Master Thesis

Optimal Resource Allocation for Secure Wireless Communication Systems

Dongfang Xu

Institute for Digital Communications
Prof. Dr.-Ing. Robert Schober
University of Erlangen-Nuremberg

Supervisors: Prof. Dr.-Ing. Robert Schober
M.Sc. Yan Sun

September 15, 2017

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

Institute for Digital Communications

Prof. Dr.-Ing. Robert Schober
University of Erlangen-Nürnberg

Master Thesis

Optimal Resource Allocation for Secure Wireless Communication Systems
for
Xu Dongfang

Security is a crucial issue for wireless communication due to the broadcast nature of the wireless medium. Recently, physical layer security has received significant attention for preventing eavesdropping in wireless communication systems. An important technique to facilitate physical layer security is multiple-antenna transmission which utilizes the spatial degrees of freedom for degrading the quality of the eavesdroppers' channels. In particular, on the one hand, information beamforming is performed for limiting the information leakage to eavesdroppers. On the other hand, artificial noise transmission is employed to deliberately impair the information reception at the eavesdroppers.

The system secrecy throughput is a significant performance measure for secure wireless communications. However, most of the literature in this field proposed suboptimal resource allocation schemes for the maximization of the system secrecy throughput and the optimal resource allocation design for secure wireless communication is still an open problem. Motivated by this, in this thesis, we aim to investigate the optimal resource allocation algorithm design for a multiuser communication system with the objective to maximize the system secrecy throughput. The resulting system performance shall be compared against existing suboptimal resource allocation schemes in the literature.

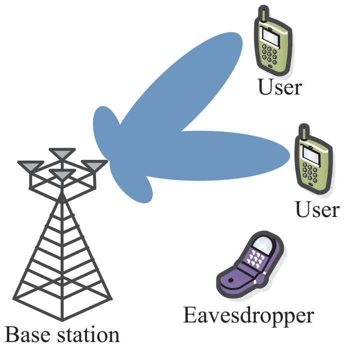

Figure 1: Information beamforming.

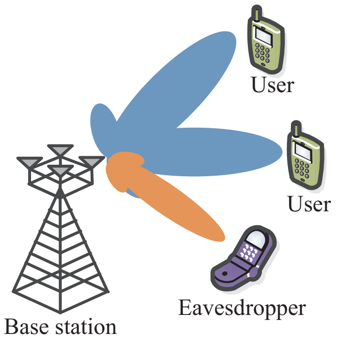

Figure 2: Artificial noise generation.

Main guidelines for the work:

- Development of the system model for guaranteeing secure transmission in multiuser wireless communication systems by means of the information beamforming
- Optimization problem formulation and algorithm design for optimal resource allocation in the considered secure communication systems
- If possible, extension to the case of concurrent artificial noise transmission to further improve the system secrecy throughput

Supervisor: Yan Sun, Wetterkreuz 15, Room 00.217, yan.sun@fau.de

Start date: March 15, 2017
End date: September 15, 2017

. . . .
(Prof. Dr.-Ing. R. Schober)

Declaration

To the best of my knowledge and belief this work was prepared without aid from any other sources except where indicated. Any reference to material previously published by any other person has been duly acknowledged. This work contains no material which has been submitted or accepted for the award of any other degree in any institution.

Erlangen, September 15, 2017

Dongfang Xu
Bierlachweg, 41,
Erlangen, Germany

Contents

Title i

Abstract ix

Glossary xi
Abbreviations . . . xi
Operators . . . xi
Symbols . . . xii

1 Introduction 1

2 Multiuser System Model 5
2.1 Multiuser Downlink Channel Model . . . 5
2.2 Channel State Information . . . 7

3 Optimization Problem Formulation 9
3.1 Achievable Rate and Achievable Secrecy Rate . . . 9
3.2 Resource Allocation Problem Formulation . . . 10

4 Solution of the Optimization Problem 13
4.1 Mathematical Preliminaries . . . 13
4.2 Optimal Resource Allocation Scheme . . . 15
4.3 Suboptimal Resource Allocation Scheme . . . 21

5 Extension to Robust SST Optimization 27
5.1 CSI Uncertainty Constraint Transformation . . . 27
5.2 Robust SST Optimization Problem Reformulation . . . 30

6 Simulation Results 33
6.1 Sum Secrecy Throughput versus Maximum Transmit Power . . . 34
6.2 Sum Secrecy Throughput versus Number of Active Users . . . 35
6.3 Sum Secrecy Throughput versus Number of Potential Eavesdroppers . . . 37
6.4 Sum Secrecy Throughput versus Minimum Required SINR . . . 39

7 Conclusion 41

Bibliography 43

Abstract

In this thesis, we study resource allocation in multiuser wireless communication systems. In particular, we focus on secure downlink transmission in presence of potential eavesdroppers. The resource allocation design aims to maximize the sum secrecy throughput of the considered system by jointly optimizing the downlink beamformer and artificial noise. The algorithm design results in a non-convex optimization problem. Besides, the problem formulation also includes quality-of-service requirement which imposes a minimum required signal-to-interference-plus-noise ratio at active users. Despite the non-convexity of the considered problem formulation, we solve it optimally by employing monotonic optimization theory. In particular, we obtain the globally optimal solution of the considered problem via adopting a polyblock outer approximation algorithm. Considering the high computational complexity of the proposed optimal scheme, a suboptimal resource allocation scheme based on a successive convex approximation algorithm is developed to achieve the balance between optimality and efficiency. Furthermore, we investigate an extensional case where imperfect channel state information of the multiple potential eavesdroppers is taken into account. In view of the intractability of the optimization problem, we reformulate the considered problem by replacing a semi-infinite constraint with a tractable constraint involving a finite number of linear matrix inequalities and then propose an optimal resource allocation scheme to maximize the robust sum secrecy throughput of the considered case. The simulation results confirm that the proposed optimal resource allocation scheme achieves significant sum secrecy throughput improvement compared to the two baseline schemes. Besides, our results also show that the proposed algorithm is robust against the imperfectness of the channel state information of the eavesdroppers.

Glossary

Abbreviations

AF	Amplify-and-Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BF	Beamforming
BS	Base Station
CSI	Channel State Information
DCP	Difference of Convex Programming
DoF	Degree of Freedom
KKT	Karush-Kuhn-Tucker
LMIs	Linear Matrix Inequalities
MIMO	Multiple-Input Multiple-Output
MO	Monotonic Optimization
MRT	Maximum Ratio Transmission
MUI	Multiuser Interference
POA	Polyblock Outer Approximation
PHY	Physical Layer
QoS	Quality-of-Service
SDP	Semidefinite Programming
SCA	Successive Convex Approximation
SINR	Signal-to-Interference-plus-Noise Ratio
SST	Sum Secrecy Throughput
ZF-BF	Zero-Forcing Beamforming

Operators

$\triangleq$	Defined as
$\mathbb{R}$	The set of all real numbers
$\mathbb{C}$	The set of all complex numbers
$\mathbb{R}^{N\times 1}$	The set of all real-valued vectors
$\mathbb{R}_{+}^{N\times 1}$	The set of all non-negative real-valued vectors
$\mathbb{C}^{N\times 1}$	The set of all complex-valued vectors
$\mathbb{R}^{N\times M}$	The set of all $N \times M$ real-valued matrices
$\mathbb{C}^{N\times M}$	The set of all $N \times M$ complex-valued matrices
$\mathbb{H}^{N}$	The set of all $N \times N$ Hermitian matrices
$\mathbf{I}_N$	The $N \times N$ identity matrix
$x \in \mathscr{S}$	x is a member of the set $\mathscr{S}$

$\forall x$	Means that a statement holds for all x
$\mathbf{x}^H$	Conjugate transpose of $\mathbf{x}$
$\lvert x \rvert$	Absolute value of a complex scalar x
$\lvert\lvert \mathbf{x} \rvert\rvert$	Euclidean norm of a vector $\mathbf{x}$
$[x]^+$	Stands for $\max\{0, x\}$
$\mathrm{Tr}(\mathbf{A})$	The trace of matrix $\mathbf{A}$
$\mathrm{Rank}(\mathbf{A})$	Rank of a matrix $\mathbf{A}$
$\mathbf{A} \succeq 0$	Means matrix $\mathbf{A}$ is positive semidefinite
$\mathcal{E}\{x\}$	Statistical expectation of random variable x
$x \sim \mathcal{X}(\cdot)$	The random variable x has distribution $\mathcal{X}(\cdot)$
$\mathcal{CN}(\mu, \mathbf{R})$	The circularly symmetric complex Gaussian distribution with mean μ and covariance matrix $\mathbf{R}$

Symbols

d_k	Information bearing signal to active use k
δ	Optimal solution approximation factor in projection bisection search algorithm
Γ_k	Received SINR at active user k
$\Gamma^E_{m,k}$	Received SINR at idle user m for eavesdropping active user k
Γ_{req}	Minimum required SINR for active users
$\mathbf{h}_k$	Channel vector between the base station and active user k
K	Number of active users
$\mathbf{l}_m$	Channel vector between the base station and idle user m
$\widehat{\mathbf{l}}_m$	Channel estimate of idle user m available at the base station
$\Delta\mathbf{l}_m$	Channel uncertainty of idle user m
M	Number of idle users
M_{OPA}	Maximum iteration in polyblock outer approximation algorithm
M_{SCA}	Maximum iteration in successive convex approximation algorithm
N_T	Number of antennas at the base station
Ω_m	Channel state information uncertainty set of idle user m
$P_{\max}$	Maximum transmit power at the base station [dBm]
p_k	Gain for the channel between the base station and the k-th active user
$\pi_{\mathcal{G}}(\mathbf{x})$	Projection of vector $\mathbf{x}$ on set $\mathcal{G}$
R_k	Achievable rate of active user k [bit \ s \ Hz]
R	Achievable sum rate of [bit \ s \ Hz]
$R^E_{m,k}$	Achievable rate of idle user m for eavesdropping desired active user k [bit \ s \ Hz]
R^{Sec}_k	Achievable secrecy rate of active user k [bit \ s \ Hz]
R^{Sec}	Achievable sum secrecy rate [bit \ s \ Hz]
ε	Optimal solution tolerance factor in polyblock outer approximation algorithm
$\mathbf{v}$	Artificial noise vector
$\mathbf{V}$	Artificial noise covariance matrix
$\mathbf{w}_k$	Beamforming vector for active use k
w_{kn}	The n-th element of beamforming vector for active use k

$\mathbf{x}$	Combined transmit signal vector
$\mathbf{x}_k$	Transmit signal to active user k
y_k	Received signal at active user k
y_m^E	Received signal at idle user m

Chapter 1

Introduction

Secure transmission, an old but pivotal issue in radio frequency communication systems, has been raised for nearly 90 years [1]. Due to the free propagation of electromagnetic waves in wireless communication systems, all users receive the information signal from the Base Station (BS) via a broadcast channel. In most wireless communication systems, data encoding and encryption techniques in upper layers have been widely adopted to prevent wiretapping. However, these techniques are not flexible enough since codebooks are necessary to be stored in advance at the receivers to decode the desired information, and they are meaningless once the codebooks are stolen by eavesdroppers. Moreover, these techniques may become invalid since today's new computing technologies (e.g. quantum computing) can decipher the encryption. These disadvantages spur people to explore more applicable and effective techniques to achieve security. Recently, much work have be done to achieve security in Physical Layer (PHY) [2]–[4]. Specifically, the aim of PHY-security is to ensure a positive secrecy rate of the desired user by exploiting wireless Channel State Information (CSI). To make it attainable, the quality of the desired user's channel is required to be better than the eavesdroppersâĂŹ. However, in reality, this condition may be violated due to the randomness of channel fading. Conventionally, one possible way to improve PHY-security of a multiple-input single-output system is to utilize the extra spatial Degree of Freedom (DoF) to design Beamforming (BF) vectors at the multiple antenna transmitter [5]–[7]. This technique facilitates the transmit signal stream to focus on the intended userâĂŹs direction while reducing the information signal leakage to eavesdroppers.

Lately, a more flexible and effective technique to impair the quality of eavesdroppers' channels with an intentionally generated noise has also been proposed [8]. The basic idea of Artificial Noise (AN) is generating a noise signal which is able to deliberately degrade the quality of the eavesdroppers' channels [9], [10]. In particular, AN is yielded based on the CSI of the eavesdroppers at the BS. For instance, if the CSI of the eavesdroppers is hardly available at the BS, one simple but effective scheme is to generate an isotropic

AN [8] which is uniformly distributed on the nullspace of the active users' channels. Based on BF and AN, many resource allocation algorithms have been proposed to achieve PHY-security. The authors of [11] proposed a suboptimal resource allocation algorithm for maximizing the Sum Secrecy Throughput (SST) of a multiuser communication system with a single eavesdropper. In [12], the authors considered a simple Amplify-and-Forward (AF) scheme to achieve the maximization of the AF secrecy rate in a unicast communication over multi-hop wireless relay networks. The authors of [13] derived a lower bound for the ergodic secrecy rate of a given user under the condition where matched filter data precoding and AN transmission are employed in a downlink massive Multiple-Input Multiple-Output (MIMO) systems in the presence of a passive multiple-antenna eavesdropper. However, the above-mentioned resource allocation algorithms are suboptimal for maximizing the secrecy rate under the assumption that the considered wireless communication system contains only one eavesdropper. Therefore, they are not applicable for achieving optimal secrecy throughput in a multiuser wireless communication system in the presence of multiple eavesdroppers.

Recently, robust resource allocation algorithm design for multiuser wireless communication systems has attracted much attention since perfect CSI of all the users are not always accessible at the BS. In particular, the CSI of the active users is assumed to be perfectly known at the BS. The is due to the fact that these users constantly interact with the BS in each scheduling time slot, and their channel estimations are relatively seasonable and precise. Yet, this assumption may not be true when we consider the potential eavesdroppers. In multiuser wireless communication systems, there are mainly two categories of potential eavesdroppers, i.e., idle users and passive eavesdroppers. On the one hand, idle users are legitimate users who are already registered in the system. However, they may badly behave themselves and attempt to overhear the information signals for the desired active users. On the other hand, passive eavesdroppers are illegitimate users who remain silent in the system, wherefore the BS may not be aware of their existence. Thus, the CSI of these potential eavesdroppers are usually supposed to be partially available at the BS. In [14], the authors designed a robust resource allocation algorithm to maximize the achievable secrecy rate with respect to a single-antenna legitimate receiver based on formulating a tightened relaxation convex optimization problem. The authors of [15] solved the resource allocation optimization problem of maximizing the SST in a user-eavesdropper pair wiretapping model by employing a first-order approximation technique based on Taylor expansion. However, we note that the proposed resource allocation algorithms in [11]–[15] solve the optimization problems in a way which aims to formulate the objective function and the constraints into a form of a convex function, and the formulation procedures are lengthy and complicated. As a result of this, Monotonic Optimization (MO), a more general and flexible optimization approach, is proposed [16] to facilitate succinct algorithm design for resource allocation optimization problems. Moreover, many resource allocation optimization problems in wireless communication systems can be classified into MO problems and efficaciously solved [17]–[23]. In [23], the authors proposed a monotonic optimization and semidefinite programming algorithm to maximize the SST with the help of an AF relay in a multiple-source multiple-destination network in the presence of multiple eavesdroppers. However, maximizing the SST of a multiuser downlink system which consists of multiple active users and multiple potential eavesdroppers with imperfect CSI at the BS, is still an open problem.

In this thesis, we aim to optimally solve the resource allocation optimization problem of maximizing the SST in a multiuser wireless communication system. In particular, we first formulate an MO problem and then design an optimal resource allocation algorithm based on Polyblock Outer Approximation (POA) to maximize the SST in the considered system model in presence of perfect CSI of all users at the BS. Due to the high computational complexity of the proposed optimal scheme, a suboptimal resource allocation algorithm based on Successive Convex Approximation (SCA) is posed to achieve the balance between optimality and computational complexity. Furthermore, we extend to a more practical case where the multiuser wireless communication system contains multiple eavesdroppers whose CSI are imperfect at the BS, and the previously mentioned optimal resource allocation algorithm is modified and adapted to the considered optimization problem to achieve the optimal solution.

The rest of the thesis is structured as follows. In Chapter 2, we present the considered multiuser wireless communication system model and then discuss the CSI of two different kinds of users. In Chapter 3, we introduce the adopted performance metrics for the considered system model and formulate the resource allocation optimization problem. In Chapter 4, we propose an optimal scheme and a suboptimal scheme to solve the formulated problem. In Chapter 5, we design a resource allocation algorithm to obtain the optimal solution in an extensional case where the optimization problem involves multiple-eavesdropper with imperfect CSI at the BS. Simulation results and corresponding analysis are presented in Chapter 6. Chapter 7 concludes the thesis and poses interesting future work.

Chapter 2

Multiuser System Model

In this chapter, we present the considered multiuser wireless communication system model. In Section 2.1, we describe the considered system in detail and then express the transmit signal at the BS, received signals at both active users and idle users, respectively. In Section 2.2, we discuss the CSI of different types of users and give the corresponding reasons.

2.1 Multiuser Downlink Channel Model

We adopt a multiuser communication system downlink model which contains a BS, K active users, and M idle users, cf. Fig. 2.1. The BS is equipped with $N_\mathrm{T} > 1$ antennas. All $K+M$ users are single-antenna devices and are able to decode information from transmit signal. In each scheduling time slot, active users receive a signal stream consisting of all the desired user signals from the BS while the idle users remain silent but are able to receive the signal stream during the transmission period. However, if the idle users are insidious, and then they may eavesdrop the information signal of the desired user. In consequence, we consider the idle users as potential eavesdroppers which have to be taken into account for a resource allocation algorithm design to guarantee communication security.

At the beginning of each time slot, the BS transmits a signal stream consisting of K independent information signals to K active users. Specifically, the transmit signal to active user $k \in \{1, \cdots, K\}$ can be expressed as

$$\mathbf{x}_k = \mathbf{w}_k d_k, \tag{2.1}$$

where $d_k \in \mathbb{C}$ and $\mathbf{w}_k \in \mathbb{C}^{N_\mathrm{T}\times 1}$ are the information bearing signal to active use k and the corresponding beamforming vector, respectively. Without loss of generality, we assume $\mathcal{E}\left\{|d_k|^2\right\} = 1$, $\forall k \in \{1, \cdots, K\}$. Moreover, we adopt AN technique in this thesis

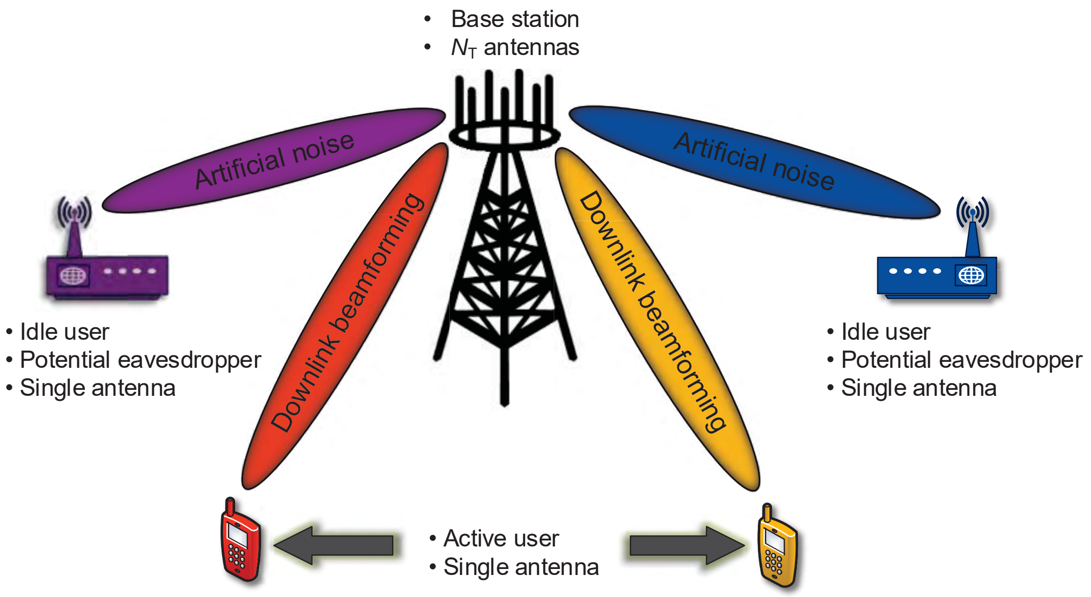

Figure 2.1: Illustration of the considered system model comprising $K = 2$ active users and $M = 2$ idle users.

to improve the PHY-security of the considered system. Hence, the transmit signal vector, containing K information signals and AN, is expressed by

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{x}_k + \mathbf{v}, \tag{2.2}$$

where $\mathbf{v} \in \mathbb{C}^{N_\mathrm{T}\times 1}$ denotes the AN vector generated by the BS to intentionally degrade the channels of the m potential eavesdroppers. In particular, $\mathbf{v}$ follows a complex Gaussian distribution where $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{V})$ with $\mathbf{V} \in \mathbb{H}^{N_\mathrm{T}}$, $\mathbf{V} \succeq \mathbf{0}$ representing the covariance matrix of the AN.

On the other hand, the received signal at active user $k \in \{1, \ldots, k\}$ and idle user $m \in \{1, \ldots, m\}$ are given by, respectively

$$y_k = \mathbf{h}_k^H \mathbf{x}_k + \underbrace{\sum_{i \neq k}^{K} \mathbf{h}_k^H \mathbf{x}_i}_{\text{Multiuser interference}} + \underbrace{\mathbf{h}_k^H \mathbf{v}}_{\text{Artificial noise}} + n_k, \tag{2.3}$$

$$y_m^E = \sum_{k=1}^{K} \mathbf{l}_m^H \mathbf{x}_k + \underbrace{\mathbf{l}_m^H \mathbf{v}}_{\text{Artificial noise}} + n_m, \tag{2.4}$$

where $\mathbf{h}_k \in \mathbb{C}^{N_\mathrm{T}\times 1}$ is the channel vector between the BS and active user $k \in \{1, \cdots, K\}$, and $\mathbf{l}_m \in \mathbb{C}^{N_\mathrm{T}\times 1}$ is the channel vector between the BS and idle user $m \in \{1, \cdots, M\}$, respectively. We assume all the channels are slowly time-varying frequency flat fading channel. We note that variables $\mathbf{h}_k$ and $\mathbf{l}_m$ collect the effects of the path loss, shadowing and multipath fading of the corresponding frequency flat fading channels. Besides, n_k and n_m include background noises and thermal noises resulting from the receive antennas at active user k and idle user m, respectively. We model them as Additive White Gaussian Noise (AWGN) which follow the same complex normal distribution with zero mean and variance σ_n^2.

2.2 Channel State Information

The active users send handshaking signals to the BS at the beginning of each scheduling time slot. Based on these signals, the BS is able to obtain the CSI to facilitate downlink transmission. Thus, the channel between the BS and active user k, $\mathbf{h}_k$, $\forall k \in \{1,\cdots,K\}$, can be reliably estimated at the BS with negligible estimation errors. In addition, automatic repeat request protocol is considered in data link layer to guarantee fluent and timely estimations of $\mathbf{h}_k$. Therefore, we can assume perfect CSI for the channel between the BS and active user $k \in \{1,\cdots,K\}$ during the whole transmission period. However, an idle user does not constantly interact with the BS, and this leads to an outdated and inaccurate CSI estimation of the channel between the BS and the idle user m, i.e., $\mathbf{l}_m$, $\forall m \in \{1,\cdots,M\}$. To capture this effect, a deterministic model proposed in [22], [24] is adopted in this thesis to represent the resulting CSI uncertainty. The channel vector $\mathbf{l}_m$ between the BS and idle user m is given by

$$\begin{aligned} \mathbf{l}_m &= \widehat{\mathbf{l}}_m + \Delta\mathbf{l}_m,\ m \in \{1,\cdots,M\}, && (2.5) \\ \Omega_m &= \left\{\Delta\mathbf{l}_m \in \mathbb{C}^{N_\mathrm{T}\times 1} : \Delta\mathbf{l}_m^H \Delta\mathbf{l}_m \le \varepsilon_m^2\right\}, && (2.6) \end{aligned}$$

where $\widehat{\mathbf{l}}_m \in \mathbb{C}^{N_\mathrm{T}\times 1}$ is the channel estimate of idle user m available at the BS at the beginning of a time slot. $\Delta\mathbf{l}_m$ represents the unknown channel uncertainty of idle user m due to the slow timing varying nature of the channel. A set Ω_m is defined in (6), and it contains all the possible CSI uncertainties of idle user m. It should be noted that we model the CSI uncertainty region as a hyperball with the radius $\varepsilon_m > 0$ in a N_T-dimensional space, and ε_k indicates the size of the uncertainty region of the estimated CSI of idle user. Additionally, a larger ε_m means less CSI of idle user m can be obtained at the BS. In practice, the value of $\varepsilon_m^2 > 0$ depends on the coherence time of the associated channel and the time between channel estimation and packet transmission.

Chapter 3

Optimization Problem Formulation

In this chapter, we formulate the resource allocation optimization problem. In Section 3.1, we define the system sum rate and sum secrecy rate as the performance metrics. Then, the optimization problem for maximizing the SST of the considered system is formulated in Section 3.2.

3.1 Achievable Rate and Achievable Secrecy Rate

The achievable rate of active user $k \in \{1, \cdots, K\}$ and system sum rate are given by, respectively,

$$R_k = \log_2(1+\Gamma_k) \text{ and } R = \sum_{k=1}^{K} \log_2(1+\Gamma_k), \tag{3.1}$$

where Γ_k is the received Signal-to-Interference-plus-Noise Ratio (SINR) at active user k and is given by

$$\Gamma_k = \frac{\left|\mathbf{h}_k^H \mathbf{w}_k\right|^2}{\sum_{r \neq k}^{K} \left|\mathbf{h}_k^H \mathbf{w}_r\right|^2 + \left|\mathbf{h}_k^H \mathbf{v}\right|^2 + \sigma_n^2}. \tag{3.2}$$

In this thesis, we also take into account Quality-of-Service (QoS) for all active users. Specifically, the SINR of active users K, Γ_k, is required to be greater than or equal to a threshold Γ_{req} to ensure a good link quality. As stated before, due to the broadcast nature of wireless medium, all idle users are able to receive the information stream from the BS, and they may also decode the transmit signals to the desired active users. Therefore, in order to guarantee PHY-security, we consider the worst-case scenario for maximizing the SST of the considered system. Specifically, for the case potential eavesdropper $m \in \{1, \cdots, m\}$ wiretapping active user $k \in \{1, \cdots, K\}$, we suppose that the potential eavesdropper m can eliminate all Multiuser Interference (MUI) introduced by all active users except for active user k in advance of decoding the desired information to active use k. Thus, under this assumption, the achievable rate between the BS and idle user m for eavesdropping desired active user k can be written as

$$R^E_{m,k} = \log_2(1 + \Gamma^E_{m,k}), \tag{3.3}$$

where $\Gamma^E_{m,k}$ is the received SINR at idle user m for eavesdropping active user k and is given by

$$\Gamma^E_{m,k} = \frac{\left|\mathbf{l}^H_m \mathbf{w}_k\right|^2}{\left|\mathbf{l}^H_m \mathbf{v}\right|^2 + \sigma^2_n}. \tag{3.4}$$

Therefore, the achievable secrecy rate between the BS and active user $k \in \{1, \cdots, K\}$ and the system SST are given by [8]–[25], respectively,

$$R^{Sec}_k = \left[R_k - \max_{m\in\{1,\cdots,M\}} R^E_{m,k}\right]^+ \tag{3.5}$$

$$R^{Sec} = \sum_{k=1}^{K} \left[R_k - \max_{m\in\{1,\cdots,M\}} R^E_{m,k}\right]^+, \tag{3.6}$$

where R^{Sec}_k quantifies the achievable data rate at which BS can reliably transmit secret information to active user k, meanwhile, the potential eavesdroppers are unable to decode the received signal.

3.2 Resource Allocation Problem Formulation

In this section, we first design an optimal resource allocation algorithm for maximizing the SST of a multiuser single-eavesdropper system with perfect CSI at the BS. Hence, we let $M = 1$ and omit the index m in the rest of this chapter as well as in next chapter. For the sake of notational simplicity, we define the following variable, $\mathbf{W}_k = \mathbf{w}_k\mathbf{w}^H_k$, $\mathbf{H}_k = \mathbf{h}_k\mathbf{h}^H_k$, $k \in \{1, \cdots, K\}$, and $\mathbf{L}_m = \mathbf{l}_m\mathbf{l}^H_m$, $m \in \{1, \cdots, M\}$. Then, we rewrite the received SINR at active user k in (3.2) and the received SINR at idle user m for eavesdropping active user k in (3.4) as follows, respectively

$$\Gamma_k = \frac{\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_k)}{\sum^K_{r\neq k} \mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k\mathbf{V}) + \sigma^2_n}, \tag{3.7}$$

$$\Gamma^E_k = \frac{\mathrm{Tr}(\mathbf{L}\mathbf{W}_k)}{\mathrm{Tr}(\mathbf{L}\mathbf{V}) + \sigma^2_n}. \tag{3.8}$$

The optimal resource allocation policy, $\left\{\mathbf{W}_k^*, \mathbf{V}^*\right\}$, for maximizing the system SST can be obtained by solving

$$\begin{aligned}
&\underset{\mathbf{W}_k, \mathbf{V} \in \mathbb{H}^{N_\mathrm{T}}}{\text{maximize}} \quad && \sum_{k=1}^{K} \left[R_k - R_k^E\right]^+ \\
&\text{subject to} && \text{C1: } \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{W}_k) + \mathrm{Tr}(\mathbf{V}) \le P_{\max}, \\
& && \text{C2: } \frac{\mathrm{Tr}(\mathbf{H}_k \mathbf{W}_k)}{\sum_{r \neq k}^{K} \mathrm{Tr}(\mathbf{H}_k \mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k \mathbf{V}) + \sigma_n^2} \ge \Gamma_{\mathrm{req}_k}, \forall k, \\
& && \text{C3: } \mathbf{V} \succeq \mathbf{0}, \quad \text{C4: } \mathrm{Rank}(\mathbf{W}_k) \le 1, \ \forall k, \quad \text{C5: } \mathbf{W}_k \succeq \mathbf{0}, \ \forall k.
\end{aligned} \tag{3.9}$$

In constraint C1, we consider the physical limitation of the maximum transmit power at the BS restricting by $P_{\max}$. According to the proposed resource allocation policy, the BS is able to freely distribute the transmit power on each antenna as long as this constraint holds. In constraint C2, we set a threshold Γ_{req} which denotes the minimum required SINR for active users to achieve reliable information decoding. It should be noted that, on the one hand, a relatively high threshold Γ_{req} may lead to a better QoS for all active users. On the other hand, increasing this threshold also adversely influences the feasibility of the considered optimization problem. Hence, an advisable choice of Γ_{req} is at a level which a good QoS is just met. Constraint C3 and $\mathbf{V} \in \mathbb{H}^{N_\mathrm{T}}$ are imposed since covariance matrix $\mathbf{V}$ has to be a positive semi-definite Hermitian matrix. Constraint C4 and C5 are imposed to guarantee that $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ holds and covariance matrix $\mathbf{W}_k$ to be a positive semi-definite Hermitian matrix after optimization, respectively. In addition, the operator $[\cdot]^+$ in the objective function can be safely removed without affecting the optimal solution of the considered optimization problem. Specifically, if the achievable secrecy rate between the BS and active user $k \in \{1, \cdots, K\}$, R_k^{Sec}, is nonpositive, it implies the fact that the BS consumes power to transmit information to desired user k while the SST of the considered system is reduced, which contradicts to our target of maximizing the system SST. Yet, we indicate that the above-mentioned issue can be overcome by applying the proposed resource allocation algorithm in a way that insecure transmission of active user k is shut down, and the corresponding power is redistributed to other active users.

It should be noted that the considered resource allocation optimization problem 3.9 is a non-convex optimization problem. Specifically, the non-convexity with respect to the beamforming vector $\mathrm{w}_k, \forall k \in \{1, \cdots, K\}$ and artificial noise covariance matrix $\mathbf{V}$, is due to the objective function and constraint C4. In next chapter, we propose an optimal resource allocation algorithm based on monotonic optimization to achieve the optimal solution of the considered non-convex optimization problem. In addition, we also design a less computationally complex suboptimal resource allocation algorithm by formulating the considered optimization problem into a form of Difference of Convex Programming (DCP).

Chapter 4

Solution of the Optimization Problem

In this chapter, we propose an optimal resource allocation algorithm based on MO, which achieves a globally optimal solution for problem 3.9. Then, considering the hardware limits of practical systems, we also pose a suboptimal algorithm with low computational complexity which obtains a locally optimal solution for problem 3.9. In addition, some mathematical preliminaries are introduced before we present the algorithms.

4.1 Mathematical Preliminaries

In this section, we introduce some mathematical preliminaries which are related to the proposed optimal resource allocation algorithm in next section.

*Definition 1 (**Increasing function**):* A function f: $\mathbb{R}_+^n \rightarrow \mathbb{R}$ is increasing if $f(x) \leq f(y)$ when $0 \leq x \leq y$.

*Definition 2 (**Box**):* Given a vector $\mathbf{x} \in \mathbb{R}^n$, the hyper rectangle $[\mathbf{0}, \mathbf{b}] = \{\mathbf{x} \mid \mathbf{0} \preceq \mathbf{x} \preceq \mathbf{b}\}$ is referred to as a box with vertex $\mathbf{b}$.

*Definition 3 (**Normal set**):* A set $\mathscr{G} \in \mathbb{R}_+^n$ is normal if for any point $\mathbf{x} \in \mathscr{G}$, all other points $\mathbf{x}'$ such that $\mathbf{0} \leq \mathbf{x}' \leq \mathbf{x}$ are also in set $\mathscr{G}$.

*Definition 4 (**Conormal set**):* A set $\mathscr{H} \in \mathbb{R}_+^n$ is conormal if for any point $\mathbf{x} \in \mathscr{G}$, all other points $\mathbf{x}'$ such that $\mathbf{x}' \geq \mathbf{x}$ are also in set $\mathscr{H}$. Besides, if a set $\mathscr{H}$ is conormal in a box $[\mathbf{0}, \mathbf{b}]$, then the set $\mathscr{H}$ is normal.

Proposition 1: The union and the intersection of normal sets are still normal set.

*Definition 5 (**Polyblock**):* A set $\mathscr{P} \in \mathbb{R}_+^n$ is called a polyblock if it is a union of a finite number of boxes $[\mathbf{0}, \mathbf{x}]$, where vertex $\mathbf{x} \in \mathscr{T}$ and $|\mathscr{T}| < +\infty$.

Proposition 2: Any polyblock is closed and normal. The intersection of finitely many polyblocks is a polyblock.

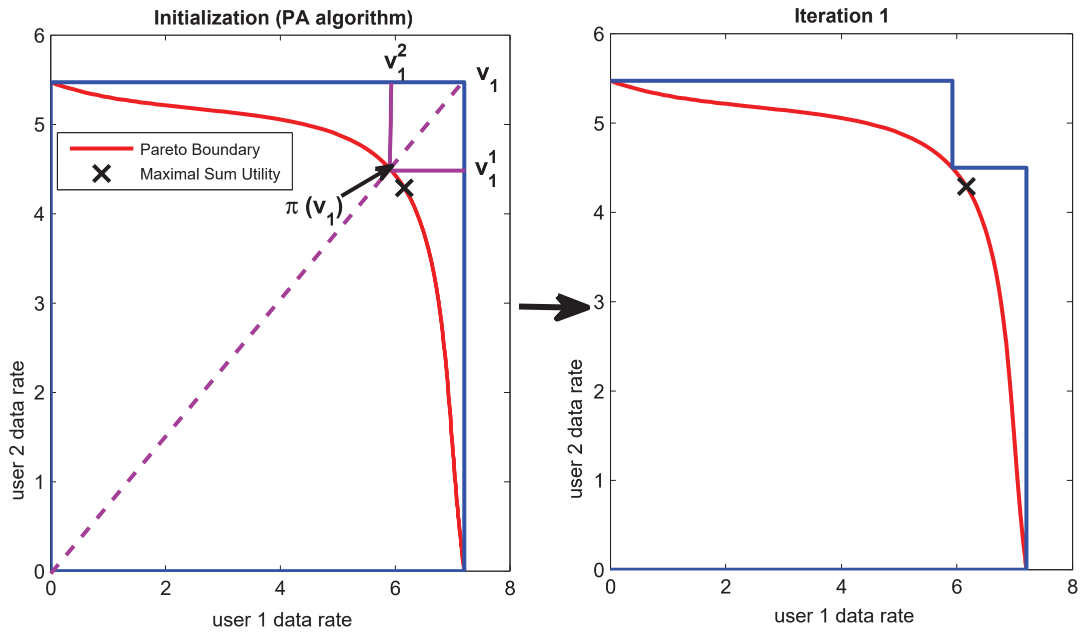

Figure 4.1: Illustration of the mathematical preliminaries which are related to the proposed optimal resource allocation algorithm.

*Definition 6 (**Proper**):* An element $\mathbf{x} \in \mathscr{T}$ is said to be proper if there is no element $\mathbf{x}' \in \mathscr{T}$ such that $\mathbf{x} \preceq \mathbf{x}'$ and $\mathbf{x} \neq \mathbf{x}'$. A set $\mathscr{T}$ is a proper set if every element $\mathbf{x} \in \mathscr{T}$ is proper.

Proposition 3: If vector variable $\mathbf{x}$ belongs to a polyblock $\mathscr{P}$, and $f(\mathbf{x}) : \mathbb{R}_+^n \to \mathbb{R}$ is an increasing function of $\mathbf{x}$, then the maximum of $f(\mathbf{x})$ over polyblock $\mathscr{P}$ must occur at one proper vertex of $\mathscr{P}$.

*Definition 7 (**Projection**):* Given any vector variable $\mathbf{x} \in \mathbb{R}_+^n$ and any nonempty normal set $\mathscr{G} \in \mathbb{R}_+^n$, $\pi_{\mathscr{G}}(\mathbf{x})$ is a projection of $\mathbf{x}$ on $\mathscr{G}$ if $\pi_{\mathscr{G}}(\mathbf{x}) = \lambda\mathbf{x}$ with $\lambda = \max\{\eta \mid \eta\mathbf{x} \in \mathscr{G}\}$.

*Definition 8 (**Upper boundary**):* A point $\mathbf{y} \in \mathbb{R}_+^n$ is an upper boundary point of a bounded normal set $\mathscr{G}$ if $\mathbf{x} \in \mathscr{G}$ while $\mathscr{K}_{\mathbf{y}} \in \mathbb{R}_+^n \setminus \mathscr{G}$ with $\mathscr{K}_{\mathbf{y}} = \left\{\mathbf{y}' \in \mathbb{R}_+^n | \mathbf{y}' \succeq \mathbf{y} \text{ and } \mathbf{y}' \neq \mathbf{y}\right\}$.

In Fig. 4.1, we illustrate the above concepts. Specifically, the blue rectangle in the left part represents the box $[\mathbf{0}, \mathbf{v}_1]$, and $\mathbf{v}_1$ is the respective vertex of the box. The area below the blue curves represents polyblocks $\mathscr{P}_1 = [\mathbf{0}, \mathbf{v}_1]$ with proper vertex $\mathbf{v}_1$ and $\mathscr{P}_2 = \left[\mathbf{0}, \mathbf{v}_1^1\right] \cup \left[\mathbf{0}, \mathbf{v}_1^2\right]$ with proper vertex set $\mathscr{T} = \{\mathbf{v}_1, \mathbf{v}_2\}$, respectively. It can be seen that if a point $\mathbf{x}$ is in polyblock $\mathscr{P}_1$ and $\mathscr{P}_2$, then any point $\mathbf{x}'$ such that $\mathbf{0} \leq \mathbf{x}' \leq \mathbf{x}$ also belongs to these polyblocks. Hence, polyblocks $\mathscr{P}_1$ and $\mathscr{P}_2$ are said to be normal.

Moreover, we indicate the red curve as the upper boundary of a normal set $\mathscr{G}$. Then, the point $\pi_{\mathscr{G}}(\mathbf{v}_1)$ is a projection of $\mathbf{v}_1$ on set $\mathscr{G}$. We suppose a function $f(\mathbf{v})$ is increasing on polyblock $\mathscr{P}_2$, then $f(\mathbf{v}) \leq \max\{f(\mathbf{v}_1), f(\mathbf{v_2})\}$ for all $\mathbf{v} \in \mathscr{P}_2$ which means the maximum of the increasing function $f(\mathbf{v})$ occurs only at the proper vertex of polyblock $\mathscr{P}_2$.

4.2 Optimal Resource Allocation Scheme

We notice that the objective function in problem 3.9 is the sum of difference of two logarithmic functions which are monotonically increasing in their domains. After several mathematical transformation steps, the objective function can be reformulated into a canonical form of monotonically increasing function. Moreover, the feasible set of the optimization problem 3.9 is an intersection of a normal set and a conormal set, where the normal set is defined by constraint C1, C3, C4, C5 and the conormal set is defined by constraint C2, C3, C4, C5. Therefore, we can obtain the optimal solution of the considered optimization problem by adopting monotonic optimization approach.

The issue of transforming the objective function into a form of monotonically increasing function can be resolved by rewriting the achievable rate between the BS and potential eavesdropper for eavesdropping desired active user k, i.e., R_k^E, into a form of a constant subtracting a variable. Specifically, we first seek an upper bound of R_k^E as follows,

$$R_k^{E,upper} = \max_{\mathbf{W}_k, \mathbf{V}} \left\{ \log_2\Big(1 + \frac{\mathrm{Tr}(\mathbf{LW}_k)}{\mathrm{Tr}(\mathbf{LV}) + \sigma_n^2}\Big) \right\}. \tag{4.1}$$

Since $\mathbf{L}, \mathbf{V}, \mathbf{W}_k \in \mathbb{H}^{N_\mathrm{T}}$ are positive semi-definite matrices of the same size, we derive a sequence of inequalities,

$$\frac{\mathrm{Tr}(\mathbf{LW}_k)}{\mathrm{Tr}(\mathbf{LV}) + \sigma_n^2} \overset{(a)}{\leq} \frac{\mathrm{Tr}(\mathbf{LW}_k)}{\sigma_n^2} \overset{(b)}{\leq} \frac{\mathrm{Tr}(\mathbf{L})\mathrm{Tr}(\mathbf{W}_k)}{\sigma_n^2} \overset{(c)}{\leq} \frac{P_{\max}\mathrm{Tr}(\mathbf{L})}{\sigma_n^2} \tag{4.2}$$

where inequality (a) always holds as both the numerator and denominator are non-negative. Inequality (b) can be proven by CauchyâĂŞSchwarz inequality. Inequality (c) always holds since constraint C1 bounds $\mathrm{Tr}(\mathbf{W}_k) \leq P_{\max}$. Hence, we obtain an upper bound of R_k^E, where

$$R_k^{E,upper} = \log_2(1 + \frac{P_{\max}\mathrm{Tr}(\mathbf{L})}{\sigma_n^2}). \tag{4.3}$$

It can be observed that the upper bound is a constant as long as the channel vector between the BS and the potential eavesdropper is perfectly known at the BS. As a result, we omit the active user index k of the upper bound $R_k^{E,upper}$ in the rest part of this chapter, since perfect CSI is assumed at the BS.

We note that the constant to rewrite R_k^E is possessed now, and then we define a new slack t_k and rewrite R_k^E and the objective function in problem 3.9 as follows, respectively

$$R_k^E = R^{E,upper} - t_k, \tag{4.4}$$

$$\sum_{k=1}^{K}(R_k - t_k) - KR^{E,upper}, \tag{4.5}$$

and for the sake of notational simplicity, we define $t = \sum_{k=1}^{K} t_k$ to collect all t_k.

On the other hand, it should be noted that the achievable rate between the BS and the k-th active user, R_k, is a monotonic increasing function of the received SINR at k-th active user, Γ_k. To facilitate monotonic optimization, we introduce a slack $\mathbf{z} \in \mathcal{G}$, where $\mathcal{G} \in \mathbb{R}^K$ is a normal set, and

$$\mathcal{G} = \{\, \mathbf{z} \mid 1 \leq z_k \leq 1 + \Gamma_k(\mathbf{W}, \mathbf{V}),\ \mathbf{W} \in \mathcal{P},\ \mathbf{V} \in \mathcal{Q},\ \forall k \in \{1, \cdots, K\}\}$$

where $\mathcal{P}$ is a set defined by C1, C2, C4 and C5, and $\mathcal{Q}$ is a set defined by C1, C2 and C3.

Now we can rewrite problem 3.9 as a canonical monotonic optimization problem:

$$\underset{(\mathbf{z},t)\in\mathcal{D}}{\text{maximize}} \ \ \Phi(\mathbf{z}, t) = \sum_{k=1}^{K} \log_2(z_k) + t, \tag{4.6}$$

where the feasible set $\mathcal{D} \in \mathbb{R}^K \times \mathbb{R}$ is defined as

$$\mathcal{D} = \left\{ \, (\mathbf{z}\,, t) \mid \mathbf{z} \in \mathcal{G},\ 0 \leq t \leq KR^{E,upper} \right\} \tag{4.7}$$

We note that the objective function of problem 4.6 is a monotonic increasing function of $(\mathbf{z}, t)$ over the feasible set $\mathcal{D}$, and the optimal solution for problem 4.6, denoted by $(\mathbf{z}^*, t^*)$, must occur at the upper boundary of the feasible set $\mathcal{D}$, where $z_k = 1 + \Gamma_k(\mathbf{W}_k, \mathbf{V})$ for all k. Conversely, if a solution $(\mathbf{W}^*, \mathbf{V}^*)$ leads to the optimal solution $\mathbf{z}^*$, where $z_k^* = \Gamma_k(\mathbf{W}_k, \mathbf{V})$ for all k, then such $(\mathbf{W}^*, \mathbf{V}^*)$ is the optimal solution for problem 3.9. As a result, problem 3.9 and 4.6 are equivalent to each other. Besides, it should be noted that the feasible $\mathcal{D}$ is a subspace of $\mathbb{R}^K \times \mathbb{R}$, where the vector $\mathbf{z}$ is in $\mathbb{R}^K$, and variable t belongs to a plane which is orthogonal to $\mathbb{R}^K$.

Next, we design an optimal resource allocation algorithm to solve the monotonic optimization problem 4.6 based on the polyblock outer approximation [16], [20], [26]. Since the upper boundary of the feasible set $\mathcal{D}$ is unknown in advance, we approach the boundary by iteratively pruning a polyblock which always contains the feasible set. Specifically, we initially construct a polyblock $\mathcal{P}_1$ which includes the feasible set $\mathcal{D}$ with only one vertex $(\mathbf{s}_1, t_1)$ in the vertex set $\mathcal{T}_1$. It should be noted that $\mathbf{s}_1$ consists of all the

Algorithm 1 Polyblock Outer Approximation Algorithm

```
Set polyblock $\mathscr{P}_1$ with vertex set $\mathscr{T}_1 = (\mathbf{s}_1, t_1)$, where $\mathbf{s}_1$ consists of optimum points of all single-user optimization problem under the same constraints and $t_1 = KR^E_{k,upper}$; set convergence tolerance $0 \le \varepsilon \ll 1$ and maximum iteration $M_{\mathrm{POA}}$
Initialize $CBV_0 = 0$ and iteration index $i = 1$.
repeat
    $i = i + 1$
    Select $(\mathbf{s}_i, t_i) = \arg\max_{(\mathbf{s}_i, t_i) \in \mathscr{T}_i} \Phi(\mathbf{s}_i, t_i)$
    Compute $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$, the projection of $(\mathbf{s}_i, t_i)$ on the boundary of $\mathscr{D}$ based on Algorithm 2
    if $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i) = (\mathbf{s}_i, t_i)$ then
        set $(\mathbf{s}^*_{\mathbf{i}}, t^*_i) = (\mathbf{s}_i, t_i)$ and $CBV_i = \Phi(\mathbf{s}_i, t_i)$, and terminate the algorithm
    else if $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i) \in \mathscr{D}$ and $\Phi(\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)) \ge CBV_{i-1}$ then
        set $(\mathbf{s}^*_{\mathbf{i}}, t^*_i) = \pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$ and $CBV_i = \Phi(\pi_{\mathscr{D}}(\mathbf{s}_i, t_i))$
    else
        Set $(\mathbf{s}^*_{\mathbf{i}}, t^*_i) = (\mathbf{s}^*_{i-1}, t^*_{i-1})$ and $CBV_i = CBV_{i-1}$
    end if
    Update vertex set based on $\mathscr{T}_{i+1} = (\mathscr{T}_i \backslash \mathscr{T}_*) \cup \{(\mathbf{s}^k_i, \widetilde{t}_i) \mid \mathbf{s}^k_i = \mathbf{s}_i - (s^k_i - \pi^k_{\mathscr{D}}(\mathbf{s}_i, t_i))\mathbf{e}^k\}$, where $\widetilde{t}_i \in \{t_i, \widehat{t}_i\}$, $\widehat{t}_i = \pi^{K+1}_{\mathscr{D}}(\mathbf{s}_i, t_i), (\mathbf{s}_i, t_i) \in \mathscr{T}_*$, $\mathscr{T}_* = \{(\mathbf{s}, t) \in \mathscr{T}_i \mid (\mathbf{s}, t) > \pi_{\mathscr{D}}(\mathbf{s}_i, t_i)\}$.
until $|\Phi(\mathbf{s}_i, t_i) - CBV_i| \le \varepsilon$ or $i > M_{\mathrm{OPA}}$.
Obtain the optimal solution $(\mathbf{s}^*_i, t^*_i)$ and optimal value $\Phi(\mathbf{s}^*_i, t^*_i)$.
```

optimum points [1] and $t_1 = KR^{E,upper}$. Then, in the i-th iteration, we take every vertex $(\mathbf{s}_i, t_i)$ in the vertex set $\mathscr{T}_i$ back into the objective function of the monotonic optimization problem to compute $\Phi(\mathbf{s}_i, t_i)$. The largest function value $\Phi(\mathbf{s}_i, t_i)$ in the i-th iteration is defined as the current best value, i.e., CBV_i. Next, we choose the vertex which gives the largest function value, and then compute its projection on the feasible set $\mathscr{D}$, $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$ and the corresponding function value $\Phi(\pi_{\mathscr{D}}(\mathbf{s}_i, t_i))$, respectively.

Based on the aforementioned CBV_i, $\Phi(\mathbf{s}_i, t_i)$, $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$, and $\Phi(\pi_{\mathscr{D}}(\mathbf{s}_i, t_i))$, we update the current best value CBV_i and the vertex set $\mathscr{T}_i$. Every vertex $(\mathbf{s}_i, t_i)$ in the vertex set is replaced by K new vertices $\{(\mathbf{s}^1_i, \widetilde{t}_i), \cdots, (\mathbf{s}^k_i, \widetilde{t}_i), \cdots, (\mathbf{s}^K_i, \widetilde{t}_i)\}$, $k \in \{1, \cdots, K\}$. In particular, we have $\mathbf{s}^k_i = \mathbf{s}_i - (s^k_i - \pi^k_{\mathscr{D}}(\mathbf{s}_i, t_i))\mathbf{e}^k$, where s^k_i is the k-th element of $\mathbf{s}_i$, $\pi^k_{\mathscr{D}}(\mathbf{s}_i, t_i)$ is the the k-th element of $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$, and $\mathbf{e}^k$ is a unit-norm vector whose k-th element is one. Besides, $\widetilde{t}_i$ belongs to the set $\{t_i, \widehat{t}_i\}$, and $\widehat{t}_i$ can be obtained by $\widehat{t}_i = \pi^{K+1}_{\mathscr{D}}(\mathbf{s}_i, t_i)$, where $\pi^{K+1}_{\mathscr{D}}(\mathbf{s}_i, t_i)$ is the $K+1$-th element of $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$. The algorithm is terminated if $|\Phi(\mathbf{s}_i, t_i) - CBV_i| \le \varepsilon$ or $i > M_{\mathrm{POA}}$, where $0 \le \varepsilon \ll 1$ is the optimal solution tolerance factor which specifies the accuracy of the approximation, and M_{POA} is the maximum iterations which guarantee the termination of the algorithm within a finite amount of time. The proposed POA algorithm is summarized in **Algorithm 1**. The projection of the vertex $(\mathbf{s}_i, t_i)$, i.e., $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i)$, can be obtained by using **Algorithm 2** which is based

[1] The optimum points are obtained by solving the optimization problems for maximizing secrecy rate of the considered system in presence of single active user and single potential eavesdropper under the same constraints.

Algorithm 2 Projection Bisection Search Algorithm

```
Initialize $\lambda_{\min} = 0$, $\lambda_{\max} = 1$, iteration index $j = 1$, and convergence tolerance $0 < \delta \ll 1$
repeat
    Calculate $\lambda_j$ based on $\lambda_j = (\lambda_{\min} + \lambda_{\max})/2$
    if $\lambda_j(\mathbf{s}_i, t_i) \in \mathscr{D}$ then
        set $\lambda_{\min} = \lambda_j$
    else
        set $\lambda_{\max} = \lambda_j$
    end if
    $j = j + 1$
until $\lambda_{\max} - \lambda_{\min} \le \delta$
Calculate projection $\pi_{\mathscr{D}}(\mathbf{s}_i, t_i) = \lambda_{\min}(\mathbf{s}_i, t_i)$
```

on bisection search algorithm. The optimal solution approximation factor $0 < \delta \ll 1$ in **Algorithm 2** specifies the accuracy of computing projection.

It should be noted that checking $\lambda_j(\mathbf{s}_i, t_i) \in \mathscr{D}$ in **Algorithm 2** involving solving a one-dimensional optimization problem in each iteration j as follows:

$$\begin{aligned} & \max\left\{\lambda_j \mid \lambda_j s_i^k \le 1 + \Gamma_k(\mathbf{W},\mathbf{V}),\ \mathbf{W} \in \mathscr{P},\ \mathbf{V} \in \mathscr{Q},\ \forall k \in \{1,\cdots,K\}\right\} \\ = \quad & \max\left\{\lambda_j \mid \lambda_j \le \min_{k\in\{1,\cdots,K\}} \frac{f_k(\mathbf{W},\mathbf{V})}{g_k(\mathbf{W},\mathbf{V})s_i^k},\ \mathbf{W} \in \mathscr{P},\ \mathbf{V} \in \mathscr{Q},\ \forall k \in \{1,\cdots,K\}\right\} \\ = \quad & \max_{\mathbf{W}\in\mathscr{P},\ \mathbf{V}\in\mathscr{Q}} \ \min_{k\in\{1,\cdots,K\}} \frac{f_k(\mathbf{W},\mathbf{V})}{g_k(\mathbf{W},\mathbf{V})s_i^k}, \end{aligned} \tag{4.8}$$

where

$$f_k(\mathbf{W},\mathbf{V}) = \sum_{r=1}^{K} \mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k\mathbf{V}) + \sigma_n^2, \tag{4.9}$$

$$g_k(\mathbf{W},\mathbf{V}) = \sum_{r\neq k}^{K} \mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k\mathbf{V}) + \sigma_n^2, \tag{4.10}$$

and 4.8 is a standard linear fractional programming problem. In consequence, it can be solved by the Dinkelbach algorithm [27] in polynomial time or be reformulated into a convex problem via applying the Charnes-Cooper transformation [28] and then be solved by using interior point method. On the other hand, the optimal resource allocation policy

$(\mathbf{W}_j^*, \mathbf{V}_j^*)$ in each iteration j in **Algorithm 2** can be obtained by solving the following non-convex problem:

$$\begin{aligned} (\mathbf{W}_j^*, \mathbf{V}_j^*) = & \arg\max_{\mathbf{W},\mathbf{V},\mu} \mu \\ \text{subject to} \quad & \text{C1-C5}, \text{C6}: f_k(\mathbf{W},\mathbf{V}) - \lambda_j s_i^k g_k(\mathbf{W},\mathbf{V}) \geq \mu, \ \forall k. \end{aligned} \tag{4.11}$$

We note that by applying the Semidefinite Programming (SDP) relaxation method which is proposed in [29]–[31], we can omit the non-convex constraint C4 and transform the problem 4.11 into a convex SDP which can be efficiently solved by mature convex program solvers such as CVX [32] and CVXOPT [33]. At the end of this section, we will give the corresponding proof that solving the relaxed 4.11 yields the optimal rank-one matrix $\mathbf{W}^*$.

Furthermore, as the optimal solution factors ε and δ tend to 0, we obtain the globally optimal resource allocation policy of problem 4.6. However, the above-mentioned algorithms are extremely time-consuming, since the computational complexity of the proposed algorithm grows exponentially with the number of active users, K, used in each iteration. In order to achieve a balance between optimality and efficiency, we propose a suboptimal scheme which requires polynomial time computational complexity in next section. Notwithstanding, it should be noted that the proposed optimal algorithm is useful, since it can be regarded as a performance benchmark for any other scheme.

Next, we give the proof that the solving the considered relaxed problem 4.11 always yields an optimal rank-one matrix $\mathbf{W}_j^*$. We first write the Lagrangian dual function of the relaxed problem 4.11 as follows:

$$\begin{aligned} \mathscr{L} = & \ \zeta \sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k) - \sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k \mathbf{Y}_k) - \sum_{k=1}^{K} \kappa_k \left[f_k(\mathbf{W},\mathbf{V}) - \lambda_j s_i^k g_k(\mathbf{W},\mathbf{V}) \right] \\ + & \sum_{k=1}^{K} \eta_k \Big(\Gamma_{\text{req}} \sum_{r=1}^{K} \text{Tr}(\mathbf{H}_k \mathbf{W}_r) - (1+\Gamma_{\text{req}}) \text{Tr}(\mathbf{H}_k \mathbf{W}_k) \Big) + \Psi, \end{aligned} \tag{4.12}$$

where Ψ denotes the collection of primal and dual variables and constants that are not related to the proof. Variables ζ, η_k, and κ_k are the Lagrange multipliers associated with constraints C1, C2, and C6, respectively. Matrices $\mathbf{X} \in \mathbb{C}^{N_\text{T} \times N_\text{T}}$ and $\mathbf{Y}_k \in \mathbb{C}^{N_\text{T} \times N_\text{T}}$ are the Lagrange multipliers associated with the positive semidefinite constraints C3 and C5 with respect to matrices $\mathbf{V}$ and $\mathbf{W}_k$, respectively. Therefore, the dual problem for the SDP relaxed problem is given by

$$\underset{\mathbf{X},\mathbf{Y}_k \succeq \mathbf{0}, \zeta, \eta_k, \kappa_k}{\text{maximize}} \ \underset{\mathbf{W}_k, \mathbf{V} \in \mathbb{H}^{N_\text{T}}, \mu}{\text{minimize}} \ \mathscr{L}(\mathbf{W}_k, \mathbf{V}, \mu, \mathbf{Y}_k, \mathbf{X}, \zeta, \eta_k, \kappa_k). \tag{4.13}$$

We note that the relaxed SDP problem in dual problem 4.13 is jointly convex with respect to the optimization variables and satisfies the Slater's constraint qualification. Thus, solving the primal and dual optimal values are attained and equal, and strong duality holds [34]. Then, noticing the functions in primal optimization problem are differentiable, we follow a similar approach as proposed in [11], [35], to reveal the structure of the optimal $\mathbf{W}_k$ of dual problem 4.13 by studying the Karush-Kuhn-Tucker (KKT) conditions. The KKT conditions for the optimal $\mathbf{W}_k^*$ are given by:

$$\zeta^*, \eta_k^*, \kappa_k^* \geq 0, \mathbf{Y}_k^* \succeq \mathbf{0}, \tag{4.14}$$

$$\mathbf{Y}_k^* \mathbf{W}_k^* = \mathbf{0}, \tag{4.15}$$

$$\nabla_{\mathbf{W}_k^*} \mathscr{L} = \mathbf{0}, \tag{4.16}$$

where ζ^*, η_k^*, $\kappa_k^* \geq 0$, and $\mathbf{Y}_k^*$ are the optimal Lagrange multipliers for dual problem 4.13, and $\nabla_{\mathbf{W}_k^*} \mathscr{L}$ denotes the gradient of Lagrangian function with respect to $\mathbf{W}_k^*$. Moreover, we express 4.16 as

$$\mathbf{Y}_k^* = \zeta^* \mathbf{I}_{N_\mathrm{T}} - \Phi, \tag{4.17}$$

where

$$\Phi = \sum_{r=1}^{K} (1 - \lambda_j s_i^k) \kappa_r^* \mathbf{H}_r - \Gamma_{\mathrm{req}} \sum_{r=1}^{K} \eta_r^* \mathbf{H}_r + \left[\lambda_j s_i^k \kappa_k^* + (1 + \Gamma_{\mathrm{req}}) \eta_k^* \right] \mathbf{H}_k. \tag{4.18}$$

Next, we give the explanation why Φ must be positive semidefinite. We first assume Φ is a negative definite matrix, then from 4.17, $\mathbf{Y}_k^*$ need to be a full-rank positive definite matrix. Considering 4.15, $\mathbf{W}_k^*$ must be a zero matrix which cannot be the optimal solution. Hence, we concentrate on the case where Θ is a positive semidefinite matrix in the rest part of the proof. Due to the fact that matrix $\mathbf{Y}_k^* = \zeta^* \mathbf{I}_{N_\mathrm{T}} - \Phi$ is positive semidefinite, we have

$$\zeta^* \geq \nu_\Phi^{\max} \geq 0, \tag{4.19}$$

where $\nu_\Phi^{\max}$ is the real-valued maximum eigenvalue of matrix Θ. Reviewing the rewritten KKT condition in 4.17, we note that if $\zeta^* > \nu_\Phi^{\max}$, matrix $\mathbf{Y}_k^*$ is a full-rank positive definite matrix. Yet, this will lead to that the solution $\mathbf{W}_k^*$ becomes a zero matrix which conflicts with the KKT condition in 4.14 where $\zeta^* > 0$ and $P_{\max} > 0$. Thus, for the optimal solution, the optimal Lagrange multiplier ζ^* has to be equal to the maximum eigenvalue of matrix Φ, i.e., $\zeta^* = \nu_\Phi^{\max}$. In addition, we note that there must exist a vector $\mathbf{p}_{\nu_\Phi^{\max}}$ of matrix $\mathbf{Y}_k^*$ satisfying $\mathbf{Y}_k^* \mathbf{p}_{\nu_\Phi^{\max}} = \mathbf{0}$, where $\mathbf{p}_{\lambda_\Phi^{\max}} \in \mathbb{C}^{N_\mathrm{T} \times 1}$ and $\mathbf{p}_{\lambda_\Phi^{\max}}$ is the unit-norm eigenvector of matrix Φ corresponding to eigenvalue $\nu_{\Phi}^{\max}$. As a result, the optimal beamforming matrix $\mathbf{W}_k^*$ must be a rank-one matrix which can be expressed as

$$\mathbf{W}_k^* = \xi \mathbf{p}_{\nu_{\Phi}^{\max}} \mathbf{p}_{\nu_{\Phi}^{\max}}^H, \tag{4.20}$$

where ξ is a parameter which fulfills the maximum transmit power constraint C1 at the BS.

4.3 Suboptimal Resource Allocation Scheme

In this section, we design a low computationally complex suboptimal resource allocation algorithm based on successive convex approximation to achieve a locally optimal solution of problem 3.9. To facilitate the presentation, we first rewrite the objective function in problem 3.9 as

$$F(\mathbf{W},\mathbf{V}) - G(\mathbf{W},\mathbf{V}), \tag{4.21}$$

where

$$F(\mathbf{W},\mathbf{V}) = \sum_{k=1}^{K} \log_2(\sum_{r=1}^{K} \mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k\mathbf{V}) + \sigma_n^2) + K\log_2(\mathrm{Tr}(\mathbf{L}\mathbf{V}) + \sigma_n^2), \tag{4.22}$$

$$G(\mathbf{W},\mathbf{V}) = \sum_{k=1}^{K} \log_2(\sum_{r\neq k}^{K} \mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k\mathbf{V}) + \sigma_n^2) + \sum_{k=1}^{K} \log_2(\mathrm{Tr}(\mathbf{L}\mathbf{W}_k) + \sigma_n^2). \tag{4.23}$$

For the sake of notational simplification, we collect all $\mathbf{W}_k$ in $\mathbf{W} \in \mathbb{C}^{K\times N_{\mathrm{T}}}$.

We notice that the rewritten objective function in Eq. (4.21) has a canonical form of DCP. As discussed in [36]–[38], finding an algorithm that optimally solves a DCP is in general an open problem. On the other hand, several convex-based approaches have been proposed to obtain a locally optimal solution in DCP optimization problems [38], [39]. In this thesis, we design a suboptimal resource allocation algorithm based on SCA as proposed in [40]. Specifically, since $G(\mathbf{W},\mathbf{V})$ is a differentiable convex function, for any feasible point $\mathbf{W}^{(m)}$ and $\mathbf{V}^{(m)}$, the following inequality can be derived,

$$\begin{aligned} G(\mathbf{W},\mathbf{V}) \;\geq\; & G(\mathbf{W}^{(m)},\mathbf{V}^{(m)}) + \mathrm{Tr}(\nabla_{\mathbf{W}} G(\mathbf{W}^{(m)},\mathbf{V}^{(m)})^H(\mathbf{W}-\mathbf{W}^{(m)})) && (4.24)\\ + \;& \mathrm{Tr}(\nabla_{\mathbf{V}} G(\mathbf{W}^{(m)},\mathbf{V}^{(m)})^H(\mathbf{V}-\mathbf{V}^{(m)})), && (4.25)\end{aligned}$$

and we note that the inequality can be proven by applying the first-order conditions of convex function [34]. Moreover, we define the right hand side of the above inequality as $\overline{G}(\mathbf{W},\mathbf{V})$ which is an affine function and represents the global underestimation of

Algorithm 3 Successive Convex Approximation Algorithm

```
1: Set initial point $\mathbf{W}^{(1)}, \mathbf{V}^{(1)}$, iteration index $m = 1$, convergence tolerance $0 < \epsilon_{\text{SCA}} \ll$, and the maximum number of iterations $M_{\text{SCA}}$
2: repeat
3:     Solve problem 4.26 for a given $\mathbf{W}^{(m)}$ and $\mathbf{V}^{(m)}$, and store the intermediate resource allocation policy $(\mathbf{W}, \mathbf{V})$
4:     Set $\mathbf{W}^{(m)} = \mathbf{W}$ and $\mathbf{V}^{(m)} = \mathbf{V}$
5:     Set $m = m + 1$
6: until $m = M_{\text{SCA}}$ or $\frac{r(\mathbf{W}^{(m)}, \mathbf{V}^{(m)}) - r(\mathbf{W}^{(m-1)}, \mathbf{V}^{(m-1)})}{r(\mathbf{W}^{(m-1)}, \mathbf{V}^{(m-1)})} \leq \epsilon_{\text{SCA}}$
7: Obtain the suboptimal solution $\mathbf{W}^{(*)} = \mathbf{W}^{(m)}$, $\mathbf{V}^{(*)} = \mathbf{V}^{(m)}$
```

$G(\mathbf{W}, \mathbf{V})$. To obtain an upper bound of 4.21 with respect to any feasible point $\mathbf{W}^{(m)}$ and $\mathbf{V}^{(m)}$, we can solve the following optimization problem:

$$\begin{aligned} \underset{\mathbf{W}_k, \mathbf{V} \in \mathbb{H}^{N_\text{T}}}{\text{maximize}} \quad & r(\mathbf{W}, \mathbf{V}) \overset{\Delta}{=} F(\mathbf{W}, \mathbf{V}) - \overline{G}(\mathbf{W}, \mathbf{V}) \\ \text{subject to} \quad & \text{C1} : \sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k) + \text{Tr}(\mathbf{V}) \leq P_{\max}, \\ & \text{C2} : \frac{\text{Tr}(\mathbf{H}_k \mathbf{W}_k)}{\sum_{r \neq k}^{K} \text{Tr}(\mathbf{H}_k \mathbf{W}_r) + \text{Tr}(\mathbf{H}_k \mathbf{V}) + \sigma_n^2} \geq \Gamma_{\text{req}}, \ \forall k, \\ & \text{C3} : \mathbf{V} \succeq \mathbf{0}, \quad \text{C4} : \text{Rank}(\mathbf{W}_k) \leq 1, \ \forall k, \quad \text{C5} : \mathbf{W}_k \succeq \mathbf{0}, \ \forall k. \end{aligned} \tag{4.26}$$

In problem 4.26, the only obstacle to implement SCA algorithm is the non-convex rank-one constraint C4. Following the similar approach as in [41]–[43], we can omit constraint C4 and transform the problem 4.26 into a convex SDP which can be efficiently solved by mature convex program solvers such as CVX [32] and CVXOPT [33]. In the end of this section, we verify the tightness of the adopted semidefinite relaxation. The proposed SCA algorithm is summarized in **Algorithm 3**.

It should be noted that the optimal value of problem 4.26 serves as an upper bound of the original optimization problem 3.9. However, as we iteratively apply SCA algorithm, the upper bound can gradually be tightened. After reaching the maximum number of iterations M_{SCA} or the local convergence, the proposed algorithm generate the candidate solution $(\mathbf{W}^*, \mathbf{V}^*)$, and the locally optimal value can be obtained by taking the $(\mathbf{W}^*, \mathbf{V}^*)$ back into the objective function in problem 3.9. It can be shown that the proposed SCA algorithm converges to the locally optimal value of problem 3.9 with polynomial time computational complexity [39]–[45].

Next, we give the proof that the considered relaxation method is tightened when the maximum transmit power at the BS is greater than 0, i.e., $P_{\max} > 0$. We rewrite the problem 4.26 into the following equivalent form:

$$\begin{aligned} \underset{\mathbf{W}_k,\mathbf{V}\in\mathbb{H}^{N_{\mathrm{T}}},\tau,u_k,x}{\text{maximize}} \;\; & \tau \\ \text{subject to} \;\; & \text{C1-C3}, \text{C5}, \\ & \text{C6}: \widetilde{F}(\mathbf{W},\mathbf{V}) - \overline{G}(\mathbf{W},\mathbf{V}) \geq \tau, \\ & \text{C7}: \sum_{r=1}^{K}\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) + \mathrm{Tr}(\mathbf{H}_k\mathbf{V}) \geq u_k, \; \forall k, \\ & \text{C8}: \mathrm{Tr}(\mathbf{L}\mathbf{V}) \geq x, \end{aligned} \tag{4.27}$$

where $\widetilde{F}$ is defined as follows

$$\widetilde{F}(\mathbf{W},\mathbf{V}) = \sum_{k=1}^{K}\log_2(u_k+\sigma_n^2) + K\log_2(x+\sigma_n^2) \tag{4.28}$$

and τ, u_k, and x are auxiliary optimization variables.

We note that the relaxed SDP problem in dual problem 4.27 is jointly convex with respect to the optimization variables and satisfies the Slater's constraint qualification. Hence, strong duality holds and solving the dual problem is equivalent to solving the primal problem [34]. Then, we formulate the dual problem by writing the Lagrangian function of the primal problem in dual problem 4.27:

$$\begin{aligned} \mathscr{L} = & \; \zeta\sum_{k=1}^{K}\mathrm{Tr}(\mathbf{W}_k) - \sum_{k=1}^{K}\mathrm{Tr}(\mathbf{W}_k\mathbf{Y}_k) - \sum_{k=1}^{K}\alpha_k\sum_{r=1}^{K}\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) \\ & + \sum_{k=1}^{K}\eta_k\Big(\Gamma_{\mathrm{req}}\sum_{r=1}^{K}\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r) - (1+\Gamma_{\mathrm{req}})\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_k)\Big) \\ & + \; \theta\mathrm{Tr}(\nabla_{\mathbf{W}}G(\mathbf{W}^{(m)},\mathbf{V}^{(m)})^H(\mathbf{W}-\mathbf{W}^{(m)})) + \Psi, \end{aligned} \tag{4.29}$$

where Ψ indicates the collection of primal and dual variables and constants that are not related to the proof. Variables ζ, η_k, θ, α_k, and ϕ are the Lagrange multipliers associated with constraints C1, C2, C6, C7, and C8, respectively. Matrices $\mathbf{X} \in \mathbb{C}^{N_{\mathrm{T}}\times N_{\mathrm{T}}}$ and $\mathbf{Y}_k \in \mathbb{C}^{N_{\mathrm{T}}\times N_{\mathrm{T}}}$ are the Lagrange multipliers for the positive semidefinite constraints C3 and C5 on matrices $\mathbf{V}$ and $\mathbf{W}_k$, respectively. Therefore, the dual problem for the SDP relaxed problem is given by

$$\underset{\mathbf{X},\mathbf{Y}_k\succeq\mathbf{0},\zeta,\eta_k,\theta,\alpha_k,\phi}{\text{maximize}} \;\; \underset{\mathbf{W}_k,\mathbf{V}\in\mathbb{H}^{N_{\mathrm{T}}},\tau,u_k,x}{\text{minimize}} \;\; \mathscr{L}(\mathbf{W}_k,\mathbf{V},\tau,\mathbf{Y}_k,\mathbf{X},\zeta,\eta_k,\theta,\alpha_k,\phi). \tag{4.30}$$

Then, we reveal the structure of the optimal $\mathbf{W}_k$ of dual problem 4.30 by investigating the KKT conditions. The KKT conditions for the optimal $\mathbf{W}_k^*$ are given by:

$$\begin{aligned} \zeta^*, \eta_k^*, \theta^*, \alpha_k^*, \phi^* \geq 0,\ \mathbf{Y}_k^* &\succeq \mathbf{0}, && (4.31)\\ \mathbf{Y}_k^* \mathbf{W}_k^* &= \mathbf{0}, && (4.32)\\ \nabla_{\mathbf{W}_k^*} \mathscr{L} &= \mathbf{0}, && (4.33) \end{aligned}$$

where ζ^*, η_k^*, θ^*, α_k^*, $\phi^* \geq 0$, and $\mathbf{Y}_k^*$ are the optimal Lagrange multipliers for the dual problem in 4.30, and $\nabla_{\mathbf{W}_k^*} \mathscr{L}$ denotes the gradient of Lagrangian function with respect to $\mathbf{W}_k^*$. Moreover, we rewrite 4.33 as

$$\mathbf{Y}_k^* = \zeta^* \mathbf{I}_{N_\mathrm{T}} - \Theta, \tag{4.34}$$

where

$$\Theta = -\theta^* \nabla_{\mathbf{W}_k} G(\mathbf{W}^{(m)}, \mathbf{V}^{(m)}) + \sum_{r=1}^{K} \alpha_r^* \mathbf{H}_r - \Gamma_{\mathrm{req}} \sum_{r=1}^{K} \eta_r^* \mathbf{H}_r + (1 + \Gamma_{\mathrm{req}}) \eta_k^* \mathbf{H}_k. \tag{4.35}$$

It should be noted that $\zeta^* > 0$ due to the fact that the equality in constraint C1 must hold for the optimal solution. Next, we give the reason that Θ must be positive semidefinite. We first assume Θ is a negative definite matrix, then according to 4.34, $\mathbf{Y}_k^*$ must be a full-rank positive definite matrix. Considering 4.32, $\mathbf{W}_k^*$ must be a zero matrix which cannot be the optimal solution for $P_{\max} > 0$. Hence, we only consider the case where Θ is a positive semidefinite matrix in the following discussion. Because matrix $\mathbf{Y}_k^* = \zeta^* \mathbf{I}_{N_\mathrm{T}} - \Theta$ is positive semidefinite, we have

$$\zeta^* \geq \lambda_\Theta^{\max} \geq 0, \tag{4.36}$$

where $\lambda_\Theta^{\max}$ is the real-valued maximum eigenvalue of matrix Θ. Recalling the rewritten KKT condition in 4.34, we note that if $\zeta^* > \lambda_\Theta^{\max}$, matrix $\mathbf{Y}_k^*$ is a full-rank positive definite matrix. Again, this will result in the solution $\mathbf{W}_k^*$ to be a zero matrix which contradicts the KKT condition in 4.31 where $\zeta^* > 0$ and $P_{\max} > 0$. Thus, for the optimal solution, the optimal Lagrange multiplier ζ^* has to be equal to the maximum eigenvalue of matrix Θ, i.e., $\zeta^* = \lambda_\Theta^{\max}$. In addition, we note that there must exist a vector $\mathbf{q}_{\lambda_\Theta^{\max}}$ of matrix $\mathbf{Y}_k^*$ such that $\mathbf{Y}_k^* \mathbf{q}_{\lambda_\Theta^{\max}} = \mathbf{0}$, where $\mathbf{q}_{\lambda_\Theta^{\max}} \in \mathbb{C}^{N_\mathrm{T} \times 1}$ and $\mathbf{q}_{\lambda_\Theta^{\max}}$ is the unit-norm eigenvector of matrix Θ corresponding to eigenvalue $\lambda_\Theta^{\max}$. As a result, the optimal beamforming matrix $\mathbf{W}_k^*$ must be a rank-one matrix which can be expressed as

$$\mathbf{W}_k^* = \omega \mathbf{q}_{\lambda_\Theta^{\max}} \mathbf{q}_{\lambda_\Theta^{\max}}^H \tag{4.37}$$

where ω is a parameter which satisfies the maximum transmit power constraint C1 at the BS.

Chapter 5

Extension to Robust SST Optimization

In this chapter, we extend the resource allocation optimization problem 3.9 by involving multiple potential eavesdroppers in the presence of imperfect CSI.

5.1 CSI Uncertainty Constraint Transformation

As discussed in Section 2.2, we adopt a deterministic model to capture the CSI uncertainty at all potential eavesdroppers. The optimal resource allocation policy can be obtained by solving the following optimization problem:

$$\begin{aligned} \underset{\mathbf{W}_k,\mathbf{V}\in\mathbb{H}^{N_\mathrm{T}}}{\text{maximize}} \quad & \sum_{k=1}^{K}\left[R_k - \max_{m\in\{1,\cdots,M\}}\sup_{\Delta\mathbf{l}_m\in\Omega_m}\log_2\left(1+\Gamma_{m,k}^{E}\right)\right] \\ \text{subject to} \quad & \text{C1: } \sum_{k=1}^{K}\mathrm{Tr}(\mathbf{W}_k)+\mathrm{Tr}(\mathbf{V})\le P_{\max},\ \forall k, \\ & \text{C2: } \frac{\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_k)}{\sum_{r\neq k}^{K}\mathrm{Tr}(\mathbf{H}_k\mathbf{W}_r)+\mathrm{Tr}(\mathbf{H}_k\mathbf{V})+\sigma_n^2}\ge\Gamma_{\mathrm{req}},\ \forall k, \\ & \text{C3: } \mathbf{V}\succeq\mathbf{0}, \quad \text{C4: } \mathrm{Rank}(\mathbf{W}_k)\le 1,\ \forall k, \quad \text{C5: } \mathbf{W}_k\succeq\mathbf{0},\ \forall k. \end{aligned} \tag{5.1}$$

We note that the objective function in problem 5.1 is more complicated than the previous ones, since it contains both supremum over $\Delta\mathbf{l}_m \in \Omega_m$ and maximization over $m \in \{1,\cdots,M\}$. For each potential eavesdropper, due to the CSI uncertainty, the achievable rate between the BS and idle user m for eavesdropping the k-th active user $\log_2(1+\Gamma_{m,k}^{E})$ now belongs to an infinite set in which each $\log_2(1+\Gamma_{m,k}^{E})$ corresponds to a specific $\Delta\mathbf{l}_m$. To ensure the optimal resource allocation policy is valid for all $\Delta\mathbf{l}_m$ in the CSI uncertainty set Ω_m, we suppose that the unknown channel uncertainty of idle user m, $\Delta\mathbf{l}_m$, is the most favorable one for potential eavesdropper m to wiretap the active users.

As a result, the least upper bound of the achievable rate between the BS and idle user m for eavesdropping desired active user k, i.e., the supremum of $\log_2(1+\Gamma^E_{m,k})$ over $\Delta\mathbf{l}_m \in \Omega_m$, is considered here. Then, we calculate the achievable secrecy rate between the BS and k-th active user, $R^E_{m,k}$, according to 3.5.

In order to obtain the globally optimal solution of problem 5.1, the similar monotonic optimization approach which is proposed in Section 4.2 is applied here. To facilitate monotonic optimization method, we move maximization over $m \in \{1,\cdots,M\}$ and supremum over $\Delta\mathbf{l}_m \in \Omega_m$ inside $\log_2(\cdot)$ function, since $\log_2(\cdot)$ is a monotonically increasing function. As a result, our objective function is given by

$$\underset{\mathbf{W}_k,\mathbf{V}\in\mathbb{H}^{N_\mathrm{T}}}{\text{maximize}} \quad \sum_{k=1}^{K}\left[R_k - \log_2\Big(1+\max_{m\in\{1,\cdots,M\}}\sup_{\Delta\mathbf{l}_m\in\Omega_m}\Gamma^E_{m,k}\Big)\right]. \tag{5.2}$$

However, to optimally solve the objective function, we have to spend much computational power to constantly search for the supremum in each iteration with respect to each $\Delta\mathbf{l}_m \in \Omega_m$. In order to tackle the aforesaid issue, we apply the following steps to simplify the objective function. Specifically, we define a slack $\gamma_k \in \mathbb{R}$, where

$$\gamma_k \geq \max_{m\in\{1,\cdots,M\}}\sup_{\Delta\mathbf{l}_m\in\Omega_m}\Gamma_{m,k} = \max_{m\in\{1,\cdots,M\}}\sup_{\Delta\mathbf{l}_m\in\Omega_m}\frac{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{W}_k)}{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{V})+\sigma_n^2}. \tag{5.3}$$

We note that the slack γ_m omits the supremum in the objective function by introducing a new constraint in 5.3. This constraint does not change the optimal solution of the optimization problem, since the maximum of the considered objective function still occurs at the places where equality holds in the new constraint. The considered optimization problem 5.1 is rewritten as follows:

$$\begin{aligned}\underset{\mathbf{V},\mathbf{W}_k\in\mathbb{H}^{N_\mathrm{T}},\gamma_k\in\mathbb{R}}{\text{maximize}} \quad & \sum_{k=1}^{K}[R_k - \log_2(1+\gamma_k)]\\ \text{subject to} \quad & \text{C1-C5},\\ & \text{C6: } \gamma_k \geq \max_{m\in\{1,\cdots,M\}}\sup_{\Delta\mathbf{l}_m\in\Omega_m}\frac{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{W}_k)}{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{V})+\sigma_n^2},\ \forall k,\end{aligned} \tag{5.4}$$

where constraint C6 is the new constraint introduced by slack γ_k. We notice that it contains both maximization and semi-infinite constraint which are intractable for resource allocation algorithm design. To facilitate the solution, we first deal with the maximization. Specifically, we split each constraint with respect to k further into M constraints. In other words, the left hand part γ_k is required to be greater or equal than all of the M constraints rather than the maximal one. Hence, the maximization over $m \in \{1,\cdots,M\}$ can be omitted.

Next, we handle the semi-infinite constraint of C6. In particular, instead of finding the supremum of the received SINR at potential eavesdropper m for eavesdropping active user k over uncertainty set Ω_m,

$$\sup_{\Delta\mathbf{l}_m\in\Omega_m} \frac{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{W}_k)}{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{V})+\sigma_n^2},\ \forall k, \tag{5.5}$$

we substitute $\mathbf{l}_m = \widehat{\mathbf{l}}_m + \Delta\mathbf{l}_m$ into $\Gamma_{m,k}^E$ and find an upper bound of $\Gamma_{m,k}^E$ by deriving a sequence of inequalities:

$$\begin{aligned}\Gamma_{m,k}^E &= \frac{\mathrm{Tr}\Big((\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m)(\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m)^H\mathbf{W}_k\Big)}{\mathrm{Tr}\Big((\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m)(\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m)^H\mathbf{V}\Big)+\sigma_n^2} \overset{(a)}{\leq} \frac{\mathrm{Tr}\Big((\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m)(\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m)^H\mathbf{W}_k\Big)}{\sigma_n^2}\\ &\overset{(b)}{\leq} \frac{\left|\widehat{\mathbf{l}}_m+\Delta\mathbf{l}_m\right|^2\mathrm{Tr}(\mathbf{W}_k)}{\sigma_n^2} \overset{(c)}{\leq} \frac{P_{\max}^{DL}\left(\left|\widehat{\mathbf{l}}_m\right|^2+|\Delta\mathbf{l}_m|^2\right)}{\sigma_n^2} \overset{(d)}{\leq} \frac{P_{\max}^{DL}\left(\left|\widehat{\mathbf{l}}_{\max}\right|^2+\varepsilon_{\max}^2\right)}{\sigma_n^2}.\end{aligned} \tag{5.6}$$

Specifically, inequality (a) always holds as both the numerator and denominator are non-negative. Inequality (b) and inequality (c) can be proven by CauchyâĂŞSchwarz inequality. In inequality (d), we represent $\widehat{\mathbf{l}}_{\max}$ as the channel vector $\widehat{\mathbf{l}}_m$ with the greatest absolute value and $\varepsilon_{\max}^2$ as the maximal of ε_m^2, $\forall m \in \{1,\cdots,M\}$, respectively. Therefore, an upper bound of $\Gamma_{m,k}^E$ is obtained, where

$$\Gamma^{E,upper} = \frac{P_{\max}^{DL}\left(\left|\widehat{\mathbf{l}}_{\max}\right|^2+\varepsilon_{\max}^2\right)}{\sigma_n^2}. \tag{5.7}$$

We note that the upper bound $\Gamma^{E,upper}$ is the maximum of $\Gamma_{m,k}^E$ under all constraints in the considered optimization problem, and it is independent of index k and m. Then, we define a new slack t_k which is given by

$$t_k = \log_2(1+\Gamma^{E,upper}) - \log_2(1+\gamma_k),\ \forall k \in \{1,\cdots,K\}. \tag{5.8}$$

It should be indicated that we omit the variable γ_k by replacing it with $2^{(R^{E,upper}-t_k)}-1$, where where $R^{E,upper} = \log_2(1+\Gamma^{E,upper})$. Then, we substitute $\gamma_k = 2^{(R^{E,upper}-t_k)}-1$ into constraint C6, where

$$\overline{\text{C6}}\text{: } 2^{(R^{E,upper}-t_k)}-1 \geq \sup_{\Delta\mathbf{l}_m\in\Omega_m} \frac{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{W}_k)}{\mathrm{Tr}(\mathbf{l}_m\mathbf{l}_m^H\mathbf{V})+\sigma_n^2},\ \forall k,\ \forall m. \tag{5.9}$$

Furthermore, we transform the semi-infinite constraint resulting from the CSI uncertainty set into Linear Matrix Inequalities (LMIs) using the following lemma.

Lemma (S-Procedure): let a function $f_m(\mathbf{x})$, $m \in \{1,2\}$, $\mathbf{x} \in \mathbb{C}^{N\times 1}$, be defined as

$$f_m(\mathbf{x}) = \mathbf{x}^H \mathbf{A}_m \mathbf{x} + 2\mathrm{Re}\left\{\mathbf{b}_m^H \mathbf{x}\right\} + c_m \tag{5.10}$$

where $\mathbf{A}_m \in \mathbb{H}$, $\mathbf{b}_m \in \mathbb{C}^{N\times 1}$, and $\mathrm{c}_m \in \mathbb{R}^{1\times 1}$. Then, the implication $f_1(\mathbf{x}) \le 0 \Rightarrow f_2(\mathbf{x}) \le 0$ holds if and only if there exists a $\delta \ge 0$ such that

$$\delta \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{bmatrix} - \begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{bmatrix} \succeq 0 \tag{5.11}$$

provided that there exists a point $\widehat{\mathbf{x}}$ such that $f_k(\widehat{\mathbf{x}}) < 0$.

As a result, we can apply Lemma to constraint C6. In particular, we substitute $\mathbf{l}_m = \widehat{\mathbf{l}}_m + \Delta \mathbf{l}_m$ in constraint C6. Therefore, the implication

$$\begin{aligned} \Delta \mathbf{l}_m^H \Delta \mathbf{l}_m &\le \varepsilon_m^2 & (5.12)\\ \Rightarrow 0 &\ge \Delta \mathbf{l}_m^H \left(\frac{\mathbf{W}_k}{2^{(R^{E,upper}-t_k)}-1} - \mathbf{V} \right) \Delta \mathbf{l}_m & (5.13)\\ &+ 2\mathrm{Re}\left\{ \widehat{\mathbf{l}}_m^H \left(\frac{\mathbf{W}_k}{2^{(R^{E,upper}-t_k)}-1} - \mathbf{V} \right) \Delta \mathbf{l}_m \right\} & (5.14)\\ &+ \widehat{\mathbf{l}}_m^H \left(\frac{\mathbf{W}_k}{2^{(R^{E,upper}-t_k)}-1} - \mathbf{V} \right) \widehat{\mathbf{l}}_m - \sigma_n^2, \ \forall m, \ \forall k & (5.15) \end{aligned}$$

holds if and only if there exist $\delta_{m,k} \ge 0$, $m \in \{1, \cdots, M\}$, $k \in \{1, \cdots, K\}$, and such that the following LMIs constraints hold:

$$\begin{aligned} &\widetilde{\mathrm{C6}}\text{: } \mathbf{S}_{\mathrm{C6}_{m,k}}(\mathbf{W}_k, \mathbf{V}, \delta_{m,k}, t_k) \\ &= \begin{bmatrix} \delta_{m,k}\mathbf{I}_{N_\mathrm{T}} + \mathbf{V} & \mathbf{V}\widehat{\mathbf{l}}_m \\ \widehat{\mathbf{l}}_m^H \mathbf{V} & -\delta_{m,k}\varepsilon_m^2 + \sigma_n^2 + \widehat{\mathbf{l}}_m^H \mathbf{V} \widehat{\mathbf{l}}_m \end{bmatrix} - \frac{1}{2^{(R^{E,upper}-t_k)}-1} \mathbf{U}_{\mathbf{l}_m}^H \mathbf{W}_k \mathbf{U}_{\mathbf{l}_m} \succeq 0, \ \forall m, \forall k, \end{aligned} \tag{5.16}$$

where $\mathbf{U}_{\mathbf{l}_m} = \left[\mathbf{I}_{N_\mathrm{T}} \ \widehat{\mathbf{l}}_m \right]$. We note that now constraint C6 involve only a finite number of constraint which facilitate the resource allocation algorithm design.

5.2 Robust SST Optimization Problem Reformulation

Next, following the similar line of thought in Section 4.2, we rewrite the objective function into a canonical form of monotonically increasing function. Specifically, we define a new slack $\mathbf{z}$ whose elements meet the following inequalities

$$1 \le z_k \le 1 + \Gamma_k, \ \forall k \in \{1, \cdots, K\}, \tag{5.17}$$

and $\mathbf{z} \in \mathscr{G}$, where $\mathscr{G} \in \mathbb{R}^K$ is an intersection of a normal set and a conormal set, which is given by

$$\mathscr{G} = \{\, \mathbf{z} \mid 1 \leq z_k \leq 1 + \Gamma_k(\mathbf{W}_k, \mathbf{V}),\ \mathbf{W} \in \mathscr{P},\ \mathbf{V} \in \mathscr{Q},\ \forall k \}, \tag{5.18}$$

where $\mathscr{P}$ is a set defined by C1, C2, C4, C5, $\widetilde{\text{C6}}$ and $\mathscr{Q}$ is a set defined by C1, C2, C3 and $\widetilde{\text{C6}}$. Moreover, in order to simplify notation, we define t collects all the t_k which is given by

$$t = \sum_{k=1}^{K} t_k = K\log_2(1 + \Gamma^{E,upper}) - \sum_{k=1}^{K} \log_2(1 + \gamma_k), \tag{5.19}$$

where $t \in \mathscr{D}$, $\mathscr{D} \in \mathbb{R}$ is a subset of real number set, and

$$\mathscr{D} = \left\{\, t \mid 0 \leq t \leq K\log_2(1 + \Gamma^{E,upper}),\ \forall k \right\}. \tag{5.20}$$

Then, we substitute $K\log_2(1+\Gamma^{E,upper})-t$ for $\sum_{k=1}^{K} \log_2(1+\gamma_k)$ in the objective function of the considered optimization problem. In particular, we note the term $K\log_2(1+\Gamma^{E,upper})$ can be omitted in the objective function, since it is a constant, and it has no influence on finding the optimal solution of the considered resource allocation optimization problem.

For facilitating the presentation, we further rewrite the problem 5.4 into the following monotonic optimization problem:

$$\begin{aligned} &\underset{\mathbf{z},t}{\text{maximize}} \;\; \Phi(\mathbf{z}, t) = \sum_{k=1}^{K} \log_2(z_k) + t \\ &\text{subject to} \;\; (\mathbf{z}, t) \in \mathscr{S}, \end{aligned} \tag{5.21}$$

where the feasible set $\mathscr{S} \in \mathbb{R}^{\mathbb{K}} \times \mathbb{R}$ is defined as

$$\mathscr{S} = \{\, (\mathbf{z}, t) \mid \mathbf{z} \in \mathscr{G},\ t \in \mathscr{D} \}. \tag{5.22}$$

We note that the problem 5.21 has the similar structure as problem 4.26 in Section 4.2. Hence, we can optimally solve the problem 5.21 by applying **Algorithm 1** and **Algorithm 2**. Considering the optimal resource allocation policy can be obtained by solving the similar relaxed SDP problem, we omit the problem formulation and the corresponding proof here.

Chapter 6

Simulation Results

In this chapter, we evaluate the system performance of the proposed resource allocation schemes via simulations. In particular, we first study the system performance of the proposed optimal scheme and suboptimal scheme with respect to a single eavesdropper in presence of perfect CSI at the BS. Then, we move towards the case involving multiple potential eavesdroppers with imperfect CSI. Moreover, we compare the system performance of the proposed optimal scheme with or without AN to reveal the extra gain by applying AN. Besides, we also investigate the influence of the optimal solution tolerance factor ε and the optimal solution approximation factor δ on the system performance of the proposed optimal resource allocation algorithm. The adopted simulation parameters are listed in Table 6.1, unless it is expressly specified. The simulation model is a single cell where the BS is equipped with N_T antennas and located at the center of the cell. The K active users and M potential eavesdroppers randomly appear within the whole area of the cell, and all of them follow a uniform distribution between the reference distance (30 meters) and the maximum service distance of 600 meters. The multipath fading channels between the BS and all users in the considered system follow an independent and identical Rayleigh distribution. The minimum required SINR of all active users, Γ_{req}, is set to be 10 dB unless otherwise noted. In order to facilitate the presentation in sequel, we define the normalized maximum channel estimation error of idle receiver $\rho^2_{\text{est}} = \varepsilon^2_m / \|\mathbf{l}_m\|^2, \forall k \in \{1, \cdots, K\}$, which indicates the CSI uncertainty at the potential eavesdroppers. All the simulation results shown in this chapter are averaged over different channel realizations of path loss, shadowing and multipath fading.

To show the average SST improvement of the proposed schemes, we also consider two baseline schemes for comparison. For baseline scheme 1, we adopt Zero-Forcing Beamforming (ZF-BF) scheme where each beamforming vector $\mathbf{w}_k$ for active user k nulls the channel vectors for all the other active users by fixing the beamforming direction, i.e., $\mathbf{h}_i^H \mathbf{w}_k = 0$, for all $i \neq k$. In consequence, we jointly manipulate the covariance matrix of AN $\mathbf{V}$ and the power allocation for each element $w_{k,n}$ in beamforming vector $\mathbf{w}_k$,

Table 6.1: System Parameters in Simulations

Carrier center frequency	1.9 GHz
Frequency bandwidth	5 MHz
Path loss exponent	3.6
Reference distance	30 meters
Active user noise power	−110 dBm
Potential eavesdropper noise power	−110 dBm
Base station antenna gain	10 dBi
Convergence tolerance factors ε, δ, ϵ_{SCA}	0.001
Maximum number of iterations M_{SCA} and M_{OPA}	100

where $w_{k,n}$ is the n-th element in $\mathbf{w}_k$, $n \in \{1, \cdots, N_{\mathrm{T}}\}$. For baseline scheme 2, we employ Maximum Ratio Transmission (MRT) scheme such that the beamforming vector removes the channel inversion and maximizes the signal-to-noise ratio, i.e., $\mathbf{w}_k = \sqrt{p_k}\frac{\mathbf{h}_k}{\|\mathbf{h}_k\|}$, where p_k is the gain for channel between the BS and the k-th active user. Thence, we jointly optimize the covariance matrix of AN $\mathbf{V}$ and the gain for k-th channel p_k.

6.1 Sum Secrecy Throughput versus Maximum Transmit Power

In Fig. 6.1, we investigate the average sum secrecy throughput versus the maximum transmit power at the BS, $P_{\max}$, for $K = 3$ active users, $M = 1$ potential eavesdropper and perfect CSI at the BS. Specifically, it can be seen that the average SSTs of the proposed schemes boost with the maximum BS transmitting power $P_{\max}$ while the slopes of these curves gradually decrease due to the fact that the achievable rate is logarithmic proportional to the transmitting power. Meanwhile, as we increase the number of antennas at the BS, the average SSTs of the proposed schemes improve. This can be explained by that the extra DoFs provided by additional antennas facilitate more accurate and efficient beamforming. The proposed optimal scheme with AN achieves the best system performance among all the proposed schemes. The reason behind is twofold. First, compared to the propose optimal scheme without AN, the optimal scheme with AN allows us to effectively degrade the potential eavesdroppers' channels. Second, compared to the propose suboptimal scheme, the globally optimal solution can be obtained by applying MO method. Besides, it can be observed that the proposed suboptimal scheme also significantly outperforms the two baseline schemes, since the locally optimal solution can be acquired via applying SCA algorithm.

On the contrary, two baseline schemes achieve substantially lower average SSTs compared to the proposed schemes. This is due to the fact that both of them sacrifice much

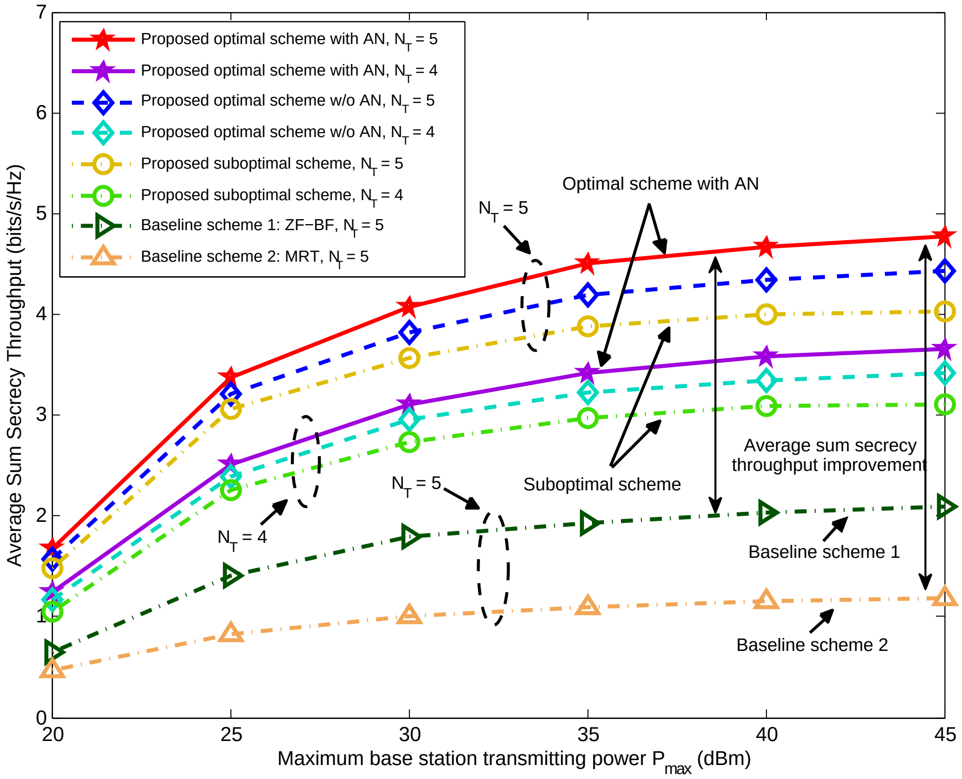

Figure 6.1: Average sum secrecy throughput (bit/s/Hz) versus the maximum transmit power at the base station (dBm), $P_{\max}$, for different resource allocation schemes with 3 active users, 1 potential eavesdropper and perfect channel state information at the base station. The double-headed arrow indicate the average sum secrecy rate improvement of the proposed schemes compared to the baseline schemes.

DoFs for a simple implementation. In particular, the direction of beamforming vector is fixed for baseline 1 while the only term which can be optimized in the beamforming vector is the channel gain $\sqrt{p_k}$ for baseline scheme 2. Additionally, baseline scheme 1 achieves a better system performance compared to baseline scheme 2, since ZF-BF has the ability to remove the MUI introduced by the active users in the considered system.

6.2 Sum Secrecy Throughput versus Number of Active Users

Fig. 6.2 illustrates the average sum secrecy throughput versus the number of active users, K, for the maximum transmit power of $P_{\max} = 40$ dBm, number of antennas $N_{\mathrm{T}} = 10$, $M = 1$ potential eavesdropper and perfect CSI at the BS. As expected, along

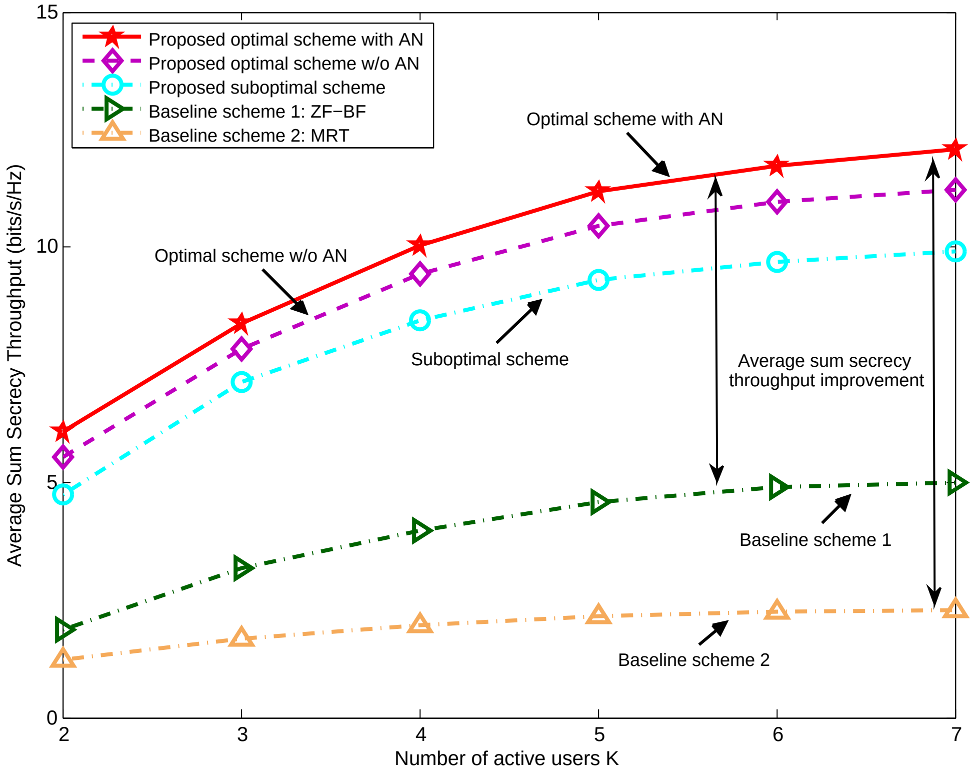

Figure 6.2: Average sum secrecy throughput (bit/s/Hz) versus the number of active users, K, for different resource allocation schemes with $P_{\max} = 40$ dBm, $N_{\mathrm{T}} = 10$, 1 potential eavesdropper and perfect channel state information at the base station. The double-headed arrow indicate the average sum secrecy rate improvement of the proposed schemes compared to the baseline schemes.

with the number of active users grows, the average SSTs of all the proposed schemes monotonically increases due to the exploit of multiuser diversity. Meantime, it can be observed that the proposed optimal scheme with AN surpasses all the other proposed schemes while the optimal scheme without AN is only a slightly worse than the former, since they both attain the globally optimal solution for the considered optimization problem. Moreover, the gap between the optimal schemes and the suboptimal scheme expands in pace with K. This can be explained as follow: with the number of the active users grows, the dimension of the feasible set increases, and then there may be more locally optimal solutions within the feasible set. As a result, the suboptimal scheme may stick to one of the local optimums which is much worse than the global optimum whereas the proposed optimal schemes always focus on finding the globally optimal solution. In other words, the expanding gap represents the cost of proposed suboptimal scheme for striking the trade-off between optimality and computational complexity.

On the other hand, all the proposed schemes remarkably outmatch the two baseline schemes. The reason is that both of the baseline schemes compromise with balance between simplicity and optimality while all the proposed schemes fully utilize the spatial DoFs in resource allocation by optimizing the beamforming vectors which leads to a higher multiuser diversity. However, it can be seen that the average SST of baseline scheme 1 continuously achieves a slight increase whilst the curve of baseline scheme 2 is almost straight. This is due to the fact that, as the number of active users rises, MUI becomes dominated in the considered system. As a result, ZF-BF scheme has the ability to suppress MUI while MRT scheme is not able to handle the aforesaid issue.

6.3 Sum Secrecy Throughput versus Number of Potential Eavesdroppers

In Fig. 6.3, we study the average sum secrecy throughput versus the number of idle users, i.e., potential eavesdroppers, for the maximum transmit power at the BS, $P_{\max} = 40$ dBm, the number of antennas $N_{\mathrm{T}} = 10$, $K = 4$ active users and imperfect CSI of the potential eavesdroppers at the BS. It is expected that, as the number of idle users increases, the average SSTs of all the proposed schemes decrease. The reason behind this is twofold. First, with the increase of M, for each potential eavesdropper, a channel vector $\mathbf{l}_m$ which is more conducive for eavesdropping active users emerges with a higher probability. In other words, the quality of the channel between the BS and the potential eavesdropper m becomes better, which results in a higher achievable rate between the BS and potential eavesdropper for overhearing the desired active user. Second, as the number of potential eavesdroppers rises, more DoFs are used to impair the potential eavesdroppers to wiretap the active users, which leads to a decline in the achievable rate between the BS and active users.

On the other hand, as stated at the beginning of this chapter, we define the normalized maximum channel estimation error of idle user, ρ_{est}, to indicate the CSI uncertainty at the potential eavesdroppers. It can be observed that the average SSTs of the proposed schemes with $\rho_{\mathrm{est}} = 20\%$ dramatically decrease compared to those schemes with $\rho_{\mathrm{est}} = 5\%$. Meantime, the three proposed schemes with $\rho_{\mathrm{est}} = 5\%$ slowly fall with the growth of M while those with $\rho_{\mathrm{est}} = 20\%$ decline much faster. This is because the CSI uncertainty is much greater for $\rho_{\mathrm{est}} = 20\%$, wherefore to find the optimal resource allocation policy that is valid for the CSI uncertainty set, more DoFs are sacrificed to compromise with uncertainty. Besides, as can be observed, for $\rho_{\mathrm{est}} = 20\%$, the proposed scheme with AN has better robustness to CSI uncertainty compared to those without AN. This is due to the fact that AN offers additional DoFs to demote the channels between the BS and the

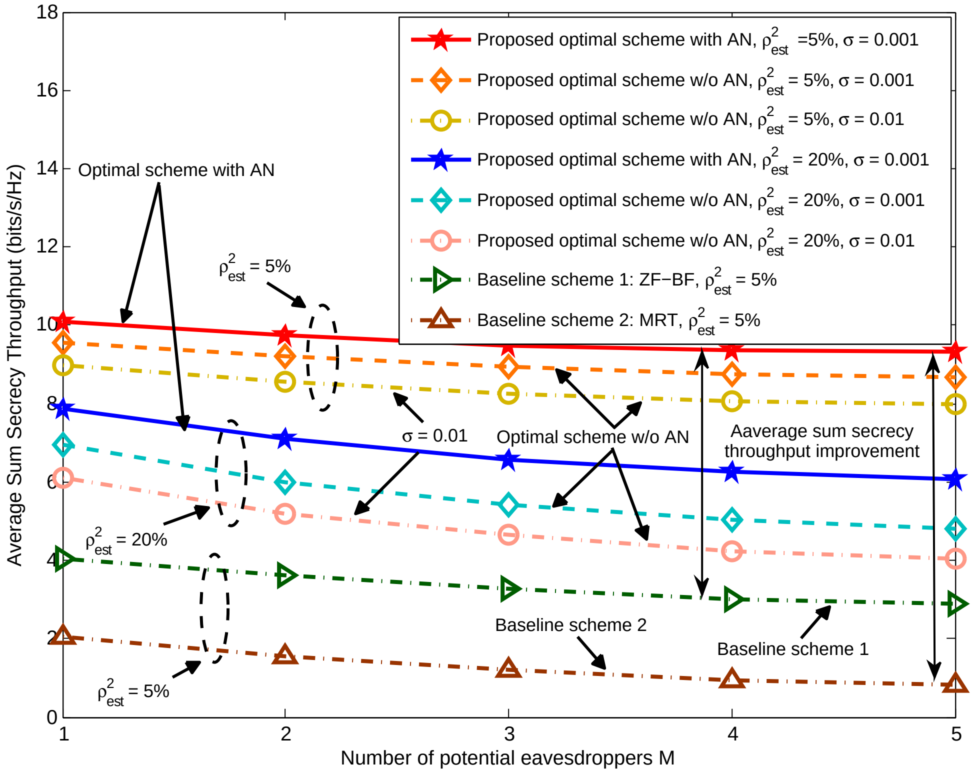

Figure 6.3: Average sum secrecy throughput (bit/s/Hz) versus the number of idle users, M, for different resource allocation schemes with $P_{\max} = 40$ dBm, $N_{\mathrm{T}} = 10$, 4 active user and imperfect CSI of the potential eavesdropper. The double-headed arrow indicate the average sum secrecy throughput improvement of the proposed schemes compared to the baseline schemes.

potential eavesdroppers. Furthermore, we notice that the optimal solution approximation factor δ also affects the system performance, since it is used to determine whether or not the **Algorithm 2** is terminated. Specifically, a larger δ lowers the accuracy of computing the projection, wherefore more error is accumulated in each iteration of algorithm. As a result, the proposed schemes with a smaller δ achieve better average SSTs. In addition, the lower computational complexity of the baseline schemes comes at the expense of a substantially lower average SSTs compared to the other schemes. Yet, the curves of these baseline schemes gently decay due to the almost perfect CSI, i.e., $\rho_{\text{est}} = 5\%$.

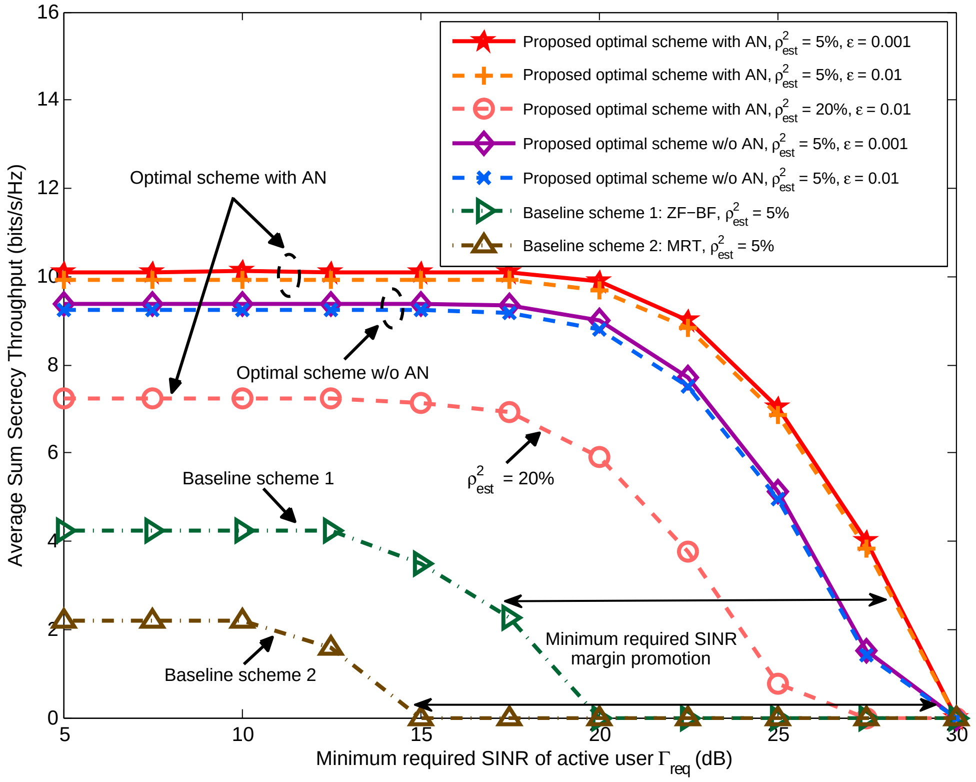

Figure 6.4: Average sum secrecy throughput (bit/s/Hz) versus Minimum required SINR of active users, for different resource allocation schemes with $P_{\text{max}} = 40$ dBm, $N_{\text{T}} = 10$, 4 active user and imperfect channel state information of the potential eavesdropper. The double-headed arrow indicate the average sum secrecy rate improvement of the proposed schemes compared to the baseline schemes.

6.4 Sum Secrecy Throughput versus Minimum Required SINR

Fig. 6.4 depicts the average sum secrecy throughput versus the minimum required SINR of active user, for the maximum transmit power of $P_{\text{max}} = 40$ dBm, the number of antennas $N_{\text{T}} = 10$, $K = 4$ active users, $M = 2$ idle users and imperfect CSI of the potential eavesdroppers. It can be observed that the average SSTs of the proposed schemes firstly remain unchanged (ranges from 5 dB to 15 dB) and then decrease (ranges from 15 dB to 30 dB) with Γ_{req}. To explain this, we recall the discussion in Chapter 4 that, depending on its value, the threshold Γ_{req} has a different impact on the feasibility of the optimization problem. Specifically, a relatively low Γ_{req} can be regarded as a loose constraint, wherefore it hardly reduces the feasible set, and the optimal solution [2] maintains feasible. However, an excessively high Γ_{req} (higher than

25 dB in our simulation scheme) forces the BS to unevenly allocate the its power, i.e., distributing the transmitting power on one beamforming vector while suppress all the other beamforming vectors and AN, which is self-contradictory when we consider all the active users. As a result, the resource allocation problem is optimized in a drastically squeezed feasible set or even become infeasible.

On the other hand, we can see that the optimal solution tolerance factor ε does not have a large impact on the average SST of the system, since one percent accuracy is enough to guarantee the optimum of the considered optimization problem. Moreover, the optimal scheme with AN and $\rho_{\text{est}} = 20\%$ achieves a low SST compared to the other proposed schemes. The reason behind this is double. First, due to the imperfect CSI of the potential eavesdropper, the considered problem is optimized over the CSI uncertainty set Ω_m such that all possible CSI uncertainties of potential eavesdropper m achieve the optimal solution. A larger ρ_{est}, i.e., a set Ω_m containing more possible CSI uncertainties of potential eavesdropper m, hinders the BS from applying more precise beamforming. Second, the CSI uncertainty compacts the feasible set of the optimization problem since some feasible resource allocation policies in perfect CSI case now are infeasible. Besides, it can be observed that all the proposed schemes gain minimum required SINR margin promotion compared to the baseline schemes. Specifically, the proposed schemes are able to fully exploit the DoFs of the considered system by optimizing the beamforming which results in a wider and more flexible range on SINR of the active users and improve the system performance even if a relatively high Γ_{req} is required.

Chapter 7

Conclusion

In this thesis, we investigated the resource allocation algorithm design for a secure multiuser wireless communication system. An MO problem was formulated to maximize the SST of the considered system in the presence of a single potential eavesdropper with perfect CSI at the BS. The optimal solution is obtained by applying the POA algorithm and the projection bisection search algorithm. Considering the fact that the computational complexity of the proposed optimal scheme is extremely high, a suboptimal resource allocation algorithm based on SCA is proposed to strike a balance between optimality and efficiency. Furthermore, we extend the optimization problem to a case where the system contains multiple potential eavesdroppers in the presence of imperfect CSI. Due to the intractability of the resulting resource allocation optimization problem, we reformulate it by replacing the semi-infinite constraint with finite LMIs constraints. Then, we adopt the similar MO method mentioned before to achieve the optimal resource allocation policy in the extensional case.

Simulation results revealed the excellent performance of all the proposed resource allocation schemes compared to the baseline schemes. Moreover, AN was proven to be a promising technique to facilitate secure transmission. In the case of multiple potential eavesdroppers with imperfect CSI at the BS, the system performance of all the proposed schemes declines compared to those in the case of a single potential eavesdropper with perfect CSI at the BS. The optimal solution approximation factor σ has a large impact on the system performance while the optimal solution tolerance factor ε slightly affects the average SST of the considered system.

Through the resource allocation optimization problem for maximization of system SST, we notice that obtaining the optimal solution to the considered problem is a tough task. This can be explained by "degrees of freedom mismatch". Specifically, convex optimization problems can be regarded as a special case of monotonic optimization problems, since almost all convex optimization problems can be reformulated to monotonic optimization problems and then optimally solved [26]. Moreover, solving a problem with non-convex objective function and constraints, in general, requires more DoFs than that with convex objective function and constraints, because non-convexity means less structured and contains more freedom[3]. It should be noted that, in the extensional case, the considered optimization problem becomes more uncertain and complex due to the fact that the multiple potential eavesdroppers and the imperfect CSI at the BS introduce more freedom. As a result, more DoFs are needed to rectify the mismatch between freedom and DoFs to obtain the optimal solution of the considered optimization problem. For ZF-BF scheme and MRT scheme, much DoFs are already eliminated by fixing the partial solution of the considered optimization problem, wherefore DoFs mismatch occurs which results in an unsatisfactory solution. Overall, MO method is a more powerful and flexible tool than the conventional convex optimization method when we face complicated problems in the future.

Bibliography

[1] R. Hartley. Transmission of information. *Bell Labs Technical Journal*, 7(3):535–563, 1928.

[2] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen. Physical layer security in wireless networks: A tutorial. *IEEE Wireless Commun.*, 18(2):66–74, Apr. 2011.

[3] M. Bloch and J. Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.*, 53(4):20–27, Apr. 2015.

[5] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire. Secure massive MIMO transmission with an active eavesdropper. *IEEE Trans. Inf. Theory*, 62(7):3880–3900, Jul. 2016.

[6] Y. Sun, D. W. K. Ng, Z. Ding, and R. Schober. Optimal Joint Power and Subcarrier Allocation for MC-NOMA Systems. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, Dec 2016.

[7] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen. A Survey on Multiple-Antenna Techniques for Physical Layer Security. *IEEE Communications Surveys & Tutorials*, 2017.

[8] R. Negi et al. Secret communication using artificial noise. In *Proc. IEEE Veh. Technol. Conf.*, pages 1906–1910, Dallas, TX, USA, Sept. 2005.

[9] D. W. K. Ng, E. S. Lo, and R. Schober. Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks. *IEEE Trans. Wireless Commun.*, 10(10):3528–3540, Oct. 2011.

[10] P. H. Lin, S. H. Lai, and H. J. Su. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels. *IEEE J. Sel. Areas Commun.*, 31(9):1728–1740, Sept. 2013.

[11] Y. Sun, D. W. K. Ng, and R. Schober. Resource Allocation for Secure Full-Duplex Radio Systems. In *Proc. International ITG Workshop on Smart Antennas*, pages 1–6, Berlin, Germany, Mar. 2017.

[12] T. Agrawal and S. Agnihotri. Secure amplify-and-forward relaying in linear chains with a single eavesdropper. In *Signal Processing and Communications (SPCOM), 2016 International Conference on*, pages 1–5. IEEE, 2016.

[13] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava. Analysis and design of secure massive MIMO systems in the presence of hardware impairments. *IEEE Transactions on Wireless Communications*, 16(3):2001–2016, 2017.

[14] Q. Li and W. K. Ma. Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization. *IEEE Transactions on Signal Processing*, 61(10):2704–2717, 2013.

[15] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen. Robust beamforming design for sum secrecy rate optimization in MU-MISO networks. *IEEE Transactions on Information forensics and Security*, 10(9):1812–1823, 2015.

[16] H. Tuy. Monotonic optimization: Problems and solution approaches. *SIAM Journal on Optimization*, 11(2):464–494, 2000.

[17] L. P. Qian, Y. J. Zhang, and J. Huang. MAPEL: Achieving global optimality for a non-convex wireless power control problem. *IEEE Transactions on Wireless Communications*, 8(3):1553–1563, 2009.

[18] Y. Sun, D. W. K. Ng, Z. Ding, and R. Schober. Optimal Joint Power and Subcarrier Allocation for Full-Duplex Multicarrier Non-Orthogonal Multiple Access Systems. *IEEE Transactions on Communications*, 65(3):1077–1091, 2017.

[19] S. Bi, L. Qian, and Y. J. A. Zhang. Monotonic optimization method for general utility maximization in random-access networks. In *Communications in China (ICCC), 2013 IEEE/CIC International Conference on*, pages 391–396. IEEE, 2013.

[20] Y. J. A. Zhang, L. Qian, and J. Huang. Monotonic optimization in communication and networking systems. *Foundations and Trends® in Networking*, 7(1):1–75, 2013.

[21] Y. Sun, D. W. K. Ng, and R. Schober. Optimal resource allocation for multicarrier MISO-NOMA systems. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–7, May 2017.

[22] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober. Multi-Objective Optimization for Robust Power Efficient and Secure Full-Duplex Wireless Communication Systems. *IEEE Transactions on Wireless Communications*, 15(8):5511–5526, 2016.

[23] M. Zhang, M. Ding, L. Gui, H. Luo, and M. Bennis. Sum Secrecy Rate Maximization for Relay-Aided Multiple-Source Multiple-Destination Networks. *IEEE Transactions on Vehicular Technology*, 66(5):4098–4109, 2017.

[24] G. Zheng, K. K. Wong, and T. S. Ng. Robust linear MIMO in the downlink: A worst-case optimization with ellipsoidal uncertainty regions. *EURASIP Journal on Advances in Signal Processing*, 2008:154, 2008.

[25] C. Shen, T. H. Chang, K. Y. Wang, Z. D. Qiu, and C. Y. Chi. Distributed robust multicell coordinated beamforming with imperfect CSI: An ADMM approach. *IEEE Transactions on signal processing*, 60(6):2988–3003, 2012.

[26] E. Björnson and E. Jorswieck. Optimal resource allocation in coordinated multi-cell systems. *Foundations and Trends® in Communications and Information Theory*, 9(2–3):113–381, 2013.

[27] W. Dinkelbach. On nonlinear fractional programming. *Management science*, 13(7):492–498, 1967.

[28] A. Charnes and W. Cooper. Programming with linear fractional functionals. *Naval Research Logistics (NRL)*, 9(3-4):181–186, 1962.

[29] Z. Q. Luo, W. K. Ma, A. M. C. So, Y. Ye, and S. Zhang. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Processing Magazine*, 27(3):20–34, 2010.

[30] Y. Ye. Approximating quadratic programming with bound and quadratic constraints. *Mathematical programming*, 84(2):219–226, 1999.

[31] Y. Sun, D. W. K. Ng, N. Zlatanov, and R. Schober. Robust resource allocation for full-duplex cognitive radio systems. In *2016 24th European Signal Processing Conference (EUSIPCO)*, pages 773–777, Aug 2016.

[32] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. *http://cvxr.com/cvx*, Mar. 2017.

[33] J. Dahl and L. Vandenberghe. Cvxopt: A python package for convex optimization, version 1.1.9. *Available at http://cvxopt.org/*, Nov. 2016.

[34] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[35] E. Boshkovska, D. W. K. Ng, N. Zlatanov, A. Koelpin, and R. Schober. Robust resource allocation for MIMO wireless powered communication networks based on a non-linear EH model. *IEEE Transactions on Communications*, 2017.

[36] P. D. Tao and L. T. H. An. Convex analysis approach to dc programming: Theory, algorithms and applications. *Acta Mathematica Vietnamica*, 22(1):289–355, 1997.

[37] R. Horst and N. V. Thoai. DC programming: overview. *Journal of Optimization Theory and Applications*, 103(1):1–43, 1999.

[38] P. D. Tao. The DC programming and DCA revisited with DC models of real world nonconvex optimization problems. *Annals of operations research*, 133(1-4):23–46, 2005.

[39] Q. T. Dinh and M. Diehl. Local convergence of sequential convex programming for nonconvex optimization. In *Recent Advances in Optimization and its Applications in Engineering*, pages 93–102. Springer, 2010.

[40] Y. Sun, D. W. K. Ng, and R. Schober. Joint power and subcarrier allocation for multicarrier full-duplex systems. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 6548–6552, March 2017.

[41] D. W. K. Ng and R. Schober. Resource allocation for secure communication in systems with wireless information and power transfer. In *2013 IEEE Globecom Workshops (GC Wkshps)*, pages 1251–1257, Dec 2013.

[42] D. W. K. Ng and R. Schober. Resource allocation for coordinated multipoint networks with wireless information and power transfer. In *2014 IEEE Global Communications Conference*, pages 4281–4287, Dec. 2014.

[43] Y. Nesterov. Semidefinite relaxation and nonconvex quadratic optimization. *Optimization methods and software*, 9(1-3):141–160, 1998.

[44] S. Boyd. Sequential convex programming. *Lecture Notes, Stanford University*, 2008.

[45] J. Kaleva, A. TÃűlli, and M. Juntti. Weighted sum rate maximization for interfering broadcast channel via successive convex approximation. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 3838–3843, 2012.