \\
&\quad \lambda_s \geq 0, \lambda_{e,k} \geq 0, \beta_s \geq 0, \beta_{e,k} \geq 0, \alpha_l \geq 0\} \in \Omega, \ \forall k, l, i. && (6.40\text{h})
\end{aligned}$$

The above problem is convex for a given $\bar{y}_k$ and $\bar{y}_0$ at each iteration, and can be solved by using the interior-point method to update the solution for the next iteration until the algorithm converges. Thus the SCA based robust scheme is similar to Table 6.2. On the other hand, there exists a rank-onel solution to (6.40), and the proof is similar to that of *Theorem* 6.2.

6.4 Simulation Results

Simulation results are provided to validate the proposed algorithms. A MISO secrecy system is considered in the presence of three eavesdroppers and two EH receivers. The legitimate transmitter is equipped with four transmit antennas (i.e., $N_T = 4$), whereas the other receivers (i.e., legitimate user, eavesdroppers and EH receivers) are equipped with a single antenna. It is assumed that the channel coefficients are modelled as both large-scale fading and small-scale fading. The simplified large-scale fading model is given by

$$D = A_0 \left(\frac{d}{d_r} \right)^{-\alpha}, \text{for } d \geq d_r, \tag{6.41}$$

where $A_0 = 1$, d represents the distance between the transmitter and all receivers (i.e., legitimate user d_s, passive eavesdroppers d_e, and the energy receivers d_l), d_r denotes a reference distance set to be 20 meters, and $\alpha = 3$ is the path loss exponent. The small scale fading channel coefficients are assumed to be Rician fading with Rician factor 5 dB. Note that for the involved line-of-sight (LOS) component is modelled as the far-field uniform linear antenna array [108]. In addition, it is assumed that $\sigma_s^2 = \sigma_e^2 = -40$ dBm, and the distances between the transmitter and the legitimate user, the passive eavesdroppers, as well as the energy receivers are set to be 100, 50, 25 meters unless specified. The target transmit power is assumed to be 30 dBm (1w), and the target harvested power is set to be 1mw. All error bounds (i.e., ε_s, $\varepsilon_{e,k}$ and ε_l) are set to be 0.1 or 0.2 unless specified.

First, the secure transmit beamformer for secrecy rate maximization is evaluated. Fig. 6.1 shows the achieved secrecy rate with different transmit powers, where it is easily observed that the achieved secrecy rate increases with transmit power, and the proposed scheme achieves the same performance with the SDP relaxation based scheme in terms of achieved secrecy rate. In order to improve the security in

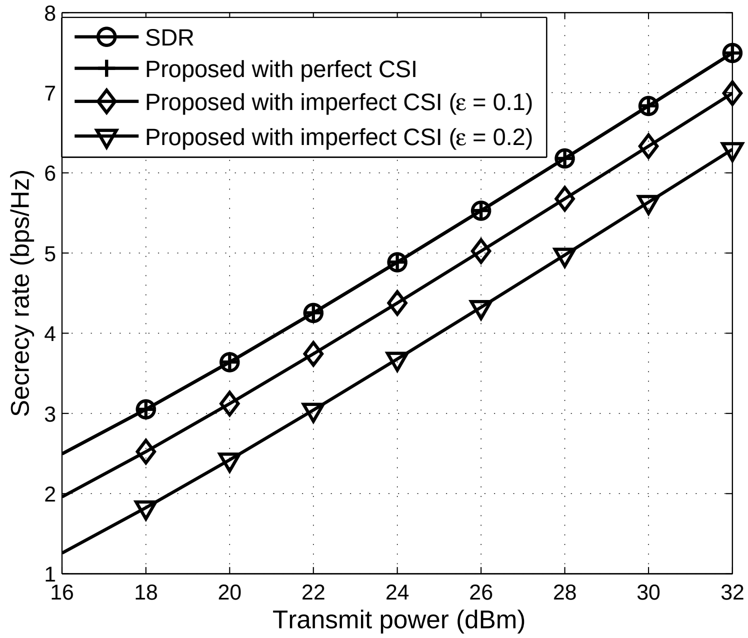

Figure 6.1: Achieved secrecy rate with different transmit powers.

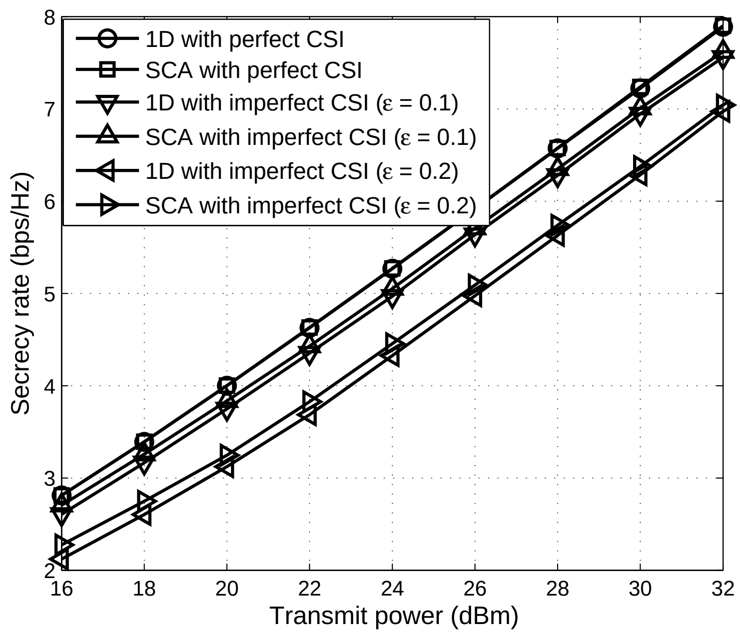

Figure 6.2: AN assisted achieved secrecy rate with different transmit powers.

SWIPT system, AN-aided secrecy rate versus transmit power is plotted in Fig. 6.2 based on both reformulations: two-level optimization and SCA. From this result, one can observe that the secrecy rate of the two proposed schemes increase with transmit power, and both schemes have a similar performance in terms of secrecy rate. In addition, the SCA based scheme outperforms two-level optimization scheme in lower transmit power regime.

Then, the security performance with EH performance is evaluated in Fig. 6.3,

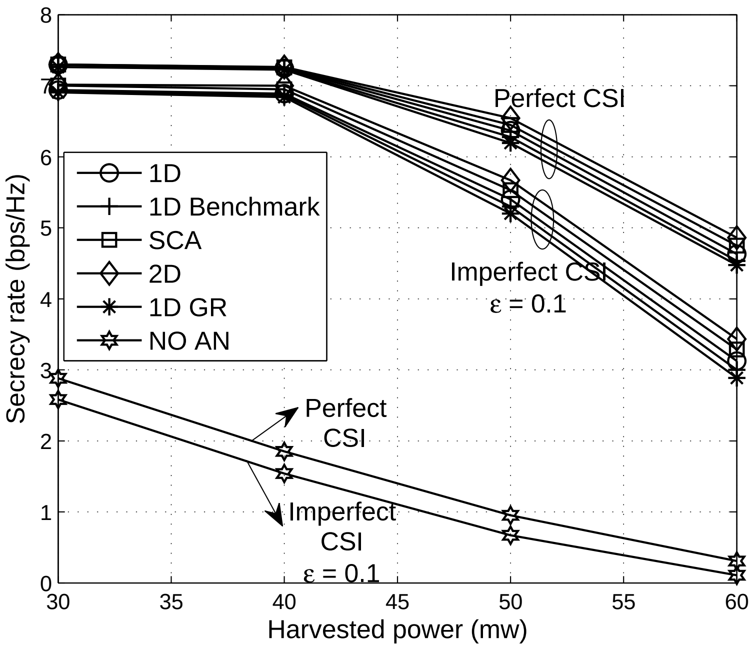

Figure 6.3: Achieved secrecy rate with target harvested power.

which shows that the achieved secrecy rate versus the target harvested power. One can be observed from this result that the secrecy rate decreases with the target harvested power based on perfect and imperfect CSI. Also, we compare our proposed schemes (‘1D’ and ‘SCA’) with the robust schemes (‘1D Benchmark’), 1D based scheme with Gaussian randomization (‘1D GR’), and two-dimensional search based scheme (‘2D’) shown in [61], as well as the case without AN (‘NO AN’), in which the proposed SCA based scheme outperforms our proposed 1D scheme, 1D Benchmark scheme, 1D GR scheme, and NO AN scheme. The SCA based scheme has a similar performance to 2D based scheme in terms of secrecy rate. Fig. 6.4 shows the percentage of AN power consumption in the total transmit power P versus transmit power, which shows that the proportion of AN power consumed to interfere the eavesdroppers or energy harvesting. It is observed that this proportion

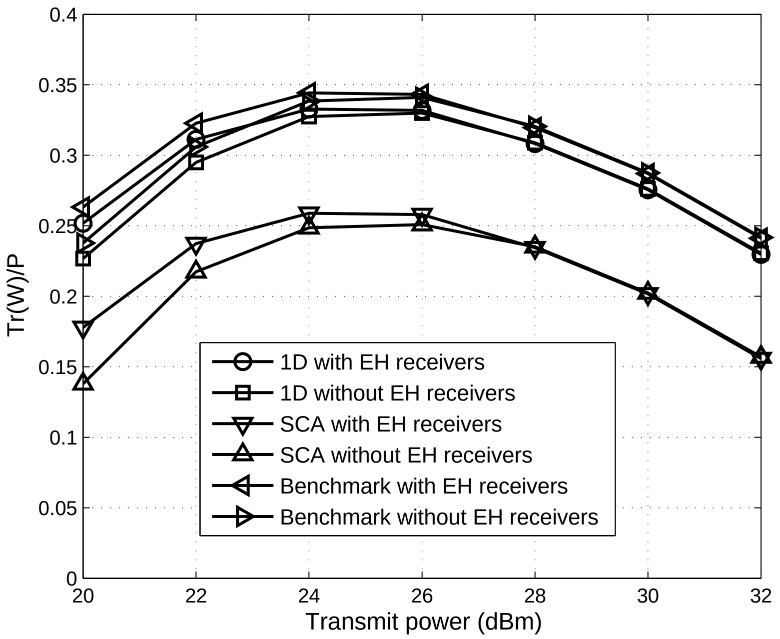

Figure 6.4: The proportion of AN power consumption versus transmit power.

increases and then declines with the increase in transmit power at lower transmit power regime, the percentage of consumed AN power should increase which ensures secure communications and satisfies the EH constraint. When transmit power is high enough, in order to further increase the secrecy rate required, more power should be allocated to the message-bearing signals so that the AN power may get decreased. The scheme without EH receivers has a lower proportion than the scheme with EH receivers, since the AN is introduced to interfere with the passive eavesdropper only in the system without EH receiver.

Finally, the achieved secrecy rate and the harvested power versus the distances between the transmitter and the legitimate user (i.e., d_s), as well as the EH receivers (i.e., d_l) are evaluated, respectively. Fig. 6.5 shows the secrecy rate versus d_s, where the achieved secrecy rate decreases with d_s. In addition, the SCA based scheme outperforms the 1D based scheme in terms of the achieved secrecy rate. Fig. 6.6 shows the EH performance versus d_l. From this result, the harvested power decreases with d_l, approaching zero after $d_s = 40$ m.

6.5 Summary

In this chapter, the secrecy rate maximization problem has been investigated for a MISO SWIPT secure channel in the presence of multiple eavesdroppers and EH

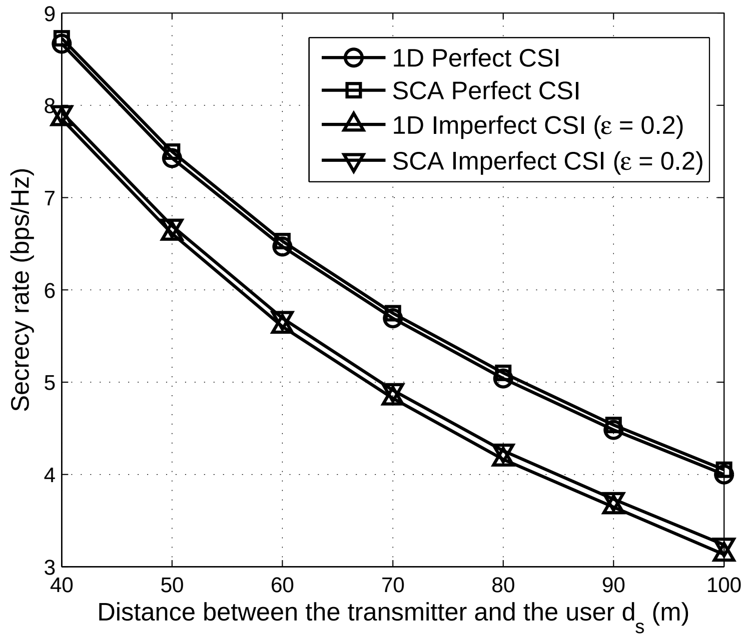

Figure 6.5: Achieved secrecy rate versus distance between the transmitter and the legitimate user.

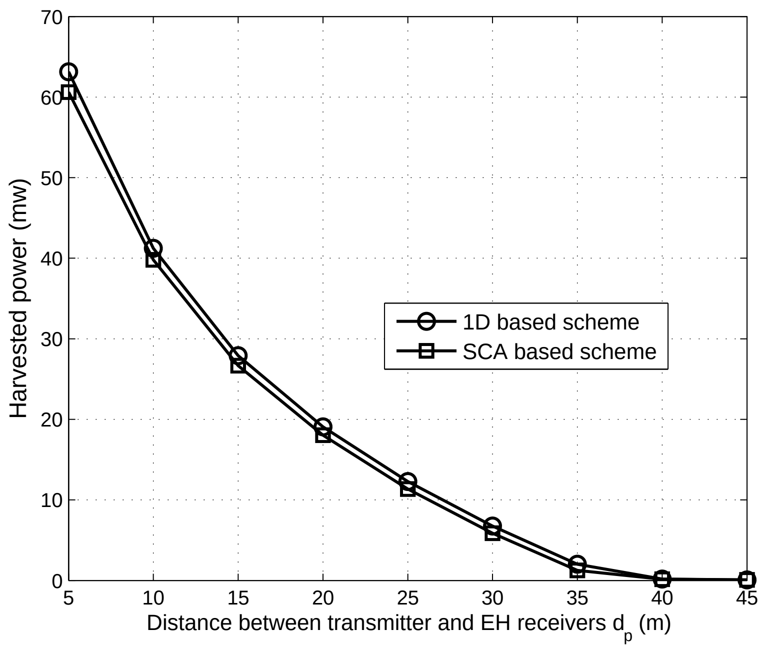

Figure 6.6: Harvested power versus distance between the transmitter and the energy receivers.

receivers. Transmit beamformer was designed to maximize the achieved secrecy rate while satisfying the transmit power and the EH constraints. A two-step approach with SOCP approximation was considered to design secure transmit optimization for the secrecy rate maximization problem. While AN-aided transmit optimization was developed to solve this secrecy rate maximization problem by exploiting two-level optimization and SCA. Furthermore, tightness analyses have been provided to guarantee the optimal condition for the SDP relaxation.

6.6 Appendix

6.6.1 Proof of Lemma 6.1

In order to prove *Lemma* 6.1, the secrecy rate constraint in (6.5) is written as

$$\frac{1}{\sigma_s^2}|\mathbf{w}^H\mathbf{h}_s|^2 \geq \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\mathbf{h}_{e,k} \\ (2^R-1)^{\frac{1}{2}} \end{bmatrix}^H \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\mathbf{h}_{e,k} \\ (2^R-1)^{\frac{1}{2}} \end{bmatrix} \tag{6.42}$$

Then, the following lemma is required to convert (6.42) as a linear matrix inequality (LMI)

Lemma 6.3 *(Schur complement) [70]: Let* $\mathbf{X}$ *be a complex hermitian matrix,*

$$\mathbf{X} = \mathbf{X}^H = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^H & \mathbf{C} \end{bmatrix} \tag{6.43}$$

Thus, $\mathbf{S} = \mathbf{C} - \mathbf{B}^H\mathbf{A}^{-1}\mathbf{B}$ *is the* Schur complement *of* $\mathbf{A}$ *in* $\mathbf{X}$, *and the following statements hold:*

- $\mathbf{X} \succ \mathbf{0}$, *if and only if* $\mathbf{A} \succ \mathbf{0}$ *and* $\mathbf{S} \succ \mathbf{0}$.
- *if* $\mathbf{A} \succ \mathbf{0}$ *then* $\mathbf{X} \succ \mathbf{0}$ *if and only if* $\mathbf{S} \succ \mathbf{0}$.

By exploiting the *Schur complement*, (6.42) can be reformulated as

$$\begin{bmatrix} \frac{1}{\sigma_s}\mathbf{w}^H\mathbf{h}_s\mathbf{I} & \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\mathbf{h}_{e,k} \\ (2^R-1)^{\frac{1}{2}} \end{bmatrix} \\ \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\mathbf{h}_{e,k} \\ (2^R-1)^{\frac{1}{2}} \end{bmatrix}^H & \frac{1}{\sigma_s}\mathbf{w}^H\mathbf{h}_s \end{bmatrix} \succeq \mathbf{0}, \tag{6.44}$$

In addition, the reformulation of the EH constraint (6.5) is considered. In order to express this constraint clearly, two variables (i.e., $x_l \in \mathbb{R}$ and $y_l \in \mathbb{R}$) are introduced such that this constraint can be equivalently modified as

$$x_l^2 + y_l^2 \geq E, \tag{6.45a}$$

$$x_l = \Re\{\mathbf{w}^H \mathbf{h}_l\},\ y_l = \Im\{\mathbf{w}^H \mathbf{h}_l\},\ \forall l. \tag{6.45b}$$

The constraint (6.45b) is convex (linear), whereas (6.45a) is not convex, thus, a first-order Taylor approximation is considered to obtain the desired upper bound. Setting $\mathbf{u}_l = [x_l\ y_l]^T$, gives, $x_l^2 + y_l^2 = \mathbf{u}_l^T \mathbf{u}_l$. $\mathbf{u}_l^{(n)}$ is the n-th iteration of the vector $\mathbf{u}_l$. Thus, (6.45a) can be approximated as

$$\mathbf{u}_l^T \mathbf{u}_l \approx \|\mathbf{u}_l^{(n)}\|^2 + 2\sum_{i=1}^{2} \mathbf{u}_l^{(n)}(i)[\mathbf{u}_l(i) - \mathbf{u}_l^{(n)}(i)], \tag{6.46}$$

where i denotes the i-th element of the vector $\mathbf{u}_l$. This completes *Lemma* 6.1. ■

6.6.2 Proof of Lemma 6.2

The second constraint (6.8) can be written by exploiting the *Schur complement* as

$$\mathbf{S}_k^{'} = \begin{bmatrix} f^{(n)}(t_2)\mathbf{I} & \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}) \\ (2^R - 1)^{\frac{1}{2}} \end{bmatrix} \\ \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H(\bar{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}) \\ (2^R - 1)^{\frac{1}{2}} \end{bmatrix}^H & f^{(n)}(t_2) \end{bmatrix} \succeq \mathbf{0}, \tag{6.47}$$

where $f^{(n)}(t_2)$ has been defined in (6.9). The the following *lemma* is given to remove the impact of the channel uncertainty

Lemma 6.4 *[100, 109]: For a given set of matrices* $\mathbf{A} = \mathbf{A}^H$, $\mathbf{B}$ *and* $\mathbf{C}$, *the following linear matrix inequality is satisfied:*

$$\mathbf{A} \succeq \mathbf{B}\mathbf{X}\mathbf{C} + \mathbf{C}^H\mathbf{X}^H\mathbf{B}, \|\mathbf{X}\| \leq t, \tag{6.48}$$

if and only if there exist non-negative real numbers a such that

$$\begin{bmatrix} \mathbf{A} - a\mathbf{C}^H\mathbf{C} & -t\mathbf{B}^H \\ -t\mathbf{B} & a\mathbf{I} \end{bmatrix} \succeq 0. \tag{6.49}$$

By exploiting *Lemma* 6.4, the constraint (6.47) is written as

$$\mathbf{S}_k \succeq \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \mathbf{e}_{e,k} \begin{bmatrix} \mathbf{0} & -1 \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ -1 \end{bmatrix} \mathbf{e}_{e,k}^H \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \tag{6.50}$$

where

$$\mathbf{S}_k = \begin{bmatrix} f^{(n)}(t_2)\mathbf{I} & \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\bar{\mathbf{h}}_{e,k} \\ (2^R - 1)^{\frac{1}{2}} \end{bmatrix} \\ \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H\bar{\mathbf{h}}_{e,k} \\ (2^R - 1)^{\frac{1}{2}} \end{bmatrix}^H & f^{(n)}(t_2) \end{bmatrix} \tag{6.51}$$

Thus, (6.47) can be reformulated as

$$\bar{\mathbf{S}}_k = \begin{bmatrix} \mathbf{S}_k - \lambda_k \begin{bmatrix} \mathbf{0} & -1 \end{bmatrix} \begin{bmatrix} \mathbf{0} \\ -1 \end{bmatrix} & -\varepsilon_{e,k} \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \\ -\varepsilon_{e,k} \begin{bmatrix} \frac{2^{\frac{R}{2}}}{\sigma_e}\mathbf{w}^H & \mathbf{0} & \mathbf{0} \end{bmatrix} & \lambda_k\mathbf{I} \end{bmatrix} \succeq \mathbf{0}, \forall k. \tag{6.52}$$

This completes *Lemma* 6.2. ■

6.6.3 Proof of Theorem 6.1

In order to show *Theorem* 6.1, first, the Lagrange dual function to (6.24) can be written as

$$\mathcal{L}(\mathbf{Q}_s, \mathbf{V}, \mathbf{Y}, \mathbf{Z}, \lambda, \mu, \eta_i, \nu_l, \tau_k) = \mathrm{Tr}(\mathbf{Q}_s) - \lambda\Big[\mathrm{Tr}[\mathbf{h}_s\mathbf{h}_s^H(\mathbf{Q}_s - f(t)\mathbf{V})] - \sigma_s^2 f(t)\Big]$$
$$+ \mu\Big[\mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) - P\Big] + \sum_{i=1}^{N_T}\eta_i\Big[\mathrm{Tr}[\mathbf{A}_i(\mathbf{Q}_s + \mathbf{V})] - p_i\Big] - \sum_{l=1}^{L}\nu_l\Big[\mathrm{Tr}[\mathbf{h}_l\mathbf{h}_l^H(\mathbf{Q}_s + \mathbf{V})]$$
$$- E_l\Big] + \sum_{k=1}^{K}\tau_k\Big[\mathrm{Tr}[\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H(\mathbf{Q}_s - (t-1)\mathbf{V})] - (t-1)\sigma_e^2\Big] - \mathrm{Tr}(\mathbf{Y}\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{V}), \tag{6.53}$$

where $\mathbf{Y} \in \mathbb{H}_+^{N_T}$, $\mathbf{Z} \in \mathbb{H}_+^{N_T}$, $\lambda \in \mathbb{R}_+$, $\mu \in \mathbb{R}_+$, $\eta_i \in \mathbb{R}_+$, $\nu_l \in \mathbb{R}_+$, $\tau_k \in \mathbb{R}_+$ denote the dual variables of $\mathbf{Q}_s$, $\mathbf{V}$, (6.23), (6.14a), (6.14b), and (6.19), respectively. Then, the related KKT conditions is considered as follows:

$$\frac{\partial\mathcal{L}}{\partial\mathbf{Q}_s} = 0, \Rightarrow \mathbf{Y} = \mathbf{I} - \lambda\mathbf{h}_s\mathbf{h}_s^H + \mu\mathbf{I} + \sum_{i=1}^{N_T}\eta_i\mathbf{A}_i - \sum_{l=1}^{L}\nu_l\mathbf{h}_l\mathbf{h}_l^H + \sum_{k=1}^{K}\tau_k\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H, \tag{6.54a}$$

$$\frac{\partial\mathcal{L}}{\partial\mathbf{V}} = 0, \Rightarrow \mathbf{Z} = \lambda f(t)\mathbf{h}_s\mathbf{h}_s^H + \mu\mathbf{I} + \sum_{i=1}^{N_T}\eta_i\mathbf{A}_i - \sum_{l=1}^{L}\nu_l\mathbf{h}_l\mathbf{h}_l^H - \sum_{k=1}^{K}\tau_k(t-1)\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H, \tag{6.54b}$$

$$\mathbf{Q}_s\mathbf{Y} = \mathbf{0}, \mathbf{Z} \succeq \mathbf{0},\ \lambda \geq 0,\ \forall i, l, k. \tag{6.54c}$$

By subtracting (6.54b) from (6.54a), we have

$$\mathbf{Y} - \mathbf{Z} = \mathbf{I} - \lambda(1 + f(t))\mathbf{h}_s\mathbf{h}_s^H + \sum_{k=1}^{K}\tau_k t\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H,$$
$$\Rightarrow \mathbf{Y} = \mathbf{A} - \lambda(1 + f(t))\mathbf{h}_s\mathbf{h}_s^H, \tag{6.55}$$

where $\mathbf{A} = \mathbf{I} + \mathbf{Z} + \sum_{k=1}^{K}\tau_k t\mathbf{h}_{e,k}\mathbf{h}_{e,k}^H$. From (6.55), one can easily observe that $\mathbf{A}$ is positive definite, and $\mathrm{rank}(\mathbf{A}) = N_T$, whereas $\mathrm{rank}(\mathbf{Y}) = N_T$ or $N_T - 1$. However, if $\mathrm{rank}(\mathbf{Y}) = N_T$, then it violates $\mathbf{Q}_s \neq \mathbf{0}$. Thus, $\mathrm{rank}(\mathbf{Y}) = N_T - 1$ always holds, which implies $\mathbf{Q}_s$ lies in the null space of $\mathbf{Y}$ from (6.54c), thus $\mathrm{rank}(\mathbf{Q}_s) = 1$. This completes *Theorem* 6.1. ■

6.6.4 Proof of Theorem 6.2

The dual function to (6.36) is written as follows:

$$\begin{aligned}
&\mathcal{L}(\mathbf{Q}_s, \mathbf{V}, \mathbf{Y}, \mathbf{Z}, \lambda, \gamma_i, \mathbf{T}_s, \mathbf{T}_{e,k}, \mathbf{T}_l) = \mathrm{Tr}(\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Y}\mathbf{Q}_s) - \mathrm{Tr}(\mathbf{Z}\mathbf{V}) + \lambda[\mathrm{Tr}(\mathbf{Q}_s + \mathbf{V}) \\
&\quad - P] + \sum_{i=1}^{N_T} \gamma_i \Big[\mathrm{Tr}[\bar{\mathbf{A}}_i(\mathbf{Q}_s + \mathbf{V})] + \epsilon_i \|\mathbf{Q}_s + \mathbf{V}\|_F - p_i\Big] - \mathrm{Tr}(\mathbf{T}_s \mathbf{A}_1) \\
&\quad - \mathrm{Tr}[\mathbf{T}_s \mathbf{H}_s^H (\mathbf{Q}_s - f(t)\mathbf{V})\mathbf{H}_s] - \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{T}_{e,k}\mathbf{B}_k) + \sum_{k=1}^{K} \mathrm{Tr}\Big[\mathbf{T}_{e,k}\mathbf{H}_{e,k}^H [\mathbf{Q}_s - (t^{-1} - 1)\mathbf{V}]\mathbf{H}_{e,k}\Big] \\
&\quad - \sum_{l=1}^{L} \mathrm{Tr}(\mathbf{T}_l \mathbf{C}_l) - \sum_{l=1}^{L} \mathrm{Tr}[\mathbf{T}_l \mathbf{H}_l^H (\mathbf{Q}_s + \mathbf{V})\mathbf{H}_l],
\end{aligned} \tag{6.56}$$

where $\mathbf{Y} \in \mathbb{H}_+^{N_T}$, $\mathbf{Z} \in \mathbb{H}_+^{N_T}$, $\lambda \in \mathbb{R}_+$, $\gamma_i \in \mathbb{R}_+$, $\mathbf{T}_s \in \mathbb{H}_+^{N_T+1}$, $\mathbf{T}_{e,k} \in \mathbb{H}_+^{N_T+1}$ and $\mathbf{T}_l \in \mathbb{H}_+^{N_T+1}$ are dual variables of $\mathbf{Q}_s$, $\mathbf{V}$, (6.33a), (6.33c) and (6.33b), respectively. In addition,

$$\begin{aligned}
\mathbf{A}_1 &= \begin{bmatrix} \beta_s \mathbf{I} & \mathbf{0} \\ \mathbf{0}^H & -f(t)\sigma_s^2 - \beta_s \varepsilon_s^2 \end{bmatrix}, \ \mathbf{H}_s = \begin{bmatrix} \mathbf{I}_{N_T} & \bar{\mathbf{h}}_s \end{bmatrix}, \\
\mathbf{B}_k &= \begin{bmatrix} \lambda_{e,k} \mathbf{I} & \mathbf{0} \\ \mathbf{0}^H & (t^{-1} - 1)\sigma_e^2 - \lambda_{e,k}\varepsilon_{e,k}^2 \end{bmatrix}, \ \mathbf{H}_{e,k} = \begin{bmatrix} \mathbf{I}_{N_T} & \bar{\mathbf{h}}_{e,k} \end{bmatrix}, \\
\mathbf{C}_l &= \begin{bmatrix} \alpha_l \mathbf{I} & \mathbf{0} \\ \mathbf{0}^H & -E_l - \alpha_l \varepsilon_l^2 \end{bmatrix}, \ \mathbf{H}_l = \begin{bmatrix} \mathbf{I}_{N_T} & \bar{\mathbf{h}}_l \end{bmatrix}.
\end{aligned}$$

The related KKT conditions are considered as follows:

$$\begin{aligned}
&\frac{\partial \mathcal{L}}{\partial \mathbf{Q}_s} = 0, \Rightarrow \mathbf{Y} = \mathbf{I} + \lambda \mathbf{I} + \sum_{i=1}^{N_T} \gamma_i [\bar{\mathbf{A}}_i + \epsilon_i \|\mathbf{Q}_s + \mathbf{W}\|_F^{-1} \mathbf{I}] - \mathbf{H}_s \mathbf{T}_s \mathbf{H}_s^H \\
&+ \sum_{k=1}^{K} \mathbf{H}_{e,k} \mathbf{T}_{e,k} \mathbf{H}_{e,k}^H - \sum_{l=1}^{L} \mathbf{H}_l \mathbf{T}_l \mathbf{H}_l^H,
\end{aligned} \tag{6.57a}$$

$$\begin{aligned}
&\frac{\partial \mathcal{L}}{\partial \mathbf{V}} = 0, \Rightarrow \mathbf{Z} = \lambda \mathbf{I} + \sum_{i=1}^{N_T} \gamma_i [\bar{\mathbf{A}}_i + \epsilon_i \|\mathbf{Q}_s + \mathbf{W}\|_F^{-1} \mathbf{I}] + f(t) \mathbf{H}_s \mathbf{T}_s \mathbf{H}_s^H \\
&- \sum_{k=1}^{K} (t^{-1} - 1) \mathbf{H}_{e,k} \mathbf{T}_{e,k} \mathbf{H}_{e,k}^H - \sum_{l=1}^{L} \mathbf{H}_l \mathbf{T}_l \mathbf{H}_l^H,
\end{aligned} \tag{6.57b}$$

$$\mathbf{Q}_s \mathbf{Y} = \mathbf{0}, \mathbf{Z} \succeq \mathbf{0}, \ \forall i, k, l, \tag{6.57c}$$

$$[\mathbf{A}_1 + \mathbf{H}_s^H (\mathbf{Q}_s - f(t)\mathbf{V})\mathbf{H}_s]\mathbf{T}_s = \mathbf{0}. \tag{6.57d}$$

By subtracting (6.57b) from (6.57a), the following equality holds:

$$\mathbf{Y}-\mathbf{Z}=\mathbf{I}-[1+f(t)]\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H+\sum_{k=1}^{K}t^{-1}\mathbf{H}_{e,k}\mathbf{T}_{e,k}\mathbf{H}_{e,k}^H,$$

$$\Rightarrow \mathbf{Y}+[1+f(t)]\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H=\mathbf{I}+\mathbf{Z}+\sum_{k=1}^{K}t^{-1}\mathbf{H}_{e,k}\mathbf{T}_{e,k}\mathbf{H}_{e,k}^H. \tag{6.58}$$

Premultiply (6.58) by $\mathbf{Q}_s$

$$\mathbf{Q}_s\left(\mathbf{I}+\mathbf{Z}+\sum_{k=1}^{K}t^{-1}\mathbf{H}_{e,k}\mathbf{T}_{e,k}\mathbf{H}_{e,k}^H\right)=[1+f(t)]\mathbf{Q}_s\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H. \tag{6.59}$$

The following rank relation holds:

$$\begin{aligned}\operatorname{rank}(\mathbf{Q}_s)&=\operatorname{rank}\left[\mathbf{Q}_s\left(\mathbf{I}+\mathbf{Z}+\sum_{k=1}^{K}t^{-1}\mathbf{H}_{e,k}\mathbf{T}_{e,k}\mathbf{H}_{e,k}^H\right)\right]\\&=\operatorname{rank}(\mathbf{Q}_s\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H)\leq\min\{\operatorname{rank}(\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H),\operatorname{rank}(\mathbf{Q}_s)\}.\end{aligned} \tag{6.60}$$

Based on the above rank relation, it is necessary to show $\operatorname{rank}(\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H)\leq 1$ if we claim $\operatorname{rank}(\mathbf{Q}_s)\leq 1$, thus, the two facts is considered as

$$\begin{bmatrix}\mathbf{I}_{N_T} & \mathbf{0}\end{bmatrix}\mathbf{H}_s^H=\mathbf{I}_{N_T},$$
$$\begin{bmatrix}\mathbf{I}_{N_T} & \mathbf{0}\end{bmatrix}\mathbf{A}_1=\beta_s\left(\mathbf{H}_s-\begin{bmatrix}\mathbf{0}_{N_T} & \bar{\mathbf{h}}_s\end{bmatrix}\right).$$

Premultiply $\begin{bmatrix}\mathbf{I}_{N_T} & \mathbf{0}\end{bmatrix}$ and postmultiply $\mathbf{H}_s^H$ by (6.57d), respectively, and applying the above two equalities, the following relations hold:

$$\beta_s\left(\mathbf{H}_s-\begin{bmatrix}\mathbf{0}_{N_T} & \bar{\mathbf{h}}_s\end{bmatrix}\right)\mathbf{T}_s\mathbf{H}_s^H+[\mathbf{Q}_s-f(t)\mathbf{V}]\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H=0,$$

$$\Rightarrow\left(\beta_s\mathbf{I}+[\mathbf{Q}_s-f(t)\mathbf{V}]\right)\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H=\beta_s\begin{bmatrix}\mathbf{0}_{N_T} & \bar{\mathbf{h}}_s\end{bmatrix}\mathbf{T}_s\mathbf{H}_s^H. \tag{6.61}$$

Lemma 6.5 *If a block hermitian matrix* $\mathbf{P}=\begin{bmatrix}\mathbf{P}_1 & \mathbf{P}_2\\ \mathbf{P}_3 & \mathbf{P}_4\end{bmatrix}\succeq\mathbf{0}$, *then the main diagonal matrices* $\mathbf{P}_1$ *and* $\mathbf{P}_4$ *are always PSD matrices [93].*

Now, it can be shown that $\beta_s\mathbf{I}+[\mathbf{Q}_s-f(t)\mathbf{V}]\succeq\mathbf{0}$ and is nonsingular, thus pre(post)multiply by a nonsingular matrix will not change the matrix rank. Thus, the following rank relation holds:

$$\mathrm{rank}(\mathbf{H}_s\mathbf{T}_s\mathbf{H}_s^H) = \mathrm{rank}\left(\begin{bmatrix} \mathbf{0}_{N_T} & \bar{\mathbf{h}}_s \end{bmatrix}\mathbf{T}_s\mathbf{H}_s^H\right) \leq \mathrm{rank}\left(\begin{bmatrix} \mathbf{0}_{N_T} & \bar{\mathbf{h}}_s \end{bmatrix}\right) \leq 1. \quad (6.62)$$

This completes *Theorem* 6.2. ■

Chapter 7

Conclusions and Future Work

7.1 Conclusions

This thesis has investigated various transmit optimization techniques of secrecy rate optimization problems (power minimization and secrecy rate maximization) for physical layer security using convex optimization techniques and game theory. Transmit beamformer has been developed to obtain the optimal power allocation. The proposed optimization problems were reformulated into convex ones, and associated robust schemes have been proposed by incorporating different forms of channel uncertainty models.

In Chapter 4, transmit optimization for a multiple-input single-output (MISO) secrecy channel has been investigated. Power minimization was first considered to design the secure transmit beamformer and a second-order cone programming (SOCP) based reformulation was proposed to solve this problem. In addition, a closed-form solution of transmit beamformer for the scenario of an eavesdropper was derived by employing Karush-Kuhn-Tucker (KKT) conditions. Second, the robust schemes were investigated subject to outage probability secrecy rate constraint by incorporating two statistical channel uncertainty models. A two-step algorithm with both conservative reformulations (i.e., *Bernstein-type* inequality and *S-Procedure*) was presented to handle this nonconvex optimization problem. Furthermore, an initial proof has been proposed to show that the optimal solution to the reformulated problem was rank-one to guarantee its solution is also optimal to the original problem.

In Chapter 5, transmit optimization for a multiple-input multiple-output (MIMO) wiretap channel has been studied, where a multi-antenna cooperative jammer (CJ) was employed to provide the jamming service to improve secure communication. Power minimization and secrecy rate maximization have also been considered. To solve these two non-convex problems, the transmit covariance matrices of the legitimate transmitter and the CJ were designed, alternatively. For a given transmit covariance matrix at the CJ, both problems were handled with a first-order Taylor approximation. In addition, the robust scheme incorporating channel uncertainty has been solved by exploiting *S-Procedure*, which can be formulated into a SDP. Moreover, game theory based secure transmit optimization has been designed when a private CJ is employed to introduce charges for its jamming service in terms of interference and caused to the eavesdropper. This scheme was formulated as a *Stackelberg* game, where the private CJ and the transmitter have been modelled as the leader and the follower, respectively, and both were to maximize their own revenue function. For this proposed game, *Stackelberg* equilibrium has been analytically derived with closed-form solutions.

In Chapter 6, transmit optimization for a MISO secure simultaneous wireless information power transfer (SWIPT) system has been investigated, where secure transmit beamformer was developed to maximize the achieved secrecy rate while satisfying the transmit power budget and the EH constraint. A two-step algorithm with SOCP reformulation was proposed to handle the nonconvex secrecy rate constriant, and first-order Taylor approximation was considered to linearize the EH constraint. In addition, Secure transmit beamformer and AN were jointly designed, where a two-level optimization and SCA have been proposed to relax this secrecy rate maximization problem. Besides, it has been shown that the relaxed problem yields a rank-one solution, which guarantees that its solution is optimal to the original problem.

7.2 Future Work

The potential areas of future research stem from fifth generation (5G) wireless communication networks, which has attracted more and more attention in recent years. 5G denotes the next major phase of mobile telecommunications standards beyond the current 4G/IMT-Advanced standards, which provide much more than just fast data speeds on mobile devices, envisioned as the key to providing seamless commu-

nications. Spectral efficiency (SE), energy efficiency (EE), and security have been considered for the evolutions of 5G wireless communication networks and can be achieved by taking full advantage of limited radio spectrum effectively. Therefore, SE and EE, together with security in 5G wireless communication networks will be an important and promising topic for future research.
There are a series of key techniques in 5G wireless communications, including:

1. Non-orthogonal multiple access (NOMA) - a shift from conventional telecommunication systems relying on interference free assumptions.

2. Massive multiple input and multiple output (MIMO) system - offering excess degrees of freedom due to the use of hundreds of antennas at a single base station, an important breakthrough due to recent advances in semiconductor technologies.

3. Cooperative communications, and full duplex (FD) communication - important physical layer solutions for spectrum crunch, a global phenomenon where mobile communications are always hungry for more bandwidth resource.

4. Millimetre wave communications - a promising enabling technology for future cellular networks since it operates in the 10-300GHz band, in which more spectrum can be used for telecommunications

5. Device-to-device (D2D) communications and cognitive radio (CR) - important for merging telecommunication networks with mobile internet, internet of things, etc.

The key techniques of 5G, coupled with existing interests (i.e., physical layer security and SWIPT), will become more and more attractive in the research of the future wireless communications. Due to the issue of spectrum scarcity, the system can be designed for realizing spectral and energy efficient with secure transmission. Resource allocation algorithms is developed optimally to achieve these requirements.

First, FD system with security and SWIPT can be considered as a promising area, where the FD base station (BS) employs the PS scheme to harvest power and decode information from the uplink channel and self-interference (SI) channel with self-energy recycling. At the same time, the FD BS broadcast their own information to the user by utilizing the harvested power. The eavesdropper is considered to overhear the uplink and downlink transmission simultaneously. Thus, the FD BS will guarantee the uplink and downlink secrecy rates to satisfy the reliability criteria, and EH target to the FD BS for uplink transmission and self-energy recycling.

Second, secure energy efficiency (SEE) with SWIPT is another interesting area that considers the ratio of the secure spectral efficiency (SSE) with the difference between the total transmit power and the harvested power. The formulated problem involves a fractional programming, which can be typically solved by employing Dinkelbach's algorithm. In addition, according to the property of fractional programming, the novel reformulation can be proposed based on *Charnes-Cooper* transformation and one-dimensional (1D) search. Also, the trade-off between SEE and SSE can be analysed theoretically and numerically.

Third, CR (or D2D) system with security, where the primary system will share their spectrum with the CR (or D2D) transceivers, also guarantees secure communications in the presence of passive eavesdroppers, or even when CR transceivers (or D2D nodes) are untrusted that overhear the information from the primary system. In this system, two schemes can be modelled, underlay and cooperative schemes. The underlay scheme is that the primary transmitter and the secondary transmitter send information to their dedicated receivers in a spectrum-sharing manner, whereas for the cooperative scheme, the second user is willing to assist the primary transmission by employing amplify-and-forward (AF) or decode-and-forward (DF) relaying to access the channel.

Based on the aforementioned analyses, the key techniques of 5G with the research works in this thesis are promising to realize the optimal resource allocation for secure wireless networks.

References

[1] A. Goldsmith, *Wireless Communications.* Cambridge University Press, 2005.

[2] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications.* Cambridge University Press, 2005.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge University Press, 2011. [Online]. Available: https://books.google.co.uk/books?id=ov5jYjrrNCIC

[4] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography.* CRC Press, 1996.

[5] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends Commun. Info. Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[6] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Tech. J.*, vol. 1, no. 2, pp. 41–59, Autumn 1996.

[7] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Trans. on Telecomm.*, vol. 10, no. 6, pp. 585–596, Nov. 1999.

[8] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol. 6, pp. 311–335, 1998.

[9] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. Poor, *MIMO Wireless Communications.* Cambridge University Press, 2007.

[10] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[12] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform Theory*, vol. 54, no. 6, pp. 2470 –2492, Jun. 2008.

[13] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications.* CRC Press, 2013.

[14] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[15] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge University Press, 2011.

[16] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. Inform. Forens. Security*, vol. 6, no. 3, pp. 682–692, Sep. 2011.

[17] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[18] ——, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[19] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[20] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[21] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[22] J. Huang and A. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[23] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[24] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Vehicular Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[25] Z. Chu, M. Johnston, and S. Le Goff, "Alternating optimization for MIMO secrecy channel with a cooperative jammer," in *Proc. IEEE, VTC Spring, Glasgow, Scotland*, May. 2015, pp. 1–5.

[26] ——, "Robust beamforming techniques for MISO secrecy communication with a cooperative jammer," in *Proc. IEEE, VTC Spring, Glasgow, Scotland*, May. 2015, pp. 1–5.

[27] C. Wang, H.-M. Wang, X.-G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May 2015.

[28] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[29] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May, 2013.

[30] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, "Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications," *IET Commun.*, vol. 9, no. 3, pp. 396–403, Feb. 2015.

[31] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[32] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[33] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[34] J. Huang and L. A. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1702, Apr. 2012.

[35] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[36] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[37] Z. Ding and K. K. Leung, "Impact of imperfect channel state information on bi-directional communications with relay selection," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5657–5662, Nov. 2011.

[38] J. Li and A. Petropulu, "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels," [Available online]: http://arxiv.org/pdf/0909.2622.pdf, Sept. 2009.

[39] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2013.

[40] Z. Han, D. Niyato, and W. Saad, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*, ser. Cambridge

books online. Cambridge University Press, 2011. [Online]. Available: http://books.google.co.uk/books?id=oSnz5ngb9YkC

[41] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inform. Forens. Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[42] K. Cumanan, R. Krishna, V. Sharma, and S. Lambotharan, "Robust interference control techniques for multi-user cognitive radios using worst-case performance optimization," in *Proc. Asilomar Conf. Sign., Syst. and Comp., Pacific Grove, CA*, Oct. 2008, pp. 378–382.

[43] ——, "A robust beamforming based interference control technique and its performance for cognitive radios," in *Proc. Int. Symp. Commun. and Inform. Techno. (ISCIT) 2008*, Oct. 2008, pp. 9–13.

[44] ——, "Robust interference control techniques for cognitive radios using worst-case performance optimization," in *Proc. ISITA 2008, Auckland, New Zealand*, Dec. 2008, pp. 1–5.

[45] G. Zheng, K.-K. Wong, and T.-S. Ng, "Energy-efficient multiuser SIMO: achieving probabilistic robustness with Gaussian channel uncertainty," *IEEE Trans. Commun.,*, vol. 57, no. 6, pp. 1866–1878, Jun. 2009.

[46] G. Zheng, K.-K. Wong, and B. Ottersten, "Robust cognitive beamforming with bounded channel uncertainties," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4871–4881, Dec. 2009.

[47] A. Mukherjee and L. A. 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.

[48] K. Cumanan, Z. Ding, B. Sharif, G. Tian, and K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Vehicular Technol.*, vol. 63, no. 4, pp. 1678–1690, May, 2014.

[49] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *IEEE GLOBECOM 2009*, Nov 2009, pp. 1–5.

[50] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[51] E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "Evolution toward 5G multi-tier cellular wireless networks: An interference management perspective," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 118–127, Jun. 2014.

[52] V. Raghunathan, S. Ganeriwal, and M. Srivastava, "Emerging techniques for long lived wireless sensor networks," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 108–114, Apr. 2006.

[53] L. Varshney, "Transporting information and energy simultaneously," in *Proc. 2008 IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.

[54] P. Grover and A. Sahai, "Shannon meets tesla: Wireless information and power transfer," in *Proc. 2010 IEEE Int. Symp. Inf. Theory*, June, 2010, pp. 2363–2367.

[55] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[56] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[57] Q. Li, W.-K. Ma, and A.-C. So, "Robust artificial noise-aided transmit optimization for achieving secrecy and energy harvesting," in *Proc. 2014 IEEE ICASSP*, May 2014, pp. 1596–1600.

[58] D. Ng, E. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[59] D. Ng and R. Schober, "Max-min fair wireless energy transfer for secure multiuser communication systems," in *IEEE Information Theory Workshop (ITW)*, Nov. 2014, pp. 326–330.

[60] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure transmission in MISO simultaneous wireless information and power transfer system," *IEEE Trans. Vehicular Technol.*, vol. 64, no. 1, pp. 400–405, Jan. 2015.

[61] M. Tian, X. Huang, Q. Zhang, and J. Qin, "Robust AN-Aided secure transmission scheme in MISO channels with simultaneous wireless information and power transfer," *IEEE, Signal Process. Lett.*, vol. 22, no. 6, pp. 723–727, Jun. 2015.

[62] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 906–915, Mar. 2015.

[63] Z. Chu, Z. Zhu, M. Johnston, and S. L. Goff, "Simultaneous wireless information power transfer for MISO secrecy channel," *to appear in IEEE Trans. Vehicular Techno.*, 2015.

[64] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in ofdma systems," *to appear in IEEE Tran. Wireless Commun.*, 2016.

[65] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. J.*, pp. 379–423, 1948.

[66] D. Palomar and M. A. Lagunas, "Joint transmit-receive space-time equalization in spatially correlated MIMO channels: a beamforming approach," *IEEE J. Sel. Areas in Commun.*, vol. 21, no. 5, pp. 730–743, June. 2003.

[67] D. Palomar, J. Cioffi, and M. Lagunas, "Joint Tx-Rx beamforming design for multicarrier MIMO channels: a unified framework for convex optimization," *IEEE Trans. Signal Process.*, vol. 51, no. 9, pp. 2381–2401, Sept. 2003.

[68] D. Palomar, M. Lagunas, and J. Cioffi, "Optimum linear joint transmit-receive processing for MIMO channels with QoS constraints," *IEEE Trans. Signal Process.*, vol. 52, no. 5, pp. 1179–1197, May 2004.

[69] G. Strang, *Linear Algebra and its Applications.* Fourth edition: Thomson Brooks/Cole, 2006.

[70] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge, UK: Cambridge University Press, 2004.

[71] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[72] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949. [Online]. Available: http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x

[73] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[74] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[75] J. Li and A. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[76] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.

[77] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[78] S. Boyd, L. Xiao, and A. Mutapcic, "Subgradient methods," 2003. [Online]. Available: http://www.stanford.edu/class/ee392o/subgrad_method.pdf

[79] S. Vorobyov, A. Gershman, and Z.-Q. Luo, "Robust adaptive beamforming using worst-case performance optimization: A solution to the signal mismatch problem," *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 313–324, Feb. 2003.

[80] R. Lorenz and S. Boyd, "Robust minimum variance beamforming," *IEEE Trans. Signal Process.*, vol. 53, no. 5, pp. 1684–1696, May 2005.

[81] A. Abdel-Samad, T. Davidson, and A. Gershman, "Robust transmit eigen beamforming based on imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 54, no. 2, pp. 1596–1609, May 2006.

[82] S. Vorobyov, H. Chen, and A. Gershman, "On the relationship between robust minimum variance beamformers with probabilistic and worst-case distortionless response constraints," *IEEE Trans. Signal Process.*, vol. 56, no. 11, pp. 5719–5724, Nov. 2008.

[83] K.-Y. Wang, A.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans., Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.

[84] Z.-Q. Luo, "Applications of convex optimization in signal processing and digital communication," *Math Program Series, B97*, pp. 177–207, 2003.

[85] Z.-Q. Luo and W. Yu, "An introduction to convex optimization for communications and signal processing," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1426–1438, Aug. 2006.

[86] D. Palomar and Y. Eldar, *Convex Optimization in Signal Processing and Communications.* Cambridge, UK: Cambridge University Press, 2010.

[87] Y. Ye, *Interior Point Algorithms. Theory and Analysis.* John Wiley & Sons, 1997.

[88] J. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods and Software*, vol. 11-12, pp. 625–653, 1999, special issue on Interior Point Methods (CD supplement with software). [Online]. Available: citeseer.ist.psu.edu/sturm99using.html

[89] J. Lofberg, "Yalmip: A toolbox for modelling and optimizationin MATLAB," in *Proc. IEEE Int. Symp. on Comp. Aided Control Sys. Design*, Taipei, Sept. 2004, pp. 284–289.

[90] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," *Optimization Methods and Software*, Apr. 2012, http://stanford.edu/~boyd/cvx.

[91] H. Hindi, "A tutorial on convex optimization," in *Proc. American Control Conference*, Jul. 2004, pp. 3252–3265.

[92] ——, "A tutorial on convex optimization ii: duality and interior point methods," in *Proc. American Control Conference*, Jun. 2006.

[93] R. A. Horn and C. R. Johnson, *Matrix Analysis.* New York: Cambridge University Press, 1985.

[94] O. Gungor, J. Tan, C. Koksal, H. El-Gamal, and N. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory,*, vol. 59, no. 9, pp. 5379–5397, Sept., 2013.

[95] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, Oct. 2014.

[96] I. Bechar, "A Bernstein-type inequality for stochastic processes of quadratic forms of gaussian variables," *Available[online]: http://arxiv.org/abs/0909.3595.*, 2009.

[97] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory.* Philadelphia PA: SIAM Studies in Applied Mathematics, 1994.

[98] A. Pascual-Iserte, D. Palomar, A. Perez-Neira, and M. Lagunas, "A robust maximin approach for MIMO communications with imperfect channel state information based on convex optimization," *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 346–360, Jan. 2006.

[99] W. Ai and S. Zhang, "Strong duality for the CDT problem: A necessary and sufficient condition," *SIAM J. Optim.*, vol. 19, pp. 1735–1756, Feb. 2009.

[100] Y. Eldar, A. Ben-Tal, and A. Nemirovski, "Robust mean-squared error estimation in the presence of model uncertainties," *IEEE Trans. Signal Process.*, vol. 53, no. 1, pp. 168–181, Jan. 2005.

[101] M. Khandaker and K. Wong, "Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 40–54, Jan. 2015.

[102] A. Mukherjee and A. Swindlehurst, “Detecting passive eavesdroppers in the MIMO wiretap channel,” in *Proc. IEEE ICASSP, Tokyo, Japan*, Mar. 2012, pp. 2809–2812.

[103] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, “Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks,” in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 3145–3150.

[104] Z. Ding, C. Zhong, D. Ng, M. Peng, H. Suraweera, R. Schober, and H. Poor, “Application of smart antenna technologies in simultaneous wireless information and power transfer,” *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 86–93, Apr. 2015.

[105] L. Tran, M. Hanif, A. Tolli, and M. Juntti, “Fast converging algorithm for weighted sum rate maximization in multicell MISO downlink,” *IEEE, Signal Process. Lett.*, vol. 19, no. 12, pp. 872–875, Dec. 2012.

[106] L.-N. Tran, M. Hanif, and M. Juntti, “A conic quadratic programming approach to physical layer multicasting for large-scale antenna arrays,” *IEEE, Signal Process. Lett.*, vol. 21, no. 1, pp. 114–117, Jan. 2014.

[107] W.-C. Li, T.-H. Chang, C. Lin, and C.-Y. Chi, “Coordinated beamforming for multiuser MISO interference channel under rate outage constraints,” *IEEE Trans., Signal Process.*, vol. 61, no. 5, pp. 1087–1103, Mar. 2013.

[108] E. Karipidis, N. Sidiropoulos, and Z.-Q. Luo, “Far-field multicast beamforming for uniform linear antenna arrays,” *IEEE Trans. Signal Process.*, vol. 55, no. 10, pp. 4916–4927, Oct 2007.

[109] A. Ben-Tal, L. El Ghaoui, and A. Nemirovski, *Robust Optimization*, ser. Princeton, NJ, USA: Princeton University Press, 2009.