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\textsuperscript{3}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 ix

List of Tables xi

Nomenclature xii

1 Introduction 1

1.1 Wireless Security Motivations 2

1.2 Literature Review 4

1.3 Main Contributions and Thesis Outline 8

1.3.1 Main Contributions 8

1.3.2 Thesis Outline 9

1.4 Publications Lists 10

1.4.1 Journal Publications 10

1.4.2 Conference Publications 10

2 Preliminaries 12

2.1 Multiple-Antenna Wireless Communications 12

2.1.1 MIMO Channel and Signal Model 13

2.2 Capacity Limits of of Wireless System 14

2.2.1 Mutual Information and Shannon Capacity 14

2.2.2 Mathematical Definition of Capacity 14

2.3 Multi-Antenna Beamforming Techniques 15

2.3.1 MIMO Beamforming Design 15

2.4 Information-theoretical Security 18

2.4.1 Information-Theoretical Security 18

2.4.2 Gaussian Wiretap Channel 22

2.5 Secure Communications for Multiple-Antenna Transceiver 23
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Transmit Optimization for MIMO Wiretap Channel</td>
<td>23</td>
</tr>
<tr>
<td>2.5.2 Robust Secrecy Rate Optimization</td>
<td>25</td>
</tr>
<tr>
<td><strong>3 Convex Optimization Theory</strong></td>
<td>27</td>
</tr>
<tr>
<td>3.1 Convex Set</td>
<td>28</td>
</tr>
<tr>
<td>3.2 Convex Cone</td>
<td>28</td>
</tr>
<tr>
<td>3.3 Convex Function</td>
<td>28</td>
</tr>
<tr>
<td>3.4 Convex Optimization Problems</td>
<td>29</td>
</tr>
<tr>
<td>3.4.1 Linear Programming</td>
<td>30</td>
</tr>
<tr>
<td>3.4.2 Quadratic Programming</td>
<td>30</td>
</tr>
<tr>
<td>3.4.3 Quadratically Constrained Quadratic Programming</td>
<td>30</td>
</tr>
<tr>
<td>3.4.4 Second-Order Cone Programming</td>
<td>31</td>
</tr>
<tr>
<td>3.4.5 Semidefinite Programming</td>
<td>31</td>
</tr>
<tr>
<td>3.4.6 Duality and KKT Conditions</td>
<td>32</td>
</tr>
<tr>
<td>3.5 Summary</td>
<td>34</td>
</tr>
<tr>
<td><strong>4 Transmit Optimization for MISO Secure Communications</strong></td>
<td>35</td>
</tr>
<tr>
<td>4.1 System Model</td>
<td>36</td>
</tr>
<tr>
<td>4.2 Power Minimization</td>
<td>36</td>
</tr>
<tr>
<td>4.3 Robust Outage Secrecy Rate Optimization</td>
<td>38</td>
</tr>
<tr>
<td>4.3.1 Problem Formulation</td>
<td>38</td>
</tr>
<tr>
<td>4.3.2 Channel Uncertainty Models</td>
<td>39</td>
</tr>
<tr>
<td>4.3.3 Robust Power Minimization Based on Partial Channel Uncertainty</td>
<td>40</td>
</tr>
<tr>
<td>4.3.3.1 Bernstein-Type Inequality</td>
<td>41</td>
</tr>
<tr>
<td>4.3.3.2 S-Procedure</td>
<td>43</td>
</tr>
<tr>
<td>4.3.4 Robust Power Minimization Based on Full Channel Uncertainty</td>
<td>44</td>
</tr>
<tr>
<td>4.3.4.1 Bernstein-Type Inequality</td>
<td>45</td>
</tr>
<tr>
<td>4.3.4.2 S-Procedure</td>
<td>47</td>
</tr>
<tr>
<td>4.4 Simulation Results</td>
<td>48</td>
</tr>
<tr>
<td>4.4.1 Power Minimization</td>
<td>49</td>
</tr>
<tr>
<td>4.4.2 Robust Outage Secrecy Rate Optimization with Partial Channel Un-</td>
<td>49</td>
</tr>
</tbody>
</table>
4.4.3 Robust Outage Secrecy Rate Optimization with Full Channel Uncertainties .................................................. 51

4.5 Summary ....................................................................................................................................................... 53

4.6 Appendix ....................................................................................................................................................... 54
  4.6.1 Proof of Theorem 4.1 .............................................................................................................................. 54
  4.6.2 Proof of Proposition 4.1 .......................................................................................................................... 55
  4.6.3 Proof of Theorem 4.2 .................................................................................................................................. 56
  4.6.4 Proof of Theorem 4.3 .................................................................................................................................. 59
  4.6.5 Proof of Theorem 4.4 .................................................................................................................................. 61
  4.6.6 Proof of Theorem 4.5 .................................................................................................................................. 63

5 Transmit Optimization for MIMO Secure Communications with Cooperative Jammer 67

5.1 System Model .................................................................................................................................................. 68

5.2 Secrecy Rate Optimizations .................................................................................................................................. 70
  5.2.1 Null Space Method ...................................................................................................................................... 71
  5.2.2 Maximizing Cooperative Jammer Rate ......................................................................................................... 71
  5.2.3 Power Minimization with Secrecy Rate Constraint ...................................................................................... 72
  5.2.4 Secrecy Rate Maximization with Transmit Power Constraint .......................................................................... 74

5.3 Robust Secrecy Rate Optimization ..................................................................................................................... 75
  5.3.1 Channel Uncertainty .................................................................................................................................... 75
  5.3.2 Robust Power Minimization ........................................................................................................................ 76

5.4 Secrecy Rate Optimization Based on Game Theory ............................................................................................ 79
  5.4.1 Stackelberg Game ......................................................................................................................................... 80
  5.4.2 Stackelberg Equilibrium ............................................................................................................................... 81
  5.4.3 Solution of Proposed Stackelberg Game ....................................................................................................... 82

5.5 Simulation Results ................................................................................................................................................ 83
  5.5.1 Secrecy Rate Optimizations with Perfect CSI ............................................................................................. 86
  5.5.2 Robust Secrecy Rate Optimizations ............................................................................................................. 87
  5.5.3 Secrecy Rate Optimization based on Game Theory ......................................................................................... 87

5.6 Summary ............................................................................................................................................................ 89

5.7 Appendix .......................................................................................................................................................... 91
  5.7.1 Proof of Problem (5.19) ............................................................................................................................... 91
  5.7.2 Proof of Constraint (5.21) ............................................................................................................................. 92
5.7.3 Proof of Lemma 5.1 ........................................... 94
5.7.4 Proof of Lemma 5.2 ........................................... 95

6 Transmit Optimization for Secure MISO SWIPT System 98

6.1 System Model ................................................. 99
6.2 Transmit Optimization for Secrecy Rate Maximization .......... 100
  6.2.1 Power Minimization ..................................... 101
  6.2.2 Robust Power Minimization ............................... 102
    6.2.2.1 Channel Uncertainty ............................... 103
    6.2.2.2 Robust Power Minimization ....................... 103
6.3 AN-aided Transmit Optimization for Secrecy Rate Maximization ... 105
  6.3.1 Problem Formulation .................................. 105
  6.3.2 Secrecy Rate Maximization ............................. 106
    6.3.2.1 Two-Level Optimization ......................... 106
    6.3.2.2 Optimality Conditions for SDP Relaxation ....... 108
    6.3.2.3 Successive Convex Approximation ............. 109
  6.3.3 Robust Secrecy Rate Maximization ........................ 111
    6.3.3.1 Two-Level Optimization ......................... 112
    6.3.3.2 Successive Convex Approximation ............. 114
6.4 Simulation Results .......................................... 116
6.5 Summary .................................................. 119
6.6 Appendix .................................................. 121
  6.6.1 Proof of Lemma 6.1 .................................. 121
  6.6.2 Proof of Lemma 6.2 .................................. 122
  6.6.3 Proof of Theorem 6.1 ................................ 124
  6.6.4 Proof of Theorem 6.2 ................................ 125

7 Conclusions and Future Work 128

7.1 Conclusions .............................................. 128
7.2 Future Work ............................................... 129

References 132
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Layer protocol</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>Encryption diagram</td>
<td>3</td>
</tr>
<tr>
<td>2.1</td>
<td>MIMO channel</td>
<td>13</td>
</tr>
<tr>
<td>2.2</td>
<td>Transmit precoding and receiver shaping</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Parallel decomposition of the MIMO channel</td>
<td>17</td>
</tr>
<tr>
<td>2.4</td>
<td>Water-filling power allocations</td>
<td>18</td>
</tr>
<tr>
<td>2.5</td>
<td>Shannon secrecy model</td>
<td>19</td>
</tr>
<tr>
<td>2.6</td>
<td>Simple wiretap channel</td>
<td>20</td>
</tr>
<tr>
<td>2.7</td>
<td>Broadcast wiretap channel with confidential message</td>
<td>21</td>
</tr>
<tr>
<td>2.8</td>
<td>Gaussian wiretap channel</td>
<td>22</td>
</tr>
<tr>
<td>4.1</td>
<td>The CDF of secrecy rate with partial channel uncertainties</td>
<td>50</td>
</tr>
<tr>
<td>4.2</td>
<td>The secrecy rate with different transmit powers based on partial channel uncertainties</td>
<td>50</td>
</tr>
<tr>
<td>4.3</td>
<td>The secrecy rate with different error variances based on partial channel uncertainties</td>
<td>51</td>
</tr>
<tr>
<td>4.4</td>
<td>The CDF of secrecy rate with full channel uncertainties</td>
<td>52</td>
</tr>
<tr>
<td>4.5</td>
<td>The secrecy rate with different transmit powers based on full channel uncertainties</td>
<td>52</td>
</tr>
<tr>
<td>4.6</td>
<td>The secrecy rate with different error variances based on full channel uncertainties</td>
<td>53</td>
</tr>
<tr>
<td>4.7</td>
<td>The secrecy rate with different numbers of the eavesdropper based on full channel uncertainties</td>
<td>54</td>
</tr>
<tr>
<td>5.1</td>
<td>A MIMO secrecy channel with a CJ in the presence of a multi-antenna eavesdropper</td>
<td>69</td>
</tr>
<tr>
<td>5.2</td>
<td>Convergence of the transmit power for power minimization</td>
<td>84</td>
</tr>
</tbody>
</table>
5.3 Convergence of the secrecy rate for power minimization. ........ 84
5.4 Convergence of the secrecy rate for secrecy rate maximization. ... 85
5.5 The transmit power with different target secrecy rates. ............ 85
5.6 The secrecy rate with different transmit powers. .................. 86
5.7 Achieved secrecy rate versus transmit power. ..................... 88
5.8 Achieved secrecy rate versus error bound. ......................... 88
5.9 Revenue function of the legitimate transmitter. .................... 89
5.10 Revenue function of the private CJ. .............................. 90
5.11 Optimal revenue function of the legitimate transmitter. ......... 90
6.1 Achieved secrecy rate with different transmit powers. ............ 117
6.2 AN assisted achieved secrecy rate with different transmit powers. . 117
6.3 Achieved secrecy rate with target harvested power. ............... 118
6.4 The proportion of AN power consumption versus transmit power. . 119
6.5 Achieved secrecy rate versus distance between the transmitter and
the legitimate user. .................................................. 120
6.6 Harvested power versus distance between the transmitter and the
energy receivers. ..................................................... 120
List of Tables

4.1 The transmit power for three schemes. 49

5.1 Cooperative jammer rate maximization algorithm 72
5.2 Power minimization algorithm 74
5.3 Alternative optimization algorithm 77
5.4 The comparison of achieved secrecy rates of robust and non-robust power minimization scheme with target rate $\bar{R}_s = 1$ bps/Hz. 87
5.5 The comparison of achieved secrecy rates of robust and non-robust secrecy rate maximization scheme. 87

6.1 Bisection methods 101
6.2 SCA algorithm for the robust secrecy rate maximization problem (6.27).111
Nomenclature

Symbols

(·)*  Complex Conjugate

(·)⁻¹  Inverse

(·)ᴴ  Hermitian Transpose

(·)ᵀ  Transpose

[x]⁺  max{x, 0}

ℍ{·}  Imaginary Part

λ_{max}(·)  Maximum Eigenvalue

𝔼{·}  Statistical Expectation

A ≥ 0  A is a Positive Semidefinite Matrix

I  Identity Matrix

ℒ(·)  Lagrange Dual Function

| A |  Determinant of A

⊗  Kronecker Products

∥ · ∥₆  Frobenius Norm

∥ · ∥₂  Euclidean Norm

ℜ{·}  Real Part

Tr(·)  Trace Operator

Vec(A)  Vectorization of 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
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>LHS</td>
<td>Left Hand Side</td>
</tr>
<tr>
<td>LMI</td>
<td>Linear Matrix Inequality</td>
</tr>
<tr>
<td>LP</td>
<td>Linear Programming</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple-input Multiple-output</td>
</tr>
<tr>
<td>NOMA</td>
<td>Non-Orthogonal Multiple Access</td>
</tr>
<tr>
<td>OFDMA</td>
<td>Orthogonal Frequency-Division Multiple Access</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Density Function</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>PSD</td>
<td>Positive Semidefinite</td>
</tr>
<tr>
<td>QCQP</td>
<td>Quadratically Constrained Quadratic Programming</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>QP</td>
<td>Quadratic Programming</td>
</tr>
<tr>
<td>RF</td>
<td>Radio-Frequency</td>
</tr>
<tr>
<td>RHS</td>
<td>Right Hand Side</td>
</tr>
<tr>
<td>SCA</td>
<td>Successive Convex Approximation</td>
</tr>
<tr>
<td>SDP</td>
<td>Semidefinite Programming</td>
</tr>
<tr>
<td>SE</td>
<td>Spectral Efficiency</td>
</tr>
<tr>
<td>SEE</td>
<td>Secure Energy Efficiency</td>
</tr>
<tr>
<td>SI</td>
<td>Self-Interference</td>
</tr>
<tr>
<td>SISO</td>
<td>Single-input Single-output</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-Noise Ratio</td>
</tr>
<tr>
<td>SOC</td>
<td>Second-Order Cone</td>
</tr>
<tr>
<td>SOCP</td>
<td>Second-Order Cone Programming</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>SSE</td>
<td>Secure Spectral Efficiency</td>
</tr>
<tr>
<td>SVD</td>
<td>Singular Value Decomposition</td>
</tr>
<tr>
<td>SWIPT</td>
<td>Simultaneous Wireless Information Power Transfer</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
</tbody>
</table>
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.
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
1.1 Wireless Security Motivations

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 de-
sired 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
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 ap-
proximation 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


1.4.2 Conference Publications


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].
2.1 Multiple-Antenna Wireless Communications

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

$$H = \begin{bmatrix} H_{1,1} & \cdots & H_{1,M_T} \\ \vdots & \ddots & \vdots \\ H_{M_R,1} & \cdots & H_{M_R,M_T} \end{bmatrix}, \quad (2.1)$$

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

$$y = \sqrt{P} H x + n, \quad (2.2)$$

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

$$I(X;Y) = \int_{S_x, S_y} f(x,y) \log \left( \frac{f(x,y)}{f(x)f(y)} \right) dx dy,$$  \hspace{1cm} (2.3)

where the integral of $S_x, S_y$ denotes the random variables $X$ and $Y$, respectively, and $f(x), f(x), \text{ and } f(x,y)$ 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

$$C = \max_{f(x)} I(X;Y) = \int_{S_x, S_y} f(x, y) \log \left( \frac{f(x, y)}{f(x)f(y)} \right).$$  \hfill (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 $\gamma$ based on the assumption that $f(x)$ follows the Gaussian distribution as

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

\section{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.

\subsection{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

$$y = Hx + n,$$  \hfill (2.6)

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

Figure 2.2: Transmit precoding and receiver shaping

\[ x = V\bar{x}, \quad y = Hx + n \quad \text{and} \quad \bar{y} = U^H y \]

\[ \bar{y} = U^H (Hx + n) = U^H U \Sigma \Sigma^H V \bar{x} + U^H n = \Sigma \bar{x} + \bar{n}, \]
2.3 Multi-Antenna Beamforming Techniques

Figure 2.3: Parallel decomposition of the MIMO channel

associated SISO channel. Each channel performance depends on $\delta_i$. 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.

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

where $P$ and $p_i$ are the total transmit power and power allocated to the $i$-th independent channel, respectively. $B$, $\delta_i$ and $\sigma^2$ 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:

$$\alpha_i \geq 0, \hspace{1em} (2.12a)$$

$$\alpha_i p_i = 0, \hspace{1em} (2.12b)$$

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

where $\alpha_i$ and $\beta$ are the dual multipliers of $i$-th individual power and total power constraints, respectively. From complementary slackness as in (2.12b) and (2.12c),
the optimal power allocation is written in terms of closed-form solution as

$$p^*_i = \begin{cases} 
\left[ \frac{B}{\beta} - \frac{\sigma^2}{\delta^2} \right]^+, & \alpha_i = 0, \\
0, & \alpha_i \neq 0.
\end{cases} \quad (2.13)$$

In addition, the optimal value of $\beta$ is given by (2.14),

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

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 $\beta^*$ is the optimal value of $\beta$, 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-
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 $X$, two discrete output alphabets $Y$ and $Z$, and a probability transition function $p_{YZ|X}(y, z|x)$. It is assumed that this channel is memoryless,
thus, the transition probability of a sequence of $n$ symbols is expressed as

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

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** $S_0 = \{1, 2, ..., 2^{nR_0}\}$ and $S_M = \{1, 2, ..., 2^{nR_M}\}$.

- **An encoding function** $f_n : S_0 \times S_M \rightarrow X^n$, which maps each message pair $(s_0, s_M) \in S_0 \times S_M$ to a codeword $x^n \in X^n$.

- **Two decoding functions** $g_n : Y^n \rightarrow S_0 \times S_M$ and $h_n : Z^n \rightarrow S_0$, which map an observation $y^n$ to a message pair $(\hat{s}_0, \hat{s}_M)$ and an observation $z^n$ to a message $\tilde{s}_0$.

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

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

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

$$P[g_n(Y^n) \neq (S_0, S_M) \text{ or } h_n(Z^n \neq S_0)] < \epsilon,$$

$$\frac{1}{n} H(S_M|Z^n) \geq R_E - \epsilon.$$ 

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:

$$C = \bigcup_{U \rightarrow V \rightarrow X \rightarrow YZ} \left\{ \begin{array}{l}
0 \leq R_E \leq R_M, \\
R_E \leq I(V;Y|U) - I(V;Z|U), \\
R_0 + R_M \leq I(V;Y|U) + \min(I(U;Y), I(U;Z)), \\
0 \leq R_0 \leq \min(I(U;Y), I(U;Z)).
\end{array} \right. \tag{2.17}$$

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,
2.4 Information-theoretical Security

The secrecy capacity can be written as

\[ C = \max_{V \rightarrow X \rightarrow YZ} [I(V;Y) - I(V;Z)]. \] (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 \( \sigma_S^2 \) and \( \sigma_E^2 \), respectively. In addition, assuming that the messages transmitted over the channels are subject to the average transmit power constraint

\[ \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}(X_i) \leq P. \] (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 \(H_s \in \mathbb{C}^{N_T \times N_R}\) and \(H_e \in \mathbb{C}^{N_T \times N_E}\), respectively. The maximum transmit power available at the legitimate transmitter is denoted by \(P\). The received signal at the legitimate user is written as
\[
y_s = H_s^H x + n_s, \quad y_e = H_e^H x + n_e, \tag{2.21}
\]
where \(x \in \mathbb{C}^{N_T \times 1}\) denotes the desired signal intended to the legitimate receiver. The transmit covariance matrix is defined as \(Q_s = \mathbb{E}\{xx^H\}\). The noises, \(n_s\) and \(n_e\), are
set to be zero-mean circularly symmetric Gaussian random variables with covariances $\sigma_s^2 I \in \mathbb{C}^{NR \times NR}$ and $\sigma_e^2 I \in \mathbb{C}^{NE \times NE}$, respectively. The achievable transmission rate to the legitimate user and the eavesdropper can be expressed, respectively, as [7]

$$R_s = \log \left| I + \frac{1}{\sigma_s^2} H_s^H Q_s H_s \right|, \quad R_e = \log \left| I + \frac{1}{\sigma_e^2} H_e^H Q_e H_e \right|$$

(2.22)

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

$$R = [R_s - R_e]^+, \quad (2.23)$$

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:

$$\min_{Q_s \succeq 0} \text{Tr}(Q_s), \quad s.t. \ R \geq \bar{R}. \quad (2.24)$$

2. Secrecy rate maximization:

$$\max_{Q_s \succeq 0} R, \quad s.t. \ \text{Tr}(Q_s) \leq P. \quad (2.25)$$

Both above problems are not convex in terms of transmit covariance matrix $Q_s$, 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 $\tilde{Q}_s$ as follows:

$$R \simeq \log \left| I + \frac{1}{\sigma_s^2} H_s^H Q_s H_s \right| - \log \left| I + \frac{1}{\sigma_e^2} H_e^H \tilde{Q}_e H_e \right| - \text{Tr} \left[ \frac{1}{\sigma_s^2} \left( I + \frac{1}{\sigma_e^2} H_e^H \tilde{Q}_e H_e \right)^{-1} H_e^H Q_s H_e \right]$$

$$+ \text{Tr} \left[ \frac{1}{\sigma_e^2} \left( I + \frac{1}{\sigma_e^2} H_e^H \tilde{Q}_e H_e \right)^{-1} H_e^H \tilde{Q}_e H_e \right] \triangleq \tilde{R}. \quad (2.26)$$
It can be easily observed that $\tilde{R}$ is a concave function in terms of $Q_s$. Based on this approximation, the power minimization problem in (2.24) is modified as

$$\min_{Q_s \succeq 0} \text{Tr}(Q_s), \quad s.t. \quad \tilde{R} \geq \bar{R}. \quad (2.27)$$

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

$$\max_{\lambda \geq 0} \min_{Q_s \succeq 0} \left[ \text{Tr}(Q_s) + \lambda (\bar{R} - \tilde{R}) \right], \quad (2.28)$$

where $\lambda$ 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 Slater’s 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, \textit{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 \textit{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 $S$ is convex if it can be written as

$$\theta y_1 + (1 - \theta)y_2 \in S, \quad \forall \theta \in [0, 1], \text{ and } y_1, y_2 \in S.$$ (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 $S$ is defined as a cone, or nonnegative homogeneous, if for every $y \in S$ and $\alpha \geq 0$, $\alpha y \in S$ holds. A set $S$ is a convex cone if it is convex and a cone, and the following inequality holds for any $y_1, y_2 \in S$ and $\theta_1, \theta_2 \geq 0$

$$\theta_1 y_1 + \theta_2 y_2 \in S.$$ (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): $S = \{(y, x) | \|x\| \leq y\}$.
3. Positive semidefinite cone: $S = \{Y | Y \text{ is symmetric and } X \succeq 0\}$.

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:

$$f(\theta x_1 + (1 - \theta)x_2) \leq \theta f(x_1) + (1 - \theta)f(x_2), \quad \forall \theta \in [0, 1].$$ (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 \( \text{dom} f(x) \). 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

\[
f(y) \geq f(x) + \nabla f(x) (y - x)
\]

(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),

\[
\nabla^2 f(x) \succeq 0, \quad \forall \ x \in \mathbb{R}^n.
\]

(3.5)

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

### 3.4 Convex Optimization Problems

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

\[
\begin{align*}
\min \quad & f_0(x), \\
\text{s.t.} \quad & f_i(x) \leq 0, \ i = 1, \ldots, m, \\
& h_i(x) = 0, \ i = 1, \ldots, p,
\end{align*}
\]

(3.6)

where \( x \in \mathbb{R}^n \) is the optimization variable, the functions \( f_0, \ldots, f_m : \mathbb{R}^n \to \mathbb{R} \) are convex functions, and the functions \( h_1, \ldots, h_p \) are linear functions. In addition, \( f_i(x) \leq 0, \ i = 1, \ldots, m \), are defined as the inequality constraints, and \( h_i(x) = 0, \ i = 1, \ldots, p \), 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

\[
\mathcal{D} = \bigcap_{i=0}^{m} \text{dom} f_i \cap \bigcap_{i=1}^{p} \text{dom} h_i
\]

(3.7)

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

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

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

$$\min_x c^T x + d, \quad s.t. \quad Gx \preceq h, \quad Ax = b, \quad (3.9)$$

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

### 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:

$$\min_x x^T P x + q^T x + r, \quad s.t. \quad Gx \preceq h, \quad Ax = b, \quad (3.10)$$

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

\[
\begin{align*}
\min_x & \quad x^T P_0 x + q_0^T x + r_0, \\
\text{s.t.} & \quad x^T P_i x + q_i^T x + r_i \leq 0, \quad i = 1, \ldots, m, \\
& \quad Ax = b,
\end{align*}
\]

(3.11)

where \( P_i \in S_{++}^n, i = 0, \ldots, m \). In a QCQP, a quadratic convex function is minimized over a feasible region that is the intersection of ellipsoids with \( P_i > 0 \). It is easily observed that LP is also a special case of QCQP with \( P_i = 0 \).

### 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

\[
\begin{align*}
\min_x & \quad f^T x, \\
\text{s.t.} & \quad \|A_i x + b_i\|_2 \leq c_i^T x + d_i, \quad i = 1, \ldots, m, \\
& \quad Fx = g,
\end{align*}
\]

(3.12)

where \( x \in \mathbb{R}^n \) is the optimization variable, \( A_i \in \mathbb{R}^{n_i \times n} \), and \( F \in \mathbb{R}^{p \times n} \). The constraint \( \|A x + b\|_2 \leq c^T x + d \), where \( A \in \mathbb{R}^{k \times n} \), is called as second-order cone constraint, since it is the same as requiring the affine function \( (A x + b, c^T x + d) \) 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 \( A_i = 0, i = 1, \ldots, m \), 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

\[
\begin{align*}
\min_x & \quad c^T x, \\
\text{s.t.} & \quad x_1 F_1 + x_2 F_2 + \ldots + x_n F_n + G \preceq 0, \\
& \quad Ax = b,
\end{align*}
\]

(3.13)
where $G, F_1, ..., F_n \in S^k$, and $A \in \mathbb{R}^{p \times n}$. The inequality here is called linear matrix inequality (LMI). If the matrices $G, F_1, ..., F_n$ 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

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

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 $\lambda$ and $\nu$ 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 $\lambda \in \mathbb{R}^m$, $\nu \in \mathbb{R}^p$:

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

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 $(\lambda, \nu)$. The dual function $g(\lambda, \nu)$ yields a lower bound on the optimal value $f_0(x^*)$ to (3.6). For any $\lambda \succeq 0$ and any $\nu$,

$$
g(\lambda, \nu) \leq f_0(x^*), \quad (3.16)
$$
For any feasible set \((x, \lambda, \nu)\), the following inequality holds

\[
f_0(x) \geq f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x)
\geq \inf_{y \in D} \left( f_0(y) + \sum_{i=1}^{m} \lambda_i f_i(y) + \sum_{i=1}^{p} \nu_i h_i(y) \right)
\geq g(\lambda, \nu),
\] (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:

\[
\max_{\lambda, \nu} g(\lambda, \nu),
\quad \text{s.t.} \quad \lambda \succeq 0,
\] (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: \(f_i(x) \leq 0, i = 1, \ldots, m; h_i(x) = 0, i = 1, \ldots, p\).

2. Dual constraints: \(\lambda \succeq 0\).

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

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

\[
\nabla f_0(x) + \sum_{i=1}^{m} \lambda_i \nabla f_i(x) + \sum_{i=1}^{p} \nu_i \nabla h_i(x) = 0.
\] (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 non-convex 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

\[
y_s = \mathbf{h}_s^H \mathbf{x} + n_s, \quad y_{e,k} = \mathbf{H}_{e,k}^H \mathbf{x} + n_{e,k}, \quad k = 1, \ldots, K,
\]

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

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

\[
\min_{\mathbf{Q}_s \succeq 0} \text{Tr} (\mathbf{Q}_s), \quad s.t. \min_k R_{s,k} \geq R, \quad \forall k, \tag{4.2}
\]

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]:

\[
|\mathbf{I} + \mathbf{A}| \geq 1 + \text{Tr}(\mathbf{A}), \tag{4.3}
\]
where the equality holds if and only if \( \text{rank}(A) = 1 \). If \( Q_s \) is rank-one, the relaxed problem is equivalent to the original problem (4.2), which can be written as

\[
\min_{Q_s \succeq 0} \text{Tr}(Q_s) \\
\text{s.t. } 1 + \frac{1}{\sigma_s^2} h_s^H Q_s h_s \geq 2^R \left[ 1 + \text{Tr} \left( \frac{1}{\sigma_{e,k}^2} H_{e,k}^H Q_s H_{e,k} \right) \right], \quad \forall k, \\
\text{rank}(Q_s) \leq 1. 
\tag{4.4}
\]

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), \( Q_s \) can be decomposed as \( Q_s = w w^H \), thus, the problem (4.4) can be formulated into a SOCP as follows:

\[
\min_w \|w\|_2 \\
\text{s.t.} \\
\begin{bmatrix}
\frac{1}{\sigma_s^2} h_s^H w \\
\frac{2^R}{\sigma_{e,k}} H_{e,k}^H w \\
(2^R - 1)^{\frac{1}{2}}
\end{bmatrix} \succeq K_0, \quad \forall k. 
\tag{4.5}
\]

**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

\[
w^* = \sqrt{p^*} v^*, \quad v^* = \frac{v_1}{\|v_1\|_2}, \quad p^* = \lambda^* (2^R - 1), \quad \lambda^* = \frac{1}{\lambda_{\text{max}} \left( \frac{1}{\sigma_s^2} h_s h_s^H - \frac{2^R}{\sigma_e^2} H_e H_e^H \right)}, 
\tag{4.6}
\]

where \( v_1 = v_{\text{max}} \left( \frac{1}{\sigma_s^2} h_s h_s^H - \frac{2^R}{\sigma_e^2} H_e H_e^H \right) \).

**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 modeled 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

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

and

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

The problems (4.7) can be reformulated as

\[
\min_{\mathbf{Q}_s \succeq 0} \text{Tr}(\mathbf{Q}_s), \quad \text{s.t.} \quad \Pr\left\{ \log(1 + \frac{1}{\sigma_s^2} \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log \left| I + \frac{1}{\sigma_{e,k}^2} \mathbf{H}_{e,k}^H \mathbf{Q}_s \mathbf{H}_{e,k} \right| \geq R \right\} \geq 1 - \rho, \quad \forall k, \tag{4.8a}
\]
4.3 Robust Outage Secrecy Rate Optimization

and

$$\max_{Q_s \geq 0} R, \quad s.t. \quad \Tr(Q_s) \leq P,$$

$$\Pr \left\{ \log(1 + \frac{1}{\sigma^2_s} h_s^H Q_s h_s) - \log \left| I + \frac{1}{\sigma^2_{e,k}} H_{e,k}^H Q_s H_{e,k} \right| \geq R \right\} \geq 1 - \rho, \quad \forall k, \quad (4.8b)$$

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 $\rho$ % (i.e., 100 $\rho$ %-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., $\Tr(Q_s)$). 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
4.3 Robust Outage Secrecy Rate Optimization

the eavesdropper. Accordingly, the channel uncertainty model is given

\[ \mathbf{H}_{e,k} = \bar{\mathbf{H}}_{e,k} + \mathbf{E}_{e,k}, \quad \forall k, \]

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 \( \text{vec}(\mathbf{E}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k}) \) are the statistical information of channel error at the \( k \)-th eavesdropper, \( \mathbf{R}_{e,k} \) is a positive semidefinite (PSD) matrix (\( \succeq 0 \)).

- **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

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

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 \( \mathbf{e}_s \sim \mathcal{CN}(0, \mathbf{R}_s) \), \( \text{vec}(\mathbf{E}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k}) \) 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., \( \mathbf{R}_s \succeq 0, \mathbf{R}_{e,k} \succeq 0 \)).

### 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

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

\[
\Pr \left\{ \frac{\sigma^2_{e,k}}{2R} \left( 1 + \frac{1}{\sigma^2_s} h^H_s Q_s h_s \right) - \sigma^2_{e,k} \right\} \geq 1 - \rho, \ \forall k. \tag{4.10}
\]

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,

\[
\begin{align*}
\text{Vec}(AXB) &= (B^T \otimes A)\text{Vec}(X), \tag{4.11a} \\
\text{Tr}(ATB) &= \text{Vec}(A)^T \text{Vec}(B), \tag{4.11b} \\
(A \otimes B)^T &= A^T \otimes B^T. \tag{4.11c}
\end{align*}
\]

The constraint (4.10) is written as

\[
\Pr \left\{ e^H_{e,k}(I \otimes Q_s)e_{e,k} + 2\Re \left\{ e^H_{e,k}(I \otimes Q_s)\bar{h}_{e,k} \right\} + \bar{h}^H_{e,k}(I \otimes Q_s)\bar{h}_{e,k} \leq c_k \right\} \geq 1 - \rho, \ \forall k, \tag{4.12}
\]

where \( c_k = \frac{\sigma^2_{e,k}}{2R} \left( 1 + \frac{1}{\sigma^2_s} h^H_s Q_s h_s \right) - \sigma^2_{e,k}, \ \bar{h}_{e,k} = \text{vec}(\bar{H}_{e,k}) \) and \( e_{e,k} = \text{vec}(E_{e,k}) \). Since \( e_{e,k} \sim \mathcal{CN}(0, R_{e,k}) \), the following transformation is given

\[
e_{e,k} = R^\frac{1}{2}_{e,k} v_{e,k}, \tag{4.13}
\]

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

\[
\Pr \left\{ v^H_{e,k} \left[ -R^\frac{1}{2}_{e,k}(I \otimes Q_s)R^\frac{1}{2}_{e,k} \right] v_{e,k} + 2\Re \left( v^H_{e,k}[-R^\frac{1}{2}_{e,k}(I \otimes Q_s)\bar{h}_{e,k}] \right) + [c_k - \bar{h}^H_{e,k}(I \otimes Q_s)\bar{h}_{e,k}] \geq 0 \right\} \geq 1 - \rho, \ \forall k. \tag{4.14}
\]

### 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 \((A, u, c)\), where \(A \in \mathbb{C}^{N \times N}\) is a complex hermitian
4.3 Robust Outage Secrecy Rate Optimization

matrix, \( u \in \mathbb{C}^{N \times 1} \), \( x \sim \mathcal{CN}(0, I_N) \) and \( \rho \in (0, 1] \), the following inequalities hold:

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

\[
\begin{equation}
\begin{cases}
\text{Tr}(A) - \sqrt{-2 \ln(\rho)} w + \ln(\rho) y + c \geq 0 \\
\left\| \begin{bmatrix} \text{vec}(A) \\ \sqrt{2} u \end{bmatrix} \right\| \leq w \\
y I_N + A \succeq 0
\end{cases}
\end{equation}
\]

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

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

\[
\begin{align}
\text{Tr} \left[ R_{e,k}^2 (I \otimes Q_s) R_{e,k}^2 \right] + \sqrt{-2 \ln(\rho)} w_k - \ln(\rho) y_k - \frac{\sigma_s^2}{2 R^2} \text{Tr}[h_s h_s^H Q_s] \\
+ \bar{h}^H_{e,k} (I \otimes Q_s) \bar{h}_{e,k} \leq \sigma_s^2 \left( \frac{1}{2R} - 1 \right),
\end{align}
\]

\[
\left\| \begin{bmatrix} \text{vec}(R_{e,k}^2 (I \otimes Q_s) R_{e,k}^2) \\ \sqrt{2} (R_{e,k}^2 (I \otimes Q_s) \bar{h}_{e,k}) \end{bmatrix} \right\|_2 \leq w_k,
\]

\[
y_k I - R_{e,k}^2 (I \otimes Q_s) R_{e,k}^2 \succeq 0, y_k \geq 0, \forall k.
\]

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

\[
\min_{Q_s} \text{Tr}(Q_s), \quad \text{s.t.} \quad (4.17), \quad Q_s \succeq 0.
\]

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 \( Q_s \) 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 \( Q_s \).

**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. \( \blacksquare \)
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 $S \subseteq \mathbb{C}^{N \times 1}$ with $\Pr\{v \in S\} \geq 1 - \rho$ such that $\forall v \in S, v^H Av + 2\Re\{v^H u\} + c \geq 0$, then

$$\Pr\{v^H Av + 2\Re\{v^H u\} + c \geq 0\} \geq 1 - \rho$$  \hspace{1cm} (4.19)

From Lemma 4.2, given the following deterministic quadratic constraint

$$v_{e,k}^H[- R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) R_{e,k}^{\frac{1}{2}}] v_{e,k} + 2\Re\{v_{e,k}^H[- R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) \bar{h}_{e,k}]\} + (c_k - \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k}) \geq 0, \forall k,$$  \hspace{1cm} (4.20)

such that $v_{e,k}$ belongs to the following set

$$S = \{v_{e,k}|\Pr(v_{e,k}^H v_{e,k} \leq \gamma_{e,k}^2) \geq 1 - \rho\}, \forall k.$$  \hspace{1cm} (4.21)

Since $v_{e,k} \sim \mathcal{CN}(0, I_{N_{E,k}N_T})$, it can be easily shown that $\|v_e\|^2$ 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

$$\begin{cases} v_{e,k}^H[- R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) R_{e,k}^{\frac{1}{2}}] v_{e,k} + 2\Re\{v_{e,k}^H[- R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) \bar{h}_{e,k}]\} \\ + (c_k - \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k}) \geq 0, \forall k, \\ -v_{e,k}^H v_{e,k} + \gamma_{e,k}^2 \geq 0. \end{cases}$$  \hspace{1cm} (4.22)

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

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

$$f_k(x) = x^H A_k x + 2\Re\{b_k^H x\} + c_k,$$  \hspace{1cm} (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 \( f_1(\mathbf{x}) \geq 0 \implies f_2(\mathbf{x}) \geq 0 \) holds if and only if there exists \( \mu \geq 0 \) such that

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

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

\[
\min_{\mathbf{Q}_s, \lambda_k} \text{Tr}(\mathbf{Q}_s) \quad \text{s.t.} \quad \begin{bmatrix}
\lambda_k \mathbf{I} - [\sigma^2_{e,k}(\mathbf{I} \otimes \mathbf{Q}_s)\mathbf{R}^\frac{1}{2}_{e,k}] - \mathbf{R}^\frac{1}{2}_{e,k}(\mathbf{I} \otimes \mathbf{Q}_s)\mathbf{h}_{e,k}
- \mathbf{h}_{e,k}^H(\mathbf{I} \otimes \mathbf{Q}_s)\mathbf{R}^\frac{1}{2}_{e,k}
\end{bmatrix} \succeq 0,
\]

\[
\mathbf{Q}_s \succeq 0, \lambda_k \geq 0, \forall k,
\]

where \( t_k = (\frac{1}{\sigma^2_{e,k}} - 1)\sigma^2_{e,k} + \frac{\sigma^2_{e,k}}{2\sigma^2_{e,k}}\mathbf{h}_s^H\mathbf{Q}_s\mathbf{h}_s - \mathbf{h}_{e,k}^H(\mathbf{I} \otimes \mathbf{Q}_s)\mathbf{h}_{e,k} \). 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

\[
\min_{Q_s \succeq 0} \text{Tr}(Q_s), \quad \text{s.t.} \quad \Pr \left\{ \log \left( 1 + \frac{1}{\sigma_s^2} (\mathbf{h}_s + e_s)^H Q_s (\mathbf{h}_s + e_s) \right) \right. \\
- \log \left| \mathbf{I} + \frac{1}{\sigma_{e,k}^2} (\mathbf{h}_{e,k} + \mathbf{e}_{e,k})^H Q_s (\mathbf{h}_{e,k} + \mathbf{e}_{e,k}) \right| \geq R \left\} \geq 1 - \rho,
\]

\[
e_s \sim \mathcal{CN}(0, \mathbf{R}_s), \quad \text{vec} (\mathbf{e}_{e,k}) \sim \mathcal{CN}(0, \mathbf{R}_{e,k}), \quad \forall k. \tag{4.26}
\]

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

### 4.3.4.1 Bernstein-Type Inequality

In this subsection, the \textit{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

\[
\Pr \left\{ \frac{1}{\sigma_s^2} \mathbf{e}_s^H Q_s \mathbf{e}_s + 2\Re \{ \mathbf{e}_s^H Q_s \mathbf{h}_s \} + \mathbf{h}_s^H Q_s \mathbf{h}_s \right\} - \frac{2^R}{\sigma_{e,k}^2} \mathbf{e}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{e}_{e,k} \\
+ 2\Re \{ \mathbf{e}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{h}_{e,k} \} + \mathbf{h}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{h}_{e,k} \geq 2^R - 1 \left\} \geq 1 - \rho, \quad \forall k. \tag{4.27}
\]

The above constraint is rewritten in terms of matrix form as

\[
\Pr \left\{ \left[ \begin{array}{c} \mathbf{e}_s^H, \mathbf{e}_{e,k}^H \end{array} \right] \left[ \begin{array}{ccc} \frac{1}{\sigma_s^2} Q_s & 0 \\ 0 & -\frac{2^R}{\sigma_{e,k}^2} (\mathbf{I} \otimes \mathbf{Q}_s) \end{array} \right] \left[ \begin{array}{c} \mathbf{e}_s^H, \mathbf{e}_{e,k}^H \end{array} \right]^H \right\} \\
+ 2\Re \left\{ \left[ \begin{array}{c} \mathbf{e}_s^H, \mathbf{e}_{e,k}^H \end{array} \right] \left[ \begin{array}{ccc} \frac{1}{\sigma_s^2} Q_s & 0 \\ 0 & -\frac{2^R}{\sigma_{e,k}^2} (\mathbf{I} \otimes \mathbf{Q}_s) \end{array} \right] \left[ \begin{array}{c} \mathbf{h}_s^H, \mathbf{h}_{e,k}^H \end{array} \right]^H \right\} \\
+ \left[ \mathbf{h}_s^H, \mathbf{h}_{e,k}^H \right] \left[ \begin{array}{ccc} \frac{1}{\sigma_s^2} Q_s & 0 \\ 0 & -\frac{2^R}{\sigma_{e,k}^2} (\mathbf{I} \otimes \mathbf{Q}_s) \end{array} \right] \left[ \begin{array}{c} \mathbf{h}_s^H, \mathbf{h}_{e,k}^H \end{array} \right]^H \geq 2^R - 1 \left\} \geq 1 - \rho, \quad \forall k. \tag{4.28}
\]

In order to handle the above outage probability constraint by the \textit{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

\[
\Pr\left\{ v_k^H A_k v_k + 2\Re\{v_k^H u_k\} + c_k \geq 0 \right\} \geq 1 - \rho, \ \forall k, \tag{4.29}
\]

where

\[
A_k = \begin{bmatrix}
\frac{1}{\sigma_k^2} R_{x,s}^{\frac{1}{2}} R_{s}^{\frac{1}{2}} & 0 \\
0 & -\frac{2R}{\sigma_{e,k}} R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) R_{e,k}^{\frac{1}{2}}
\end{bmatrix},
\]

\[
u_k = \begin{bmatrix}
\frac{1}{\sigma_k^2} R_{x,s}^{\frac{1}{2}} Q_s & 0 \\
0 & -\frac{2R}{\sigma_{e,k}} R_{e,k}^{\frac{1}{2}} (I \otimes Q_s)
\end{bmatrix} [\bar{h}_s^H \bar{h}_{e,k}^H]^H,
\]

\[
c_k = [\bar{h}_s^H \bar{h}_{e,k}^H] \begin{bmatrix}
\frac{1}{\sigma_k^2} Q_s & 0 \\
0 & -\frac{2R}{\sigma_{e,k}} (I \otimes Q_s)
\end{bmatrix} [\bar{h}_s^H \bar{h}_{e,k}^H]^H + 1 - 2R.
\]

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

\[
\begin{align*}
\text{Tr}(A_k) - \sqrt{-2\ln(\rho) w_k + \ln(\rho) y_k} + c_k & \geq 0, \quad \text{(4.30a)} \\
\left\| \begin{bmatrix} \text{vec}(A_k) \end{bmatrix} \right\|_2 & \leq w_k, \quad \text{(4.30b)} \\
y_k I + A_k & \succeq 0, y_k \geq 0, \forall k. \quad \text{(4.30c)}
\end{align*}
\]

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

\[
\begin{array}{ll}
\min_{Q_s \succeq 0} & \text{Tr}(Q_s), \\
\text{s.t.} & (4.30), \forall k.
\end{array} \tag{4.31}
\]

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 $Q_s$. 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

\[
\min_{Q_s \geq 0} \text{Tr}(Q_s)
\]

subject to

\[
\begin{align*}
&\text{Pr}\left\{ \frac{1}{\sigma_s^2} \{ \bar{h}_s^H Q_s \bar{h}_s + 2 \Re \{ \bar{e}_s^H Q_s \bar{e}_s \} + \bar{e}_s^H Q_s e_s \} - \frac{2R}{\sigma_{e,k}^2} \{ \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k} \\
&\quad + 2 \Re \{ e_{e,k} (I \otimes Q_s) \bar{h}_{e,k} \} + e_{e,k}^H (I \otimes Q_s) e_{e,k} \} \geq 2^R - 1 \right\} \geq 1 - \rho, \forall k.
\end{align*}
\]

(4.32)

In order to tackle the outage probability constraint (4.32), \(e_s = R_s^\frac{1}{2} v_s\) and \(e_{e,k} = R_{e,k}^\frac{1}{2} v_{e,k}\) are considered, respectively, where \(v_s \sim \mathbb{C}\mathbb{N}(0, I_{N_T})\) and \(v_{e,k} \sim \mathbb{C}\mathbb{N}(0, I_{N_T N_E,k})\), and thus (4.32) is reformulated as

\[
\min_{Q_s \geq 0} \text{Tr}(Q_s)
\]

subject to

\[
\begin{align*}
&\text{Pr}\left\{ \frac{1}{\sigma_s^2} \{ v_s^H R_s^\frac{1}{2} Q_s R_s^\frac{1}{2} v_s + 2 \Re \{ v_s^H R_s^\frac{1}{2} Q_s \bar{h}_s \} + \bar{h}_s^H Q_s \bar{h}_s \} - \frac{2R}{\sigma_{e,k}^2} [ v_{e,k} R_{e,k}^\frac{1}{2} (I \otimes Q_s) R_{e,k}^\frac{1}{2} v_{e,k} \\
&\quad + 2 \Re \{ v_{e,k} R_{e,k}^\frac{1}{2} (I \otimes Q_s) \bar{h}_{e,k} \} + \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k} \} \geq 2^R - 1 \right\} \geq 1 - \rho, \forall k.
\end{align*}
\]

(4.33)

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

\[
\Rightarrow \mathbb{R}_s = \{ v_s : v_s^H v_s \leq \gamma_s^2 \}, \quad \mathbb{R}_{e,k} = \{ v_{e,k} : v_{e,k}^H v_{e,k} \leq \gamma_{e,k}^2 \}.
\]

(4.34)

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

\[
\min_{Q_s \geq 0} \text{Tr}(Q_s)
\]

subject to

\[
\begin{align*}
&\frac{1}{\sigma_s^2} \{ v_s^H R_s^\frac{1}{2} Q_s R_s^\frac{1}{2} v_s + 2 \Re \{ v_s^H R_s^\frac{1}{2} Q_s \bar{h}_s \} + \bar{h}_s^H Q_s \bar{h}_s \} - \frac{2R}{\sigma_{e,k}^2} [ v_{e,k} R_{e,k}^\frac{1}{2} (I \otimes Q_s) R_{e,k}^\frac{1}{2} v_{e,k} \\
&\quad + 2 \Re \{ v_{e,k} R_{e,k}^\frac{1}{2} (I \otimes Q_s) \bar{h}_{e,k} \} + \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k} \} \geq 2^R - 1, \\
&v_s^H v_s \leq \gamma_s^2, \quad v_{e,k}^H v_{e,k} \leq \gamma_{e,k}^2, \forall k.
\end{align*}
\]

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

\[
\begin{align*}
\min_{Q_s \succeq 0, t_s, t_{e,k} \geq 0} & \quad \text{Tr}(Q_s), \quad \text{s.t.} \quad t_s - t_{e,k} \geq 2^R - 1, \\
& \frac{1}{\sigma_s^2} (v_s^H R_s^\frac{1}{2} Q_s R_s^\frac{1}{2} v_s + 2R \{v_s^H R_s^\frac{1}{2} Q_s \bar{h}_s\} + \bar{h}_s^H Q_s \bar{h}_s) \geq t_s, \\
& \frac{2^R}{\sigma_{e,k}^2} [v_{e,k}^H R_{e,k}^\frac{1}{2} (I \otimes Q_s) R_{e,k}^\frac{1}{2} v_{e,k} + 2R \{v_{e,k}^H R_{e,k}^\frac{1}{2} (I \otimes Q_s) \bar{h}_{e,k}\} + \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k}] \leq t_{e,k}, \\
& v_s^H v_s \leq \gamma_s^2, \quad v_{e,k}^H v_{e,k} \leq \gamma_{e,k}^2, \quad \forall k.
\end{align*}
\]

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

\[
\begin{align*}
\min_{Q_s \succeq 0} & \quad \text{Tr}(Q_s), \\
\text{s.t.} & \quad t_s - t_{e,k} \geq 2^R - 1, \\
& \begin{bmatrix} \mu_s I + \frac{1}{\sigma_s^2} R_s^\frac{1}{2} Q_s R_s^\frac{1}{2} & \frac{1}{\sigma_s^2} R_s^\frac{1}{2} Q_s \bar{h}_s \\
\frac{1}{\sigma_s^2} \bar{h}_s^H Q_s R_s^\frac{1}{2} & \frac{1}{\sigma_s^2} \bar{h}_s^H Q_s \bar{h}_s - t_s - \mu_s \gamma_s^2 \end{bmatrix} \succeq 0, \\
& \begin{bmatrix} \mu_k I - \frac{2^R}{\sigma_{e,k}^2} R_{e,k}^\frac{1}{2} (I \otimes Q_s) R_{e,k}^\frac{1}{2} & -\frac{2^R}{\sigma_{e,k}^2} R_{e,k}^\frac{1}{2} (I \otimes Q_s) \bar{h}_{e,k} \\
-\frac{2^R}{\sigma_{e,k}^2} \bar{h}_{e,k}^H (I \otimes Q_s) R_{e,k}^\frac{1}{2} & t_{e,k} - \frac{2^R}{\sigma_{e,k}^2} \bar{h}_{e,k}^H (I \otimes Q_s) \bar{h}_{e,k} - \mu_{e,k} \gamma_{e,k}^2 \end{bmatrix} \succeq 0, \\
& \mu_s \geq 0, \quad \mu_{e,k} \geq 0, \quad \forall k.
\end{align*}
\]

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

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

\textbf{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
4.4 Simulation Results

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.

<table>
<thead>
<tr>
<th>Channels</th>
<th>Closed-form</th>
<th>Convex optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SOCP</td>
<td>SDP in [19]</td>
</tr>
<tr>
<td>Channel 1</td>
<td>1.8081</td>
<td>1.8081</td>
</tr>
<tr>
<td>Channel 2</td>
<td>1.4943</td>
<td>1.4943</td>
</tr>
<tr>
<td>Channel 3</td>
<td>1.1292</td>
<td>1.1292</td>
</tr>
<tr>
<td>Channel 4</td>
<td>0.6896</td>
<td>0.6896</td>
</tr>
<tr>
<td>Channel 5</td>
<td>1.6659</td>
<td>1.6659</td>
</tr>
</tbody>
</table>

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 $\varepsilon_{e,k}$ 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 transmit powers, where the achieved secrecy rate increases with the transmit power,
4.4 Simulation Results

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.](image)

(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 $R_s = \varepsilon_s^2 I$, $R_{e,k} = \varepsilon_{e,k}^2 I$, where $\varepsilon_s^2$ 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
4.4 Simulation Results

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 \textit{S-Procedure} scheme has approximately 10% of the achieved secrecy rates that cannot satisfy the outage probability secrecy rate constraint, which is under the pre-defined secrecy rate. Fig. 4.5 shows the achieved secrecy rate with different transmit powers, where the achieved secrecy rate increases with transmit power, and the

Figure 4.5: The secrecy rate with different transmit powers based on full channel uncertainties.
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 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
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 $Q_s = \mathbf{w}\mathbf{w}^H$ as

$$\min_{\mathbf{w}} \|\mathbf{w}\|_2^2$$

subject to

$$1 + \frac{1}{\sigma_s^2} \mathbf{w}^H \mathbf{h}_s \mathbf{h}_s^H \mathbf{w}$$

$$\geq \frac{1}{1 + \frac{1}{\sigma_{e,k}^2} \mathbf{w}^H \mathbf{H}_{e,k} \mathbf{H}_{e,k}^H \mathbf{w}} \geq 2^R, \forall k.$$
Then, the above problem can be written as

\[
\min_w \|w\|^2_2 \\
\text{s.t.} \quad 2R \sigma_{e,k}^2 \|H_{e,k}w\|^2 + (2R - 1) \leq \frac{1}{\sigma_s^2} |h_s^H w|^2, \forall k.
\] (4.39)

From the following inequality relation

\[
\begin{bmatrix}
  x \\
  y
\end{bmatrix} \succeq_K 0, \Leftrightarrow \|y\|_2 \leq x.
\] (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 \( w = \sqrt{p}v \), the problem (4.38) for only one eavesdropper can be written as

\[
\min_{p,v} \quad p v^H v, \quad \text{s.t.} \quad \frac{v^H (I + \frac{1}{\sigma_s^2} h_s h_s^H)}{v^H (I + \frac{1}{\sigma_e^2} H_e H_e^H)} v \geq 2R, \quad v^H v = 1, p \geq 0.
\] (4.41)

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

\[
L(w, \lambda) = w^H w + \lambda 2R (I + \frac{1}{\sigma_e^2} w^H H_e H_e^H w) - \lambda (1 + \frac{1}{\sigma_s^2} w^H h_s h_s^H w)
\]

\[
= w^H \left( I + \frac{1}{\sigma_e^2} \lambda 2R H_e H_e^H - \frac{1}{\sigma_s^2} \lambda h_s h_s^H \right) w + \lambda (2R - 1),
\] (4.42)

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

\[
\max_{\lambda} \lambda \left( 2R - 1 \right), \quad \text{s.t.} \quad Z \triangleq I + \frac{1}{\sigma_e^2} \lambda 2R H_e H_e^H - \frac{1}{\sigma_s^2} \lambda h_s h_s^H \succeq 0, \quad \lambda \geq 0.
\] (4.43)

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

\[
\nabla_{ww^H} = I + \frac{1}{\sigma_e^2} \lambda 2R H_e H_e^H - \frac{1}{\sigma_s^2} \lambda h_s h_s^H.
\] (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 $\lambda^*$ is derived as

$$
\lambda^* = \frac{1}{\lambda_{\max}\left(\frac{1}{\sigma_s^2} h_s h_s^H - \frac{2R}{\sigma_e^2} H e e^H\right)}.
$$

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

$$
p^* = \lambda^* (2^R - 1).
$$

In addition, the optimal $w$ lies in the null space of $Z$, thus

$$
v_1 = v_{\max}\left(\frac{1}{\sigma_s^2} h_s h_s^H - \frac{2R}{\sigma_e^2} H e e^H\right), \quad v = \frac{v_1}{\|v_1\|_2}.
$$

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

$$
\sqrt{\|R_{e,k}^2(I \otimes Q_s)R_{e,k}^2\|_F^2 + 2\|R_{e,k}^2(I \otimes Q_s)\bar{h}_{e,k}\|^2} \leq \sqrt{\|R_{e,k}^2(I \otimes Q_s)\|^2_F (\|R_{e,k}^2\|^2_F + 2\|\bar{h}_{e,k}\|^2)} \\
\leq \sqrt{\text{Tr}[(I \otimes Q_s)(I \otimes Q_s)^H]} \sqrt{\text{Tr}^2(R_{e,k}) + 2\text{Tr}(R_{e,k})\|\bar{h}_{e,k}\|^2} \leq w_k,
$$

$$
\Rightarrow \text{Tr}[(I \otimes Q_s)(I \otimes Q_s)^H]l_k^2 \leq w_k^2,
$$

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

\[ t_k^2 N_{E,k} \text{Tr}(Q_s Q_s^H) \leq w_k^2, \Rightarrow \lambda_{\text{max}}(Q_s Q_s^H) \leq \frac{w_k^2}{t_k^2 N_{E,k}}, \]

\[ \Rightarrow Q_s Q_s^H \preceq t_k^2 I, \Rightarrow S_k = \begin{bmatrix} t_k I & Q_s \\ Q_s^H & t_k I \end{bmatrix} \succeq 0, \tag{4.49} \]

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

\[
\begin{bmatrix} t_k I & 0 \\ 0^H & t_k I \end{bmatrix} \succeq \begin{bmatrix} I \\ 0 \end{bmatrix} Q_s \begin{bmatrix} 0 & -I \end{bmatrix} + \begin{bmatrix} 0 \\ -I \end{bmatrix} Q_s^H \begin{bmatrix} I & 0 \end{bmatrix}, \tag{4.50}
\]

\[
\|Q_s\| \leq t_k.
\]

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 \( A = A^H, B \) and \( C \), the following LMI is satisfied:

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

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

\[
\begin{bmatrix} A - aC^H C & -tB^H \\ -tB & aI \end{bmatrix} \succeq 0. \tag{4.52}
\]

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

\[
S_k = \begin{bmatrix} t_k I & 0 \\ 0 & t_k I \end{bmatrix} - a_1 \begin{bmatrix} 0 \\ -I \end{bmatrix} \begin{bmatrix} 0 & -I \end{bmatrix} - t_k \begin{bmatrix} I \\ 0 \end{bmatrix} - a_1 I \begin{bmatrix} 0 \\ -I \end{bmatrix} \begin{bmatrix} I \\ 0 \end{bmatrix} \succeq 0. \tag{4.53}
\]

From (4.53), it is claimed that constraint (4.49) can be equivalently rewritten without \( Q_s \). In order to prove rank-one of the power minimization problem, the La-
4.6 Appendix

The Lagrangian dual function of (4.18) is given in (4.54),

\[ L(Q_s, Z, \lambda, C_k) = \text{Tr}(Q_s) - \text{Tr}(ZQ_s) + \sum_{k=1}^{K} \lambda_k \left[ \text{Tr}(R_{e,k} + \bar{h}_{e,k}\bar{h}_{e,k}^H)(I \otimes Q_s) \right] - \frac{\sigma_{e,k}^2}{2R\sigma_s^2} \text{Tr}(h_s h_s^H Q_s) + \sqrt{-2 \ln(\rho) w_k - \ln(\rho) y_k} - \sigma_{e,k}^2 \left( \frac{1}{2} - 1 \right) \]

\[ - \sum_{k=1}^{K} \lambda_k \left[ C_k \left( y_k I - R_{e,k}^2 (I \otimes Q_s) R_{e,k}^2 \right) \right] \]

\[ = \text{Tr}(Q_s) - \text{Tr}(ZQ_s) + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \lambda_k \text{Tr}(H_k^{(n,n)} Q_s) - \sum_{k=1}^{K} \lambda_k \sigma_{e,k}^2 \text{Tr}(h_s h_s^H Q_s) \]

\[ + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \text{Tr}[T_{e,k}^{(n,n)} Q_s]. \quad (4.54) \]

where \( Z, \lambda, \) and \( C_k \) are dual variables associated with \( Q_s \), (4.17a) and (4.17c), respectively. In addition, \( H_k^{(n,n)} \in \mathbb{H}_{+}^{N_T \times N_T} \) and \( T_{e,k}^{(n,n)} \in \mathbb{H}_{+}^{N_T \times N_T} \) are block submatrices of \( R_{e,k} + \bar{h}_{e,k}\bar{h}_{e,k}^H \) and \( R_{e,k}^2 C_k R_{e,k}^2 \), respectively, which are expressed specifically as follows:

\[ R_{e,k} + \bar{h}_{e,k}\bar{h}_{e,k}^H = \begin{bmatrix} H_k^{(1,1)} & \ldots & H_k^{(1,N_{E,k})} \\ \vdots & \ddots & \vdots \\ H_k^{(N_{E,k},1)} & \ldots & H_k^{(N_{E,k},N_{E,k})} \end{bmatrix} \quad (4.55) \]

and

\[ R_{e,k}^2 C_k R_{e,k}^2 = \begin{bmatrix} T_{e,k}^{(1,1)} & \ldots & T_{e,k}^{(1,N_{E,k})} \\ \vdots & \ddots & \vdots \\ T_{e,k}^{(N_{E,k},1)} & \ldots & T_{e,k}^{(N_{E,k},N_{E,k})} \end{bmatrix} \quad (4.56) \]

The following KKT conditions related to the proof are considered:

\[ \frac{\partial L}{\partial Q_s} = 0, \quad (4.57a) \]

\[ ZQ_s = 0, \quad (4.57b) \]

\[ Q_s \succeq 0, \ Z \succeq 0, \ \lambda \succeq 0, \ C_k \succeq 0, \ \forall k. \quad (4.57c) \]
According to the KKT condition in (4.57a),

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

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

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

From (4.59), it is claimed that there is at least one $\lambda_k$, $\forall k$ such that $\lambda_k > 0$, which is shown by contradiction. If all $\lambda_k = 0$ for $\forall k$, then $t = 0 \Rightarrow \left( \mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{T}_{e,k}^{(n,n)} \right) \mathbf{Q}_s = 0$ (c.f. (4.59)) such that $\mathbf{Q}_s = 0$ due to $\mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{T}_{e,k}^{(n,n)} \succ 0$, 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:

$$\text{rank}(\mathbf{Q}_s) = \text{rank}
\left[ \left( \mathbf{I} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \lambda_k \mathbf{H}_k^{(n,n)} + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} \mathbf{T}_{e,k}^{(n,n)} \right) \mathbf{Q}_s \right]$$

$$= \text{rank}(\mathbf{t}^H \mathbf{h}_s^H \mathbf{Q}_s) \leq \min\{\text{rank}(\mathbf{t}^H \mathbf{h}_s^H), \text{rank}(\mathbf{Q}_s)\} \leq 1. \quad (4.60)$$

This completes the proof of Theorem 4.2.

\[\blacksquare\]

### 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:

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

where

$$\mathbf{A}_k = \begin{bmatrix}
\lambda_k \mathbf{I} + \left[ -\mathbf{R}^{\frac{1}{2}}_{e,k} (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{R}^{\frac{1}{2}}_{e,k} \right] & -\mathbf{R}^{\frac{1}{2}}_{e,k} (\mathbf{I} \otimes \mathbf{Q}_s) \bar{\mathbf{h}}_{e,k} \\
-\bar{\mathbf{h}}_{e,k}^H (\mathbf{I} \otimes \mathbf{Q}_s) \mathbf{R}^{\frac{1}{2}}_{e,k} & t_k - \lambda_k \sigma^2_{e,k}
\end{bmatrix},$$
From the above equality, it is shown that $T$ is rewritten for the convenience of notations.

$$A_k = \begin{bmatrix} \lambda_k \mathbf{I} & 0 \\ 0 & (\frac{1}{2\pi} - 1)\sigma^2_{e,k} - \lambda_k \gamma^2_{e,k} \end{bmatrix} + \frac{\sigma^2_{e,k}}{2\mathbf{R}_s^2} \begin{bmatrix} 0 & \mathbf{h}_s \\ \mathbf{h}_s & \mathbf{Q}_s \end{bmatrix}^H \mathbf{Q}_s \begin{bmatrix} 0 & \mathbf{h}_s \\ \mathbf{h}_s & \mathbf{0} \end{bmatrix}$$

\begin{equation} \label{4.62} - \left[ \mathbf{R}^{\frac{1}{2}}_{e,k} \, \mathbf{h}_{e,k} \right]^H (\mathbf{I} \otimes \mathbf{Q}_s) \left[ \mathbf{R}^{\frac{1}{2}}_{e,k} \, \mathbf{h}_{e,k} \right]. \end{equation}

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

$$L(\mathbf{Q}_s, \mathbf{Z}, \mathbf{Y}_k) = \text{Tr}(\mathbf{Q}_s) - \text{Tr}(\mathbf{Z}\mathbf{Q}_s) + \sum_{k=1}^{K} \text{Tr} \left( \mathbf{Y}_k \left[ \mathbf{R}^{\frac{1}{2}}_{e,k} \, \mathbf{h}_{e,k} \right]^H (\mathbf{I} \otimes \mathbf{Q}_s) \left[ \mathbf{R}^{\frac{1}{2}}_{e,k} \, \mathbf{h}_{e,k} \right] \right)$$

$$- \sum_{k=1}^{K} \text{Tr} \left( \mathbf{Y}_k \left[ \lambda_k \mathbf{I} \right. \right.$$ 

$$\left. \begin{bmatrix} 0 & \mathbf{h}_s \\ \mathbf{h}_s & \mathbf{Q}_s \end{bmatrix} \right) \left[ \mathbf{0} \right. \right.$$ 

$$\left. \begin{bmatrix} 0 & \mathbf{h}_s \\ \mathbf{h}_s & \mathbf{0} \end{bmatrix} \right]\right) - \sum_{k=1}^{K} \frac{\sigma^2_{e,k}}{2\mathbf{R}_s^2} \text{Tr} \left( \mathbf{Y}_k \left[ \mathbf{0} \right. \right.$$ 

$$\left. \begin{bmatrix} \mathbf{h}_s \\ \mathbf{h}_s \end{bmatrix} \right] \right) - \sum_{k=1}^{K} \frac{\sigma^2_{e,k}}{2\mathbf{R}_s^2} \text{Tr} \left( \mathbf{Y}_k \left[ \mathbf{0} \right. \right.$$ 

$$\left. \begin{bmatrix} \mathbf{h}_s \\ \mathbf{h}_s \end{bmatrix} \right] \right). \right)$$

\begin{equation} \label{4.63} \end{equation}

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

\begin{equation} \label{4.64} \end{equation}

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

\begin{equation} \label{4.65} \end{equation}

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

\[
\text{rank}(Q_s) = \text{rank}\left( (I + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} S_k^{(n,n)}) Q_s \right) = \text{rank}\left( \begin{bmatrix} 0 & h_s \end{bmatrix} \begin{bmatrix} 0 & h_s \end{bmatrix}^H Q_s \right) \\
\leq \text{rank}\left( \begin{bmatrix} 0 & h_s \end{bmatrix} \right) \leq 1,
\]

(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

\[
\min_{Q_s} \text{Tr}(Q_s) \\
\text{s.t. } \frac{1}{\sigma_s^2} \left[ \text{Tr}(\tilde{h}_s \tilde{h}_s^H Q_s) + \text{Tr}(R_s Q_s) \right] - \frac{2R}{\sigma_e^2} \text{Tr}[\tilde{h}_{e,k} \tilde{h}_{e,k}^H + R_{e,k})(I \otimes Q_s)] + a_k \geq 0, \\
\begin{bmatrix}
w_k I & f_k \\
f_k^H & w_k
\end{bmatrix} \succeq 0, \\
y_k I_{N_T} + \frac{1}{\sigma_s^2} R_s^{\frac{1}{2}} Q_s R_s^{\frac{1}{2}} \geq 0, \\
y_k I_{N_T N_{E,k}} - \frac{2R}{\sigma_e^2} R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) R_{e,k}^{\frac{1}{2}} \geq 0,
\]

(4.67a)

where

\[
a_k = 1 - 2R - \sqrt{-2 \ln \rho_w} + \ln \rho_y,
\]

and

\[
f_k = \begin{bmatrix}
\text{vec}\left( \begin{bmatrix}
\frac{1}{\sigma_s^2} R_s^{\frac{1}{2}} Q_s R_s^{\frac{1}{2}} & 0 \\
0 & -\frac{2R}{\sigma_e^2} R_{e,k}^{\frac{1}{2}} (I \otimes Q_s) R_{e,k}^{\frac{1}{2}}
\end{bmatrix}\right) \\
\sqrt{2} \begin{bmatrix}
\frac{1}{\sigma_s^2} R_s^{\frac{1}{2}} Q_s \\
0
\end{bmatrix}
\begin{bmatrix}
\tilde{h}_s H \\
\tilde{h}_{e,k}^H
\end{bmatrix}
\end{bmatrix}.
\]

(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

\[ \mathcal{L}(Q_s, Z, \lambda_k, B_k, C_k) = \text{Tr}(Q_s) - \text{Tr}(ZQ_s) - \sum_{k=1}^{K} \lambda_k \left( \frac{1}{\sigma^2_s} \left[ \text{Tr}(\bar{h}_s \bar{h}_H Q_s) + \text{Tr}(R_s Q_s) \right] - \frac{2R}{\sigma^2_{e,k}} \text{Tr} \left[ (\bar{h}_{e,k} \bar{h}_{e,k}^H + R_{e,k})(I \otimes Q_s) \right] + a_k \right) - \sum_{k=1}^{K} \text{Tr} \left[ C_k \left( y_k I_{N_{TE,k}} \right) \right] \]

\[ - \frac{2R}{\sigma^2_{e,k}} R_{e,k}^2 (I \otimes Q_s) R_{e,k}^2 \right) \right], \quad (4.69) \]

According to the relevant KKT condition,

\[ \frac{\partial \mathcal{L}}{\partial Q_s} = I - \sum_{k=1}^{K} \frac{\lambda_k}{\sigma^2_s} \bar{h}_s \bar{h}_s^H - \sum_{k=1}^{K} \frac{\lambda_k}{\sigma^2_s} R_s + \sum_{k=1}^{K} \sum_{n=1}^{N_{TE,k}} \frac{\lambda_k 2R}{\sigma^2_{e,k}} H_k^{(n,n)} - \sum_{k=1}^{K} \sum_{n=1}^{N_{TE,k}} \frac{\sigma R}{\sigma^2_{e,k}} R_k^{(n,n)} - Z = 0, \]

\[ \quad (4.70) \]

where \( H_k^{(n,n)} \in \mathbb{H}^{N_T} \) is a block submatrix of \( h_{e,k} h_{e,k}^H + R_{e,k} \), and \( R_k^{(n,n)} \in \mathbb{H}^{N_T} \) is a block submatrix of \( H_{e,k} C_k H_{e,k} \). Then, setting

\[ T = I + \sum_{k=1}^{K} \sum_{n=1}^{N_{TE,k}} \frac{2R}{\sigma^2_{e,k}} \left( \lambda_k H_k^{(n,n)} + R_k^{(n,n)} \right) - \left( \sum_{k=1}^{K} \frac{\lambda_k}{\sigma^2_s} \right) R_s, \]

\[ \quad (4.71) \]

the following equality holds:

\[ Z = T - \left( \sum_{k=1}^{K} \frac{\lambda_k}{\sigma^2_s} \right) \bar{h}_s \bar{h}_s^H. \]

\[ \quad (4.72) \]

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

if \( T \succ 0 \), then this implies \( r_T = N_T \), according to [101, Lemma 5], \( \text{rank}(Z) \geq N_T - 1 \).

It is claimed that \( \text{rank}(Z) \neq N_T \) due to \( Q_s \neq 0 \). Thus, \( \text{rank}(Z) = N_T - 1 \) only when \( \text{rank}(Q_s) = 1 \) due to the KKT condition \( ZQ_s = 0 \). Therefore, the remaining part is to show that \( T \succ 0 \). By exploiting [101, Appendix D], it is concluded that \( T \succ 0 \) such that \( \text{rank}(Q_s) = 1 \).

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), $T_s$ and $T_{e,k}$ can be modified as follows:

\[ T_s = \Xi_s + V_s^H Q_s V_s, \quad (4.73a) \]
\[ T_{e,k} = \Xi_{e,k} - V_{e,k}^H (I \otimes Q_s) V_{e,k}, \quad (4.73b) \]

where

\[ \Xi_s = \begin{bmatrix} \mu_s I & 0 \\ 0 & -t_s - \mu_s \gamma^2_s \end{bmatrix}, V_s = \frac{1}{\sigma_s} \begin{bmatrix} R_s^{\frac{1}{2}} & h_s \end{bmatrix}, \]
\[ \Xi_{e,k} = \begin{bmatrix} \mu_k I & 0 \\ 0 & t_{e,k} - \mu_{e,k} \gamma^2_{e,k} \end{bmatrix}, V_{e,k} = \frac{2\sigma_k}{\sigma_e} \begin{bmatrix} R_{e,k}^{\frac{1}{2}} & h_{e,k} \end{bmatrix}. \]

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,

\[ \mathcal{L}(Q_s, Z, A_s, A_{e,k}, \nu_k, \lambda_s, \lambda_{e,k}) = \text{Tr}(Q_s) - \text{Tr}(Q_s Z) - \text{Tr}(T_s A_s) - \sum_{k=1}^{K} \text{Tr}(T_{e,k} A_{e,k}) \]
\[ - \sum_{k=1}^{K} \nu_k(t_s - t_{e,k} - 2^R + 1) - \lambda_s \mu_s - \sum_{k=1}^{K} \lambda_{e,k} \mu_{e,k}, \quad (4.74) \]

where $Z$, $A_s$, $A_{e,k}$, $\nu_k$, $\lambda_s$ and $\lambda_{e,k}$ are dual variables associated with $Q_s$, $T_s$, $T_{e,k}$, $\mu_s$, $\mu_{e,k}$, and (4.37a), respectively. The relevant KKT conditions are considered as follows:

\[ \frac{\partial \mathcal{L}}{\partial Q_s} = 0, \quad (4.75a) \]
\[ Q_s Z = 0, \quad (4.75b) \]
\[ T_s A_s = 0, \quad (4.75c) \]
\[ A_s \succeq 0, A_{e,k} \succeq 0, Q_s \succeq 0, \lambda_s \geq 0. \quad (4.75d) \]

From (4.75a),

\[ \frac{\partial \mathcal{L}}{\partial Q_s} = I - Z - V_s A_s V_s^H + \sum_{k=1}^{K} \sum_{n=1}^{N_{e,k}} S^{(n,n)}_{e,k} = 0, \quad (4.76) \]
where \( S_{e,k}^{(n,n)} \in \mathbb{H}_{NT}^N \) is a block submatrix of \( V_e,k A_{e,k} V_{e,k}^H \).

\[
V_{e,k} A_{e,k} V_{e,k}^H = \begin{bmatrix}
S_{e,k}^{(1,1)} & \cdots & S_{e,k}^{(1,N_{E,k})} \\
\vdots & \ddots & \vdots \\
S_{e,k}^{(N_{E,k},1)} & \cdots & S_{e,k}^{(N_{E,k},N_{E,k})}
\end{bmatrix}
\] (4.77)

By premultiplying \( Q_s \) by both sides of (4.76),

\[
Q_s \left( I + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} S_{e,k}^{(n,n)} \right) = Q_s V_s A_s V_{s}^H
\] (4.78)

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

\[
\text{rank}(Q_s) = \text{rank} \left( Q_s \left( I + \sum_{k=1}^{K} \sum_{n=1}^{N_{E,k}} S_{e,k}^{(n,n)} \right) \right) = \text{rank} \left( Q_s V_s A_s V_{s}^H \right).
\] (4.79)

In order to prove \( \text{rank}(Q_s) \leq 1 \), it will be shown that \( \text{rank}(Q_s V_s A_s V_{s}^H) \leq 1 \) holds.

Due to (4.75c), we postmultiply \( V_s^H \) by the two sides of this KKT condition,

\[
\Xi_s A_s V_{s}^H + V_{s}^H Q_s V_s A_s V_{s}^H = 0.
\] (4.80)

As a result of the following equalities,

\[
\frac{1}{\sigma_s} \begin{bmatrix}
R_s^2 & 0 \\
0 & 0
\end{bmatrix} \Xi_s = \mu_s \left( V_s - \frac{1}{\sigma_s} \begin{bmatrix}
0 & \bar{h}_s
\end{bmatrix} \right),
\]

\[
\frac{1}{\sigma_s} \begin{bmatrix}
R_s & 0 \\
0 & 0
\end{bmatrix} V_{s}^H = \frac{1}{\sigma_s^2} R_s.
\]

By premultiplying both sides of (4.80) by \( \frac{1}{\sigma_s} \begin{bmatrix}
R_s & 0 \\
0 & 0
\end{bmatrix} \),

\[
\mu_s \left( V_s - \frac{1}{\sigma_s} \begin{bmatrix}
0 & \bar{h}_s
\end{bmatrix} \right) A_s V_{s}^H + \frac{1}{\sigma_s^2} R_s Q_s V_s A_s V_{s}^H = 0,
\]

\[
\Rightarrow \left( \mu_s I + \frac{1}{\sigma_s^2} R_s Q_s \right) V_s A_s V_{s}^H = \frac{\mu_s}{\sigma_s} \begin{bmatrix}
0 & \bar{h}_s
\end{bmatrix} A_s V_{s}^H.
\] (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),

\[
T_s = \begin{bmatrix}
0 & 0 \\
0 & -t_s
\end{bmatrix} + V_{s}^H Q_s V_s.
\] (4.82)
4.6 Appendix

Assuming that \( \text{rank}(V_s^H Q_s V_s) = r_s \), it thus straightforwardly follows from (4.82) that

\[
\text{rank}(T_s) \geq \text{rank}(V_s^H Q_s V_s) - \text{rank}\begin{bmatrix}
0 & 0 \\
0 & t_s
\end{bmatrix} = r_s - 1,
\]

\[
\Rightarrow \text{rank}(\text{null}(T_s)) \leq N_T + 1 - (r_s - 1).
\] (4.83)

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

\[
\xi^H T_s \xi = \xi^H \begin{bmatrix}
0 & 0 \\
0 & -t_s
\end{bmatrix} \xi \geq 0.
\] (4.84)

It is easily verified that \( \xi^H T_s \xi = 0 \) due to \( t_s > 0 \) and therefore,

\[
\forall \xi \in \text{null}(V_s^H Q_s V_s) \Rightarrow \xi \in \text{null}(T_s),
\]

\[
\Rightarrow \text{null}(V_s^H Q_s V_s) \subseteq \text{null}(T_s).
\] (4.85)

According to (4.85),

\[
\text{rank}(\text{null}(V_s^H Q_s V_s)) \leq \text{rank}(\text{null}(T_s)),
\]

\[
\Rightarrow \text{rank}(\text{null}(T_s)) \geq N_T + 1 - r_s.
\] (4.86)

Combining (4.83) with (4.86),

\[
N_T + 1 - r_s \leq \text{rank}(\text{null}(T_s)) \leq N_T + 1 - (r_s - 1).
\] (4.87)

Since \( T_s A_s = 0 \),

\[
N_T + 1 - r_s \leq \text{rank}(A_s) \leq N_T + 1 - (r_s - 1).
\] (4.88)
Accordingly, \( A_s \) is of the following structure:

\[
A_s = \sum_{i=1}^{N_T+1-r_s} \alpha_i \xi_i^H + \beta \eta H, \quad (\alpha_i > 0, \forall i, \beta \geq 0).
\] (4.89)

If \( \beta = 0 \), then

\[
Q_s V_s A_s V_s^H = Q_s^\frac{1}{2} Q_s^\frac{1}{2} V_s \left( \sum_{i=1}^{N_T+1-r_s} \alpha_i \xi_i^H \right) V_s^H = Q_s^\frac{1}{2} \sum_{i=1}^{N_T+1-r_s} \alpha_i \left( Q_s^\frac{1}{2} V_s \xi_i^H V_s^H \right) = 0.
\] (4.90)

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

\[
Q_s V_s A_s V_s^H = Q_s^\frac{1}{2} Q_s^\frac{1}{2} V_s \left( \sum_{i=1}^{N_T+1-r_s} \alpha_i \xi_i^H + \beta \eta H \right) V_s = Q_s^\frac{1}{2} \left( 0 + \beta Q_s^\frac{1}{2} V_s \eta H V_s^H \right) = \beta Q_s V_s \eta H V_s^H.
\] (4.91)

One can easily observe from (4.91) that \( \text{rank}(Q_s V_s A_s V_s^H) \leq \text{rank}(\eta H) = 1 \).

Moreover, the case of \( \mu_s > 0 \) is provided, since \( \mu_s I + \frac{1}{\sigma_s^2} R_s Q_s \) is of full-rank, according to (4.81),

\[
\text{rank}(V_s A_s V_s^H) = \text{rank} \left[ \frac{\mu_s}{\sigma_s} \left( \mu_s I + \frac{1}{\sigma_s^2} R_s Q_s \right)^{-1} \begin{bmatrix} 0 & \bar{h}_s \end{bmatrix} V_s A_s V_s^H \right]
\leq \text{rank} \left( \begin{bmatrix} 0 & \bar{h}_s \end{bmatrix} \right) \leq 1, \Rightarrow \text{rank}(Q_s V_s A_s V_s^H) \leq 1,
\] (4.92)

which completes the proof of Theorem 4.5.

\[\blacksquare\]
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 Stackelberg 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
5.1 System Model

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 \( H_s \in \mathbb{C}^{M_R \times N_T} \) and \( H_e \in \mathbb{C}^{M_E \times N_T} \), respectively. On the other hand, \( H_j \in \mathbb{C}^{M_R \times N_J} \) and \( H_{je} \in \mathbb{C}^{M_E \times N_J} \) 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

\[
y_r = H_s x_1 + H_j x_2 + n_r, \quad y_e = H_s x_1 + H_{je} x_2 + n_e,
\]

(5.1)

where \( x_1 \in \mathbb{C}^{N_T \times 1} \) is the signal vector intended for the legitimate user, whereas \( x_2 \in \mathbb{C}^{N_J \times 1} \) represents the jamming signal vector. \( n_r \in \mathbb{C}^{M_R \times 1} \) and \( n_e \in \mathbb{C}^{M_E \times 1} \) 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 \( \sigma_r^2 I \) and \( \sigma_e^2 I \), respectively. The transmit covariance matrices of the transmitter and the CJ are defined as \( Q_1 = \mathbb{E} \{ x_1 x_1^H \} \) and \( Q_2 = \mathbb{E} \{ x_2 x_2^H \} \). Thus, the achieved secrecy rate is written as [18]:

\[
R_{sr} = [I_r - I_e]^+ = \begin{bmatrix}
\log \left| \frac{I + \frac{1}{\sigma_r^2} H_s Q_1 H_s^H + \frac{1}{\sigma_j^2} H_j Q_2 H_j^H}{I + \frac{1}{\sigma_e^2} H_{je} Q_2 H_{je}^H} \right| \\
- \log \left| \frac{I + \frac{1}{\sigma_e^2} H_{je} Q_1 H_{je}^H + \frac{1}{\sigma_j^2} H_{je} Q_2 H_{je}^H}{I + \frac{1}{\sigma_e^2} H_{je} Q_2 H_{je}^H} \right|
\end{bmatrix}^+,
\]

(5.2)
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

$$\min_{Q_1, Q_2} \text{Tr}(Q_1) + \text{Tr}(Q_2), \quad s.t. \ R_{sr} \geq \bar{R}_{sr}, \ Q_1 \succeq 0, \ Q_2 \succeq 0,$$ (5.3)

where $\bar{R}_{sr}$ is the required secrecy rate. Assume that the legitimate transmitter and the CJ have perfect CSI (i.e., $H_e$ and $H_{je}$) 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

$$\max_{Q_1, Q_2} \ R_{sr}, \quad s.t. \ \text{Tr}(Q_1) \leq P_1, \ Q_1 \succeq 0, \ \text{Tr}(Q_2) \leq P_2, \ Q_2 \succeq 0,$$ (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 $Q_1$ and $Q_2$, 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., $Q_1$) for a fixed jammer transmit covariance matrix (i.e., $Q_2$). 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., $Q_2$) can be optimally designed based on a null space scheme and CJ maximization method, which will be shown in the following.
5.2 Secrecy Rate Optimizations

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., $H_j$). 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 $H_j U = 0$ as

$$U = (I - H_j^H (H_j H_j^H)^{-1} H_j) H_j D_1,$$

(5.5)

where $D_1$ 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

$$\max_D \log |I + V|, \quad s.t. \quad \text{Tr}(PH_j H_j^H P) \leq P_2, \quad D \succeq 0,$$

(5.6)

where $D = D_1^2$, $V = \frac{1}{\sigma^2_e} H_j^H P H_j^H D_1 H_j^H P H_j^H$ and $P = I - H_j^H (H_j H_j^H)^{-1} H_j$. 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 $Q_2 = UU^H$.

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 $Q_2$ 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

$$\max_{Q_2 \succeq 0} R_j = \log \left| I + \frac{1}{\sigma^2_e} H_j Q_2 H_j^H \right| - \log \left| I + \frac{1}{\sigma^2_e} H_j Q_2 H_j^H \right|,$$

s.t. $\text{Tr}(Q_2) \leq P_2, \quad Q_2 \succeq 0$.

(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
5.2 Secrecy Rate Optimizations

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

$$\max_{Q_2} \hat{R}_j \triangleq \log \left| I + \frac{1}{\sigma_r^2} H_{jx} Q_2 H_{jx}^H \right| - \log \left| I + \frac{1}{\sigma_r^2} H_{jy} \tilde{Q}_2 H_{jy}^H \right| - \text{Tr} \left[ \frac{1}{\sigma_r^2} \left( I + \frac{1}{\sigma_r^2} H_{jx} \tilde{Q}_2 H_{jx}^H \right)^{-1} H_{jy} (Q_2 - \tilde{Q}_2) H_{jy}^H \right]$$

s.t. $\text{Tr} (Q_2) \leq P_2$, $Q_2 \succeq 0$. \hfill (5.8)

The problem (5.8) is easily shown to be convex and hence $Q_2$ can be obtained iteratively by solving (5.8). The proposed iterative algorithm for optimizing the CJ transmit covariance matrix $Q_2$ is summarized in Table 5.1.

The approximated transmit covariance matrix $\tilde{Q}_2$ can be updated at each iteration by $Q_2^*$, which is obtained from the previous iteration. It is noted that $Q_2$ is equal to $Q_2^*$ at the convergence of the proposed algorithm, which confirms that the approximated rate $\hat{R}_j$ is equal to the actual rate $R_j$.

### Table 5.1: Cooperative jammer rate maximization algorithm

1. Initialize: $\tilde{Q}_2 = 0$.

2. Repeat
   - (a) Solve (5.8) to obtain $Q_2^*$ for a given $\tilde{Q}_2$.
   - (b) Update $\tilde{Q}_2 \leftarrow Q_2^*$.

3. Until the required accuracy.

5.2.3 Power Minimization with Secrecy Rate Constraint

In the previous subsections, the CJ transmit covariance matrix $Q_2^*$ has been designed by employing the null space method and the CJ rate maximization. Here, the transmit covariance matrix of the legitimate transmitter $Q_1$ is optimally designed to minimize the transmit power such that it satisfies the achieved secrecy rate. This
power minimization problem is formulated as

$$\min_{Q_1 \succeq 0} \text{Tr}(Q_1), \quad s.t. \quad R_{sr} = \log \left| \frac{I + \frac{1}{\sigma_e^2} H_s Q_1 H_s^H}{I + \frac{1}{\sigma_e^2} H_j Q_2 H_j^H} \right| \geq \bar{R}_{sr}. \tag{5.9}$$

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

$$R_{sr} \approx \log \left| I + \frac{1}{\sigma_e^2} H_s Q_1 H_s^H + \frac{1}{\sigma_e^2} H_j Q_2 H_j^H \right| + \log \left| I + \frac{1}{\sigma_e^2} H_{je} Q_2 H_{je}^H \right| - \log \left| I + \frac{1}{\sigma_e^2} H_e \tilde{Q}_1 H_e^H + \frac{1}{\sigma_e^2} H_{je} Q_2 H_{je}^H \right|$$

$$- \text{Tr} \left[ \frac{1}{\sigma_e^2} \left( I + \frac{1}{\sigma_e^2} H_e \tilde{Q}_1 H_e^H + \frac{1}{\sigma_e^2} H_{je} Q_2 H_{je}^H \right)^{-1} H_e \tilde{Q}_1 H_e^H \right] + \text{Tr} \left[ \frac{1}{\sigma_e^2} \left( I + \frac{1}{\sigma_e^2} H_e \tilde{Q}_1 H_e^H + \frac{1}{\sigma_e^2} H_{je} Q_2 H_{je}^H \right)^{-1} H_e \tilde{Q}_1 H_e^H \right] \triangleq \tilde{R}_{sr}. \tag{5.10}$$

The proof is similar to the proof to the problem (5.8). (5.10) is a concave function in terms of $Q_1$, 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

$$\min_{Q_1 \succeq 0} \text{Tr}(Q_1), \quad s.t. \quad Q_1 \succeq 0, \quad \tilde{R}_{sr} \geq \bar{R}_{sr}. \tag{5.11}$$

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

$$\max_{\lambda \geq 0} \min_{Q_1 \succeq 0} L(Q_1, \lambda) = \text{Tr}(Q_1) + \lambda \left( \tilde{R}_{sr} - \bar{R}_{sr} \right), \tag{5.12}$$

where $\lambda$ 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 $\lambda$ by using the subgradient method [78]. The solution to (5.11) is dependent on $\tilde{Q}_1$, and two initializations are
Table 5.2: Power minimization algorithm

1. Initialize: $\lambda$ and $\tilde{Q}_1 = 0$ or $\tilde{Q}_1 = Q_{WF}$.
2. **Iteration loop begin**
   - (a) Solve the problem in (5.12) to obtain $Q_1^*$ for a given $\lambda$.
   - (b) Update $\lambda$ based on the sub-gradient method.
3. **Until** the required accuracy.
4. **Iteration loop end**
5. Update $\tilde{Q}_1 \leftarrow Q_1^*$.
6. **Until** required accuracy.

considered: a) an all zero element matrix (i.e., $\tilde{Q}_1 = 0$) and b) a water-filling solution (i.e., $\tilde{Q}_1 = \tilde{Q}_{WF}$). 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 $\tilde{Q}_1$ and $Q_1$ are equal, then the approximated rate ($\tilde{R}_{sr}$) at $\tilde{Q}_1$ 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 $Q_1$ can be optimally designed for a given $Q_{2}^*$. This optimization problem is written as

$$\max_{Q_1 \succeq 0} R_{sr}, \text{ s.t. } \operatorname{Tr}(Q_1) \leq P_1, \ Q_1 \succeq 0. \quad (5.13)$$
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

$$\max_{Q_1} \tilde{R}_{sr}, \quad \text{s.t. } \text{Tr}(Q_1) \leq P_1, \quad Q_1 \succeq 0. \quad (5.14)$$

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:

$$L(Q_1, \lambda, Z) = -\tilde{R}_{sr} + \lambda [\text{Tr}(Q_1) - P_1] - \text{Tr}(ZQ_1) \quad (5.15)$$

and the corresponding Lagrange dual problem is expressed as

$$\min_{\lambda \geq 0} \max_{Q_1 \succeq 0} [\tilde{R}_{sr} - \lambda [\text{Tr}(Q_1) - P_1]], \quad (5.16)$$

where $\lambda$ 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 $\tilde{Q}_1$ is equal to $Q_1$ 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

\[
\begin{align*}
\hat{H}_e &= H_e + E_e, \\
\hat{H}_{je} &= H_{je} + E_{je},
\end{align*}
\] (5.17)

where \(H_e\) and \(H_{je}\) represent the channel mean of the corresponding channels, and \(E_e\) and \(E_{je}\) 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]:

\[\varepsilon_1 = \{E_e : \text{Tr}(E_e P_e^{-1} E_e^H) \leq \varepsilon_e^2\}, \quad \varepsilon_2 = \{E_{je} : \text{Tr}(E_{je} P_{je}^{-1} E_{je}^H) \leq \varepsilon_{je}^2\},\]

where \(P_e\) and \(P_{je}\) are known positive definite matrices, which are assumed to be identity matrices such that the channel errors are considered to be bounded by Frobenius norms (\(\|E_e\|_F \leq \varepsilon_e\) and \(\|E_{je}\|_F \leq \varepsilon_{je}\)). \(\varepsilon_e\) and \(\varepsilon_{je}\) 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., \(Q_1\)) and the CJ (i.e., \(Q_2\)) incorporating the channel uncertainty shown in Section 5.3.1. This robust power minimization problem can be written as

\[
\begin{align*}
\min_{Q_1 \succeq 0, Q_2 \succeq 0} & \quad \text{Tr}(Q_1) + \text{Tr}(Q_2) \\
\text{s.t.} & \quad \log \left| I + \frac{1}{\sigma^2} H_s Q_1 H_s^H \right| \\
& \quad \left| I + \frac{1}{\sigma^2} H_j Q_2 H_j^H \right| \\
& \quad - \log \left| I + \frac{1}{\sigma^2} \tilde{H}_e Q_1 \tilde{H}_e^H + \frac{1}{\sigma^2} \tilde{H}_{je} Q_2 \tilde{H}_{je}^H \right| \geq \bar{R}_{sr}, \\
& \quad \hat{H}_e = H_e + E_e, \quad \hat{H}_{je} = H_{je} + E_{je}, \quad \|E_e\|_F \leq \varepsilon_e, \quad \|E_{je}\|_F \leq \varepsilon_{je}.
\end{align*}
\] (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 \(Q_1\) (or \(Q_2\)) only are considered, and an alternative optimization algorithm is presented to design \(Q_1\) (or \(Q_2\)) for a given \(Q_2\) (or \(Q_1\)), respectively, each of which is reformulated into a SDP by exploiting linear
5.3 Robust Secrecy Rate Optimization

Table 5.3: Alternative optimization algorithm

1. Initialize: $Q_2 = 0$ or $Q_2 = Q_{WF}$; $\tilde{Q}_1 = Q_{WF}$ for approximation.

2. Iteration loop begin
   (a) Solve the robust power minimization problem in (5.19) to obtain $\tilde{Q}_1^*$ for a given $Q_2$.
   (b) $Q_1 \leftarrow \tilde{Q}_1^*$.
   (c) Solve the robust power minimization problem in (5.22) to obtain $\tilde{Q}_2^*$ for a given $Q_1$.
   (d) $Q_2 \leftarrow \tilde{Q}_2^*$.

3. Until the required accuracy.

4. Iteration loop end

5. Update $Q_1^* \leftarrow \tilde{Q}_1$, and $Q_2^* \leftarrow \tilde{Q}_2$.

matrix transformations.

First, $Q_2$ is assumed to be given to optimally design $Q_1$ 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

$$\begin{align*}
\min_{Q_1, \mu_1, t_2} \text{Tr}(Q_1) \\
\text{s.t.} \log \left| I + H_s Q_1 H_s^H + H_j Q_2 H_j^H \right| - t_1 - \log \left| I + \frac{1}{\sigma_r^2} H_j Q_2 H_j^H \right| \\
+ \log \left| I + \frac{1}{\sigma_c^2} H_j e Q_2 H_j^H e \right| \geq \bar{R}_{sr}, \\
\mu_1 I - B_1 - (Q_1^T \otimes I)^T a \\
- a^H (Q_1^T \otimes I)^* - \mu \varepsilon_c^2 - \alpha_1 + \beta_1 + t_1 - h_e^H B_1 h_e \succeq 0, \\
Q_1 \succeq 0, \mu_1 \geq 0, t_1 \geq 0,
\end{align*}$$

(5.19)
where

\[ \alpha_1 = \log \left| I + H_e \tilde{Q}_1 H_e^H + H_{je} Q_2 H_{je}^H \right|, \]
\[ \beta_1 = \text{Tr} \left[ \left( I + H_e \tilde{Q}_1 H_e^H + H_{je} Q_2 H_{je}^H \right)^{-1} H_e \tilde{Q}_1 H_e^H \right], \]
\[ S_1 = \left( I + H_e \tilde{Q}_1 H_e^H + H_{je} Q_2 H_{je}^H \right)^{-1}, \]
\[ B_1 = (Q_1^T \otimes I) T(I \otimes S_1), h_e = \text{vec}(H_e), \quad a = \text{vec}(S_1 H_e). \]

**Proof** Please refer to Section 5.7.1.

Similarly, \( Q_2 \) is optimized for a given \( Q_1 \) by solving (5.18), which can be expressed as

\[
\begin{align*}
\min_{Q_2,t_2,t_4} & \quad \text{Tr}(Q_2) \\
\text{s.t.} & \quad \log \left| I + H_s Q_1 H_s^H + H_j Q_2 H_j^H \right| - \log \left| I + H_j \tilde{Q}_2 H_j^H \right| \\
& \quad + \text{Tr} \left[ \left( I + H_j \tilde{Q}_2 H_j^H \right)^{-1} H_j \tilde{Q}_2 H_j^H \right] - \text{Tr} \left[ \left( I + H_j \tilde{Q}_2 H_j^H \right)^{-1} H_j Q_2 H_j^H \right] \\
& \quad + \log(t_2) - t_3 \geq \bar{R}_{sr}, \\
& \quad \log \left| I + \tilde{H}_{je} Q_2 \tilde{H}_{je}^H \right| \geq \log(t_2), \\
& \quad \alpha_2 - \beta_2 + \text{Tr} \left[ S_2 \tilde{H}_{je} Q_2 \tilde{H}_{je}^H \right] \leq t_3, \\
& \quad Q_2 \succeq 0, \quad t_2 \geq 0, \quad t_3 \geq 0,
\end{align*}
\]

where

\[ \alpha_2 = \log \left| I + H_e Q_1 H_e^H + H_{je} \tilde{Q}_2 H_{je}^H \right|, \]
\[ \beta_2 = \text{Tr} \left[ \left( I + H_e Q_1 H_e^H + H_{je} \tilde{Q}_2 H_{je}^H \right)^{-1} H_{je} \tilde{Q}_2 H_{je}^H \right], \]
\[ S_2 = \left( I + H_e Q_1 H_e^H + H_{je} \tilde{Q}_2 H_{je}^H \right)^{-1}. \]
The constraints (5.20b) and (5.20c) can be converted into semidefinite constraints similar to (5.19) as

\[
\begin{bmatrix}
\lambda_1 I + (Q_2^T \otimes I) & (Q_2^T \otimes I) h_{je} \\
 h_{je}^H (Q_2^T \otimes I)^* & -\lambda_1 \varepsilon_{je}^2 - t_2 + h_{je}^H (Q_2^T \otimes I) h_{je} + 1
\end{bmatrix} \succeq 0,
\]

(5.21a)

\[
\begin{bmatrix}
\lambda_2 I - B_2 & -(Q_2^T \otimes I)^T a_1 \\
 -a_1^H (Q_2^T \otimes I)^* & -\lambda_2 \varepsilon_{je}^2 - \alpha_2 + \beta_2 + t_3 - h_{je}^H B_2 h_{je}
\end{bmatrix} \succeq 0,
\]

(5.21b)

where \( h_{je} = \text{vec}(H_{je}), a_1 = \text{vec}(S_2 H_{je}) \) and \( B_2 = (Q_2^T \otimes I)^T (I \otimes S_2). \)

**Proof** Please refer to Section 5.7.2. □

Hence, the problem (5.20) can be reformulated as

\[
\begin{align*}
\min_{Q_2, \lambda_1, \lambda_2, t_2, t_3} & \quad \text{Tr}(Q_2), \\
\text{s.t.} & \quad (5.20a), (5.21a), (5.21b), Q_2 \succeq 0,
\end{align*}
\]

\[
\lambda_1 \geq 0, \lambda_2 \geq 0, t_2 \geq 0, t_3 \geq 0.
\]

(5.22)

Both (5.19) and (5.22) are convex problems, each of which can be solved to optimize \( Q_1 \) (or \( Q_2 \)) 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

$$R_s = \log |I + \frac{1}{\sigma_r^2}H_sQ_1H_s^H| - \log \frac{|I + \frac{1}{\sigma_r^2}(H_sQ_1H_e^H + p_1gg^H)|}{|I + \frac{1}{\sigma_r^2}p_1gg^H|}, \quad (5.23)$$

where $g$ 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

$$U_j(p_1, \mu_0) = \mu_0p_1\|g\|^2_2, \quad (5.24)$$

where $\mu_0$ 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):*

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

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

\[
U_L(Q_1, p_1) = \lambda_0 R_s - \mu_0 p_1 \|g\|_2^2
= \lambda_0 \left( \log \left| I + \frac{1}{\sigma_e^2} H_s Q_1 H_s^H \right| - \log \left| I + \frac{1}{\sigma_e^2} (H_e Q_1 H_e^H + p_1 g g^H) \right| \right) + \lambda_0 \log \left| I + \frac{1}{\sigma_e^2} p_1 g g^H \right| - \mu_0 p_1 \|g\|_2^2, \tag{5.26}
\]

where \(\lambda_0\) 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):**

\[
\max_{Q_1, p_1} U_L(Q_1, p_1), \quad \text{s.t.} \quad Q_1 \succeq 0, p_1 \geq 0. \tag{5.27}
\]

**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 \(Q_1^*\) and \(p_1^*\) be the optimal solution for **Problem (B)**, whereas \(\mu_0^*\) is the best price for **Problem (A)**. The solutions \(Q_1^*, p_1^*\) and \(\mu_0^*\) can be defined as the Stackelberg equilibrium if the following conditions hold for any set of \(Q_1, p_1\) and \(\mu_0\):

\[
U_L(Q_1^*, p_1^*, \mu_0^*) \geq U_L(Q_1, p_1, \mu_0^*), \quad U_j(Q_1^*, p_1^*, \mu_0^*) \geq U_j(Q_1, p_1, \mu_0^*). \tag{5.28}
\]
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 $Q_1$, then the best interference price $\mu_0^*$ can be achieved by solving Problem (A).

First, the interference requirement $p_1$ can be obtained for a given $Q_1$ by solving Problem (B), where the following lemma holds

**Lemma 5.1** The problem (5.27) for a given $Q_1$ 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:

$$\frac{\partial U_L(Q_1,p_1)}{\partial p_1} = 0, \quad \lambda_0 \text{Tr}[A_1^{-1}gg^H - A_2^{-1}gg^H] - \mu_0 \|g\|_2^2 = 0, \quad (5.28)$$

where

$$A_1 = \left(I + \frac{p_1}{\sigma^2}gg^H\right), \quad A_2 = I + \frac{1}{\sigma^2}(HcQ_1H^H + p_1gg^H).$$

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

$$p_1^* = \frac{-c_1 + c_2}{\sigma^2} + \sqrt{\frac{(c_1 - c_2)^2}{\sigma^4} + \frac{4\lambda_0 c_1 c_2 (c_1 - c_2)}{\mu_0 \|g\|_2^2}}, \quad (5.29)$$

where $c_1 = g^Hg$, $c_2 = g^HA^{-1}g$ and $A = I + \frac{1}{\sigma^2}Q_1H^H$, 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:

$$\max_{\mu_0} U_j(p_1^*,\mu_0), \quad s.t. \mu_0 \geq 0. \quad (5.30)$$
Substituting (5.30) with (5.29), the optimal solution of $\mu_0$ can be derived by the following Lemma:

**Lemma 5.2** The problem (5.30) for a fixed $Q_1$ is a convex problem in terms of $\mu_0$, and the optimal solution of $\mu_0$ can be expressed as

$$\mu_0^* = \frac{e}{x\|g\|^2},$$  \hspace{1cm} (5.31)

where

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

$$= -2(d - b^2 - b\sqrt{b^2 - d})$$

$$= 2\sqrt{b^2 - d}(\sqrt{b^2 - d} + b),$$ \hspace{1cm} (5.32)

where $a = \frac{c_1c_2}{\sigma^2}$, $b = \frac{c_1 + c_2}{\sigma^2}$, $d = \frac{(c_1 - c_2)^2}{\sigma^2}$ and $e = 4\lambda_0c_1c_2(c_1 - c_2)$.

**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 $\mu_0$, respectively. This confirms that there exists a Stackelberg equilibrium $(p_1^*, \mu_0^*)$ for the proposed Stackelberg game. To achieve this Stackelberg equilibrium, first, the private CJ announces a relatively low interference price $\mu_0$, 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 ($N_T = N_J = 4$) 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., $H_s$, $H_j$, $H_e$ and $H_{je}$) 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.
5.5 Simulation Results

![Graph showing convergence of the secrecy rate](image)

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

![Graph showing transmit power comparison](image)

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

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 $\tilde{Q}_1$ (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 $\|E_e\|^2 = 0.1$ and $\|E_{je}\|^2 = 0.1$. 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.

<table>
<thead>
<tr>
<th>Random channels</th>
<th>Robust scheme</th>
<th>Non-robust scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel 1</td>
<td>1.1695</td>
<td>0.9848</td>
</tr>
<tr>
<td>Channel 2</td>
<td>1.1445</td>
<td>0.9753</td>
</tr>
<tr>
<td>Channel 3</td>
<td>1.1096</td>
<td>0.9966</td>
</tr>
<tr>
<td>Channel 4</td>
<td>1.1006</td>
<td>0.9875</td>
</tr>
<tr>
<td>Channel 5</td>
<td>1.1131</td>
<td>0.9682</td>
</tr>
</tbody>
</table>

Table 5.4: The comparison of achieved secrecy rates of robust and non-robust power minimization scheme with target rate $R_s = 1$ bps/Hz.

<table>
<thead>
<tr>
<th>Random channels</th>
<th>Robust scheme</th>
<th>Non-robust scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel 1</td>
<td>2.4121</td>
<td>1.8112</td>
</tr>
<tr>
<td>Channel 2</td>
<td>3.8684</td>
<td>3.6255</td>
</tr>
<tr>
<td>Channel 3</td>
<td>2.3065</td>
<td>1.7519</td>
</tr>
<tr>
<td>Channel 4</td>
<td>3.0274</td>
<td>2.9007</td>
</tr>
<tr>
<td>Channel 5</td>
<td>1.3999</td>
<td>1.1407</td>
</tr>
</tbody>
</table>

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-
5.5 Simulation Results

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., $\mu_0$). As seen from Fig. 5.10, the private CJ revenue function is concave in terms of $\mu_0$, which supports the convexity of the private CJ revenue function. The optimal $\mu_0$ derived in (5.31) is validated by this result. Fig. 5.11 shows the optimal revenue function of the legitimate transmitter for a given $\mu_0^*$, and then a corresponding optimal value $p_1^*$ can be achieved, hence, $(p_1^*, \mu_0^*)$ defines the Stackelberg equilibrium as indicated in Fig. 5.11.

![Figure 5.9: Revenue function of the legitimate transmitter.](image)

### 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 Stackelberg 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

\[
\min_{Q_1} \text{Tr}(Q_1),
\]

\[
s.t. \quad \log \left| I + H_s Q_1 H_s^H + H_j Q_2 H_j^H \right| - t_1 - \log \left| I + \frac{1}{\sigma^2_e} H_j Q_2 H_j^H \right| + \log \left| I + \frac{1}{\sigma^2_e} H_{je} Q_2 H_{je}^H \right| \geq R_{sr},
\]

\[
\alpha - \beta + \text{Tr}[S_1 (H_e + E_e) Q_1 (H_e + E_e)^H] \leq t_1,
\]

\[
Q_1 \succeq 0, t_1 \geq 0, \|E_e\|_F^2 \leq \varepsilon^2_e.
\]

(5.33)

where

\[
\alpha = \log \left| I + H_e \tilde{Q}_1 H_e^H + H_{je} Q_2 H_{je}^H \right|, \quad \beta = \text{Tr} \left[ \left( I + H_e \tilde{Q}_1 H_e^H + H_{je} Q_2 H_{je}^H \right)^{-1} H_e \tilde{Q}_1 H_e^H \right],
\]

\[
S_1 = \left( I + H_e \tilde{Q}_1 H_e^H + H_{je} Q_2 H_{je}^H \right)^{-1}.
\]

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

\[
\alpha - \beta + \text{Tr}[S_1 (H_e + E_e) Q_1 (H_e + E_e)^H] \leq t_1 \iff \alpha - \beta + h_e^H B_1 h_e + 2\Re[a^H (Q_1 \otimes I)e_e] + e_e^H B_1 e_e \leq t_1,
\]

(5.34)
where
\[ h_e = \text{vec}(H_e), \quad e_e = \text{vec}(E_e), \quad a = \text{vec}(S_1H_e), \quad B_1 = (Q_1^T \otimes I)^T(I \otimes S_1). \]

In addition, the constraint \( e_e^H e_e \leq \varepsilon_e^2 \) 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 \( f_k(x), k = 1, 2, \) be defined as
\[
f_k(x) = x^H A_k x + 2\Re\{b_k^H x\} + c_k, \quad (5.35)
\]
where \( A_k = A_k^H \in \mathbb{C}^{n \times n}, \ b_k \in \mathbb{C}^n \) and \( c_k \in \mathbb{R}. \) The implication \( f_1(x) \geq 0 \implies f_2(x) \geq 0 \) holds if and only if there exists \( \mu \geq 0 \) such that
\[
\begin{bmatrix}
A_2 & b_2 \\
\frac{1}{2}b_2^H & c_2
\end{bmatrix} - \mu \begin{bmatrix}
A_1 & b_1 \\
\frac{1}{2}b_1^H & c_1
\end{bmatrix} \succeq 0, \quad (5.36)
\]
provided there exists a point \( \tilde{x} \) with \( f_1(\tilde{x}) > 0. \)

By exploiting S-Procedure shown in Lemma 5.3, the constraint in (5.34) can be written as
\[
\begin{bmatrix}
\mu_1 I - B_1 \\
-a^H (Q_1^T \otimes I)^* - \mu \varepsilon_e^2 - \alpha + \beta + t_1 - h_e^H B_1 h_e
\end{bmatrix} \succeq 0. \quad (5.37)
\]
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:
\[
\log \left| I + \tilde{H}_j e Q_2 \tilde{H}_j^H \right| \geq \log(t_2), \quad (5.38a)
\]
\[
\alpha_2 - \beta_2 + \text{Tr} \left[ S_2 \tilde{H}_j e Q_2 \tilde{H}_j^H \right] \leq t_3. \quad (5.38b)
\]
For (5.38a), the following matrix inequality is required

$$|I + A| \geq 1 + \text{Tr}(A), \quad (5.39)$$

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

$$\log |I + \tilde{H}_{je}Q_2\tilde{H}_{je}^H| \geq \log(t_2) \Rightarrow \log[1 + \text{Tr}(\tilde{H}_{je}Q_2\tilde{H}_{je}^H)] \geq \log(t_2),$$

$$\Rightarrow \text{Tr}(\tilde{H}_{je}Q_2\tilde{H}_{je}^H) \geq t_2 - 1. \quad (5.40)$$

Besides, from the following matrix identities:

$$\text{Vec}(AXB) = (B^T \otimes A)\text{Vec}(X), \quad \text{Tr}(ATB) = \text{Vec}(A)^T\text{Vec}(B),$$

$$(A \otimes B)^T = A^T \otimes B^T.$$  

The constraint in (5.40) can be expressed as,

$$e_{je}^H A e_{je} + 2\Re \left[ a_{je}^H A e_{je} \right] + h_{je}^H A h_{je} - t_2 + 1 \geq 0,$$

$$e_{je}^H e_{je} \leq \varepsilon_{je}^2, \quad (5.41)$$

where $A = Q_2^T \otimes I$, $h_{je} = \text{vec}(H_{je})$, and $e_{je} = \text{vec}(E_{je})$. Similarly, by exploiting Lemma 5.3, the constraint (5.38a) is reformulated into the following linear matrix inequality (LMI):}

$$\begin{bmatrix} \lambda_1 I + (Q_2^T \otimes I) & (Q_2^T \otimes I)h_{je} \\ h_{je}^T(Q_2^T \otimes I) & -\lambda_1 \varepsilon_{je}^2 - t_2 + h_{je}^H(Q_2^T \otimes I)h_{je} + 1 \end{bmatrix} \succeq 0. \quad (5.42)$$

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

$$\begin{bmatrix} \lambda_2 I - B_2 & -(Q_2^T \otimes I)^T a_1 \\ -a_1^T(Q_2^T \otimes I)^* & -\lambda_2 \varepsilon_{je}^2 - \alpha_2 + \beta_2 + t_3 - h_{je}^H B_2 h_{je} \end{bmatrix} \succeq 0, \quad (5.43)$$

where $\alpha_2$, $\beta_2$, $S_2$, $h_{je}$, $a_1$ and $B_2$ 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

\[ U_L(Q_1,p_1) = \lambda_0 \left( \log |A_0| - \log |I + \frac{1}{\sigma_e^2}(H_s Q_1 H_e^H + p_1 g g^H)| \right) \]
\[ + \lambda_0 \log |I + \frac{1}{\sigma_e^2}p_1 g g^H| - \mu_0 p_1 \|g\|_2^2, \]  

(5.44)

where \( A_0 = I + \frac{1}{\sigma_e^2}H_s Q_1 H_e^H \). In order to show that the function (5.44) is convex with respect to \( p_1 \), its first derivative is considered as follows:

\[
\frac{\partial U_L(Q_1,p_1)}{\partial p_1} = -\lambda_0 \frac{\partial}{\partial p_1} \left( \log |I + \frac{1}{\sigma_e^2}(H_s Q_1 H_e^H + p_1 g g^H)| \right) \\
+ \lambda_0 \frac{\partial}{\partial p_1} \left( \log |I + \frac{p_1}{\sigma_e^2}g g^H| - \mu_0 p_1 \|g\|_2^2 \right).
\]

(5.45)

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

\[
\frac{\partial \ln(\det X)}{\partial X} = \text{Tr}[X^{-1} \partial X], \quad \frac{\partial \ln(\det AZ^{-1})}{\partial Z} = \text{Tr}[Z^{-1} AZ^{-1} \partial Z].
\]

For the term \( \log |I + \frac{p_1}{\sigma_e^2}g g^H| \):

First derivative:

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

(5.46)

Second derivative:

\[
\frac{\partial^2}{\partial^2 p_1} \log |I + \frac{p_1}{\sigma_e^2}g g^H| = -\text{Tr} \left( A_{\frac{1}{\sigma_e^2}}^{-1} g g^H A_{\frac{1}{\sigma_e^2}}^{-1} g g^H \right).
\]

(5.47)

Similarly, for the term \( \log |I + \frac{1}{\sigma_e^2}(H_s Q_1 H_e^H + p_1 g g^H)| \):

First derivative:

\[
\frac{\partial}{\partial p_1} \left( \log |I + \frac{1}{\sigma_e^2}(H_s Q_1 H_e^H + p_1 g g^H)| \right) = \text{Tr} \left( \left( I + \frac{1}{\sigma_e^2}(H_s Q_1 H_e^H + p_1 g g^H) \right)^{-1} g g^H \right) \sigma_e^2.
\]

(5.48)
Second derivative:
\[
\frac{\partial^2}{\partial^2 p_1} \left( \log \left| I + \frac{1}{\sigma_e^2} (H_e Q_1 H_e^H + p_1 gg^H) \right| \right) = - \text{Tr} \left[ A_2^{-1} \frac{gg^H}{\sigma_e^2} A_2^{-1} \frac{gg^H}{\sigma_e^2} \right].
\] (5.49)

Thus
\[
\frac{\partial^2}{\partial^2 p_1} U_L(Q_1, p_1) = \text{Tr} \left[ A_2^{-1} \frac{gg^H}{\sigma_e^2} A_2^{-1} \frac{gg^H}{\sigma_e^2} \right] - \text{Tr} \left[ A_1^{-1} \frac{gg^H}{\sigma_e^2} A_1^{-1} \frac{gg^H}{\sigma_e^2} \right],
\] (5.50)

where
\[
A_1 = I + \frac{1}{\sigma_e^2} p_1 gg^H, \quad A_2 = I + \frac{1}{\sigma_e^2} \left( H_e Q_1 H_e^H + p_1 gg^H \right).
\]

Since the eigenvalues of \(A_2^{-1}\) are smaller than that of \(A_1^{-1}\), the following holds:
\[
A_2^{-1} - A_1^{-1} \leq 0, \quad g^H (A_2^{-1} - A_1^{-1}) g \leq 0,
\]
\[
g^H A_2^{-1} gg^H A_2^{-1} g \leq g^H A_1^{-1} gg^H A_1^{-1} g.
\]
\[
\text{Tr} \left[ A_2^{-1} \frac{gg^H}{\sigma_e^2} A_2^{-1} \frac{gg^H}{\sigma_e^2} \right] \leq \text{Tr} \left[ A_1^{-1} \frac{gg^H}{\sigma_e^2} A_1^{-1} \frac{gg^H}{\sigma_e^2} \right].
\]

Hence, \(\frac{\partial^2 U_L(Q_1, p_1)}{\partial^2 p_1} \leq 0\), which proves that \(U_L(Q_1, p_1)\) is a concave function in terms of \(p_1\) for a fixed \(Q_1\). This completes the proof.

\[\Box\]

### 5.7.4 Proof of Lemma 5.2

The KKT condition in (5.28) is rewritten as
\[
\lambda_0 \text{Tr} \left[ A_1^{-1} gg^H - A_2^{-1} gg^H \right] - \mu_0 \| g \|_2^2 = 0,
\] (5.51)

where \(A_1\) and \(A_2\) have been defined after (5.28). From the following matrix identity,
\[
(A + bc^T)^{-1} = A^{-1} - \frac{A^{-1} bc^T A^{-1}}{1 + c^T A^{-1} b},
\] (5.52)
\(A_i^{-1}\) and \(A_2^{-1}\) in (5.51) can be expressed as follows:

\[
A_i^{-1} = I - \frac{\frac{p_1}{\sigma_e} gg^H}{1 + \frac{p_1}{\sigma_e} g^H g}, \quad (5.53a)
\]

\[
A_2^{-1} = A^{-1} - \frac{\frac{p_1}{\sigma_e} A^{-1} gg^H A^{-1}}{1 + \frac{p_1}{\sigma_e} g^H A^{-1} g}, \quad (5.53b)
\]

where \(A = I + \frac{1}{\sigma_e} H_e Q_e H_e^H\). Based on (5.53), the KKT condition in (5.51) can be equivalently modified as

\[
\begin{align*}
\lambda_0 \text{Tr}(gg^H) - \lambda_0 \frac{\frac{p_1}{\sigma_e} \text{Tr}(gg^H gg^H)}{1 + \frac{p_1}{\sigma_e} g^H g} - 
\lambda_0 \text{Tr}(A^{-1} gg^H) \\
+ \lambda_0 \frac{\frac{p_1}{\sigma_e} \text{Tr}(A^{-1} gg^H A^{-1} gg^H)}{1 + \frac{p_1}{\sigma_e} g^H A^{-1} g} - \mu_0 \|g\|^2 = 0.
\end{align*}
\]

(5.54)

Setting \(c_1 = g^H g, c_2 = g^H A^{-1} g\),

\[
\begin{align*}
\frac{\lambda_0 c_1}{1 + \frac{p_1}{\sigma_e} c_1} - \frac{\lambda_0 c_2}{1 + \frac{p_1}{\sigma_e} c_2} - \mu_0 \|g\|^2 = 0, \quad (5.55)
\end{align*}
\]

\[
\frac{c_1 c_2}{\sigma_e^4} p_1^2 + \frac{c_1 + c_2}{\sigma_e^2} p_1 + \left(1 - \frac{\lambda_0 (c_1 - c_2)}{\mu_0 \|g\|^2}\right) = 0, \quad (5.56)
\]

It is easy to show that

\[\sqrt{(\frac{c_1 + c_2}{\sigma_e^2})^2 - 4 \frac{c_1 c_2}{\sigma_e^2} \left[1 - \frac{\lambda_0 (c_1 - c_2)}{\mu_0 \|g\|^2}\right]} \geq 0\]

by showing \(c_1 - c_2 \geq 0\), which holds if \(g^H (I - A^{-1}) g \geq 0\). Thus, \(I - A^{-1} \succeq 0\) can be shown as follows:

\[
I - A^{-1} \succeq 0, \iff I \succeq A^{-1} \iff \text{Tr}(I) \geq \text{Tr}(A^{-1}), \quad (5.57)
\]

Since \(\text{Tr}(A) = \sum_{i=1}^{N_E} \lambda_i\) and \(A\) is positive definite matrix, and \(\lambda_i \geq 1\) represents the \(i\)-th eigenvalue of the matrix \(A\), the \(i\)-th eigenvalue of \(A^{-1}\) is \(\frac{1}{\lambda_i} \leq 1\) holds if \(\lambda_i \neq 0\) in terms of \(\lambda_i \geq 1\), which implies \(\text{Tr}(A^{-1}) \leq \text{Tr}(I) = M_E\). Thus, \(c_1 \geq c_2\) holds.

From \(p_1 \geq 0\), the optimal solution of \(p_1\) can be derived as

\[
p_1^* = \frac{-c_1 + c_2}{\sigma_e^2} + \sqrt{\left(\frac{c_1 + c_2}{\sigma_e^2}\right)^2 + \frac{4 \lambda_0 c_1 c_2 (c_1 - c_2)}{\mu_0 \|g\|^2}} \cdot \frac{2 c_1 c_2}{\sigma_e^4}.
\]

(5.58)
The revenue function of the jammer can be written in terms of \( \mu_0 \) by substituting \( p_1^* \) as

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

(5.59)

where \( a = \frac{c_1\sigma_z}{\sigma_c^4} \), \( b = \frac{c_1 + c_2}{\sigma_c^2} \) and \( d = \frac{(c_1 - c_2)^2}{\sigma_c^2} \). 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 \( \mu_0 \) as follows:

\[
\frac{\partial U_j}{\partial \mu_0} = -\frac{b}{2a} \|g\|^2 + \frac{\|g\|^2}{2a} \left( d + 2 \frac{4 \lambda_0 c_1 c_2 (c_1 - c_2)}{\mu_0 \|g\|^2} \right)^{\frac{1}{2}} + \frac{\|g\|^2}{4a} \left( d + \frac{4 \lambda_0 c_1 c_2 (c_1 - c_2)}{\mu_0 \|g\|^2} \right)^{-\frac{1}{2}} \left( -\frac{4 \lambda_0 c_1 c_2 (c_1 - c_2)}{\mu_0 \|g\|^2} \right),
\]

(5.60)

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

(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 \( \mu_0 \). The optimal solution of \( \mu_0 \) can be derived as follows:

\[
\frac{\partial U_j}{\partial \mu_0} = 0, \Rightarrow \mu_0^* = \frac{e}{x \|g\|^2},
\]

(5.62)

where

\[
x = -\frac{d \|g\|^2}{2a} - \frac{\|g\|^4}{4a} + \frac{\|g\|^2}{2a} \sqrt{\frac{(b^2 - d) \|g\|^4}{4a}},
\]

(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
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 $h_s \in \mathbb{C}^{N_T \times 1}$, $h_{e,k} \in \mathbb{C}^{N_T \times 1}$ and $h_l \in \mathbb{C}^{N_T \times 1}$, respectively. The noise power at the legitimate user and the eavesdroppers are assumed to be $\sigma_s^2$ and $\sigma_e^2$. The received signal at the legitimate user and the $k$-th eavesdropper can be written as

$$y_s = h_s^H w_s + n_s, \quad y_{e,k} = h_{e,k}^H w_s + n_{e,k}, \quad k = 1, ..., K,$$

where $s$ and $w \in \mathbb{C}^{N_T \times 1}$ are the desired signal for the legitimate user ($\mathbb{E}\{s^2\} = 1$) and the transmit beamformer at the legitimate transmitter, respectively. In addition, $n_s \sim \mathbb{C}\mathbb{N}(0, \sigma_s^2)$ and $n_{e,k} \sim \mathbb{C}\mathbb{N}(0, \sigma_e^2)$ 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:

$$R_s = \left[ \log \left( 1 + \frac{|h_s^H w|^2}{\sigma_s^2} \right) - \max_k \log \left( 1 + \frac{|h_{e,k}^H w|^2}{\sigma_e^2} \right) \right]^+, \forall k. \quad (6.1)$$
6.2 Transmit Optimization for Secrecy Rate Maximization

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

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

(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 dependent 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:

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

(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)
6.2 Transmit Optimization for Secrecy Rate Maximization

Table 6.1: Bisection methods

1. Given lower and upper bound of the targeted secrecy rate $R_{\text{min}}$ and $R_{\text{max}}$, and a desired solution accuracy $\tau$ (very small value).

2. Setting $R = (R_{\text{min}} + R_{\text{max}})/2$.

3. **Iteration loop begin**
   
   (a) Solve the corresponding power minimization problem in (6.4) using the relaxation method to obtain the beamformer $w$.
   
   (b) Compute the transmit power $\tilde{P} = \|w\|^2$.
   
   (c) If $\tilde{P} \leq P$, then $R_{\text{min}} = R$; otherwise, $R_{\text{max}} = R$.
   
   (d) **Until** $R_{\text{max}} - R_{\text{min}} \leq \tau$, **break**.

4. **Iteration loop end**

5. $R$ is the achieved secrecy rate of the secrecy rate maximization problem, and $w$ 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

\[
\min_w \|w\|^2, \quad \text{s.t.} \quad R_s \geq R, \quad \min_l E_l \geq E, \quad \forall k, l. \tag{6.4}
\]

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
\[
\min_w \|w\|^2, \quad \text{s.t.} \quad \log \left( 1 + \frac{|h_s^Hw|^2}{\sigma_s^2} \right) - \log \left( 1 + \frac{|h_{e,k}^Hw|^2}{\sigma_e^2} \right) \geq R, \quad \forall k,
\]
\[|h_l^Hw|^2 \geq E, \quad \forall l. \quad (6.5)\]

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:

\[
\min_{w,s_1} s_1, \quad \text{s.t.} \quad \begin{bmatrix} s_1 \\ w \end{bmatrix} \succeq_k 0,
\]
\[
S_k = \begin{bmatrix}
    \frac{1}{\sigma_s} w^H h_s I & \frac{zR}{\sigma_e} w^H h_{e,k} \\
    (2R - 1)^\frac{1}{2} & \frac{1}{\sigma_s} w^H h_s
\end{bmatrix}^H \begin{bmatrix}
    \frac{zR}{\sigma_e} w^H h_{e,k} \\
    (2R - 1)^\frac{1}{2}
\end{bmatrix} \succeq 0, \quad \forall k,
\]
\[x_l = \Re\{w^H h_l\}, \quad y_l = \Im\{w^H h_l\}, \quad u_l = [x_l \ y_l],
\]
\[\|u_l^{(n)}\|^2 + 2 \sum_{i=1}^2 u_l^{(n)}(i)[u_l(i) - u_l^{(n)}(i)] \geq E, \quad \forall l. \quad (6.6)\]

**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 \(u_l\). An initialization value of the vector \(u_l\) is randomly generated and can be updated at each iteration. The algorithm converges when \(u_l^{(n+1)} = u_l^{(n)}\) 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

\[ h_s = \bar{h}_s + e_s, \]
\[ h_{e,k} = \bar{h}_{e,k} + e_{e,k}, \forall k, \]
\[ h_l = \bar{h}_l + e_l, \forall l, \]

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

\[ \|e_s\|_2 = \|h_s - \bar{h}_s\|_2 \leq \varepsilon_s, \text{for } \varepsilon_s \geq 0, \]
\[ \|e_{e,k}\|_2 = \|h_{e,k} - \bar{h}_{e,k}\|_2 \leq \varepsilon_{e,k}, \text{for } \varepsilon_{e,k} \geq 0, \forall k, \]
\[ \|e_l\|_2 = \|h_l - \bar{h}_l\|_2 \leq \varepsilon_l, \text{for } \varepsilon_l \geq 0, \forall l, \]

where \( \varepsilon_s, \varepsilon_{e,k} \) and \( \varepsilon_l \) 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

\[
\begin{align*}
\min_{w} & \|w\|^2, \\
\text{s.t. } & \min_{e_s} \log \left(1 + \frac{|(\bar{h}_s + e_s)^H w|^2}{\sigma_s^2}\right) - \max_{e_{e,k}} \log \left(1 + \frac{|(\bar{h}_{e,k} + e_{e,k})^H w|^2}{\sigma_e^2}\right) \geq R, \forall k, \\
 & \min_{e_l} |(\bar{h}_l + e_l)^H w|^2 \geq E, \forall l.
\end{align*}
\]

(6.7a)  (6.7b)
6.2 Transmit Optimization for Secrecy Rate Maximization

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

\[
\begin{align*}
\frac{1}{\sigma_s} \left( w^H \bar{h}_s - \varepsilon_s \| w \| \right) & \geq \sqrt{t_2}, \\
\left[ \frac{2B}{\sigma_e} (\bar{h}_{e,k} + e_{e,k})^H w \right] \left( 2^R - 1 \right)^{\frac{1}{2}} & \leq t_2,
\end{align*}
\]

(6.8)

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

\[
\frac{1}{\sigma_s} \Re\{ w^H \bar{h}_s \} - \frac{\varepsilon_s}{\sigma_s} \| w \| \geq f^{(n)}(t_2),
\]

(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

\[
\bar{S}_k = \begin{bmatrix}
S_{k,1} - \lambda_k \begin{bmatrix} 0 & -1 \\ 0 & -1 \end{bmatrix} & -\varepsilon_{e,k} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\
-\varepsilon_{e,k} \begin{bmatrix} 2B_{\sigma_e} w^H \\ 0 \\ 0 \end{bmatrix} & \lambda_k \begin{bmatrix} 2B_{\sigma_e} w^H \\ (2^R - 1)^{\frac{1}{2}} \end{bmatrix}
\end{bmatrix} \succeq 0, \forall k.
\]

(6.10)

where

\[
S_{k,1} = \begin{bmatrix}
f^{(n)}(t_2)I & \frac{2B_{\sigma_e} w^H \bar{h}_{e,k}}{(2^R - 1)^{\frac{1}{2}}} \\
\frac{2B_{\sigma_e} w^H \bar{h}_{e,k}}{(2^R - 1)^{\frac{1}{2}}} & f^{(n)}(t_2)
\end{bmatrix},
\]

(6.11)

**Proof** Please refer to Section 6.6.2.
Thus, the robust power minimization problem can be written as

\[
\begin{align*}
\min_{s_2, w, \lambda_k} & \quad s_2, \quad s.t. \quad \begin{bmatrix} s_2 \\ w \end{bmatrix} \succeq_k 0, \\
\mathbf{S}_k(\lambda_k, f^n(t_2)) & \succeq 0, \quad \forall k, \\
\frac{1}{\sigma_s} w^H \mathbf{h}_s - \frac{\varepsilon_s}{\sigma_s} \|w\| & \geq f^n(t_2), \\
\Re\{\mathbf{h}_l^H w\} & \geq E_l^2 + \varepsilon_l \|w\|_2, \quad \Im\{\mathbf{h}_l^H w\} = 0, \quad \forall l.
\end{align*}
\] (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 \(x = ws + v\), and the secure transmit beamformer (i.e., \(w\)) and AN (i.e., \(v \sim \mathcal{CN}(0, V)\)) are jointly designed. This optimization problem can be formulated as

\[
\begin{align*}
\max_{w, V} & \quad \min_k R_s - R_{e,k}, \\
\text{s.t.} & \quad \|w\|^2 + \text{Tr}(V) \leq P, \quad [ww^H]_{(i,i)} + [V]_{(i,i)} \leq p_i, \quad \forall i, \\
& \quad \min_l |\mathbf{h}_l^H w|^2 + \mathbf{h}_l^H V \mathbf{h}_l \geq E_l, \quad \forall l, \quad V \succeq 0.
\end{align*}
\] (6.13)
where \([\textbf{w}\textbf{w}^H]_{(i,i)} + [\textbf{V}]_{(i,i)} \ (i = 1, ..., N_T)\) represents each antenna transmit power constraint, and the mutual information at the legitimate user and \(k\)-th eavesdropper can be written as

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

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 \(\textbf{Q}_s = \textbf{w}\textbf{w}^H\) as

\[
\max_{\textbf{Q}_s, \textbf{V}} \log \left( 1 + \frac{\textbf{h}_s^H \textbf{Q}_s \textbf{h}_s}{\textbf{h}_s^H \textbf{V}\textbf{h}_s + \sigma_s^2} \right) - \max_k \log \left( 1 + \frac{\textbf{h}_{e,k}^H \textbf{Q}_s \textbf{h}_{e,k}}{\textbf{h}_{e,k}^H \textbf{V}\textbf{h}_{e,k} + \sigma_e^2} \right),
\]

\[ \text{s.t.} \ \text{Tr}(\textbf{Q}_s + \textbf{V}) \leq P, \ \text{Tr}[\textbf{A}_i(\textbf{Q}_s + \textbf{V})] \leq p_i, \ \forall i, \quad (6.14a) \]

\[ \textbf{h}_l^H(\textbf{Q}_s + \textbf{V})\textbf{h}_l \geq E_l, \ \forall l, \quad (6.14b) \]

\[ \textbf{Q}_s \succeq 0, \ \textbf{V} \succeq 0, \quad (6.14c) \]

\[ \text{rank}(\textbf{Q}_s) = 1, \]

where \(\textbf{A}_i = \textbf{a}_i\textbf{a}_i^H\) is the given antenna design parameters to adjust each antenna power budget, and \(\textbf{a}_i\) is a unit \(i\)-th vector (i.e., \([\textbf{a}_i]_j = 1\) for \(i = j\) and \([\textbf{a}_i]_j = 0\) 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

$$\max_{Q_s, V, t} R_s + \log(t),$$
\[s.t. \log\left(1 + \frac{h_{e,k}^H Q_s h_{e,k}}{h_{e,k}^H V h_{e,k} + \sigma_e^2}\right) \leq \log\left(\frac{1}{t}\right), \forall k, \quad (6.15a)\]
\[(6.14a), (6.14b), (6.14c), \text{rank}(Q_s) = 1. \quad (6.15b)\]

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

$$\max_t \log(1 + f(t)) + \log(t), \quad s.t. \ t_{\min} \leq t \leq 1, \quad (6.16)$$

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

$$t \geq \left(1 + \frac{h_s^H Q_s h_s}{h_s^H V h_s + \sigma_s^2}\right)^{-1} \geq \left(1 + \frac{h_s^H Q_s h_s}{\sigma_s^2}\right)^{-1} \geq \left(1 + \frac{\lambda_{\max}(Q_s)\|h_s\|^2}{\sigma_s^2}\right)^{-1} \geq \left(1 + \frac{\text{Tr}(Q_s)\|h_s\|^2}{\sigma_s^2}\right)^{-1} \geq \left(1 + \frac{P\|h_s\|^2}{\sigma_s^2}\right)^{-1} = t_{\min}, \quad (6.17)$$

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

$$f(t) = \max_{Q_s, V} \frac{h_s^H Q_s h_s}{h_s^H V h_s + \sigma_s^2},$$
\[s.t. (6.15a), (6.14a), (6.14b), (6.14c), \quad \text{rank}(Q_s) = 1. \quad (6.18)\]

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

$$h_{e,k}^H \left[Q_s - \left(\frac{1}{t} - 1\right)V\right] h_{e,k} \leq \left(\frac{1}{t} - 1\right)\sigma_e^2. \quad (6.19)$$
Then, (6.18) can be recast for a given $t$ as

$$f(t) = \max_{Q, V} \frac{h_s^H Q_s h_s}{h_s^H V h_s + \sigma_s^2},$$

s.t. (6.19), (6.14a), (6.14b), (6.14c), rank($Q_s$) = 1. \hspace{1cm} (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 $\delta$ so that the following relations hold:

$$Q_s = \frac{\bar{Q}_s}{\delta}, \hspace{0.5cm} V = \frac{\bar{V}}{\delta}$$ \hspace{1cm} (6.21)

Thus, the problem (6.20) is relaxed as

$$f(t) = \max_{\bar{Q}_s, \bar{V}, \delta} \bar{h}_s^H \bar{Q}_s \bar{h}_s,$$

s.t. $\bar{h}_s^H \bar{V} \bar{h}_s + \delta \sigma_s^2 = 1,$

$$\bar{h}_{e,k}^H \left[ \bar{Q}_s - \left( \frac{1}{t} - 1 \right) \bar{V} \right] \bar{h}_{e,k} \leq \left( \frac{1}{t} - 1 \right) \delta \sigma_e^2,$$

$$\text{Tr}(\bar{Q}_s + \bar{V}) \leq \delta P, \hspace{0.5cm} \text{Tr}[A_i(\bar{Q}_s + \bar{V})] \leq \delta p_i, \forall i,$$

$$\bar{h}_l^H (\bar{Q}_s + \bar{V}) \bar{h}_l \geq \delta E_l, \forall l, \hspace{0.5cm} \bar{Q}_s \succeq 0, \hspace{0.5cm} \bar{V} \succeq 0.$$ \hspace{1cm} (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,

$$\frac{h_s^H Q_s h_s}{h_s^H V h_s + \sigma_s^2} \geq f(t) \Rightarrow h_s^H [Q_s - f(t) V] h_s \geq f(t) \sigma_s^2,$$ \hspace{1cm} (6.23)
Thus, the following power minimization problem is considered

$$\begin{align*}
\min_{Q_s, V} & \quad \text{Tr}(Q_s) \\
\text{s.t.} & \quad (6.23), (6.19), (6.14a), (6.14b), (6.14c). 
\end{align*}$$

(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 \((Q_s, V)\) to (6.24) such that \(\text{rank}(Q_s) = 1\).

**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

$$\begin{align*}
\min_{Q_s, V} & \quad \max_k \frac{\left(\sigma_e^2 + \text{Tr}[h_{e,k}h_{e,k}^H(Q_s + V)]\right)\left(\sigma_s^2 + \text{Tr}(h_s h_s^H V)\right)}{\left(\sigma_e^2 + \text{Tr}[h_s h_s^H(Q_s + V)]\right)\left(\sigma_e^2 + \text{Tr}(h_{e,k} h_{e,k}^H V)\right)} \\
\text{s.t.} & \quad \text{Tr}(Q_s + V) \leq P, \quad \text{Tr}[A_i(Q_s + V)] \leq p_i, \quad \forall i, \\
& \quad h_i^H(Q_s + V)h_i \geq E_i, \quad \forall l, \\
& \quad Q_s \succeq 0, \quad V \succeq 0, \quad \text{rank}(Q_s) = 1. 
\end{align*}$$

(6.25a)

(6.25b)

(6.25c)

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

$$\begin{align*}
e^{x_0} &= \sigma_s^2 + \text{Tr}[h_s h_s^H(Q_s + V)] \quad e^{x_k} = \sigma_e^2 + \text{Tr}(h_{e,k} h_{e,k}^H V), \\
e^{y_k} &= \sigma_e^2 + \text{Tr}[h_{e,k} h_{e,k}^H(Q_s + V)] \quad e^{y_0} = \sigma_s^2 + \text{Tr}(h_s h_s^H V). 
\end{align*}$$

(6.26)
Thus, (6.25) can be written by introducing a slack variable $\tau$ as

$$
\min_{Q_s, V, x_0, y_0, x_k, y_k} \tau \\
\text{s.t.} \ e^{y_0 - x_0 + y_k - x_k} \leq \tau,
$$

(6.27a)

$$
\sigma_s^2 + \text{Tr}[h_s h_s^H (Q_s + V)] \geq e^{x_0}, \sigma_e^2 + \text{Tr}(h_e h_e^H V) \geq e^{x_k},
$$

(6.27b)

$$
\sigma_s^2 + \text{Tr}[h_e h_e^H (Q_s + V)] \leq e^{y_k}, \sigma_e^2 + \text{Tr}(h_s h_s^H V) \leq e^{y_0},
$$

(6.27c)

$$
(6.25a), (6.25b), (6.25c), \forall k, l, i.
$$

(6.27d)

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

$$
\sigma_e^2 + \text{Tr}[h_e h_e^H (Q_s + V)] \leq e^{y_k} (y_k - \hat{y}_k + 1),
$$

(6.28a)

$$
\sigma_s^2 + \text{Tr}(h_s h_s^H V) \leq e^{y_0} (y_0 - \hat{y}_0 + 1),
$$

(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

$$
\min_{Q_s, V, x_0, y_0, x_k, y_k, \tau} \tau \\
\text{s.t.} \ (6.25a), (6.25b), (6.27b), (6.27c), (6.28), \forall k, l, i, \\
Q_s \succeq 0, \ V \succeq 0, \ \text{rank}(Q_s) = 1.
$$

(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 $(Q_s^*(n), V^*(n), x_0^*(n), y_0^*(n), x_k^*(n), y_k^*(n), \tau^*(n))$, 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 $(Q_s^*, V^*)$ 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 \((Q_s[0], V[0])\) so that (6.27) is feasible, and given \(\kappa\) 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 \((Q_s[n], V[n])\).

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:

\[
\min_{Q_s, V} \text{Tr}(Q_s) \\
s.t. (6.25a), (6.25b), Q_s \succeq 0, V \succeq 0, \\
\sigma_s^2 + \text{Tr}(h_s h_s^H (Q_s + V)) \geq e_x^s, \sigma_e^2 + \text{Tr}(h_{e,k} h_{e,k}^H V) \geq e_x^e, \\
\sigma_e^2 + \text{Tr}(h_{e,k} h_{e,k}^H (Q_s + V)) \leq e_y^e, \sigma_s^2 + \text{Tr}(h_s h_s^H V) \leq e_y^s, \\
\forall k, l, i. \\
\tag{6.30}
\]

It is assumed that the optimal solutions to (6.30) can be denoted as \((\hat{Q}_s, \hat{V})\), which are the feasible solutions to (6.25) with the objective value \(\hat{\tau}\) obtained by substituting \((\hat{Q}_s, \hat{V})\) into (6.25), and \(\hat{\tau} \leq \tau^*\) holds, which implies \((\hat{Q}_s, \hat{V})\) is at least the same optimal solution \((Q^*_s, V^*)\) 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

$$\mathbf{A}_i = \bar{\mathbf{A}}_i + \Delta_i, \quad \| \Delta_i \|_F \leq \epsilon_i, \quad \forall i,$$

(6.31)

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

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

s.t. \( (\tilde{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k})^H \left[ \mathbf{Q}_s - \left( \frac{1}{t} - 1 \right) \mathbf{V} \right] (\tilde{\mathbf{h}}_{e,k} + \mathbf{e}_{e,k}) \leq \left( \frac{1}{t} - 1 \right) \sigma^2_e, \)

$$\text{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P, \quad \max_{\Delta_i} \text{Tr}[(\tilde{\mathbf{A}}_i + \Delta_i)(\mathbf{Q}_s + \mathbf{V})] \leq p_i,$$

$$(\tilde{\mathbf{h}}_l + \mathbf{e}_l)^H (\mathbf{Q}_s + \mathbf{V})(\tilde{\mathbf{h}}_l + \mathbf{e}_l) \geq E_l, \quad \forall l,$$

$$\mathbf{Q}_s \succeq 0, \mathbf{V} \succeq 0, \text{rank}(\mathbf{Q}_s) = 1.$$

(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

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

s.t. \( \text{Tr}(\mathbf{Q}_s + \mathbf{V}) \leq P, \quad \text{Tr}[\tilde{\mathbf{A}}_i(\mathbf{Q}_s + \mathbf{V})] + \epsilon_i \| \mathbf{Q}_s + \mathbf{V} \|_F \leq p_i, \quad \forall i, \)

$$\left[ \begin{array}{c} \lambda_{e,k} \mathbf{I} - [\mathbf{Q}_s - (\frac{1}{t} - 1) \mathbf{V}] - [\mathbf{Q}_s - (\frac{1}{t} - 1) \mathbf{V}] \tilde{\mathbf{h}}_{e,k} \\ -\tilde{\mathbf{h}}_{e,k}^H [\mathbf{Q}_s - (\frac{1}{t} - 1) \mathbf{V}] \end{array} \right] \succeq 0, \quad \forall k, \quad (6.33a)$$

$$\left[ \begin{array}{c} \alpha_l \mathbf{I} + (\mathbf{Q}_s + \mathbf{V}) (\mathbf{Q}_s + \mathbf{V}) \tilde{\mathbf{h}}_l \\ \tilde{\mathbf{h}}_l^H (\mathbf{Q}_s + \mathbf{V}) \tilde{\mathbf{h}}_l - E_l - \alpha_l \epsilon^2_l \end{array} \right] \succeq 0, \quad \forall l, \quad (6.33b)$$

$$\mathbf{Q}_s \succeq 0, \mathbf{V} \succeq 0, \quad \text{rank}(\mathbf{Q}_s) = 1.$$

(6.33d)
where \( c_k = -\widetilde{h}_{e,k}^H[(\bar{Q}_s - \frac{1}{t} - 1)\bar{V}]\bar{h}_{e,k} + (\frac{1}{t} - 1)\sigma^2_e - \lambda e_k\varepsilon^2 e_k \). Then, a slack variable \( \tau \) 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

\[
 f(t) = \max_{Q_s, V, \lambda, \mu, \lambda_e, \alpha, \delta, \tau} \tau, \\
 \text{s.t.} \left[ \begin{array}{cc} \lambda s I + \bar{Q}_s & \bar{Q}_s \bar{h}_s \\ \bar{h}_s^H \bar{Q}_s & \bar{h}_s^H \bar{Q}_s \bar{h}_s - \tau - \lambda \varepsilon^2_s \\ \mu s I - \bar{V} & -\bar{V} \bar{h}_s \\ -\bar{h}_s^H \bar{V} & -\bar{h}_s^H \bar{V} \bar{h}_s - \delta \sigma^2_s - 1 - \mu \varepsilon^2_s \\ \lambda e_k I - [\bar{Q}_s - (\frac{1}{t} - 1)\bar{V}] & -[\bar{Q}_s - (\frac{1}{t} - 1)\bar{V}]\bar{h}_{e,k} \\ -\bar{h}_s^H [\bar{Q}_s - (\frac{1}{t} - 1)\bar{V}] & \bar{h}_{e,k} \\ \alpha l I + (\bar{Q}_s + \bar{V}) & (\bar{Q}_s + \bar{V}) \bar{h}_l \\ \bar{h}_l^H (\bar{Q}_s + \bar{V}) & \bar{h}_l^H (\bar{Q}_s + \bar{V}) \bar{h}_l - \delta E_l - \alpha \varepsilon^2_l \\ \text{Tr}[\bar{A}_l (\bar{Q}_s + \bar{V})] + \epsilon_l \|\bar{Q}_s + \bar{V}\|_F \leq \delta p_l, \forall l. \\ \text{Tr}(\bar{Q}_s + \bar{V}) \leq \delta P, Q_s \geq 0, \bar{V} \succeq 0, t \geq 0. \quad (6.34) \right.
\]

where \( \bar{c}_k = -\widetilde{h}_{e,k}^H[(\bar{Q}_s - \frac{1}{t} - 1)\bar{V}]\bar{h}_{e,k} + \delta(\frac{1}{t} - 1)\sigma^2_e - \lambda e_k\varepsilon^2 e_k \). 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

\[
 \frac{(\bar{h}_s + e_s)^H Q_s (\bar{h}_s + e_s)}{(\bar{h}_s + e_s)^H V (\bar{h}_s + e_s) + \sigma^2_s} \geq f(t)^*, \\
 \Rightarrow (\bar{h}_s + e_s)^H [Q_s - f(t)^* V] (\bar{h}_s + e_s) \geq f(t)^* \sigma^2_s. \quad (6.35) 
\]

Thus, the associated power minimization problem is considered as

\[
 \min_{Q_s, V, \alpha, l, \beta, \lambda} \text{Tr}(Q_s), \\
 \text{s.t.} \quad (6.33a) - (6.33c), \\
 \left[ \begin{array}{cc} \beta s I + [Q_s - f(t)^* V] & [Q_s - f(t)^* V] \bar{h}_s \\ \bar{h}_s^H [Q_s - f(t)^* V] & d_s \\ \end{array} \right] \succeq 0, \quad (6.36a) 
\]

where \( d_s = \bar{h}_s^H [Q_s - f(t)^* V] \bar{h}_s - f(t)^* \sigma^2_s - \beta e^2_s \). (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($Q_s$) ≤ 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

\[
\min_{Q_s, V} \max_k \frac{t_{e,k}r_s}{t_s r_{e,k}}
\]

s.t. \( \text{Tr}(Q_s + V) \leq P \), \( \text{Tr}[(\bar{A}_i + \Delta_i)(Q_s + V)] \leq p_t, \forall i \),

\[
(\bar{h}_l + e_l)^H(Q_s + V)(\bar{h}_l + e_l) \geq E_l, \forall l,
\]

\( Q_s \succeq 0, V \succeq 0, \text{rank}(Q_s) = 1 \).

The above problem is convex in terms of (6.37a) and (6.37c). First, the exponential variables are introduced to modified (6.37a) as

\[
e^{x_0} \leq \sigma_s^2 + \min_{e_s} (\bar{h}_s + e_s)^H(Q_s + V)(\bar{h}_s + e_s),
\]

\[
e^{x_k} \leq \sigma_s^2 + \min_{e_{e,k}} (\bar{h}_{e,k} + e_{e,k})^H V(\bar{h}_{e,k} + e_{e,k}),
\]

\[
e^{y_k} \geq \sigma_e^2 + \max_{e_{e,k}} (\bar{h}_{e,k} + e_{e,k})^H(Q_s + V)(\bar{h}_{e,k} + e_{e,k}),
\]

\[
e^{y_0} \geq \sigma_s^2 + \max_{e_s} (\bar{h}_s + e_s)^H V(\bar{h}_s + e_s),
\]
6.3 AN-aided Transmit Optimization for Secrecy Rate Maximization

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

$$\min_{\Omega} \tau,$$

s.t. $e^{y_0+y_k-x_0-x_k} \leq \tau$, (6.37b), (6.37c), (6.37d),

$$e^{y_0} \leq \sigma_s^2 + u_s, \min_{e_s} (\hat{h}_s + e_s)\bar{H}_s + e_s) \geq u_s,$$  \hspace{1cm} (6.39a)

$$e^{x_0} \leq \sigma_e^2 + u_{e,k}, \min_{e_{e,k}} (\hat{h}_{e,k} + e_{e,k})\bar{H}(\hat{h}_{e,k} + e_{e,k}) \geq u_{e,k},$$  \hspace{1cm} (6.39b)

$$e^{y_k} \geq \sigma_e^2 + u_{e,k}, \max_{e_{e,k}} (\hat{h}_{e,k} + e_{e,k})\bar{H}(\hat{h}_{e,k} + e_{e,k}) \leq v_{e,k},$$  \hspace{1cm} (6.39c)

$$e^{y_0} \geq \sigma_s^2 + v_s, \max_{e_s} (\hat{h}_s + e_s)\bar{H}(\hat{h}_s + e_s) \leq v_s,$$  \hspace{1cm} (6.39d)

$$\{q_s, v, e_s, e_{e,k}, x_0, y_0, x_k, y_k, u_s, u_{e,k}, v_s, v_{e,k}\} \in \Omega, \forall k, l, i.$$  \hspace{1cm} (6.39e)

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

$$\min_{\Omega} \tau,$$

s.t. $e^{y_0+y_k-x_0-x_k} \leq \tau$, $e^{y_0} \leq \sigma_s^2 + u_s$, $e^{x_0} \leq \sigma_e^2 + u_{e,k},$  \hspace{1cm} (6.40a)

$$e^{y_k}(y_k - \tilde{y}_k + 1) \geq \sigma_e^2 + u_{e,k}, e^{y_0}(y_0 - \tilde{y}_0 + 1) \geq \sigma_s^2 + v_s,$$  \hspace{1cm} (6.40b)

$$\begin{bmatrix}
\lambda_s I + (q_s + v) & (q_s + v)\hat{h}_s \\
\hat{h}_s^T(q_s + v) & \hat{h}_s^T(q_s + v)\hat{h}_s - u_s - \lambda_s e_s^2
\end{bmatrix} \succeq 0,$$  \hspace{1cm} (6.40c)

$$\begin{bmatrix}
\lambda_{e,k} I + v & \hat{h}_{e,k} \bar{v} \\
\hat{h}_{e,k}^T v & \hat{h}_{e,k}^T v\hat{h}_{e,k} - u_{e,k} - \lambda_{e,k} e_{e,k}^2
\end{bmatrix} \succeq 0,$$  \hspace{1cm} (6.40d)

$$\begin{bmatrix}
\beta_{e,k} I - (q_s + v) & -(q_s + v)\hat{h}_{e,k} \\
-\hat{h}_{e,k}^T(q_s + v) & -\hat{h}_{e,k}^T(q_s + v)\hat{h}_{e,k} - v_{e,k} - \beta_{e,k} e_{e,k}^2
\end{bmatrix} \succeq 0,$$  \hspace{1cm} (6.40e)

$$\begin{bmatrix}
\beta_s I - v & -\hat{h}_s \bar{v} \\
-\hat{h}_s^T v & -\hat{h}_s^T v\hat{h}_s + v_s - \beta_s e_s^2
\end{bmatrix} \succeq 0,$$  \hspace{1cm} (6.40f)

$$\begin{bmatrix}
\alpha_l I + (q_s + v) & (q_s + v)\hat{h}_l \\
\hat{h}_l^T(q_s + v) & \hat{h}_l^T(q_s + v)\hat{h}_l - E_l - \alpha_l e_l^2
\end{bmatrix} \succeq 0,$$  \hspace{1cm} (6.40g)

$$\text{Tr}(q_s + v) \leq P, \text{Tr}[(\hat{A}_l(q_s + v))] + e_i\|q_s + v\|_F \leq p_i,$$

$$\{q_s \succeq 0, v \succeq 0, x_0, y_0, x_k, y_k, u_s, u_{e,k}, v_s, v_{e,k}\},$$

$$\lambda_s \succeq 0, \lambda_{e,k} \succeq 0, \beta_s \succeq 0, \beta_{e,k} \succeq 0, \alpha_l \succeq 0 \in \Omega, \forall k, l, i.$$  \hspace{1cm} (6.40h)
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-one 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

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

(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., $\varepsilon_s$, $\varepsilon_{e,k}$ and $\varepsilon_l$) 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
6.4 Simulation Results

Figure 6.1: Achieved secrecy rate with different transmit powers.

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

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, 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 6.3: Achieved secrecy rate with target harvested power.](image-url)
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

\[ \frac{1}{\sigma_s^2} |w^H h_s|^2 \geq \left[ \frac{2^R}{\sigma_e} w^H h_{e,k} \right]^H \left[ \frac{2^R}{\sigma_e} w^H h_{e,k} \right] \left( \frac{2^R - 1}{2} \right)^{1/2} \]  

(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 X be a complex hermitian matrix,

\[ X = X^H = \begin{bmatrix} A & B \\ B^H & C \end{bmatrix} \]  

(6.43)

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

- \( X \succ 0 \) if and only if \( A \succ 0 \) and \( S \succ 0 \).
- if \( A \succ 0 \) then \( X \succ 0 \) if and only if \( S \succ 0 \).

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

\[ \begin{bmatrix} \frac{1}{\sigma_s} w^H h_s I & \left[ \frac{2^R}{\sigma_e} w^H h_{e,k} \right] \\ \left[ \frac{2^R}{\sigma_e} w^H h_{e,k} \right]^H & \frac{1}{\sigma_s} w^H h_s \end{bmatrix} \left( \frac{2^R - 1}{2} \right)^{1/2} \] \[ \succeq 0, \]  

(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

\[
x_l^2 + y_l^2 \geq E, \quad (6.45a)
\]

\[
x_l = \Re\{w^H h_l\}, \quad y_l = \Im\{w^H h_l\}, \quad \forall l. \quad (6.45b)
\]

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 \( u_l = [x_l \ y_l]^T \), gives,

\[
x_l^2 + y_l^2 = u_l^T u_l.
\]

\( u_l^{(n)} \) is the \( n \)-th iteration of the vector \( u_l \). Thus, (6.45a) can be approximated as

\[
u_l^T u_l \approx \|u_l^{(n)}\|^2 + 2 \sum_{i=1}^{2} u_l^{(n)}(i)[u_l(i) - u_l^{(n)}(i)], \quad (6.46)
\]

where \( i \) denotes the \( i \)-th element of the vector \( u_l \). 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

\[
S'_k = \begin{bmatrix}
  f^{(n)}(t_2) I \\
  \begin{bmatrix}
    \frac{2R}{\sigma_x} w^H (\bar{h}_{e,k} + e_{e,k}) \\
    (2R - 1)^{\frac{1}{2}}
  \end{bmatrix}^H \\
  \begin{bmatrix}
    \frac{2R}{\sigma_x} w^H (\bar{h}_{e,k} + e_{e,k}) \\
    (2R - 1)^{\frac{1}{2}}
  \end{bmatrix}
\end{bmatrix} \succeq 0, \quad (6.47)
\]

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

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

\[
A \succeq B C + C^H X H B, \|X\| \leq t, \quad (6.48)
\]
if and only if there exist non-negative real numbers $a$ such that

\[
\begin{bmatrix}
A - aC^H C & -tB^H \\
-tB & aI
\end{bmatrix} \succeq 0.
\] (6.49)

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

\[
S_k \succeq \begin{bmatrix}
\frac{2R}{\sigma_e} w^H \\
0 \\
0
\end{bmatrix}
\begin{bmatrix}
0 & -1 \\
0 & -1
\end{bmatrix}
\begin{bmatrix}
0 \\
\frac{2R}{\sigma_e} w 0 0
\end{bmatrix},
\] (6.50)

where

\[
S_k = \begin{bmatrix}
f^{(n)}(t_2)I & \frac{2R}{\sigma_e} w^H \bar{h}_{c,k} \\
\frac{2R}{\sigma_e} w^H \bar{h}_{c,k} & (2R-1)\frac{1}{2}
\end{bmatrix}^H
\begin{bmatrix}
\frac{2R}{\sigma_e} w^H \\
(2R-1)\frac{1}{2}
\end{bmatrix} f^{(n)}(t_2)
\] (6.51)

Thus, (6.47) can be reformulated as

\[
\bar{S}_k = \begin{bmatrix}
S_k - \lambda_k & 0 & -\varepsilon_{e,k} \\
-\varepsilon_{e,k} & 0 & 0 \\
0 & 0 & \lambda_k I
\end{bmatrix} \succeq 0, \forall k.
\] (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

\[ L(Q_s, V, Y, Z, \lambda, \eta_i, \nu_l, \tau_k) = \text{Tr}(Q_s) - \lambda \left[ \text{Tr}[h_s h_s^H (Q_s - f(t) V)] - \sigma_s^2 f(t) \right] \]
\[ + \mu \left[ \text{Tr}(Q_s + V) - P \right] + \sum_{i=1}^{N_T} \eta_i \left[ \text{Tr}[A_i (Q_s + V)] - p_i \right] - \sum_{l=1}^{L} \nu_l \left[ \text{Tr}[h_l h_l^H (Q_s + V)] \right] \]
\[ - E_l + \sum_{k=1}^{K} \tau_k \left[ \text{Tr}[h_{e,k} h_{e,k}^H (Q_s - (t-1) V)] - (t-1) \sigma_e^2 \right] - \text{Tr}(YQ_s) - \text{Tr}(ZV), \]

(6.53)

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

\[ \frac{\partial L}{\partial Q_s} = 0, \Rightarrow Y = I - \lambda h_s h_s^H + \mu I + \sum_{i=1}^{N_T} \eta_i A_i - \sum_{l=1}^{L} \nu_l h_l h_l^H + \sum_{k=1}^{K} \tau_k h_{e,k} h_{e,k}^H, \]

(6.54a)

\[ \frac{\partial L}{\partial V} = 0, \Rightarrow Z = \lambda f(t) h_s h_s^H + \mu I + \sum_{i=1}^{N_T} \eta_i A_i - \sum_{l=1}^{L} \nu_l h_l h_l^H - \sum_{k=1}^{K} \tau_k (t-1) h_{e,k} h_{e,k}^H, \]

(6.54b)

\[ Q_s Y = 0, Z \succeq 0, \ \lambda \geq 0, \ \forall i, l, k. \]

(6.54c)

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

\[ Y - Z = I - \lambda (1 + f(t)) h_s h_s^H + \sum_{k=1}^{K} \tau_k h_{e,k} h_{e,k}^H, \]
\[ \Rightarrow Y = A - \lambda (1 + f(t)) h_s h_s^H, \]

(6.55)

where \( A = I + Z + \sum_{k=1}^{K} \tau_k h_{e,k} h_{e,k}^H \). From (6.55), one can easily observe that \( A \) is positive definite, and \( \text{rank}(A) = N_T \), whereas \( \text{rank}(Y) = N_T \) or \( N_T - 1 \). However, if \( \text{rank}(Y) = N_T \), then it violates \( Q_s \neq 0 \). Thus, \( \text{rank}(Y) = N_T - 1 \) always holds, which implies \( Q_s \) lies in the null space of \( Y \) from (6.54c), thus \( \text{rank}(Q_s) = 1 \). This completes Theorem 6.1. \( \blacksquare \)
6.6.4 Proof of Theorem 6.2

The dual function to (6.36) is written as follows:

\[
\mathcal{L}(Q_s, V, Y, Z, \lambda, \gamma_i, T_s, T_{e,k}, T_l) = \text{Tr}(Q_s) - \text{Tr}(Y Q_s) - \text{Tr}(Z V) + \lambda [\text{Tr}(Q_s + V) - P] + \sum_{i=1}^{N_T} \gamma_i \left[ \text{Tr}(\bar{A}_i(Q_s + V)) + \epsilon_i \|Q_s + V\|_F - \nu_i \right] - \text{Tr}(T_s A_1)
\]

\[
- \text{Tr}(T_s H_s^H(Q_s - f(t) V) H_s) - \sum_{k=1}^{K} \text{Tr}(T_{e,k} B_k) + \sum_{k=1}^{K} \text{Tr} \left[ T_{e,k} H_{e,k}^H [Q_s - (t^{-1} - 1)V] H_{e,k} \right]
\]

\[
- \sum_{l=1}^{L} \text{Tr}(T_l C_l) - \sum_{l=1}^{L} \text{Tr}[T_l H_l^H (Q_s + V) H_l], \quad (6.56)
\]

where \( Y \in \mathbb{H}_+^{N_T}, Z \in \mathbb{H}_+^{N_T}, \lambda \in \mathbb{R}_+, \gamma_i \in \mathbb{R}_+, T_s \in \mathbb{H}_+^{N_T}, T_{e,k} \in \mathbb{H}_+^{N_T} \) and \( T_l \in \mathbb{H}_+^{N_T} \) are dual variables of \( Q_s, V, (6.33a), (6.33c) \) and \( (6.33b), \) respectively.

In addition,

\[
A_1 = \begin{bmatrix}
\beta_i I & 0 \\
0^H & -f(t) \sigma_s^2 - \beta_i \varepsilon_s^2
\end{bmatrix}, \quad H_s = \begin{bmatrix}
I_{N_T} & \bar{h}_s \\
\end{bmatrix},
\]

\[
B_k = \begin{bmatrix}
\lambda_{e,k} I & 0 \\
0^H & (t^{-1} - 1) \sigma_e^2 - \lambda_{e,k} \varepsilon_e^2
\end{bmatrix}, \quad H_{e,k} = \begin{bmatrix}
I_{N_T} & \bar{h}_{e,k} \\
\end{bmatrix},
\]

\[
C_l = \begin{bmatrix}
\alpha_l I & 0 \\
0^H & -E_l - \alpha_l \varepsilon_l^2
\end{bmatrix}, \quad H_l = \begin{bmatrix}
I_{N_T} & \bar{h}_l \\
\end{bmatrix}.
\]

The related KKT conditions are considered as follows:

\[
\frac{\partial \mathcal{L}}{\partial Q_s} = 0, \Rightarrow Y = I + \lambda I + \sum_{i=1}^{N_T} \gamma_i [\bar{A}_i + \epsilon_i Q_s + W]_{F}^{-1} I - H_s T_s H_s^H
\]

\[
+ \sum_{k=1}^{K} H_{e,k} T_{e,k} H_{e,k}^H - \sum_{l=1}^{L} H_l T_l H_l^H, \quad (6.57a)
\]

\[
\frac{\partial \mathcal{L}}{\partial V} = 0, \Rightarrow Z = \lambda I + \sum_{i=1}^{N_T} \gamma_i [\bar{A}_i + \epsilon_i Q_s + W]_{F}^{-1} I + f(t) H_s T_s H_s^H
\]

\[
- \sum_{k=1}^{K} (t^{-1} - 1) H_{e,k} T_{e,k} H_{e,k}^H - \sum_{l=1}^{L} H_l T_l H_l^H, \quad (6.57b)
\]

\[
Q_s Y = 0, Z \succeq 0, \quad \forall i, k, l, \quad (6.57c)
\]

\[
[A_1 + H_s^H (Q_s - f(t) V) H_s] T_s = 0. \quad (6.57d)
\]
By subtracting (6.57b) from (6.57a), the following equality holds:

\[ Y - Z = I - [1 + f(t)]H_sT_sH_s^H + \sum_{k=1}^{K} t^{-1}H_{e,k}T_{e,k}H_{e,k}^H, \]

\[ \Rightarrow Y + [1 + f(t)]H_sT_sH_s^H = I + Z + \sum_{k=1}^{K} t^{-1}H_{e,k}T_{e,k}H_{e,k}^H. \quad (6.58) \]

Premultiply (6.58) by \( Q_s \)

\[ Q_s\left( I + Z + \sum_{k=1}^{K} t^{-1}H_{e,k}T_{e,k}H_{e,k}^H \right) = [1 + f(t)]Q_sH_sT_sH_s^H. \quad (6.59) \]

The following rank relation holds:

\[ \text{rank}(Q_s) = \text{rank}\left[ Q_s\left( I + Z + \sum_{k=1}^{K} t^{-1}H_{e,k}T_{e,k}H_{e,k}^H \right) \right] \]

\[ = \text{rank}(Q_sH_sT_sH_s^H) \leq \min\{\text{rank}(H_sT_sH_s^H), \text{rank}(Q_s)\}. \quad (6.60) \]

Based on the above rank relation, it is necessary to show \( \text{rank}(H_sT_sH_s^H) \leq 1 \) if we claim \( \text{rank}(Q_s) \leq 1 \), thus, the two facts is considered as

\[
\begin{bmatrix}
I_{N_T} & 0 \\
I_{N_T} & 0
\end{bmatrix} H_s^H = I_{N_T},
\]

\[
\begin{bmatrix}
I_{N_T} & 0
\end{bmatrix} A_1 = \beta_s \left( H_s - \begin{bmatrix} 0_{N_T} & \bar{h}_s \end{bmatrix} \right).
\]

Premultiply \( \begin{bmatrix} I_{N_T} & 0 \end{bmatrix} \) and postmultiply \( H_s^H \) by (6.57d), respectively, and applying the above two equalities, the following relations hold:

\[
\beta_s \left( H_s - \begin{bmatrix} 0_{N_T} & \bar{h}_s \end{bmatrix} \right) T_sH_s^H + [Q_s - f(t)V]H_sT_sH_s^H = 0,
\]

\[
\Rightarrow \left( \beta_s I + [Q_s - f(t)V] \right) H_sT_sH_s^H = \beta_s \begin{bmatrix} 0_{N_T} & \bar{h}_s \end{bmatrix} T_sH_s^H. \quad (6.61)
\]

**Lemma 6.5** If a block hermitian matrix \( P = \begin{bmatrix} P_1 & P_2 \\ P_3 & P_4 \end{bmatrix} \succeq 0 \), then the main diagonal matrices \( P_1 \) and \( P_4 \) are always PSD matrices [93].

Now, it can be shown that \( \beta_s I + [Q_s - f(t)V] \succeq 0 \) and is nonsingular, thus pre(post)multiply by a nonsingular matrix will not change the matrix rank. Thus,
the following rank relation holds:

$$\text{rank}(H_s T_s H_s^H) = \text{rank}\left( \begin{bmatrix} 0_{N_T} & h_s \\ \end{bmatrix} T_s H_s^H \right) \leq \text{rank}\left( \begin{bmatrix} 0_{N_T} & h_s \end{bmatrix} \right) \leq 1. \quad (6.62)$$

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 constraint, 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-
7.2 Future Work

Communications. 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


