Cost-Effective Signal Processing Algorithms for Physical-Layer Security in Wireless Networks

Xiaotao Lu

Ph.D.

University of York
Electronics

August 2016

Abstract

Data privacy in traditional wireless communications is accomplished by cryptography techniques at the upper layers of the protocol stack. This thesis aims at contributing to the critical security issue residing in the physical-layer of wireless networks, namely, secrecy rate in various transmission environments. Physical-layer security opens the gate to the exploitation of channel characteristics to achieve data secure transmission.

Precoding techniques, as a critical aspect in pre-processing signals prior to transmission has become an effective approach and recently drawn significant attention in the literature. In our research, novel non-linear precoders are designed focusing on the improvement of the physical-layer secrecy rate with consideration of computational complexity as well as the Bit Error Ratio (BER) performance. In the process of designing the precoder, strategies such as Lattice Reduction (LR) and Artificial Noise (AN) are employed to achieve certain design requirements.

The deployment and allocation of resources such as relays to assist the transmission also have gained significant interest. In multiple-antenna relay networks, we examine various relay selection criteria with arbitrary knowledge of the channels to the users and the eavesdroppers. Furthermore, we provide novel effective relay selection criteria that can achieve a high secrecy rate performance. More importantly they do not require knowledge of the channels of the eavesdroppers and the interference.

Combining the jamming technique with resource allocation of relay networks, we investigate an opportunistic relaying and jamming scheme for Multiple-Input Multiple-Output (MIMO) buffer-aided downlink relay networks. More specifically, a novel Relaying and Jamming Function Selection (RJFS) algorithm as well as a buffer-aided RJFS algorithm are developed along with their ability to achieve a higher secrecy rate. Relying on the proposed relay network, we detail the characteristics of the system, under various relay selection criteria, develop exhaustive search and greedy search-based algorithms, with or without inter-relay Interference Cancellation (IC).

Contents

List of Tables

List of Figures

List of Symbols

$\mathrm{Tr}(\cdot)$	The trace of an square matrix
$\det(\cdot)$	Determinant of a matrix
$\log(\cdot)$	Logarithm of a number
$E(\cdot)$	Expectation
D	Diversity order
r_{mux}	Multiplexing order
N_t^{total}	Total number of transmit antennas
N_t	Number of active transmit antennas
N_r	Number of receive antennas for rth user
h	Channel coefficient
P	Total transmit power
C	Channel capacity
C_{sec}	Channel capacity
$\boldsymbol{H}$	MIMO channel matrix
$\boldsymbol{s}$	Transmit signal
$\boldsymbol{y}$	Received signal
$\boldsymbol{n}$	Gaussian noise
$\boldsymbol{P}$	Precoding matrix

$\boldsymbol{U}$	Left unitary matrix in SVD
$\boldsymbol{V}$	Right unitary matrix in SVD
$\boldsymbol{\Sigma}$	Diagonal matrix in SVD
$\boldsymbol{B}$	Feedback matrix in THP
$\boldsymbol{G}$	Scaling matrix in THP
$\boldsymbol{F}$	Forward matrix in THP
$\boldsymbol{\Gamma}_t(\cdot)$	Modulo-t operation
$\boldsymbol{Q}$	Unitary matrix in QR or LQ decomposition
$\boldsymbol{L}$	Lower triangular matrix in QR or LQ decomposition
$\boldsymbol{R}$	Transmit covariance matrix
$\boldsymbol{\Omega}$	Total relay set
$\boldsymbol{\Psi}$	T-combination matrix from total relay set
$\boldsymbol{\varphi}$	one combination from matrix $\boldsymbol{\Psi}$

Preface

All of the work presented henceforth was conducted in the communication group laboratory at the University of York.

The work provides a framework of a new approach supporting secure data transmission in wireless networks. Proved by Shannon's theory and established by A. D. Wyner, this new approach known as physical-layer security draws great attention since it is posed. Compared with traditional cryptography techniques, it provides a more efficient and reliable way to achieve transmission security.

This dissertation should be of interest to wireless secure transmission developers

Acknowledgments

This dissertation would not be possible without the contribution of several people. I would firstly like to gratefully acknowledge my supervisor Prof. Rodrigo C. de Lamare for his helpful support and constant encouragement. He has always been available to advise me and I am deeply benefited from his enthusiasm and knowledge in communications.

Special thanks to Prof. Alister Burr, for his help, valuable supervision and useful advice for my research. I would also thank Dr. Keke Zu who is now working in the Ericsson Research Group in Sweden, for his help in the beginning of this work. Further I would like to thank all University of York Communications Group members for their help and support throughout my research.

I would like to thank my girlfriend for this unconditional support and encouragement on my research. I dedicate this work to my parents, Ying Sun and Ping Lu, to whom I owe more than I will ever be able to repay

Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References. The related work published or under review are listed as follows:

- Xiaotao Lu, Rodrigo C. de Lamare and Keke Zu, "Successive Optimization Tomlinson-Harashima Precoding Strategies for Physical-Layer Security in Wireless Networks", EURASIP Journal on Wireless Communications and Networking, 2016, accepted.
- Xiaotao Lu and Rodrigo C. de Lamare, "Opportunistic Relaying and Jamming Scheme for Physical-Layer Security in Buffer-aided Relay Networks", IEEE Transactions on Communications, 2016, major revision.
- X. Lu and R. C. d. Lamare, "Relay Selection Based on the Secrecy Rate Criterion for Physical-Layer Security in Buffer-Aided Relay Networks," WSA 2016; 20th International ITG Workshop on Smart Antennas, Munich, Germany, 2016, pp. 1-5.
- X. Lu and R. C. de Lamare, "Opportunistic relay and jammer cooperation techniques for physical-layer security in buffer-aided relay networks," 2015 International Symposium on Wireless Communication Systems (ISWCS), Brussels, 2015, pp. 691-695.
- X. Lu and R. C. d. Lamare, "Buffer-Aided Relay Selection for Physical-Layer Security in Wireless Networks," WSA 2015; 19th International ITG Workshop on Smart Antennas, Ilmenau, Germany, 2015, pp. 1-5.
- X. Lu, K. Zu and R. C. de Lamare, "Lattice-reduction aided Successive Optimization Tomlinson-Harashima Precoding strategies for physical-layer security in wireless networks," Sensor Signal Processing for Defence (SSPD), 2014, Edinburgh, 2014, pp. 1-5.

Chapter 1

Introduction

1.1 Motivation

Around our life, changes are happening at every second. We are stepping into a "Wireless" world. Talking to each other through thousands of miles away is no longer a dream. Traveling around the world can be guided by the Global Positioning System (GPS). Looking back to the development of wireless communications, people are always seeking faster, more reliable and more convenient ways to send messages. Among all the demands, transmission security is an unavoidable critical aspect.

In daily life, people put the information into a locked box before transmission to keep the privacy of message. This can also be regarded as a secure transmission system. Inspired by the idea of using a key and a locker, the conventional wireless secure transmission in essence performs in the same way. The 'box' in wired or wireless transmission is created with different types of encryption techniques, for example, the most common email encryption techniques are called PKI (Public Key Infrastructure), WEP (Wired Equivalent Privacy) used to secure IEEE 802.11 wireless networks as well as WPA (Wi-Fi Protected Access) developed to provide stronger security. The 'key' is created using an encryption or a decryption algorithm to lock or unlock the 'box'. Based on the type of keys, traditional cryptography can be divided into symmetric key cryptography (also known as shared key cryptography) and public key cryptography. The security level of this kind of encryption significantly depends on the encryption algorithm used to generate the keys.

Although the traditional encryptions have great performance in reality, theoretically given unlimited computing power, these encryptions can still be broken. Is there existing a secure technique theoretically unbreakable? To achieve information-theoretically secure transmission, scientists are trying to develop a crypto-system with the capability of achieving security derived from information theory. This means that it cannot be broken even when the adversary has unlimited computing power.

Future development in computing power brings great challenges to the traditional encryption protocols, but information-theoretic security does not rely its effectiveness on assumptions about computational hardness, which makes it not vulnerable to such challenges. The concept of information-theoretically secure communication was introduced in 1949 by Claude Shannon, who proved the feasibility of secure transmission in physical layer from the viewpoint of information theory. In cryptography, if a cipher text produced using it provides no information about the plaintext without knowledge of the key, we say it is perfectly secure. In common transmissions, information-theoretic security communications is not necessary to be perfectly secure. It can tolerate a certain level of leakage of information.

Under the inspiration of information-theoretic security, A. D. Wyner in his initial physical-layer security work [1] in the 1970s described the wiretap channel. By utilizing the physical wireless channel, Wyner maintained the security properties by communications, signal processing and coding techniques. The details of the problem is described as Alice wants to send a message to Bob without Eve decoding it. It was shown that if the channel from Alice to Bob is statistically better than the channel from Alice to Eve, secure transmission is possible. The most critical point in his work is that Wyner defines the secrecy capacity as the rate at which Alice can transmit secret information to Bob. Shortly after, Csiszar and Korner [2] found that the assumption in Wyner's work that Bob has statistically better channel to Alice than did Eve can be released without destroying secret transmission. More recently, secrecy capacity and optimal power allocation in broadcast fading channels becomes popular in the physical-layer security research. Among which, the knowledge of the channels from Alice to Eve is always an unavoidable assumption. If the knowledge can be obtained or is available, Alice could simply place a null in Eves direction.

Less theoretically than the seminal papers in the field, new schemes have been proposed

attempting to assist the existing secure transmission. One physical-layer security scheme is to broadcast artificial noise in all directions except that of Bobs channel, basically jamming Eve. One paper by Goel and Negi [3] details the implementation, and Khisti and Wornell [4] compute the secrecy capacity when only statistics about Eves channel are known. Secrecy capacity for MIMO and multiple colluding eavesdroppers is more recent and ongoing work, and these results still make the non-useful assumption about eavesdropper channel state information knowledge.

1.2 Problems and Contributions

1.2.1 Problems

In more recent works, secrecy capacity is investigated with different precoding techniques. The secrecy capacity with linear precoding algorithm such as zero-forcing (ZF), minimum mean square error (MMSE) and block diagonalization (BD) are investigated in various scenarios [5; 6; 7]. Then in MISO scenario, robust secure transmission is investigated [8; 4]. Following the MISO scenario, the closed-form expression of secrecy capacity for some special MIMO scenario is carried out [9]. However the secrecy capacity of general MIMO scenarios is still an open problem.

As aforementioned, resource allocation is one of the directions of physical-layer security research. Different resource allocation will have various effects on the system. For example, power allocation will give the optimal performance in terms of transmission rate of the investigated system [10]. In ongoing works, the selection of relays shows great advantage in assisting with fading in wireless communications [11]. So far, there are few important works considering physical-layer security in systems with selection of relays [12; 13].

The jamming problem is another critical aspect. The combination of jamming techniques and selection of relays is a novel topic in the physical-layer security research [14; 15; 16].

1.2.2 Contributions

Associated with the problems posed, the contribution in this dissertation can be divided into three aspects. First, to improve the secrecy rate performance, we study and propose novel

non-linear precoding algorithms and also some extended versions with an improvement in specific performance metric. Secondly, for the selection of relays, effective relay selection criteria are developed to achieve high secrecy rate performance in relay systems. In the last contribution, a jamming technique is combined with relay networks to provide a superior secrecy rate performance.

Design of non-linear precoder

We develop and study successive optimization Tomlinson-Harashima precoding (SO-THP) algorithms based on the generalized MMSE channel inversion (GMI) approach reported in [17]. Specifically, the proposed non-linear precoders exploit both successive interference cancellation, lattice-reduction and block diagonalization, which can impose near-orthogonality between the channels of the desired users. The major contributions are summarized as follows:

- A multiuser MIMO downlink network is constructed in the presence of multiple eavesdroppers.
- Novel non-linear precoding technique, namely, SO-THP+GMI is proposed in MU-MIMO downlink wireless network. SO-THP+GMI algorithm combines the SO-THP precoding with the GMI technique to maintain an outstanding secrecy rate with reduced computational complexity.
- SO-THP+GMI precoding algorithm is extended to a S-GMI version which we call SO-THP+S-GMI algorithm. SO-THP+S-GMI algorithm can further reduce the computational complexity.
- Based on aforementioned SO-THP+S-GMI algorithm, lattice-reduction (LR) strategy is employed to achieve full receive diversity and artificial noise (AN) strategy is applied to contribute to a further secrecy rate improvement.
- Secrecy rate analysis of proposed non-linear precoding algorithms is carried out along with an assessment of their computational complexity.
- When different power levels are allocated to generate artificial noise, an analysis of the power ratio which can achieve the optimal value in terms of secrecy rate is given.

Effective relay selection criteria

We investigate the physical-layer security performance in a multiuser MIMO downlink relay network. With arbitrary knowledge of the channels to users and the eavesdroppers, we examine the effect of applying different relay selection criteria on the secrecy rate performance. Then novel effective relay selection algorithms which can achieve high secrecy rate is proposed without the knowledge of the channels to the eavesdroppers. The main contributions include:

- The structure of a multiuser MIMO downlink relay network with linear precoding techniques.
- Examine the effect of applying max-ratio criterion, SINR criterion as well as Secrecy-Rate (SR) criterion on physical-layer secrecy rate in single antenna and MIMO scenarios.
- Derivation of the proposed Simplified SINR-Based (S-SINR) relay selection criterion with linear precoding. The S-SINR criterion requires only the channels of the legitimate users and can achieve close secrecy rate performance to the full knowledge information SINR criterion.
- Derivation of the proposed Simplified SR-Based (S-SR) relay selection criterion with linear precoding. The S-SR criterion eliminates the requirement of the information of channels to the eavesdroppers and has almost the similar level of secrecy rate performance to the full knowledge information SR criterion.
- The proposed S-SINR criterion and S-SR criterion are compatible with rank-deficient systems.

Opportunistic relaying and jamming scheme

Opportunistic relaying and jamming select scheme and algorithms are investigated in MIMO buffer-aided downlink relay networks. The opportunistic scheme is combined with a jamming technique to improve the secrecy rate performance. In the opportunistic scheme, the problem of inter-relay interference cancellation is concerned with a comparison between implementing the interference cancellation or not. Computational complexity of the algorithms also consider a solution of employing a greedy search in the relay selection. The main contributions are:

- An opportunistic multiuser MIMO downlink buffer-aided relay network is constructed with linear precoding techniques.

- Novel Relaying and Jamming Function Selection (RJFS) algorithm is proposed to contributed to the secrecy rate performance and a buffer-aided RJFS algorithm is further developed with noisy signals stored in the buffers. The buffer-aided system is capable of achieving higher secrecy rate by requiring extra computational complexity.
- In the opportunistic scheme, inter-relay interference is an unavoidable issue. In our work we study the feasibility of implementing interference cancellation (IC) at relay nodes and compare the effect on secrecy rate performance with or without IC.
- In both proposed algorithms, computational complexity is a critical point. To reduce the algorithm complexity, a greedy search is developed for use instead of an exhaustive search. With the cooperation between the greedy search and proposed relay selection algorithm, high secrecy rate performance is maintained with reduced computational complexity.

1.3 Thesis Outline

In Chapter 2, a comprehensive literature review is provided. Not only the concept of physical-layer security from the view of information theory but also some less theoretical techniques such as lattice reduction (LR) and artificial noise (AN). A brief introduction of our work which relies on the development of introduced techniques is given along with summaries of novel algorithms.

In Chapter 3, a multiuser MIMO downlink system is constructed and novel non-linear precoding algorithms which contribute to the secrecy rate performance are introduced. In addition, some extended version of non-linear precoding algorithms are shown with concurrent consideration of various requirements in wireless transmission, namely, computational complexity, bit error ratio (BER).

Chapter 4 includes a design of effective relay selection criterion in multiple antenna relay networks. Novel relay selection criteria are proposed aiming at secrecy rate improvement. Based on which, Further simplified criteria research focus on the elimination of the knowledge of the channels to the eavesdroppers. Eventually, novel simplified criteria are developed maintaining the secrecy rate performance without knowledge of the channels to the eavesdroppers.

In Chapter 5, an opportunistic scheme as well as a jamming technique are combined to achieving high secrecy rate performance in a buffer-aided relay network. Details of the opportunistic scheme with consideration of inter-relay interference cancellation and jamming process with jammer nodes are given in the construction of the system, based on which the Relaying and Jamming Function Selection (RJFS) algorithm as well as its buffer-aided version are proposed.

In Chapter 6, a summary of our work, conclusions and a brief discussion of future work, which is of great interest in physical-layer security research are given based on the obtained results.

1.4 Notation

Bold uppercase letters $\boldsymbol{A} \in \mathbb{C}^{M\times N}$ denote matrices with size $M \times N$ and bold lowercase letters $\boldsymbol{a} \in \mathbb{C}^{M\times 1}$ denote column vectors with length M. Conjugate, transpose, and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$, respectively; $\boldsymbol{I}_M$ is the identity matrix of size $M \times M$; diag$\{\boldsymbol{a}\}$ denotes a diagonal matrix with the elements of the vector $\boldsymbol{a}$ along its diagonal; $\mathcal{CN}(0, \sigma_n^2)$ represents complex Gaussian random variables with independent and identically distributed $(i.i.d)$ entries with zero mean and variance equal to σ_n^2. $\log(\cdot)$ denotes the base-2 logarithm of the argument.

Chapter 2

Literature Review

2.1 Introduction

This Chapter presents a literature review of recent developments in physical-layer security research. Major definitions as well as applied techniques throughout the history of physical-layer security are also illustrated according to the original works by[1; 18; 2; 3]. First of all, the application of physical-layer security is introduced and the performance metrics are given with the help of a wire-tap channel model. Following this, transmit processing techniques are presented with its potential of assisting physical-layer security transmission. Then, a review of resource allocation involving relays are given along with the consideration of buffers implemented in the relay nodes. Finally, jamming techniques are introduced to achieve further improvement in security performance.

2.2 Applications

Recently, rapid development of novel security technique in wireless communications is motivated by advanced eavesdropping techniques. Physical-layer security, as a more efficient and practical way of ensuring wireless transmission security, is developed to realize the desire of protecting information privacy. By taking advantage of wireless characteristics of the channels, physical-layer security contributes to further development in wireless networks. Based on its properties, physical-layer security techniques have great potential of application in the following aspects:

- Military applications: communication systems play an important role in modern mili-

tary operations. Traditional cryptography techniques are challenged by unimaginable computing power developments such as quantum computers. In this context, physical-layer security gives an idea of providing wireless communications with privacy even under unlimited computing power eavesdropping.

- Commercial applications: wireless payments as an advanced technique are popular and convenient in our life. During the payment processing, important personal data, such as order details, bank account information is easily leaked to eavesdroppers. Physical-layer security is capable of dealing with such personal information protection issues, especially in the processing through wireless networks.

- Home applications: wireless communications enable the implementation of modern networks such as wireless sensor networks (WSN), internet of things (IoT) in our daily life. However, data from or to sensors or general devices is transmitted without protection. Physical-layer security provides the capability of secure data transmission in modern networks.

Overall, physical-layer security is compatible with existing wireless transmission systems. With low cost in implementation and excellent performance of data protection, it has great potential for deployment in future wireless communication networks.

2.3 Channel Modeling and System Models

2.3.1 Diversity and Multiplexing

MIMO Diversity

Developed from Single-Input Single-Output (SISO) systems, Single-Input Multiple-Output (SIMO) systems and Multiple-Input Single-Output (MISO) systems show their ability of achieving more reliable wireless transmission in fading channels. In SIMO systems, receive diversity can be used via multiple receive antennas seeing independently faded versions of the same signal [19]. The received signals are combined to obtain a resulting signal with considerably reduced fading. The maximum receive diversity order is equal to the number receive antennas. Similarly, in MISO systems, transmit diversity is achieved by transmitting a symbol through multiple fading paths. Therefore the maximum transmit diversity order is equal to the number of transmit antennas [20]. For a general MIMO system, with N_r receive

antennas and N_t transmit antennas, the maximum diversity order can be obtained by,

$$D = N_t \times N_r \tag{2.1}$$

where each pair of transmit antenna and receive antenna has independently fading.

MIMO Multiplexing

In spatial multiplexing, multiple low-rate signals are multiplexed over a single high-rate link. According to [21], Foschini has proved that in high SNR-regime the capacity of a channel with Rayleigh fading for each transmit and receive antenna can be expressed as:

$$C(\text{SNR}) = \min\{N_t, N_r\} \log \text{SNR} + O(1) \tag{2.2}$$

where SNR is the signal-to-noise ratio. For a Bell Laboratory Layered Space-Time (BLAST) system, according to [22], the multiplexing order can be obtained using:

$$r_{\text{mux}} = \min\{N_t, N_r\} \tag{2.3}$$

The multiplexing configuration can also be employed in a multiuser system.

2.3.2 Channel Modeling

In wireless communications, the characteristics of the wireless channel include the fading, which might adversely affect signal transmission. The fading happens due to the reflecting, scattering and diffracting of the signal. As a result, the received signals will suffer from fluctuating in amplitude, phase and angle which is called multi-path fading. In [23], considering path loss, shadowing fading and multi-path fading, the envelop of the received signal follows a Rayleigh density function given as:

$$f(x) = \frac{2x}{\Omega} e^{-\frac{x^2}{\Omega}} u(x), \tag{2.4}$$

where Ω is the average power of received signal and $u(x)$ is the step function. We restrict the channel model to Rayleigh fading in our work for simplicity but we note that the techniques proposed can also be used for other fading scenarios.

2.3.3 System Model

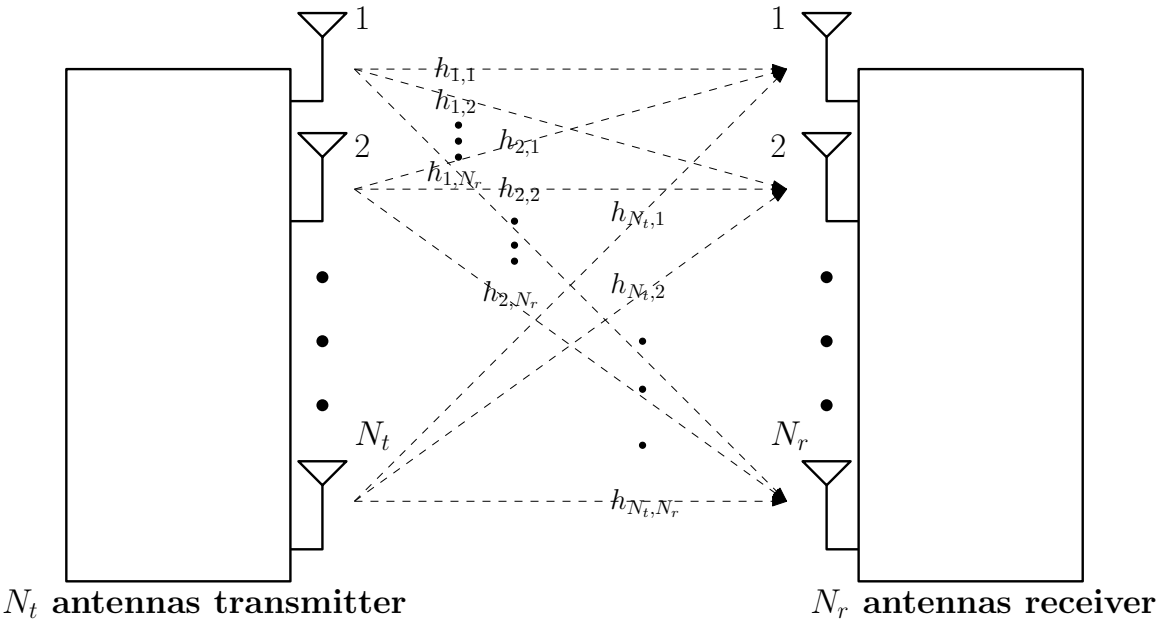

Figure 2.1: SU-MIMO channel model with N_t transmit antennas and N_r receive antennas

In MIMO systems, a single-user MIMO (SU-MIMO) system is a critical example. SU-MIMO systems have been investigated with an N_t multiple antenna transmitter and an N_r multiple antenna receiver as illustrated in Figure 2.1. The vector $\boldsymbol{s}$ represents the transmit data, $\boldsymbol{y}$ denotes the received signal and $\hat{\boldsymbol{s}}$ is the estimated data. The statistical channel expressed as:

$$\boldsymbol{H}(\tau, t) = \sum_{l=0}^{L-1} \boldsymbol{A}_l(t)\delta(\tau - \tau_l), \tag{2.5}$$

where $\boldsymbol{A}_l(t)$ denotes the lth path between transmitter and receiver. If $h_{i,j}(\tau, t)$ which denotes a function of the fading coefficient is employed, we can express the channel matrix as:

$$\boldsymbol{H}(\tau, t) = \begin{bmatrix} h_{1,1}(\tau,t) & h_{1,2}(\tau,t) & h_{1,3}(\tau,t) & \dots & h_{1,N_t}(\tau,t) \\ h_{2,1}(\tau,t) & h_{2,2}(\tau,t) & h_{2,3}(\tau,t) & \dots & h_{2,N_t}(\tau,t) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{N_r,1}(\tau,t) & h_{N_r,2}(\tau,t) & h_{N_r,3}(\tau,t) & \dots & h_{N_r,N_t}(\tau,t) \end{bmatrix} \tag{2.6}$$

Given the transmit signal vector $\boldsymbol{s} \in \mathbb{C}^{N_t \times 1}$, the received signal can be described by,

$$\boldsymbol{y}(t) = \boldsymbol{H}(\tau, t) * \boldsymbol{s}(t) + \boldsymbol{n}(t), \tag{2.7}$$

where $\boldsymbol{n}(t)$ is the Gaussian noise. In a flat-fading channel, as the output is independent of

inputs at a previous time instant, the received signal can be expressed as:

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{s} + \boldsymbol{n} \tag{2.8}$$

Equation 2.8 gives a general expression of the received signal for a SU-MIMO system experiencing flat-fading channel. During the transmission, spatial correlation caused by the limited scattering and insufficient spacing between adjacent antennas are described with a correlated channel matrix which is expressed by

$$\boldsymbol{H}_c = \boldsymbol{R_r}^{\frac{1}{2}} \boldsymbol{H} \boldsymbol{R_t}^{\frac{1}{2}} \tag{2.9}$$

where $\boldsymbol{R_r}$ and $\boldsymbol{R_t}$ are receive and transmit covariance matrices with $Tr(\boldsymbol{R_r}) = Nr$ and $Tr(\boldsymbol{R_t}) = Nt$. Both $\boldsymbol{R_r}$ and $\boldsymbol{R_t}$ are positive semi-definite Hermitian matrices. For the case of an urban wireless environment, the UE is always surrounded by rich scattering objects and the channel is most likely independent Rayleigh fading at the receive side. Hence, we assume $\boldsymbol{R_r} = \boldsymbol{I}_{N_r}$, and we have

$$\boldsymbol{H}_c = \boldsymbol{H} \boldsymbol{R_t}^{\frac{1}{2}} \tag{2.10}$$

To study the effect of antenna correlations, random realizations of correlated channels are generated according to the exponential correlation model such that the elements of $\boldsymbol{R_t}$ are given by

$$\boldsymbol{R_t}(i,j) = \begin{cases} r^{j-i} & \text{if } i \leq j \\ r_{j,i}^{*} & \text{if } i > j \end{cases}, |r| \leq 1 \tag{2.11}$$

where r is the correlation coefficient between any two neighbouring antennas.

Multiuser MIMO System Model

In Figure 2.2, a description of the downlink of a multiuser MIMO (MU-MIMO) system is given. In this scenario, the transmitter broadcasts signals to M users. We can regard the MU-MIMO system as a combination of T SU-MIMO systems. As a result, the total channel matrix $\boldsymbol{H} \in \mathbb{C}^{MN_r \times N_t}$ and precoding matrix $\boldsymbol{P} \in \mathbb{C}^{N_t \times MN_r}$ can be obtained as

$$\boldsymbol{H} = [\boldsymbol{H}_1^T \quad \boldsymbol{H}_2^T \quad \cdots \quad \boldsymbol{H}_M^T]^T \tag{2.12}$$

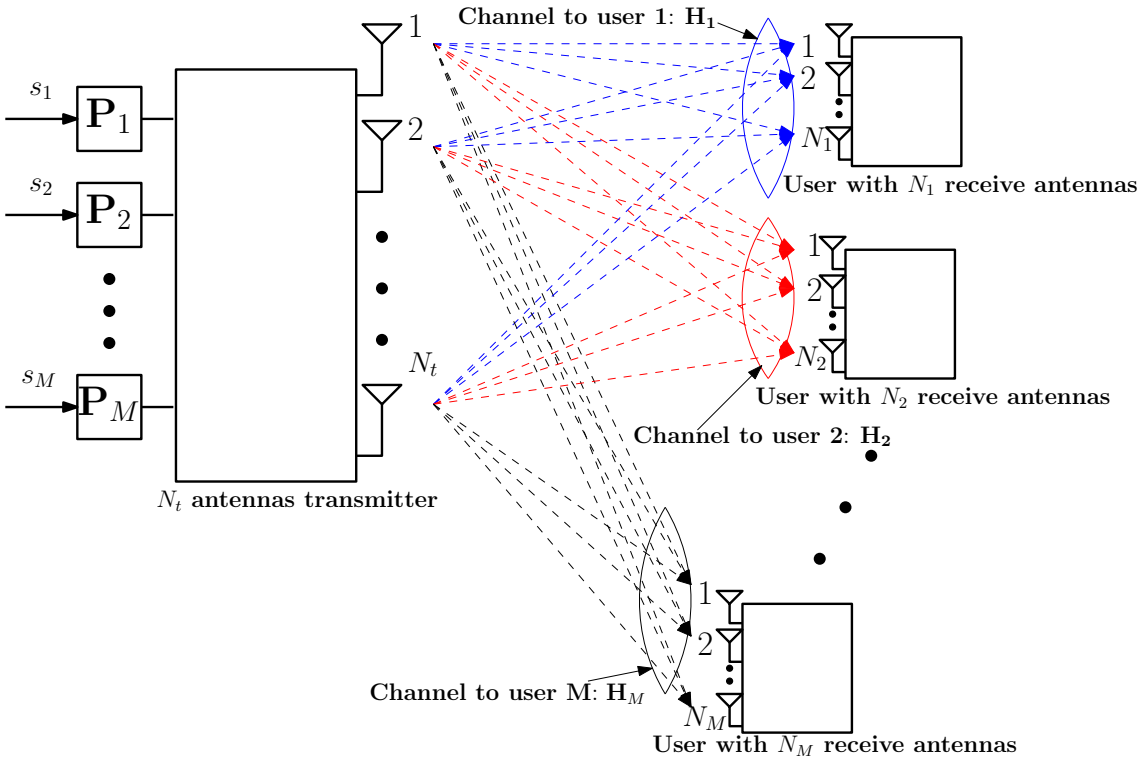

Figure 2.2: MU-MIMO channel model with one transmitter and M users. The source node is equipped with N_t antennas and the rth user is equipped with N_r receive antennas.

and

$$\boldsymbol{P} = [\boldsymbol{P}_1 \quad \boldsymbol{P}_2 \quad \cdots \quad \boldsymbol{P}_M] \tag{2.13}$$

For the rth user, the channel and precoding matrices can be expressed as $\boldsymbol{H}_r \in \mathbb{C}^{N_r \times N_t}$ and $\boldsymbol{P}_r \in \mathbb{C}^{N_t \times N_r}$ respectively. The received signal for user r in flat-fading channel is obtained as

$$\boldsymbol{y}_r = \boldsymbol{H}_r \boldsymbol{P}_r \boldsymbol{s}_r + \sum_{j=1, j\neq r}^{M} \boldsymbol{H}_r \boldsymbol{P}_j \boldsymbol{s}_j + \boldsymbol{n}_r, \tag{2.14}$$

where $\sum_{j=1,j\neq r}^{M} \boldsymbol{H}_r \boldsymbol{P}_j \boldsymbol{s}_j$ denotes the interference between different users.

Multiuser MIMO System Model with Relays

Due to the broadcast nature of radio wave, fading effects lead to an unreliable transmission especially for a long distance communication. To support the wireless transmission which suffers fading effects, relays are implemented between the transmitter and the receivers to compensate for the signal attenuation. Compared with direct transmission, relay systems divide the transmission into two parts. According to Figure 2.3, based on a MU-MIMO system, multiple-antenna relays are placed between the transmitter and users. If we assume

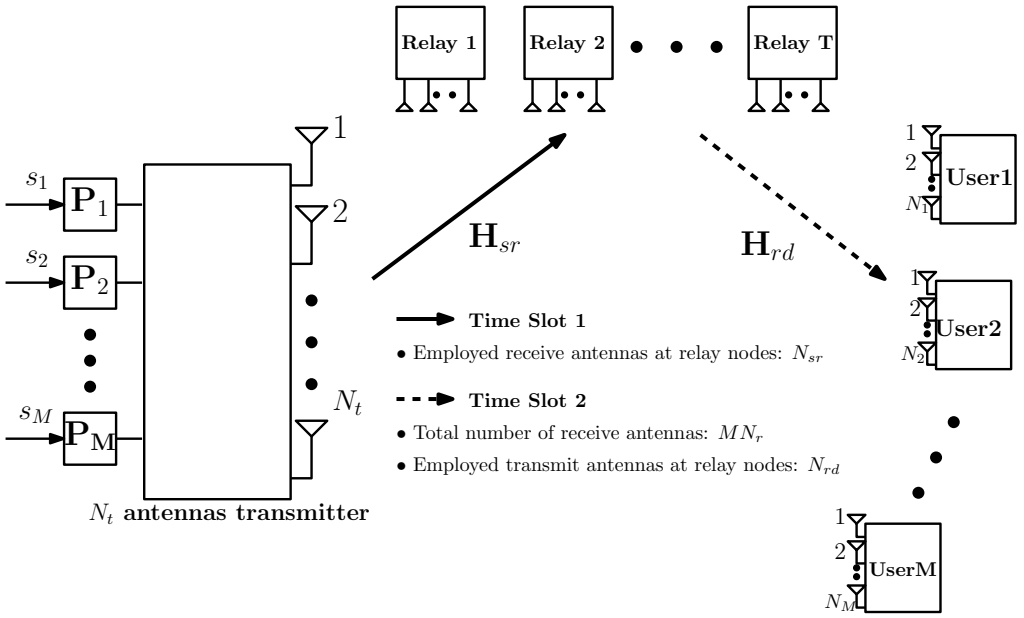

Figure 2.3: T relays are placed in a MU-MIMO channel model. The ith relay is equipped with N_i antennas.

each relay is equipped with N_i antennas and T relays are applied, to transmit signals to M users, the required number of relay antennas should satisfy $TN_i \geq MN_r$. Then we use $N_{rd} = MN_r$, which represents the number of antennas used at relays to forward signals to users and $N_{sr} = N_{rd}$ denotes the number of antennas applied to receive signals from the transmitter. With the total channel from the transmitter to the relays given as $\boldsymbol{H}_{sr} \in \mathbb{C}^{N_{sr} \times N_t}$, the received signal at the relays $\boldsymbol{y}_{sr} \in \mathbb{C}^{N_{sr} \times 1}$ is expressed as:

$$\boldsymbol{y}_{sr} = \boldsymbol{H}_{sr}\boldsymbol{P}_{sr}\boldsymbol{s} + \boldsymbol{n}_{sr}. \tag{2.15}$$

Given the total channel matrix from the relays to the users $\boldsymbol{H}_{rd} \in \mathbb{C}^{MN_r \times N_{rd}}$, the received signals at all users $\boldsymbol{y} \in \mathbb{C}^{MN_r \times 1}$ can be obtained as:

$$\boldsymbol{y} = \boldsymbol{H}_{rd}\boldsymbol{P}_{rd}\boldsymbol{y}_{sr} + \boldsymbol{n}_{rd} \tag{2.16}$$

In (2.15) and (2.16), the precoding matrices $\boldsymbol{P}_{sr}$ and $\boldsymbol{P}_{rd}$ are implemented at the source and at the relays, respectively. The details of how to obtain these matrices can be found in [24; 25].

2.4 Performance Metrics

In this thesis, the proposed techniques are developed and evaluated with the comparison to existing ones in terms of several metrics of particular relevance. Based on the properties of the constructed communication systems, in our work we have adopted the following metrics: the secrecy capacity and the associated secrecy rates, the bit error ratio and the computational complexity.

2.4.1 Secrecy Capacity

Since defined in the wire-tap channel model posed by Wyner [1], secrecy capacity became a critical evaluation value in the measurement of the security level in wireless networks. As

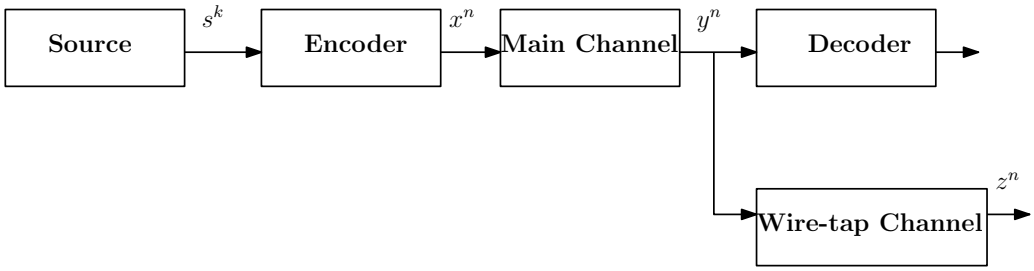

Figure 2.4: Wiretap channel model [1]: Degraded version of the Main channel

depicted in Figure 2.4, the received message y^n will pass the wiretap channel which is a probabilistically degraded version of the main channel. The eavesdropper will observe z^n. In [1], Wyner defined the equivocation rate of the eavesdropper, which is

$$R_e \leq H(s^k; z^n)/n, \tag{2.17}$$

where the conditional entropy $H(s^k; z^n)$ is the eavesdropper's equivocation. When the equivocation rate R_e is arbitrarily close to the information rate R, then the optimal R is the secrecy capcity of the wiretap channel. Starting from the wire-tap channel, Csisżar and Körner considered a more general non-degraded version in [2], where they obtained a single-letter characterization of the achievable private message rate, equivocation rate and common message rate for a two-receiver broadcast channel. The secrecy capacity was defined as

$$C_{Secrecy} = \max_{s^k \to x^n \to y^n, z^n} I(s^k; y^n) - I(s^k; z^n), \tag{2.18}$$

which is achieved by maximizing over all joint probability distributions such that a Markov chain $s^k, x^n, y^n z^n$ is formed. This concept is the fundamental idea for the physical-layer secrecy rate. Based on dirty-paper coding arguments, the achievable secrecy rate region can be enhanced by non-causal side information in [26]. This introduces other techniques, such as artificial noise or interference systems which we will present in the Jamming Techniques section.

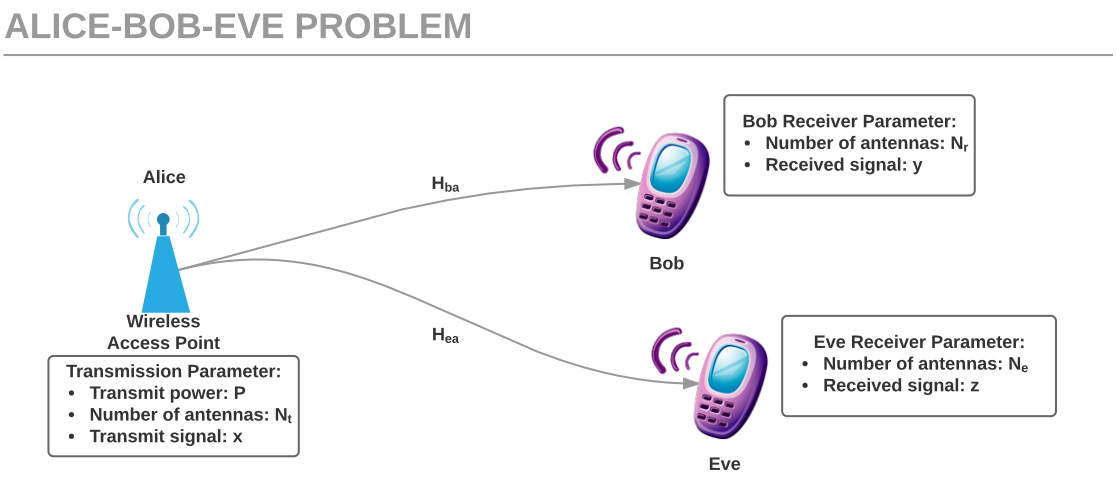

Figure 2.5: Wiretap channel model: Alice, Bob and Eve

In Wyner's work, the wire-tap channel is described. According to Figure 2.5, the channel from Alice to Bob is usually called the main channel and the transmission to Eve is known as the wire-tap channel. In single-antenna scenarios, the message s^k is encoded into a codeword x^n. The output of the main channel is given by,

$$y^n = h_{ba} x^n + n_{ba}, \tag{2.19}$$

where h_{ba} is the quasi-static fading coefficient for the main channel and n_{ba} represents the complex Gaussian noise. The received signal at the eavesdropper side is expressed as

$$z^n = h_{ea} x^n + n_{ea}, \tag{2.20}$$

where h_{ea} is the quasi-static fading coefficient for Eve and n_{ea} represents the complex Gaussian noise to Eve. Given the power assumption that the total transmit power P satisfies the

following constraint

$$\frac{1}{n}\sum_{i=1}^{n} E[|x(i)|^2] < P, \tag{2.21}$$

and the power of noise to Bob and Eve is obtained as N_{ba} and N_{ea} respectively, the instantaneous signal to noise ratio (SNR) of the main channel from Alice to Bob can be expressed as:

$$\gamma_{ba} = \frac{P|h_{ba}|^2}{N_{ba}} \tag{2.22}$$

Similarly, the instantaneous SNR to the eavesdropper is given by,

$$\gamma_{ea} = \frac{P|h_{ea}|^2}{N_{ea}} \tag{2.23}$$

According to the Shannon-Hartley theorem proved in [27], the channel capacity is expressed as a function of the bandwidth and the signal-to-noise ratio (SNR). With instantaneous SNR, the channel capacity of the transmission from Alice to Bob and Eve can be respectively obtained as:

$$C_{ba} = \frac{1}{2}\log(1+\gamma_{ba}) \tag{2.24}$$

and

$$C_{ea} = \frac{1}{2}\log(1+\gamma_{ea}). \tag{2.25}$$

Taking into account the monotonically increasing property of the log function, we can obtain the expression for the secrecy capacity:

$$C_{secrecy}^{\text{single-antenna}} = \begin{cases} \frac{1}{2}\log(1+\gamma_{ba}) - \frac{1}{2}\log(1+\gamma_{ea}) & \text{if } \gamma_{ba} > \gamma_{ea} \\ 0 & \text{if } \gamma_{ba} < \gamma_{ea} \end{cases} \tag{2.26}$$

Due to the development of expressions for the channel capacity in general MIMO networks and the non-convex property of the secrecy capacity expression, physical-layer security gains limited improvements in MIMO systems. Recently, research results on MU-MIMO technology have emerged. In a MIMO system [28], the channel capacity with perfect CSI is defined as:

$$C_{\text{perfect-CSI}} = E[\max_{\boldsymbol{R};\text{Tr}(\boldsymbol{R})\leq 1} \log(\det(\boldsymbol{I} + \gamma \boldsymbol{H}\boldsymbol{R}\boldsymbol{H}^H))], \tag{2.27}$$

where γ is the ratio between transmit power and noise power. The signal covariance matrix $\boldsymbol{R} = \boldsymbol{V}\boldsymbol{S}\boldsymbol{V}^H$ is obtained through Singular Value Decomposition (SVD) of the channel matrix $\boldsymbol{H} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H$ along with the optimal power allocation applying the water-filling procedure.

The scenario in which the CSI is available at the transmitter side is known as Closed-loop (CL) system. Then in an Open-loop (OL) system, when the CSI is unavailable at the transmitter and only the statistics of $\boldsymbol{H}$ are known, the transmit energy will be distributed equally to all transmit antennas. The channel capacity with no CSI means the signal covariance $\boldsymbol{R}$ to maximize channel capacity is under worst-case statistics. That is $\boldsymbol{R} = \frac{1}{N_t}\boldsymbol{I}$, if we have N_t transmitter antennas. So we have the channel capacity as

$$C_{\text{no-CSI}} = E[\log(\det(\boldsymbol{I} + \gamma \boldsymbol{H}\boldsymbol{H}^H/N_t)), \tag{2.28}$$

In the OL scenario, the distribution of the channel is assumed known at the transmitter. According to different equations, we are capable of measuring the physical-layer secrecy rate in different scenarios.

To improve the decoding accuracy of the wireless channel, different error control codes such as convolutional coding or BCH coding are implemented. By adding redundancy, these error control codes are capable of avoiding errors at the receiver side. Furthermore, turbo coding, LDPC are developed to closely approach the theoretical limits imposed by Shannon's theorem. At the same time, turbo coding can provide much lower decoding complexity than the Viterbi algorithm on the long convolutional codes that would be required for the same performance.

Relying on the derivation of channel capacity in MIMO scenarios, Oggier and Hassibi [18] proved the secrecy capacity under the constraints that the power of the noise is equal for Bob and Eve [18]. This result was obtained as follows:

$$\begin{aligned} C_{\text{sec}} &= \max_{\boldsymbol{R}_s \succeq 0} I(X_s; Y_i) - I(X_s; Y_k) \\ &= \max_{\boldsymbol{R}_s \succeq 0, \text{Tr}(\boldsymbol{R}_s)=\text{E}_\text{s}} \log(\det(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H)) \\ &\quad - \log(\det(\boldsymbol{I} + \boldsymbol{H}_{ea}\boldsymbol{R}_s\boldsymbol{H}_{ea}^H)), \end{aligned} \tag{2.29}$$

where in (2.29) $I(X_s; Y_i)$ and $I(X_s; Y_k)$ represent the mutual information between the transmitter to Bob as well as Eve. X_s, Y_i, Y_k are the counterparts of different signal symbols. $\boldsymbol{R}_s$ is the covariance matrix associated with the information signal $\boldsymbol{s}_r$. The quantity E_s corresponds the total transmit power. The matrices $\boldsymbol{H}_{ba} \in \mathcal{CN}(0, 1)$ and $\boldsymbol{H}_{ea} \in \mathcal{CN}(0, 1/m)$ represent the channel to the users and eavesdroppers, respectively, and $m = \frac{\sigma_{ea}^2}{\sigma_{ba}^2}$ designates the gain ratio between the main and wire-tap channel. The secrecy capacity is defined as the maximization of the difference between two mutual information terms. However, in practice

the channels are usually not perfectly known. This situation known as the imperfect channel state information (CSI) is discussed in [3]. For the imperfect channel state information $\boldsymbol{H}_{ea}$, the distribution of the eavesdroppers' channel is required by the transmitter.

2.4.2 Bit Error Ratio (BER)

The BER performance is employed to measure the transmission reliability in wireless networks. BER is defined as the number of bit errors divided by the total number of transferred bits during a studied time interval. The BER can be considered as an approximate estimate of the bit error probability. The BER performance of the system can be improved by error control codes. By adding redundancy, the received bits can be decoded more accurately.

2.4.3 Computational Complexity

In assessing the computational complexity, the number of Floating-Point Operations Per Second (FLOPS) is used as a measurement of the cost of an algorithm. In [29], the FLOPS for real QR, SVD and complex QR algorithms are given. 2 FLOPS are needed for a real multiplication with one addition, while for a complex multiplication with one addition it accounts for 8 FLOPS.

According to [30] for an $m \times n$ complex matrix $\boldsymbol{A}$,the FLOPS of the SVD of the complex matrix $\boldsymbol{A}$ are equivalent to its $2m \times 2n$ extended real matrix. The SVD of the matrix is $\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H$, where $\boldsymbol{U}$ and $\boldsymbol{V}$ are unitary matrices and $\boldsymbol{\Sigma}$ is a diagonal matrix containing the singular values of matrix $\boldsymbol{A}$.

$$\begin{bmatrix} \boldsymbol{A}_r & \boldsymbol{A}_i \\ -\boldsymbol{A}_i & \boldsymbol{A}_r \end{bmatrix} = \begin{bmatrix} \boldsymbol{U}_r & \boldsymbol{U}_i \\ \boldsymbol{U}_i & -\boldsymbol{U}_r \end{bmatrix} \begin{bmatrix} \boldsymbol{\Sigma} & 0 \\ 0 & \boldsymbol{\Sigma} \end{bmatrix} \begin{bmatrix} \boldsymbol{V}_r^T & \boldsymbol{V}_i^T \\ \boldsymbol{V}_i^T & -\boldsymbol{V}_r^T \end{bmatrix} \tag{2.30}$$

The number of FLOPS of the multiplication, the QR decomposition, the matrix inversion as well as SVD with different matrices obtained have been reported in [30]. Some of them are given in Table 2.1.

Table 2.1: Computational Complexity of Some Common Operations

Operation	Type of matrix	Size of matrix	FLOPs
Multiplication	Complex	$m \times n$ and $q \times p$	$8mnqp$
QR decomposition	Complex	$m \times n$	$16(n^2m - nm^2 + 1/3m^3)$
SVD where only $\boldsymbol{\Sigma}$	Complex	$m \times n$	$32(nm^2 + 2m^3)$
and $\boldsymbol{V}$ obtained			
SVD all matrix obtained	Complex	$m \times n$	$8(4n^2m + 8nm^2 + 9m^3)$
Inversion	Real	$m \times m$	$2m^3 - 2m^2 + m$

2.5 Transmit Processing Strategies

In a multiuser dowlink network, transmit processing is applied to mitigate multiuser interference. Precoding techniques are used in the downlink of a cellular network. According to the channel information between the transmitter and receiver, appropriate weightings are generated before the transmission to achieve the maximization of a particular metric of the system. These weights form the precoding matrix and the particular metric can be the received signal power for a single-steam transmission or the total throughput for a multiuser MIMO system. Precoding, as a key technique, basically can be divided into two categories, linear and non-linear. Linear precoding techniques have low computational complexity, but the BER performance is not often satisfactory. Non-linear precoding techniques have excellent BER performance at a cost of high computational complexity. In the following, some traditional precoding techniques are briefly reviewed.

2.5.1 Linear Precoding

Zero-Forcing (ZF) and Minimum Mean Square Error (MMSE)

In this section, the implementation of precoding is detailed based on a multiuser MIMO system. The precoding matrix $\boldsymbol{P}_r$ is used to beamform the streams to a particular user r. To obtain the precoding matrix $\boldsymbol{P}_r$, the total channel information $\boldsymbol{H} \in \mathbb{C}^{MN_r \times N_t}$ is assumed known to the transmitter. For ZF and MMSE precoders the precoding matrix are generated as

$$\boldsymbol{P}^{\text{zf}} = \boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H)^{-1} \tag{2.31}$$

and

$$\boldsymbol{P}^{\text{mmse}} = \boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H + \alpha_n^2 I)^{-1} \tag{2.32}$$

where $\boldsymbol{P}^{\text{zf}} \in \mathbb{C}^{N_t \times MN_r}$ and $\boldsymbol{P}^{\text{mmse}} \in \mathbb{C}^{N_t \times MN_r}$. Linear precoding techniques such as Zero-Forcing (ZF), Minimum Mean Square Error (MMSE) have the advantage of low complexity. However, ZF or MMSE precoding can hardly approach the capacity which often leads to unsatisfactory performance in physical-layer security.

Singular Value Decomposition (SVD)

Further research aim at the development of the capacity-achievable precoding techniques. SVD precoding is a typical capacity-achievable precoding. If power allocation is employed at the transmitter, the MIMO channel capacity can be achieved by implementing the Singular Value Decomposition (SVD) technique. The SVD procedure shows that

$$\boldsymbol{H} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H \tag{2.33}$$

The total channel $\boldsymbol{H}$ is decomposed into a diagonal matrix $\boldsymbol{\Sigma} \in \mathbb{C}^{MN_r \times N_t}$ with two unitary matrices $\boldsymbol{U} \in \mathbb{C}^{MN_r \times MN_r}$, $\boldsymbol{V} \in \mathbb{C}^{N_t \times N_t}$ multiplied at the transmitter and receiver sides. The diagonal entries of $\boldsymbol{\Sigma}$ are known as the singular values of $\boldsymbol{H}$ which are the absolute values of the eigenvalues. Based on the obtained diagonal matrix $\boldsymbol{\Sigma}$, a water-filling algorithm can be employed to achieve the capacity of the MIMO channel.

Block Diagonalization (BD)

Block Diagonalization (BD) precoding technique is developed especially for multiuser MIMO systems. It can be regarded as a two-step SVD precoding technique. Suppose we have a single user MIMO system, the channel capacity can be realized by using the SVD technique and water-filling algorithm. This is the second step SVD. Before this, the first step SVD aims to suppress the interference between different users. In general, the precoding constraints in the first step SVD is supposed to achieve

$$\boldsymbol{H}_r\boldsymbol{F}_j = 0 \quad for \quad r = 1, \cdots, j-1, j+1, \cdots, R, \tag{2.34}$$

where $\boldsymbol{F}_j \in \mathbb{C}^{N_t \times N_r}$ is defined as a null space of $\tilde{\boldsymbol{H}}_r \in \mathbb{C}^{(M-1)N_r \times N_t}$ which is described as,

$$\tilde{\boldsymbol{H}}_r = [\boldsymbol{H}_1^T \quad \boldsymbol{H}_2^T \quad \cdots \quad \boldsymbol{H}_{r-1}^T \quad \boldsymbol{H}_{r+1}^T \quad \cdots \quad \boldsymbol{H}_R^T]^T \tag{2.35}$$

From the SVD of $\tilde{\boldsymbol{H}}_r$

$$\tilde{\boldsymbol{H}}_r = \tilde{\boldsymbol{U}}_r \tilde{\boldsymbol{\Sigma}}_r [\tilde{\boldsymbol{V}}_r{}^{(1)} \tilde{\boldsymbol{V}}_r{}^{(0)}]^H \tag{2.36}$$

$\tilde{\boldsymbol{V}}_r{}^{(0)} \in \mathbb{C}^{N_t \times N_r}$ is obtained as the precoding matrix $\boldsymbol{F}_j$. Through the first SVD step the multi-user MIMO channel can be transformed into parallel effective single user MIMO channels $\boldsymbol{H}_{\text{eff,r}} = \boldsymbol{H}_r \boldsymbol{F}_r = \boldsymbol{H}_r \tilde{\boldsymbol{V}}_r{}^{(0)} \in \mathbb{C}^{N_r \times N_r}$, then the second SVD of $\boldsymbol{H}_{\text{eff,r}}$ is given by

$$\boldsymbol{H}_{\text{eff,r}} = \boldsymbol{U}_r \boldsymbol{\Sigma}_r \boldsymbol{V}_r{}^H. \tag{2.37}$$

where $\boldsymbol{V}_r \in \mathbb{C}^{N_r \times N_r}$. From equations (2.36) and (2.37) we can have the resulting precoding matrix

$$\boldsymbol{P}_r^{\text{BD}} = \tilde{\boldsymbol{V}}_r{}^{(0)} \boldsymbol{V}_r \tag{2.38}$$

$$\boldsymbol{P}^{\text{BD}} = [\tilde{\boldsymbol{V}}_1{}^{(0)} \boldsymbol{V}_1 \quad \tilde{\boldsymbol{V}}_2{}^{(0)} \boldsymbol{V}_2 \quad \cdots \quad \tilde{\boldsymbol{V}}_M{}^{(0)} \boldsymbol{V}_M] \tag{2.39}$$

where $\boldsymbol{P}_r^{\text{BD}} \in \mathbb{C}^{N_t \times N_r}$ and $\boldsymbol{P}^{\text{BD}} \in \mathbb{C}^{N_t \times N_t}$. It is worth noting that we need to use β to control the transmission power. And β can be obtained as:

$$\beta = \sqrt{\frac{E_r}{\text{Tr}(\boldsymbol{P}_r^{\text{BD}} \boldsymbol{s}_r \boldsymbol{s}_r^H \boldsymbol{P}_r^{\text{BD}^H})}} \tag{2.40}$$

2.5.2 Non-linear Precoding

Tomlinson-Harashima Precoding (THP)

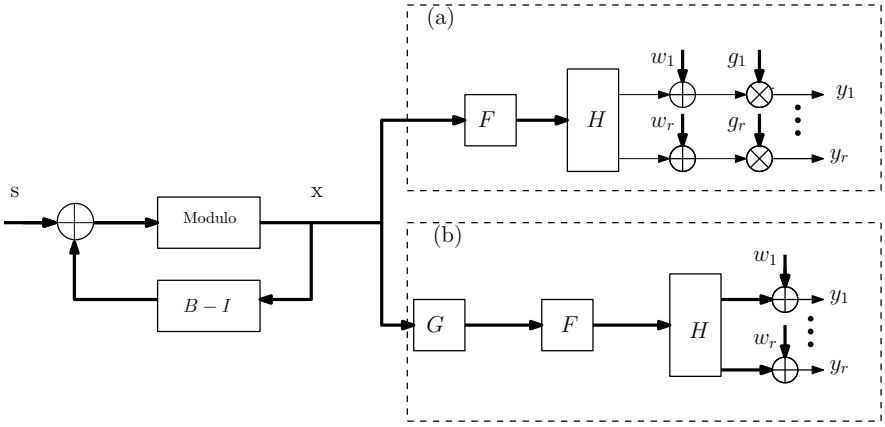

Figure 2.6: Different THP Precoding structures. (a) Decentralized THP Precoding (dTHP) (b) Centralized THP Precoding (cTHP)

THP precoding is introduced in [31]. Figure 2.6 gives a brief structure of the THP precoding. Based on the placement of the diagonal weighted matrix $\boldsymbol{G}$, THP precoding can be divided into two sub-structures. In the decentralized structure, the diagonal weighted matrix $\boldsymbol{G}$ is at the receiver side and each receiver is allocated with a diagonal entry g_k. This kind of THP precoding is known as dTHP and it leads to larger system capacity and more flexible subchannel management [32]. The other centralized structure THP precoding (cTHP) places the diagonal weighted matrix $\boldsymbol{G}$ at the transmitter. In this work we will focus on dTHP structure.

Conventional THP employs LQ decomposition. With implementing LQ decomposition of the channel matrix in a MU-MIMO system, we can obtain

$$\boldsymbol{H} = \boldsymbol{L}\boldsymbol{Q}, \tag{2.41}$$

where $\boldsymbol{L} \in \mathbb{C}^{MN_r \times N_t}$ is a lower triangular matrix and $\boldsymbol{Q} \in \mathbb{C}^{N_t \times N_t}$ is a unitary matrix. Then we can have the filters for the THP algorithm as:

$$\boldsymbol{F} = \boldsymbol{Q}^H, \tag{2.42}$$

$$\boldsymbol{G} = \mathrm{diag}[l_{1,1} \quad l_{2,2} \quad \cdots \quad l_{MN_r,MN_r}], \tag{2.43}$$

$$\boldsymbol{B}^{\mathrm{dTHP}} = \boldsymbol{G}\boldsymbol{L}, \tag{2.44}$$

where $l_{i,i}$ is the ith diagonal element of the matrix $\boldsymbol{L}$. According to Figure 2.6, the received signal for dTHP structure can be expressed as,

$$\boldsymbol{y}^{\mathrm{dTHP}} = \boldsymbol{G}(\boldsymbol{HFx} + \boldsymbol{n}) \tag{2.45}$$

where $\boldsymbol{x} \in \mathbb{C}^{N_t \times 1}$ is the combined transmit signal which can be calculated by

$$x_i = s_i - \sum_{j=1}^{i-1} b_{i,j} x_j, \quad i = 1, 2, \cdots, N_t, \tag{2.46}$$

following that, to control the power of the combined signal, modulo operation is applied before transmitting. Here we use the symbol $\Gamma_t(\cdot)$ to represent the modulo-t operation.

$$\Gamma_t(x_i) = x_i - \lfloor \frac{\mathrm{Re}(x_i)}{t} + \frac{1}{2} \rfloor t - j \lfloor \frac{\mathrm{Im}(x_i)}{t} + \frac{1}{2} \rfloor t \tag{2.47}$$

where $\lfloor \cdot \rfloor$ is the floor function and t is a constant for the periodic extension of the constellation. ZF-THP algorithm is originally proposed by Tomlinson and Harashima. With the AWGN channel CSI, the overall ZF-THP is a memoryless channel with input $\boldsymbol{s}$ and output $\boldsymbol{y}$ is given by [33]

$$\boldsymbol{y} = \Gamma_t(\boldsymbol{s} + \boldsymbol{a} + \boldsymbol{n}) = \Gamma_t(\boldsymbol{s} + \boldsymbol{n}). \tag{2.48}$$

In equation (2.48), $\boldsymbol{a}$ represents the interference from other users. When ZF is applied, the interference $\boldsymbol{a}$ is eliminated. Thus, the ZF-THP memoryless channel has mutual information

$$\begin{aligned} I(\boldsymbol{s}; \boldsymbol{y}) &= H(\boldsymbol{y}) - H(\boldsymbol{y}|\boldsymbol{s}) \\ &= H(\Gamma_t(\boldsymbol{s} + \boldsymbol{n})) - H(\Gamma_t(\boldsymbol{n})) \\ &\leq \log_2(t) - H(\Gamma_t(\boldsymbol{n})), \end{aligned} \tag{2.49}$$

where $H(\cdot)$ represent the differential entropy and the upper bound of equation (2.49) can be achieved if $\boldsymbol{s}$ is chosen to independent and identically distributed (i.d.d) uniform random variables distributed over the interval $(-t/2, t/2]$. In [33], the value t is chosen to satisfy the power constraint. Small values give a lower achievable information rate and large values will cause the power constraint to be violated.

Successive Optimization (SO) and SO-THP

Successive Optimization (SO) algorithm is employed in fading channels with the capability of achieving capacity. In the approach described in [34] each transmit matrix is optimized such that it does not interfere with any of the previous users. Each user will adjust its transmit power to compensate for the interference received from users and subject to the constraint that it does not interfere with any of those users. This approach applies the SO algorithm to optimize the transmitter power to eliminate the ISI. Similar capacity-achieving schemes are introduced in [35; 36; 37], but they assume at each successive step that the interfering signals are known completely and use knowledge of these signals in coding the next signal.

In [34], the authors give a successive precoding algorithm in order to define a simplified solution of the power control problem. By allowing a certain amount of interference, this algorithm can also reduces the capacity loss due to the subspace cancellation. It also can be applied to maintain a higher throughput for MU-MIMO transmission. First, for each user is calculated the optimal capacity in a SISO system, which means the capacity one user can achieve without any interference. Using SO, the modulation matrix for each user is designed in such a way that it lies only in the null space of the channel matrices of previous users. As a consequence, they will only generate the interference to this user. Let us define the previous $i-1$ users combined channel matrix as

$$\tilde{\boldsymbol{H}}_i = [\boldsymbol{H}_1^T \quad \boldsymbol{H}_2^T \quad \cdots \quad \boldsymbol{H}_{i-1}^T]^T. \tag{2.50}$$

As in the BD algorithm, the precoding matrix lies in the null space of $\tilde{\boldsymbol{H}}_i$. Thereby, the i-th user will not have any interference from any subsequent user $(i+1, \cdots, M)$

In [31], Successive Optimization Tomlinson-Harashima Precoding (SO-THP) is a combination of the Successive Optimization technique and Tomlinson-Harashima Precoding. In the SO-THP algorithm we initially consider the channel capacity for each user without the interference from other users as the optimal channel capacities for users in a multi-user MIMO system.Then the SO technique is used to reorder the transmit signals and performs interference cancellation. The replacement of the order of the transmit signals depends on which THP precoding matrices minimize the difference between the optimal channel capacities with that of the effective multi-user MIMO system channels. The main steps are introduced in [31]. SO-THP algorithm has the advantage of improving the BER and the secrecy rate performance, however, the complexity of this algorithm is high due to the successive optimization

process and the multiple SVD operations.

Generalized Matrix Inversion and Simplified Generalized MMSE Channel Inversion (S-GMI)

Generalized matrix inversion techniques have been introduced in [38]. Two approaches Generalized Zero-Forcing Channel Inversion (GZI) and Generalized MMSE Channel Inversion (GMI) are illustrated. For GZI, we have the same goal as the BD algorithm, which is to compute the null space of $\tilde{\boldsymbol{H}}_r$. Different from the BD algorithm, the first SVD is replaced by the QR decomposition which is computationally simpler, as described by

$$\hat{\boldsymbol{H}}_r = [\hat{\boldsymbol{Q}}_r^{(0)} \quad \hat{\boldsymbol{Q}}_r^{(1)}]\hat{\boldsymbol{R}}_r \qquad for \qquad r = 1, \cdots, M, \tag{2.51}$$

where $\hat{\boldsymbol{Q}}_r^{(0)} \in \mathbb{C}^{N_t \times N_r}$, $\hat{\boldsymbol{Q}}_r^{(1)} \in \mathbb{C}^{N_t \times (M-1)N_r}$, $\hat{\boldsymbol{R}}_r \in \mathbb{C}^{N_t \times N_r}$ and $\hat{\boldsymbol{H}}_r \in \mathbb{C}^{N_t \times N_r}$ is the rth element of the pseudo-inverse of the channel matrix $\hat{\boldsymbol{H}} \in \mathbb{C}^{N_t \times MN_r}$ is given by

$$\hat{\boldsymbol{H}} = \boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H)^{-1} = [\hat{\boldsymbol{H}}_1 \quad \hat{\boldsymbol{H}}_2 \quad \cdots \quad \hat{\boldsymbol{H}}_M]. \tag{2.52}$$

From equation (2.52) we can have $\tilde{\boldsymbol{H}}_r\hat{\boldsymbol{H}}_r = \boldsymbol{0}$. Following that, based on equation (2.51) we can then obtain $\tilde{\boldsymbol{H}}_r\hat{\boldsymbol{Q}}_r^{(0)} = \boldsymbol{0}$, which means the columns of $\hat{\boldsymbol{Q}}_r^{(0)}$ are orthonormal bases for the null space of $\tilde{\boldsymbol{H}}_r$. Following that the second step is the same as the SVD operation in the BD algorithm:

$$\boldsymbol{H}_r\hat{\boldsymbol{Q}}_r^{(0)} = \boldsymbol{U}_r^{(2)}\boldsymbol{\Sigma}_r^{(2)}{\boldsymbol{V}_r^{(2)}}^H, \tag{2.53}$$

where $\boldsymbol{U}_r^{(2)} \in \mathbb{C}^{N_r \times N_r}$, $\boldsymbol{\Sigma}_r^{(2)} \in \mathbb{C}^{N_r \times N_t}$, $\boldsymbol{V}_r^{(2)} \in \mathbb{C}^{N_t \times N_t}$. The precoding matrix and the receive filter are given by

$$\boldsymbol{P}_{\mathrm{GZI}} = [\hat{\boldsymbol{Q}}_1^{(0)}{\boldsymbol{V}_1}^{(2)} \quad \hat{\boldsymbol{Q}}_2^{(0)}{\boldsymbol{V}_2}^{(2)} \quad \cdots \quad \hat{\boldsymbol{Q}_M}^{(0)}{\boldsymbol{V}_M}^{(2)}], \tag{2.54}$$

$$\boldsymbol{M}_{\mathrm{GZI}} = \mathrm{diag}\{{\boldsymbol{U}_1^{(2)}}^H \quad {\boldsymbol{U}_2^{(2)}}^H \quad \cdots \quad {\boldsymbol{U}_M^{(2)}}^H\}, \tag{2.55}$$

where $\boldsymbol{P}_{\mathrm{GZI}} \in \mathbb{C}^{N_t \times N_t}$,$\boldsymbol{M}_{\mathrm{GZI}} \in \mathbb{C}^{N_t \times N_t}$. Similar to the GZI approach, the GMI scheme also uses the QR decomposition to decompose the MMSE channel inversion $\bar{\boldsymbol{H}} \in \mathbb{C}^{N_t \times MN_r}$ as expressed by

$$\bar{\boldsymbol{H}} = (\boldsymbol{H}^H\boldsymbol{H} + \alpha\boldsymbol{I})^{-1}\boldsymbol{H}^H, \tag{2.56}$$

$$\bar{\boldsymbol{H}}_r = [\bar{\boldsymbol{Q}}_r^{(0)} \quad \bar{\boldsymbol{Q}}_r^{(1)}]\bar{\boldsymbol{R}}_r \qquad for \qquad r = 1, \cdots, M, \tag{2.57}$$

where $\bar{\boldsymbol{H}}_r \in \mathbb{C}^{N_t \times N_r}$, $\bar{\boldsymbol{Q}}_r{}^{(0)} \in \mathbb{C}^{N_t \times N_r}$, $\bar{\boldsymbol{Q}}_r{}^{(1)} \in \mathbb{C}^{N_t \times (M-1)N_r}$ and $\bar{\boldsymbol{R}}_r \in \mathbb{C}^{N_t \times N_r}$. Compared to GZI, GMI takes the noise into account. It overcomes the noise enhancement in the BD algorithm. Meanwhile in the second step SVD scheme, extra interference may be introduced. To solve this problem, a transmit combining matrix $\boldsymbol{T}_r$ is applied to $\bar{\boldsymbol{Q}}_r{}^{(0)}$. Under the total transmit power constraint we use the minimum total MSE criterion to obtain the transmit combining matrix $\boldsymbol{T}_r$. In [31] the transmit combining matrix $\boldsymbol{T}_r$ is given by $\boldsymbol{T}_r = \beta \bar{\boldsymbol{T}}_r$ as described by

$$\bar{\boldsymbol{T}}_r = \left(\bar{\boldsymbol{Q}}_r{}^{(0)H} \sum_{j=1}^{R} \boldsymbol{H}_j^H \boldsymbol{H}_j \bar{\boldsymbol{Q}}_r{}^{(0)} + \alpha \boldsymbol{I} \right)^{-1} \bar{\boldsymbol{Q}}_r{}^{(0)H} \boldsymbol{H}_r^H \boldsymbol{H}_r \bar{\boldsymbol{Q}}_r{}^{(0)}, \tag{2.58}$$

where $\boldsymbol{T}_r$, $\bar{\boldsymbol{T}}_r \in \mathbb{C}^{N_t \times N_t}$. Once we have $\bar{\boldsymbol{Q}}_r$ and $\boldsymbol{T}_r$, the second SVD approach is

$$\boldsymbol{H}_r \bar{\boldsymbol{Q}}_r{}^{(0)} \boldsymbol{T}_r = \boldsymbol{U}_r^{(3)} \boldsymbol{\Sigma}_r^{(3)} \boldsymbol{V}_r{}^{(3)H}, \tag{2.59}$$

Similarly to the GZI scheme, the precoding matrix as well as the receive filter for the GMI scheme are

$$\boldsymbol{P}_{\mathrm{GMI}} = [\bar{\boldsymbol{Q}}_1{}^{(0)} \boldsymbol{T}_1 \boldsymbol{V}_1{}^{(3)} \quad \bar{\boldsymbol{Q}}_2{}^{(0)} \boldsymbol{T}_2 \boldsymbol{V}_2{}^{(3)} \quad \cdots \quad \bar{\boldsymbol{Q}}_M{}^{(0)} \boldsymbol{T}_M \boldsymbol{V}_M{}^{(3)}], \tag{2.60}$$

$$\boldsymbol{M}_{\mathrm{GMI}} = \mathrm{diag}\{\boldsymbol{U}_1^{(3)H} \quad \boldsymbol{U}_2^{(3)H} \quad \cdots \quad \boldsymbol{U}_R^{(3)H}\}, \tag{2.61}$$

where $\boldsymbol{P}_{\mathrm{GMI}} \in \mathbb{C}^{N_t \times N_t}$,$\boldsymbol{M}_{\mathrm{GMI}} \in \mathbb{C}^{N_t \times N_t}$. In [6], it has been proved that the transmit combining matrix $\boldsymbol{T}_r$ is not necessary since the regularized block diagonalization (RBD) constraint is already satisfied. Therefore, a simplified GMI (S-GMI) is developed in [30] as an improvement of the original RBD precoding in [39]. Based on the S-GMI algorithm, the second SVD approach and the receive filter are obtained as:

$$\boldsymbol{H}_r \bar{\boldsymbol{Q}}_r = \boldsymbol{U}_r^{(4)} \boldsymbol{\Sigma}_r^{(4)} \boldsymbol{V}_r{}^{(4)H}, \tag{2.62}$$

$$\boldsymbol{P}_{\mathrm{S-GMI}} = [\bar{\boldsymbol{Q}}_1{}^{(0)} \boldsymbol{V}_1{}^{(4)} \quad \bar{\boldsymbol{Q}}_2{}^{(0)} \boldsymbol{V}_2{}^{(4)} \quad \cdots \quad \bar{\boldsymbol{Q}}_M{}^{(0)} \boldsymbol{V}_M{}^{(4)}], \tag{2.63}$$

$$\boldsymbol{M}_{\mathrm{S-GMI}} = \mathrm{diag}\{\boldsymbol{U}_1^{(4)H} \quad \boldsymbol{U}_2^{(4)H} \quad \cdots \quad \boldsymbol{U}_M^{(4)H}\}, \tag{2.64}$$

where $\boldsymbol{P}_{\mathrm{S-GMI}} \in \mathbb{C}^{N_t \times N_t}$, $\boldsymbol{M}_{\mathrm{S-GMI}} \in \mathbb{C}^{N_t \times N_t}$.

2.5.3 Lattice Reduction

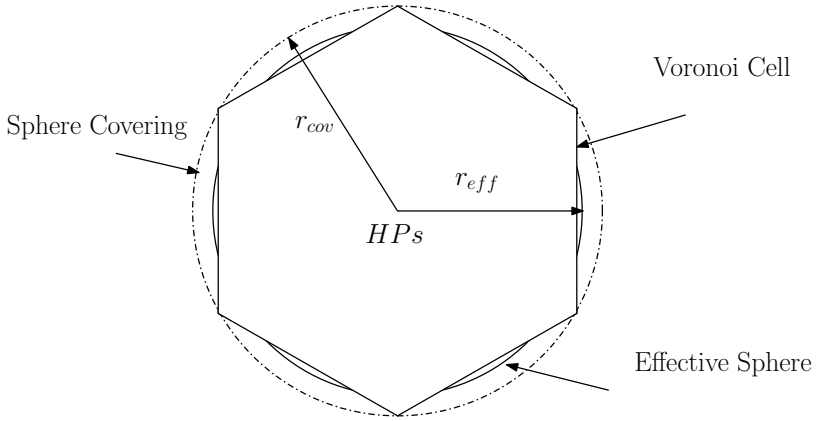

Figure 2.7: Voronoi Cell, Effective Radius and Covering Radius

An n-dimensional real lattice in an m-dimensional Euclidean space $\mathbf{R}^m$ can be described as the set of integer linear combinations of n independent vectors:

$$\boldsymbol{L}_{\mathbf{R}} = (\boldsymbol{B}_{LR}\boldsymbol{\lambda} : \lambda \in \mathbf{Z}^n) \tag{2.65}$$

where $\boldsymbol{B}_{LR} = [\boldsymbol{b}_1 \quad \boldsymbol{b}_2 \quad \cdots \quad \boldsymbol{b}_n]$ is a basis of the lattice $\boldsymbol{L}_{\mathbf{R}}$. In the wireless transmission system, $\boldsymbol{B}_{LR}$ can be regarded as the channel matrix and $\boldsymbol{L}_{\mathbf{R}}$ will be the channel matrix after Lattice-Reduction (LR). Before the LR aided algorithms we will introduce some basic lattice parameters mentioned in [40]. The shortest vector of the lattice $\boldsymbol{L}_{\mathbf{R}}$ is a non-zero vector in $\boldsymbol{L}_{\mathbf{R}}$ with the smallest Euclidean norm. The length of the shortest vector is represented by $\varepsilon(\boldsymbol{B}_{LR})$. The voronoi region of a lattice point α_i is described by,

$$\Phi_{\boldsymbol{L}_{\mathbf{R}}} = (\boldsymbol{y} \in \mathbf{R}^m : \|\boldsymbol{y} - \alpha_i\| \leq \|\boldsymbol{y} - \alpha_j\|, \forall \alpha_i \neq \alpha_j) \tag{2.66}$$

where $\Phi_{\boldsymbol{L}_{\mathbf{R}}}$ is the n-dimensional volume and it is determined by the determinant of $\mathbf{R}$, $det(\boldsymbol{L}_{\mathbf{R}}) = \sqrt{det(\boldsymbol{B}_{LR}^T \boldsymbol{B}_{LR})}$.

In Figure 2.7 two important lattice parameters related to the volume are given. The first one is the effective radius of lattice volume $\Phi_{\boldsymbol{L}_{\mathbf{R}}}$ which is denoted by $r_{\text{eff}}(\boldsymbol{L}_{\mathbf{R}})$. the effective radius is the radius of an effective sphere $S_{\text{eff}}(\boldsymbol{L}_{\mathbf{R}})$. For large n, it is approximately

$$r_{\text{eff}}(\text{Ł}_{\mathbf{R}}) \approx \sqrt{n/(2\pi e)}\det(\text{Ł}_{\mathbf{R}})^{1/n} \tag{2.67}$$

The covering radius of the lattice volume $\Phi_{\boldsymbol{L}_{\mathbf{R}}}$, denoted by $r_{\text{cov}}(\boldsymbol{L}_{\mathbf{R}})$, is the radius of the

smallest sphere centred at a lattice point which covers $\Phi_{\boldsymbol{L_R}}$. In wireless communications, the signals are represented by a complex number. The real lattice definition can be extended to complex values. The formula is similar,

$$Ł_{\mathbf{C}} = \boldsymbol{B_C u_C} : \boldsymbol{u_C} \in \mathbf{Z}[\mathbf{i}]^n \tag{2.68}$$

where $\boldsymbol{B_C}$ is a basis of the complex lattice $\boldsymbol{L_C}$.

While as described in [41], a basis change cannot always lead to optimum performance, it can in general improve performance. In particular, changing the lattice basis to be nearly orthogonal and shorter, the sense of which we will make precise later, we can generally obtain better decision boundaries. Based on the system described in Figure 2.1, the more correlated the columns of $\boldsymbol{H}$, the more significant the improvements. We also need to note that changing lattice basis does not change the lattice. The problem of finding the optimal lattice basis is called the lattice reduction (LR) problem.

For the LR aided strategy, we employ the complex lattice reduction algorithm (CLR) [30] to implement the size reduction before the reordering with the SO processing. Therefore, the LR transformed channel for the rth user is obtained as

$$\boldsymbol{H}^H_{\mathrm{red}_r} = \boldsymbol{H}^H_r \boldsymbol{T}_r, \tag{2.69}$$

where $\boldsymbol{H}_{\mathrm{red}_r} \in \mathbb{C}^{N_r \times N_t}$ is the transposed reduced channel matrix. The quantity $\boldsymbol{T}_r \in \mathbb{C}^{N_r \times N_r}$ is the transform matrix generated by the CLR algorithm [38]. Note that the transmit power constraint is satisfied since $\boldsymbol{T}_r$ is a unimodular matrix.

The basic idea behind using lattice reduction in conjunction with traditional low-complexity detectors is to operate in a chosen lattice basis that is optimized for those detectors. In the traditional system, the detector compensates for the original channel $\boldsymbol{H}$ to produce $\hat{\boldsymbol{z}}$. In the new system, we perform a basis change via a matrix $\boldsymbol{T}$, which is illustrated by

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{s} + \boldsymbol{n} = \boldsymbol{H}_{\mathrm{red}}\boldsymbol{z} + \boldsymbol{n} \tag{2.70}$$

with the basis change, the traditional detector is first used to compensate for the new LR transformed channel $\boldsymbol{H}_{\mathrm{red}}$ to produce $\hat{\boldsymbol{z}}$, then we can obtain the received signal $\hat{\boldsymbol{s}}$.

2.6 Relay Selection Techniques

In wireless networks, path loss or shadowing effect leads to the great attenuation of the signal power during the broadcasting . Novel relay techniques are developed to accomplish promising gain in throughput and energy efficiency in high attenuation scenarios [42; 43; 44]. In the presence of multiple relay nodes, transmission to the destination can be supported by relays which experience desired channel fading and interference [45]. Recent research are also developing the potential of applying relay system with security constraints [46; 47].

2.6.1 Relay Scheme

Depending on the processing of the received signal at the relay node, relay schemes can be divided into two categories: amplify-and-forward (AF) and decode-and-forward(DF).

Amplify-and-Forward (AF)

In AF protocol relay network, the received signal at the relay node is processed by a multiplication with an amplification coefficient. This amplification enlarges the power of the desired signal which in some extent compensates the channel fading effect in the transmission. Meanwhile, the noise and interference remain in the amplification which determines the limited application of the AF protocol in noise and interference channel. By transmitting the same information through several nodes, AF relaying method is a critical cooperative diversity scheme. The most attractive point of AF protocol relay network is the low complexity [48].

Decode-and-Forward (DF)

DF protocol employs decoding and encoding technique in the relay node. The transmission performance relies on the decoding performance at the relay node. Efficient decoding procedures enable the elimination of the channel fading and interference occurred during the transmission from transmitter to the relay [49]. By mitigating the channel fading and interference effects, the DF protocol is capable of achieving better performance than AF protocol in a high noisy and interference channel. However the decoding and encoding process brings much more complexity of implementation at relay nodes.

Recent researches combine two protocols together. A hybrid technique is illustrated in [50] which performs AF in a less noisy and interference environment and DF in a high noisy and interference scenario.

2.6.2 Buffer-aided Relay Schemes

Selection of relays make it possible of realizing spatial application of multiple relays in a wireless system. Buffers implemented at relay nodes provide an explore of the temporal application with relays. The received signal can be stored in the buffers and wait for a suitable forward time at which the signal will suffer low channel fading and interference. In buffer-aided relay networks, the length of buffers can be assumed infinite to obtain an optimal result which takes into account the full use of temporal benefit. Under assumption of finite buffer length, it is suggested that sufficient buffer length can result in a close performance to the optimal result [51; 52].

2.6.3 Relay Selection

In the presence of multiple relays, relay selection provides an efficient way of taking the advantage of spatial application in relay systems [14; 15]. Traditional relay selection techniques are using a particular thresholds to maintain the relay selection. The threshold can be coefficients of the channel, SNRs and even BER values. Various threshold require different knowledge of transmit information.

2.7 Jamming Techniques

Along with the development in the physical-layer security, the less theoretical jamming technique is considered to assist the secure transmission even in the scenario without knowledge of eavesdroppers' channel information. Artificial noise is generated at the transmit side. Broadcasting at all directions expect to legitimate users, artificial noise is capable of improving the physical-layer security performance by jamming the signal to eavesdroppers. With sufficient power, the noise or interference can be introduced by an extra helper, which denotes a helper or interference system.

2.7.1 Artificial Noise

Recently, artificial noise is applied in a physical-layer security scheme to degrade the eavesdroppers' reception [3]. The intended user is unaffected, so that a non-zero secrecy rate is ensured. A Gaussian artificial noise is generated with the assumption that the number of eavesdropper antennas N_{T+k} is strictly smaller than the number of transmitter antennas N_i. To overcome the restriction $N_{T+k} < N_i$, we can aim at maximizing the eavesdroppers' error probability P_E rather than the secrecy rate [3]. Defining the notion of practical secrecy as $P_E \to 1$ exponentially as the number of receiver antennas $N_i \to \infty$, for any signal-to-noise ratio (SNR) at the eavesdropper. More importantly, the definition of the covering ratio is proposed as a fundamental secrecy parameter which guarantees the convergence of P_E and characterizes the amount of the artificial noise required.

First, to simplify the scenario, we can consider that both the receiver and the eavesdropper have a single antenna each, and that multiple eavesdroppers cannot collude (i.e., $N_i = N_{T+k} = 1$). Wireless LAN is an example of such a scenario. With the base station as the transmitter. The concept of artificial noise can be clearly illustrated in this scenario. The artificial noise is produced such that it lies in the null space of the receiver's channel, while the information signal is transmitted in the range space of the receiver's channel. This design relies on knowledge of the receiver's CSI, but not of the eavesdropper's channel. The receivers of the users are able to null out the artificial noise, and hence, the receiver is not affected by the noise. However, in general, the eavesdropper's channel will be degraded, since its range space will be different from that of the receiver's channel, and hence, some component of artificial noise will lie in its range space. We now describe how the transmitter can generate artificial noise to degrade the eavesdropper's channel. The transmitter chooses $\boldsymbol{x}_r \in \mathbb{C}^{N_r \times 1}$ as the sum of information bearing signal $\boldsymbol{s}_r \in \mathbb{C}^{N_r \times 1}$ and the artificial noise signal $\boldsymbol{f}_r \in \mathbb{C}^{N_r \times 1}$ as given by

$$\boldsymbol{x}_r = \boldsymbol{s}_r + \boldsymbol{f}_r \tag{2.71}$$

Both $\boldsymbol{s}_r$ and $\boldsymbol{f}_r$ are assumed complex Gaussian vectors. $\boldsymbol{f}_r$ is chosen to lie in the null space of $\boldsymbol{H}_r$, such that $\boldsymbol{H}_r \boldsymbol{f}_r = 0$. If $\boldsymbol{Z}_r \in \mathbb{C}^{N_r \times 1}$ is an orthonormal basis for the null space of $\boldsymbol{H}_r$, with the assumptions that $\boldsymbol{f}_r = \boldsymbol{Z}_r v_r$, and $\boldsymbol{Z}_r \boldsymbol{Z}_r^H = \boldsymbol{I}$, the signals received by the receiver and the eavesdropper are given by, respectively,

$$\boldsymbol{y} = \boldsymbol{H}_r \boldsymbol{s}_r + \boldsymbol{n}_r \tag{2.72}$$

$$\boldsymbol{y} = \boldsymbol{H}_e \boldsymbol{s}_r + \boldsymbol{H}_e \boldsymbol{f}_r + \boldsymbol{n}_e \tag{2.73}$$

Note how the artificial noise $\boldsymbol{f}_r$ is nulled out by the receivers channel but not necessarily by the eavesdroppers channel. Thus, the eavesdropper channel is degraded with high probability, while that of the receiver remains unaffected. If $\boldsymbol{f}_r$ was chosen fixed, the artificial noise seen by the eavesdropper would be small if $\boldsymbol{H}_e \boldsymbol{f}_r$ is small. To avoid this possibility, the sequence of $\boldsymbol{f}_r$ is chosen to be complex Gaussian random vectors in the null space of $\boldsymbol{H}_r$. In particular, the transmitter chooses elements of $\boldsymbol{v}_r$ to be i.i.d. complex Gaussian random variables with variance σ_v^2, and independent in time as well. It follows that the elements of $\boldsymbol{f}_r$ are also Gaussian distributed. Based on channel matrix $\boldsymbol{H}_r$, the transmitter chooses the information bearing signal as $\boldsymbol{x}_r = \boldsymbol{P}_r \boldsymbol{s}_r$, where $\boldsymbol{s}_r$ is the information signal. We assume that Gaussian codes are used. $\boldsymbol{P}_r$ is chosen such that $\boldsymbol{H}_r \boldsymbol{P}_r \neq 0$. Now, secrecy capacity is bounded below by the difference in mutual information between the transmitter and the receiver versus the transmitter and the eavesdropper.

For a passive eavesdropper, $\boldsymbol{H}_e$ is not known to the transmitter, so using the concavity of $log(\cdot)$ and the i.i.d. assumption of $\boldsymbol{H}_r$, the average secrecy capacity is maximized by choosing $\boldsymbol{P}_r = \boldsymbol{H}_r^\dagger / \|\boldsymbol{H}_r\|$. Thus, the information bearing signal $\boldsymbol{x}_r$ lies in the range space of $\boldsymbol{H}_r^\dagger$ whereas the artificial noise lies in the null space of $\boldsymbol{H}_r^\dagger$.

2.7.2 Interference Systems

Besides the artificial noise, an interferer or helper is employed to assist the physical-layer security transmission. This kind of systems using Gaussian interference channels are investigated in [53] with an exploration of the capacity for MIMO scenario. With the jamming signal generated separately at the interference or helper node, secrecy rate of the transmission is improved [16; 54]. Then the scenario with multiple users are investigated in [55] with MISO channel.

2.8 Summary

In this chapter we summarize some applications and some fundamental metrics of physical-layer security research. The investigation of physical-layer security in our work locates in three critical aspects: transmit processing strategies, allocation of relays and jamming techniques. Following, based on the introduced techniques we will propose novel ideas to accomplish a

further development in physical-layer research.

Chapter 3

Successive Optimization Tomlinson-Harashima Precoding Strategies for Physical-Layer Security in Wireless Networks

3.1 Introduction

In this chapter we explore novel non-linear precoding techniques with secrecy constraints to ensure secure transmission in a multiuser MIMO downlink system. As an alternative technique to linear precoding approches, non-linear precoding techniques are compatible of mitigating interferences for small number multiuser systems [56]. This capacity-achievable technique is of great potential for some future wireless networks, such as distributed networks or wireless sensor networks.

3.1.1 Prior and Related Work

In recent years, precoding techniques, which rely on knowledge of channel state information (CSI), have been widely studied in the downlink of multiuser MIMO (MU-MIMO) systems. Linear precoding techniques such as zero-forcing (ZF), minimum mean-square error (MMSE) and block diagonalization (BD) have been introduced and studied in[39; 5; 17]. Linear precoding techniques accomplish multiuser interference mitigation in MU-MIMO systems with

low complexity and acceptable throughput performance. Furthermore, non-linear precoding techniques like Tomlinson-Harashima precoding (THP) [57], vector perturbation (VP) precoding [58] are reported and investigated with their capability of ensuring higher throughput than linear precoding techniques.

In the previous mentioned works, CSI knowledge is necessary for a precoding technique to maintain a high throughput performance. In the context of a physical-layer security problem, this assumption is strengthened to a more strict one with full CSI knowledge to eavesdroppers [1; 2; 18]. To ensure a secure transmission with more reasonable assumptions, in [3] the authors posed an artificial noise (AN) technique. Several criteria or strategies applying AN to wireless systems have been introduced in [59; 60]. In particular, the approaches reported in [61] have been applied to the downlink of MU-MIMO systems.

Apart from the studies in precoding techniques there are also some works that introduce lattice-reduction (LR) strategies [40; 62]. The LR strategies are introduced prior to the transmission aiming at achieving full diversity in the downlink MU-MIMO systems.

3.1.2 Motivation and Contributions

Prior work about physical-layer security systems based on [3; 61] indicate that linear precoding techniques can effectively improve the secrecy rate of wireless systems. In terms of throughput performance, non-linear precoding techniques can outperform linear approaches. In particular, reduced complexity non-linear precoding techniques can maintain a higher level of the sum-rate performance than linear schemes in high frequency transmission when the set of active users is small [56; 63]. Meanwhile, non-linear precoding techniques have not been investigated in physical-layer security systems with regards to their great potential of improving the secrecy rate of a wireless network. In this chapter we investigate non-linear precoding algorithms to assist the secrecy rate performance in a MU-MIMO system. With less power consumption or reduced complexity, novel non-linear precoding algorithms are desired to maintain full diversity in the MIMO systems.

In this chapter, we first present a study of conventional successive optimization Tomlinson-Harashima precoding (SO-THP) algorithm. Following that developments of SO-THP algorithm based on the generalized matrix inversion approach reported in [17] are given with detailed algorithmic steps. More specifically, the novel algorithms exploit techniques including block diagonalization, successive interference cancellation and lattice-reduction to balance the performances between secrecy rate and complexity. The main idea of the proposed ap-

proaches is to achieve a higher secrecy rate than existing non-linear and linear precoding algorithms. In addition, full diversity of the MIMO system is sought by the proposed algorithms. The major contributions in this chapter are summarized as follows:

- A novel non-linear precoding technique, namely, SO-THP+GMI is proposed for the downlink of MU-MIMO networks in the presence of multiple eavesdroppers.
- The proposed SO-THP+GMI algorithm combines the SO-THP precoding with the GMI technique to achieve a higher secrecy rate.
- The proposed SO-THP+GMI precoding algorithm is extended to a S-GMI version which aims to reduce computational complexity of the SO-THP+GMI algorithm.
- An LR strategy is combined with the aforementioned S-GMI version proposed algorithm and this so-called LR-aided version algorithm achieves full receive diversity.
- An analysis of the secrecy rate achieved by the proposed non-linear precoding algorithms is carried out along with an assessment of their computational complexity.
- When different power levels are allocated to generate artificial noise, an analysis of the power ratio which can achieve the optimal value in terms of secrecy rate is given.

3.2 System Model and Performance Metrics

In this section a downlink system model of a MU-MIMO network is considered. Following that, performance metrics used in the assessment of the proposed and existing techniques are described.

3.2.1 System Model

Here we consider a MU-MIMO downlink wireless network similar to the wiretap channel. In Figure 3.1, the system contains one transmitter, M users and K eavesdroppers. Here we assume that one eavesdropper tries to intercept the data for the specific user. The transmitter is equipped with N_t antennas. Each user and each eavesdropper node are equipped with N_r and N_k receive antennas, respectively. In this system we assume that the eavesdroppers do not jam the transmission and the channel from the transmitter to each user or eavesdropper follows a flat-fading channel model. The quantities $\boldsymbol{H}_r \in \mathbb{C}^{N_r \times N_t}$ and $\boldsymbol{H}_k \in \mathbb{C}^{N_k \times N_t}$ denote the channel matrix of the rth user and kth eavesdropper, respectively. Following [31], the

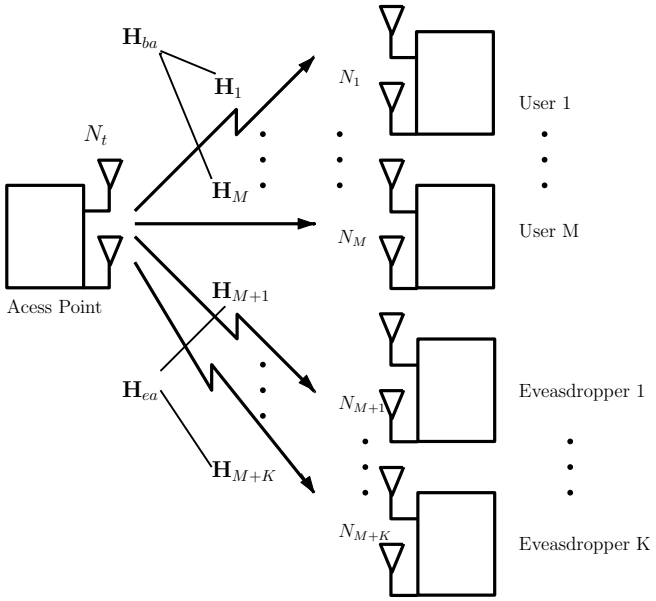

Figure 3.1: System model of a MU-MIMO system with M users and K eavesdroppers

number of antennas is assumed satisfying $N_t^{\text{total}} \geqslant M \times N_r$. During the transmission, $N_t = M \times N_r$ antennas at the transmitter are activated to perform the precoding procedure. In other words, the precoding matrix is assumed here for convenience to be always a square matrix.

We use the vector $\boldsymbol{s}_r \in \mathbb{C}^{N_r \times 1}$ to represent the data symbols to be transmitted to user r. An artificial noise (AN) can be injected before the data transmission to enhance the physical-layer secrecy. We use the vector $\boldsymbol{s}'_r \in \mathbb{C}^{m \times 1}$ with $m \leqslant (N_t^{\text{total}} - M \times N_r)$ to denote the independently generated jamming signal. Assume the transmit power of user r is E_r, and $0 < \rho < 1$ is the power fraction devoted to the user. Then, the power of user and jamming signal can be respectively expressed as $E[\boldsymbol{s}_r^H \boldsymbol{s}_r] = \rho E_r$ and $E[\boldsymbol{s}_r'^H \boldsymbol{s}'_r] = (1-\rho)E_r$. Finally, the signal after precoding can be expressed as

$$\boldsymbol{x}_r = \boldsymbol{P}_r \boldsymbol{s}_r + \boldsymbol{P}'_r \boldsymbol{s}'_r, \tag{3.1}$$

where the quantities $\boldsymbol{P}_r \in \mathbb{C}^{N_t \times N_r}$ and $\boldsymbol{P}'_r \in \mathbb{C}^{N_t \times m}$ are the corresponding precoding matrices. Here we take zero-forcing precoding as an instance. Given the total channel matrix $\boldsymbol{H} = [\boldsymbol{H}_1^T \quad \boldsymbol{H}_2^T \quad \cdots \quad \boldsymbol{H}_r^T \quad \cdots \quad \boldsymbol{H}_M^T]^T$, the total precoding matrix can be obtained as $\boldsymbol{P}^{\text{ZF}} = \boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H)^{-1}$. The precoding matrix $\boldsymbol{P}^{\text{ZF}}$ can be expanded to $\boldsymbol{P}^{\text{ZF}} = [\boldsymbol{P}_1 \quad \boldsymbol{P}_2 \quad \cdots \quad \boldsymbol{P}_r \quad \cdots \quad \boldsymbol{P}_M]$. Simultaneously, the precoding matrix $\boldsymbol{P}'_r$ can be generated from the null space of the rth user channel $\boldsymbol{H}_r$ by singular value decomposition (SVD) [61]. As a result, we have $\boldsymbol{H}_r \boldsymbol{P}'_r = \boldsymbol{0}$, which means the jamming signal does not interfere

the user's signal. The received data for each user or eavesdropper considering jamming and multiuser interferences can be described by

$$\boldsymbol{y}_r = \beta_r^{-1}(\boldsymbol{H}_r\boldsymbol{P}_r\boldsymbol{s}_r + \boldsymbol{H}_r\boldsymbol{P}'_r\boldsymbol{s}'_r + \boldsymbol{H}_r\sum_{j=1,j\neq r}^{T}\boldsymbol{P}_j\boldsymbol{s}_j + \boldsymbol{n}_r), \tag{3.2}$$

where $\beta_r = \sqrt{\frac{E_r}{||\boldsymbol{P}_r|| + ||\boldsymbol{P}'_r||}}$ is used to ensure that the transmit power after precoding remains the same as the original transmit power E_r for user r.

3.3 Review of the SO-THP Algorithm

In this section, a brief review of the conventional successive optimization THP (SO-THP) in [39] is given. The general structure of the SO-THP algorithm is illustrated in Figure 3.2 and its main implementation steps are introduced in the following.

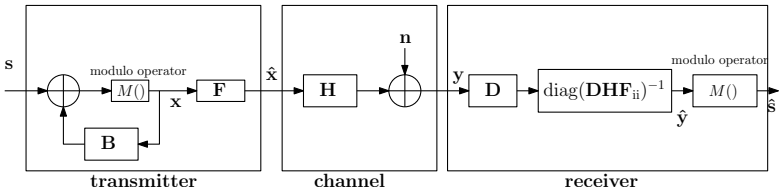

Figure 3.2: Centralized SO-THP structure

In Figure 3.2, a modulo operation $M(\cdot)$ which is defined in [64] is employed in the SO-THP algorithm. The details of modulo operation are given in the literature review chapter. Based on [31], THP can be equivalently implemented in a successive block diagonalization manner. In particular, the precoding matrix is given by

$$\boldsymbol{P}_r^{\mathrm{BD}} = \tilde{\boldsymbol{V}}_r^{(0)}\boldsymbol{V}_{\mathrm{eff}}, \tag{3.3}$$

where $\tilde{\boldsymbol{V}}_r^{(0)} \in \mathbb{C}^{N_t \times N_r}$ is the nulling matrix of the rth user's channel, $\boldsymbol{V}_{\mathrm{eff}}$ is a unitary matrix of the corresponding effective channel and the demodulation matrix of the rth user is chosen as $\boldsymbol{D}_r = \boldsymbol{U}_{\mathrm{eff}}^H$, where $\boldsymbol{U}_{\mathrm{eff}}^H$ is also obtained from the effective channel. Given a channel matrix $\tilde{\boldsymbol{H}}_r = [\tilde{\boldsymbol{H}}_1^T \quad \tilde{\boldsymbol{H}}_2^T \quad \cdots \quad \tilde{\boldsymbol{H}}_{r-1}^T \quad \tilde{\boldsymbol{H}}_{r+1}^T \cdots \quad \tilde{\boldsymbol{H}}_T^T]^T$, $\tilde{\boldsymbol{V}}_r^{(0)}$ can be obtained by the SVD operation $\tilde{\boldsymbol{H}}_r = \tilde{\boldsymbol{U}}_r\tilde{\boldsymbol{\Sigma}}_r[\tilde{\boldsymbol{V}}_r^{(1)}\tilde{\boldsymbol{V}}_r^{(0)}]^H$. Based on $\tilde{\boldsymbol{V}}_r^{(0)}$, an effective channel can be calculated and with second SVD operation $\boldsymbol{H}_{\mathrm{eff}} = \boldsymbol{H}_r\tilde{\boldsymbol{V}}_r^{(0)} = \boldsymbol{U}_{\mathrm{eff}}\boldsymbol{\Sigma}_{\mathrm{eff}}\boldsymbol{V}_{\mathrm{eff}}^H$ we can arrive at getting $\boldsymbol{V}_{\mathrm{eff}}$ and $\boldsymbol{U}_{\mathrm{eff}}^H$.

For each iteration, the SO-THP algorithm selects the user with maximum capacity from the

remaining users and process it first. The selection criterion is described as

$$\min_r (C_{max,r} - C_r); \tag{3.4}$$

where $C_{max,r}$ denotes the maximum capacity of the rth user and C_r is the capacity considering the interference from the other users. Here we use the criterion to select a better channel for user r to achieve a as high capacity as possible for the MU-MIMO channel. If we assume there is no interference from other users and the capacity can be achieved by the SVD procedure, we have

$$\boldsymbol{H}_r = \boldsymbol{U}_r \boldsymbol{\Sigma}_r [\boldsymbol{V}_r{}^{(1)} \boldsymbol{V}_r{}^{(0)}]^H, \tag{3.5}$$

$$C_{max,r} = \log_2 \det \left(\boldsymbol{I} + \boldsymbol{H}_r \boldsymbol{V}_r{}^{(1)} \boldsymbol{V}_r{}^{(1)H} \boldsymbol{H}_r{}^H \right). \tag{3.6}$$

In the scenario considering the interference from the other users, the BD decomposition is implemented on the channels of the remaining users in each iteration:

$$C_r = \log_2 \det \left(\boldsymbol{I} + \boldsymbol{H}_r \boldsymbol{P}_r^{\mathrm{BD}} \boldsymbol{P}_r^{\mathrm{BD}\,H} \boldsymbol{H}_r{}^H \right); \tag{3.7}$$

Therefore, the filters for the SO-THP algorithm can be obtained as

$$\boldsymbol{F} = \left(\boldsymbol{P}_1^{\mathrm{BD}} \cdots \boldsymbol{P}_T^{\mathrm{BD}} \right), \tag{3.8}$$

$$\boldsymbol{D} = \begin{pmatrix} \boldsymbol{U}_{\mathrm{eff1}}^H & & \\ & \ddots & \\ & & \boldsymbol{U}_{\mathrm{effT}}^H \end{pmatrix}, \tag{3.9}$$

$$\boldsymbol{B} = \text{lower triangular} \left(\boldsymbol{DHF} \bullet \mathrm{diag} \left([\boldsymbol{DHF}]_{ii}^{-1} \right) \right). \tag{3.10}$$

It is worth noting that $\boldsymbol{F}$ in (3.8), $\boldsymbol{D}$ in (3.9) are calculated in the reordered way according to the criterion (3.4), and the scaling matrix $\boldsymbol{G} = \mathrm{diag} \left([\boldsymbol{DHF}]_{ii}^{-1} \right)$.

3.4 Proposed Precoding Algorithms

In this section, we present three non-linear precoding algorithms SO-THP+GMI, SO-THP+S-GMI and LR-SO-THP+S-GMI for the downlink of MU-MIMO systems, and a selection criterion based on capacity is devised for these algorithms. We then derive filters for the three proposed precoding techniques, which are computationally simpler than the conventional

SO-THP.

According to [31], the conventional SO-THP algorithm aims at improving the sum rate performance. Successive optimization using BD precoder provides a more practical way of approaching capacity than traditional THP techniques. However, the complexity of this approach is high due to the successive optimization procedure and the multiple SVD operations. In [38], an approach called generalized MMSE channel inversion (GMI) is developed with QR decomposition to overcome the noise enhancement drawback of BD precoder caused by its focus on the suppression of multi-user interference. In particular, GMI supplies a much lower complexity than BD precoder. Later in [6],it is shown that the complete suppression of multi-user interference is not necessary and residual interference is small and cannot affect the sum-rate performance. This approach is called simplified GMI (S-GMI). Inspired by works done in dirty paper coding (DPC) [65] and other non-linear precoding techniques [31; 32; 66], we propose more practical non-linear precoding techniques to assist physical-layer security transmission with a balance between complexity and BER performance.

SO-THP+GMI Algorithm

The proposed SO-THP+GMI algorithm focuses on achieving higher secrecy rate performance than the conventional SO-THP algorithm with less computational complexity. Conventional SO-THP algorithm employs BD precoding technique to obtain the precoding matrix (3.3) as well as receive filter matrix. However, mitigating interference by BD precoding technique leads to the noise enhancement in the procedure. In [38], a GMI scheme uses QR decomposition to perform interference cancellation of the MMSE channel inversion $\bar{\boldsymbol{H}} \in \mathbb{C}^{N_t \times MN_r}$ as expressed by

$$\bar{\boldsymbol{H}} = (\boldsymbol{H}^H \boldsymbol{H} + \alpha \boldsymbol{I})^{-1} \boldsymbol{H}^H, \tag{3.11}$$

$$\bar{\boldsymbol{H}}_r = [\bar{\boldsymbol{Q}}_r^{(0)} \quad \bar{\boldsymbol{Q}}_r^{(1)}] \bar{\boldsymbol{R}}_r \qquad for \qquad r = 1, \cdots, M, \tag{3.12}$$

where $\bar{\boldsymbol{H}}_r \in \mathbb{C}^{N_t \times N_r}$, $\bar{\boldsymbol{Q}}_r^{(0)} \in \mathbb{C}^{N_t \times N_r}$, $\bar{\boldsymbol{Q}}_r^{(1)} \in \mathbb{C}^{N_t \times (M-1)N_r}$ are orthogonal matrices, $\bar{\boldsymbol{R}}_r \in \mathbb{C}^{N_t \times N_r}$ is an upper triangular matrix. According to (3.11), the noise effect is taken into account in GMI technique. As a result, the generation of the precoding matrix will mitigate the noise enhancement. When the GMI generated precoding matrix is used to calculate the channel capacity with (3.7), the reduced noise contributes to the increase of secrecy rate. Also with (3.12), the QR decomposition reduces the computational complexity as compared with the conventional SO-THP algorithm implementing SVD decomposition. In the GMI

algorithm, to completely mitigate the interference and noise, a transmit combining matrix $\boldsymbol{T}_r$ given in [38] is applied to $\bar{\boldsymbol{Q}}_r{}^{(0)}$. Once we have $\bar{\boldsymbol{Q}}_r{}^{(0)}$ and $\boldsymbol{T}_r$, we can write the relation

$$\boldsymbol{H}_r\bar{\boldsymbol{Q}}_r{}^{(0)}\boldsymbol{T}_r = \bar{\boldsymbol{U}}_r\bar{\boldsymbol{\Sigma}}_r\bar{\boldsymbol{V}}_r{}^H, \tag{3.13}$$

Then the precoding matrix as well as the receive filter for the GMI scheme are given by

$$\boldsymbol{P}_{\text{GMI}} = [\bar{\boldsymbol{Q}}_1{}^{(0)}\boldsymbol{T}_1\bar{\boldsymbol{V}}_1 \quad \bar{\boldsymbol{Q}}_2{}^{(0)}\boldsymbol{T}_2\bar{\boldsymbol{V}}_2 \quad \cdots \quad \bar{\boldsymbol{Q}}_M{}^{(0)}\boldsymbol{T}_M\bar{\boldsymbol{V}}_M], \tag{3.14}$$

$$\boldsymbol{M}_{\text{GMI}} = \text{diag}\{\bar{\boldsymbol{U}}_1{}^H \quad \bar{\boldsymbol{U}}_2{}^H \quad \cdots \quad \bar{\boldsymbol{U}}_M{}^H\}, \tag{3.15}$$

where $\boldsymbol{P}_{\text{GMI}} \in \mathbb{C}^{N_t\times N_t}$,$\boldsymbol{M}_{\text{GMI}} \in \mathbb{C}^{N_t\times N_t}$. The details of the proposed SO-THP+GMI algorithm to obtain the precoding and receive filter matrices are given in the table of Algorithm 1.

SO-THP+S-GMI Algorithm

Further development on SO-THP+GMI with complexity reduction leads to a novel SO-THP+S-GMI alogrithm. A simplified GMI (S-GMI) algorithm has been posed in [6] as an improvement of the original RBD precoding in [39]. In (3.13), to achieve complete interference cancellation between different users,a transmit combining matrix is applied. However, this procedure can be simplified according to the results shown in [6]. In the case that the interference is not completely mitigated, the complexity will have a significant reduction with just a slight decrease of sum-rate performance. Here, we incorporate the S-GMI technique into an SO-THP scheme and devise the SO-THP+S-GMI algorithm. The transmit precoding and receive filter matrices of the proposed SO-THP+S-GMI algorithm are described by

$$\boldsymbol{H}_r\bar{\boldsymbol{Q}}_r{}^{(0)} = \tilde{\boldsymbol{U}}_r\tilde{\boldsymbol{\Sigma}}_r\tilde{\boldsymbol{V}}_r{}^H, \tag{3.16}$$

$$\boldsymbol{P}_{\text{S-GMI}} = [\bar{\boldsymbol{Q}}_1{}^{(0)}\tilde{\boldsymbol{V}}_1 \quad \bar{\boldsymbol{Q}}_2{}^{(0)}\tilde{\boldsymbol{V}}_2 \quad \cdots \quad \bar{\boldsymbol{Q}}_M{}^{(0)}\tilde{\boldsymbol{V}}_M], \tag{3.17}$$

$$\boldsymbol{M}_{\text{S-GMI}} = \text{diag}\{\tilde{\boldsymbol{U}}_1{}^H \quad \tilde{\boldsymbol{U}}_2{}^H \quad \cdots \quad \tilde{\boldsymbol{U}}_M{}^H\}, \tag{3.18}$$

where $\boldsymbol{P}_{\text{S-GMI}} \in \mathbb{C}^{N_t\times N_t}$, $\boldsymbol{M}_{\text{S-GMI}} \in \mathbb{C}^{N_t\times N_t}$.

With reduced computational complexity, the SO-THP+S-GMI algorithm is capable of achieving better secrecy rate performance especially at lower SNR. The detailed S-GMI procedure implemented in the proposed SO-THP+S-GMI algorithm is shown in Algorithm 2. Cooper-

Algorithm 1 Proposed SO-THP+GMI Precoding

for $r = 1 : T$ **do**
  $\boldsymbol{G}_r = \boldsymbol{H}_r$;
  $\boldsymbol{G}_r = \boldsymbol{U}_r \boldsymbol{\Sigma}_r [\boldsymbol{V}_r{}^{(1)} \boldsymbol{V}_r{}^{(0)}]^H$;
  $\boldsymbol{F}_r = \boldsymbol{V}_r{}^{(1)}$;
  $C_{max,r} = \log_2 \det \left(\boldsymbol{I} + \boldsymbol{N}_{k,r}^{-1} \boldsymbol{G}_r \boldsymbol{F}_r \boldsymbol{F}_r{}^H \boldsymbol{G}_r{}^H \right)$;
end for
$\boldsymbol{M} = \boldsymbol{H}$;
loop
  while $r = T : 1$ **do**
    for $n = 1 : r$ **do**
      $\boldsymbol{G} = (\boldsymbol{M}^H \boldsymbol{M} + \alpha \boldsymbol{I})^{-1} \boldsymbol{M}^H$
      $\boldsymbol{G}_n = [\bar{\boldsymbol{Q}}_r{}^{(0)} \quad \bar{\boldsymbol{Q}}_r{}^{(1)}] \bar{\boldsymbol{R}}_n$
      $\boldsymbol{M}_n \bar{\boldsymbol{Q}}_r{}^{(0)} \boldsymbol{T}_r = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n{}^H$
      $\boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n{}^{(0)} \boldsymbol{T}_r \tilde{\boldsymbol{V}}_n{}^{(1)}$
    end for
    for $j = 1 : r$ **do**
      $C_j = \log_2 \det \left(\boldsymbol{I} + \boldsymbol{N}_{k,j}^{-1} \boldsymbol{M}_j \boldsymbol{P}_j \boldsymbol{P}_j{}^H \boldsymbol{M}_j{}^H \right)$;
    end for
    $a_r = \min_j (C_{max,j} - C_j)$;
    $\boldsymbol{F}_r = \boldsymbol{P}_{a_r}$;
    $\boldsymbol{D}_r = \tilde{\boldsymbol{U}}_{a_r}{}^H$;
    $\boldsymbol{M} = [\boldsymbol{H}_1{}^T \cdots \boldsymbol{H}_{a_r-1}{}^T \boldsymbol{H}_{a_r+1}{}^T \cdots \boldsymbol{H}_M{}^T]^T$
  end while
end loop
$\boldsymbol{F} = (\boldsymbol{F}_1 \cdots \boldsymbol{F}_M)$;
$\boldsymbol{D} = \begin{pmatrix} \boldsymbol{D}_1 & & \\ & \ddots & \\ & & \boldsymbol{D}_M \end{pmatrix}$
$\boldsymbol{B} = \text{lower triangular} \left(\boldsymbol{DHF} \bullet \text{diag} \left([\boldsymbol{DHF}]_{rr}^{-1} \right) \right)$

ated with Algorithm 1, the precoding and receive filter matrices can be obtained.

Algorithm 2 S-GMI Precoding

1: **for** $n = 1 : r$ **do**
2: $\boldsymbol{G} = (\boldsymbol{M}^H \boldsymbol{M} + \alpha \boldsymbol{I})^{-1} \boldsymbol{M}^H$
3: $\boldsymbol{G}_n = [\bar{\boldsymbol{Q}}_n{}^{(0)} \quad \bar{\boldsymbol{Q}}_n{}^{(1)}] \bar{\boldsymbol{R}}_n$
4: $\boldsymbol{M}_n \bar{\boldsymbol{Q}}_n{}^{(0)} = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n{}^H$
5: $\boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n{}^{(0)} \tilde{\boldsymbol{V}}_n{}^{(1)}$
6: **end for**

LR-SO-THP+S-GMI Algorithm

The development in linear algebra contribute to the lattice reduction technique application in wireless networks. According to study in [40], a basis change may lead to improved performance as corroborated by lattice reduction techniques. More specifically, in wireless networks the more correlated the columns of the wireless channel $\boldsymbol{H}$, the more significant the improvements will be if lattice reduction technique is applied. In [62], lattice reduction technique is proved that it has the capability of achieving full diversity of a MIMO system. With complex lattice reduction algorithm (CLR) employed in [30], the LR transformed channel for the rth user is obtained as

$$\boldsymbol{H}_{\mathrm{red}_r}^H = \boldsymbol{H}_r^H \boldsymbol{L}_r \tag{3.19}$$

where $\boldsymbol{H}_{\mathrm{red}_r} \in \mathbb{C}^{N_r \times N_t}$ is the transposed reduced channel matrix. The quantity $\boldsymbol{L}_r \in \mathbb{C}^{N_r \times N_r}$ is the transform matrix generated by the CLR algorithm. Note that the transmit power constraint is satisfied since $\boldsymbol{L}_r$ is a unimodular matrix.

Compared to the conventional SO-THP algorithm, the lattice reduced channel matrix $\boldsymbol{H}_{\mathrm{red}_n}$ is employed in the conventional S-GMI algorithm. The details of the LR aided S-GMI Procedure are given in Algorithm 3. Cooperated with Algorithm 1, we can complete the calculation of precoding and receive filter matrices.

Algorithm 3 Lattice-Reduction aided S-GMI Procedure

1: **for** $n = 1 : r$ **do**
2: $\boldsymbol{G} = (\boldsymbol{H}^H \boldsymbol{H} + \alpha \boldsymbol{I})^{-1} \boldsymbol{H}^H$
3: $[\boldsymbol{H}_{\mathrm{red}_n}{}^H \quad \bar{\boldsymbol{Q}}_n^{(0)}] = \mathrm{CLLL}(\boldsymbol{G}_{\mathrm{n}}^{\mathrm{H}})$
4: $\boldsymbol{M}_n = \boldsymbol{H}_{black_n}$
5: $\boldsymbol{M}_n \bar{\boldsymbol{Q}}_n{}^{(0)} = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n{}^H$
6: $\boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n{}^{(0)} \tilde{\boldsymbol{V}}_n{}^{(1)}$
7: **end for**

3.5 Analysis of the Algorithms

In this section, we conduct an analysis of the secrecy rate of the proposed precoding algorithms with a comparison in terms of computational complexity.

Computational Complexity Analysis

Table 3.1: Computational complexity of the proposed SO-THP+GMI algorithm

Steps	Operations	Flops	Case $(2,2,2)\times 6$
1	$\boldsymbol{G}_r = \boldsymbol{U}_r\boldsymbol{\Sigma}_r[\boldsymbol{V}_r{}^{(1)}\boldsymbol{V}_r{}^{(0)}]^H$;	$32R(N_tN_r^2$ $+N_r^3)$	3072
2	$\bar{\boldsymbol{G}} =$ $\boldsymbol{G} = (\boldsymbol{H}^H\boldsymbol{H} + \alpha\boldsymbol{I})^{-1}\boldsymbol{H}^H$	$(2N_t^3 - 2N_t^2$ $+N_t + 16N_RN_t^2)$	3822
3	$\bar{\boldsymbol{G}}_n = \bar{\boldsymbol{Q}}_n\bar{\boldsymbol{R}}_n$	$\sum_{r=1}^{R} 16r(N_t^2N_r$ $+N_tN_r^2 + \frac{1}{3}N_r^3)$	9472
4	$\boldsymbol{H}_{eff,n} = \boldsymbol{H}_n\bar{\boldsymbol{Q}}_n\boldsymbol{T}_n$	$\sum_{r=1}^{R} 16rN_RN_t^2$	20736
5	$\boldsymbol{H}_{eff,n} = \boldsymbol{U}_n^{(4)}\boldsymbol{\Sigma}_n^{(4)}\boldsymbol{V}_n{}^{(4)H}$	$\sum_{r=1}^{R} 64r(\frac{9}{8}N_r^3+$ $N_tN_r^2 + \frac{1}{2}N_t^2N_r)$	26496
6	$\boldsymbol{B}$ = lower triangular $\left(\boldsymbol{DHF} \bullet \text{diag}\left([\boldsymbol{DHF}]_{rr}^{-1}\right)\right)$	$16N_RN_t^2$	3456
			total 67054

According to [30], it can be calculated that the cost of the QR in FLOPs is 22.4% lower than BD. The results shown in Table 3.1 indicate that the complexity is reduced about 22.4% by the proposed SO-THP+GMI compared with the conventional SO-THP calculated in the same way. Among all investigated algorithms, SO-THP+S-GMI achieves a complexity reduction about 34.4% less than that of the conventional SO-THP algorithm and becomes the lowest computational complexity non-linear precoding technique.

Figure 3.3 shows the required FLOPS of the proposed and existing precoding algorithms. Linear precoding gives lower computational complexity but the BER performance is worse than non-linear ones. The three proposed algorithms show an advantage over the conventional SO-THP algorithm in terms of complexity. Among all the three proposed algorithms,

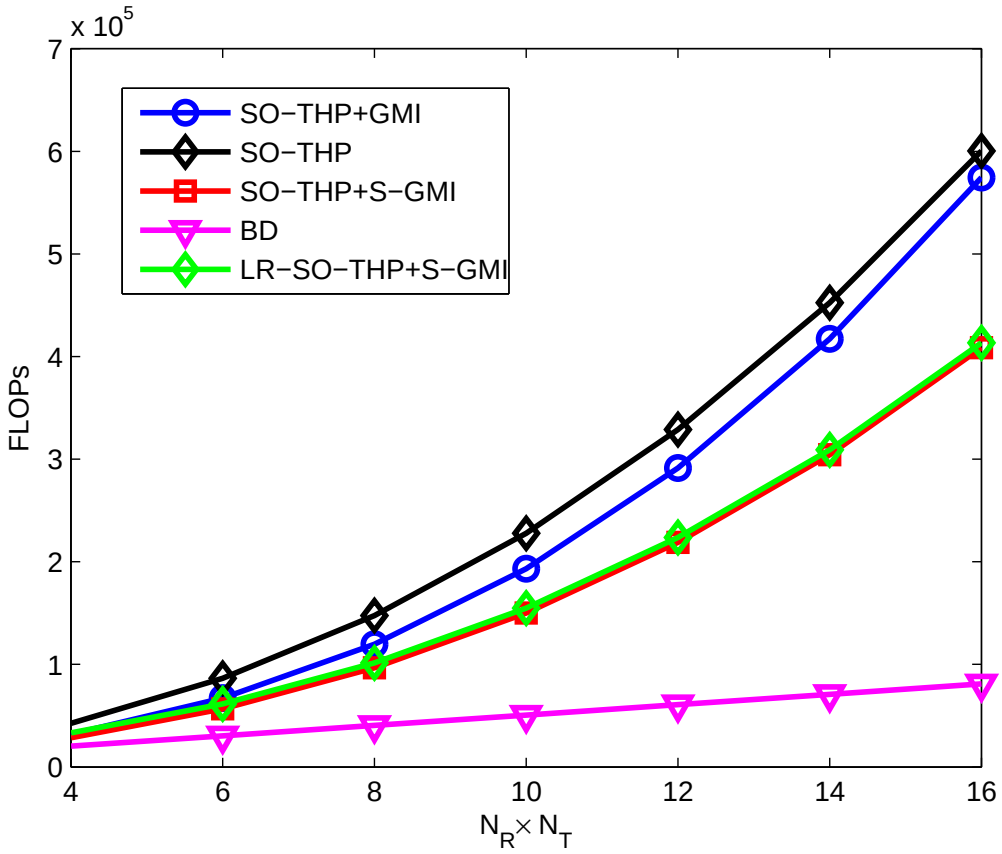

Figure 3.3: Computational complexity in FLOPs for MU-MIMO systems

SO-THP+S-GMI has the lowest complexity followed by LR-SO-THP+S-GMI algorithm. SO-THP+GMI requires the highest complexity. In Figure 3.3, SO-THP+S-GMI algorithm has similar performance as LR-SO-THP+S-GMI algorithm. Although the lattice reduction procedure is implemented in the LR-SO-THP+S-GMI, the matrices produced in the lattice reduction can be also used in the S-GMI algorithm. The complexity of the LR-SO-THP+S-GMI algorithm is slightly higher than SO-THP+S-GMI.

Secrecy rate Analysis

Proposition 1. *In full-rank MU-MIMO systems with perfect knowledge of CSI, the proposed algorithms are capable of achieving a high secrecy rate and in the high-SNR regime (i.e., $P \to \infty$) the secrecy rate will converge to $C_{\text{sec}}^{P\to\infty}$ which is given as (3.20),*

$$C_{\text{sec}}^{P\to\infty} = \log\left(\det\left((\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^{H})^{-1}(\boldsymbol{H}_{ba}\boldsymbol{H}_{ba}^{H})\right)\right) \tag{3.20}$$

$$C_s = \max_{\boldsymbol{R}_s \succeq 0, \mathrm{Tr}(\boldsymbol{R}_s)=P} \log\left(\det\left((\boldsymbol{I} + \boldsymbol{H}_{ea}\boldsymbol{R}_s\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H)\right)\right) \tag{3.24}$$

$$C_s = \max_{\boldsymbol{R}_s \succeq 0, \mathrm{Tr}(\boldsymbol{R}_s)=P} \log\left(\det\left(\Gamma_{ba}(\boldsymbol{P})\Phi_1(\boldsymbol{P}, \boldsymbol{R}_s)^{-1}\Phi_2(\boldsymbol{P}, \boldsymbol{R}_s)\right)\right) \tag{3.25}$$

$$\Phi_1(\boldsymbol{P}, \boldsymbol{R}_s) = (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{I} + \boldsymbol{H}_{ea}\boldsymbol{R}_s\boldsymbol{H}_{ea}^H) \tag{3.26}$$

$$\Phi_2(\boldsymbol{P}, \boldsymbol{R}_s) = (\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H) \tag{3.27}$$

Under the conditions

$$\boldsymbol{H}_{ba}^H\boldsymbol{H}_{ba} \succeq \boldsymbol{H}_{ea}^H\boldsymbol{H}_{ea} \tag{3.21}$$

$$\mathrm{rank}(\boldsymbol{H}_{\mathrm{ba}}) = \mathrm{rank}(\boldsymbol{H}_{\mathrm{ea}}) \tag{3.22}$$

and based on (2.29) we can have the secrecy capacity expressed as (3.24). If we assume

$$\Gamma(\boldsymbol{P}) = (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H) \tag{3.23}$$

the equation (3.24) can be converted to (3.25) with (3.23) .

In (3.25), (3.26) and (3.27), $\boldsymbol{P}$ is the precoding matrix derived from the legitimate users' channel. With $\boldsymbol{R}_s = E[\boldsymbol{x}_s\boldsymbol{x}_s^H] = E[\boldsymbol{P}\boldsymbol{s}\boldsymbol{s}^H\boldsymbol{P}^H]$, $E[\boldsymbol{s}\boldsymbol{s}^H] = \boldsymbol{R}_P$ and $\boldsymbol{P}\boldsymbol{P}^H = \boldsymbol{I}$, we can have,

$$E[(\boldsymbol{P}\boldsymbol{P}^H)^{-1}\boldsymbol{R}_s] = \boldsymbol{R}_P \tag{3.28}$$

Then

$$E[(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}\boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H] = \boldsymbol{R}_P \tag{3.29}$$

$$E[(\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}\boldsymbol{H}_{ea}\boldsymbol{R}_s\boldsymbol{H}_{ea}^H] = \boldsymbol{R}_P \tag{3.30}$$

In (3.25), the expectation value is given as (3.31). Substituting (3.29) into (3.31) the formula can be expressed as (3.33).

According to (3.33), in the high-SNR regime and when SNR $\to \infty$, $P \to \infty$, $SA \to \boldsymbol{I}$. Then, the secrecy rate expressed in (3.25) will result in (3.34). To satisfy the power constrain, we always have $E[\boldsymbol{P}\boldsymbol{P}^H] = \boldsymbol{I}$, then the secrecy rate C_{sec} will converge to a constant, that is,

$$C_{\mathrm{sec}}^{P\to\infty} = \log\left(\det(\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ba}\boldsymbol{H}_{ba}^H)\right) \tag{3.35}$$

This completes the derivation.

$$\begin{aligned} SA &= E\Big[\Phi_1(\boldsymbol{P},\boldsymbol{R}_s)^{-1}\Phi_2(\boldsymbol{P},\boldsymbol{R}_s)\Big] \\ &= E\Bigg[\Phi_3(\boldsymbol{P},\boldsymbol{R}_s)^{-1}\Big((\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1} + (\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}\boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H)\Big)\Bigg] \end{aligned} \tag{3.31}$$

$$\Phi_3(\boldsymbol{P},\boldsymbol{R}_s) = (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1} + (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}\boldsymbol{H}_{ea}\boldsymbol{R}_s\boldsymbol{H}_{ea}^H \tag{3.32}$$

$$\begin{aligned} SA &= E\Bigg[\Big((\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1} + \boldsymbol{R}_P\Big)^{-1}\Big((\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1} + \boldsymbol{R}_P\Big)\Bigg] \\ &= E\Bigg[\boldsymbol{I} + \Big((\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1} + \boldsymbol{R}_P\Big)^{-1}\Big((\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1} - (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}\Big)\Bigg] \end{aligned} \tag{3.33}$$

$$C_{\text{sec}}^{P\to\infty} = \log\left(\det\Big((\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)\Big)\right) \tag{3.34}$$

In the following, the percentage of the injected artificial noise power is set to 40% of the total transmit power. The percentage of the artificial noise power as compared to signal transmit power is determined to achieve an optimal result in terms of secrecy rate. The details of the derivation are expressed in the Appendix A. When AN is added during the transmission, equation (2.29) can be transformed to:

$$\begin{aligned} &\log\Big(\det(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H)\Big) \\ &-\log\left(\det\Big(\boldsymbol{I} + (\boldsymbol{I} + \boldsymbol{H}_{ea}\boldsymbol{R}_s'\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ea}\boldsymbol{R}_s\boldsymbol{H}_{ea}^H)\Big)\right) \end{aligned} \tag{3.36}$$

To assess the influence of different channel gain ratios between legitimate users and the eavesdroppers, we fix the legitimate users' channel gain and change the eavesdroppers'. The above equation (3.36) can be further transformed to

$$\begin{aligned} &\log(\det(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H)) \\ &-\log(\det(\boldsymbol{I} + ((\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H)^{-1} + \boldsymbol{R}_s')^{-1}\boldsymbol{R}_s) \end{aligned} \tag{3.37}$$

In the high-SNR regime, $P \to \infty$, according to (3.28), $\text{Tr}(R_s), \text{Tr}(R_s') \to \infty$, the term $(\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H)^{-1}$ then can be omitted and the result is the following expression

$$\log(\det(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{R}_s\boldsymbol{H}_{ba}^H)) - \log(\det(\boldsymbol{I} + (\boldsymbol{R}_s')^{-1}\boldsymbol{R}_s), \tag{3.38}$$

Considering artificial noise, $(\boldsymbol{R}_s')^{-1}\boldsymbol{R}_s = \rho/(1-\rho)\boldsymbol{I}$. When ρ is fixed, then $\log(\det(\boldsymbol{I} + (\boldsymbol{R}_s')^{-1}\boldsymbol{R}_s))$ would be a constant. From (3.38), the secrecy rate will increase even when the eavesdroppers have better statistical channel knowledge than the legitimate users. The secrecy rate can be positive in the scenario that the eavesdroppers have better statistical channel knowledge. With more power allocated to the artificial noise $1-\rho \to 1$, less power will be available for the users $\rho \to 0$, which will lead to a fast decrease of the capacity to the intended users which is expressed as $\log(\det(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H))$. As a result, the secrecy rate will finally fall to zero. By changing the variable ρ from 0.1 to 0.9, the secrecy rate will rise, achieve its maximum value and then gradually decline.

3.6 Simulation Results

A system with $N_t^{\text{total}} = 4$ transmit antennas and $T = 2$ users as well as $K = 1, 2$ eavesdroppers is considered. Each user or eavesdropper is equipped with $N_r = 2$ and $N_k = 2$ receive antennas. $m = \frac{\sigma_{ea}^2}{\sigma_{ba}^2}$ represents the gain ratio between the main and the wire-tap channel. In the simulations, the channels are generated according to fast fading channel model.

Perfect Channel State Information

In Figure 3.4 the proposed LR-SO-THP+S-GMI algorithm has the best uncoded BER performance. From the figure, we can see that when the lattice reduction technique is employed, the BER performance of the MU-MIMO system will improve. Here are the BER performances of the intended users and we use them to show the differences in BER when different precoding algorithms are applied. Although this is not directly relevant to PLS, the results indicate the algorithms which can be used to achieve a more reliable transmission. In Figure 3.7, in the scenario where $T > K$ the secrecy rate of the proposed algorithms have around 5 bits/Hz higher rate than the other precoding techniques. When $T = K$, Figure 3.5 shows that the proposed algorithms achieve a higher secrecy rate than the other techniques at low SNRs. Moreover, the secrecy rate will converge to a constant which will depend on the gain ratio between the main and the wire-tap channels m.

Imperfect Channel State Information

In the simulations, the channel errors are modeled as a complex random Gaussian noise matrix $\boldsymbol{E}$ following the distribution $\mathcal{CN}(0, \sigma_e^2)$. Then, the imperfect channel matrix $\boldsymbol{H}^e$ is

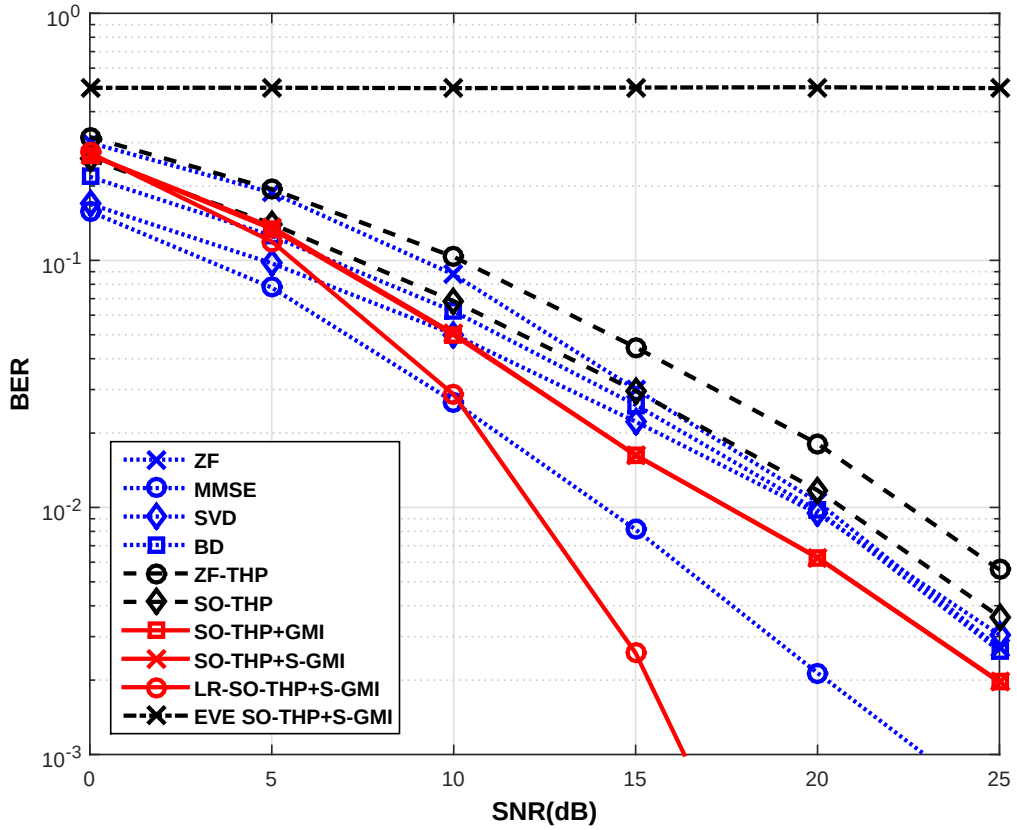

Figure 3.4: BER performance with precoding techniques in $4 \times 4 \times 2$ MU-MIMO broadcast channel, $m = 0.5$

defined as

$$\boldsymbol{H}^e = \boldsymbol{H} + \boldsymbol{E} \tag{3.39}$$

We assume the channels of the legitimate users are perfect and the transmitter has inaccurate CSI to the eavesdroppers.

In Figure 3.6, the secrecy rate performance is evaluated in the imperfect CSI scenario. Compared with the secrecy rate performance in Figure 3.5, the secrecy rate will suffer a huge decrease in the imperfect CSI scenario. When $T = K$, Figure 3.5 shows that the secrecy rate at low SNR is degraded and the secrecy rate requires very high SNR to converge to a constant. It is worth noting that the proposed SO-THP+S-GMI has the best secrecy rate performance amongst the studied precoding techniques.

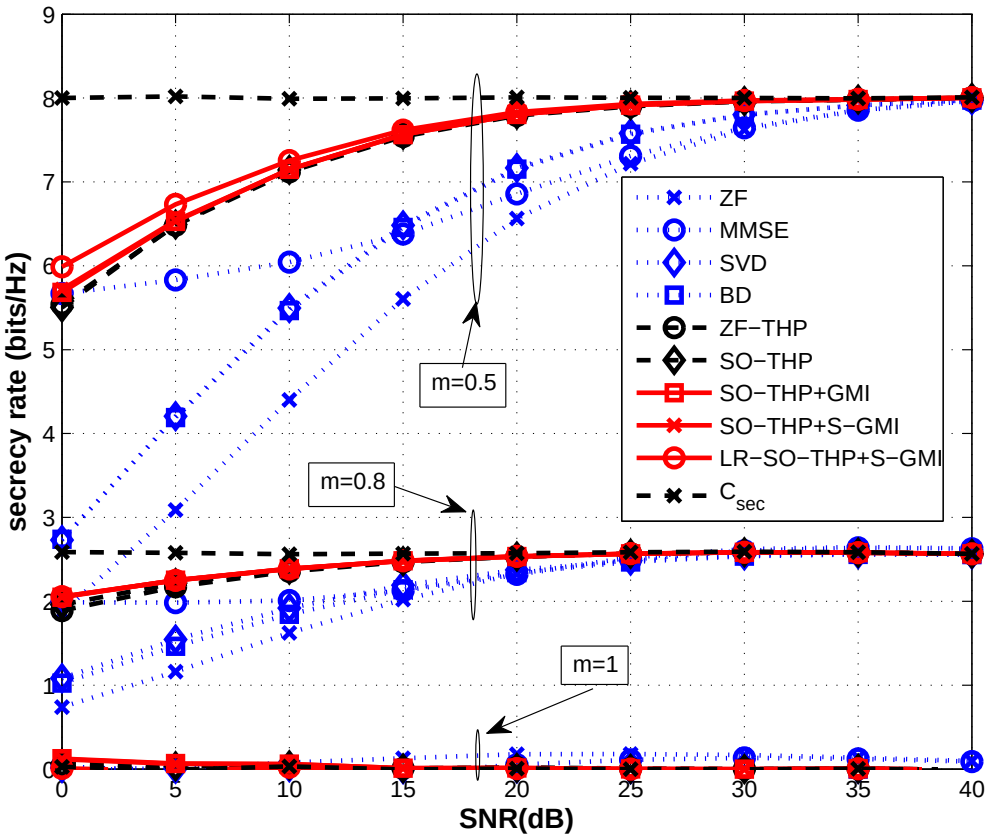

Figure 3.5: Secrecy rate performance with precoding techniques in $4 \times 4 \times 4$ MU-MIMO broadcast channel

Imperfect Channel State Information With Artificial Noise

In Figure 3.7 AN is added and the total transmit power E_s is the same as before. Comparing the results in Figure 3.5 and Figure 3.7, it is clear that by injecting artificial noise, the secrecy rate achieved can be much higher than that without artificial noise in the high SNR scenario. In Figure 3.7, we consider the secrecy rate performance with the channel gain ratio $m = 2$. According to the secrecy performance of Figure 3.8, 40% of the transmit power E_s is used to generate AN. In Figure 3.8, the secrecy rate is plotted against the ratio of the transmit signal power to the artificial noise, where the channel gain ratio is $m = 1$. Comparing the theoretical and the simulation results, the optimal values match ($\rho = 0.6$). .

3.7 Summary

Precoding techniques are widely used in the downlink of MU-MIMO wireless networks to

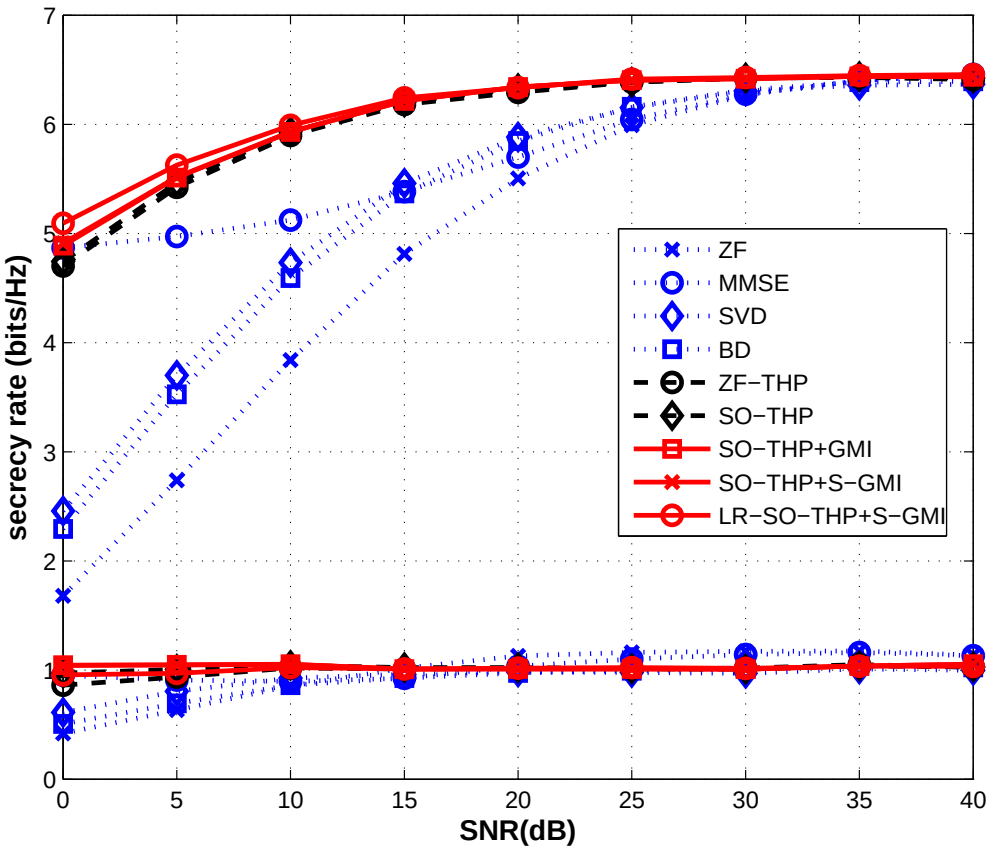

Figure 3.6: Secrecy rate with precoding techniques $4 \times 4 \times 4$ MU-MIMO broadcast channel with imperfect CSI

achieve good BER performance. The three proposed algorithms can all achieve higher secrecy rate performance than conventional techniques. Firstly if we consider the complexity as the most important metric, among all the studied non-linear precoding techniques, the proposed SO-THP+S-GMI algorithm requires the lowest computational complexity which results in a significant improvement on the efficiency. The BER and the secrecy rate performances of the SO-THP+S-GMI algorithm are also superior to the existing linear and non-linear algorithms considered. Secondly, if transmission reliability comes first in the design, the LR-SO-THP+S-GMI algorithm is also superior to the existing linear and non-linear algorithms considered.

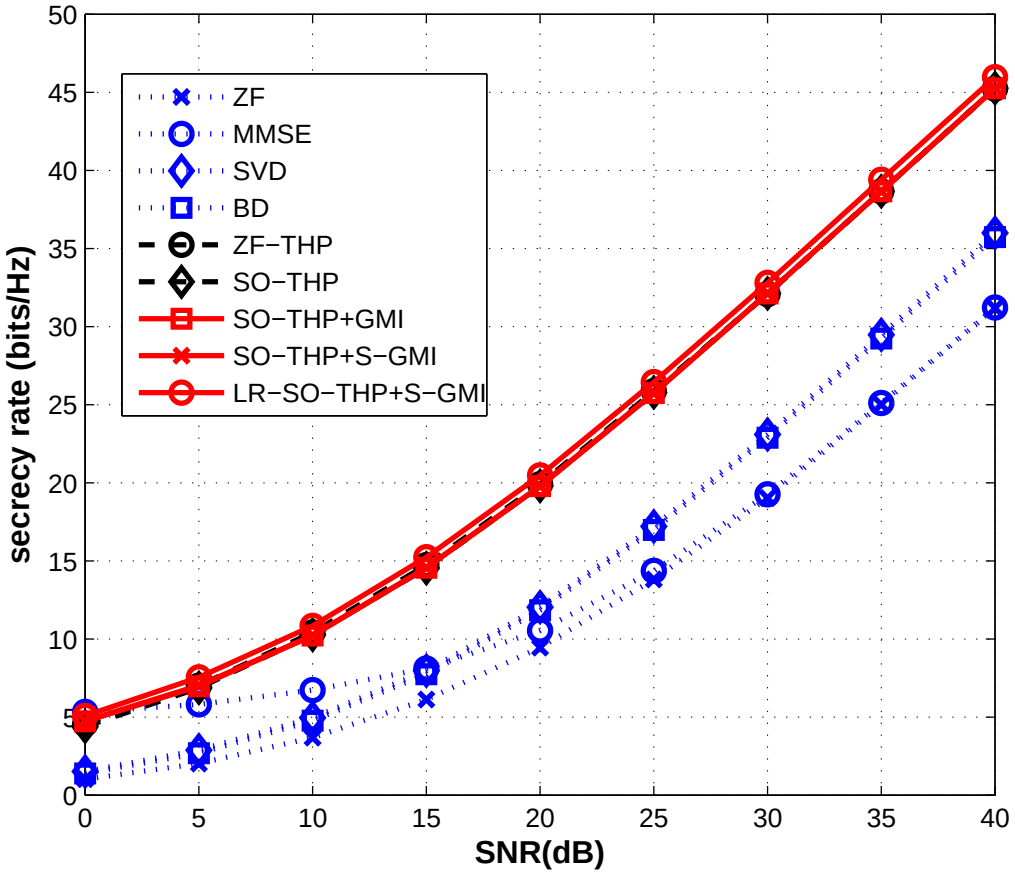

Figure 3.7: Secrecy rate with precoding techniques $4 \times 4 \times 2$ MU-MIMO broadcast channel with imperfect CSI, AN and $m = 2$

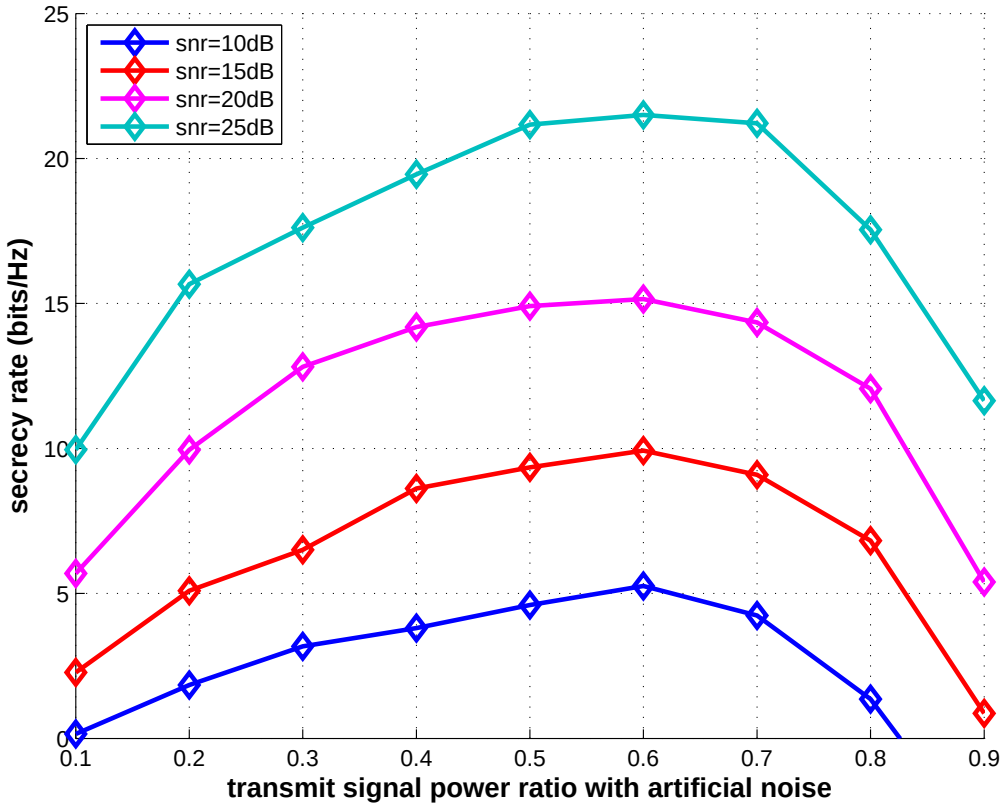

Figure 3.8: Secrecy rate change with different artificial noise power ratio

Chapter 4

Effective Relay Selection Algorithms for Physical-Layer Security in Multiple-Antenna Relay Networks

Contents

4.1 Introduction

Relay selection scheme as an important role in relay systems is investigated in various scenarios such as multiuser relay networks [67], cooperative relay systems [11] and cognitive relay networks [68]. In [69], relay selection methods are considered with the impact of co-channel interference. The performance in terms of secrecy rate can be significantly affected by the relay selection criterion adopted [70]. Existing relay selection algorithms depend on the knowledge of the channels between the source to the relays and the relays to the users [47]. Taking the channels from the source to the eavesdroppers into account, a relay selec-

tion approach denoted max-ratio criterion has been proposed in [12] based on knowledge of the channels to both legitimate users and eavesdroppers. In prior work, the assumption of knowledge of the channels to the eavesdroppers has been adopted even though it is impractical. Studies have considered the max-ratio relay selection policy, which employs the signal-to-interference-plus-noise ratio (SINR) as the relay selection criterion and requires the knowledge of the interference between users and the channels to the eavesdroppers.

In this chapter, we examine the secrecy rate performance of multiple-relay selection algorithms based on the SINR and the SR criteria, which require the knowledge of the interference and the channels to the eavesdroppers in single-antenna as well as multiuser MIMO relay networks. Novel effective relay selection algorithms based on the SINR and SR criteria that do not require knowledge of the channels of the eavesdroppers and interference are developed by exploiting linear algebra properties and a simplification of the expressions. The secrecy rate performance of the proposed algorithms is shown to approach that of techniques with full knowledge of the interference and the channels to the eavesdroppers.

4.2 System Model

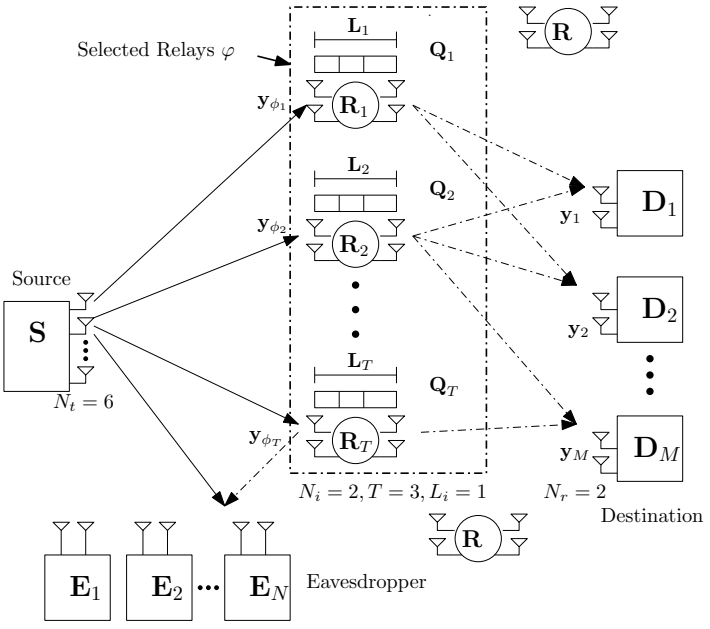

Figure 4.1: Multiuser MIMO network with eavesdroppers.

A description of the downlink multiuser MIMO relay network considered in this chapter is shown in Fig. 4.1, where the system employs two time slots to transmit the data from the source node to the users. Each relay and each user are equipped with N_i and N_r antennas, re-

spectively. We consider a source node, which transmits $\boldsymbol{s} = [\boldsymbol{s}_1^T \quad \boldsymbol{s}_2^T \quad \cdots \quad \boldsymbol{s}_M^T]^T \in \mathbb{C}^{MN_r \times 1}$ to relays. To broadcast the signal to M users, the total number of transmit antennas should be limited according to $N_t^{\text{total}} \geqslant MN_r$. For convenience, we assume that the number of the active antennas used for transmitting user signals is N_t and $N_t = MN_r$. At the same time, in order to receive the signals with a set of T relays, $T \times N_i = N_t$ antennas at relays are employed. In the second time slot, the relays will forward the signals to M users. During the transmission from the source to the users, there are N eavesdroppers, which attempt to decode the signals. Each eavesdropper is equipped with N_e antennas.

In this system, we assume that the eavesdroppers do not jam the transmission and the data transmitted to each user, relay, jammer and eavesdropper experience a flat-fading MIMO channel. The source node has full knowledge of the channels from the source to the relays as well as from the relays to the users. The quantities $\boldsymbol{H}_{\phi_i} \in \mathbb{C}^{N_i \times N_t}$ and $\boldsymbol{H}_{e_k} \in \mathbb{C}^{N_e \times N_t}$ denote the channel matrices of the ith relay and the kth eavesdropper, respectively. If we assume $\boldsymbol{\Psi}$ contains sets of T-combinations of the total relay set $\boldsymbol{\Omega}$ then the task of relay selection is to choose the set of relays that satisfies a chosen criterion. Given the set of selected relays expressed as $\boldsymbol{\varphi} = [\phi_1 \quad \phi_2 \quad \cdots \quad \phi_T] \in \boldsymbol{\Psi}$, the channel from the transmitter to the relays and the eavesdroppers can be obtained as $\boldsymbol{H}_i = [\boldsymbol{H}_{\phi_1}^T \quad \boldsymbol{H}_{\phi_2}^T \quad \cdots \quad \boldsymbol{H}_{\phi_T}^T]^T \in \mathbb{C}^{TN_i \times N_t}$ and $\boldsymbol{H}_e = [\boldsymbol{H}_{e_1}^T \quad \boldsymbol{H}_{e_2}^T \quad \cdots \quad \boldsymbol{H}_{e_K}^T]^T \in \mathbb{C}^{KN_e \times N_t}$. The matrix $\boldsymbol{H}_{\phi_i r} \in \mathbb{C}^{N_r \times N_i}$ represents the channel between the ith relay and the rth user. The channels from the selected relays to the rth user can be described by

$$\boldsymbol{H}_r = [\boldsymbol{H}_{\phi_1 r} \quad \boldsymbol{H}_{\phi_2 r} \quad \cdots \quad \boldsymbol{H}_{\phi_T r}], \tag{4.1}$$

where $\boldsymbol{H}_r \in \mathbb{C}^{N_r \times TN_i}$ and ϕ_i represents the ith selected relay with a chosen relay selection criterion. In the following section we will further discuss various relay selection criteria, where T is the total number of selected relays.

In Phase I, the signal is transmitted from the source to the relays. If a precoder matrix $\boldsymbol{U} = [\boldsymbol{U}_1 \quad \boldsymbol{U}_2 \quad \cdots \quad \boldsymbol{U}_M] \in \mathbb{C}^{N_t \times MN_r}$ is applied, when the relay is selected, the received signal in all relays can be expressed as

$$\boldsymbol{y}_i = \boldsymbol{H}_i \boldsymbol{U} \boldsymbol{s} + \boldsymbol{n}_i, \tag{4.2}$$

where $\boldsymbol{n}_i = [\boldsymbol{n}_{\phi_1} \quad \boldsymbol{n}_{\phi_2} \quad \cdots \quad \boldsymbol{n}_{\phi_T}] \in \mathbb{C}^{TN_i \times 1}$ is the noise vector that is assumed to be Gaussian. If the interference for relay i is described by $\boldsymbol{H}_{\phi_i} \sum_{j \neq i, j=1}^{T} \boldsymbol{U}_j \boldsymbol{s}_j$, then the received

signal is given by

$$\boldsymbol{y}_{\phi_i} = \boldsymbol{H}_{\phi_i}\boldsymbol{U}_i\boldsymbol{s}_i + \boldsymbol{H}_{\phi_i}\sum_{j\neq i, j=1}^{T}\boldsymbol{U}_j\boldsymbol{s}_j + \boldsymbol{n}_{\phi_i}. \tag{4.3}$$

In Phase II, the signal is transmitted from the relays to the users. The signal at the relay nodes is given by $\boldsymbol{y}_i = [\boldsymbol{y}_{\phi_1}^T \quad \boldsymbol{y}_{\phi_2}^T \quad \cdots \quad \boldsymbol{y}_{\phi_T}^T]^T \in \mathbb{C}^{TN_i\times 1}$. When we use the amplify-and-forward technique, the received signal at user r is described by

$$\boldsymbol{y}_r = \boldsymbol{H}_r\boldsymbol{y}_i + \boldsymbol{n}_r. \tag{4.4}$$

In the presence of multiple relay nodes, relay selection is performed before transmission to the relays. In a half-duplex system, we use $\eta_1 = \max_{\boldsymbol{\varphi}_1}\{\cdot\}$ to represent a metric obtained with the channel information from the source to the relays and $\eta_2 = \max_{\boldsymbol{\varphi}_2}\{\cdot\}$ as another metric calculated with information from the relays to the users. $\boldsymbol{\varphi}_1$ and $\boldsymbol{\varphi}_2$ denote the set of relays used for transmitting or receiving signals, respectively. Then if $\eta_1 \geq \eta_2$ we receive using the set of relays $\boldsymbol{\varphi}_1$; otherwise we transmit using $\boldsymbol{\varphi}_2$.

A multiple-relay selection algorithm for this scenario is shown in Algorithm 4. More specifically, step 33 takes the channel gain as the selection criterion and it can be replaced with different selection criteria. Depending on the choice of relay selection a designer must alter steps 7, 22 and 33.

4.3 Relay Selection Criteria

In this section, we examine relay selection criteria for the system under consideration.

4.3.1 Max-ratio criterion

Conventional relay selection is based on the full channel information between the source to the relays and the relays to the users. A max-link relay selection is developed based on the max-min relay selection for decode-and-forward (DF) relay systems [71]. With the consideration of the eavesdropper, a max-ratio selection [12] in a single-antenna scenario is given by

$$\phi^{\text{max-ratio}} = \max_{\phi_i\in\boldsymbol{\varphi}}\left(\eta_1^{\text{max-ratio}}, \eta_2^{\text{max-ratio}}\right), \tag{4.5}$$

where

$$\eta_1^{\text{max-ratio}} = \frac{\max_{\phi_i\in\boldsymbol{\varphi}:Q(\phi_i)\neq L}\|h_{S,\phi_i}\|^2}{\|h_{se}\|^2} \tag{4.6}$$

Algorithm 4 Relay selection algorithm

$\boldsymbol{\Omega}^0 = \boldsymbol{\Omega}$
$\phi^{\text{total}} = \text{length}(\boldsymbol{\Omega})$
$Q = \text{zeros}(1 : \phi^{\text{total}})$
for $k = 1 : T$ **do**
  for $i = 1 : \phi^{\text{total}}$ **do**
    if $Q(i) = 0$ **then**
      $\theta_{\phi_i} = trace(\boldsymbol{H}_{\phi_i}\boldsymbol{H}_{\phi_i}^H)$
      $Q(i) = Q(i) + 1$
    else
      $\theta_{\phi_i} = 0$
    end if
  end for
  $\boldsymbol{\varphi}_k^{\text{select}} = \max_{\phi_i \in \boldsymbol{\Omega}^0}\{\theta_{\phi_i}\}$
  $\eta_k = \theta_{\boldsymbol{\varphi}_k^{\text{select}}}$
  $\boldsymbol{\Omega}^0 = [1 \quad 2 \quad \cdots \quad \phi_i - 1 \quad \phi_i + 1 \cdots \phi^{\text{total}}]$
end for
$\eta_1 = \sum_{k=1}^{T} \eta_k$
$\boldsymbol{\Omega}^1 = \boldsymbol{\Omega}$
for $r = 1 : M$ **do**
  for $i = 1 : \phi^{\text{total}}$ **do**
    if $Q(i) \neq 0$ **then**
      $\theta_{\phi_i} = trace(\boldsymbol{H}_{\phi_i r}\boldsymbol{H}_{\phi_i r}{}^H)$
      $Q(i) = Q(i) - 1$
    else
      $\theta_{\phi_i} = 0$
    end if
  end for
  $\boldsymbol{\varphi}_r^{\text{select}} = \max_{\phi_i \in \boldsymbol{\Omega}^1}\{\theta_{\phi_i}\}$
  $\eta_r = \theta_{\boldsymbol{\varphi}_r^{\text{select}}}$
  $\boldsymbol{\Omega}^1 = [1 \quad 2 \quad \cdots \quad \phi_i - 1 \quad \phi_i + 1 \cdots \phi^{\text{total}}]$
end for
$\eta_2 = \sum_{r=1}^{M} \eta_r$
$\boldsymbol{\varphi}^{\text{select}} = \max_{\boldsymbol{\varphi}} (\eta_1, \eta_2)$

and

$$\eta_2^{\max-\text{ratio}} = \max_{\phi_i \in \boldsymbol{\varphi}: Q(\phi_i) \neq 0} \frac{\|h_{\phi_i,D}\|^2}{\|h_{\phi_i e}\|^2}. \tag{4.7}$$

Furthermore, in the scenario with only statistical distribution of the CSI to the eavesdroppers, the channel parameters in (4.6) and (4.7) are replaced by statistical values.

4.3.2 SINR criterion

Based on the max-ratio criterion, when we consider a multiuser MIMO system, the interference from other users is taken into account in the relay selection criterion. According to (4.3), the SINR criterion can be expressed similarly as

$$\boldsymbol{\varphi}^{\text{SINR}} = \max_{\boldsymbol{\varphi}} \left(\eta_{\text{SINR}_1}, \eta_{\text{SINR}_2} \right), \tag{4.8}$$

where η_{SINR_1} is the average value of SINR over relay set $\boldsymbol{\varphi}$. The SINR of the selected relay node ϕ_i can be obtained by

$$\begin{aligned} \eta_{\varphi_{\phi_i}}^{\text{SINR}} &= \max_i \overline{\text{SINR}_{\text{i}}} \\ &= \max_i \frac{1}{N_i} \sum_{n=1}^{N_i} \text{SINR}_{\text{n}} \\ &= \max_i \frac{1}{N_i} \sum_{n=1}^{N_i} \frac{\boldsymbol{h}_{\phi_{\text{in}}}^{\text{H}} \boldsymbol{R}_{\text{d}} \boldsymbol{h}_{\phi_{\text{in}}}}{\boldsymbol{h}_{\phi_{\text{in}}}^{\text{H}} \boldsymbol{R}_{\text{In}} \boldsymbol{h}_{\phi_{\text{in}}}}. \end{aligned} \tag{4.9}$$

in (4.9), $\boldsymbol{h}_{\phi_{in}} \in \mathbb{C}^{N_t \times 1}$ represents the nth stream for the ith relay. $\boldsymbol{R}_d = \boldsymbol{U}_i \boldsymbol{s}_i \boldsymbol{s}_i^H \boldsymbol{U}_i^H \in \mathbb{C}^{N_t \times N_t}$ is the correlation matrix of the received signal for node i and $\boldsymbol{R}_{\text{In}} = \sum_{j \neq i, j=1}^{m} \boldsymbol{U}_j \boldsymbol{s}_j \boldsymbol{s}_j^H \boldsymbol{U}_j^H + \boldsymbol{n}_j \boldsymbol{n}_j^H \in \mathbb{C}^{N_t \times N_t}$ represents the sum of the correlation matrix of the interference and correlation matrix of the noise. Similarly, η_{SINR_2} is the average value of SINR with relay set $\boldsymbol{\varphi}$ to users. The SINR of user r can then be calculated by

$$\eta_{\boldsymbol{\varphi},r}^{\text{SINR}} = \max_r \frac{1}{N_r} \sum_{n=1}^{N_r} \frac{\boldsymbol{h}_{\phi_{\text{in}}\text{r}}^{\text{H}} \boldsymbol{R}_{\text{r}} \boldsymbol{h}_{\phi_{\text{in}}\text{r}}}{\boldsymbol{h}_{\phi_{\text{in}}\text{r}}^{\text{H}} \boldsymbol{R}_{\text{In}} \boldsymbol{h}_{\phi_{\text{inr}}}}, \tag{4.10}$$

where $\boldsymbol{R}_r = \boldsymbol{y}_i \boldsymbol{y}_i^H \in \mathbb{C}^{TN_i \times TN_i}$ and $\boldsymbol{h}_{\phi_{in}r} \in \mathbb{C}^{TN_i \times 1}$ is the nth stream for user r.

4.3.3 Secrecy rate criterion

In a multi-user MIMO system, the secrecy-rate criterion considering interferences [72] is given by

$$\boldsymbol{\varphi} = \max_{\phi_i \in \boldsymbol{\varphi}, \boldsymbol{\varphi} \in \boldsymbol{\Psi}} \left\{ \log[\det(\boldsymbol{I} + \boldsymbol{\Gamma}_{r,i})] - \log[\det(\boldsymbol{I} + \boldsymbol{\Gamma}_{e,i})] \right\}, \tag{4.11}$$

where $\boldsymbol{\Gamma}_{r,i}$ is given as

$$\boldsymbol{\Gamma}_{r,i} = (\boldsymbol{H}_i \boldsymbol{R}_{\text{In}} \boldsymbol{H}_i^H)^{-1} (\boldsymbol{H}_i \boldsymbol{R}_d \boldsymbol{H}_i^H), \tag{4.12}$$

and

$$\boldsymbol{\Gamma}_{e,i} = (\boldsymbol{H}_e \boldsymbol{R}_{\text{In}} \boldsymbol{H}_e^H)^{-1} (\boldsymbol{H}_e \boldsymbol{R}_r \boldsymbol{H}_e^H), \tag{4.13}$$

In (4.11), the criterion is based on the SR related to destination i and the destination can be relays as well as users.

4.4 Proposed relay selection algorithms

In prior work, the channels of the source to eavesdroppers as well as the interference are assumed to be available at the transmitter. However, this assumption is impractical in wireless transmissions [73]. To obviate this need, we propose effective relay selection algorithms with partial channel information.

4.4.1 Simplified SINR-Based Relay Selection (S-SINR)

In the following, we choose the SINR criterion and develop a simplified SINR-based (S-SINR) relay selection algorithm with consideration of only the channels of the users, which can be readily obtained via feedback channels. If at the transmitter, a linear precoder $\boldsymbol{U}$ is applied, the received signal can be expressed as

$$\boldsymbol{h}_{\phi_{\text{in}}}^H \boldsymbol{R}_d \boldsymbol{h}_{\phi_{\text{in}}} = \boldsymbol{h}_{\phi_{\text{in}}}^H \boldsymbol{U}_i \boldsymbol{s}_i \boldsymbol{s}_i^H \boldsymbol{U}_i^H \boldsymbol{h}_{\phi_{\text{in}}}. \tag{4.14}$$

With linear zero-forcing precoding, we have $\boldsymbol{h}_{\phi_{\text{in}}}^H \boldsymbol{U}_i = [1 \quad 0 \quad \cdots \quad 0]$ and (4.14) can be written as

$$\boldsymbol{h}_{\phi_{\text{in}}}^H \boldsymbol{R}_d \boldsymbol{h}_{\phi_{\text{in}}} = \sigma_d^2, \tag{4.15}$$

where $\boldsymbol{R}_d$ holds for independent and identically distributed entries of $\boldsymbol{s}$ with σ_d^2 being the variance of the transmit signal. Based on (4.9) and (4.15), the proposed S-SINR algorithm

solves

$$\eta_{\varphi_{\phi_i}}^{\mathrm{SINR}} = \max_i \frac{1}{N_i} \sum_{n=1}^{N_i} \frac{\sigma_{\mathrm{d}}^2}{\boldsymbol{h}_{\phi_{\mathrm{in}}}^{\mathrm{H}} \boldsymbol{R}_{\mathrm{In}} \boldsymbol{h}_{\phi_{\mathrm{in}}}}. \tag{4.16}$$

According to (4.16), the maximization performed over N_i data steams is costly and requires the CSI to the relays and the correlation matrix of the interference. Moreover, the SINR for each receive antenna is calculated with the obtained information. In order to simplify the maximization we assume that the streams for a device or relay have similar SINR. With this assumption we can have

$$\eta_{\varphi_{\phi_i}}^{\mathrm{SINR}} = \min_i \boldsymbol{h}_{\phi_{\mathrm{in}}}^H \boldsymbol{R}_{\mathrm{In}} \boldsymbol{h}_{\phi_{\mathrm{in}}}, \tag{4.17}$$

We assume $\boldsymbol{R}_{\mathrm{In}} = \boldsymbol{D}_{\mathrm{In}} + \boldsymbol{G}$, $\boldsymbol{D}_{\mathrm{In}}$ is a diagonal matrix with the diagonal elements of $\boldsymbol{R}_{\mathrm{In}}$ and $\boldsymbol{G}$ containing the other elements of $\boldsymbol{R}_{\mathrm{In}}$. With $\boldsymbol{D}_{\mathrm{In}}$ and $\boldsymbol{G}$, we have

$$\begin{aligned} \boldsymbol{h}_{\phi_{\mathrm{in}}}^H \boldsymbol{R}_{\mathrm{In}} \boldsymbol{h}_{\phi_{\mathrm{in}}} &= \boldsymbol{h}_{\phi_{\mathrm{in}}}^H \boldsymbol{D}_{\mathrm{In}} \boldsymbol{h}_{\phi_{\mathrm{in}}} + \boldsymbol{h}_{\phi_{\mathrm{in}}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{\mathrm{in}}} \\ &= \sigma_{\mathrm{In}}^2 \|\boldsymbol{h}_{\phi_{\mathrm{in}}}\|^2 + \|\boldsymbol{h}_{\phi_{\mathrm{in}}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{\mathrm{in}}}\|, \end{aligned} \tag{4.18}$$

If we have two data streams and $\mathrm{SINR}_1 > \mathrm{SINR}_2$, based on (4.16), we get

$$\boldsymbol{h}_{\phi_{i1}}^H \boldsymbol{R}_{In} \boldsymbol{h}_{\phi_{i1}} < \boldsymbol{h}_{\phi_{i2}}^H \boldsymbol{R}_{In} \boldsymbol{h}_{\phi_{i2}}, \tag{4.19}$$

with (4.18), (4.19) can be expressed as

$$\sigma_{\mathrm{In}}^2 \|\boldsymbol{h}_{\phi_{i1}}\|^2 + \|\boldsymbol{h}_{\phi_{i1}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{i1}}\| < \sigma_{\mathrm{In}}^2 \|\boldsymbol{h}_{\phi_{i2}}\|^2 + \|\boldsymbol{h}_{\phi_{i2}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{i2}}\|, \tag{4.20}$$

rewrite (4.20), we can obtain

$$\|\boldsymbol{h}_{\phi_{i1}}\|^2 < \|\boldsymbol{h}_{\phi_{i2}}\|^2 + \frac{1}{\sigma_{\mathrm{In}}^2} (\|\boldsymbol{h}_{\phi_{i2}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{i2}}\| - \|\boldsymbol{h}_{\phi_{i1}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{i1}}\|), \tag{4.21}$$

If $\boldsymbol{G}$ is small compared with $\sigma_{\mathrm{In}}^2 \boldsymbol{I}$, we omit the term $(\|\boldsymbol{h}_{\phi_{i2}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{i2}}\| - \|\boldsymbol{h}_{\phi_{i1}}^H \boldsymbol{G} \boldsymbol{h}_{\phi_{i1}}\|)$. Finally if $\mathrm{SINR}_1 > \mathrm{SINR}_2$, we have

$$\|\boldsymbol{h}_{\phi_{i1}}\|^2 < \|\boldsymbol{h}_{\phi_{i2}}\|^2, \tag{4.22}$$

As a result, the SINR criterion can be simplified to the selection of the channel information as described by

$$\eta_{\varphi_{\phi_i}}^{\hat{\mathrm{SINR}}} = \min_{i,n} \|\boldsymbol{h}_{\phi_{in}}\|^2. \tag{4.23}$$

With the criterion expressed in (4.23), the interference can be omitted and only the channel information is necessary. Comparing (4.23) and (4.16), the optimization is performed by calculating channel gains for each antenna which is obviously easier than calculating SINRs for every antenna. Similarly, (4.10) can be obtained as

$$\eta_{\boldsymbol{\varphi},r}^{\hat{\mathrm{SINR}}} = \min_{r,n} \|\boldsymbol{h}_{\phi_{in}r}\|^2. \tag{4.24}$$

Based on (4.23) and (4.24), the SINR criterion in (4.8) can be simplified and the proposed S-SINR algorithm is given by

$$\boldsymbol{\varphi}^{\mathrm{S-SINR}} = \max_{\boldsymbol{\varphi}} \left(\eta_{\hat{\mathrm{SINR}}_1}, \eta_{\hat{\mathrm{SINR}}_2}\right), \tag{4.25}$$

which only needs the channel information. In (4.25), the calculation of $\eta_{\hat{\mathrm{SINR}}_1}$ and $\eta_{\hat{\mathrm{SINR}}_2}$ is in the same way as in (4.8). With the S-SINR criterion, the step 7, step 22 and step 33 in Algorithm 4 can be replaced by the step 5, step 20 and step 31 in Algorithm 5, respectively.

4.4.2 Simplified SR-Based (S-SR) Multiple-Relay Selection

In the proposed S-SR algorithm with partial channel information, the covariance matrix of the interference and the signal can be described as $\boldsymbol{R}_I = \boldsymbol{H}_i{}^{-1}\boldsymbol{H}_i{}^{H^{-1}} + \sum_{j\neq i}\boldsymbol{U}_j\boldsymbol{s}_j^{(t)}\boldsymbol{s}_j^{(t)^H}\boldsymbol{U}_j{}^H$ and $\boldsymbol{R}_d = \boldsymbol{U}_i\boldsymbol{s}_i^{(t)}\boldsymbol{s}_i^{(t)^H}\boldsymbol{U}_i{}^H$, respectively. If channel matrices are assumed perfectly known prior to transmission, we can further obtain an alternative way of expressing the SR criterion. The proposed SR-based relay selection algorithm is given by

$$\begin{aligned}\boldsymbol{\varphi}^{\mathrm{S-SR}} = \max_{\phi_i\in\boldsymbol{\varphi},\boldsymbol{\varphi}\in\boldsymbol{\Psi}} \Big\{ &\log\left(\det\left[\boldsymbol{I}+\boldsymbol{\Gamma}_{r,i}\right]\right) \\ &- \log\left(\det\left[\boldsymbol{I}+\boldsymbol{U}_i^H\boldsymbol{R}_I^{-1}\boldsymbol{U}_i\boldsymbol{R}_d\right]\right)\Big\},\end{aligned} \tag{4.26}$$

which can be achieved without knowledge of the channels of the eavesdroppers. In what follows, we detail the derivation of the S-SR relay selection algorithm.

From the original expression for the SR criterion, which is shown in (4.11), we propose the following approach:

$$\boldsymbol{\varphi} = \max_{\phi_i\in\boldsymbol{\varphi},\boldsymbol{\varphi}\in\boldsymbol{\Psi}} \left\{\frac{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_{r,i})}{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_{e,i})}\right\}, \tag{4.27}$$

In (4.27), our aim is to eliminate the channel information of eavesdroppers from the denom-

Algorithm 5 Relay selection algorithm with S-SINR criterion

$\boldsymbol{\Omega}^0 = \boldsymbol{\Omega}$
for $k = 1 : T$ **do**
  for $i = 1 : \phi^{\text{total}}$ **do**
    if $Q(i) = 0$ **then**
      $\theta_{\phi_i} = \sum_1^n \|\boldsymbol{h}_{\phi_{in}}\|^2$
      $Q(i) = Q(i) + 1$
    else
      $\theta_{\phi_i} = 0$
    end if
  end for
  $\boldsymbol{\varphi}_k^{\text{select}} = \min_{\phi_i \in \boldsymbol{\Omega}^0} \{\theta_{\phi_i}\}$
  $\eta_k = \theta_{\varphi_k^{\text{select}}}$
  $\boldsymbol{\Omega}^0 = [1 \quad 2 \quad \cdots \quad \phi_i - 1 \quad \phi_i + 1 \cdots \phi^{\text{total}}]$
end for
$\eta_{\hat{\text{SINR}}_1} = \frac{1}{T} \sum_{k=1}^T \eta_k$
$\boldsymbol{\Omega}^1 = \boldsymbol{\Omega}$
for $r = 1 : M$ **do**
  for $i = 1 : \phi^{\text{total}}$ **do**
    if $Q(i) \neq 0$ **then**
      $\theta_{\phi_i} = \sum_1^n \|\boldsymbol{h}_{\phi_{in}r}\|^2$
      $Q(i) = Q(i) - 1$
    else
      $\theta_{\phi_i} = 0$
    end if
  end for
  $\boldsymbol{\varphi}_r^{\text{select}} = \min_{\phi_i \in \boldsymbol{\Omega}^1} \{\theta_{\phi_i}\}$
  $\eta_r = \theta_{\varphi_r^{\text{select}}}$
  $\boldsymbol{\Omega}^1 = [1 \quad 2 \quad \cdots \quad \phi_i - 1 \quad \phi_i + 1 \cdots \phi^{\text{total}}]$
end for
$\eta_{\hat{\text{SINR}}_2} = \sum_{r=1}^M \eta_r$
$\boldsymbol{\varphi}^{\text{select}} = \max_{\boldsymbol{\varphi}} \left(\eta_{\hat{\text{SINR}}_1}, \eta_{\hat{\text{SINR}}_2}\right)$

inator. The denominator can be expressed as

$$\det[{\boldsymbol{\Lambda}_1}^{-1}\boldsymbol{\Lambda}_1 + {\boldsymbol{\Lambda}_1}^{-1}(\boldsymbol{H}_e\boldsymbol{R}_d\boldsymbol{H}_e^H)], \tag{4.28}$$

where $\boldsymbol{\Lambda}_1 = \boldsymbol{H}_e\boldsymbol{R}_I\boldsymbol{H}_e^H$. Since $\boldsymbol{\Lambda}_1$ is square and with square matrices we have $\det(\boldsymbol{A}B) = \det(\boldsymbol{A})\det(\boldsymbol{B})$, (4.28) results in

$$\det[{\boldsymbol{\Lambda}_1}^{-1}]\det[\boldsymbol{\Lambda}_1 + (\boldsymbol{H}_e\boldsymbol{R}_d\boldsymbol{H}_e^H)], \tag{4.29}$$

Using the property $\det(\boldsymbol{A}^{-1}) = \frac{1}{\det(\boldsymbol{A})}$ [74], we have

$$\det[\boldsymbol{\Lambda}_1]^{-1}\det[\boldsymbol{\Lambda}_1 + (\boldsymbol{H}_e\boldsymbol{R}_d\boldsymbol{H}_e^H)], \tag{4.30}$$

In (4.30), we separate the equation into two parts:

$$\begin{aligned}\det[\boldsymbol{\Lambda}_1]^{-1} &= \det[\boldsymbol{H}_e\boldsymbol{R}_I\boldsymbol{H}_e^H]^{-1} \\ &= \det[\boldsymbol{H}_e(\sum_{j\neq i}\boldsymbol{U}_j\boldsymbol{s}_j^{(t)}{\boldsymbol{s}_j^{(t)}}^H{\boldsymbol{U}_j}^H)\boldsymbol{H}_e^H]^{-1}.\end{aligned} \tag{4.31}$$

On the left-hand side of (4.31), we multiply $\boldsymbol{U}_i{\boldsymbol{U}_i}^{-1} = \boldsymbol{I}$ and on the right side we multiply ${\boldsymbol{U}_i^H}^{-1}{\boldsymbol{U}_i}^H = \boldsymbol{I}$, yielding

$$\begin{aligned}\det[\boldsymbol{\Lambda}_1]^{-1} = \{&\det[\boldsymbol{H}_e\boldsymbol{U}_i] \\ &\det[(\sum_{j\neq i}{\boldsymbol{U}_i}^{-1}\boldsymbol{U}_j\boldsymbol{s}_j^{(t)}{\boldsymbol{s}_j^{(t)}}^H{\boldsymbol{U}_j}^H{\boldsymbol{U}_i^H}^{-1})] \\ &\det[\boldsymbol{U}_i^H\boldsymbol{H}_e^H]\}^{-1},\end{aligned} \tag{4.32}$$

Similarly, the second part in equation (4.30) can be obtained as

$$\begin{aligned}&\det[\boldsymbol{\Lambda}_1 + (\boldsymbol{H}_e\boldsymbol{R}_d\boldsymbol{H}_e^H)] = \det[\boldsymbol{H}_e\boldsymbol{U}_i] \\ &\det[(\sum_{j\neq i}{\boldsymbol{U}_i}^{-1}\boldsymbol{U}_j\boldsymbol{s}_j^{(t)}{\boldsymbol{s}_j^{(t)}}^H{\boldsymbol{U}_j}^H{\boldsymbol{U}_i^H}^{-1}) + \boldsymbol{s}_i^{(t)}{\boldsymbol{s}_i^{(t)}}^H] \\ &\det[\boldsymbol{U}_i^H\boldsymbol{H}_e^H],\end{aligned} \tag{4.33}$$

As the matrices $\boldsymbol{H}_e\boldsymbol{U}_i$ and $\boldsymbol{U}_i^H\boldsymbol{H}_e^H$ are square and have equal size, based on (4.30), (4.32) and (4.33) we can eliminate the term $\det[\boldsymbol{H}_e\boldsymbol{U}_i]$ and $\det[\boldsymbol{U}_i^H\boldsymbol{H}_e^H]$. The secrecy rate selection

criterion (4.27) can then be rewritten as

$$\boldsymbol{\varphi} = \max_{\phi_i \in \boldsymbol{\varphi}, \boldsymbol{\varphi} \in \boldsymbol{\Psi}} \left\{ \frac{\det[\boldsymbol{I} + \boldsymbol{\Gamma}_{r,i}]}{\det[\boldsymbol{\Lambda}_2]} \right\}, \tag{4.34}$$

where $\boldsymbol{\Lambda}_2$ require only the information of precoding matrices and transmit symbols which is expressed as:

$$\begin{aligned} \boldsymbol{\Lambda}_2 = & (\sum_{j \neq i} \boldsymbol{U}_i{}^{-1} \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} \boldsymbol{s}_j^{(t)H} \boldsymbol{U}_j{}^H \boldsymbol{U}_i^{H^{-1}})^{-1} \\ & [(\sum_{j \neq i} \boldsymbol{U}_i{}^{-1} \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} \boldsymbol{s}_j^{(t)H} \boldsymbol{U}_j{}^H \boldsymbol{U}_i^{H^{-1}}) + \boldsymbol{s}_i^{(t)} \boldsymbol{s}_i^{(t)H}] \end{aligned} \tag{4.35}$$

with $\boldsymbol{R}_I$ and $\boldsymbol{R}_d$, we can have

$$\boldsymbol{\Lambda}_2 = \boldsymbol{I} + \boldsymbol{U}_i^H \boldsymbol{R}_I^{-1} \boldsymbol{U}_i \boldsymbol{R}_d, \tag{4.36}$$

By adding log to (4.36), we obtain

$$\boldsymbol{\varphi}^{\mathrm{S-SR}} = \max_{\phi_i \in \boldsymbol{\varphi}, \boldsymbol{\varphi} \in \boldsymbol{\Psi}} \left\{ \log \left(\frac{\det[\boldsymbol{I} + \boldsymbol{\Gamma}_{r,i}]}{\det[\boldsymbol{I} + \boldsymbol{U}_i^H \boldsymbol{R}_I^{-1} \boldsymbol{U}_i \boldsymbol{R}_d]} \right) \right\}, \tag{4.37}$$

which is equivalent to (5.40). In the derivation, we assume the channel matrices of the users have the same size as the channel of the eavesdroppers and the matrices are full rank.

Based on the proposed S-SR criterion, the relay selection in the buffer-aided relay system can be implemented according to Algorithm 6. The substitution of steps 7, 22 and 33 are given as steps 7, 24 and 35 in Algorithm 6 which require only the channel and signal information to the corresponding relays and users.

As a conclusion, in Table 4.1, the required information to do the relay selection are listed. Among all investigated relay selection approaches, S-SR can achieve high secrecy rate performance without the channel information to the eavesdroppers in a relay system.

4.5 Simulation Results

In this section, we assess the secrecy rate performance in a multiuser MIMO downlink relay system via simulations. Zero-forcing precoding is adopted and we assume that the channel for each user is uncorrelated with the remaining channels and the channel gains are generated following a complex circular Gaussian random variable with zero mean and unit variance.

Algorithm 6 Relay selection algorithm with S-SR criterion

$\boldsymbol{\Omega}^0 = \boldsymbol{\Omega}$
for $k = 1 : T$ **do**
  for $i = 1 : \phi^{\text{total}}$ **do**
    if $Q(i) = 0$ **then**
      $\boldsymbol{R}_I = \boldsymbol{H}_i{}^{-1}\boldsymbol{H}_i{}^{H-1} + \sum_{j\neq i}^{M} \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} \boldsymbol{s}_j^{(t)H} \boldsymbol{U}_j{}^H$
      $\boldsymbol{R}_d = \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} \boldsymbol{s}_i^{(t)H} \boldsymbol{U}_i{}^H$
      $\theta_{\phi_i} = \log\left(\frac{\det[\boldsymbol{I}+\boldsymbol{\Gamma}_{r,i}]}{\det[\boldsymbol{I}+\boldsymbol{U}_i^H \boldsymbol{R}_I^{-1} \boldsymbol{U}_i \boldsymbol{R}_d]}\right)$
      $Q(i) = Q(i) + 1$
    else
      $\theta_{\phi_i} = 0$
    end if
  end for
  $\boldsymbol{\varphi}_k^{\text{select}} = \max_{\phi_i \in \boldsymbol{\Omega}^0}\{\theta_{\phi_i}\}$
  $\eta_k = \theta_{\boldsymbol{\varphi}_k^{\text{select}}}$
  $\boldsymbol{\Omega}^0 = [1 \quad 2 \quad \cdots \quad \phi_i - 1 \quad \phi_i + 1 \cdots \phi^{\text{total}}]$
end for
$\eta_{\text{S}-\hat{\text{SR}}_1} = \sum_{k=1}^{T} \eta_k$
$\boldsymbol{\Omega}^1 = \boldsymbol{\Omega}$
for $r = 1 : M$ **do**
  for $i = 1 : \phi^{\text{total}}$ **do**
    if $Q(i) \neq 0$ **then**
      $\boldsymbol{R}_I = \boldsymbol{H}_{\phi_i r}{}^{-1}\boldsymbol{H}_{\phi_i r}{}^{H-1} \sum_{j\neq i}^{M} \boldsymbol{y}_{\phi_j} \boldsymbol{y}_{\phi_j}{}^H$
      $\boldsymbol{R}_d = \boldsymbol{y}_{\phi_i} \boldsymbol{y}_{\phi_i}{}^H$
      $\theta_{\phi_i} = \log\left(\frac{\det[\boldsymbol{I}+(\boldsymbol{H}_{\phi_i r} \boldsymbol{R}_I \boldsymbol{H}_{\phi_i r}^H)^{-1}(\boldsymbol{H}_{\phi_i r} \boldsymbol{R}_d \boldsymbol{H}_{\phi_i r}^H)]}{\det[\boldsymbol{I}+\boldsymbol{R}_I^{-1}\boldsymbol{R}_d]}\right)$
      $Q(i) = Q(i) - 1$
    else
      $\theta_{\phi_i} = 0$
    end if
  end for
  $\boldsymbol{\varphi}_r^{\text{select}} = \max_{\phi_i \in \boldsymbol{\Omega}^1}\{\theta_{\phi_i}\}$
  $\eta_r = \theta_{\boldsymbol{\varphi}_r^{\text{select}}}$
  $\boldsymbol{\Omega}^1 = [1 \quad 2 \quad \cdots \quad \phi_i - 1 \quad \phi_i + 1 \cdots \phi^{\text{total}}]$
end for
$\eta_{\text{S}-\hat{\text{SR}}_2} = \sum_{r=1}^{M} \eta_r$
$\boldsymbol{\varphi}^{\text{select}} = \max_{\boldsymbol{\varphi}}(\eta_{\text{S}-\hat{\text{SR}}_1}, \eta_{\text{S}-\hat{\text{SR}}_2})$

Table 4.1: Comparison of different relay selection algorithms

Relay selection approach	Required information		Summary
Max-ratio (4.5)	User or relay channel information	Eavesdropper channel information	Low complexity, low secrecy rate performance
SINR (4.8)	All channel information	Covariance matrix of transmit signal and interference	High complexity, hard to achieve in reality
Secrecy rate (4.11)	All channel information	Covariance matrix of transmit signal and interference	Best secrecy rate performance requiring most information
Simplified SINR (S-SINR) (4.25)	User or relay channel information		Low complexity and high secrecy rate performance
Simplified secrecy-based (S-SR) (4.26)	User or relay channel information	covariance matrix of transmit signal and interference	Close to the best secrecy rate performance with partial channel information

The details of the simulation parameters are given in Table 4.2.

Table 4.2: Simulation Parameters for Single-antenna and MIMO scenario

Parameter	Symbol	Single-antenna	MIMO
Number of transmit antennas	N_t	3	6
Number of antennas for each relay	N_i	1	2
Number of antennas for each user	N_r	1	2
Number of antennas for each eavesdropper	N_e	1	2
Number of relays	T	5	5
Number of buffer size	L	1	1
Number of users	M	3	3
Number of eavesdroppers	N	3	3

In Fig. 5.8 single-antenna scenario, the SINR and SR criteria have a comparable SR performance. However, the SINR criterion requires the interference knowledge and the SR criterion needs the channels of the eavesdroppers, which are both impractical. The proposed S-SR algorithm only requires the channels to the relays and the legitimate users and can achieve almost the same SR performance as the SR criterion with full channel knowledge. The proposed

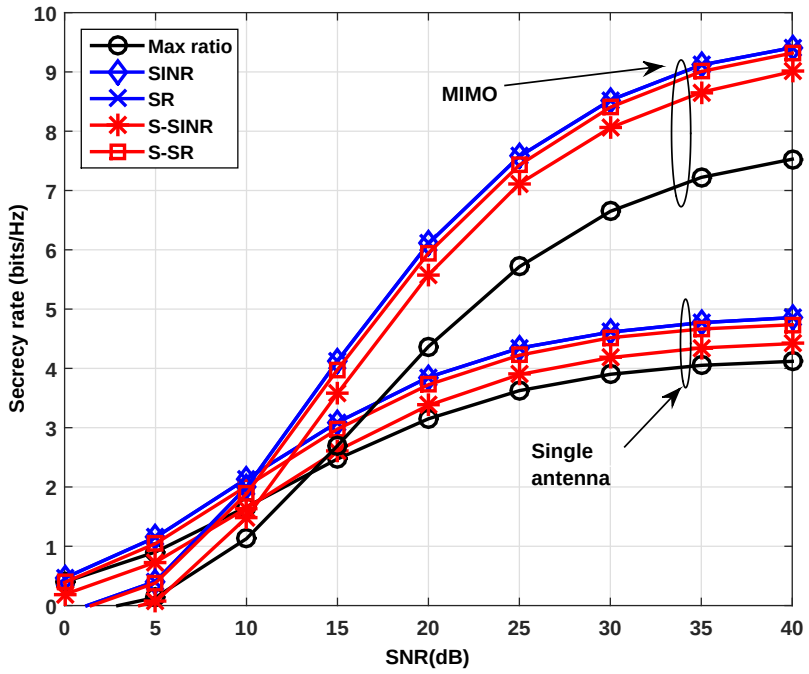

Figure 4.2: Single antenna ($N_t = 3, N_r = N_i = N_k = 1, T = 5, M = N = 3$) and MIMO ($N_t = 6, N_r = N_i = N_k = 2, T = 5, M = N = 3$) multi-user system secrecy rate performance with different relay selection criteria

S-SINR algorithm suffers a larger degradation than that of the SR criterion.

In Fig. 4.3, we compare the SR performance for scenarios with square and equal channel matrices and that with the zeros filled out. When we decrease the number of eavesdroppers, the SR performance improves. In this scenario, the proposed S-SR relay selection algorithm can still perform close to the SR relay selection criterion with full information.

Figure 4.4 shows the secrecy rate performance in the presence of different relay numbers for the single-antenna and the MIMO scenarios. Higher number of relays provide a better spatial advantage which contributes to the increase of the secrecy rate. According to Figure 4.4, in the scenario with full CSI knowledge, the SINR criterion and SR criterion can achieve the same secrecy rate performance. However, it also leads to a higher computational complexity.

Furthermore, in Figure 4.5, simplified criteria are compared along with different numbers of relays. The S-SR criterion provides the best SR performance among all investigated criteria. With more relays distributed between the source and users, the SR performance can be further improved by employing the proposed S-SR and S-SINR algorithms.

In the simulation, we assume perfect CSI is achievable in the criteria calculation. For a scenario with imperfect CSI, there is a performance degradation for all curves as expected

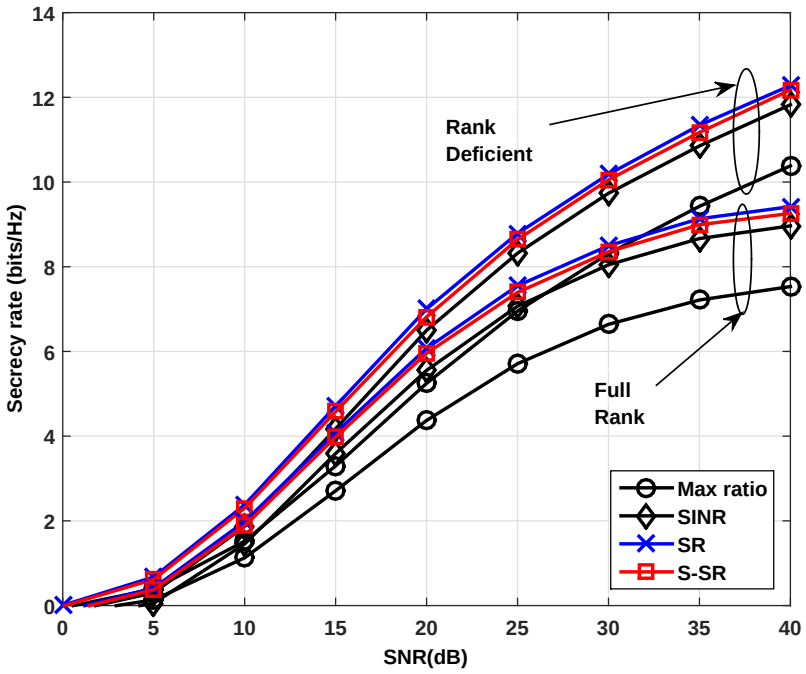

Figure 4.3: Secrecy rate performance with different relay selection criteria in full-rank ($N_t = 6, N_r = N_i = N_k = 2, T = 5, M = N = 3$) and rank-deficient ($N_t = 6, N_r = N_i = N_k = 2, T = 5, M = 3, N = 2$) systems

but the proposed algorithms still outperform the Max-ratio approach.

4.6 Summary

In this work, we have proposed effective multiple-relay selection algorithms for multiuser MIMO relay systems to enhance the legitimate users' transmission. The proposed algorithms exploit the use of the available channel information to perform relay selection. Simulation results show that the proposed algorithms can provide a significantly better secrecy rate performance than existing approaches.

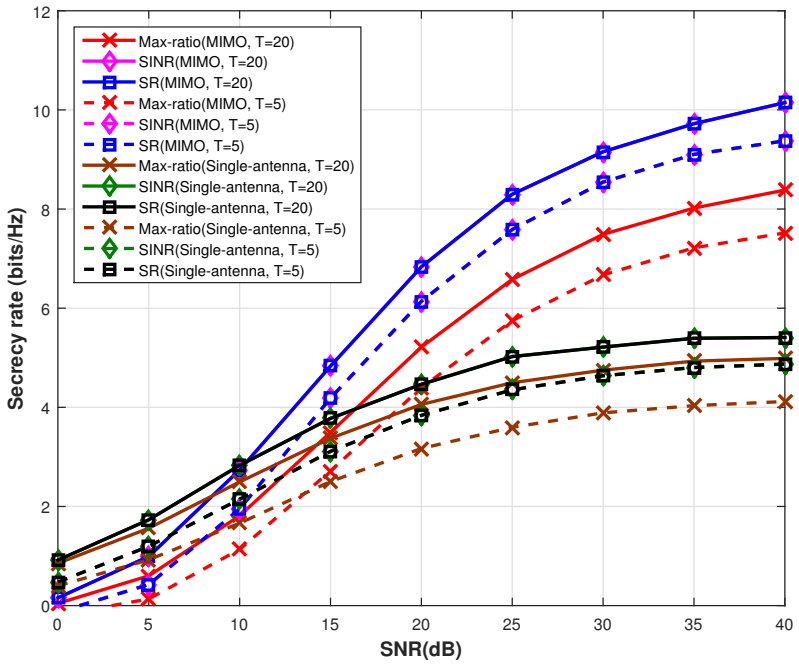

Figure 4.4: Effect of different numbers of relays $T = 5$ (dash line), $T = 20$ (solid line) on the secrecy rate performance with full CSI knowledge in single-antenna ($N_t = 3, N_r = N_i = N_k = 1, M = N = 3$) and MIMO ($N_t = 6, N_r = N_i = N_k = 2, M = N = 3$) scenarios.

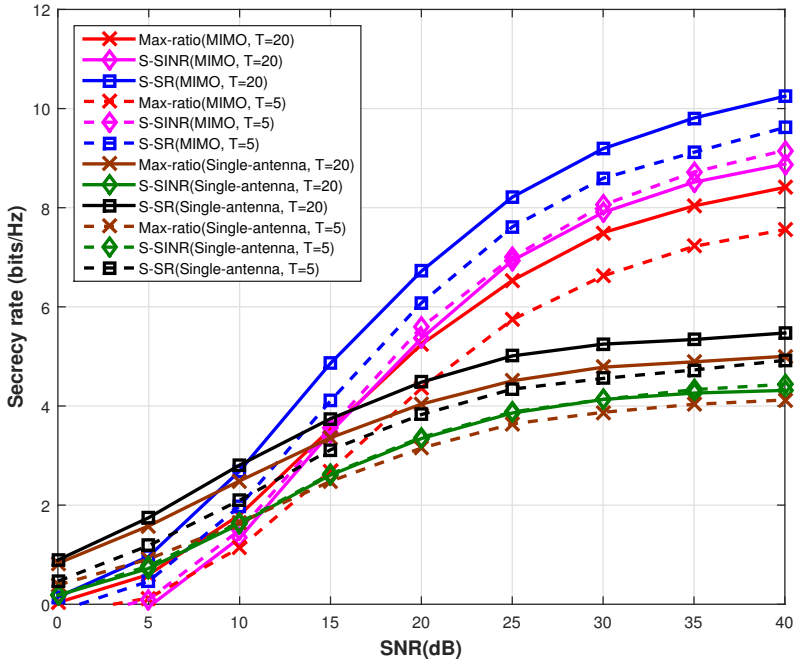

Figure 4.5: Effect of different numbers of relays $T = 5$ (dash line), $T = 20$ (solid line) on the secrecy rate performance with simplified CSI knowledge in single-antenna ($N_t = 3, N_r = N_i = N_k = 1, M = N = 3$) and MIMO ($N_t = 6, N_r = N_i = N_k = 2, M = N = 3$) scenarios.

Chapter 5

Opportunistic Relay and Jammer Scheme for Physical-Layer Security in Buffer-aided Relay Networks

Contents

5.1 Introduction

In this chapter, we investigate an opportunistic relaying and jamming scheme and develop relay selection algorithms for multiple-input multiple-output (MIMO) buffer-aided downlink relay networks with physical layer security constraints. The proposed relaying and jamming function selection (RJFS) algorithms select multiple relay nodes as well as multiple jamming nodes to assist the transmission. In the proposed RJFS algorithm inter-relay interference cancellation (IC) techniques are taken into account. Firstly, IC is implemented to improve the transmission rate to legitimate users. Secondly, the inter-relay interference (IRI) is applied to amplify the jamming signal to the eavesdroppers. In particular, we consider a buffer-aided system in which the jamming signal can be stored at the relay nodes and a buffer-aided relaying and jamming function selection (BF-RJFS) algorithm is proposed. In both RJFS and BF-RJFS algorithms, a relay selection strategy is developed to maximize the secrecy rate based on exhaustive searches. Greedy RJFS and BF-RJFS algorithms are then developed for relay selection with reduced complexity. Simulation results show that the proposed RJFS and BF-RJFS algorithms can achieve a higher secrecy rate performance than previously reported techniques even in the absence of channel state information of the eavesdroppers.

5.1.1 Prior and Related Work

Research on buffer-aided relay systems with secure constraints has been carried out in half-duplex and full-duplex systems. In [51], the system model is described as one source, one half-duplex decode-and-forward (DF) buffer relay and one destination. Regarding the availability of the channel state information at the transmitter (CSIT), fixed-rate transmission and mixed-rate transmission schemes are proposed in this study. Based on the instantaneous signal-to-noise ratio (SNR) of the source-relay and relay-destination links the approach in [51] gives a solution to the throughput-optimal problem. Then in [12], with one eavesdropper which can intercept data from both the source and relay nodes, secure transmission is investigated in a half-duplex buffer-aided cooperative wireless network. A max-ratio relay selection policy in a single-antenna system is developed to optimize the secrecy transmission rate with the consideration of exact and average gain eavesdropper channel strength scenarios. The studies in [75; 76] have investigated physical-layer security in MIMO systems. Furthermore, in [13] a two-hop half-duplex buffer-aided relay system is studied, where a relay selection which adapts reception and transmission time slots based on the channel quality is proposed and the selection thresholds are set to maximize the secrecy throughput or minimize the secrecy

outage probability (SOP). Half-duplex systems avoid the IRI occurred in the relay poll, however, the transmission rate is reduced by the use of two time slots. This can be further complicated by the need for two or more time slots for the transmission with buffers at relay nodes and the associated delay constraints. Compared with half-duplex systems, full-duplex systems can provide higher transmission rates [77]

Opportunistic relay schemes have recently been applied to buffer-aided systems [14], [15] and [78]. In this context, inter-relay interference cancellation (IC) at relay nodes is a fundamental aspect in opportunistic relay schemes. In [14], IC has been combined with buffer-aided relays and power adaptation to mitigate inter-relay interference (IRI) and minimize the energy expenditure. In a point-to-point system, a new relay selection policy is analyzed in terms of outage probability and diversity. Furthermore, in [15] a distributed joint relay-pair selection has been proposed with the aim of rate maximization in each time slot. Examining the feasibility of IC at the relay nodes, the study in [15] derives the threshold to avoid increased relay-pair switching and CSI acquisition. Based on relay selection techniques, in [78] and [79], a jammer selection algorithm and a joint relay and jammer selection technique have been investigated. The studies in [78] and [79] show that relaying contributes to a better transmission rate for legitimate users, whereas jamming can deteriorate the transmission to the eavesdropper. Therefore, relaying and jamming leads to an improvement in secrecy rate performance. However, there are few works which consider the combination of opportunistic buffer-aided relay schemes with jamming techniques for improving physical layer security.

5.1.2 Contributions

In this chapter, we investigate an opportunistic relaying and jamming scheme and develop relay selection algorithms for the downlink of multiuser multiple-input multiple-output (MIMO) buffer-aided relay networks with the constraints of physical layer security. We focus on the downlink channel and the secrecy rate performance of the proposed scheme and algorithms. Unlike the IC focus of [14], we examine an opportunistic relaying and jamming scheme along with relay selection algorithms. The proposed relaying and jamming function selection (RJFS) algorithms, whose preliminary results were reported in [80], select multiple relay nodes as well as multiple jamming nodes to assist the transmission. In particular, based on the opportunistic jamming selection performed with independent groups of jammers [78], we consider an opportunistic relaying and jamming scheme in which relaying or jamming is performed within the same set of relays at different time slots. The proposed opportunistic

relaying and jamming scheme is capable of achieving a high secrecy rate than recently reported approaches. In the proposed RJFS algorithm jamming is taken into account. Firstly, jamming is employed to improve the transmission rate to legitimate users. Secondly, The remaining interference is leveraged to amplify the jamming signal to the eavesdroppers. We also consider a buffer-aided system in which the jamming signal can be stored at the relay nodes and a buffer-aided relaying and jamming function selection (BF-RJFS) algorithm is proposed. In both RJFS and BF-RJFS algorithms, a relay selection strategy is developed to maximize the secrecy rate based on an exhaustive search. Greedy RJFS and BF-RJFS algorithms are then developed for relay selection with reduced complexity. Simulation results show that the proposed RJFS and BF-RJFS algorithms can outperform recently reported techniques in the absence of channel state information of the eavesdroppers. In addition, the proposed greedy RJFS and BF-RJFS algorithms achieve a close performance to the proposed exhaustive search-based RJFS and BF-RJFS algorithms, while requiring a much lower computational cost. The main contributions of the chapter are:

- An opportunistic relaying and jamming scheme for multiuser MIMO networks with buffer-aided relay nodes.
- Novel relaying and jamming function selection algorithms, denoted RJFS and BF-RJFS, are developed for multi-user MIMO systems with multiple relay nodes.
- A selection criterion is devised for the RJFS and BF-RJFS algorithms which does not require the CSI to the eavesdroppers.
- Greedy RJFS and BF-RJFS algorithms are developed to reduce the computational complexity of exhaustive search-based RJFS and BF-RJFS algorithms.
- Secrecy rate analysis of the proposed relaying and jamming selection algorithms.

5.2 System Model and Performance Metrics

In this section, a brief introduction to the buffer-aided relay system model is given along with details of the proposed opportunistic relaying and jamming scheme. In addition, the problem formulation of physical layer security associated with the proposed opportunistic relaying and jamming scheme is detailed.

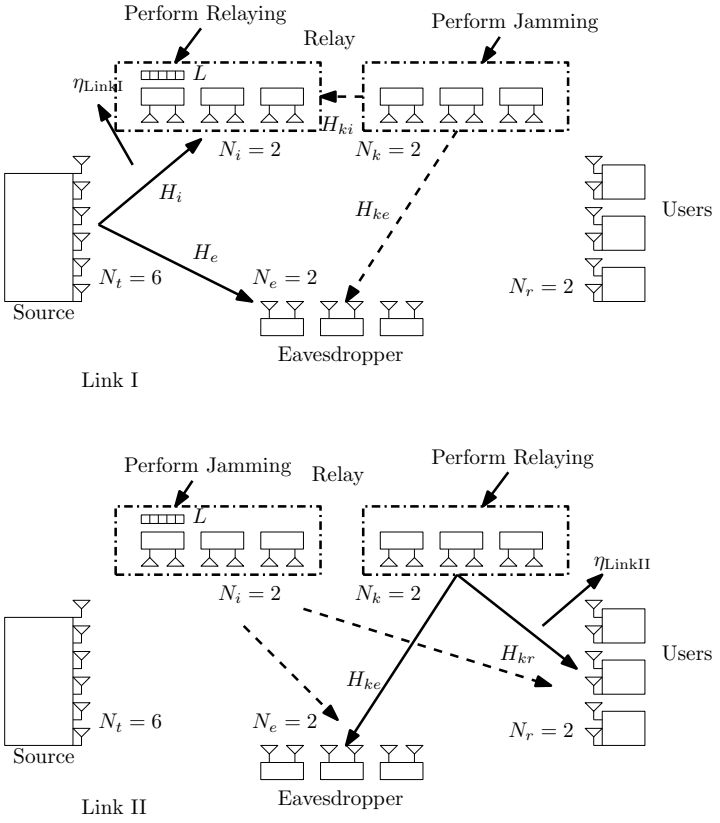

Figure 5.1: System model of a MU-MIMO system with M users, N eavesdroppers S_{total} relays

5.2.1 System Model

Figure 5.1 gives a description of an opportunistic multiuser MIMO relay system with N_t antennas employed to transmit the data streams to M users in the presence of N eavesdroppers. In the relay selection scheme, S represents the number of selected relay nodes. To show the states of the relays, the matrix $\boldsymbol{L}_{\text{state}} \in \mathbb{C}^{S_{\text{total}}N_i \times L}$ is introduced. Each column of the matrix $\boldsymbol{L}_{\text{state}}$ represents the signals stored in the buffers in one time slot. The initial elements in the buffer state matrix are zeros. Similar to traditional relay systems, the transmission can be divided into two parts, Link I and Link II, respectively. In Fig. 5.1, the solid lines represent the transmission of intended signals and dashed lines denote the transmission of jamming signals. The key difference of an opportunistic scheme is that at the same time slot the relays can be selected to perform different functions. Depending on the relay buffer size, the opportunistic scheme can be considered in two scenarios:

- **Buffer size** $L = 1$: In the first time slot, only Link I occurs. In the following transmission, Link I and Link II happens in the same time slot. This scenario is equivalent to that of relays without buffers.

- **Buffer size** $L > 1$: Thresholds η are calculated separately for Link I and Link II and relays performing relaying or jamming are determined.
  - If $\eta_{\text{LinkI}} > \eta_{\text{LinkII}}$, Link I occurs. It indicates that the channels from the source to the relays can provide a better transmission environment. In this scenario, the jamming signals are generated independently at the relays which are selected to perform jamming function. The selection of the relays which perform the relaying function can be done according to different relay selection criteria. And the selection of the relays which perform jamming can be achieved in the remaining relays based on the feasibility of IRI cancellation . The jamming signal will also be stored at the buffers.
  - If $\eta_{\text{LinkI}} \leq \eta_{\text{LinkII}}$, Link II transmissions occur. It indicates that the channels from the relays to the users can provide a better transmission environment. In this scenario, relays will forward the signals to the destination. The jamming signals in Link II are the stored jamming signals in Link I which means that the jamming signals in Link II do not need to be generated independently in Link II.

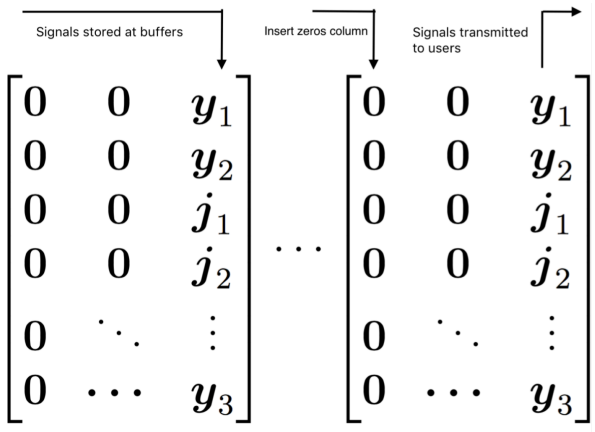

Figure 5.2: Relaying and Jamming function in buffer state matrix

In Fig. 5.2, we take a $S_{\text{total}}N_i \times L$ buffer state matrices as an example. The buffer state matrix are shown with relaying and jamming function relays. In Link I, the received signals as well as the jamming signal will be stored in the first zero column from the right side of the matrix. In Link II, the first non-zero column counting from the right side of the matrix will be transmitted to the user and at the same time an all-zero column will be added to the left of the matrix. The transmission follows a first in first out procedure.

Each relay node is equipped with N_i antennas. To indicate the difference when the relays are performing the jamming function, the number of relay antennas is represented by N_k. For

one relay we can have $N_k = N_i$. At the receiver side each user and eavesdropper is equipped with N_r and N_e receive antennas, respectively.

In this system, we assume that the eavesdroppers do not jam the transmission and the data transmitted to each user, relay, jammer and eavesdropper experience a flat-fading MIMO channel. The quantities $\boldsymbol{H}_i \in \mathbb{C}^{N_i \times N_t}$ and $\boldsymbol{H}_e \in \mathbb{C}^{N_e \times N_t}$ denote the channel matrices of the ith relay and the eth eavesdropper, respectively. The quantities $\boldsymbol{H}_{ke} \in \mathbb{C}^{N_e \times N_k}$ and $\boldsymbol{H}_{kr} \in \mathbb{C}^{N_r \times N_k}$ denote the channel matrices of the kth jammer to the eth eavesdropper and the kth jammer to the rth user, respectively. The channel between the kth relay to the ith relay is represented by $\boldsymbol{H}_{ki} \in \mathbb{C}^{N_i \times N_k}$. To support the transmission of data to M users, the source is equipped with $N_t \geqslant N_r M$ antennas. The number of antennas equipped with relaying function nodes as well as the jamming function nodes should satisfy $N_i S \geqslant N_r M$ and $N_k K \geqslant N_r M$, respectively. In order to satisfy the precoding constraints that the total number of transmit antennas should be larger than the total number of receive antennas, we assume that $N_r M$ transmit antennas are used to transmit signals to M users. We also assume that the total number of antennas of the eavesdroppers is $N_e N \geqslant N_r M$ [6; 81].

The vector $\boldsymbol{s}_i^{(t)} \in \mathbb{C}^{N_i \times 1}$ represents the data symbols to be transmitted corresponding to each user in time slot t. The total transmit signal at the transmitter can be expressed as:

$$\boldsymbol{s}^{(t)} = \begin{bmatrix} \boldsymbol{s}_1^{(t)^T} & \boldsymbol{s}_2^{(t)^T} & \boldsymbol{s}_3^{(t)^T} & \cdots & \boldsymbol{s}_M^{(t)^T} \end{bmatrix}^T. \tag{5.1}$$

In prior work [82; 83], precoding techniques have been applied to mitigate the interference between different users. In this work, we adopt for simplicity linear zero-forcing precoding and the precoding matrix can be described by

$$\boldsymbol{U}^{(t)} = \boldsymbol{H}^{(t)^H} (\boldsymbol{H}^{(t)} \boldsymbol{H}^{(t)^H})^{-1}. \tag{5.2}$$

With $\boldsymbol{U}_i \in \mathbb{C}^{N_t \times N_i}$, the total precoding matrix can be expressed as

$$\boldsymbol{U}^{(t)} = \begin{bmatrix} \boldsymbol{U}_1^{(t)} & \boldsymbol{U}_2^{(t)} & \boldsymbol{U}_3^{(t)} & \cdots & \boldsymbol{U}_M^{(t)} \end{bmatrix}, \tag{5.3}$$

and the total channel matrix to S selected relays is given by

$$\boldsymbol{H}^{(t)} = \begin{bmatrix} \boldsymbol{H}_1^{(t)^T} & \boldsymbol{H}_2^{(t)^T} & \boldsymbol{H}_3^{(t)^T} & \cdots & \boldsymbol{H}_S^{(t)^T} \end{bmatrix}^T \in \mathbb{C}^{S N_i \times N_t}, \tag{5.4}$$

if the number of antennas equipped at each relay and each user are the same, the minimum

required number of relays is $S = M$. The channels of the selected relays forwarding the signals to the rth user are described by

$$\boldsymbol{H}_{Kr}{}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{1r}^{(t)} & \boldsymbol{H}_{2r}^{(t)} & \boldsymbol{H}_{3r}^{(t)} & \cdots & \boldsymbol{H}_{Kr}^{(t)} \end{bmatrix} \in \mathbb{C}^{N_r \times KN_k} \tag{5.5}$$

and the total channel from relays to users is,

$$\boldsymbol{H}_{M}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{K1}^{(t)\,T} & \boldsymbol{H}_{K2}^{(t)\,T} & \boldsymbol{H}_{K3}^{(t)\,T} & \cdots & \boldsymbol{H}_{KM}^{(t)\,T} \end{bmatrix}^T \in \mathbb{C}^{MN_r \times KN_k}. \tag{5.6}$$

The selected relays also perform jamming for the Link I transmission to the eavesdroppers, whereas the channels of the jammers to the ith relay are given by

$$\boldsymbol{H}_{Ki}{}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{1i}^{(t)} & \boldsymbol{H}_{2i}^{(t)} & \boldsymbol{H}_{3i}^{(t)} & \cdots & \boldsymbol{H}_{Ki}^{(t)} \end{bmatrix} \in \mathbb{C}^{N_i \times KN_k}. \tag{5.7}$$

In each link, the received signal $\boldsymbol{y}_i^{(t)} \in \mathbb{C}^{N_i \times 1}$ at each relay node can be expressed as:

$$\boldsymbol{y}_i^{(t)} = \boldsymbol{H}_i \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} + \sum_{j \neq i} \boldsymbol{H}_i \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} + \boldsymbol{H}_{Ki}^{(t)} \boldsymbol{J} + \boldsymbol{n}_i \tag{5.8}$$

In (5.8), $\boldsymbol{n}_i \in \mathcal{CN}(0, \sigma)$ and the superscript pt designates the previous time slot when the signal is stored as a jamming signal in the buffer at the relay nodes. The symbol σ represents the noise variance at the relay. The term $\boldsymbol{H}_{Ki}\boldsymbol{y}^{(pt)}$ is regarded as the IRI between the ith relay and the K jammers. The total jamming signal $\boldsymbol{y}^{(pt)} = [\boldsymbol{y}_1^{(pt_1)^T} \quad \boldsymbol{y}_2^{(pt_2)^T} \quad \cdots \quad \boldsymbol{y}_K^{(pt_K)^T}]^T$ is chosen as the jamming signal according to a signal-to-interference and noise ratio (SINR) criterion, which is explained later on in this work. The superscript pt represents the previous time slot and due to the characteristics of buffer relay nodes, the values can be different for each relay node According to the theorem in [14], IRI can be eliminated. The jammers are targeted towards the eth eavesdropper channel described by

$$\boldsymbol{H}_{Ke}{}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{1e}^{(t)} & \boldsymbol{H}_{2e}^{(t)} & \boldsymbol{H}_{3e}^{(t)} & \cdots & \boldsymbol{H}_{Ke}^{(t)} \end{bmatrix} \in \mathbb{C}^{N_e \times KN_k} \tag{5.9}$$

The received signal at the eth eavesdropper is then given by

$$\boldsymbol{y}_e^{(t)} = \boldsymbol{H}_e \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} + \sum_{j \neq i} \boldsymbol{H}_e \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} + \boldsymbol{H}_{Ke}^{(t)} \boldsymbol{J} + \boldsymbol{n}_e. \tag{5.10}$$

where $\boldsymbol{n}_e \in \mathcal{CN}(0, \sigma)$ is the noise vector at the eavesdropper. For the eavesdropper, the term $\boldsymbol{H}_{Ke}^{(t)}\boldsymbol{y}^{(pt)}$ acts as the jamming signal and this jamming signal can not be removed without

the knowledge of the channel from the kth jammer to the eth eavesdropper.

If we assume that the transmitted signals from the relays to the users are expressed as $\boldsymbol{r}^{(t)}$ which is the last column in the buffer state matrix. The received signal at the destination is expressed by

$$\boldsymbol{y}_r^{(t)} = \boldsymbol{H}_M \boldsymbol{r}^{(t)} + \boldsymbol{n}_r. \tag{5.11}$$

where $\boldsymbol{n}_r \in \mathcal{CN}(0, \sigma)$ is the noise vector from the relays to users.

In the existing IRI scenario, based on (5.8), when the transmit signals $\boldsymbol{s}$ are independent with unit average energy $\mathbb{E}[\boldsymbol{s}\boldsymbol{s}^H] = \boldsymbol{I}$, the SINR at relay node i $\Gamma_{\mathrm{IRI-i}}^{(t)}$ can be expressed as:

$$\Gamma_{\mathrm{IRI-i}}^{(t)} = \frac{\gamma_{S_i,R_i}}{\varphi(k,i)\gamma_{R_K,R_i} + \gamma_{S_j,R_i} + N_i}, \tag{5.12}$$

where $\boldsymbol{\gamma}_{m,n}$ represents the instantaneous received signal power for the links $m \longrightarrow n$ as described by

$$\gamma_{S_i,R_i} = \|\boldsymbol{H}_i \boldsymbol{U_i}\|_{\mathrm{F}}, \quad \gamma_{S_j,R_i} = \|\sum_{j \neq i} \boldsymbol{H}_i \boldsymbol{U_j}\|_{\mathrm{F}}, \tag{5.13}$$

$$\gamma_{R_K,R_i} = \|\boldsymbol{H}_{Ki} \boldsymbol{J}\|_{\mathrm{F}}. \tag{5.14}$$

The SINR at the eth eavesdropper node $\Gamma_e^{(t)}$ as well as the rth legitimate user $\Gamma_r^{(t)}$ can be expressed as:

$$\Gamma_{\mathrm{IRI-e}}^{(t)} = \frac{\gamma_{S_i,E_e}}{\gamma_{R_K,E_e} + \gamma_{S_j,E_e} + N_e}, \tag{5.15}$$

and

$$\Gamma_{\mathrm{IRI-r}}^{(t)} = \frac{\gamma_{R_k,R_r}}{\gamma_{R_K,R_r} + N_r}, \tag{5.16}$$

where the terms in (5.15) and (5.16) are given by

$$\gamma_{S_i,E_e} = \|\boldsymbol{H}_e \boldsymbol{U_i}\|_{\mathrm{F}}, \quad \gamma_{S_j,E_e} = \|\sum_{j \neq i} \boldsymbol{H}_e \boldsymbol{U_j}\|_{\mathrm{F}}, \tag{5.17}$$

$$\gamma_{R_K,E_e} = \|\boldsymbol{H}_{Ke} \boldsymbol{J}\|_{\mathrm{F}} \tag{5.18}$$

and

$$\gamma_{R_k,R_r} = \|\boldsymbol{H}_{kr} \boldsymbol{J}_k\|_{\mathrm{F}}. \tag{5.19}$$

$$\gamma_{R_K,R_r} = \|\boldsymbol{H}_{Kr} \boldsymbol{J} - \boldsymbol{H}_{kr} \boldsymbol{J}_k\|_{\mathrm{F}}. \tag{5.20}$$

Depending on the IRI conditions at the relay nodes, two types of scheme can be applied: IRI or jamming. According to [14], if we assume $\mathbb{E}[\boldsymbol{s}\boldsymbol{s}^H] = \boldsymbol{I}$ and $\mathbb{E}[\boldsymbol{y}^{(pt)}{\boldsymbol{y}^{(pt)}}^H] = \boldsymbol{I}$, the

feasibility of jamming can be described by a factor $\varphi(K,i)$ which is expressed as:

$$\varphi(K,i)=\begin{cases}0 & \text{if } \det\left((\boldsymbol{H}_i\boldsymbol{H}_i^H+\boldsymbol{I})^{-1}\boldsymbol{H}_{Ki}\boldsymbol{H}_{Ki}^H\right)\geqslant\gamma_0\\ 1 & \text{otherwise,}\end{cases} \tag{5.21}$$

where $\varphi(K,i)=0$ means the interference can be amplified in the received signal at the relays. The quantity γ_0 is the threshold set to evaluate the feasibility of jamming.

In this scenario, jamming can be performed at the relay nodes by setting $\varphi(K,i)=0$. The SINR expressions at relay node i, eavesdropper e and receiver r can be respectively expressed as:

$$\Gamma_{\mathrm{IC-i}}^{(t)}=\frac{\gamma_{S_i,R_i}}{\gamma_{S_j,R_i}+N_i},\quad \Gamma_{\mathrm{IC-e}}^{(t)}=\frac{\gamma_{S_i,E_e}}{\gamma_{R_K,E_e}+\gamma_{S_j,E_e}+N_e} \tag{5.22}$$

and

$$\Gamma_{\mathrm{IC-r}}^{(t)}=\frac{\gamma_{R_k,R_r}}{\gamma_{R_K,R_r}+N_r}. \tag{5.23}$$

5.2.2 Problem Formulation

In this subsection, we describe the secrecy rate used in the literature to assess the performance of the proposed algorithms in physical layer security research. The MIMO system secrecy capacity is expressed as [18]:

$$\begin{aligned}C_s=&\max_{\boldsymbol{Q}_s\succeq 0,\mathrm{Tr}(\boldsymbol{Q}_s)=\mathrm{E_s}}\log(\det(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H))\\&-\log(\det(\boldsymbol{I}+\boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H)),\end{aligned} \tag{5.24}$$

where $\boldsymbol{Q}_s$ is the covariance matrix associated with the signal and $\boldsymbol{H}_{ba}$ and $\boldsymbol{H}_{ea}$ represent the links between the source to the users and the eavesdroppers, respectively. For the relay system [78], according to (5.8) and (5.11), with equal power P allocated to the transmitter and the relays, the achievable rate of the users can be expressed as:

$$R_r=\log(\det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})) \tag{5.25}$$

where $\boldsymbol{\Gamma}_r^{(t)}$ according to (5.16) is given by

$$\boldsymbol{\Gamma}_r^{(t)}=\frac{P}{\sum_{k=1}^{K}N_k}\boldsymbol{H}_{Kr}\boldsymbol{H}_{Kr}^H(\boldsymbol{I}+\frac{P}{N_t}\boldsymbol{H}^{(pt)}\boldsymbol{U}^{pt}\boldsymbol{U}^{pt\,H}\boldsymbol{H}^{(pt)\,H}). \tag{5.26}$$

Similarly, for the eavesdropper the achievable rate with the assumption that a global knowledge for all the links available can be expressed as:

$$R_e = \log(\det(\boldsymbol{I} + \boldsymbol{\Gamma}_e^{(t)})) \tag{5.27}$$

and the $\boldsymbol{\Gamma}_{e,i}^{(t)}$ according to (5.15) is described by

$$\boldsymbol{\Gamma}_e^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta})^{-1} \frac{P}{N_t} \boldsymbol{H}_e \boldsymbol{U} \boldsymbol{U}^H \boldsymbol{H}_e{}^H, \tag{5.28}$$

where

$$\boldsymbol{\Delta} = \sum_{e=1}^{N} \frac{P}{\sum_{k=1}^{K} N_k} \boldsymbol{H}_{Ke} \boldsymbol{H}_{Ke}^H (\boldsymbol{I} + \frac{P}{N_t} \boldsymbol{H}^{(pt)} \boldsymbol{U}^{pt} \boldsymbol{U}^{pt\,H} \boldsymbol{H}^{(pt)\,H}). \tag{5.29}$$

In (5.28), $\boldsymbol{\Delta}$ represents the jamming signal to the eavesdropper. Using (5.25) and (5.27) the secrecy rate for the multiple users can be expressed as:

$$R = \sum_{r=1}^{T} \sum_{e=1}^{N} [R_r - R_e]^+ \tag{5.30}$$

where $[x]^+ = max(0, x)$.

Our objective is to select the set of relay nodes to perform relaying or jamming in order to maximize the secrecy rate. Therefore, the proposed optimization problem can be formulated as:

$$\begin{aligned} &\underset{k,i}{\text{maximize}} \quad R \\ &\text{subject to} \quad k, i \in \boldsymbol{\Psi} \end{aligned} \tag{5.31}$$

where $\boldsymbol{\Psi}$ represents the relay node poll, and k and i denote the kth selected jamming function node and ith relaying function node, respectively.

5.2.3 Relay Selection Algorithms

In the conventional relaying or jamming systems, relays often serve as the receiver and as the transmitter in order to enhance the reliability of the signal transmission from the source to the destination. We first review several algorithmic solutions under this conventional relay scenario and then describe an approach to relay selection without channel state information (CSI) to the eavesdroppers.

Conventional Selection

The conventional selection does not take the jamming function of relay nodes into account and the relay nodes are selected with different selection criteria to assist the transmission between the source and the destination without consideration of eavesdroppers [71] or with only one eavesdropper [12].

In [71], a max-min relay selection has been considered as the optimal selection scheme for conventional decode-and-forward (DF) relay setups. In a single-antenna scenario the relay selection policy is given by

$$R_i^{\max-\min} = \max_{R_i \in \mathbf{\Psi}} \min(\|h_{S,R_i}\|^2, \|h_{R_i,D}\|^2) \tag{5.32}$$

where h_{S,R_k} is the channel gain between the source and the relay and $h_{R_k,D}$ is the channel gain between the relay k and the destination. Similarly, a max-link approach has also been introduced to relax the limitation that the source and the relay transmission must be fixed. The max-link relay selection strategy can be described by

$$\begin{aligned} R_i^{\max-\text{link}} = \max_{R_i \in \mathbf{\Psi}} \Big(& \bigcup_{R_i \in \zeta : \varphi(Q_p) \neq L} \|h_{S,R_i}\|^2, \\ & \bigcup_{R_i \in \mathbf{\Psi} : \varphi(Q_p) \neq 0} \|h_{R_i,D}\|^2 \Big) \end{aligned} \tag{5.33}$$

With the consideration of the eavesdropper, a max-ratio selection policy is proposed in [12] and is expressed by

$$R_i^{\max-\text{ratio}} = \max_{R_i \in \mathbf{\Psi}} (\eta_1, \eta_2) \tag{5.34}$$

with

$$\eta_1 = \frac{\max_{R_i \in \mathbf{\Psi} : \varphi(Q_p) \neq L} \|h_{S,R_i}\|^2}{\|h_{se}\|^2} \tag{5.35}$$

$$\eta_2 = \max_{R_i \in \mathbf{\Psi} : \varphi(Q_p) \neq 0} \frac{\|h_{R_i,D}\|^2}{\|h_{R_{ie}}\|^2} \tag{5.36}$$

The aforementioned relay selection procedure is based on CSI. In [79] a conventional selection as well as the optimal selection based on the signal-to-interference-plus-noise ratio (SINR) criterion are reported.

Optimal Selection (OS)

Since the conventional selection reported in [79] may not support systems with secrecy constraints, we consider optimal selection (OS) which takes the eavesdropper into consideration. The SINR of OS in the downlink of the multiuser MIMO relay systems under consideration can be expressed similarly to (5.15) and (5.16) as is described by

$$\Gamma_e^{(t)} = \frac{\gamma_{S,E_e}}{N_e \sigma_e^2} \tag{5.37}$$

and

$$\Gamma_r^{(t)} = \frac{\gamma_{R_k,R_r}}{N_r \sigma_r^2}. \tag{5.38}$$

The OS algorithm is given by

$$\begin{aligned} R^{OS} &= \max[R_r - R_e]^+ \\ &= \max[\log(1+\Gamma_r^{(t)})) - \log(1+\Gamma_e^{(t)})]^+ \end{aligned} \tag{5.39}$$

Relay Selection without CSI to Eavesdroppers

IIn the previously described relay selection algorithms, the CSI to the eavesdroppers is an unavoidable assumption in the design of relay selection techniques based on secrecy constraints. However, in the optimization problem in (5.31), the global instantaneous information of the eavesdropper's CSI is hard to obtain and often not available. In order to circumvent this limitation, we propose a novel relay selection criterion without CSI to the eavesdroppers to be incorporated in the multiuser MIMO relay system under study. The details of this relay selection criterion are given in Appendix. The so-called simplified secrecy rate (S-SR) based multiple relay selection is expressed by

$$\begin{aligned} \boldsymbol{\varphi}^{\mathrm{S-SR}} = \max_{\phi_i \in \boldsymbol{\varphi}, \boldsymbol{\varphi} \in \boldsymbol{\Psi}} \Big\{ & \log\left(\det\left[\boldsymbol{I} + \boldsymbol{\Gamma}_{r,i}\right]\right) \\ & - \log\left(\det\left[\boldsymbol{I} + \boldsymbol{U}_i^H \boldsymbol{R}_I^{-1} \boldsymbol{U}_i \boldsymbol{R}_d\right]\right) \Big\}, \end{aligned} \tag{5.40}$$

where the covariance matrix of the interference and the signal can be described as $\boldsymbol{R}_I = \boldsymbol{H}_i{}^{-1}\boldsymbol{H}_i{}^{H^{-1}} + \sum_{j\neq i} \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} \boldsymbol{s}_j^{(t)H} \boldsymbol{U}_j{}^H$ and $\boldsymbol{R}_d = \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} \boldsymbol{s}_i^{(t)H} \boldsymbol{U}_i{}^H$, respectively. In (5.40), no CSI to the eavesdroppers is required and the criterion only depends on the channel information

to the intended receiver and the covariance matrix of the interference and the signal. In the following proposed relaying and jamming schemes, the S-SR technique is applied to avoid the requirement for global instantaneous information of the eavesdropper's CSI.

5.3 Selection with Jamming Function Relays

In this section novel approaches to relaying and jamming function selection are presented. We start with a simple single-antenna scenario and then consider the MIMO scenario. Moreover, we also develop a relaying and jamming function selection for multiuser MIMO buffer-aided relay systems.

5.3.1 Relaying and Jamming Function Selection (RJFS)

We assume that the total number of relay nodes is S_{total} and $\boldsymbol{\Omega}$ represents the total relay set. To apply the opportunistic scheme in the system, an initial state is set according to the channel:

$$\boldsymbol{\Omega}^0 = \max_{\boldsymbol{\Omega}^0} \det\left(\boldsymbol{H}_{\boldsymbol{\Omega}^0}\boldsymbol{H}_{\boldsymbol{\Omega}^0}{}^H\right), \tag{5.41}$$

in the initial state, we assume the relays will not perform jamming function. S relay nodes are selected according to the criterion. With the total number of relaying and jamming nodes S_{total} and the number of selected nodes in each group S, the selection operation can be expressed as:

$$\boldsymbol{\Psi} = \binom{S_{\text{total}}}{S}, \tag{5.42}$$

where $\boldsymbol{\Psi}$ represents total sets of T-combination and in each set there are S number of selected relaying or jamming nodes. For a particular selected set $\boldsymbol{\Omega}^m$, we assume $\boldsymbol{H}_{\boldsymbol{\Omega}^m}$ represents the total channel matrix of selected sets, then the corresponding channel for set m can be described by

$$\boldsymbol{H}_{\boldsymbol{\Omega}^m} = \left[\boldsymbol{H}_{\boldsymbol{\Omega}_1^m}^{(t)\,T} \quad \boldsymbol{H}_{\boldsymbol{\Omega}_2^m}^{(t)\,T} \quad \boldsymbol{H}_{\boldsymbol{\Omega}_3^m}^{(t)\,T} \quad \cdots \quad \boldsymbol{H}_{\boldsymbol{\Omega}_{S^m}}^{(t)\,T}\right]^T. \tag{5.43}$$

If the total collection of selected sets is represented by $\boldsymbol{\Psi}_{\text{Relaying}}$, for each set the relay selection is given by

$$\boldsymbol{\Omega}^m = \max_{\boldsymbol{\Omega}^m \in \boldsymbol{\Psi}_{\text{Relaying}}} \sum_{\phi_i \in \boldsymbol{\Omega}^m} \left\{ \log\left(\det\left(\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^m}^{(t)}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^e}^{(t)}\right)\right) \right\} \tag{5.44}$$

where

$$\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^m}^{(t)} = \boldsymbol{I} + (\boldsymbol{H}_i \boldsymbol{R}_I^{\boldsymbol{\Omega}^m} \boldsymbol{H}_i^H)^{-1} (\boldsymbol{H}_i \boldsymbol{R}_d^{\boldsymbol{\Omega}^m} \boldsymbol{H}_i^H) \tag{5.45}$$

and

$$\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^e}^{(t)} = \boldsymbol{I} + \boldsymbol{U}_i^H \boldsymbol{R}_I^{\boldsymbol{\Omega}^m -1} \boldsymbol{U}_i \boldsymbol{R}_d^{\boldsymbol{\Omega}^m} \tag{5.46}$$

In (5.45) and (5.46), the covariance matrices $\boldsymbol{R}_d^{\Omega^m}$ can be obtained in the same way illustrated in (5.40). The only difference of the proposed RJFS algorithm resides in the calculation of $\boldsymbol{R}_I^{\Omega^m}$, apart from the interference from different users, there is also existing interference from the jamming function relay nodes. With the same distributions of the channels from the jamming function relay nodes to the eavesdropper, the interference $\boldsymbol{R}_I^{\Omega^m}$ can be also calculated in a similar way to that shown in (5.40). In Algorithm 7 the main steps for relay selection are given.

Algorithm 7 RJFS Algorithm

1: **for** $t = 1 : S$ **do**
2: **for** $q = 1 : S_{\text{total}}$ **do**
3: $\Gamma_q = \max_{q \in \boldsymbol{\Omega}} \det(\boldsymbol{H}_q \boldsymbol{H}_q{}^H)$
4: **end for**
5: $\boldsymbol{\Omega}_t^0 = q$
6: **end for**
7: $\boldsymbol{\Psi}_{\text{Relaying}} = \binom{S_{\text{total}}}{S}$
8: $[\Omega_c \quad \Omega_r] = \text{size}(\boldsymbol{\Psi}_{\text{Relaying}})$
9: **for** $m = 1 : \Omega_c$ **do**
10: $\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^m}^{(t)} = \boldsymbol{I} + (\boldsymbol{H}_i \boldsymbol{R}_I^{\boldsymbol{\Omega}^m} \boldsymbol{H}_i^H)^{-1} (\boldsymbol{H}_i \boldsymbol{R}_d^{\boldsymbol{\Omega}^m} \boldsymbol{H}_i^H)$
11: $\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^e}^{(t)} = \boldsymbol{I} + \boldsymbol{U}_i^H \boldsymbol{R}_I^{\boldsymbol{\Omega}^m -1} \boldsymbol{U}_i \boldsymbol{R}_d^{\boldsymbol{\Omega}^m}$
12: $\boldsymbol{\Omega}^m = \max_{\boldsymbol{\Omega}^m \in \boldsymbol{\Psi}_{\text{Relaying}}} \sum_{\phi_i \in \boldsymbol{\Omega}^m} \left\{ \log\left(\det\left(\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^m}^{(t)}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}_{\boldsymbol{\Omega}^e}^{(t)}\right)\right) \right\}$
13: **end for**

In Algorithm 7, from step 1 to step 7, S relay nodes are selected out of S_{total} relay nodes. To simplify the initialization, the S relay nodes are selected one by one. The loop from step 2 to step 4 is used to investigate all relay nodes. $\boldsymbol{\Omega}^0$ contains the initial relay nodes and these nodes will have the initial signal $\boldsymbol{H}_{\boldsymbol{\Omega}^0} \boldsymbol{s}_0 + \boldsymbol{n}_0$ from the relays to the users. With no buffers implemented at relay nodes, RJFS only selects the relays in Link I. The relays used in Link II is the same as the selected relays in Link I in previous time slot.

5.3.2 Buffer-aided Relaying and Jamming Function Selection (BF-RJFS)

Here we described the proposed BF-RJFS algorithm, which exploits relays equipped with buffers. Based on the RJFS algorithm, the selection of the S relays used for signal reception

is the same as that in the buffer relay scenario. The main difference between the proposed BF-RJFS and RJFS algorithms relies on the selection of the jammer. In the following, we will detail the jammer selection procedure. The selection of the set of jamming relays is performed simultaneously. According to (5.44), we assume the corresponding threshold is expressed as $C_{\boldsymbol{\Omega}^m}$. Given the total collection of jamming selects $\boldsymbol{\Psi}_{\text{Jamming}}$, the remaining relays are selected according to the S-SR criterion outlined as described by

$$\boldsymbol{\Omega}^r = \max_{\boldsymbol{\Omega}^r \in \boldsymbol{\Psi}_{\text{Jamming}}} \sum_{\phi_i \in \boldsymbol{\Omega}^r} \left\{ \log\left(\det\left(\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,n}}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,e}}\right)\right) \right\} \tag{5.47}$$

where $\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,n}}$ is given by

$$\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,n}} = \boldsymbol{I} + (\boldsymbol{H}_{\boldsymbol{\Omega}^r} \boldsymbol{R}_I^{BF} \boldsymbol{H}^H_{\boldsymbol{\Omega}^r})^{-1} (\boldsymbol{H}_{\boldsymbol{\Omega}^r} \boldsymbol{R}_d^{BF} \boldsymbol{H}^H_{\boldsymbol{\Omega}^r}), \tag{5.48}$$

where $\boldsymbol{R}_d^{BF}$ is the covariance matrix of the transmit signal from the jamming function relay nodes to the users. The jamming function is the same as the received relaying signal in previous time slots. The calculation of $\boldsymbol{R}_d^{BF}$ depends on (5.20) and $\boldsymbol{R}_I^{BF}$ relies on (5.17) and (5.18). In this procedure, the calculation for the transmission to eavesdroppers is given by

$$\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,e}} = \boldsymbol{I} + \boldsymbol{U}_r^H \boldsymbol{R}_I^{BF^{-1}} \boldsymbol{U}_r \boldsymbol{R}_d^{BF} \tag{5.49}$$

where the relays used for jamming in the next time slot are selected. With the selection of receiving relays and jamming relays the system can provide a better secrecy performance as compared to conventional relay systems. In Algorithm 8 the main steps are outlined.

In Algorithm 8, step 2 to step 7 are eliminating the relay nodes with empty buffer because empty buffer relay nodes can not perform relaying function. Step 14 to step 19 are eliminating relay nodes with full buffer as the signals from the source can not be stored in these relay nodes.

5.3.3 Greedy Algorithm in Relay Selection

In both RJFS and BF-RJFS algorithms, exhaustive searches are implemented to select the relaying and jamming nodes. The incorporation of a greedy strategy in both RJFS and BF-RJFS algorithms can significantly reduce the computational cost of the proposed exhaustive search-based RJFS and BF-RJFS algorithms.

In the presence of multiple relays, exhaustive search is capable of achieving optimal relay

Algorithm 8 BF-RJFS Algorithm

loop
  $\boldsymbol{Q} = \boldsymbol{L}_{\text{state}}(:, L)$
  for $q = 1 : S_{\text{total}}$ **do**
    if $\boldsymbol{Q}(qN_i) = 0$ **then**
      $\boldsymbol{\Omega}/q = [1 \quad 2 \quad \cdots \quad q-1 \quad q+1 \cdots S_{\text{total}}]$
    end if
  end for
  ${\Omega_c}^1 = \text{length}(\boldsymbol{\Omega})$
  for $r = 1 : {\Omega_c}^1$ **do**
    $\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,n}} = \boldsymbol{I} + (\boldsymbol{H}_{\boldsymbol{\Omega}^r} \boldsymbol{R}_I^{BF} \boldsymbol{H}^H_{\boldsymbol{\Omega}^r})^{-1} (\boldsymbol{H}_{\boldsymbol{\Omega}^r} \boldsymbol{R}_d^{BF} \boldsymbol{H}^H_{\boldsymbol{\Omega}^r})$
    $\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,e}} = \boldsymbol{I} + \boldsymbol{U}_r^H \boldsymbol{R}_I^{BF^{-1}} \boldsymbol{U}_r \boldsymbol{R}_d^{BF}$
    $[\eta_{\text{LinkII}} \quad \boldsymbol{\Omega}^r] = \max_{\boldsymbol{\Omega}^r \in \boldsymbol{\Psi}_{\text{Relaying}}} \sum_{\phi_i \in \boldsymbol{\Omega}^r} \left\{ \log\left(\det\left(\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,n}}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^{r,e}}\right)\right) \right\}$
  end for
  $\boldsymbol{Q} = \boldsymbol{L}_{\text{state}}(:, 1)$
  for $q = 1 : S_{\text{total}}$ **do**
    if $\boldsymbol{Q}(qN_i) \neq 0$ **then**
      $\boldsymbol{\Omega}/q = [1 \quad 2 \quad \cdots \quad q-1 \quad q+1 \cdots S_{\text{total}}]$
    end if
  end for
  $\Omega^2 = \text{length}(\boldsymbol{\Omega})$
  $\boldsymbol{\Psi}_{\text{Jamming}} = \binom{\Omega^2}{S}$
  $[{\Omega_c}^2 \quad {\Omega_r}^2] = \text{size}(\boldsymbol{\Psi}_{\text{Jamming}})$
  for $m = 1 : {\Omega_c}^2$ **do**
    $\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^m} = \boldsymbol{I} + (\boldsymbol{H}_i \boldsymbol{R}_I^{\boldsymbol{\Omega}^m} \boldsymbol{H}_i^H)^{-1} (\boldsymbol{H}_i \boldsymbol{R}_d^{\boldsymbol{\Omega}^m} \boldsymbol{H}_i^H)$
    $\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^e} = \boldsymbol{I} + \boldsymbol{U}_i^H \boldsymbol{R}_I^{\boldsymbol{\Omega}^{m\,-1}} \boldsymbol{U}_i \boldsymbol{R}_d^{\boldsymbol{\Omega}^m}$
    $[\eta_{\text{LinkI}} \quad \boldsymbol{\Omega}^m] = \max_{\boldsymbol{\Omega}^m \in \boldsymbol{\Psi}_{\text{Jamming}}} \sum_{\phi_i \in \boldsymbol{\Omega}^m} \left\{ \log\left(\det\left(\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^m}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}^{(t)}_{\boldsymbol{\Omega}^e}\right)\right) \right\}$
  end for
end loop

selection with S-SR criterion. However, it leads to an exponential increase in computational complexity. To reduce the complexity of the algorithm while maintaining the high secrecy rate performance, we employ greedy search instead of exhaustive search.

In an exhaustive search, all possible combinations are investigated to obtain optimal results. In contrast, a greedy search implements the calculation with individual relays and in every iteration of the greedy search, the relay with best output threshold is selected. Then in the next iteration the remaining relays are calculated in the same way. The selection process continues until the necessary relays are selected. The total number of considered relays can be calculated with the following expression as:

$$\Omega_c = S_{\text{total}} + S_{\text{total}} - 1 + \cdots + S_{\text{total}} - S. \tag{5.50}$$

From (5.50), we can see that total number of request investigate relays is increased linearly to the total number of relays which contributes to the reduction of computational complexity.

In the following we describe the proposed greedy RJFS algorithm. Here we choose relays according to the S-SR criterion. When the K relays that forward the signals to the users are determined, the relays used for signal reception are chosen based on the S-SR criterion, as given by

$$m = \max_{m\in\boldsymbol{\Omega}}\big[\log\big(\det\left(\boldsymbol{\Gamma}_m^{(t)}\right)\big) - \log\big(\det\left(\boldsymbol{\Gamma}_e^{(t)}\right)\big)\big] \tag{5.51}$$

where $\boldsymbol{\phi}_m$ represents the selected relays and $\boldsymbol{\Gamma}_m^{(t)}$ corresponds to the mth relay which is calculated based on (5.12) and is given by

$$\boldsymbol{\Gamma}_m^{(t)} = \boldsymbol{I} + (\boldsymbol{H}_m\boldsymbol{R}_I^m\boldsymbol{H}_m^H)^{-1}(\boldsymbol{H}_m\boldsymbol{R}_d^m\boldsymbol{H}_m^H), \tag{5.52}$$

and $\boldsymbol{\Gamma}_e^{(t)}$ is described by

$$\boldsymbol{\Gamma}_e^{(t)} = \boldsymbol{I} + \boldsymbol{U}_m^H\boldsymbol{R}_I^{m-1}\boldsymbol{U}_m\boldsymbol{R}_d^m \tag{5.53}$$

Instead of the exhaustive search of the selected set $\boldsymbol{\Omega}^m$, the mth relay is calculated with the aim of finding the relay that provides the highest secrecy rate based on $\boldsymbol{\phi}_m$. In (5.52), $\boldsymbol{R}_d^m$ and $\boldsymbol{R}_I^m$ are obtained in the same way as in (5.45) and (5.46).

The main steps are described in Algorithm 9. Similarly to the BF-RJFS algorithm, the greedy-BF-RJFS algorithm substitutes the exhaustive search of all combinations with a greedy search of individual relays. The main difference is the selection of jamming relays. Specifically, for a particular user r each relay computes a threshold and the relay k with the

Algorithm 9 Greedy-RJFS Algorithm

for $t = 1 : S$ **do**
  for $q = 1 : S_{\text{total}}$ **do**
    $\Gamma_q = \max_{q \in \mathbf{\Omega}} \det(\boldsymbol{H}_q \boldsymbol{H}_q{}^H)$
  end for
  $\Gamma_t{}^0 = \Gamma_q$
  $\mathbf{\Omega}/q = [1 \quad 2 \quad \cdots \quad q-1 \quad q+1 \cdots \Omega^{\text{total}}]$
end for
$\Omega^0 = \text{length}(\mathbf{\Omega})$
for $t = 1 : T$ **do**
  for $m = 1 : \Omega^0$ **do**
    $\mathbf{\Gamma}_m^{(t)} = \boldsymbol{I} + (\boldsymbol{H}_m \boldsymbol{R}_I^m \boldsymbol{H}_m^H)^{-1} (\boldsymbol{H}_m \boldsymbol{R}_d^m \boldsymbol{H}_m^H)$
    $\mathbf{\Gamma}_e^{(t)} = \boldsymbol{I} + \boldsymbol{U}_m^H \boldsymbol{R}_I^{m-1} \boldsymbol{U}_m \boldsymbol{R}_d^m$
    $m = \max_{m \in \mathbf{\Omega}} [\log\left(\det\left(\mathbf{\Gamma}_m^{(t)}\right)\right) - \log\left(\det\left(\mathbf{\Gamma}_e^{(t)}\right)\right)]$
  end for
  $\boldsymbol{\Omega}_t^{\text{select}} = m$
  $\mathbf{\Omega} = \mathbf{\Omega}/m$
end for

highest threshold is selected until S relays are selected to forward the signal to all users. The details of the algorithm are given in Algorithm 10. Comparing the algorithms in Chapter 5, as the complexity of greedy algorithms is increasing linearly, Algorithm 9 and 10 will have a much lower complexity and with buffers implemented, Algorithm 8 will have a higher complexity than Algorithm 7. As a conclusion, in terms of complexity Algorithm 9 < Algorithm 10<Algorithm 7<Algorithm 8 for systems with a large number of relays.

5.4 Secrecy Analysis

In this section, we analyze the secrecy performance of a standard MIMO relay system as well as the proposed buffer-aided MIMO relay system with relaying and jamming function selection. We carry out the derivation considering a scenario with channel information to eavesdroppers. The output results indicate the theoretical benchmark for the proposed RJFS and BF-RJFS algorithms. First let us recall a standard MIMO relay system. According to [12], the overall secrecy capacity of a single-antenna relay system is given as follows:

Definition 1. *With selected relay k and channels from source to relay k, relay k to destination, source to eavesdropper, relay k to eavesdropper expressed as $h_{sr_k}, h_{r_k d}, h_{se}, h_{r_k e}$ respectively, the following equation is obtained:*

$$C_k = \max\{\frac{1}{2}\log_2 \frac{\min\{1 + P\|h_{sr_k}\|^2, 1 + P\|h_{r_k d}\|^2\}}{1 + P\|h_{se}\|^2 + P\|h_{r_k e}\|^2}\} \tag{5.54}$$

Algorithm 10 Greedy-BF-RJFS Algorithm

loop
  $\boldsymbol{Q} = \boldsymbol{L}_{\text{state}}(:, L)$
  for $q = 1 : S_{\text{total}}$ **do**
    if $\boldsymbol{Q}(qN_i) = 0$ **then**
      $\boldsymbol{\Omega}/q = [1 \quad 2 \quad \cdots \quad q-1 \quad q+1 \cdots S_{\text{total}}]$
    end if
  end for
  $\Omega^1 = \text{length}(\boldsymbol{\Omega})$
  for $r = 1 : M$ **do**
    for $k = 1 : \Omega^1$ **do**
      $\boldsymbol{\Gamma}_{kr}^{(t)} = \boldsymbol{I} + (\boldsymbol{H}_{kr}\boldsymbol{R}_I^{BF}\boldsymbol{H}_{kr}^H)^{-1}(\boldsymbol{H}_{kr}\boldsymbol{R}_d^{BF}\boldsymbol{H}_{kr}^H)$
      $\boldsymbol{\Gamma}_{ke}^{(t)} = \boldsymbol{I} + \boldsymbol{U}_k^H\boldsymbol{R}_I^{BF^{-1}}\boldsymbol{U}_k\boldsymbol{R}_d^{BF}$
      $[\boldsymbol{\eta}_r^1 \quad k] = \arg\max_{k\in\boldsymbol{\Omega}} \log\left(\det\left(\boldsymbol{\Gamma}_{kr}^{(t)}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}_{ke}^{(t)}\right)\right)$
    end for
    $\boldsymbol{\Omega}_r^{\text{transmit}} = k$
    $\eta_{\text{LinkII}} = \sum \boldsymbol{\eta}^1$
  end for
  $\boldsymbol{Q} = \boldsymbol{L}_{\text{state}}(:, 1)$
  for $q = 1 : S_{\text{total}}$ **do**
    if $\boldsymbol{Q}(qN_i) \neq 0$ **then**
      $\boldsymbol{\Omega}/q = [1 \quad 2 \quad \cdots \quad q-1 \quad q+1 \cdots S_{\text{total}}]$
    end if
  end for
  $\Omega^2 = \text{length}(\boldsymbol{\Omega})$
  for $t = 1 : S$ **do**
    for $m = 1 : \Omega^2$ **do**
      $\boldsymbol{\Gamma}_m^{(t)} = \boldsymbol{I} + (\boldsymbol{H}_m\boldsymbol{R}_I^m\boldsymbol{H}_m^H)^{-1}(\boldsymbol{H}_m\boldsymbol{R}_d^m\boldsymbol{H}_m^H)$
      $\boldsymbol{\Gamma}_e^{(t)} = \boldsymbol{I} + \boldsymbol{U}_m^H\boldsymbol{R}_I^{m-1}\boldsymbol{U}_m\boldsymbol{R}_d^m$
      $[\boldsymbol{\eta}_r^2 \quad m] = \arg\max_{\mathrm{m}\in\boldsymbol{\Omega}}[\log\left(\det\left(\boldsymbol{\Gamma}_{\mathrm{m}}^{(\mathrm{t})}\right)\right) - \log\left(\det\left(\boldsymbol{\Gamma}_{\mathrm{e}}^{(\mathrm{t})}\right)\right)]$
    end for
    $\boldsymbol{\Omega}_t^{\text{receive}} = m$
    $\eta_{\text{LinkI}} = \sum \boldsymbol{\eta}^2$
  end for
end loop

Equation (5.54) can be rewritten as (5.55) in which the first part calculates the capacity to the user and the second part the capacity to the eavesdropper.

$$C_k = \max\left[\frac{1}{2}\log_2\left(\min\{1+P\|h_{sr_k}\|^2, 1+P\|h_{r_kd}\|^2\}\right) - \frac{1}{2}\log_2\left(1+P\|h_{se}\|^2+P\|h_{r_ke}\|^2\right)\right] \tag{5.55}$$

In a half-duplex MIMO relay system, based on equations (5.26) and (5.28), the calculation of the capacity from the source to the relay and to the eavesdropper can be respectively expressed as:

$$C_i = \max\left[\frac{1}{2}\log_2\left(\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H{\boldsymbol{H}_i^{(t)}}^H\right)\right)\right] \tag{5.56}$$

$$C_e = \max\left[\frac{1}{2}\log_2\left(\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\right)\right] \tag{5.57}$$

The capacity from relay to destination is given by

$$C_r = \max\left[\frac{1}{2}\log_2\left(\det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})\right)\right]. \tag{5.58}$$

With equations (5.56), (5.57) and (5.58) based on the overall secrecy capacity of a single-antenna relay system, we present the overall secrecy capacity of a MIMO relay system, which can be obtained by solving:

$$C_k^{\text{MIMO}} = \max\left[\frac{1}{2}\log_2\left(\min\{M_i, M_r\}\right) - \frac{1}{2}\log_2\left(\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\right)\right], \tag{5.59}$$

where $M_i = \det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H{\boldsymbol{H}_i^{(t)}}^H\right)$ and $M_r = \det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})$. Note that the value $\frac{1}{2}$ is due to the half-duplex system.

Proposition 2. *With size L buffers implemented at relay nodes, the secrecy-rate performance can be improved. The secrecy rate difference changes between* 0 *to* $\Delta_{\text{R-BF}}$.

Based on the half-duplex MIMO relay system, in the presence of multiple relay nodes, relay selection can be implemented prior to transmission. If we use $\boldsymbol{\Psi}$ to represent a set of relay nodes, based on (5.59), relay selection can be expressed as:

$$\max_{i\in\boldsymbol{\Psi}} \min\{\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H{\boldsymbol{H}_i^{(t)}}^H\right), \det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})\} \tag{5.60}$$

Under the condition that $\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_i^{(t)^H}\right) < \det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})$, relay selection can be simplified and described by

$$\max_{i_R\in\boldsymbol{\Psi}}\left\{\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_i^{(t)^H}\right)\right\}, \tag{5.61}$$

where i_R represents the selected relay. In this scenario, the secrecy rate of the relay system can be obtained by

$$\begin{aligned} I_{\text{Relay}}^{(1)} = &\frac{1}{2}\log_2\left(\left\{\det\left(\boldsymbol{I}+\boldsymbol{H}_{i_R}^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_{i_R}^{(t)^H}\right)\right\}\right) \\ &-\frac{1}{2}\log_2\left(\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\right). \end{aligned} \tag{5.62}$$

Under the condition that $\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_i^{(t)^H}\right) > \det(\boldsymbol{I}+\boldsymbol{\Gamma}_{r,i}^{(t)})$, the secrecy rate can be obtained in the same way and the result is given by

$$\begin{aligned} I_{\text{Relay}}^{(2)} = &\frac{1}{2}\log_2\left(\left\{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})\right\}\right) \\ &-\frac{1}{2}\log_2\left(\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\right). \end{aligned} \tag{5.63}$$

When each relay node is equipped with an infinite buffer, the signals can be stored in the buffers which means that the signals can wait at the relay nodes until the condition $\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_i^{(t)^H}\right) < \det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})$ is satisfied. If we use $\det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(pt)})$ to represent the condition that is experienced in the previous time slot which follows the constraint that $\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(pt)}\boldsymbol{U}^{(pt)}\boldsymbol{U}^{(pt)^H}\boldsymbol{H}_i^{(pt)^H}\right) > \det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(pt)})$, the expression of the secrecy rate with infinite buffers is described by

$$\begin{aligned} I_{\text{R-BF}} = &\frac{1}{2}\log_2\left(\left\{\det\left(\boldsymbol{I}+\boldsymbol{H}_{i_R}^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_{i_R}^{(t)^H}\right)\right\}\right) \\ &-\frac{1}{2}\log_2\left(\left\{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(pt)})\right\}\right). \end{aligned} \tag{5.64}$$

More specifically, with a length L buffer, the condition $\det\left(\boldsymbol{I}+\boldsymbol{H}_i^{(t)}\boldsymbol{U}\boldsymbol{U}^H\boldsymbol{H}_i^{(t)^H}\right) > \det(\boldsymbol{I}+\boldsymbol{\Gamma}_r^{(t)})$ will not hold, then the difference of the secrecy rate will be between 0 to $I_{\text{R-BF}}$.

In most scenarios, to avoid the interference in the transmission to or from the relays, a half-duplex scheme is employed. To release the limit on time slots, an opportunistic scheme can be applied to the MIMO relay system.

Proposition 3. *An opportunistic scheme is capable of improving the secrecy rate as compared with traditional half-duplex MIMO relay systems.*

According to [15], in the opportunistic scheme we have concurrent transmissions by the source and relays taking place at the same time-slot. This will result in IRI and as a result its effect on the relay that receives the source signal must be considered during the opportunistic scheme. In [15], Nomikos also points out that jamming can be performed at the relay node. To simplify the proof, we first assume jamming is performed which will enlarge the value of $I^{(1)}_{\text{Relay}}, I^{(2)}_{\text{Relay}}$ and the coefficient of the improvement is $m_{op} > 1$. The secrecy rate can be expressed as:

$$I^{(1)}_{\text{Opportunistic}-\text{Relay}} = m_{op} \times I^{(1)}_{\text{Relay}}, \tag{5.65}$$

$$I^{(2)}_{\text{Opportunistic}-\text{Relay}} = m_{op} \times I^{(2)}_{\text{Relay}}, \tag{5.66}$$

where

$$I_{\text{Opportunistic}-\text{Relay}-\text{buffer}} = m_{op} \times I_{\text{R}-\text{BF}} \tag{5.67}$$

From this analysis we can verify that the secrecy rate of the opportunistic scheme doubles. If jamming cannot be performed, based on (5.62), the secrecy rate is expressed as:

$$\begin{aligned} I^{(1)}_{\text{Opp}-\text{Relay}} = \frac{m_{op}}{2} \log_2 \left(\{ \det \left(\boldsymbol{I} + (\boldsymbol{I} + \boldsymbol{\Delta}'_{i_R})^{-1} \boldsymbol{H}^{(t)}_{i_R} \boldsymbol{U} \boldsymbol{U}^H \boldsymbol{H}^{(t)^H}_{i_R} \right) \} \right) \\ - \frac{m_{op}}{2} \log_2 \left(\det(\boldsymbol{I} + \boldsymbol{\Gamma}^{(t)}_e) \right), \end{aligned} \tag{5.68}$$

where

$$\boldsymbol{\Delta}'_{i_R} = \sum_{k=1}^{K} \boldsymbol{H}_{k i_R} \boldsymbol{H}^{(pt)}_{i_R} \boldsymbol{U}^{(pt)} \boldsymbol{U}^{(pt)^H} \boldsymbol{H}^{(pt)^H}_{i_R} \boldsymbol{H}^H_{k i_R}, \tag{5.69}$$

which represents IRI. Then the secrecy rate difference between the original relay system with an opportunistic scheme relay buffer system is obtained by

$$\begin{aligned} \Delta_{\text{Opp}-\text{R}-\text{BF}} = \frac{m_{op}}{2} \log_2 \left(\{ \det \left(\boldsymbol{I} + (\boldsymbol{I} + \boldsymbol{\Delta}'_{i_R})^{-1} \boldsymbol{H}^{(t)}_{i_R} \boldsymbol{H}^{(t)^H}_{i_R} \right) \} \right) \\ - \frac{m_{op}}{2} \log_2 \left(\{ \det(\boldsymbol{I} + \boldsymbol{\Gamma}^{(pt)}_r) \} \right). \end{aligned} \tag{5.70}$$

5.4.1 Relaying and Jamming Function Selection (RJFS)

Proposition 4. *When* SNR $\to \infty$*, the secrecy rate* $C_{\text{Opportunstic}-\text{Relay}-\text{buffer}} \to \infty$ *and the secrecy rate with IRI cancellation outperforms without IRI cancellation.*

In all aforementioned systems, we have not taken any jamming signal into consideration.

In the presence of systems with multiple relay nodes, without obtaining more resources, some relay nodes can perform the jamming function by introducing jamming signals to the eavesdroppers. More specifically, the IRI can be applied. In the RJFS algorithm, the selected relay at the current time interval is the jammer as well as forward relay in the next time interval. The aim of the RJFS algorithm is to seek the relay that provides the highest secrecy rate performance.

According to Algorithm 1, the relay selection criterion is given by

$$\boldsymbol{\phi}_{i_R} = \max_{i_R \in \boldsymbol{\Psi}} \det\left((\boldsymbol{I} + \boldsymbol{\Gamma}_e^{(t)})^{-1}(\boldsymbol{I} + \boldsymbol{\Gamma}_{i_R}^{(t)})\right) \tag{5.71}$$

where i_R represents the selected relay. Based on (5.71), the secrecy rate with the selected relay can be expressed as:

$$\begin{aligned} I_{\text{RJFS}-\text{IRI}} = &\log_2\left(\{\det\left(\boldsymbol{I} + \boldsymbol{\Gamma}_{i_R}^{(t)}\right)\}\right) \\ &- \log_2\left(\{\det(\boldsymbol{I} + \boldsymbol{\Gamma}_e^{(t)})\}\right). \end{aligned} \tag{5.72}$$

When jamming is performed at the relay nodes, (5.72) can be simplified to

$$\begin{aligned} I_{\text{RJFS}-\text{J}} = &\log_2\left(\{\det\left(\boldsymbol{I} + \boldsymbol{H}_{i_R}^{(t)}\boldsymbol{U}\boldsymbol{U}^H{\boldsymbol{H}_{i_R}^{(t)}}^H\right)\}\right) \\ &- \log_2\left(\{\det(\boldsymbol{I} + \boldsymbol{\Gamma}_e^{(t)})\}\right). \end{aligned} \tag{5.73}$$

Equation (5.73) was obtained in our previous study [82] when SNR $\to \infty$. Comparing (5.72) with (5.73), we can have $I_{\text{RJFS}-\text{J}} > I_{\text{RJFS}-\text{IRI}}$ which is indicated in Fig. 5.6.

5.4.2 Buffer-aided Relaying and Jamming Function Selection (BF-RJFS)

Proposition 5. *According to Proposition 2, the secrecy-rate performance can be improved with buffers. This can also be applied to the RJFS algorithm. In the IC scenario, when more power is allocated to the transmitter the secrecy rate will suffer from a dramatic decrease in the existing IRI scenario.*

In the buffer-aided RJFS algorithm, the relay selection and jamming selection can be implemented simultaneously with the following selection criterion:

$$\boldsymbol{\phi}_{i_R} = \max_{i_R \in \boldsymbol{\Psi}} \det\left((\boldsymbol{I} + \boldsymbol{\Gamma}_e^{(t)})^{-1}(\boldsymbol{I} + \boldsymbol{\Gamma}_{i_R}^{(t)})\right) \tag{5.74}$$

and

$$\boldsymbol{\phi}_n = \max_{n\in\boldsymbol{\Psi}} \det\left((\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})^{-1}(\boldsymbol{I}+\boldsymbol{\Gamma}_n^{(t)})\right), \tag{5.75}$$

where in both transmissions we can achieve high secrecy rate performance with separate selection from source to relays and relays to destinations. Considering power allocation, with the parameter η indicating the power allocated to the transmitter, we assume the power allocated to the transmitter is ηP and the power allocated to the relays is $(2-\eta)P$. When $\eta \to 0$, more power will be allocated to the transmitter, according to:

$$\begin{aligned} I^{(1)}_{\mathrm{BF-RJFS-IRI}} = \log_2\left(\{\det\left(\boldsymbol{I}+\boldsymbol{\Gamma}_{i_R}^{(t)}\right)\}\right) \\ - \log_2\left(\{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\}\right) \end{aligned} \tag{5.76}$$

and

$$\begin{aligned} I^{(2)}_{\mathrm{BF-RJFS-IRI}} = \log_2\left(\{\det\left(\boldsymbol{I}+\boldsymbol{\Gamma}_{n}^{(t)}\right)\}\right) \\ - \log_2\left(\{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\}\right), \end{aligned} \tag{5.77}$$

where the secrecy rate $I^{(1)}_{\mathrm{BF-RJFS-IRI}}$ will have an increase, while $I^{(2)}_{\mathrm{BF-RJFS-IRI}}$ will have a reduction. As a result, the overall secrecy rate suffers from a decrease. More specifically, with less power allocated in the relay or the jammer, the IRI that acts as a jamming signal to the eavesdropper will have less effect on the contribution to the secrecy rate. Then the overall secrecy rate will have a dramatic decrease.

If jamming is performed, according to (5.78) and (5.79), we have

$$\begin{aligned} I^{(1)}_{\mathrm{BF-RJFS-J}} = \log_2\left(\{\det\left(\boldsymbol{I}+\boldsymbol{H}_{i_R}^{(t)}\boldsymbol{U}\boldsymbol{U}^H{\boldsymbol{H}_{i_R}^{(t)}}^H\right)\}\right) \\ - \log_2\left(\{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\}\right) \end{aligned} \tag{5.78}$$

and

$$\begin{aligned} I^{(2)}_{\mathrm{BF-RJFS-J}} = \log_2\left(\{\det\left(\boldsymbol{I}+\boldsymbol{\Gamma}_{n}^{(t)}\right)\}\right) \\ - \log_2\left(\{\det(\boldsymbol{I}+\boldsymbol{\Gamma}_e^{(t)})\}\right), \end{aligned} \tag{5.79}$$

where more power is allocated to the transmitter and the secrecy rate $I^{(1)}_{\mathrm{BF-RJFS-J}}$ and $I^{(2)}_{\mathrm{BF-RJFS-J}}$ is less affected than in the scenario with IRI.

5.4.3 Greedy Algorithm in Relay Selection

Proposition 6. *With high* SNRs*, the greedy algorithm cooperation with the buffer-aided RJFS algorithm can achieve almost the same secrecy rate performance with a dramatic decrease in the computational complexity.*

According to (5.42), the total number of sets for an exhaustive search can be expressed as:

$$\Omega_{exhaustive} = \frac{S_{\text{total}}!}{(S_{\text{total}} - S)!S!}. \tag{5.80}$$

In the proposed greedy search algorithm, the search is implemented in the remaining relay nodes so that the total number of visited sets in the greedy search is given by

$$\Omega_{greedy} = S_{\text{total}} + S_{\text{total}} - 1 + \cdots + S_{\text{total}} - S + 1 = S_{\text{total}}S - \frac{S(S-1)}{2} \tag{5.81}$$

Based on (5.80) and (5.81), for a certain number of selected relay nodes S, when the total number of relay nodes M increases, the total number of visited sets for the exhaustive search is much higher than those for the greedy search, that is $\Omega_{exhaustive} >> \Omega_{greedy}$.

5.5 Simulation Results

In this section, we assess the secrecy-rate performance of the proposed RJFS and BF-RJFS algorithms through simulations for the downlink of a multiuser relay system where the relays are equipped with buffers. In a single-antenna scenario, the transmitter is equipped with 3 antennas to broadcast the signal to 3 legitimate users through multiple single-antenna relays in the presence of 3 eavesdroppers equipped with a single antenna. In the MIMO scenario, the transmitter is equipped with 6 antennas and each user, eavesdropper and relay has 2 antennas. When the buffer is implemented at the relay node, the size is set to store 4 symbols unless otherwise specified. In both scenarios, a zero-forcing precoding technique is implemented at the transmitter and we assume that the channel for each user is uncorrelated with the remaining channels and the channel gains are generated following independent and identically distributed complex circular Gaussian random variables with zero mean and unit variance.

We have also examined a scenario with correlated channels, where the correlated channel

matrix is described by

$$\boldsymbol{H}_c = \boldsymbol{R_r}^{\frac{1}{2}} \boldsymbol{H} \boldsymbol{R_t}^{\frac{1}{2}} \tag{5.82}$$

where $\boldsymbol{R_r}$ and $\boldsymbol{R_t}$ are receive and transmit covariance matrices with $\mathrm{Tr}(\boldsymbol{R_r}) = Nr$ and $\mathrm{Tr}(\boldsymbol{R_t}) = Nt$. Both $\boldsymbol{R_r}$ and $\boldsymbol{R_t}$ are positive semi-definite Hermitian matrices.

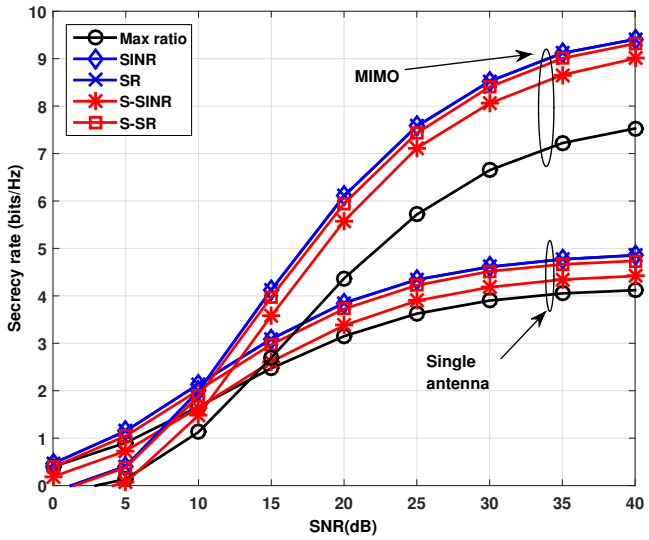

Figure 5.3: Secrecy rate performance of relay selection techniques in uncorrelated channels.

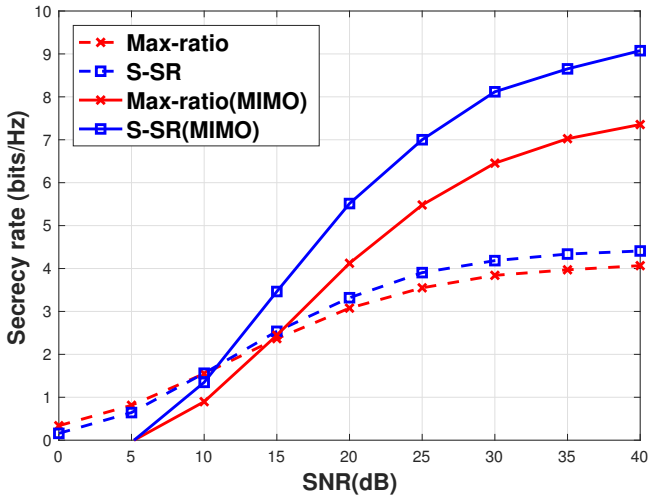

Figure 5.4: Secrecy rate performance of relay selection techniques in uncorrelated channels.

In Figs. 5.3 and 5.4 we assess the secrecy rate performance of the schemes under consideration in uncorrelated and correlated channels, respectively. The results indicate that the proposed relay selection criteria can improve the secrecy rate performance in both scenarios but correlated channels contribute to to the degradation of the performance of all algorithms, as expected. Among all the investigated relay selection criteria, the S-SR criterion achieves the

best performance and does not require the channel state information to the eavesdroppers.

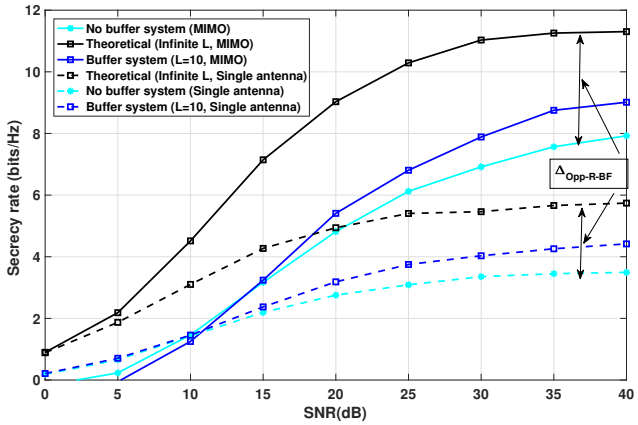

Figure 5.5: Secrecy rate performance with different buffer sizes in uncorrelated channels

In Fig. 5.5, the secrecy rate performance and the theoretical expression obtained in (5.70) are evaluated with no buffer system, infinite buffer size and finite buffers of size $L = 10$. The theoretical curve are obtained with the derived secrecy rate difference $\Delta_{\mathrm{Opp-R-BF}}$ in (5.70) and the secrecy rate curves are obtained by simulations. According to Fig. 5.5, when the buffer size is increased, the secrecy rate will have an improvement and get close to the theoretical curve. Moreover, the parameter $\Delta_{\mathrm{Opp-R-BF}}$ in (5.70) illustrated with the double arrowed line agrees well with difference between the simulated curves.

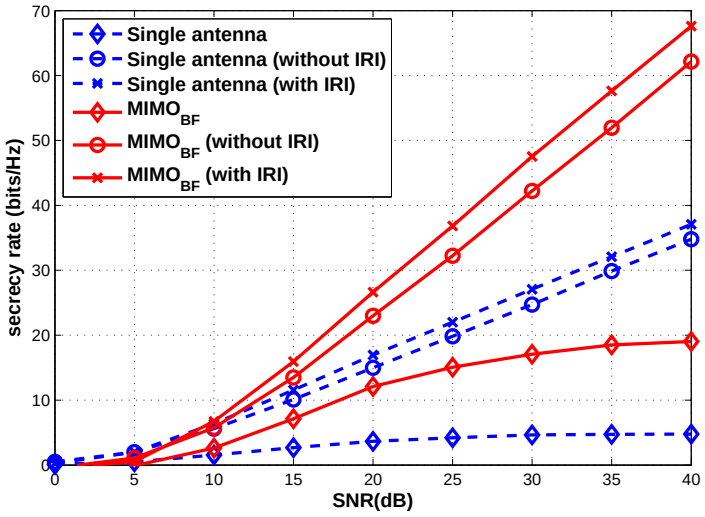

Figure 5.6: Multi-user system scenario

In Figure 5.6, in a single-antenna scenario, the secrecy-rate performance with the proposed algorithm is better than that with the conventional algorithm. With IC, the secrecy-rate performance is better than the one without IC, as expected. Compared with the single-

antenna scenario, the multiuser MIMO system contributes to the improvement in the secrecy rate as verified by the curves in 5.6. In particular, the proposed RJFS algorithm with the selected set of buffer-aided relays (SBF) selection policy is better than the conventional buffer-aided relay selection (BF).

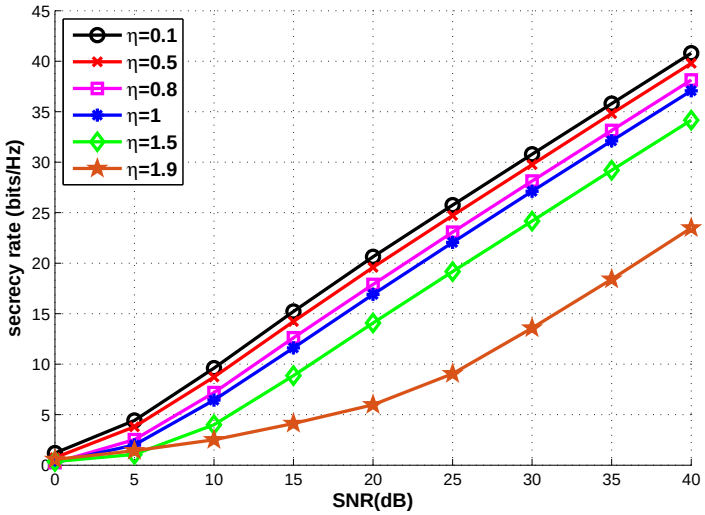

Figure 5.7: Secrecy rate performance with power allocation in IRI cancellation (IC) scenario

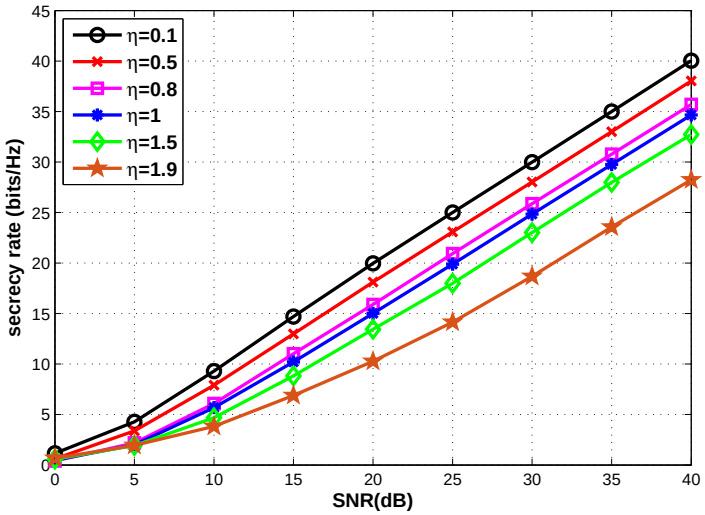

Figure 5.8: Secrecy rate performance with power allocation in existing of IRI scenario

In Figure 5.7 and Figure 5.8, a power allocation technique is considered and the parameter η indicates the power allocated to the transmitter. If we assume in the equal power scenario that the power allocated to the transmitter as well as the relays are both P, then the power allocated to the transmitter is ηP and the power allocated to the relays is $(2-\eta)P$. In Figure 5.7 and Figure 5.8 we can see that with more power allocated to the transmitter the

secrecy-rate performance will become worse. Comparing these two figures, when $\eta < 1.5$ the secrecy-rate performance in the IC scenario is better than that without IC. When $\eta > 1.5$ and without IC, the secrecy rate is improved.

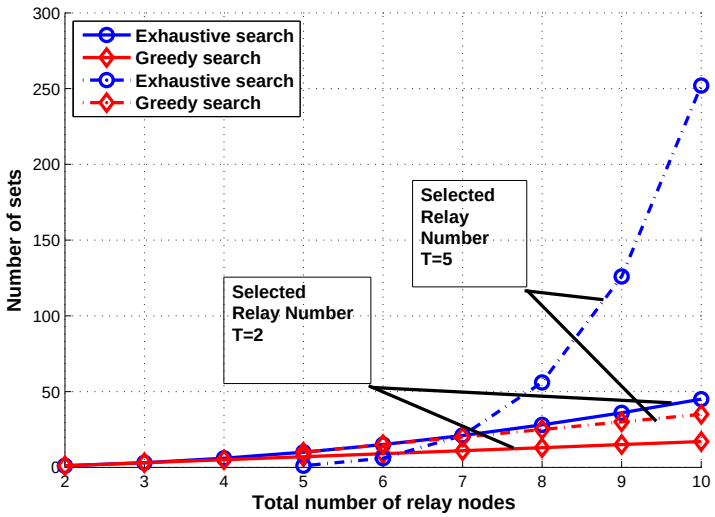

Figure 5.9: Number of visited sets for the exhaustive and greedy searches

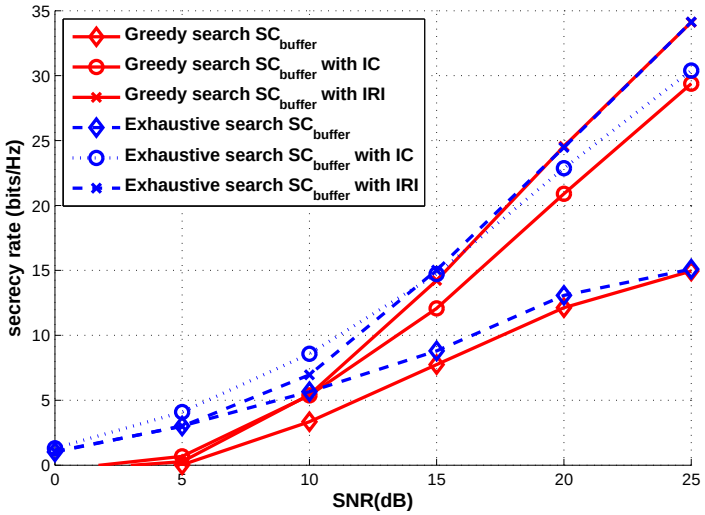

Figure 5.10: Secrecy rate performance with an exhaustive search and the proposed greedy algorithm

In Figure 5.9 with a fixed number of relays, the computational complexity for the exhaustive and the greedy searches with the RJFS and BF-RJFS algorithms is examined. The results show that the proposed greedy algorithms are substantially simpler than those with the exhaustive search and is suitable for scenarios with a higher number of relays. In Figure 5.10 a comparison between the exhaustive search and the proposed greedy algorithms is carried

out. The results show that the proposed greedy algorithms can approach the same secrecy rate performance with a much lower complexity than the exhaustive search-based techniques.

5.6 Summary

In this chapter, we have proposed algorithms to select a set of relay nodes to enhance the legitimate users' transmission and another set of relay nodes to perform jamming of the eavesdroppers. The proposed RJFS and BF-RJFS selection algorithms can exploit the use of the buffers in the relay nodes that may remain silent during the data transmission. Simulation results show that the proposed BF-RJFS can provide a significantly better secrecy rate performance in a multiuser MIMO relay system than existing algorithms for buffer-aided relay systems. In the future, buffer-aided relay nodes will be a key technique for obtaining substantial gains in secrecy rate along with other powerful techniques such physical-layer key generation strategies.

Chapter 6

Conclusions and Further Work

Contents

6.1 Conclusions

This thesis investigates the physical-layer security with downlink multiuser MIMO channels. Under the total power constraint, the secrecy capacity is expressed with channel matrix and covariance matrix [18]. Due to the characteristics of the expression, traditional optimization techniques for convex or concave functions are no longer useful to obtain the secrecy capacity. Our research is then concentrate on the approaches getting optimal transmit covariance matrix.

To start with, some work [17; 10] suggest that precoding techniques can be employed to obtain a sub-optimal result at the transmitter. As illustrated in the literature, non-linear precoding techniques are developed by mitigating interferences and noise effect to achieve the channel capacity. Following the idea, with equal power assumption, non-linear precoding SO-THP+GMI is proposed in the wiretap MIMO channel to obtain a sub-optimal

transmit covariance matrix. The corresponding secrecy rate performance has an outstanding improvement than conventional precoding techniques. Furthermore, extended versions such as SO-THP+S-GMI which is aiming at reducing computational complexity and LR-SO-THP+S-GMI which is capable of achieving full diversity are developed by considering QR decomposition and lattice-reduction respectively in the original developed SO-THP+GMI algorithm [82].

After the study of precoding techniques, to compensate the signal attenuation and provide better spatial application, relays are used to assist the transmission. In the presence of multiple relays, relay selection is a critical technique to maintain optimal transmission performance in terms of a particular metric [42]. As to the physical-layer security, max-ratio is considering eavesdropper's channel coefficients or statistical channel gain at the transmitter to perform a relay selection aiming at improve secrecy rate performance [12]. Based on the idea, we employ different criteria such as SINR or secrecy rate (SR) to achieve better secrecy rate performance. The SINR and SR criteria efficient in improving secrecy rate, however the requirement of channel information to eavesdroppers is hard to achieve. Motivated by releasing the requirement, S-SINR and S-SR criteria are developed to maintain the secrecy rate performance without CSI to eavesdroppers. Thus the optimal relay selection can be implemented to contribute to the secrecy rate performance in MIMO relay system.

Developed from relay system, buffers are employed at each relay to make full use of spatial and temporal advantage [13]. Concurrently, opportunistic scheme is performed instead of half-duplex scheme to further improve the throughput of the system [14]. Assisted with investigated relay selection criteria, novel opportunistic relaying and jamming schemes RJFS and BF-RJFS are proposed by considering jamming technique in the opportunistic scheme. Furthermore, the effect of different power allocation are investigated in terms of secrecy rate performance. At last, due to the high complexity caused by exhaustive search of the relays, greedy search is employed in the relay selection procedure [80].

6.2 Further Work

The future work is consist of two parts. The first one is the continuation and the other is developing new techniques to improve physical-layer security performance in wireless networks.

6.2.1 Continuation

Based on our research, the optimal transmit covariance matrix can be an tough but interesting aspect. Secondly, the relay systems can be extended to multi-layer relay systems or ad-hoc systems. Concurrently, some latest techniques such as massive MIMO, lattice construction are also drawing more attention in the physical-layer research.

6.2.2 Ideas

As an conclusion, current works are exploring the technique which exploits the differences of channel characteristics between the main channel and wire-tap channel.

My ideas of the future developments about physical-layer security can be located into two critical aspects. The first one is following traditional encryption techniques. Physical-layer key generation, for instance, is a technique generating keys with different channel characteristics. With shared keys between transmitter and receiver, the wireless transmission can be secured. In [84], different passive and active attacks are analyzed with the consideration of applying physical-layer key generation, A new key generation scheme using random probing signals, and combining user generated randomness and channel randomness, is introduced as a countermeasure against active attacks. Also in [85], a secret key generation based on tracking channel evolution in time division duplex systems is introduced and the information theoretic limits of this key generation schemes are investigated.

Another idea is hiding the transmission which means the eavesdropper is unaware of the transmission or in another word don't know which transmitter to eavesdrop. Although this is even harder to achieve than ensuring secure transmission, if the eavesdropper does not know the transmission occurs, the transmission is definitely secure. To implement the idea, with multiple base stations, distributed algorithms would be a good idea. By transmitting the signals with multiple based stations, it would be rather difficult for the eavesdropper to detect all the transmitted signals. Then distributed algorithms can be employed to accomplish the task of hiding the transmission.

Appendix A

Derivation for Optimal Artificial Noise

Contents

If we consider $\rho\boldsymbol{A} = \boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H$ and $(\boldsymbol{Q}_s')^{-1}\boldsymbol{Q}_s = \rho/(1-\rho)\boldsymbol{I}$, (3.38) can be rewritten as

$$\log(\det(\boldsymbol{I} + \rho\boldsymbol{A})) - \log(\det(\boldsymbol{I} + \rho/(1-\rho)\boldsymbol{I}), \tag{A.1}$$

Here we first take the derivative of $\log(\det(\boldsymbol{I} + \rho\boldsymbol{A}))$ with respect to ρ and assume that $\boldsymbol{A}$ is an $m \times m$ matrix. The eigenvalues of the matrix $\boldsymbol{I} + \rho\boldsymbol{A}$ are $1 + \rho a_1, 1 + \rho a_2, \cdots 1 + \rho a_m$. The eigenvalues of the matrix $\boldsymbol{A}(\boldsymbol{I} + \rho\boldsymbol{A})^{-1}$ are $\frac{a_1}{1+\rho a_1}$, $, \frac{a_2}{1+\rho a_2}$, $\cdots$ $\frac{a_m}{1+\rho a_m}$. With these relations, we have

$$\det(\boldsymbol{I} + \rho\boldsymbol{A}) = (1 + \rho a_1)(1 + \rho a_2)\cdots(1 + \rho a_m), \tag{A.2}$$

and

$$\mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1}) = \frac{a_1}{1+\rho a_1} + \frac{a_2}{1+\rho a_2} + \cdots + \frac{a_m}{1+\rho a_m}. \tag{A.3}$$

The derivative of $\log(\det(\boldsymbol{I}+\rho\boldsymbol{A}))$ with respect to ρ can be expressed as

$$\begin{aligned}
\frac{d\{\log(\det(\boldsymbol{I}+\rho\boldsymbol{A}))\}}{d\rho} &= \frac{d\{\log((1+\rho a_1)(1+\rho a_2)\cdots(1+\rho a_m))\}}{d\rho}, \\
&= \frac{d\{\log(1+\rho a_1)\}}{d\rho} + \frac{d\{\log(1+\rho a_2)\}}{d\rho} + \cdots + \frac{d\{\log(1+\rho a_m)\}}{d\rho}, \\
&= (\frac{a_1}{1+\rho a_1} + \frac{a_2}{1+\rho a_2} + \cdots + \frac{a_m}{1+\rho a_m})\ln(2), \\
&= \mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2).
\end{aligned} \tag{A.4}$$

Similarly, the derivative of $\log(\det(\boldsymbol{I}+\rho/(1-\rho)\boldsymbol{I})$ with respect to ρ is given by $\mathrm{Tr}(\boldsymbol{I})\ln(2)$. The optimal value of ρ can be obtained by calculating

$$\mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2) - \mathrm{Tr}(\boldsymbol{I})\ln(2) = 0 \tag{A.5}$$

which is equivalent to

$$(1-\rho)\boldsymbol{A} = \boldsymbol{I}. \tag{A.6}$$

By substituting $\boldsymbol{A}$ in $\frac{1}{\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H$, (A.6) can be rewritten as

$$(\frac{1}{\rho}-1)\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H = \boldsymbol{I}. \tag{A.7}$$

Given the constraints $\mathrm{Tr}(\boldsymbol{Q}_\mathrm{s}) = \rho E_s$ and $\boldsymbol{H}_{ba} \in \mathcal{CN}(0,1)$, in the simulation scenario, we can solve (A.7) as

$$4(\frac{1}{\rho}-1)\rho^2 = 1. \tag{A.8}$$

The optimal value is achieved at $\rho = 0.5$. However, due to the existence of Gaussian noise, the optimal value is shifted. Based on (A.5), we focus on the first term $\mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2)$. It can be rewritten as $\mathrm{Tr}((\boldsymbol{A}^{-1})^{-1}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2)$. Finally, we have

$$\mathrm{Tr}(\boldsymbol{A}^{-1}+\rho\boldsymbol{I})\ln(2), \tag{A.9}$$

when considering Gaussian noise, $\boldsymbol{A} = \frac{1}{\sigma_n^2\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H$. Here σ_n^2 represents the variance of the noise. When the signal variance is set to 1, we can have $\sigma_n^2 < 1$. If we use the matrix $\boldsymbol{N}_a$ to represent the effect of noise, we can employ $\boldsymbol{A} = \frac{1}{\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H + \boldsymbol{N}_a$, where the elements

in $\boldsymbol{N}_a$ are positive. Substituting $\boldsymbol{A}$ by $\frac{1}{\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H + \boldsymbol{N}_a$, (A.6) can be obtained as

$$(\frac{1}{\rho} - 1)(\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H + \boldsymbol{N}_a) = \boldsymbol{I}. \tag{A.10}$$

Comparing (A.7) with (A.10), it can be verified that the optimal value of (A.10) is achieved at a higher value of ρ which is 0.6 in our simulation.

Glossary of Terms

AF	Amplify-and-Forward
AN	Artificial Noise
BD	Block Diagonalization
BER	Bit Error Rate
BF-RJFS	Buffer-aided Relaying and Jamming Function Selection
CSI	Channel State Information
DF	Decode-and-Forward
FLOPS	Floating-Point Operations Per Second
GMI	Generalized MMSE channel inversion
IC	Inter-Relay Interference Cancellation
LR	Lattice Reduction
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MMSE	Minimum Mean Square Error
RJFS	Relaying and Jamming Function Selection
SIMO	Single-Input Multiple-Output

SINR	Signal-to-interference-plus-noise ratio
SISO	Single-Input Single-Output
SNR	Signal-to-noise ratio
SO	Successive Optimization
SR	Secrecy Rate
SVD	Singular Value Decomposition
THP	Tomlinson-Harashima Precoding
ZF	Zero Forcing

Bibliography

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, p. 1385 1357, October 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with condential messages," *IEEE Transcations on Information Theory*, vol. 24, no. 3, p. 339 348, May 1978.

[3] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transcations on Wireless Communications*, vol. 7, no. 6, pp. 2180 – 2189, June 2008.

[4] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[5] Y. Cai, D. L. Ruyet, R. C. de Lamare, and D. Roviras, "Linear precoding based on switched relaying processing for multiuser MIMO relay systems," *IEEE 12th International Workshop, Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 351 – 355, June 2011.

[6] K. Zu, R. C. de Lamare, and M. Haart, "Generalized design of low-complexity block diagonalization type precoding algorithms for multiuser MIMO systems," *IEEE Transactions on Communications*, vol. 61, no. 10, pp. 4232 – 4242, November 2013.

[7] C. Wang, E. Au, R. Murch, W. Mow, R. Cheng, and V. Lau, "On the Performance of the MIMO Zero-Forcing Receiver in the Presence of Channel Estimation Error," *IEEE Transactions on Wireless Communications*, vol. 6, no. 3, pp. 805 – 810, March 2007.

[8] J. Huang and A. L. Swindlehurst, "Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization, year=2012, volume=60, number=4, pages=1696-1707, month=April,," *IEEE Transactions on Signal Processing.*

[9] S. Shafiee, N. Liu, and S. Ulukus, "Towards the Secrecy Capacity of the Gaussian MIMO Wire-Tap Channel: The 2-2-1 Channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Sept 2009.

[10] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, July 2012, pp. 2321–2325.

[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[12] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. Chambers, "Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 719–729, April 2014.

[13] J. Huang and A. Swindlehurst, "Wireless physical layer security enhancement with buffer-aided relaying," in *Asilomar Conference on Signals, Systems and Computers, 2013*, Nov 2013, pp. 1560–1564.

[14] N. Nomikos, T. Charalambous, I. Krikidis, D. Skoutas, D. Vouyioukas, and M. Johansson, "Buffer-aided successive opportunistic relaying with inter-relay interference cancellation," in *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), 2013*, Sept 2013, pp. 1316–1320.

[15] N. Nomikos, P. Makris, D. Vouyioukas, D. Skoutas, and C. Skianis, "Distributed joint relay-pair selection for buffer-aided successive opportunistic relaying," in *IEEE 18th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2013*, Sept 2013, pp. 185–189.

[16] I. Krikidis, J. S. Thompson, P. M. Grant, and S. McLaughlin, "Power allocation for cooperative-based jamming in wireless networks with secrecy constraints," in *2010 IEEE Globecom Workshops*, Dec 2010, pp. 1177–1181.

[17] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding," *IEEE Transcations on Communications*, vol. 60, no. 11, pp. 3472 – 3482, November 2012.

[18] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE International Symposium on Information Theory*, pp. 524 – 528, July 2008.

[19] W. C. Jakes, *Diversity Techniques.* Wiley-IEEE Press, 1974, pp. 389–544.

[20] B. Sklar, *Digital communications.* Prentice Hall NJ, 2001, vol. 2.

[21] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Technical Journal*, vol. 1, no. 2, pp. 41–59, Autumn 1996.

[22] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-BLAST: an architecture for realizing very high data rates over the rich-scattering wireless channel," in *Signals, Systems, and Electronics, 1998. ISSSE 98. 1998 URSI International Symposium on*, Sep 1998, pp. 295–300.

[23] A. Paulraj, R. Nabar, and D. Gore, *Introduction to space-time wireless communications.* Cambridge university press, 2003.

[24] Y. Cai, R. C. de Lamare, L. L. Yang, and M. Zhao, "Robust MMSE Precoding Based on Switched Relaying and Side Information for Multiuser MIMO Relay Systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5677–5687, Dec 2015.

[25] A. P. Millar, S. Weiss, and R. W. Stewart, "Precoder Design for MIMO Relay Networks with Direct Link and Decision Feedback Equalisation," *IEEE Communications Letters*, vol. 15, no. 10, pp. 1044–1046, October 2011.

[26] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[27] R. V. L. Hartley, "Transmission of Information1," *Bell System Technical Journal*, vol. 7, no. 3, pp. 535–563, 1928.

[28] N. Chiurtu, B. Rimoldi, and E. Telatar, "On the capacity of multi-antenna Gaussian channels," 2001.

[29] G. Golub and C. V. Loan, *Matrix Computations*, ser. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, 1996.

[30] K. Zu and R. C. de Lamare, "Low-Complexity Lattice Reduction-Aided Regularized Block Diagonalization for MU-MIMO Systems," *IEEE Communications Letters*, vol. 16, no. 6, pp. 925 – 928, June 2012.

[31] V. Stankovic and M. Haardt, "Successive optimization Tomlinson-Harashima precoding (SO THP) for multi-user MIMO systems," *IEEE International Conference, Proceedings. (ICASSP '05)*, vol. 3, pp. 1117 – 1120, March 2005.

[32] M. Huang, S. Zhou, and J. Wang, "Analysis of Tomlinson-Harashima Precoding in Multiuser MIMO Systems With Imperfect Channel State Information," September 2008.

[33] R. D. Wesel and J. M. Cioffi, "Achievable rates for Tomlinson-Harashima precoding," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 824–831, Mar 1998.

[34] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 461–471, Feb 2004.

[35] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2658–2668, Oct 2003.

[36] W. Yu and J. M. Cioffi, "Sum capacity of Gaussian vector broadcast channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 1875–1892, Sept 2004.

[37] G. Caire and S. Shamai, "On achievable rates in a multi-antenna Gaussian broadcast channel," in *Information Theory, 2001. Proceedings. 2001 IEEE International Symposium on*, 2001.

[38] S. Hakjea, L. Sang-Rim, and L. Inkyu, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Transactions on Communications*, vol. 57, no. 11, pp. 3489 – 3499, November 2009.

[39] V. Stankovic and M. Haardt, "Generalized Design of Multi-User MIMO Precoding Matrices," *IEEE Transcations on Wireless Communications*, vol. 7, no. 3, pp. 953 – 961, March 2008.

[40] H. Yao and W. Wornell, "Lattice-reduction-aided detectors for MIMO communication systems," *Global Telecommunications Conference*, vol. 1, pp. 424 – 428, November 2002.

[41] S. Liu, Y. Hong, and E. Viterbo, "Practical Secrecy using Artificial Noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483 – 1486, May 2013.

[42] T. Hesketh, R. C. de Lamare, and S. Wales, "Joint partial relay selection, power allocation and cooperative maximum likelihood detection for MIMO relay systems with

limited feedback," in *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th.* IEEE, 2013, pp. 1–5.

[43] Y. Saeed, M. Imran, and O. Waqar, "Energy efficiency of base station cooperation using amplify-and-forward relay protocol," in *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, Oct 2015, pp. 37–41.

[44] L. Han, S. Shao, Y. Shen, C. Qing, and Y. Tang, "Outage Probability and Power Allocation for Amplify-and-Forward Cooperative Relaying Systems with Correlated Shadowing," in *Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th*, Sept 2013, pp. 1–5.

[45] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 379–389, February 2007.

[46] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[47] Y. Oohama, "Capacity Theorems for Relay Channels with Confidential Messages," in *IEEE International Symposium on Information Theory (ISIT) 2007.*, June 2007, pp. 926–930.

[48] Y. Zhao, R. Adve, and T. J. Lim, "Symbol error rate of selection amplify-and-forward relay systems," *IEEE Communications Letters*, vol. 10, no. 11, pp. 757–759, November 2006.

[49] T. Wang, A. Cano, G. B. Giannakis, and J. N. Laneman, "High-Performance Cooperative Demodulation With Decode-and-Forward Relays," *IEEE Transactions on Communications*, vol. 55, no. 7, pp. 1427–1438, July 2007.

[50] Y. Zhu, X. Wu, and T. Zhu, "Hybrid AF and DF with network coding for wireless Two Way Relay Networks," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2013, pp. 2428–2433.

[51] N. Zlatanov and R. Schober, "Buffer-Aided Relaying With Adaptive Link Selection-Fixed and Mixed Rate Transmission," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2816–2840, May 2013.

[52] J. Huang and A. Swindlehurst, "Wireless physical layer security enhancement with buffer-aided relaying," in *Asilomar Conference on Signals, Systems and Computers, 2013*, Nov 2013, pp. 1560–1564.

[53] X. Shang and H. V. Poor, "Capacity for MIMO Gaussian interference channels with generally strong and noisy interference," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, July 2012, pp. 2786–2790.

[54] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian Wiretap Channel With a Cooperative Jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, Oct 2011.

[55] ——, "Competing for Secrecy in the MISO Interference Channel," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 170–181, Jan 2013.

[56] *Large MIMO Systems, author=Chockalingam, A. and Rajan, B.S., year=2014, publisher=Cambridge University Press.*

[57] M. Payaro, A. Perez-Neira, and M. Lagunas, "Achievable rates for generalized spatial Tomlinson-Harashima precoding in MIMO systems," *IEEE 60th Vehicular Technology Conference*, vol. 4, pp. 2462 – 2466, 2004.

[58] M. Mazrouei-Sebdani and W. Krzymien, "Vector Perturbation Precoding for Network MIMO: Sum Rate, Fair User Scheduling, and Impact of Backhaul Delay," *IEEE Transcations on Vehicular Technology*, vol. 61, no. 9, pp. 3946 – 3957.

[59] P. Lin, S. Lai, and S. Lin, "On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, September 2013.

[60] A. Chorti and H. Poor, "Achievable secrecy rates in physical layer secure systems with a helping interferer," *Computing, Networking and Communications (ICNC)*, pp. 18 – 22, Feb 2012.

[61] A. Mukherjee and A. Swindlehurst, "Jamming Games in the MIMO Wiretap Channel With an Active Eavesdropper," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82 – 91, Jan 2013.

[62] M. Taherzadeh, A. Mobasher, and A. Khandani, "LLL Reduction Achieves the Receive Diversity in MIMO Decoding," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4801 – 4805, December 2007.

[63] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multi-cell massive MIMO systems," in *2013 IEEE Globecom Workshops (GC Wkshps)*, Dec 2013, pp. 1286–1291.

[64] F. Dietrich, P. Breun, and W. Utschick, "Robust TomlinsonHarashima Precoding for the Wireless Broadcast Channel," *IEEE Transactions on Signal Processing*, vol. 55, no. 2, pp. 631 – 644, Feb 2007.

[65] M. Costa, "Writing on dirty paper," *IEEE Transcations on Information Theory*, vol. 29, no. 3, pp. 439 – 441, May 1983.

[66] K. Zu, R. C. de Lamare, and M. Haardt, "Multi-Branch Tomlinson-Harashima Precoding Design for MU-MIMO Systems: Theory and Algorithms," *IEEE Transcations on Communications*, vol. 62, no. 3, pp. 939 – 951, March 2014.

[67] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure Transmission for Multiuser Relay Networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3724–3737, July 2015.

[68] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46–49, February 2015.

[69] T. T. Duy, T. Q. Duong, T. L. Thanh, and Q. B. V. Nguyen, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Communications*, vol. 9, no. 11, pp. 1427–1435, 2015.

[70] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, January 2015.

[71] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-Aided Relay Selection for Cooperative Diversity Systems without Delay Constraints," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1957–1967, May 2012.

[72] Q. H. Spencer and M. Haardt, "Capacity and downlink transmission algorithms for a multi-user MIMO channel," in *Signals, Systems and Computers, 2002. Conference Record of the Thirty-Sixth Asilomar Conference on*, vol. 2, Nov 2002, pp. 1384–1388.

[73] X. He and A. Yener, "Providing Secrecy Irrespective of Eavesdropper's Channel State," in *Proceedings of 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010, pp. 1–5.

[74] D. Bernstein, *Matrix Mathematics: Theory, Facts, and Formulas (Second Edition)*, ser. Princeton reference. Princeton University Press, 2009.

[75] N. Nomikos, T. Charalambous, I. Krikidis, D. N. Skoutas, D. Vouyioukas, M. Johansson, and C. Skianis, "A Survey on Buffer-Aided Relay Selection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1073–1097, Secondquarter 2016.

[76] A. E. Shafie, D. Niyato, and N. Al-Dhahir, "Enhancing the PHY-Layer Security of MIMO Buffer-Aided Relay Networks," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 400–403, Aug 2016.

[77] A. E. Shafie, A. Sultan, and N. Al-Dhahir, "Physical-Layer Security of a Buffer-Aided Full-Duplex Relaying System," *IEEE Communications Letters*, vol. 20, no. 9, pp. 1856–1859, Sept 2016.

[78] J. H. Lee and W. Choi, "Multiuser Diversity for Secrecy Communications Using Opportunistic Jammer Selection: Secure DoF and Jammer Scaling Law," *IEEE Transactions on Signal Processing*, vol. 62, no. 4, pp. 828–839, Feb 2014.

[79] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint Relay and Jammer Selection for Secure Two-Way Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb 2012.

[80] X. Lu and R. C. de Lamare, "Opportunistic relay and jammer cooperation techniques for physical-layer security in buffer-aided relay networks," in *2015 International Symposium on Wireless Communication Systems (ISWCS)*, Aug 2015, pp. 691–695.

[81] C. Windpassinger, R. F. H. Fischer, T. Vencel, and J. B. Huber, "Precoding in multi-antenna and multiuser communications," *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1305–1316, July 2004.

[82] X. Lu, K. Zu, and R. C.de Lamare, "Lattice-reduction aided Successive Optimization Tomlinson-Harashima Precoding strategies for physical-layer security in wireless networks," in *Sensor Signal Processing for Defence (SSPD), 2014*, Sept 2014, pp. 1–5.

[83] Z. K, R. de Lamare, and M. Haardt, "Multi-Branch Tomlinson-Harashima Precoding Design for MU-MIMO Systems: Theory and Algorithms," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 939–951, March 2014.

[84] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, June 2015.

[85] J. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits," in *2009 IEEE International Conference on Communications*, June 2009, pp. 1–5.