ACHIEVING PHYSICAL LAYER SECURITY IN MULTI-ANTENNA WIRETAP CHANNELS

XIONG QI

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfillment of the requirement for the degree of
Doctor of Philosophy

2016

Acknowledgements

First and foremost, I would like to take this opportunity to express my deepest and sincerest thanks to my supervisor, Dr. Liang Ying Chang from Institute for Infocomm Research (I^2R). Four years ago when I begun the journey to pursue my Ph.D degree in Nanyang Technological University (NTU), conducting the academic research was an absolute challenge to me as a fresh graduate. From time to time, I learned from his patient guidance and benefited from his abundant professional knowledge. This thesis would not be even possible if it has not been with his valuable supervisions. The unforgettable experience of working with him will place a persistent influence on my future career.

Secondly, I feel greatly grateful to my supervisor, Prof. Li Kwok Hung from NTU, for his extreme patience and valuable time taken in discussing my research works and reviewing my papers. My special appreciations go to Prof. Gong Yi from South University of Science and Technology of China (SUSTC) for the opportunity he gave me to start my Ph.D study and guided me in the early years.

Next, I would like to thank my fellow groupmates, Dr. Han Shiying, Mr. Yang Gang, Dr. Pei Yiyang, Dr. Kang Xin, Dr. Che Yueling, Dr. Cai Shensming and Dr. Tian Jian, for discussions in our group meetings and valuable advices on my research.

My special gratitude goes to Nanyang Technological University, which provided me the financial support to finish my Ph.D studies and the precious opportunities to attend the international conferences. I would also like to make a grateful acknowledgement for many professors and researchers from NTU and I^2R for inviting the top scientists and

researchers abroad to give various useful seminars in Singapore. Both the conferences and the seminars have greatly richen my knowledge on the state-of-the-art research in the area, and was very helpful in sparkling new ideas and developing my research.

Lastly but not least, most significant appreciation of all goes to my parents, my sister and my lovely girlfriend *L*ena for their consistent love and support throughout my past life.

Contents

Abstract

Achieving secure transmission in wireless network is a significantly important research topic. Classic cryptography encrypts a confidential message to an unreadable cipher message. Thus only the authentic receiver with correct secrecy key is able to decrypt the message. However, with the growing computational capability of adversaries, the requirement of secrecy key generation and distribution is getting stringent. Another method to achieve wireless security, which has attracted much attention in recent years, is through physical layer processing, named physical layer security. In a typical wiretap channel model consisting of a transmitter, a legal receiver and an adversary (illegal receiver), early works have proven that it is possible to achieve positive secrecy rate using multiple antenna techniques, such as beamforming, at the transmitter. In this thesis, we focus on two types of malicious behaviors of the adversary: passive eavesdropping and active attack.

For the passive eavesdropping, we first consider the multi-input-single-output (MISO) wiretap channel, in which the legitimate transmitter utilizes the artificial noise aided precoding strategy to maximize the achievable secrecy rate of the channel. Both scenarios of known and unknown channel state information (CSI) for the eavesdropper channels are considered. By deriving the closed-form expression of ergodic secrecy rate, we prove that there exists an optimal power ratio between the information signal and the artificial noise. We then extend our study to a four-node fading channel model in a wireless relay network, which includes two single-antenna users, one single-antenna eavesdropper and one relay node equipped with multiple antennas. By studying the

decode-and-forward (DF) scheme, cooperative jamming (CJ) scheme and one proposed hybrid relay scheme, relay-and-jamming (RJ), we aims to find the optimal relay scheme with the condition that the transmitter and the relay node are under individual power constraints and the CSI of the illegitimate channel is only statistically known. Our analysis shows that the hybrid RJ scheme is optimal when the transmitter has a relatively small power budget and/or the transmitter is far away from the intended receiver.

Besides the passive eavesdropping, the adversary could also choose the active attack. The pilot spoofing attack is one active attack conducted by the adversary during the channel estimation phase of the legitimate transmission. In practical systems, the pilot signals are usually known *a priori* and repeatedly used information. In this attack, an intelligent adversary spoofs the transmitter on the estimation of CSI by sending the identical pilot signal as the legitimate receiver. By doing so, the adversary could obtain a larger channel rate in the data transmission phase, and also drastically weaken the strength of the received signal at the legitimate receiver if the adversary utilizes large enough power. Due to the serious consequences caused by such an attack, we first propose an energy ratio detector (ERD) that explores the asymmetry of received signal power levels at the transmitter and the legitimate receiver when the attack occurs. Our analysis shows that the ERD could provide very high probability of detection with certain requirement on the false alarming probability. Furthermore, we design a two-way training based scheme to provide not only attack detection but also secure transmission. The two-way training based detector (TWTD) exploits the intrusive component created by the adversary, followed by a secure beamforming-assisted data transmission. In addition to the good detection performance, our scheme could estimate both legitimate and illegitimate channels, with which the beamforming could be designed for data transmission.

List of Figures

List of Tables

List of Abbreviations

AF	amplify-and-forward
AN	artificial noise
ANaP	artificial noise aided precoding
AP	access point
AWGN	additive white Gaussian noise
CJ	cooperative jamming
CR	cooperative relaying
CRN	cognitive radio network
CSCG	circularly symmetric complex Gaussian
CSI	channel state information
DCE	discriminatory channel estimation
DF	decode-and-forward
DMC	discrete memoryless channel
DwPTS	downlink pilot time slot
ERD	energy ratio detector
i.i.d.	independent and identically distributed
LMMSE	linear minimum mean square error
LS	least square
MF	match-and-forward
MIMO	multiple-input multiple-output

MISO	multiple-input single-output
MRT	maximum ratio transmission
NMSE	normalized mean squared error
PDF	probability density function
PSK	phase-shift keying
QoS	quality-of-service
RCI	regularized channel inversion
RJ	relaying-and-jamming
RSS	received signal strength
SDP	semi-definite program
SINR	signal-to-interference-plus-noise ratio
SISO	single-input single-output
SNR	signal-to-noise ratio
SOP	secrecy outage probability
SRM	secrecy-rate maximization
s.t.	subject to
TDD	time duplex division
UpPTS	uplink pilot time slot
w.r.t.	with respect to
ZF	zero-forcing

List of Notations

x	scalar value
$\mathbf{x}$	vector
$\mathbf{X}$	matrix
$\mathcal{CN}(0, \sigma^2)$	the distribution of a CSCG random variable with zero mean and variance σ^2
$\mathbb{C}^{M \times N}$	the complex space of a matrix of dimension $M \times N$
$H(\cdot)$, $H(\cdot\|\cdot)$	the entropy, the conditional entropy
$I(\cdot, \cdot)$	the mutual information
$\max\ f(x)$	the value of x that maximizes the function $f(x)$
$E[\cdot]$	the expectation operator
$\mathcal{Q}(\cdot)$	the $\mathcal{Q}$-function, i.e., $\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp\left(-\frac{t^2}{2}\right) dt$
$\mathrm{Re}(x)$	the real part of x
$\mathrm{Im}(x)$	the imaginary part of x
$\lceil x \rceil$	the smallest integer not less than x
$\|\mathbf{x}\|$	the Euclidean norm of vector $\mathbf{x}$
$\mathbf{X}^H$	the Hermitian transpose of matrix $\mathbf{X}$
$\mathrm{tr}(\mathbf{X})$	the trace of matrix $\mathbf{X}$
$\mathbf{X} \succeq 0$	matrix $\mathbf{X}$ is positive semidefinite
$\mathbf{I}_N$	the $N \times N$ identity matrix

Chapter 1

Introduction

1.1 Physical Layer Security

Along with the rapid development of mobile communications, billions of people around the world enjoy the convenient services provided by mobile networks. With the deployment of 4G and future 5G mobile networks. People can access the Internet whenever and wherever they want, to follow up the latest news, work on their business, enjoy multimedia and so on. Since the wireless networks are connected to our daily lifes, there is a growing demand to protect our confidential information from being eavesdropped or attacked. Therefore, one of the most important problems is to keep the communications in the wireless network secure.

Conventional methods of achieving secure communications are based on the cryptography methods[1]. The basic idea is to utilize a secrecy key to encrypt the secret information at the transmitter side, while the legitimate receiver could use the corresponding secrecy key to decrypt the cipher-message. Due to the lack of the secrecy key or insufficient computation capability, the eavesdropper could not decode the encrypted information. However, the cryptographic method would experience some significant challenges, such as the increasing complicated network infrastructure will raise higher and higher demand of key management, the vastly increasing computational capabil-

ity will allow potential eavesdroppers to have greater possibility to crack the secrecy key. With the certain considerations aforementioned, physical layer security, which try to achieve secure communication via information theoretical prospective, has received great attention in recent years. This information theoretical approach will allow transmitter to send confidential information without using encryption keys and keep the message confidential no matter how strong computation capability the eavesdropper has. The physical layer security (also known as information theoretical security) was initiated by Shannon's work [2] more than 60 years ago. Wyner introduced the classic wiretap channel model in [3] and this model was extended to general broadcast channel by Csiszár and Körner in [4]. These models will be discussed in more details in the following sections.

Figure 1.1: An illustration of information theoretical security.

The core essence of the physical layer security is to study the difference between the wireless channel to legal receiver and the wireless channel to eavesdropper as well as apply the randomness (such as fading, etc.) of physical medium to encoding process. By doing so, the transmitter expects to protect the confidential messages from being eavesdropped or attacked by illegal users. Figure 1.1 illustrate the communication model utilizing information theoretical security. From the figure, the first step, stochastic encoding contains the process of adding structure randomness into the encoding procedure [5]. When compared to the communication system using the encryption method, the stochastic coding process eliminates the key management problem and therefore reduces the resource consumption and system complexity. On the other hand, the two methods could merge to help each other. For example, the wireless channel information could be used as a natural source of secrecy key. Again, we have to emphasize that physical layer method and cryptographic method are two different perspective to provide security, the latter method is more like in the high-layer. In this thesis, we will mainly focus on how to achieve secure communication via information theoretical

method, rather than cryptographic encryption or combination of both two approaches.

1.2 Wiretap Channel Model

In this chapter, the basic wiretap channel model for study secure communication will be introduced. The wiretap channel was first proposed in Wyner's work in [3], and then extended to general channel by Csiszár and Körner in [4]. In recent years, the secure communication problem studied from the information theoretical perspective has received increasing attention and the problem has been combined with new technologies, such as the multiple antenna techniques. In the later part of this chapter, the wiretap channel models with multiple antennas will be discussed.

1.2.1 Basic Wiretap Channel

The information entropy rate was first introduced by Shannon in [2], which is the basic evaluation approach to measure the capacity of one communication channel. Extended from this information entropy rate measurement, Wyner proposed the basic measurement of secure communication channel with noise, which is the secrecy rate (perfect secrecy) within the wiretap channel model. As depicted in Figure 1.2, the basic wiretap channel model contains three parts, one transmitter (Alice), one legitimate receiver (Bob) and one eavesdropper (Eve). The following communication scenario is considered, Alice intends to send confidential message to Bob and keeps it from being interpreted by the potential eavesdropper Eve. At the transmitter side, Alice applies a $(2^{nR}, n)$ (transmission rate R in n channel use) code sequence for transmission, and the message W is uniformly distributed in the message set $\mathcal{W} = \{1, 2, ..., 2^{nR}\}$. The encoding process maps every message $w \in \mathcal{W}$ to a codeword $x^n = (x_1, ..., x_n)$, and the message is transmitted over the discrete memoryless channel (DMC) whose transmission probability is represented as $P_{YZ|X}$, then at the receiver side, Bob uses

the same codebook to decode the received message $y^n = (y_1, ..., y_n)$ and maps it to the message $w \in \mathcal{W}$, which is represented as $\hat{w}$. In Fig. 1.2 $z^n = (z_1, ..., z_n)$ denotes the received signal sequence at the eavesdropper's side.

Figure 1.2: The illustration of basic wiretap channel.

For this wiretap channel, the reliability of the communication is quantified by the average probability of error for the code of length-n, which is:

$$P_e^{(n)} = \Pr\{\hat{W} \neq W\}, \tag{1.1}$$

where $\hat{W}$ represents the decision made by the legitimate receiver and the transmitter sends out the message W. On the other hand, the secure level of this communication model is represented by the equivocation rate, which is given by

$$R_e^{(n)} = \frac{1}{n} H(W|Z^n), \tag{1.2}$$

where Z^n and W denote the channel outputs at the eavesdropper and the inputs at the transmitter, respectively, and conditional entropy $H(W|Z^n)$ represents the unknown part of W for given Z^n. Therefore, the equivocation rate describes the eavesdropper's uncertainty level about the confidential message sent from the transmitter. It is clear to see that if the equivocation rate is higher, the secrecy degree of the communication will be higher.

In this thesis, our interests are more focused on studying how to achieve the secrecy rate (also known as the case of perfect secrecy). Perfect secrecy indicates that the confidential information sent by transmitter could be completely hidden from eavesdroppers. The secrecy rate is considered as obtainable if there is a sequence of code $(2^{nR}, n)$ and proper encoder-decoder pairs that the average error probability $P_e^{(n)} \to 0$

when $n \to \infty$ as well as the transmission rate R satisfies

$$R \leq \liminf_{n\to\infty} R_e^n. \tag{1.3}$$

The secrecy capacity C_s is defined as the highest achievable rate, i.e., $C_s = \max R$. It's worth noting that perfect secrecy here does not require every bit of the information to be kept secret from eavesdroppers, but it ensures that the unsecured part of information could not achieve a positive rate.

Furthermore, Csiszár and Körner generated the single-letter expression of secrecy capacity in [4] for a general wiretap channel:

$$C_s = \max_{\mathbb{P}_{UX}\mathbb{P}_{YZ|X}} \{I(U;Y) - I(U;Z)\}, \tag{1.4}$$

where U is an auxiliary random variable that is satisfying the Markov chain $U \to X \to (Y, Z)$. X represents the input of the channel, which in some case the transmitter builds a prefix channel from U to the channel input X so that usually it can have $U \equiv X$. Moreover, $\mathbb{P}$ denotes the probability density function (PDF). For the details on proof of such certain communication scheme exists, which are the *achievability proof* (which means the secrecy capacity is achievable) and the *converse proof*, to prove the optimality of the secrecy capacity could be referred in the monograph on information theoretic security by Liang etc. in [5].

According to the expression (1.4) above, the secrecy capacity is described as the largest difference between channel rate $I(U;Y)$ of the transmitter-receiver channel and the channel rate $I(U;Z)$ of the transmitter-eavesdropper channel. Note that in the original study of wiretap channel by Wyner, the transmitter-eavesdropper channel is a degraded version of the transmitter-receiver channel, i.e., X, Y, Z satisfy such Markov chain $X \to Y \to Z$ and $\mathbb{P}_{Z|X} = \mathbb{P}_{Y|X}\mathbb{P}_{Z|Y}$. In the work of Csiszár and Körner, the broadcast channel is assumed to be a general version rather than a degraded version.

However, the above results are generated based on point to point single-antenna communication. In general channel case, it is possible that the secrecy capacity could be zero if the transmitter-eavesdropper channel has better condition than that of the transmitter-receiver channel. In that situation, the transmitter has to choose not to transmit the confidential information at all. Moreover, in a possible eavesdropping scenario, if the eavesdropper intends to steal the information from the transmitter, it is natural that the eavesdropper will create a better channel condition to the transmitter, i.e., the eavesdropper stays closer to the transmitter. Due to this case, the introduction of multiple antennas to the wiretap channel brings the possibility of achieving positive secrecy rate even when the eavesdropper has a better channel. In the next section, we will discuss the wiretap channels with multiple antennas.

1.2.2 Specific Wiretap Channels

In this section, three popular specific wiretap models, which consider the impact of additional white Gaussian noise (AWGN), fading effect and the utilization of multiple antennas, will be introduced and the expressions of the secrecy rate will be given. Other wiretap channel models include *Semi-determinate wiretap channel*, *compound wiretap channel* and wiretap channel with side information or feedback [5].

Gaussian wiretap channel

First, we consider the wiretap channel with AWGN, also referred to as a Gaussian wiretap channel [6], which indicates both the transmitter-receiver channel and the transmitter-eavesdropper channel are corrupted by additive white Gaussian noises. The output of both channels y_B and y_E are given by

$$y_B = x + r_B, \tag{1.5}$$

$$y_E = x + r_E, \tag{1.6}$$

in which the term x is the information message under the power limit P, i.e., $E\{x^2\} \leq P$. The noise components r_B and r_E are independent Gaussian random variables with zero mean, and variance σ_B^2 and σ_E^2, respectively. The secrecy capacity expression over Gaussian wiretap channel is [6]

$$C_s = \left[\frac{1}{2}\log_2\left(1+\frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_E^2}\right)\right]^+, \tag{1.7}$$

where $[a]^+$ equals a if $a \geq 0$ or equals 0 if $a < 0$. That is, if the transmitter could achieve non-positive secrecy rate, it will choose not to transmit. Moreover, the secrecy capacity is achieved by setting $x \sim \mathcal{N}(0, P)$, which means x is a zero-mean Gaussian random variable with variance P. More detailed achievable proof and converse proof could be found in [6].

Fading wiretap channel

Fading wiretap channel [8] considers the channel not only corrupted by the additional white Gaussian noise, but also impaired by the fading processes. In this case, we focus more on fast fading process. In one transmission symbol time, the fading coefficient remains the same. Therefore, the outputs (y_B, y_E) of both the transmitter-receiver channel and the transmitter-eavesdropper channel with the transmitted message x become

$$y_B = h_B x + r_B, \tag{1.8}$$

$$y_E = h_E x + r_E, \tag{1.9}$$

where r_B, r_E are the AWGN components with zero-mean and variances σ_B^2, σ_E^2, respectively. Note that the realizations of the noise are independent identically distributed (i.i.d.), proper complex Gaussian variables. Then, h_B, h_E represent the channel fading coefficients which are i.i.d. complex symmetric circularly Gaussian (CSCG) random

variables. Meanwhile, the transmitted signal x experiences the same power constraint mentioned in the previous subsection.

By considering the fading process in both channels, the secrecy capacity studied here is over all possible channel state realization due to the ergodicity of h_B, h_E. Therefore, when studying the ergodic secrecy capacity in a fading wiretap channel, we consider two scenarios: the transmitter-eavesdropper channel state information (CSI) is known or unknown to the transmitter. The former scenario regards the eavesdropper as one of the legitimate user in the whole network but not qualified for the confidential message. In this situation, though we study the fast fading process, for every symbol time, we could assume the fading coefficient is fixed and known to the transmitter. The latter scenario is more realistic for other cases. The malicious user intends to eavesdrop the confidential message from the transmitter, and the transmitter may have difficulties to know the position or even the existence of the eavesdroppers. Hence, the ergodic secrecy capacity expression for known Eve's channel situation is given by

$$C_s = \max_{P_x \leq P} \left\{ \log_2 \left(1 + \frac{P_x |h_B|^2}{\sigma_B^2}\right) - \log_2 \left(1 + \frac{P_x |h_E|^2}{\sigma_E^2}\right) \right\} \tag{1.10}$$

and the secrecy capacity expression for an unknown Eve's channel situation is given as:

$$C_s = \max_{P_x \leq P} E_{\{h_B, h_E\}} \left\{ \log_2 \left(1 + \frac{P_x |h_B|^2}{\sigma_B^2}\right) - \log_2 \left(1 + \frac{P_x |h_E|^2}{\sigma_E^2}\right) \right\}, \tag{1.11}$$

where $P_x \triangleq |x|^2$ denotes the power of transmitted signal. Note that P_x is related to the channel state realization h_B, h_E. The detailed optimal power allocation optimizes the secrecy capacity for above expression (1.11) could be found in [8]. Moreover, we will use different methods to study the secrecy capacity/rate for both scenarios, and make comparisons on the results in the following chapters.

MIMO fading wiretap channel

The utilization of multiple antennas in wiretap channels has shown that, via proper design of a transmission scheme over space-time at the transmitter side, the transmitter could enhance the information theoretical security of its communication [9]. Let us assume that the transmitter, the legitimate receiver and the eavesdropper are equipped with $N_t \geq 1, N_r \geq 1$ and $N_e \geq 1$ antennas, respectively, which forms the multiple-input-multiple-output (MIMO) wiretap channel model. The outputs $\mathbf{y}_b \in \mathbb{C}^{N_r \times 1}$ and $\mathbf{y}_e \in \mathbb{C}^{N_e \times 1}$ of both legitimate and eavesdropping channels are [12]

$$\mathbf{y}_B = \mathbf{H}_B^H \mathbf{x} + \mathbf{r}_B, \tag{1.12}$$

$$\mathbf{y}_E = \mathbf{H}_E^H \mathbf{x} + \mathbf{r}_E, \tag{1.13}$$

respectively, where $\mathbf{H}_B \in \mathbb{C}^{N_r \times N_t}, \mathbf{H}_E \in \mathbb{C}^{N_e \times N_t}$ are the CSI matrix of both channels, while the AWGN components for these channels are represented as $\mathbf{r}_b \in \mathbb{C}^{N_r \times 1}, \mathbf{r}_E \in \mathbb{C}^{N_e \times 1}$. Each element of $\mathbf{H}_B, \mathbf{H}_E$ is a CSCG random variable, and every element in $\mathbf{r}_B, \mathbf{r}_E$ follows Gaussian distribution with zero mean and unity variance. The transmitted signal vector $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$ is constrained with total power P available at the transmitter, i.e., $\mathrm{tr}\{\mathbf{x}\mathbf{x}^H\} \leq P$. Meanwhile, the secrecy capacity expression over the known eavesdropping channel scenario is given as [12]

$$C_s = \max_{\mathrm{tr}\{\mathbf{X}\} \leq P} \log_2 \Big[\frac{\det(\mathbf{I} + \mathbf{H}_B^H \mathbf{X} \mathbf{H}_B)}{\det(\mathbf{I} + \mathbf{H}_E^H \mathbf{X} \mathbf{H}_E)} \Big], \tag{1.14}$$

where $\mathbf{X} \triangleq \mathbf{x}\mathbf{x}^H \geq 0$ and $\det(\cdot)$ denotes the determinant operation. We omit the expectation before the secrecy capacity because we assume the fading coefficient is fixed and known to the transmitter during each symbol time in the transmission, which means the transmitter could achieve the ergodic secrecy capacity over the fading process. However, for the scenario with unknown eavesdropping channel, the erogdic secrecy

rate is expressed as:

$$C_s = \max_{\mathrm{tr}\{\mathbf{X}\}\leq P} E_{\{\mathbf{H}_B,\mathbf{H}_E\}}\Big\{ \log_2\left[\det(\mathbf{I}+\mathbf{H}_B^H\mathbf{X}\mathbf{H}_B)\right] - \log_2\left[\det(\mathbf{I}+\mathbf{H}_E^H\mathbf{X}\mathbf{H}_E)\right]\Big\}. \quad (1.15)$$

In this thesis, we mainly study the MISO wiretap channel model, one simplified model of MIMO situation, for which the transmitter is equipped with more than one antenna while the legitimate receiver and the eavesdropper are equipped with single antenna. Thus, the problem reduces to maximize the ergodic secrecy capacity/rate over both known and unknown eavesdropping channel situations.

Extended from the works in Wyner [3] and Csiszár and Körner [4], some more specific wiretap channels with different conditions have been studyed, besides aforementioned Gaussian wiretap channels [6], fading wiretap channels [8, 14, 25] and multiple-antenna wiretap channels [10–13]; there are wiretap channel with side information [26, 27] which considers encoding the message together with channel condition information such as known background noise signal; wiretap channel with multiple users [29, 32] and other research works like studying the outage performance rather than maximizing sum rate [33] etc. Moreover, other research work also considers wiretap channel in special networks such as in cognitive radio network (CRN) [42].

1.3 Motivation

Based on the discussions in previous sections, it is clear that achieving perfect secrecy is possible when the legal receiver has better channel than that of eavesdropper in a wiretap channel model. Moreover, using multiple antennas could provide the possibility to achieve the positive secrecy rate even with a weaker legitimate channel condition. In the past few years, many research efforts have been made to study physical layer security over various antenna deployment and CSI situations. In [11, 34], the transmitter (Alice) is equipped with multiple antennas while the intended receiver (Bob)

is only equipped with one antenna. Their results show that the optimal transmission strategy is precoding (beamforming) of the input information signal vector at Alice. The idea of the precoding strategy is to increase the signal to noise (SNR) as much as possible at Bob's side. This precoding strategy is referred to as the conventional precoding strategy in this thesis. On the other hand, because of the randomness of eavesdropper (Eve)'s position, Eve may experience a better channel than Bob. Besides, it is difficult to obtain the accurate channel condition of the illegitimate one. A precoding strategy with the assistance of artificial noise has been proposed in [36], where part of the available power at Alice is used to transmit artificial noise in an intended way to interfere Eve. The essence of this strategy is to not only increase SNR at Bob's side, but also intend to degrade the channel of Eve as much as possible. This strategy is referred to as artificial noise aided precoding (ANaP) in this thesis. In an ANaP strategy, the power ratio between information signal and artificial noise should be optimized in order to maximize the achievable secrecy rate. In [38], it is shown that Alice can obtain near-optimal secrecy rate by simply using equal power allocation when the available power at Alice is large. However, it considered a simplified case with no noise at Eve's side for the tractability reasons. This motivates the study on how the additive noise will affect the power allocation strategy and whether the conventional precoding is optimal or not.

The utilization of multiple antennas could effectively help to achieve positive secrecy rate. However, it also requires higher hardware cost (e.g., more power consumption and larger space size) so that it may not be applicable for many kinds of mobile devices. Therefore, for the single-antenna users, a promising alternative is to use multiple (collaborative) relays or a relay equipped with multiple antennas to achieve secure transmission [77, 78]. Conventionally, the relay node could operate in two ways to help the transmitter: cooperative relaying (CR) and cooperative jamming (CJ). The CR intends to increase the information signal power at the legitimate receiver as

much as possible, using decode-and-forward (DF) or amplify-and-forward (AF) relay schemes. On the contrary, the CJ intends to jeopardize the illegitimate channel by sending jamming signal (also known as artificial noise) which is usually independent of the information signal. In this thesis, we will discuss both the DF and CJ schemes. The DF scheme is a two-stage scheme. In the first stage, the relay node receives and decodes the information signal sent from the transmitter. In the second stage, it transmits the re-encoded information signal to the intended receiver. On the other hand, by using the CJ scheme, the relay node only responds to weaken the eavesdropper's reception of signals while the transmitter is responsible for the transmission of the information signal. Most works on physical layer security in relay networks focused on designing the beamformer for the information signal or the jamming signal under the condition that the global CSI is available. This motivates our study to investigate if there is a new relay scheme or which scheme is optimal for the system in the sense of secure transmission.

Besides the passive eavesdropping, the adversary could choose the active attack instead. One intelligent attack is called the spoofing attack, in which the adversary pretends to be the legitimate transmitter to spread false messages, or be the legitimate receiver to filch confidential information. This spoofing attack is originally studied in cyber networks [93, 95]. Though some related detection algorithms are designed based on utilizing the physical layer properties, e.g., comparing the channel state information (CSI) in neighbouring time slots [94, 96, 97]. However, recent study [102] illustrates that spoofing attack could also happen in the physical layer of communication systems. Due to the fact that the CSI is essential for data transmission and reception, a pilot-assisted channel estimation method is widely used in practical systems. For example, in a time duplex division (TDD) system, the legal receiver is required to send the assigned pilot signals to the transmitter, and the CSI can be estimated based on the received pilot signals due to the reciprocity of the uplink and downlink channels. The

pilot signal set is pre-designed and known to the transmitter and receiver, and different pilot signals are usually orthogonal to each other to avoid contamination phenomenon. Because of being repeatedly used and publicly known, the knowledge of pilot signals could easily be learned by an adversary, and the spoofing attack to the transmitter becomes possible by broadcasting the identical pilot signal as that of a legitimate receiver. By doing so, the adversary could manipulate the channel estimation result and benefit from the attack. If the transmitter is equipped with multiple antennas to perform beamforming during downlink transmission, e.g., maximum ratio transmission (MRT), the main beam of the data signal might be directed to the adversary or other unwanted destinations. This attack is named as the pilot spoofing attack. The terrible consequences it could cause motivate the research in this thesis to design some effective detection methods and also to recover the secure transmission.

1.4 Objective

As the fact that the channel information is critical in designing the beamformer to obtain positive secrecy rate, in this thesis, we first consider the MISO fading wiretap channels under two scenarios. In the first scenario, the CSI of Eve's channel is known at Alice; while in the second scenario, Eve's CSI is unknown at Alice. The first scenario illustrates that the eavesdropper is actally a legitimate user but not authentic for certain content, and the second scenario indicates that the eavesdropper is hiding itself from the legitimate components. Our interest is to study how to achieve the maximal secrecy rate by designing the ANaP strategy for both scenarios.

In the cooperative relay wiretap channel model, besides the two existing DF and CJ schemes, we propose a new hybrid relay scheme, called relaying-and-jamming (RJ), where the relay node responds to relay the information signal and interfere the eavesdropper at the same time. Note that the jamming signal aided strategy has been used in multiple-antenna systems, e.g., [38, 39, 76]. The RJ scheme is a two-stage scheme:

in the first stage, the relay listens to the transmitter and decodes the information signal while in the second stage, the relay node sends the re-encoded information signal and the independent jamming signal together. The key parameter to optimize the RJ scheme is the power allocation ratio between information signal and jamming signal. Accordingly, our interest is to find out which scheme is the optimal for the relay node to maximize the ergodic secrecy rate: DF, CJ or RJ?

The pilot spoofing (contamination) attack was first arose from the pilot contamination scenario in [102] and it mainly analyzes its damages. In [106, 107], two new channel estimation schemes were proposed with fundamentally modified pilot signal design and estimation process, the former suggested to transmit two random phase-shift keying (PSK) symbols as the pilot signal and tried to detect the pilot spoofing attack based on the phase difference of those two symbols; the latter proposed a new discriminatory channel estimation method and claimed to be secure from the pilot spoofing (contamination) attack by randomly choosing the newly designed stochastic pilot signals. However, the pilot signals have more rules than just to estimate the channel. With the intention of incurring as less modifications as possible to the current pilot-assisted channel estimation process, we are interested to design some effective methods to detect the pilot spoofing attack. Moreover, it is also important to have the ability to provide the secure transmission if the detection shows the existence of an attack.

1.5 Summary of Contributions

The main contributions of the thesis are summarized as follows.

Artificial Noise aided Precoding in MISO Fading Wiretap Channels

Two scenarios are considered: when the CSI of the illegitimate channel is known and when the CSI of illegitimate channel is unknown. Our main results for designing the artificial noise aided precoding in MISO fading wiretap channels are:

For the first scenario, we prove that the optimal ANaP strategy should assign all the power to the information message and no power should be allocated to the artificial noise. That is, the optimal ANaP strategy reduces to the conventional precoding strategy. For the second scenario, we show that when the available power at Alice is small, majority of the available power should be assigned to the information signal. When the power increases, the transmitter should assign larger power to generate the artificial noise. When the power is sufficiently large, the optimal power allocation ratio will approach a constant that is only dependant on the number of antennas at Alice.

Secure Transmission in Cooperative Relay Wiretap Channels

With the assistance of cooperative relay node, we intend to find the optimal relay scheme which obtains the largest ergodic secrecy rate. To match the practical situation, we consider that eavesdropper's CSI is statistically known in the relay networks. Our work has the following major contributions: first, instead of finding the optimal beamformer for a particular relay scheme, we are interested in finding the optimal relay scheme under individual power constraints; second, we propose the hybrid RJ scheme that the relay node needs to send the information signal and jamming signal at the same time. The optimal power ratio is found to maximize the ergodic secrecy rate; third, We also consider the existence of the direct link between the transmitter and the receiver (or the eavesdropper) which has been usually ignored in many of the aforementioned works using DF and AF. Note that the assumption of direct link to eavesdropper is proposed for the sake of fairness, because without such direct illegitimate link, the legitimate system could achieve higher secrecy rate; fourth, in this thesis, the white Gaussian noise at the eavesdropper is taken into account (referred to as the general case) in deriving the expression of the achievable ergodic secrecy rate, while that noise is being ignored due to the tractability reason in previous works (referred to as the worst case), e.g., in [38, 76].

Detection of Pilot Spoofing Attack

Motivated by the fact that the pilot spoofing attack can decrease the signal reception at the legitimate receiver, we propose the energy ratio detector (ERD) by exploring the asymmetry of received signal power levels at the transmitter and the legitimate receiver. Our detection method mainly includes two phases: first, the legitimate receiver (Bob) sends the assigned pilot signal to the transmitter (Alice) via uplink channel, and Alice estimates the channel based on the samples of the signal; second, Alice calculates the received signal power, modulates that as a data signal and broadcasts it via downlink channel. Bob demodulates the data and calculates the power of his received signal. Bob then decides whether the system is under pilot spoofing attack or not by comparing the two power levels. Note that Alice utilizes the same power to broadcast the data as that of Bob used for sending the pilot signal.

The main features of our ERD are summarized as follows:

- Unlike the other two methods in [106, 107], the ERD does not require drastic changes on either the design of pilot signals or the channel estimation phase structure. The main revision is to use a certain short period of the downlink data phase to calculate the power of received signal and detect the existence of the attack.

- We derive the closed-form expression of the test statistic's probability density function (PDF). We find that the detection threshold of the ERD does not depend on either the legitimate or illegitimate channel condition. It is a significant advantage because it suggests the ERD could work under all possible channel realizations. Moreover, the ERD is a two-way method for Alice and Bob to detect the pilot spoofing attack, so the ERD is equipped at both Alice and Bob. Numerical results show that the ERD could detect the pilot spoofing attack with very high probability.

- A large power utilization by Eve could increase the gain to the eavesdropper but also considerably increase the risk of Eve being detected by the legitimate system. Therefore, the trade-off brought by the power consumption of Eve is studied. Our result shows that our ERD could efficiently reduce the ergodic information leakage, which is the largest information rate that Eve could possibly obtain by choosing the optimal power budget, to a trivial level.

Recovering Secure Transmission from Pilot Spoofing Attack

Even though the energy ratio detector provides a fairly high detection probability, it does not study the rescue actions after the detection. To compensate for this, we propose a two-way training based scheme to achieve the goals of detecting the pilot spoofing attack and securely re-transmitting the data signal. The basic process is that the reverse training is still operating as usual to allow the transmitter to estimate the CSI. Before conducting confidential data transmission in the downlink phase, the transmitter first sends the channel estimation results to the receiver, and then conducts the traditional downlink training by having each antenna transmit the pilot signal to the receiver. Therefore, both uplink and downlink channel estimations are available at the receiver, which allows it to make a test based on the difference between two estimation results. The detection outcome will be fed back to the transmitter together with the downlink channel estimation if needed. More importantly, if the detection result indicates the existence of pilot spoofing attack, the transmitter could derive the estimations of both legitimate and illegitimate channels. Thus, by applying secure beamforming, the transmitter is able to immediately recover the data transmission while keeping it secret from the adversary.

The main contributions of our method are summarized in four aspects: 1) our proposed scheme needs no drastic modification to current transmission structure. For example, in the LTE-TDD system, the uplink pilot time slot (UpPTS) and downlink

pilot time slot (DwPTS) are already implemented; 2) the TWTD could achieve even higher detection probability than that of the ERD. Similar to the ERD, the threshold derived for the TWTD is also not dependent on the instantaneous channel conditions, which suggests such threshold could be used among different time frames; 3) unlike the ERD, our scheme is able to estimate both channels, switch to secure beamforming almost immediately and finally achieve positive secrecy rate within the same time frame; 4) in some cases, even without any prior information about Eve, our scheme is able to obtain the maximal secrecy rate as that of using optimal channel estimation or perfect channel information.

1.6 Organization of the Thesis

The rest of this thesis is organized as follows. In Chapter 2, a detailed review on secure transmission in MISO fading wiretap channel and cooperative relay wiretap channel is introduced as well as the research works on defending pilot spoofing attack. The designs of ANaP in MISO fading wiretap channel model are studied for the scenarios of known and unknown eavesdropper's CSI in Chapter 3. The discussion on the optimal relay scheme is given in Chapter 4. The detection methods and secure transmission recovery strategy against the pilot spoofing attack are studied in Chapters 5 and 6, respectively. Finally, the conclusions and the possible future directions of this thesis are drawn in Chapter 7.

Chapter 2

Literature Review

With the assistance of multiple antennas, it is vital to design the secure precoder (beamformer) to protect the legitimate communication from eavesdropping. In this chapter, we will give the literature review on various beamformer designs in MISO wiretap channels under different channel conditions. When considering the relay wiretap channel model, we explore several existing relay schemes that help the legitimate transmitter and receiver to achieve the positive secrecy rate. Moreover, the previous works on tackling the pilot spoofing attack problem are also discussed. However, given the large number of existing works on physical layer security, the references to be mentioned, though numerous, is far from being exhaustive.

2.1 Secure Communication with Multiple Antennas

As discussed in the previous chapter, the channel state information is vital for designing the beamforming vector. Generally, the CSI of the legitimate channel is available but not the illegitimate channel, especially when the eavesdropper remains totally passive. Therefore, most existing works study both known CSI and unknown CSI cases for

eavesdropper channels. Some works study the case if the transmitter could have partial CSI or measurable uncertainty on the CSI. All three cases will be discussed in the following subsections.

Figure 2.1: The illustration of MISO fading wiretap channel. Alice is equipped with multiple ($N > 1$) antennas. Bob and Eve are equipped with single antenna.

In a typical MISO fading wiretap channel model as shown in Fig. 2.1, the legitimate transmitter (Alice) is equipped with multiple antennas while the legitimate receiver (Bob) and eavesdropper (Eve) are equipped with single antenna, respectively. The legitimate and illegitimate channels are represented as $\mathbf{H}_B \in \mathbb{C}^{N\times 1}$ and $\mathbf{H}_E \in \mathbb{C}^{N\times 1}$, respectively, where N is the number of antennas at Alice. Therefore, the received signals at Bob and Eve are generally denoted as y_B and y_E,

$$y_B = \mathbf{H}_B^H \mathbf{x} + r_B, \tag{2.1}$$

$$y_E = \mathbf{H}_E^H \mathbf{x} + r_E, \tag{2.2}$$

respectively, where $\mathbf{x} \in \mathbb{C}^{N\times 1}$ is the precoded information signal. The other terms r_B and r_E are the Gaussian noise experienced at Bob and Eve, respectively. Based on the definition in [3, 4], the achievable secrecy capacity is expressed as

$$C_s = \max_{\mathbf{x}} \log_2 \left(1 + \frac{P|\mathbf{H}_B^H \mathbf{x}|^2}{\sigma_B^2}\right) - \log_2 \left(1 + \frac{P|\mathbf{H}_E^H \mathbf{x}|^2}{\sigma_E^2}\right), \tag{2.3}$$

where P is the power constraint and $\mathrm{tr}\{\mathbf{x}\mathbf{x}^H\} \leq \mathbf{I}_N$, and σ_B^2 and σ_E^2 are the variances for the Gaussian additive noise r_B and r_E, respectively. In order to maximize the secrecy capacity in (2.3), the design of precoder (beamformer) $\mathbf{s} \in \mathbb{C}^{N\times 1}$ to the information signal u is important, e.g., $\mathbf{x} = \mathbf{s}u$. Next, the previous works on achieving physical layer security in MISO wiretap channels under different channel conditions will be introduced.

2.1.1 Secure Transmission with Known CSI

A Gaussian MISO channel was considered in [34], where the authors assumed that the channel conditions are constants and known to all three components. It described the largest achievable secrecy rate via using Gaussian signals and proved that the beamforming method could achieve such maximal secrecy rate. Later, the authors considered the case that the eavesdropper's channels are only statistically known to the legitimate parties, in which the optimality of the beamforming method is still valid. When $\mathbf{H}_E$ is known, the secrecy rate follows the expression of (2.3). Without loss of generality, by normalizing the power of signal and noise and taking the eigenvalue decomposition for the information signal covariance matrix, the covariance matrix is first proven to be optimal when it is unit rank. Furthermore, the problem is simplified as a Rayleigh Quotient Problem and the optimal beamformer is proven to be the unit-norm generalized eigenvector that obtains the largest value of the Rayleigh Quotient Problem. Their results showed that in the presence of a eavesdropper and the requirement of secure transmission, the optimal transmission strategy is still precoding. Unlike in a normal MISO channel model in which the best beamformer design is in the direction of the main channel, the optimal precoder with secrecy constraint and known CSI is the balance of being orthogonal to the eavesdropper channel while being along with the legitimate channel as much as possible.

In [13], the authors studied the optimal transmission structure to achieve the largest secrecy rate for a MIMO system. However, it is generally difficult to solve the problem for a MIMO case. On the other hand, an analytical solution was derived for a simplified case with only single antenna equipped at Bob and Eve, i.e., the MISO case. The channel information is also assumed to be known. Firstly, reference [13] tried to design the beamformer by introducing a unitary transformation matrix. Through certain mathematical efforts, it showed that finding the proper covariance matrix of the input signal is the key to achieve the largest secrecy rate. Similar to [34], the authors in

[13] also concluded the problem in a Rayleigh Quotient Problem. Therefore, the same optimal design of the beamformer was derived under the condition that the channel conditions are available.

The role of multiple antennas to achieve the secure communication was investigated in [11] in a typical wiretap channel, however, in which the eavesdropper is also deployed with multiple antennas. The authors described the maximal secrecy rate by the generalized eigenvalues when the channels are stationary and available to each component in the model. It showed that the precoding method is able to obtain the secrecy capacity. This model is further referred to as the multi-input-single-output- multi-eavesdropper (MISOME) case. Note that the multiple eavesdroppers case could equal the that an eavesdropper equipped with multiple antennas array. One derivation in [11] could be regarded as a tight upper bound to the achievable secrecy rate, which might generate the optimal design of a random variable in the secrecy capacity expression of [4]. Reference [11] considered a case that the states of the channels are available to all three components (the transmitter, the receiver, and the eavesdropper), but the condition of the eavesdropper channel is only available at the adversary. Based on techniques designed for single-antenna wiretap channel problems, the authors developed upper and lower bounds on the maximal secrecy rate both for finite antennas case and the large antenna limit case.

Reference [29] considered the secure communication problem over a Gaussian broadcast channel, in which the transmitter intends to broadcast different but secret messages to two receivers, respectively. This case is denoted as the multi-antenna Gaussian broadcast channel with confidential messages (MGBC-CM). In this case, a dirty-paper coding scheme with secrecy constraints was proposed and the secrecy rate region was first generated based on the Gaussian codebooks. With known CSI of both legal and illegal channels, the authors found the secrecy capacity for the MISO wiretap channels. Next, a tractable Sato-type [15] outer bound was derived for the secrecy capacity.

Moreover, such a Sato-type outer bound has been proved to be consistent with the dirty-paper coding achievable rate region with secrecy constraints.

Moreover, in [25], the authors characterized the secrecy capacity of the slow-fading wiretap channel under different cases of available CSI. This work proved that the none-zero secrecy rate is possible even for the case that the eavesdropper's channel is better than the legitimate channel. Reference [30] introduced another description of secrecy rate, which is different from the one derived based on Sato-like [15] argument and matrix analysis tools. Reference [12] is the extension of [11] by considering the legitimate receiver is also equipped with multiple antennas. A computable denotion of the secrecy capacity in this case was derived as the saddle-point solution to a minimax problem. For the downlink of a multi-user MIMO system, a linear precoder design was introduced in [31]. The proposed precoder is designed according to the regularized channel inversion (RCI). The achievable secrecy rate and the expression was derived and so was the the optimal regularization parameter. Reference [16] considered a MIMO Gaussian broadcast channel with two different receivers and two corresponding messages (one normal message and one confidential message). The secrecy capacity region was depicted using an extremal entropy inequality. In both [26] and [27], the wiretap channel with side information [7] was considered by introducing additive interference in the main channel. A larger secrecy capacity region was achieved based on the extension of the dirty paper coding [28].

2.1.2 Secure Transmission with Partial CSI

Based on the discussion in Section 2.1.1, the secrecy capacity is achievable when the channel conditions are accurately obtained. However, the perfect CSI is usually difficult to obtain due to channel estimation errors or other interference. Thus, some works [43, 54, 89] considered the case that the CSI contains certain level of errors (uncertainty),

e.g., spherical uncertainty,

$$\mathbf{h}_B \in \{\mathbf{h}_B \quad | \quad \|\mathbf{h}_B - \bar{\mathbf{h}}_B\| \leq \epsilon_B\}, \tag{2.4}$$

$$\mathbf{h}_E \in \{\mathbf{h}_E \quad | \quad \|\mathbf{h}_E - \bar{\mathbf{h}}_E\| \leq \epsilon_E\}, \tag{2.5}$$

where $\bar{\mathbf{h}}_B$ and $\bar{\mathbf{h}}_E$ are the channel estimations of the legitimate and illegitimate channels, respectively. The other terms, ϵ_B and ϵ_E, are the estimation error bounds for the spherical channel uncertainty at Bob and Eve, respectively. References [52, 53] researched on another case that the channel between the transmitter and the eavesdropper is only partially known,

$$\bar{\mathbf{h}}_e = \sqrt{\kappa}\mathbf{h}_E + \sqrt{1-\kappa}\Delta\mathbf{h}_E, \tag{2.6}$$

where $\Delta\mathbf{h}_E$ denotes the unknown part (error) of the eavesdropper channel. The scalar κ represents the degree of the knowledge that the transmitter has on the channel condition. If $\kappa = 1$, the transmitter obtains the perfect channel information. If $\kappa = 0$, the transmitter has no knowledge of the eavesdropper channel and other beamforming schemes need to be developed.

A typical MISO wiretap channel model was considered in [89]. For the scenario that both the legitimate and the illegitimate channels were considered with spherical uncertainty. The maximization of worst-case secrecy rate was explored by finding the optimal input covariance with a constraint on power. Moroever, the explicit expression for the maximal worst-case secrecy rate was derived. Reference [89] concluded that the optimization problem leads to a 6-by-6 matrix based on the direct calculation from the channel estimation results. The closed-form expression of the optimal input covariance matrix was derived based on the eigenvalues of the 6-by-6 matrix. Meanwhile, the time consumption of computation for searching the eigenvalues is not dependent on the number of antennas, which is different from the methods proposed in [43, 54].

Reference [54] studied the problem of optimal transmitter design to achieve information theoretical security for a MISO cognitive radio network, where the secondary transmitter only knows the associated uncertainty parts without the information of all the channels. The problem to maximize the achievable secrecy rate for the secondary user is formulated as a max-min non-convex semi-infinite optimization issue. Two approaches have been proposed to solve the problem. The first one is to transform the problem to a optimal robust transmitter design problem in a CRN which has two primary users, and the solution is obtained by utilizing the connection between two networks. However, based on the inherent convexity, the other approach effectively redesigned the old problem as a relatively easy SDP.

Reference [43] considered the scenario of MISO channel model with the presence of multiple eavesdroppers which are all equipped with more than one antenna. The problem of secrecy-rate maximization (SRM) for this case was studied by optimizing the transmit covariance matrix. The SRM was proven to be solvable under the assumption of perfect CSI. In the imperfect CSI case, where a robust SRM was formulated under spherical CSI uncertainties, the optimal solution was derived based on the semi-definite program (SDP).

In the works [51, 52], it is assumed that only partial information of the illegitimate channel is available. The authors considered a model that was with the flat-fading MISO wiretap channel. The authors in [51] first minimized the outage probability of secure transmission under single-stream beamforming. A suboptimal beamforming scheme was then further derived based on a Markov bound. The results are generalized for the cases with and without CSI of the illegitimate channel. Moreover, the outage secrecy rates were proven to be achievable with artificial noise which is orthogonal to the legitimate channel in [52]. While in [53], the authors discussed the different beamforming strategies including maximum ratio transmission strategy, zero forcing (ZF) strategy, and an other optimized beamforming design under secrecy constraints

based on the effectiveness. The flat-fading MISO wiretap channel was considered, in which the illegitimate channel is only partially available at Alice. The scenario includes the case that both perfect and no channel information to the eavesdropper. It showed that higher achievable secrecy rates were achievable by using artificial noise beamforming which its beam direction is in the null space of the legitimate channel. Furthermore, a simple framework for precoding in the MISO fading wiretap channels under the case of partial CSI was developed.

2.1.3 Secure Transmission with Unknown CSI

The instantaneous eavesdropper's channel information is difficult to obtain when the eavesdropper is totally passive and remains hidden. In this case, with only the CSI of the legitimate channel, the transmitter cannot achieve the secrecy capacity as discussed in Section 2.1.1. Therefore, the utilization of artificial noise was proposed in designing the beamforming vector for the confidential information transmission [35, 36].

In [35], the authors considered a problem of secret communication in the wireless environment, with the presence of a passive eavesdropper. It showed that without eavesdropper's channel information how the generated artificial noise can be added to the information signal to achieve secrecy communication. With multiple antennas deployed at the transmitter, it can generate the artificial noise intelligently such that it only degrades the eavesdropper channels by allocating noise in the null space of the legitimate channels. The study was extended to the MIMO case in [36] where the eavesdropper is assumed to have multiple antennas or multiple eavesdroppers are colluding. It is showed that the MIMO secrecy capacity behaves differently from the non-secret MIMO capacity, so that MIMO design is different under the secrecy requirement. A non-zero rate for secret communication can be guaranteed, regardless of eavesdropper's position, i.e., even when the eavesdropper is much closer to the transmitter than that of the receiver. Furthermore, it is proved that low outage probabilities of secrecy capacity

can be achieved.

The study of applying the artificial noise was further investigated in [37, 38]. In [37], it studied the secure transmission in fading wiretap channels with a multi-antenna transmitter that is capable of generating artificial noise. The exact closed-form expression for the average secrecy capacity lower bound was derived. Furthermore, by using the closed-form capacity expression as the target, reference [37] searched the optimal power assignment strategy to design the the information signal as well as the artificial noise. The results have shown that an simple strategy that uses equal power allocation is close to obtain the maximal secrecy rate at any SNR values for the systems. Additionally, the adaptive power allocation based on each realization of the channel gain could not provide significant capacity gain, if there is any, over the equal power allocation strategy. In [38], the authors also studied the case when the number of colluding eavesdroppers increases, the results showed that more power should be spent on generating the artificial noise. Reference [38] provided an upper bound on the SNR. Moreover, the case of unknown CSI of the legal and illegal channel was investigated. The results suggested that if the transmitter generates more artificial noise to confound the illegal users than to improve the received signal power at the legitimate user.

In [39], the new instruction of designing artificial noise-aided transmission in slow fading multiple-antenna channels with secrecy constraint was provided based on the formulation of secrecy outage derived in [40]. It helped to quantify the secure level and reliable level for a given parameter in the wiretap channels. Therefore, it could find the parameters which achieves a desired secure level, for a given constraint on the largest secrecy outage probability. Furthermore, reference [39] provided the exact design to the rate-maximization problem under security constraints, for either non-adaptive transmission or adaptive transmission. Moreover, The extra power consumption for obtaining a higher security level for both schemes was examined.

In [17], using discriminatory channel estimation (DCE) in the training phase and

artificial noise-aided beamforming in the data transmission phase, the authors studied the optimal power allocation between the training and the data transmission phases. The multiple-input single-output single-antenna-eavesdropper (MISOSE) fast fading wiretap channel was considered in [18], which proved that the artificial noise design in [36] is suboptimal. It also characterized the optimal beamforming directions and the AN power allocation strategies. Moreover, the fundamental conditions to design the optimal AN in full rank was given. The authors in [19, 20] proposed a new beamforming strategy where the transmit beamformer and the AN were optimized simultaneously, given that the correlation matrices of the CSIs of Bob and Eves are known. Reference [22] attempted to optimizes the information and the jamming covariances in a MISO wiretap channel with unknown eavesdropper's channel, which in the end to maximize the secrecy rate in worst case. Through a careful reformulation, it is showed that the maximization problem can be tackled by a one-dimensional numerical search where a sequence of semi-definite programs (SDPs) were considered. The authors in [23, 24] presented the effect of quantized channel feedback on the secrecy capacity achievable using AN. The average secrecy capacity loss depends only on the SINR at the legitimate receiver. Moreover, the number of feedback bits must increase at least logarithmically with the transmit power in order to maintain a constant SINR degradation.

2.2 Secure Cooperative Relay Schemes

As introduced before, the single-antenna communication system has a great dependence on the channel conditions. In other words, if the illegitimate channel is stronger than the legitimate channel, positive secrecy rate is hard to obtain. Therefore, many research efforts have been made on applying multiple-antenna techniques (e.g., beamforming) to relax this dependence as discussed in previous subsections. Nevertheless, the utilization of multiple antenna requires high hardware cost (e.g., power consumption and space size) so that it is not always an optimal solution for mobile devices. Therefore, a

promising alternative is to use multiple (collaborative) relays or a relay equipped with multiple antennas to assist the single-antenna users to achieve secure transmission.

Conventionally, the relay node could operate in two ways to secure the transmission: cooperative relaying and cooperative jamming. The cooperative relaying intends to increase the information signal power at the receiver as much as possible, e.g., decode-and-forward and amplify-and-forward. On the contrary, the cooperative jamming intends to jeopardize the illegitimate channel by sending the jamming signal (also known as artificial noise) which is usually independent of the information signal. As shown in Section 2.2, the DF scheme is a two-stage scheme. In the first stage, the relay node receives and decodes the information signal sent from the transmitter, and in the second stage, it transmits the re-encoded information signal to the intended receiver. On the other hand, the relay node only responds to weaken the eavesdropper channel in the CJ scheme while the transmitter is responsible for the transmission of the information signal.

In the following subsections, the related works on cooperative relaying and cooperative jamming with secrecy constraints are introduced. Some other works on jointly design the relay selection schemes and cooperative beamforming are also discussed as well.

Figure 2.2: The illustration of the wireless relay network model, consists of one transmitter (Alice), one legitimate receiver (Bob), one eavesdropper (Eve) and one relay node.

2.2.1 Cooperative Relaying

In [71], the authors considered a scenario where a transmitter connects with a receiver with the assistance of multiple relays with the existence of one or more eavesdroppers. It is assumed that every node is equipped with a single antenna, and the CSI is available. The design of three cooperative schemes was proposed in [71] to improve

the achievable secrecy rate or minimize the total transmit power. For the decode-and-forward, amplify-and-forward, in stage one, a transmitter sends the encoded information signal to the trusted relay nodes. In stage two, by using DF, every relay node decodes the signal first, and then sends a weighted version of the received signal after re-encode. However, by using AF method, the relay node just transmits a weighted version of the received signal from stage one. Meanwhile, the case with multiple eavesdroppers was also considered in [71].

Reference [73] considered a similar scenario and problem as in [71, 72], but the purpose are either deriving the explicit solution to the optimizing problem when using the DF scheme. First, the optimal relay weight was provided to optimize the security level under a overall power limit for the DF protocol in the presence of eavesdroppers. Second, the authors studied the optimal relay beamforming that minimize the overal power consumption with a targeted secure level for the DF with only one eavesdropper. This work is different from the aforementioned [71] in the sense that [73] addressed a more general case with multiple relay nodes and multiple adversaries by using the DF scheme.

In [84], an optimization problem was studied for secure resource allocation and scheduling in orthogonal frequency division multiple access (OFDMA) half-duplex decodeand-forward (DF) relay assisted networks. The authors took into account artificial noise to deal with an eavesdropper equipped with multiple antennas. Meanwhile, the effects of imperfect CSI at the transmitter in slow fading channels were studied. By relaxing the combinatorial subcarrier allocation constraints, the considered problem is transformed into a convex problem. Thus, the optimization problem was solved by dual decomposition which resulted in maximizing the average secrecy outage capacity.

The problem of beamformer design in the relay network was studied in [85] with incomplete information of the illegitimate channel. In here, the relay running in half-duplexing mode is mounted with multiple antennas and the AF scheme was employed.

With the assumption of static legitimate links, the authors considered the beamforming designs under two different cases of the eavesdropper channel: only the statistical CSI of the illegal channel is available by the transmitter and a fixed sphere uncertainty model on the eavesdropper channel vector. The beamforming schemes including the optimal unit-rank, match-and-forward (MF), and ZF were derived to optimize an approximation of the ergodic secrecy rate.

The relay placement for physical layer security was firstly studied in [75]. In the four-node system (source, destination, relay, and eavesdropper), the authors derived the optimal power allocation for the DF strategy and found that the randomize-and-forward (RF) strategy is always better than the DF in terms of secure connection probability. When the eavesdropper is far away, placing the relay at the midpoint of the source and the destination is asymptotically optimal, and the outage probability of the RF strategy is about half of the DF. Moreover, the secure outage probability without relay was derived in cellular networks and shows the superiority of placing RF relay over DF relay through simulation. The effects of path loss on secure connection were investigated and it is found that relay transmission achieves more benefit when path loss is severer.

In [79], cooperative beamforming design by using DF was investigated with security constraints. Several beamforming schemes were optimized to achieve maximal secrecy rates for both overall and individual power limits at relay node. In [80], when there is the full CSI of the channels, the beamforming designs of the AF scheme with overall and individual power constraints were derived to obtaining the largest secrecy rates. Furthermore, robust beamforming designs with imperfect CSI were investigated for DF. Reference [81] described the DF based null space beamforming schemes and optimized the beamforming weights to achieve the maximal secrecy rate.

The optimization problem of bidirectional communications assisted by the relay nodes in the presence of an eavesdropper was addressed in [82] to achieve physical layer

security, using the metric of secrecy sum rate. Three beamforming schemes, which were direct beamforming, null-space beamforming, and artificial noise aided beamforming, were proposed with secrecy rate constraint based on utilizing two-phase analog network coding as well as power control scheme.

2.2.2 Cooperative Jamming

Despite the conventional function of the relay node, the cooperative jamming is also widely used [71, 73]. In [71], while Alice sends the information signal, the trusted relay nodes broadcast a weighted jamming signal in order to interfere with the adversaries. The jamming signal transmitted by the relays is completely orthogonal to the legitimate channel. Moreover, the optimal power allocation was obtained in closed-form for the CJ with one eavesdropper. Reference [73] effectively solved the relay beamforming design problem and power design to maximize the secrecy capacity or minimize the overall power consumption with secrecy constraints using the DF and CJ schemes in the presence of one or more eavesdroppers.

Reference [74] addressed the optimization of collaborative relay weights for CJ in maximizing the secrecy rate with individual relay power constraints. The conditions to achieve positive secrecy rate was studied and further it proposed an algorithm to obtain the optimal CJ relay beamforming solution using a combination of convex optimization and a one-dimensional search. A distributed implementation algorithm that permits each individual relay to derive its own weight was proposed based on the local CSI for achieving a near-optimal secrecy rate.

Two jamming noise schemes were studied in [56], including the local nulling noise and the general structured noise. For the former noise scheme, the jamming signal is designed to be orthogonal to the legal channel towards the legal receiver. Due to limit of cost, size, the reference only considered the case of relay with two antennas. However, the conclusion can be applied for other case with many antennas at relay

nodes. Moreover, the optimal jamming noise design was also derived that could achieve the largest secrecy rate .

In [57], the problem of designing the optimal covariance matrix of the artificial noise was addressed. There was a helper generated the jamming noise in order to optimize the secret rate between a transmitter and legitimate receiver with the existence of multiple eavesdroppers. By utilizing the CJ scheme, it has shown that the non-convex design problem is able to be recast as a sequence of convex optimization problems. Moreover, the beamforming method was proved to be the optimal approaching with multiple eavesdroppers. Furthermore, the zero-forcing solution could not maximize the secret rate in the case of two adversaries.

In [58], the security issues for a two-way relay communication model with assisting jammers were considered. An optimal power allocation vector of the source and relay nodes was derived first. Then based on a defined source optimization problem, an optimal solution of jamming power allocation was obtained. The results showed that a non-zero secrecy rate of two-way relay channel is achievable, and it can be improved with the help of helping nodes which send the jamming signals to confuse the adversary relay.

In [86], the authors gave an achievable secrecy rate for the Gaussian wire-tap channel with a helping interferer (WTC-HI) under the requirement of the eavesdropper being totally kept secret from the confidential messge. The results showed that the jammer can indeed improve the security. Moreover, a positive secrecy rate is achievable when the legitimate channel is worse. A power control strategy was proposed to maximize the achievable secrecy rate.

An alternative approach was investigated in [59] to achieve physical layer security by utilizing a assisting jammer. The interferer with similar statistical properties to the real information message, like Binary Phase Shift Keying (BPSK) or M-ary Quadrature Amplitude Modulation (M-QAM), was examined. In the region of small and middle

SNRs, a obvious improvement of the invoked SER at the potential eavesdropper exists. The benefit of incresing secrecy rates was further evaluated.

2.2.3 Relay Selection Schemes

Proper relay or jammer selection in a cooperative communication network is able to generate a huge impact to the entire communication system. Reference [61] proposed a scheme that delivers the secure communication service in the presence of multiple eavesdroppers. In the two-way cooperative networks, which is consisting of two transmitters, several intermediate nodes, and an passive eavesdropper, the physical layer security was considered. It first found that in when the intermediate relay nodes are randomly and sparsely distributed, the cooperative jamming schemes could have better performance than the conventional schemes without jamming in a given power regime. However, the proposed jamming schemes may be less effective when the Moreover, in the scenario where the intermediate nodes were colluded. An hybrid scheme to switch between jamming and non-jamming modes was introduced based on the results.

In [62], the joint relay selection and beamforming design problems to achieve physical layer security were studied. Due to the synchronization or information exchange, the cooperative beamforming may require high operational complexity especially when it is with multiple relay nodes. However, reducing the number of helping relays may degrade the coding gain of cooperative beamforming. Reference [62] proposed several joint relay selection and cooperative beamforming schemes, in which only two relays could be deployed to information transmission. Moreover, the proposed schemes claimed that there was a selection gain which could partially compensated for the limiting the working relays to two. The cases of full and partial CSI have been considered for relay selection and beamforming. The results showed that the proposed schemes could improve the secrecy rate compared to the previous proposed cooperative relays protocols.

The secrecy performance of opportunistic relay selection over Rayleigh fading channels was investigated in [63]. Two practical scenarios were considered based on the eavesdroppers CSI availability including when Alice and the relay have or have no knowledge about the eavesdroppers CSI. For the former scenario, the new analytical expressions were presented for the secrecy outage probability. In addition, in the high SNR regime, asymptotic expressions were derived for the secrecy outage probability, which facilitates the characterization of secrecy diversity order and coding gain. For the latter scenario, the closed-form expressions for the achievable secrecy rate were derived. Moreover, the effect of feedback delay (outdated CSI) on the secrecy performance was examined for both scenarios.

The authors in [64] studied the problem of secure relay and jammer selection for minimizing the secrecy outage probability (SOP) in cooperative wireless networks. A closed-form expression for the SOP was derived, and methods were developed to allow for cooperative nodes to be assigned as either relays or jammers. Besides an optimal method based on an exhaustive search for the best node assignment, several complexity reduced methods are introduced that could have SOP performance close to that of the exhaustive search.

In [65], the authors considered a cooperative wireless network with multiple relays in the presence of an eavesdropper and examined the optimal relay selection to improve physical-layer security against eavesdropping attack. The closed-form intercept probability expressions were derived for the AF and DF based optimal relay selection and other traditional methods. The proposed and traditional relay selection schemes achieved the diversity order M, which M is the cooperative relays number.

The authors in [66] investigated the problem of relay and jammer selection in cooperative systems with secrecy constraints. The proposed selection schemes select two relays which access the channel simultaneously. One of the relay re-transmits the original data to the destination, while the other broadcasts an intentional jamming signal in

order to confound the adversary. The two relays were chosen based on the performance on achieving an optimization of the perfect secrecy capacity and have been analyzed with either instantaneous or statistic knowledge of the illegitimate channels. The jamming technique was proved to be an efficient method when the eavesdropper channels are strong. With weak eavesdropper connections, an hybrid method for switching between jamming and non-jamming was also developed, which acted as a general solution and optimizes the achievable secrecy rate for all cases.

The effects of relay selection with multiple eavesdroppers under Rayleigh fading and with security constraints were studied in [67], in which three relay selection schemes were considered: minimum selection, conventional selection [68], and secrecy relay selection [69]. The relay which has the lowest SNR to the eavesdroppers was selected in the first schemes. While in the second scheme, it selects the relay that generates the highest SNR at the receiver. In the third scheme, the relay node is selected based on how much secrecy rate it could provides. Furthermore, the probability of positive achievable secrecy rate and the secrecy outage probability by using the three selection schemes were also discussed.

In [70], in addition to the CJ schemes, another scheme named noise forwarding was applied, which transmitted a dummy information from a code source which is available at both the legitimate receiver and the adversary. In a Gaussian wiretap channel, a deaf helper (relay) was deployed to interfere or confuse the eavesdropper by CJ or NF, respectively. The optimal power control policy that maximizes the achievable secrecy rate was derived for both schemes. By deaf cooperation with a single helper, it can choose one passive helper that achieves the largest secrecy rate.

2.3 Pilot Spoofing Attack

Other than the passive eavesdropping, the adversary could choose the active attack instead. In [99], an new wiretap channel model with an active eavesdropper was in-

troduced. Different from the conventional model in which the eavesdropper is usually passive, the active adversary can not only eavesdrop but also manipulate the signal transmitted over the channel. Specifically, the eavesdropper could either erase or modify the signal bits it observes. Achievable perfect secrecy rates is derived by concatenating a stochastic code, guaranteeing the secrecy at the eavesdropper. A code was found based on Varshamov construction [101], guaranteeing decoding at the legitimate receiver even after the codeword has been modified. Reference [100] considered a MIMO systems in the presence of an intelligent eavesdropper. The adversary could either passively eavesdrop or actively attack the legitimate data transmission. A game-theoretic based solution was chosen to solve the game payoff function which is defined as the ergodic MIMO secrecy rate of the legal components.

Another intelligent attack is called the spoofing attack, in which the adversary pretends to be the legitimate transmitter to spread false messages, or be the legitimate receiver to filch confidential information. This spoofing attack was originally studied in cyber networks [93, 95]. Though some related detection algorithms are designed based on utilizing the physical layer properties. In this section, the spoofing attack happened in physical layer is discussed. The pilot spoofing attack (pilot contamination attack) was first mentioned in [102], where the authors got the idea from the pilot contamination phenomenon. However, reference [102] mainly focused on illustrating the impact brought by the pilot spoofing attack, and studying the optimal energy allocation for the eavesdropper with full-duplex transmission ability to either jam the legitimate receiver or listen to the information signal. Some potential direction to defend the pilot spoofing attack were discussed, like using sufficiently long training sequence, or blind channel estimation. In a practical multiple-antenna communication system, a training

Figure 2.3: The pilot spoofing attack. Eve sends the identical pilot (training) signals to Alice as that of Bob.

phase is implemented before the actual data transmission. For example, in a TDD

system, the legitimate receiver will send the assigned pilot signal (training signal) to the transmitter through uplink channel. According to the reciprocity of the uplink and downlink channels, the transmitter could estimate the channel based on the received pilot signal. These pilot signals are repeatedly used by the system and are usually publicly known. Therefore, it provides a great chance for an intelligent eavesdropper to attack the training phase by sending the same pilot signal as that of the legal receiver and act as a normal receiver during the data transmission phase as shown in Fig. 2.3. If the eavesdropper can successfully synchronize its transmission with that of the legal receiver, the transmitter would be spoofed and utilize the estimation of legitimate channel, which is actually the combination of the legitimate channel and illegitimate channel, to design the beamformer in the data transmission phase, e.g., maximum-ratio transmission. Then such a pilot spoofing attack could lead to the information leakage to the active eavesdropper and also decrease the legitimate channel rate considerably. By increasing the power of the pilot signal, the eavesdropper could even diminish the legitimate receiver's rate approaching zero. Note that we focus on the pilot spoofing attack rather than other active attacks such as jamming attack, because jamming attack intends to degrade the legitimate transmission instead of eavesdropping the confidential information due to the half-duplex implementation.

2.3.1 Random Pilot Signal Designs

Due to all the serious damages the pilot spoofing attack could cause, it is important for the legal parties to be able to at least detect such an attack. To our best knowledge, there are few works concentrating on solving this pilot spoofing attack in the literature [106, 107]. The main idea of these two works is to propose the newly designed random pilot signals to replace current fixed training sequence design. By introducing the randomness into the pilot signals, it hopes to prevent the eavesdropper from conducting the pilot spoofing attack.

Phase Shifted Keying Symbols

The authors in [106] studied a problem about the presence of an adversary who attacks on the channel estimation using the method in [102]. A random training approach was proposed, which suggested to use the phase-shift keying symbols to replace the current pilot signals. By ignoring the additive Gaussian noise, this method intends to detect the pilot spoofing attack by randomly sending two PSK symbols and examining the phase of received signal at the legitimate transmitter. Furthermore, with the assumption of a large number of antennas (massive MIMO), the received thermal noise at Alice in the uplink can be averaged out so that the detection can be much simplified with improved performance. The results illustrated that with massive MIMO and large constellation size, the pilot spoofing attack can be detected with a probability arbitrarily close to one.

Two Way Training in Discriminatory Channel Estimation

In [107], the authors proposed a two-way training method based on discriminatory channel estimation, claiming that the method could diminish the impact of the pilot spoofing attack by randomly choosing the new designed stochastic pilot signals at the legitimate receiver. In the proposed two-way training, the reverse training signal is a private symbols at the LR and only known by itself, which is randomly generated. Thus, the randomness feature of the reverse training signal provides a natural way of protecting against the pilot contamination attack. Other two possible attack models that the adversary may adopt are using blind detection method [103] and a guessing-based attack. For the blind detection method, the adversary will suffer from a rotation ambiguity between the estimate channel and the original channel, and it is still no use to interpret the reverse training pilot without the cooperation of the legitimate receiver. For the guessing-based attack, the authors concluded that the pilot contamination attack only marginally increases the normalized mean squared error (NMSE) at the

intended receiver.

2.3.2 Detection Methods for Spoofing Attack

The spoofing attack describes that the adversary pretends to be the legitimate transmitter and sends the fake information to the receiver. Many of the current studies [93–98] focused on the spoofing attack happened at the network level, although the methods utilized in those works might be based on the physical layer properties, e.g., comparing current CSI with previous CSI to detect the spoofing attack or using the spatial information of the transmitter node to differentiate the legitimate transmitter and the active adversary. Next, some works on investigating the detection methods for spoofing attack using physical layer techniques are discussed.

Due to current full-scale authentication is not always desirable as the higher requirement on key management and more extensive computations, some non-cryptographic mechanisms were proposed in [93] which are complementary to authentication and could detect device spoofing with little or no dependency on cryptographic keys. Based on forge-resistant consistency checks, it allowed other network entities to detect spoofing activities. Several practical examples of forge-resistant relationships for detecting anomalous network activity were also provided. Instead of using the authentication keys to identify entities, the proposed strategy involves the verification of forge-resistant relationships between packets coming from a claimed network identity.

In [94], the spoofing attack was studied in frequency-selective Rayleigh channels, considering channel conditions vary with environmental changes and user mobility,and the channel estimation errors generated by the noise in the environment. Therefore, a generalized channel-based spoofing detection schemes was proposed by using the channel estimation results to find out the spoofing messages. In this network, an designed generalized likelihood ratio test (L_g) and a practical test (L) were presented. Note these tests were not dependent on the CSI. The effect of the proposed detector

was examined in a generic frequency-selective Rayleigh channel model.

The Sybil attacks, in which a malicious node illegally represents many identities and then easily uses out the system energy, was considered in [95]. In this work, the authors proposed an physical layer assisted authentication method to detect Sybil attacks. It exploited the spatial variability of the wireless channels in situations with rich scattering. The proposed detector involved a test parameter based on the number of fake identities, the number of access points (APs), and the attack schemes utilized by the attacker. It is proved that the Sybil detector can be conveniently deployed in many of the current wireless networks. Moreover, it could also cooperate with other physical layer security schemes without too much changes.

In the work of [96], a hybrid authentication protocol that integrates the fingerprints-in-the-ether (FP) algorithm into existing wireless systems was proposed, which cooperated with the existing higher-layer security mechanism. A performance bound for spoofing detection was derived by using this protocol in generalized scenarios and without assuming a reliable reference channel record. The detection performance of such PHY-authentication scheme was provided via the test on InterDigitals 802.11 Physical Layer Security Platform (IPLSVP).

In [97], it proposed a physical layer authentication scheme using a channel-based hypothesis testing method to detect spoofing behaviors through the statistical analysis of the inherent properties of channel impulse response(CIR) difference in a time-varying multipath environment. With a new test statistic based on the difference between noise-mitigated CIRs, the detection methods can minimize the impact of noise and interference from the wireless environment. Furthermore, to achieve effective authentication, an adaptive threshold was derived at the receiver based on the statistical properties of CIR variation and used for discriminating the legitimate transmitter from attackers.

Reference [98] proposed to use received signal strength (RSS) at every wireless

device. Such property is difficult to falsify and could be used as the basis to detect the spoofing attacks in wireless systems. In the theoretic analysis, the test statistic was derived based on the cluster analysis of RSS readings. The proposed method could not only detect the presence of attacks but also decide the number of adversaries. Therefore, it is possible to pinpoint the attackers and get rid of them. How to decide the number of attackers is an extremely challenging issue. A method, named as SILENCE, was proposed to test the minimum distance with the assist of cluster analysis to solve the challenge. Moreover, with the help of the pilot signals, the Support Vector Machines-based mechanism was used to further increase the determining accuracy.

Chapter 3

Secure Transmission in MISO Wiretap Channels

According to the discussion in Chapter 2, the early works have shown that achieving positive secrecy capacity is only possible when the receiver has a better channel than the eavesdropper. However, in multiple-antenna wiretap channels, the secure beamformer is derived to guarantee the positive secrecy rate even under the case that Eve has a stronger channel. The core idea of the beamforming strategy is to increase the SNR at Bob's side. This precoding strategy is referred to as the conventional precoding strategy in this chapter. On the other hand, because of the uncertainty of the eavesdropper, it may be hidden from legitimate components so that the Eve's CSI is unknown to Alice. Therefore, a precoding strategy with the assistance of artificial noise has been proposed in [36], where part of the available power at Alice is used to transmit artificial noise in an intended way to interfere with Eve. The essence of this strategy is to not only increase the SNR at Bob's side, but also intend to weaken the signal reception at Eve. This strategy is referred to as artificial noise aided precoding (ANaP) in this chapter. In the ANaP strategy, the power ratio between information signal and artificial noise should be optimized in order to maximize the achievable secrecy rate. In [38], it is shown that Alice can obtain the near-optimal secrecy rate by simply using equal power

allocation when the available power at Alice is large.

In this chapter, we consider MISO fading wiretap channels under two scenarios. In the first scenario, the CSI of Eve's channel is known at Alice; while in the second scenario, Eve's CSI is unknown at Alice. Unlike the earlier work in [38], which considers no noise experienced at the eavesdropper, we take the additional Gaussian noise components at Bob and Eve into account. Furthermore, our interest is to study how to achieve the maximal secrecy rate by designing the ANaP strategy for both scenarios. The main results of this chapter are listed in the following:

1. For the first scenario, we prove that the optimal ANaP strategy should allocate all the available power to the information signal and no power should be spent on the artificial noise. That is, the optimal ANaP strategy reduces to the conventional precoding strategy.

2. For the second scenario, we show that when the available power at Alice is small, most of the power should be allocated to the information signal. When the power increases, more power should be assigned to the artificial noise. When the power is sufficiently large, the optimal power allocation ratio will approach a constant that is only dependant on the number of antennas at Alice.

The rest of this chapter is organized as follows. In Section 3.1, the system model setup utilized in this chapter is introduced and the corresponding problems are formulated as well. Two scenarios, namely, known and unknown illegitimate channel conditions are studied in Sections 3.2 and 3.3, respectively. The proof of numerical results is given in Section 3.4, while the conclusion is drawn in Section 3.5.

3.1 System Model and Problem Formulation

Consider a wiretap channel where there are one transmitter (Alice) with N ($N > 1$) antennas, one receiver (Bob) and one eavesdropper (Eve). Both with a single antenna.

Alice intends to send precoded signal vector $\mathbf{x} \in \mathbb{C}^{N\times 1}$ to Bob, where the time index of x is omitted. The signals received at Bob and Eve are, respectively, given by

$$y_B = \mathbf{h}_B^H \mathbf{x} + r_B, \tag{3.1}$$

$$y_E = \mathbf{h}_E^H \mathbf{x} + r_E, \tag{3.2}$$

where $\mathbf{h}_B$, $\mathbf{h}_E \in \mathbb{C}^{N\times 1}$ represent the CSI of receiver's channel and eavesdropper's channel, respectively. Each element of $\mathbf{h}_B$ and $\mathbf{h}_E$ is independently and identically distributed as a CSCG random variable with zero mean and unit variance. Note that the position of eavesdropper may be not clear to the legitimate users, so here we assume the eavesdropper's channel follows Gaussian distributions regarding the randomness of its position. The terms r_B and r_E represent the white Gaussian noise at Bob and Eve with variance $\sigma_B^2 = 1$ and $\sigma_E^2 = 1$, respectively. It is assumed that $\mathbf{h}_B$ is available at Alice while $\mathbf{h}_E$ is known at Eve. The transmitted signal vector $\mathbf{x}$ is subject to power constraint $\mathrm{tr}\{\mathbf{x}\mathbf{x}^H\} \leq P$, where P represents the total available power at Alice.

3.1.1 Conventional Precoding Strategy

In conventional precoding, the transmitted signal vector $\mathbf{x} = \mathbf{s}u$, where u is the information codeword from Gaussian codebook with zero mean and unit variance and $\mathbf{s} \in \mathbb{C}^{N\times 1}$ is the precoder for u. Clearly, we have $\mathrm{tr}\{\mathbf{s}\mathbf{s}^H\} \leq P$. With (3.1) and (3.2), the secrecy capacity can be expressed as

$$C_1 = \max_{\mathrm{tr}(\mathbf{S})\leq P} \left\{ \log_2(1 + \mathbf{h}_B^H \mathbf{S}\mathbf{h}_B) - \log_2(1 + \mathbf{h}_E^H \mathbf{S}\mathbf{h}_E) \right\}, \tag{3.3}$$

where $\mathbf{S} \triangleq \mathbf{s}\mathbf{s}^H$ is positive semi-definite.

3.1.2 Artificial Noise Aided Precoding

In the ANaP strategy, the transmitted signal $\mathbf{x}$ now consists of both information $\mathbf{s}u$ and artificial noise $\mathbf{w} \in \mathbb{C}^{N\times 1}$, i.e., $\mathbf{x} = \mathbf{s}u + \mathbf{w}$. Denoting ρ as the partition of the power allocated to information signal, we have $\text{tr}\{\mathbf{s}\mathbf{s}^H\} \leq \rho P$. The secrecy capacity is now expressed as:

$$C_2 = \max_{\text{tr}(\mathbf{S}+\mathbf{W})\leq P} \left\{ \log_2 \left(1 + \frac{\mathbf{h}_B^H \mathbf{S}\mathbf{h}_B}{\mathbf{h}_B^H \mathbf{W}\mathbf{h}_B + 1}\right) - \log_2 \left(1 + \frac{\mathbf{h}_E^H \mathbf{S}\mathbf{h}_E}{\mathbf{h}_E^H \mathbf{W}\mathbf{h}_E + 1}\right) \right\}, \tag{3.4}$$

where $\mathbf{W} \triangleq \mathbf{w}\mathbf{w}^H$ is the artificial noise covariance matrix, which is positive semi-definite. Equation (3.4) is the general expression of secrecy capacity with artificial noise. In this chapter, when considering the scenario that Alice has the knowledge of $\mathbf{h}_E$, there is no need to design $\mathbf{W}$ as we will show that the optimal choice is to put all the power in the information signal, i.e., $\rho = 1$. In the scenario when Alice has no knowledge of $\mathbf{h}_E$, we follow the original design of $\mathbf{w}$ and $\mathbf{s}$ in [5]. That is, $\mathbf{S} = \rho P(\mathbf{h}_B/||\mathbf{h}_B||)(\mathbf{h}_B/||\mathbf{h}_B||)^H$, and the artificial noise is allocated to the null space of $\mathbf{h}_B$ in order to ensure that the artificial noise will not interfere with Bob. By choosing $\mathbf{Z} = \text{null}(\mathbf{h}_B^H)$ as the orthonormal basis of the null space of $\mathbf{h}_B$, where $\mathbf{Z} \in \mathbb{C}^{N\times(N-1)}$, it follows that $\mathbf{w}$=$\mathbf{Z}\mathbf{v}$, in which $\mathbf{v} \in \mathbb{C}^{(N-1)\times 1}$ is a complex Gaussian noise vector with each element being zero mean and variance of σ_v^2. As the artificial noise power $(1-\rho)P$ is uniformly allocated to the $N-1$ elements, we get $\sigma_v^2 = (1-\rho)P/(N-1)$. Therefore, (3.1), (3.2), and (3.4) can be rewritten as

$$Y_b = \mathbf{h}_B^H \mathbf{s}u + R_b, \tag{3.5}$$

$$Y_e = \mathbf{h}_E^H \mathbf{s}u + \mathbf{h}_E^H \mathbf{Z}\mathbf{v} + R_e, \tag{3.6}$$

$$C_2 = \max_{0<\rho\leq 1} \left\{ \log_2(1 + \rho P \mathbf{h}_B^H \mathbf{h}_B) - \log_2 \left(1 + \frac{\rho P \mathbf{h}_{EB}^H \mathbf{h}_{EB}}{\frac{(1-\rho)}{N-1} P \mathbf{h}_{EZ}^H \mathbf{h}_{EZ} + 1}\right) \right\}, \tag{3.7}$$

where $\mathbf{h}_{EB} = (\mathbf{h}_B/||\mathbf{h}_B||)^H\mathbf{h}_E$ and $\mathbf{h}_{EZ} = \mathbf{Z}^H\mathbf{h}_E$.

Therefore, based on the design of $\mathbf{W}$ and $\mathbf{S}$, we need to find out the optimal power ratio ρ in order to achieve secrecy capacity. Note that the exact design of $\mathbf{W}$ is not given for the first scenario when Alice has full knowledge of $\mathbf{h}_E$. This is because we will prove that regardless of the different design of $\mathbf{W}$, the optimal design allocates no power to artificial noise. In the next two sections, the problems of how to achieve the largest secrecy rate by designing the optimal Artificial Noise aided Precoding strategy in given conditions are discussed.

3.2 Scenario 1: Illegitimate Channel is Known at the Transmitter

In this scenario, we study the optimal solution for the ANaP strategy and compare it with that for the conventional precoding strategy. The main result is presented in the following theorem.

Theorem 1. When $\mathbf{h}_E$ is known at Alice, it is always optimal to allocate all the available power to the information signal in order to achieve the maximal secrecy rate. That is, the optimal ANaP strategy reduces to the conventional precoding.

Firstly, we consider the conventional precoding strategy. As has been shown in [3] that the optimal covariance matrix for information signal, $\mathbf{S}$, is of rank one, we can write it as $\mathbf{S} = P\mathbf{e}_x\mathbf{e}_x^H$, where $\mathbf{e}_x \in \mathbb{C}^{N\times 1}$ is an auxiliary unit-norm vector. Therefore, the secrecy capacity can be rewritten as

$$C_1 = \max_{\mathbf{e}_x} \left\{ \log_2 \left(\frac{\mathbf{e}_x^H \mathbf{A} \mathbf{e}_x}{\mathbf{e}_x^H \mathbf{B} \mathbf{e}_x} \right) \right\}, \tag{3.8}$$

where $\mathbf{A} = \mathbf{I} + P\mathbf{h}_B\mathbf{h}_B^H, \mathbf{B} = \mathbf{I} + P\mathbf{h}_E\mathbf{h}_E^H$, and both $\mathbf{A}$ and $\mathbf{B}$ are positive definite matrices. Note that the expression inside the $\log_2(\cdot)$ operator is a Generalized Rayleigh

Quotient (GRQ) with the following lemma.

Lemma 1. For a GRQ in the form of $\frac{\mathbf{e}_x^H \mathbf{M} \mathbf{e}_x}{\mathbf{e}_x^H \mathbf{N} \mathbf{e}_x}$, where $\mathbf{M}$ and $\mathbf{N}$ are positive definite matrices, we have

$$\lambda_{\min} \leq \frac{\mathbf{e}_x^H \mathbf{M} \mathbf{e}_x}{\mathbf{e}_x^H \mathbf{N} \mathbf{e}_x} \leq \lambda_{\max}, \tag{3.9}$$

where $\lambda_{\min}$ and $\lambda_{\max}$ represent the minimal and maximal generalized eigenvalues, respectively, corresponding to the matrix pencil $(\mathbf{M}, \mathbf{N})$.

Based on Lemma 1, we can find the explicit solution for $\mathbf{S}$. Because of the monotonicity of $\log_2(\cdot)$ function, the optimal $\mathbf{S}$ can be easily shown to be $\mathbf{S} = P\mathbf{e}_a\mathbf{e}_a^H$, where $\mathbf{e}_a$ is the unit-norm generalized eigenvector corresponding to the largest generalized eigenvalue ($\lambda_{\max 1}$) of matrix pencil $(\mathbf{A}, \mathbf{B})$. As a result, the secrecy capacity C_1 can be written as

$$C_1 = \log_2(\lambda_{\max 1}) = \log_2 \left(\frac{\mathbf{e}_a^H \mathbf{A} \mathbf{e}_a}{\mathbf{e}_a^H \mathbf{B} \mathbf{e}_a} \right). \tag{3.10}$$

Now we consider the ANaP strategy by beginning with a lemma.

Lemma 2. The optimal design of $\mathbf{S}$ in the ANaP strategy is of rank one as well, i.e., $\mathbf{S} = \rho P \mathbf{e}_x \mathbf{e}_x^H$, where $\mathbf{e}_x \in \mathbb{C}^{N \times 1}$ is an auxiliary unit-norm vector.

Because of the monotonicity of $\log_2(\cdot)$ function, maximizing C_2 is equivalent to maximizing the expression below

$$f_1(x, y, \mathbf{S}) = \frac{1 + x\mathbf{h}_B^H \mathbf{S} \mathbf{h}_B}{1 + y\mathbf{h}_E^H \mathbf{S} \mathbf{h}_E}, \tag{3.11}$$

where $\mathrm{tr}(\mathbf{S}) \leq \rho P$ and $0 \leq x, y \leq 1$. Let the eigenvalue decomposition of $\mathbf{S}$ be $\mathbf{S} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^H$, where $\mathbf{\Lambda}$ is the diagonal matrix consisting of eigenvalues $\lambda_i, i \in \{1, 2 \cdots N\}$,

with $\sum_{i=1}^{N} \lambda_i \leq \rho P$. The expression in (3.11) can be rewritten as

$$f_2(\mathbf{a}, \mathbf{b}, \lambda) = \frac{1 + \sum_{i=1}^{N} a_i^2 \lambda_i}{1 + \sum_{i=1}^{N} b_i^2 \lambda_i}, \qquad i \in 1, 2 \cdots N, \tag{3.12}$$

where $\mathbf{a} \triangleq \sqrt{x}\mathbf{V}^H \mathbf{h}_B$ and $\mathbf{b} \triangleq \sqrt{y}\mathbf{V}^H \mathbf{h}_E$. We then have the following discussions:

1. If $a_i^2 < b_i^2$ holds for all $i \in \{1, 2, \cdots N\}$, then the maximal value of (3.12) will be equal to one, which means that Alice is not able to achieve positive secrecy capacity and it should remain silent ($\lambda_i = 0$).

2. If there exists at least one $i \in \{1, 2, \cdots N\}$, which makes $a_i^2 > b_i^2$, Alice should allocate all of its power to the information signal in one direction in order to maximize (3.12). The reason is that (3.12) is monotonically increasing or decreasing with λ_i [34].

Therefore, the optimal $\mathbf{S}$ in ANaP strategy should be of rank one as well. This completes the proof of Lemma 2.

Based on Lemmas 1 and 2, we can conclude that the optimal $\mathbf{S}$ in ANaP strategy is given by $\mathbf{S} = \rho P \mathbf{e}_b \mathbf{e}_b^H$, where $\mathbf{e}_b$ is the unit-norm generalized eigenvector corresponding to the largest generalized eigenvalue ($\lambda_{\max 2}$) of matrix pencil $(\mathbf{A}', \mathbf{B}')$. Here $\mathbf{A}' = \mathbf{I} + x\rho P \mathbf{h}_B \mathbf{h}_B^H$ and $\mathbf{B}' = \mathbf{I} + y\rho P \mathbf{h}_E \mathbf{h}_E^H$, where $x = 1/(\mathbf{h}_B^H \mathbf{W} \mathbf{h}_B + 1)$ and $y = 1/(\mathbf{h}_E^H \mathbf{W} \mathbf{h}_E + 1)$. It is clear to see that $0 \leq x, y \leq 1$.

As a result, the secrecy capacity with ANaP strategy can be written as

$$C_2 = \log_2(\lambda_{\max 2}) = \log_2 \left(\frac{\mathbf{e}_b^H \mathbf{A}' \mathbf{e}_b}{\mathbf{e}_b^H \mathbf{B}' \mathbf{e}_b} \right). \tag{3.13}$$

Before proceeding to compare C_1 and C_2, we present another lemma [44] as follows.

Lemma 3. Let $\mathbf{e}_i, i \in \{1, 2 \cdots N\}$, denote the unit-norm generalized eigenvector of matrix pencil $(\mathbf{M}, \mathbf{N})$, where $\mathbf{M}, \mathbf{N} \in \mathbb{C}^{N \times N}$ are positive definite matrices. It follows that

$$\mathbf{e}_i^H \mathbf{N} \mathbf{e}_j = \begin{cases} 1, & \text{if } i = j \in \{1, 2 \cdots N\} \\ 0, & \text{if } i \neq j \in \{1, 2 \cdots N\}. \end{cases} \tag{3.14}$$

Based on Lemma 3, it can be shown that

$$\begin{aligned} \lambda_{\max 1} &= \frac{\mathbf{e}_a^H \mathbf{A} \mathbf{e}_a}{\mathbf{e}_a^H \mathbf{B} \mathbf{e}_a} && (3.15) \\ &\geq \frac{\mathbf{e}_b^H \mathbf{A} \mathbf{e}_b}{\mathbf{e}_b^H \mathbf{B} \mathbf{e}_b} && (3.16) \\ &= \frac{\mathbf{e}_b^H (\mathbf{I} + P \mathbf{h}_B \mathbf{h}_B^H) \mathbf{e}_b}{\mathbf{e}_b^H (\mathbf{I} + P \mathbf{h}_E \mathbf{h}_E^H) \mathbf{e}_b} && (3.17) \\ &= \mathbf{e}_b^H (\mathbf{I} + P \mathbf{h}_B \mathbf{h}_B^H) \mathbf{e}_b && (3.18) \\ &\geq \mathbf{e}_b^H (\mathbf{I} + x \rho P \mathbf{h}_B \mathbf{h}_B^H) \mathbf{e}_b && (3.19) \\ &= \frac{\mathbf{e}_b^H \mathbf{A}' \mathbf{e}_b}{\mathbf{e}_b^H \mathbf{B}' \mathbf{e}_b} = \lambda_{\max 2}, && (3.20) \end{aligned}$$

where the equality in (3.16) only holds when $\mathbf{e}_b = \mathbf{e}_a$; Getting (3.18) is because $\mathbf{e}_b^H \mathbf{B}' \mathbf{e}_b = \mathbf{e}_b^H (\mathbf{I} + y \rho P \mathbf{h}_E \mathbf{h}_E^H) \mathbf{e}_b = 1$ and $\mathbf{e}_b^H \mathbf{e}_b = 1$, so $\mathbf{e}_b^H \mathbf{h}_E \mathbf{h}_E^H \mathbf{e}_b = 0$, which leads to $\mathbf{e}_b^H (\mathbf{I} + P \mathbf{h}_E \mathbf{h}_E^H) \mathbf{e}_b = \mathbf{e}_b^H \mathbf{B} \mathbf{e}_b = 1$.

From the above, it is clear to see that $C_1 \geq C_2$ and the maximal secrecy rate (denoted as C_2^*) is equal to C_1. C_2^* is achieved when all the transmit power is allocated to the information signal, i.e., $\rho = 1$. In other words, the best strategy in this case is not to use artificial noise and thus the best ANaP strategy reduces to the conventional precoding. This completes the proof of Theorem 1.

3.3 Scenario 2: Illegitimate Channel is Unknown at the Transmitter

In this section, after deriving the closed-form expression of the ergodic secrecy rate, we study how to design the optimal JP strategy that achieves the maximal ergodic secrecy rate when $\mathbf{h}_E$ is unknown at Alice.

3.3.1 Main Results

Our main result is summarized in the theorem below.

Theorem 2. When $\mathbf{h}_E$ is unknown to Alice, the optimal power allocation ratio maximizing the ergodic secrecy rate is found to be dependent on P and N only. In the low power region ($P \to 0$), most of the power should be allocated to the information signal (i.e., $\rho \to 1$), while in the high power region ($P \to \infty$), the optimal power ratio should approach a constant that is only dependent on N.

The ergodic secrecy rate in this case is defined as

$$\begin{aligned}\tilde{C}_2 \triangleq \tilde{C}_{\text{2-AB}} - \tilde{C}_{\text{2-AE}} &\triangleq E_{x_1}\{\log_2(1+\rho P x_1)\} \\ &-E_{x_2,x_3}\left\{\log_2\left(1+\frac{\rho P x_2}{\frac{1-\rho}{N-1}Px_3+1}\right)\right\},\end{aligned} \tag{3.21}$$

where $\tilde{C}_{\text{2-AB}}$ and $\tilde{C}_{\text{2-AE}}$ represent the ergodic channel rate of the legitimate channel and the illegitimate channel, respectively. Moreover, $x_1 \triangleq ||\mathbf{h}_B||^2$, $x_2 \triangleq ||\mathbf{h}_{eb}||^2$, and $x_3 \triangleq ||\mathbf{h}_{ez}||^2$ follow gamma distribution, i.e., $x_1 \sim \Gamma(N,1)$, $x_2 \sim \Gamma(1,1)$, and $x_3 \sim \Gamma(N-1,1)$.

Firstly, the ergodic channel rate between Alice and Bob can be expressed as

$$\tilde{C}_{\text{2-AB}} = \frac{1}{\ln 2}\int_0^\infty \left[\ln(1+\rho P x_1)x_1^{N-1}\frac{\exp(-x_1)}{\Gamma(N)}\right]dx_1 \frac{1}{\ln 2}\exp\left(\frac{1}{\rho P}\right)\sum_{i=1}^{N}\mathrm{G}_i\left(\frac{1}{\rho P}\right) \tag{3.22}$$

where $\mathrm{G}_i(\cdot)$ is the generalized exponential integral [47].

Next, we derive the ergodic channel rate between Alice and Eve. By denoting $x = \rho P x_2/(\frac{1-\rho}{N-1}Px_3 + 1)$, it is easy to show that x is denoted as the signal-to-interference-plus-noise ratio (SINR) of a single-branch MMSE diversity combiner with $N-1$ interferers [49]. The complementary cumulative distribution function (CCDF) of x is given by

$$R(x) = \frac{\exp(-ax)}{(1+bx)^{N-1}}, \tag{3.23}$$

where $a = 1/(\rho P)$ and $b = (1-\rho)/((N-1)\rho)$. Accordingly, $\tilde{C}_{\text{2-AE}}$ becomes

$$\begin{aligned} \tilde{C}_{\text{2-AE}} &= \int_0^\infty \big[\log_2(1+x)f(x)\big]dx \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{\exp(-ax)}{(1+x)(1+bx)^{N-1}}dx, \end{aligned} \tag{3.24}$$

where (3.24) is obtained through integration by parts. Generally, it is not straightforward to obtain the closed-form expression of (3.24). Through the partial fraction decomposition [47], it can be shown that

$$\begin{aligned} \frac{1}{(1+x)(1+bx)^{N-1}} &= \frac{a_1}{(1+bx)} + \frac{a_2}{(1+bx)^2} + \cdots \\ &\quad + \frac{a_{N-1}}{(1+bx)^{N-1}} + \frac{a_N}{(1+x)}, \end{aligned} \tag{3.25}$$

where the calculation of coefficients a_i $(1 \le i \le N)$ is omitted due to space limit. Therefore, (3.24) is rewritten as

$$\tilde{C}_{\text{2-AE}} = \frac{1}{\ln 2}\int_0^\infty \left[\sum_{j=1}^{N-1} \frac{a_j e^{-ax}}{(1+x)(1+bx)^j} + \frac{a_N e^{-ax}}{1+x}\right]dx. \tag{3.26}$$

From [47], we get the following integral evaluations:

$$\int_0^\infty \frac{\exp(-\mu x)}{x+\beta}dx = -\exp(\beta\mu)\mathrm{E}_i(-\mu\beta) \tag{3.27}$$

$$\int_0^\infty \frac{\exp(-\mu x)}{(x+\beta)^n}dx = \frac{1}{(n-1)!}\sum_{k=1}^{n-1}(k-1)!(-\mu)^{n-k-1}\beta^{-k} - \frac{-\mu^{n-1}}{(n-1)!}\exp(\beta\mu)\mathrm{E}_i(-\mu\beta) \quad (\mu \geq 0, \beta \geq 0, n \geq 2), \tag{3.28}$$

where $\mathrm{E}_i(\cdot)$ is the exponential integral function [47]. Baesd on (3.27) and (3.28), we obtain the expression of $\tilde{C}_{\text{2-AE}}$ as

$$\tilde{C}_{\text{2-AE}} = \frac{1}{\ln 2}\Bigg\{\sum_{i=2}^{N-1}\Big[\frac{a_i}{b^i(i-1)!}\sum_{k=1}^{i-1}(k-1)!(-a)^{i-k-1}b^k - \frac{\text{-}a^{i-1}}{(i-1)!}e^{\frac{a}{b}}\mathrm{E}_i\left(\text{-}\frac{a}{b}\right)\Big] - \frac{a_1}{b}e^{\frac{a}{b}}\mathrm{E}_i\left(\text{-}\frac{a}{b}\right) - a_N e^a \mathrm{E}_i(\text{-}a)\Bigg\}. \tag{3.29}$$

With (3.21), (3.22) and (3.29), the ergodic secrecy rate $\tilde{C}_2$ is now expressed in closed-form, which involves ρ, N and P only. This suggests that the optimal ρ, denoted as ρ^*, depends on N and P only, and numerical methods can be used to find ρ^*.

When the available power is sufficiently large (i.e., $P \to \infty$), we can ignore the noise at Eve's side by letting $\sigma_e^2 = 0$. Therefore, the CCDF of x can be rewritten as

$$R(x) = \frac{1}{(1+bx)^{N-1}} \tag{3.30}$$

and the ergodic secrecy rate in this case can be found as [38]

$$\tilde{C}_2 = \frac{1}{\ln 2}\left[\exp\left(\frac{1}{\rho P}\right)\sum_{i=1}^{N}E_i\left(\frac{1}{\rho P}\right) - \frac{\rho}{\rho-1}{}_2F_1\left(1,1;N;\frac{1-\rho N}{\rho-1}\right)\right]^+, \tag{3.31}$$

where the ${}_2F_1(\cdot)$ is the Gauss hyper-geometric function. When the power is not sufficiently large, (3.31) actually reflects the ergodic secrecy rate in the worst-case scenario (i.e., no noise is experienced at Eve's side). The case of $\sigma_e^2 = 1$ is referred to as the

general-case scenario in the sequel. When $P \to \infty$, (3.31) can be shown to be

$$\lim_{P\to\infty} \tilde{C}_2 = \frac{1}{\ln 2}\left[\sum_{i=2}^{N}\left(\frac{1}{1-i}\right) + \left(\frac{N\rho-\rho}{N\rho-1}\right)^{N-1} \cdot \left(\ln\left(\frac{N\rho-\rho}{1-\rho}\right) - \sum_{j=1}^{N-2}\frac{1}{j}\left(\frac{N\rho-1}{N\rho-\rho}\right)^{j}\right)\right]^{+}. \quad (3.32)$$

Based on (3.32), it is found that the optimal ρ, which leads to the maximal secrecy rate, is dependent on N only. Note that (3.32) is not an upper bound for $\tilde{C}_2$ when $P \to \infty$. In fact, with the optimal ρ, $\tilde{C}_2$ keeps increasing with P. However, with the increasing P, the optimal ρ will approach a constant related to N only.

Next, we consider the low power region ($P \to 0$). Using $\log_2(1+x) \approx x/\ln 2$ at $x \to 0$ yields

$$\begin{aligned}
\lim_{P\to 0} \tilde{C}_2 &= \lim_{P\to 0}\Bigg\{E_{x_1}\{\log_2(1+\rho P x_1)\} \\
&\quad -E_{x_2,x_3}\left\{\log_2\left(1+\rho P x_2 + \frac{1-\rho}{N-1}P x_3\right)\right\} \\
&\quad +E_{x_3}\left\{\log_2\left(1+\frac{1-\rho}{N-1}P x_3\right)\right\}\Bigg\} \\
&\approx E_{x_1,x_2,x_3}\left\{\rho P x_1 - \left[\rho P x_2 + \frac{1-\rho}{N-1}P x_3\right] + \frac{1-\rho}{N-1}P x_3\right\}/\ln 2 \\
&= \rho P E_{x_1,x_2}\{x_1 - x_2\}/\ln 2 \\
&= \rho P (N-1)/\ln 2, \quad (3.33)
\end{aligned}$$

which clearly suggests that in the low power region ($P \to 0$), most of the transmit power should be used to precode the information signal, i.e., $\rho \to 1$. This completes the proof.

3.3.2 Discussions

Remark 1. In the worst-case scenario (i.e., $\sigma_e^2 = 0$), it can be shown that when P decreases, more power should be allocated to the jamming signal, though this may not

be directly observable from (3.31).

In the following, we illustrate this trend by considering a special case of the low power region ($P \to 0$). In this case, with $\sigma_e^2 = 0$, (3.21) can be rewritten as

$$\begin{aligned} \tilde{C}_2 &= E_{x_1,x_2,x_3}\left\{\log_2\left(\frac{1+\rho P x_1}{1+\frac{(N-1)\rho x_2}{(1-\rho)x_3}}\right)\right\} \\ &\approx E_{x_2,x_3}\left\{-\log_2\left(1+\frac{(N-1)\rho x_2}{(1-\rho)x_3}\right)\right\}. \end{aligned} \tag{3.34}$$

Clearly, $\tilde{C}_2$ is monotonically decreasing with ρ, suggesting that more power should be allocated for jamming. This is opposite to our earlier result for the general-case scenario in (3.33), where more power should be allocated to the information signal.

Furthermore, it can be shown that when P increases, more power should be allocated to the jamming signal in the general-case scenario ($\sigma_e^2 = 1$). This is different from the result for the worst-case scenario ($\sigma_e^2 = 0$) where less power should be allocated to the jamming signal when P increases [38]. The reason is given as following. When power is large, the transmitter approximately uses half of the power to send information signal, the other half to jam Eve. In the low power region ($P \to 0$), when consider $\sigma_e^2 = 1$ in the eavesdropper side, the most power should assign to information signal, which leads the conclusion that with power increase, relatively more power shall be assigned to jamming signal. In the case of $\sigma_e^2 = 0$ like in [38] where Eve has no noise, transmitter needs to assign most power to jam Eve in order to achieve positive secrecy rate, with power increase, the ratio of jamming signal power decreases.However, in both scenarios, as N increases, more power should be allocated to the information signal.

Remark 2. When P increases, the ergodic secrecy rate achieved by conventional precoding is upper bounded by

$$\begin{aligned}\lim_{P\to\infty}\tilde{C}_1 &= \lim_{P\to\infty} E_{x_1,x_2}\left\{\log_2\left(\frac{1+Px_1}{1+Px_2}\right)\right\} \\ &\approx E_{x_1,x_2}\{\log_2(x_1)-\log_2(x_2)\} \\ &= (\psi(N)-\psi(1))/\ln 2, \end{aligned} \tag{3.35}$$

where $\psi(N)$ represents the poly-gamma function [47] with parameter N and $\psi(1)/\ln 2 = 0.8327$. On the other hand, as mentioned earlier, with the optimal ρ^*, the secrecy rate of the JP strategy keeps increasing with P and $\tilde{C}_2$ is unbounded. This clearly indicates that when $\mathbf{h}_E$ is unknown to Alice, conventional precoding is no longer the optimal strategy and it is always optimal to allocate part of the power for jamming. In particular, when P increases or N decreases, more power should be allocated to the jamming signal.

3.4 Numerical Results

In this section, We provide numerical results to illustrate the performance of the ANaP strategy as well as the conventional precoding strategy. The elements of $\mathbf{h}_B$ and $\mathbf{h}_E$ are generated from CSCG independent random variables distributed as $\mathcal{CN}(0,1)$.

Figure 3.1: Average Secrecy capacity versus P. The illegitimate channels are known at Alice. The number of antennas $N = 3$.

Figure 3.1 displays the average secrecy capacity of the ANaP strategy with various ρ values, when $\mathbf{h}_E$ is known at Alice. The performance of conventional precoding is also plotted for comparison. It is clearly shown in Fig. 3.1 that with ANaP strategy, when ρ increases, the achievable secrecy capacity also increases. Furthermore, when ρ reaches the maximum value of 1, the maximal secrecy capacity is achieved. This verifies our result in the previous section. Note that the ANaP strategy with $\rho = 1$ reduces to

the conventional precoding strategy. Therefore they achieve the same performance as shown Fig. 3.1.

Figure 3.2: Average secrecy capacity versus P. The illegitimate channels are unknown at Alice.

The ergodic secrecy rate with unknown $\mathbf{h}_E$ at Alice is shown in Fig. 3.2. where both conventional precoding and ANaP with optimal ρ are considered. It is observed from Fig. 3.2 that in the low power region, there is little difference between conventional precoding and ANaP with optimal ρ. This is because in this case, the optimal ρ approaches 1 and therefore ANaP reduces to conventional precoding. However, when P further increases, their difference becomes more and more significant. For conventional precoding, it is limited by the upper bound given in (3.35), while for ANaP with optimal ρ^*, the ergodic secrecy rate is unbounded and keeps increasing with P, as discussed in Section 3.3. Figure 3.2 also shows that employing more antennas at Alice helps to improve the secrecy rate.

Figure 3.3: Optimal power allocation ratio for ANaP strategy. The illegitimate channels are unknown at Alice.

The optimal power allocation ratio used in Figure 3.2 for the ANaP strategy is shown in Fig. 3.3, for both of the considered general-case and worst-case scenarios. From Fig. 3.3, we observe opposite behaviors of these two scenarios, which are consistent with our analytical results in Section 3.3. In the general-case scenario, the optimal ρ decreases with P and eventually converges to an irreducible floor. On the contrary, in the worst-case scenario, the optimal ρ increases with P and eventually converges to an upper bound. It is worth noting that in practice, the worst-case scenario can only be justified under the large power assumption. It is observed from Fig. 3.3 that the optimal power allocation ratio is above 0.5 at various N when P is over 20 dB. Note that in other simulation environment, e.g., the transmitter with less antenna number, the optimal power allocation ratio may be smaller than 0.5. Furthermore, Fig. 3.3 also

shows that employing more antennas at Alice results in a larger ρ. This is not unexpected since when N increases, with the same ρ, the capacity of the legitimate channel increases faster than that of the eavesdropper channel by observing (3.7). Therefore, ρ should also increase to further improve the secrecy rate.

3.5 Conclusion

In this chapter, we studied a physical-layer security problem in MISO fading wiretap channels by using precoding with artificial noise. When Eve's channel knowledge is known at Alice, we prove that the optimal ANaP strategy reduces to the conventional precoding strategy, i.e., all the transmit power should be allocated to the precoding of information signal. When Eve's channel knowledge is unknown at Alice, we find that there exists an optimal power assignment ratio to balance the utilization of the information signal and the jamming signal. This assignment ratio depends on the number of antennas as well as the available transmit power at Alice. In particular, when the available transmit power at Alice increases or the number of antennas at Alice decreases, more power should be allocated to the artificial noise. Numerical results have been provided to validate the presented analytical results.

Chapter 4

Secure Transmission in Cooperative Relay Wiretap Channels

In the previous chapter, we studied the MISO wiretap model that the transmitter was equipped with multiple antennas. It has been shown that the positive secrecy rate is achievable by designing the optimal beamforming vector for signal transmission. Nevertheless, the utilization of multiple antennas requires high hardware cost (e.g., power consumption and space size) so that it may not be suitable for all current mobile devices. Therefore, a promising alternative is to exploit multiple (collaborative) relays or a relay equipped with multiple antennas to assist single-antenna users to achieve secure transmission [77, 78].

Conventionally, the relay node operates in two ways to achieve secure transmission: cooperative relaying and cooperative jamming, which were introduced in Chapter 2. Most works on physical layer security in relay networks focused on designing the beamformer for the information signal or the jamming signal under the condition that the global CSI is available. In [71, 73], the authors derived the optimal beamformer for the DF scheme and a suboptimal beamformer for the CJ scheme to achieve either the maximal secrecy rate or the least power consumption. In [56, 74], the authors found the optimal beamformer for the jamming signal. However, in practice, the instant CSI

of the eavesdropper's channel may not be accessible. In [56, 74, 91], the authors designed the beamformer for CJ without CSI of the eavesdropper's channel. In [85], the authors studied secure beamforming with imperfect CSI by making an approximation of the ergodic secrecy rate. In [84], the authors studied the secrecy outage capacity in orthogonal frequency-division multiple access (OFDMA) relay network with imperfect CSI. In this chapter, both the DF and CJ schemes will be discussed. Moreover, we consider a communication scenario that a single-antenna transmitter plans to send confidential messages to the intended single-antenna receiver. The perfect secrecy cannot be guaranteed because of the single antenna set-up. Therefore, it approaches a trusted relay node equipped with multiple antennas for assistance. Moreover, the transmitter and the relay node experience individual power constraints and only the statistical CSI of the eavesdropper's channel is available.

Besides the two existing DF and CJ schemes, we propose a new hybrid relay scheme, named relaying-and-jamming (RJ), where the relay node responds to relay the information signal and interfere with the eavesdropper at the same time[1]. The RJ scheme is a two-stage scheme. In the first stage, the relay listens to the transmitter and decodes the information signal while in the second stage, it sends the re-encoded information signal and the independent jamming signal together. The key parameter to optimize the RJ scheme is the power allocation ratio between information signal and jamming signal. Accordingly, an interesting question is which scheme is the optimal relay scheme to maximize the ergodic secrecy rate: DF, CJ or RJ?

Compared with the works that eavesdropper's CSI is statistically known in the relay networks, our work has the following major differences. 1) We are interested in finding the optimal relay scheme under individual power constraints, instead of finding the optimal beamformer for a particular relay scheme. 2) We consider the hybrid RJ scheme that the relay node needs to send the information signal and jamming signal at the same

[1]Note that the jamming signal aided strategy has been used in multiple-antenna systems, e.g., [38, 39, 76]. Here we apply it in the relay networks.

time. The optimal power ratio is found to maximize the ergodic secrecy rate. 3) We also consider the existence of the direct link between the transmitter and the receiver (or the eavesdropper) which has been ignored in many of the aforementioned works using DF and AF. 4) In this chapter, the white Gaussian noise at the eavesdropper is taken into account (referred to as the general case) in deriving the expression of the achievable ergodic secrecy rate. Note that noise is ignored due to the tractability reason in previous studies (referred to as the worst case), e.g., in [38, 76].

The rest of the chapter is organized as follows. In Section 4.1, the system model utilized in this chapter and related assumptions are introduced. In Section 4.2, the expressions of the ergodic secrecy rate are derived for all the DF, CJ and RJ schemes. The optimal power allocation ratio for the RJ scheme is studied in Sections 4.3 and 4.4, the optimal relay scheme is found for the different power budget situations. Section 4.5 contains the simulation set-up and results as well as the related discussions. The conclusion is drawn in Section 4.6.

4.1 System Model and Problem Formulation

In this chapter, we study a wireless relay network model as depicted previously in Fig. 2.2, consisting of a transmitter (Alice), a legitimate receiver (Bob), an eavesdropper (Eve) and a relay node. Alice, Bob and Eve are all equipped with single antenna while the relay is mounted with N ($N > 1$) antennas. Each antenna is omni-directional and working in half-duplex mode. Alice intends to send certain information to Bob and wants to keep the information confidential from Eve. Due to the limitation of single antenna, Alice requires the assistance from the trusted and powerful relay to accomplish the reliable and secure communication.

We use h_{AB}, $h_{\mathrm{AE}} \in \mathbb{C}^{1\times 1}$, and $\mathbf{h}_{\mathrm{RB}}$, $\mathbf{h}_{\mathrm{RE}} \in \mathbb{C}^{N\times 1}$ to represent the channel between Alice and Bob, the channel between Alice and Eve, the channel between the relay node and Bob as well as the channel between the relay node and Eve, respectively. We

assume that h_{AB}, h_{AE} and elements in $\mathbf{h}_{\mathrm{RB}}$ and $\mathbf{h}_{\mathrm{RE}}$ are CSCG random variables with distribution of $\mathcal{CN}(0,1)$. The power budgets at both Alice and relay node are denoted as P_a and P_r, respectively. Without loss of generality, we normalize the distance between the transmitter and the receiver (or the eavesdropper), and use the magnitude of the power at the transmitter to represent the physical distance, i.e., large P_a at the transmitter could indicate the receiver (or the eavesdropper) is close to the transmitter and vice versa.

Similar to that in [71, 73], we assume that the stochastic encoder is used and the codeword is Gaussian distributed. More details about the encode-decode process could be found in the related references [71, 73]. The connection between Alice and trusted relay node is assumed to be strong enough. Furthermore, we assume that the channel rate of transmitter-relay channel is no less than that of relay-receiver channel. Besides, for DF or RJ, the receiver and the eavesdropper decode the confidential message based on the signals received in two stages.

Conventionally, the ergodic secrecy capacity is defined as

$$C_{\mathrm{a}} \triangleq E_{\{h_{\mathrm{AB}},\mathbf{h}_{\mathrm{RB}},h_{\mathrm{AE}},\mathbf{h}_{\mathrm{RE}}\}}\big[\max(R_{\mathrm{B}}-R_{\mathrm{E}}),0\big]^{+}, \tag{4.1}$$

where R_{B} and R_{E} denote the information rates of legitimate and illegitimate channels. Since instant $h_{\mathrm{AE}}, \mathbf{h}_{\mathrm{RE}}$ are unknown, we cannot achieve the instant secrecy capacity. Instead, we can maximize the achievable ergodic secrecy rate which is defined as

$$C_{\mathrm{s}} \triangleq \big[\max E_{\{h_{\mathrm{AB}},\mathbf{h}_{\mathrm{RB}},h_{\mathrm{AE}},\mathbf{h}_{\mathrm{RE}}\}}(R_{\mathrm{B}}-R_{\mathrm{E}}),0\big]^{+}. \tag{4.2}$$

Note that $C_{\mathrm{s}} \leq C_{\mathrm{a}}$. For notational convenience, the operation $[\cdot,0]^{+}$ is omitted in the rest of the chapter. Next, the specific problem formulations for DF, CJ and RJ are presented. Note that the ideas of DF or CJ have been discussed in [56, 74], but our work focuses more on the ergodic secrecy rate.

4.1.1 Decode-and-Forward

As the DF scheme has two stages, the received signals at Bob and Eve in the first stage are represented as

$$Y_{\mathrm{B1}} = \sqrt{P_a} h_{\mathrm{AB}} x + r_{\mathrm{B1}}, \tag{4.3}$$

$$Y_{\mathrm{E1}} = \sqrt{P_a} h_{\mathrm{AE}} x + r_{\mathrm{E1}}, \tag{4.4}$$

respectively. In the second stage, the relay node transmits the re-encoded message. In this chapter, we assume that the relay node and Alice utilize the same Gaussian codebook to encode the confidential message. The received signals at Bob and Eve are

$$Y_{\mathrm{B2}} = \sqrt{P_r} \mathbf{h}_{\mathrm{RB}}^H \mathbf{s}_{\mathrm{DF}} x + r_{\mathrm{B2}}, \tag{4.5}$$

$$Y_{\mathrm{E2}} = \sqrt{P_r} \mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{DF}} x + r_{\mathrm{E2}}, \tag{4.6}$$

where x is Gaussian distributed with zero mean and unit variance, and the time index is omitted here. $\mathbf{s}_{\mathrm{DF}} \in \mathbb{C}^{N\times 1}$ is the precoder (beamformer) for x. r_{B1}, $r_{\mathrm{E1}}, r_{\mathrm{B2}}$ and r_{E2} denote the white Gaussian noise components(distributed in $\mathcal{CN}(0, \sigma^2)$) at Bob and Eve for each stage, respectively. The signal-to-interference-and-noise-ratios (SINRs) at Bob and Eve are represented as $\mathrm{SINR_B}$ and $\mathrm{SINR_E}$, respectively. At the receiving end, the DF scheme could be mathematically identical to a 1×2 SIMO model [73]. By using the maximal-ratio combining (MRC), we get

$$\begin{aligned} R_{\text{B-DF}} &= \frac{1}{2}\log_2(1+\mathrm{SINR}_{\text{B-DF}}) \\ &= \frac{1}{2}\log_2\left(1+\frac{P_a||h_{\mathrm{AB}}||^2 + P_r||\mathbf{h}_{\mathrm{RB}}^H \mathbf{s}_{\mathrm{DF}}||^2}{\sigma^2}\right), \end{aligned} \tag{4.7}$$

$$\begin{aligned} R_{\text{E-DF}} &= \frac{1}{2}\log_2(1+\mathrm{SINR}_{\text{E-DF}}) \\ &= \frac{1}{2}\log_2\left(1+\frac{P_a||h_{\mathrm{AE}}||^2 + P_r||\mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{DF}}||^2}{\sigma^2}\right), \end{aligned} \tag{4.8}$$

$$C_{\text{s-DF}} = \max_{\mathbf{s}_{\text{DF}}} \{E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{B-DF}}) - E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{E-DF}})\}, \tag{4.9}$$

in which the pre-factor 1/2 accounts for the fact that the DF scheme consumes two time slots for one transmission.

4.1.2 Cooperative Jamming

As the CJ scheme is a one-stage scheme, the received signals at Bob and Eve by using the CJ scheme are expressed as

$$Y_{\text{B}} = \sqrt{P_a} h_{\text{AB}} x + \sqrt{P_r} \mathbf{h}_{\text{RB}}^H \mathbf{w}_{\text{CJ}} + r_{\text{B}}, \tag{4.10}$$

$$Y_{\text{E}} = \sqrt{P_a} h_{\text{AE}} x + \sqrt{P_r} \mathbf{h}_{\text{RE}}^H \mathbf{w}_{\text{CJ}} + r_{\text{E}}, \tag{4.11}$$

where $\mathbf{w}_{\text{CJ}} \in \mathbb{C}^{N\times 1}$ denotes the precoded jamming signal vector. When Eve's channel is unknown, the expressions of channel rates become

$$\begin{aligned} R_{\text{B-CJ}} &= \log_2(1 + \text{SINR}_{\text{B-CJ}}) \\ &= \log_2\left(1 + \frac{P_a ||h_{\text{AB}}||^2}{P_r ||\mathbf{h}_{\text{RB}}^H \mathbf{w}_{\text{CJ}}||^2 + \sigma^2}\right), \end{aligned} \tag{4.12}$$

$$\begin{aligned} R_{\text{E-CJ}} &= \log_2(1 + \text{SINR}_{\text{E-CJ}}) \\ &= \log_2\left(1 + \frac{P_a ||h_{\text{AE}}||^2}{P_r ||\mathbf{h}_{\text{RE}}^H \mathbf{w}_{\text{CJ}}||^2 + \sigma^2}\right), \end{aligned} \tag{4.13}$$

respectively, and the ergodic secrecy rate is

$$C_{\text{s-CJ}} = \max_{\mathbf{w}_{\text{CJ}}} \{E_{h_{\text{AB}},\mathbf{h}_{\text{RB}}}(R_{\text{B-CJ}}) - E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{E-CJ}})\}. \tag{4.14}$$

As the relay node is only responsible for jamming the illegitimate channel, the CJ scheme has great dependence on the direct transmission from Alice to Bob.

4.1.3 Relaying-and-Jamming

For the RJ scheme, there exists an issue of power allocation between the information signal and the jamming signal at the relay node. We denote the ratio for the information signal as ρ, where $0 \leq \rho \leq 1$. By doing so, the signals received by Bob and Eve in the first stage are the same as (4.3) and (4.4).

In the second stage, the received signals at the destination and eavesdropper are

$$Y_{\mathrm{B2}} = \sqrt{\rho P_r}\mathbf{h}_{\mathrm{RB}}^H \mathbf{s}_{\mathrm{RJ}} x + \sqrt{(1-\rho)P_r}\mathbf{h}_{\mathrm{RB}}^H \mathbf{w}_{\mathrm{RJ}} + r_{\mathrm{B2}}, \tag{4.15}$$

$$Y_{\mathrm{E2}} = \sqrt{\rho P_r}\mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{RJ}} x + \sqrt{(1-\rho)P_r}\mathbf{h}_{\mathrm{RE}}^H \mathbf{w}_{\mathrm{RJ}} + r_{\mathrm{E2}}, \tag{4.16}$$

respectively, where $\mathbf{s}_{\mathrm{RJ}} \in \mathbb{C}^{N\times 1}$ denotes the precoder for the information signal and $\mathbf{w}_{\mathrm{RJ}} \in \mathbb{C}^{N\times 1}$ represents the jamming signal vector. Similar to DF, the RJ scheme could be treated as a 1×2 SIMO model as well. The rates of Bob's channel and Eve's channel by using RJ are

$$\begin{aligned} R_{\text{B-RJ}} &= \frac{1}{2}\log_2(1+\mathrm{SINR}_{\text{B-RJ}}) \\ &= \frac{1}{2}\log_2\left[1 + \frac{P_a||h_{\mathrm{AB}}||^2}{\sigma^2} + \frac{\rho P_r||\mathbf{h}_{\mathrm{RB}}^H \mathbf{s}_{\mathrm{RJ}}||^2}{(1-\rho)P_r||\mathbf{h}_{\mathrm{RB}}^H \mathbf{w}_{\mathrm{RJ}}||^2 + \sigma^2}\right], \end{aligned} \tag{4.17}$$

$$\begin{aligned} R_{\text{E-RJ}} &= \frac{1}{2}\log_2(1+\mathrm{SINR}_{\text{E-RJ}}) \\ &= \frac{1}{2}\log_2\left[1 + \frac{P_a||h_{\mathrm{AE}}||^2}{\sigma^2} + \frac{\rho P_r||\mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{RJ}}||^2}{(1-\rho)P_r||\mathbf{h}_{\mathrm{RE}}^H \mathbf{w}_{\mathrm{RJ}}||^2 + \sigma^2}\right], \end{aligned} \tag{4.18}$$

respectively, and the ergodic secrecy rate is expressed as

$$C_{\text{s-RJ}} = \max_{\mathbf{s}_{\mathrm{RJ}}, \mathbf{w}_{\mathrm{RJ}}, \rho} \{E_{h_{\mathrm{AB}}, \mathbf{h}_{\mathrm{RB}}}(R_{\text{B-RJ}}) - E_{h_{\mathrm{AE}}, \mathbf{h}_{\mathrm{RE}}}(R_{\text{E-RJ}})\}. \tag{4.19}$$

Without Eve's instant CSI, we design $\mathbf{s}_{\mathrm{RJ}} = \mathbf{h}_{\mathrm{RB}}/||\mathbf{h}_{\mathrm{RB}}||$, i.e., the maximum ratio transmission (MRT). Zero-forcing (ZF) beamforming is used for $\mathbf{w}_{\mathrm{RJ}}$, i.e., allocating the jamming signal into the null space of the legitimate channel. Therefore, we denote

$\mathbf{Z} = \text{null}(\mathbf{h}_{\text{RB}}^H)$ as the orthonormal basis of the null space of the legitimate channel $\mathbf{h}_{\text{RB}}$, i.e., $\mathbf{Z} \in \mathbb{C}^{N\times(N-1)}$. We then have $\mathbf{w}_{\text{RJ}} = \mathbf{Z}\mathbf{v}$, where $\mathbf{v} \in \mathbb{C}^{(N-1)\times 1}$ is the jamming codeword vector. Each element of $\mathbf{v}$ follows Gaussian distribution with zero mean and variance $\sigma_v^2 = 1/(N-1)$ (the power used for jamming signal is uniformly allocated in all possible directions apart from the legitimate channel direction). Therefore, we have

$$R_{\text{B-RJ}} = \frac{1}{2}\log_2\left[1 + \frac{P_a||h_{\text{AB}}||^2 + \rho P_r||\mathbf{h}_{\text{RB}}^H\mathbf{s}_{\text{RJ}}||^2}{\sigma^2}\right], \tag{4.20}$$

$$R_{\text{E-RJ}} = \frac{1}{2}\log_2\left[1 + \frac{P_a||h_{\text{AE}}||^2}{\sigma^2} + \frac{\rho P_r||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{RJ}}||^2}{\frac{(1-\rho)}{N-1}P_r||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2 + \sigma^2}\right], \tag{4.21}$$

respectively, and

$$C_{\text{s-RJ}} = \max_{\rho}\{E_{h_{\text{AB}},\mathbf{h}_{\text{RB}}}(R_{\text{B-RJ}}) - E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{E-RJ}})\}. \tag{4.22}$$

There are several observations: 1) The maximization of the achievable ergodic secrecy rate for the RJ scheme depends on finding the optimal power ratio ρ. 2) When $\rho = 1$, the relay node uses all its power in re-transmitting the information signal and the RJ scheme becomes the DF scheme. 3) When $\rho = 0$, the relay node allocates all P_r to the jamming signal. This makes the RJ scheme similar to the CJ scheme. However, the RJ scheme has half of the transmission efficiency as the CJ scheme does.

4.2 Ergodic Secrecy Rate

In this section, the expressions of ergodic secrecy rates by using DF, CJ and RJ are derived. For DF and CJ, the major effort is to find the distributions of the SINRs. For RJ, in addition to the distributions of the SINRs, the search for the optimal power allocation ratio ρ is also a vital issue to be addressed.

4.2.1 Decode-and-Forward

When using the DF scheme without instant $\mathbf{h}_{\mathrm{RE}}$, the relay node could only maximize the rate of the legitimate channel as much as possible by letting $\mathbf{s}_{\mathrm{DF}} = \mathbf{h}_{\mathrm{RB}}/||\mathbf{h}_{\mathrm{RB}}||$, where the MRT is applied. This has been proved in [34][90] for the MISO wiretap channel model, and the conclusion could be utilized for our case. Because the information signal received at Bob (Eve) consists of two parts: the direct transmission from Alice in the first stage and the re-transmission from the relay node in the second stage. Since the former one is unchanged with certain P_a and given the channel condition for a particular time slot, the maximization of secrecy rate only depends on the transmission between the relay node and Bob (Eve) which is actually a MISO fading channel mode.

Therefore, we can rephrase the ergodic secrecy rate expression as

$$\begin{aligned} C_{\text{s-DF}} &= \max_{\mathbf{s}_{\mathrm{DF}}} \{E_{h_{\mathrm{AB}},\mathbf{h}_{\mathrm{RB}}}(R_{\text{B-DF}}) - E_{h_{\mathrm{AE}},\mathbf{h}_{\mathrm{RE}}}(R_{\text{E-DF}})\} \\ &= \frac{1}{2}\{E_{x_1,x_2}[\log_2(1 + P_a x_1 + P_r x_2)] \\ &\quad - E_{x_3,x_4}[\log_2(1 + P_a x_3 + P_r x_4)]\}, \end{aligned} \tag{4.23}$$

where

$$x_1 = ||h_{\mathrm{AB}}||^2 \sim \Gamma(1,1), \tag{4.24}$$

$$x_2 = ||\mathbf{h}_{\mathrm{RB}}^H \mathbf{s}_{\mathrm{DF}}||^2 = ||\mathbf{h}_{\mathrm{RB}}||^2 \sim \Gamma(N,1), \tag{4.25}$$

$$x_3 = ||h_{\mathrm{AE}}||^2 \sim \Gamma(1,1), \tag{4.26}$$

$$\text{and} \qquad x_4 = ||\mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{DF}}||^2 \sim \Gamma(1,1). \tag{4.27}$$

Here $\Gamma(k,\theta)$ denotes the gamma distribution with parameters k and θ. Clearly, x_1, x_2, x_3 and x_4 are non-negative variables and independent from each other. Equation (4.27) is obtained since $\mathbf{h}_{\mathrm{RE}}$ is independent of $\mathbf{h}_{\mathrm{RB}}$. Without loss of generality, we let

$\sigma^2 = 1$ in the rest of this chapter.

Next, we have $P_a x_1 \sim \Gamma(1, P_a)$, $P_r x_2 \sim \Gamma(N, P_r)$, $P_a x_3 \sim \Gamma(1, P_a)$ and $P_r x_4 \sim \Gamma(1, P_r)$, respectively. We then denote $z_1 = P_a x_1 + P_r x_2$ and $z_2 = P_a x_3 + P_r x_4$. The probability distribution functions (PDFs) of z_1 and z_2 are given by

$$\begin{aligned} f(z_1) &= f(P_a x_1) * f(P_r x_2) \\ &= \frac{e^{-\frac{z_1}{P_a}} z_1^N B(1,N) {}_1F_1(N; N+1; (\frac{z_1}{P_a} - \frac{z_1}{P_r}))}{(P_r)^N P_a \Gamma(N)}, \end{aligned} \tag{4.28}$$

and

$$\begin{aligned} f(z_2) &= f(P_a x_3) * f(P_r x_4) \\ &= \frac{e^{-\frac{z_2}{P_r}} - e^{-\frac{z_2}{P_a}}}{(P_r - P_a)}, \end{aligned} \tag{4.29}$$

where $B(a, b)$ is the Beta function and ${}_1F_1(\cdot)$ is the Kummer confluent hypergeometric function [50]. Therefore, the ergodic secrecy rate by using DF is

$$\begin{aligned} C_{\text{s-DF}} &= \frac{1}{2}\{E_{z_1}[\log_2(1+z_1)] - E_{z_2}[\log_2(1+z_2)]\} \\ &= \frac{B(1,N)\int_0^\infty \ln(1+z_1) {}_1F_1(N; N+1; (\frac{z_1}{P_a} - \frac{z_1}{\rho P_r}))e^{-\frac{z_1}{P_a}} z_1^N dz_1}{2(\rho P_r)^N P_a \Gamma(N) \ln 2} \\ &\quad + \frac{1}{2(P_r - P_a)\ln 2}\left[P_r e^{\frac{1}{P_r}} \text{Ei}\left(-\frac{1}{P_r}\right) - P_a e^{\frac{1}{P_a}} \text{Ei}\left(-\frac{1}{P_a}\right)\right], \end{aligned} \tag{4.30}$$

where $\text{Ei}(\cdot)$ is the exponential integral function [47].

4.2.2 Cooperative Jamming

For the CJ scheme, the optimal design of the jamming signal $\mathbf{w}_{\text{CJ}}$ is complicated to derive even with Eve's instant CSI [56]. Therefore, a suboptimal design is to rule out the jamming signal in the legitimate channel. The authors in [56] showed that the suboptimal design would not lead to a significant secrecy rate loss. We then have

$\mathbf{w}_{\text{CJ}} = \mathbf{Z}\mathbf{v}$.

Before proceeding, we first introduce the following lemma.

Lemma 4. If $\mathbf{M} \in \mathbb{C}^{N\times N}$ is a unitary matrix and $\mathbf{h} \in \mathbb{C}^{N\times 1}$ is a vector of i.i.d. zero-mean complex circularly symmetric Gaussian random variables, $\mathbf{M}^H\mathbf{h}$ and $\mathbf{h}^H\mathbf{M}$ have the same distribution as $\mathbf{h}$, and can be replaced by $\mathbf{h}$ in the expectation [34].

We then let $\mathbf{W} = [\mathbf{h}_{\text{RB}}/||\mathbf{h}_{\text{RB}}||, \mathbf{Z}]$. As $\mathbf{Z}$ is the orthonormal basis of the null space of the legitimate channel $\mathbf{h}_{\text{RB}}$, we conclude that $\mathbf{W}$ is a unitary matrix. Moreover, the channel vector $\mathbf{h}_{\text{RE}}$ consists of N i.i.d. CSCG random variables with zero mean and unit variance. According to Lemma 4, the elements of $\mathbf{h}_{\text{RE}}^H\mathbf{Z} \in \mathbb{C}^{(N-1)\times 1}$ are also i.i.d. CSCG random variables with zero mean and unit variance.

Next, we could regard $\text{SINR}_{\text{E-CJ}}$ as the signal-to-interference-plus-noise ratio of a single-branch MMSE diversity combiner with $N-1$ interferers [49]. Thereafter, the ergodic secrecy rate for the CJ becomes

$$\begin{aligned} C_{\text{s-CJ}} &= \max_{\mathbf{w}_{\text{CJ}}}\{E_{h_{\text{AB}},\mathbf{h}_{\text{RB}}}(R_{\text{B-CJ}}) - E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{E-CJ}})\} \\ &= E_{x_1}[\log_2(1+P_a x_1)] - E_{x_5}[\log_2(1+x_5)], \end{aligned} \tag{4.31}$$

where

$$x_5 = \text{SINR}_{\text{E-CJ}} = \frac{P_a||h_{\text{AE}}||^2}{\frac{P_r}{N-1}||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2+1}. \tag{4.32}$$

For the ergodic rate of Bob's channel, we have

$$\begin{aligned} E_{x_1}(R_{\text{B-CJ}}) &= E_{x_1}[\log_2(1+P_a x_1)] \\ &= -\frac{e^{\frac{1}{P_a}}\,\text{Ei}(\text{-}\frac{1}{P_a})}{\ln 2}. \end{aligned} \tag{4.33}$$

Based on [49], the complementary cumulative distribution function (CCDF) of x_5

is given by

$$R(x_5) = \frac{e^{-\alpha_1 x}}{(1+\beta_1 x)^{N-1}}, \tag{4.34}$$

where

$$\alpha_1 = \frac{1}{P_a} \qquad \text{and} \qquad \beta_1 = \frac{P_r}{(N-1)P_a}. \tag{4.35}$$

Accordingly, the ergodic channel rate of Eve's channel $R_{\text{E-CJ}}$ becomes

$$\begin{aligned} E_{x_5}(R_{\text{E-CJ}}) &= E_{x_5}[\log_2(1+x_5)] \\ &= \frac{1}{\ln 2}\int_0^{\infty} \frac{e^{-\alpha_1 x_5}}{(1+x_5)(1+\beta_1 x_5)^{N-1}} dx_5, \end{aligned} \tag{4.36}$$

where (4.36) is obtained through integration by parts [38]. Before proceeding, we let

$$\begin{aligned} \frac{1}{(1+x_5)(1+\beta_1 x_5)^{N-1}} = &\frac{a_1}{(1+\beta_1 x_5)} + \frac{a_2}{(1+\beta_1 x_5)^2} + \cdots \\ &+ \frac{a_{N-1}}{(1+\beta_1 x_5)^{N-1}} + \frac{a_N}{(1+x_5)}, \end{aligned} \tag{4.37}$$

where a_i, $i = 1, \ldots, N$ are the coefficients that could be determined by partial fractional decomposition [50]. Thus,

$$\begin{aligned} E_{x_5}(R_{\text{E-CJ}}) = &\frac{1}{\ln 2}\int_0^{\infty} \left[\sum_{j=1}^{N-1} \frac{a_j e^{-\alpha_1 x_5}}{(1+\beta_1 x_5)^j} \right. \\ &\left. + \frac{a_N e^{-\alpha_1 x_5}}{1+x_5} \right] dx_5. \end{aligned} \tag{4.38}$$

Based on [50], the ergodic secrecy rate by using CJ is derived in the closed-form

expression

$$C_{\text{s-CJ}} = \frac{1}{\ln 2}\Bigg\{ \sum_{i=2}^{N-1} \Bigg[\frac{a_i}{\beta_1^i (i-1)!} \sum_{k=1}^{i-1} (k-1)!(-\alpha_1)^{i-k-1}\beta_1^k - \frac{\text{-}\alpha_1^{i-1}}{(i-1)!} e^{\frac{\alpha_1}{\beta_1}} \text{Ei}\left(\text{-}\frac{\alpha_1}{\beta_1}\right) \Bigg] - \frac{a_1}{\beta_1} e^{\frac{\alpha_1}{\beta_1}} \text{Ei}\left(\text{-}\frac{\alpha_1}{\beta_1}\right) - (a_N+1)e^{\alpha_1}\text{Ei}(\text{-}\alpha_1) \Bigg\}. \tag{4.39}$$

4.2.3 Relaying-and-Jamming

For the RJ scheme, as shown in Section 4.1, we design $\mathbf{s}_{\text{RJ}} = \mathbf{h}_{\text{RB}}/||\mathbf{h}_{\text{RB}}||$ and $\mathbf{w}_{\text{RJ}} = \mathbf{Z}\mathbf{v}$. We then denote $x_6 = ||\mathbf{h}_{\text{RB}}^H \mathbf{s}_{\text{RJ}}||^2$ and $x_6 \sim \Gamma(N,1)$. With the definitions of x_1 and x_6, we have the ergodic rate of Bob's channel as

$$\begin{aligned} E_{h_{\text{AB}},\mathbf{h}_{\text{RB}}}(R_{\text{B-RJ}}) &= \frac{1}{2} E_{h_{\text{AB}},\mathbf{h}_{\text{RB}}}\{\log_2(1+\text{SINR}_{\text{B-RJ}})\} \\ &= \frac{1}{2} E_{x_1,x_6}\{\log_2(1+P_a x_1 + \rho P_r x_6)\}, \end{aligned} \tag{4.40}$$

where $0 < x_1, x_6 < \infty$, and similar to x_2 in Section 4.2.1, we have $P_a x_1 \sim \Gamma(1, P_a)$ and $\rho P_r x_6 \sim \Gamma(N, \rho P_r)$. Defining $z_3 = P_a x_1 + \rho P_r x_6$, we yield the probability distribution function of z_3 as

$$f(z_3) = \frac{e^{\text{-}\frac{z_3}{P_a}} z_3^N B(1,N)_1 F_1(N; N+1; (\frac{z_3}{P_a}\text{-}\frac{z_1}{\rho P_r}))}{(\rho P_r)^N P_a \Gamma(N)}. \tag{4.41}$$

The ergodic channel rate $R_{\text{B-RJ}}$ becomes

$$E_{z_3}(R_{\text{B-RJ}}) = \frac{1}{2}\int_0^\infty \log_2(1+z_3) f(z_3) dz_3. \tag{4.42}$$

Next, we study the ergodic channel rate $R_{\text{E-RJ}}$. Let x_7 and x_8 represent

$$x_7 = P_a ||h_{\text{AE}}||^2, \tag{4.43}$$

$$x_8 = \frac{\rho P_r ||\mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{RJ}}||^2}{\frac{(1-\rho)}{N-1} P_r ||\mathbf{h}_{\mathrm{RE}}^H \mathbf{Z}||^2 + 1}, \tag{4.44}$$

where $x_7 + x_8 = \mathrm{SINR}_{\text{E-RJ}}$. According to Lemma 4, h_{AE}, $\mathbf{h}_{\mathrm{RE}}^H \mathbf{s}_{\mathrm{RJ}}$ and the elements of $\mathbf{h}_{\mathrm{RE}}^H \mathbf{Z}$ are i.i.d. CSCG random variables. Thereafter, we can represent x_8 as the SINR of the single-branch MMSE diversity combiner with $N-1$ interferers [49]. The complementary cumulative distribution function (CCDF) of x_8 is given by

$$R(x_8) = \frac{e^{-\alpha_2 x_8}}{(1+\beta_2 x_8)^{N-1}}, \tag{4.45}$$

where

$$\alpha_2 = \frac{1}{\rho P_r} \quad \text{and} \quad \beta_2 = \frac{1-\rho}{(N-1)\rho}. \tag{4.46}$$

Next, based on $x_7 \sim \Gamma(1, P_a)$ and $R(x_8)$, we have the PDF of $z_4 = x_7 + x_8$ as follows:

$$f(z_4) = f(x_7) * f(x_8) = e^{-\frac{z_4}{P_a}} \beta, \tag{4.47}$$

where

$$\begin{aligned} \beta &= (\frac{1}{P_a})^2 \int_0^\infty \frac{e^{\frac{\rho P_r - P_a}{\rho P_r P_a} x_8}}{(1+\beta_2 x_8)^{N-1}} dx_8 && (4.48) \\ &= (\frac{1}{P_a})^2 \Bigg\{ \sum_{i=2}^{N-1} \Bigg[\frac{b_i}{\beta_2^i (i-1)!} \sum_{k=1}^{i-1} (k-1)! (-\alpha)^{i-k-1} \beta_2^k \\ &\quad - \frac{\text{-}\alpha^{i-1}}{(i-1)!} e^{\frac{\alpha}{\beta_2}} \mathrm{Ei}\left(\text{-}\frac{\alpha}{\beta_2}\right) \Bigg] - \frac{b_1}{\beta_2} e^{\frac{\alpha}{\beta_2}} \mathrm{Ei}\left(\text{-}\frac{\alpha}{\beta_2}\right) \Bigg\}, && (4.49) \end{aligned}$$

where $\alpha = \frac{P_a - \rho P_r}{\rho P_r P_a}$ and b_i, $i = 1, \ldots, N-1$) are the coefficients determined by partial fractional decomposition of $\frac{1}{(1+\beta_2 x_8)^{N-1}}$, i.e., $\sum_{i=1}^{N-1} \frac{b_i}{(1+\beta_2 x_8)^i} = \frac{1}{(1+\beta_2 x_8)^{N-1}}$. Moreover, (4.48) to (4.49) is obtained by using the same method as from (4.38) to (4.39).

Then the expression of Eve's ergodic channel rate is

$$E_{z_4}(R_{\text{E-CJ}}) = \frac{1}{2}\int_0^\infty \log_2(1+z_4) f(z_4) dz_4 = -\frac{1}{2\ln 2}\beta\frac{1}{P_a}e^{\frac{1}{P_a}}\,\text{Ei}\left(-\frac{1}{P_a}\right). \tag{4.50}$$

With (4.42) and (4.50), we finally get the expression (4.51) of the ergodic secrecy rate for the RJ scheme,

$$\begin{aligned} C_{\text{s-RJ}} &= \max_{\rho}\{E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{B-RJ}}) - E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{E-RJ}})\} \\ &= \max_{\rho}\frac{1}{2\ln 2}\left\{\frac{B(1,N)\int_0^\infty \ln(1+z_3)\,{}_1F_1(N;N+1;(\frac{z_3}{P_a}\text{-}\frac{z_3}{\rho P_r}))e^{-\frac{z_3}{P_a}}z_3^N dz_3}{(\rho P_r)^N P_a \Gamma(N)} + \right. \\ &\left. \beta\frac{1}{P_a}e^{\frac{1}{P_a}}\,\text{Ei}\left(-\frac{1}{P_a}\right)\right\}. \end{aligned} \tag{4.51}$$

The mathematical tools like MatLab could be used to calculate these expressions efficiently.

4.3 Optimal Power Allocation Ratio for RJ

In this section, we study how to find the optimal power allocation ratio for the RJ scheme to achieve the maximal ergodic secrecy rate. We first propose a statistical method for the general power budget case, e.g., no specific settlement to P_a and P_r. After that, we study the optimal power allocation ratio for four special power budget cases: 1) $P_a \to 0$, $P_r \to 0$; 2) $P_a \to 0$, $P_r \to \infty$; 3) $P_a \to \infty$, $P_r \to 0$; 4) $P_a \to \infty$, $P_r \to \infty$.

4.3.1 General Power Budget Case

Due to the complexity of (4.51), it is generally difficult to have ρ_{opt} in the explicit expression. However, since the optimization problem is dependent on a single-variable,

we propose a one-dimension search over ρ ($0 \leq \rho \leq 1$) to statistically find ρ_{opt}. The searching process involves computation of $C_{\text{s-RJ}}$ with a fixed ρ. When completing the search, we could easily find the maximal ergodic secrecy rate and the respective power allocation ratio ρ. Note that the accuracy of the result is determined by the minimum step size (denoted as $\Delta\rho$) in the one-dimension search.

4.3.2 Special Power Budget Cases

Although the solution for the general power budget case provides a method to obtain the exact ρ_{opt}, the studies for special power budget cases can provide a direct understanding about the variation of ρ_{opt} under different power supply situations.

Case 1: $P_a \to 0$, $P_r \to 0$

This indicates the case that the power budgets at Alice and the reply node are both small. First, we rewrite the expression of the ergodic secrecy rate achieved by RJ as

$$C_{\text{s-RJ}}(\rho) = E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{B-RJ}}) - E_{h_{\text{AE}},\mathbf{h}_{\text{RE}}}(R_{\text{E-RJ}}). \tag{4.52}$$

Next, in this low-power case, using $\log_2(1+x) \approx x/\ln 2$ at $x \to 0$ yields

$$C_{\text{s-RJ}}(\rho) = \frac{1}{2}E\left\{\log_2\left[\frac{1+P_a||h_{\text{AB}}||^2+\rho P_r||\mathbf{h}_{\text{RB}}||^2}{1+P_a||h_{\text{AE}}||^2+\frac{\rho P_r||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{RJ}}||^2}{\frac{(1-\rho)}{N-1}P_r||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2+1}}\right]\right\} \tag{4.53}$$

$$\begin{aligned}
&\approx \frac{1}{2\ln 2}E\Bigg\{P_a||h_{\text{AB}}||^2+\rho P_r||\mathbf{h}_{\text{RB}}||^2-\Bigg[P_a||h_{\text{AE}}||^2 \\
&\quad+\rho P_r||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{RJ}}||^2+P_a||h_{\text{AE}}||^2\frac{(1-\rho)}{N-1}P_r||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2 \\
&\quad+\frac{(1-\rho)}{N-1}P_r||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2\Bigg]+\frac{(1-\rho)}{N-1}P_r||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2\Bigg\} \\
&= \frac{1}{2\ln 2}\big\{\rho P_r(N-1)-(1-\rho)P_aP_r\big\},
\end{aligned} \tag{4.54}$$

where the index of the expectation operation is omitted. Based on (4.54), the power allocation ratio should approach one in order to have a high ergodic secrecy rate, which indicates that the relay node should assign more power into the information signal rather than the jamming signal. In addition, it can be observed that more antennas equipped at the relay node could increase the achievable ergodic secrecy rate.

Case 2: $P_a \to 0$**,** $P_r \to \infty$

We now consider the relay node with a large power budget when P_a remains small. Accordingly, we can approximate (4.53) as

$$\begin{aligned} C_{\text{s-RJ}}(\rho) &\approx \frac{1}{2}E\left\{ \log_2\left[\frac{\rho P_r||\mathbf{h}_{\text{RB}}||^2}{1+P_a||h_{\text{AE}}||^2+\frac{\rho||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{RJ}}||^2}{\frac{(1-\rho)}{N-1}||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2}}\right]\right\} \\ &= \frac{1}{2}E\left\{ \log_2(P_r||\mathbf{h}_{\text{RB}}||^2) - \log_2\left[\frac{1+P_a||h_{\text{AE}}||^2}{\rho}\right.\right. \\ &\quad \left.\left. + \frac{N-1}{1-\rho}\frac{||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{RJ}}||^2}{||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2}\right]\right\}. \end{aligned} \tag{4.55}$$

Clearly, the optimal ρ depends on the second part of (4.55) which is complicated to solve. Therefore, we apply a common approximation in the study of ergodic secrecy rate, e.g., $E\{\log_2(1+x)\} \approx \log_2 E\{1+x\}$. Note that the same approximation has been used in [85] for its main objective function. The approximation is given by

$$\begin{aligned} C_{\text{s-RJ}}(\rho) \approx \frac{1}{2}E\big\{ \log_2(P_r||\mathbf{h}_{\text{RB}}||^2)\big\} \\ - \frac{1}{2}\log_2\left[\frac{1+P_a}{\rho}+\frac{1}{1-\rho}\right]. \end{aligned} \tag{4.56}$$

Based on (4.56), the optimal ρ equals 0.5 if $P_a = 0$. In real system, P_a is usually larger than 0. Then the optimal ρ should be larger than 0.5 in order to keep the second part of (4.56) small. This shows that when P_r is large enough, it is preferable for the relay node to split the power into both the information signal and the jamming signal rather

than assigning all power to either one only.

Case 3: $P_a \to \infty$**,** $P_r \to 0$

This case describes the situation that Alice owns a large power budget ($P_a \gg P_r$) but needs the relay node's help to achieve the secure transmission. We then have the approximation of (4.53) as

$$C_{\text{s-RJ}}(\rho) \approx \frac{1}{2} E\left\{ \log_2 \left[\frac{P_a ||h_{\text{AB}}||^2}{P_a ||h_{\text{AE}}||^2} \right] \right\}. \tag{4.57}$$

From (4.57), it can be observed that the ergodic secrecy rate is fairly small in this case. The difference between $\text{SINR}_{\text{B-RJ}}$ and $\text{SINR}_{\text{E-RJ}}$ is mainly obtained from the relay's transmission. Due to the advantage of multiple antennas, the relay should assign more power (e.g., $\rho \to 1$) to information signal to achieve positive secrecy rate.

Case 4: $P_a \to \infty$**,** $P_r \to \infty$

In this case, we consider both Alice and the relay node hold enough large power, e.g., $P_a = P_r \to \infty$. The ergodic secrecy rate expression could be approximated as

$$\begin{aligned} C_{\text{s-RJ}}(\rho) &\approx \frac{1}{2} \log_2 E\left\{ \frac{P_a ||h_{\text{AB}}||^2 + \rho P_r ||\mathbf{h}_{\text{RB}}||^2}{P_a ||h_{\text{AE}}||^2 + \frac{\rho ||\mathbf{h}_{\text{RE}}^H \mathbf{s}_{\text{RJ}}||^2}{\frac{(1-\rho)}{N-1} ||\mathbf{h}_{\text{RE}}^H \mathbf{Z}||^2}} \right\} \\ &\approx \frac{1}{2} \log_2 E\left\{ \frac{P_a ||h_{\text{AB}}||^2 + \rho P_r ||\mathbf{h}_{\text{RB}}||^2}{P_a ||h_{\text{AE}}||^2} \right\}. \end{aligned} \tag{4.58}$$

According to (4.58), the optimal power allocation ratio is approaching 1 in this case.

4.4 Optimal Relay Scheme

In this section, with the target to find the optimal relay scheme that obtains the largest ergodic secrecy rate, we study the performance of the three relay schemes under different power constraints.

First, we get

$$C_{\text{s-DF}} = \frac{1}{2}E\left\{ \log_2 \left[\frac{1+P_a||h_{\text{AB}}||^2+P_r||\mathbf{h}_{\text{RB}}||^2}{1+P_a||h_{\text{AE}}||^2+P_r||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{DF}}||^2} \right] \right\}, \tag{4.59}$$

$$C_{\text{s-CJ}} = E\left\{ \log_2 \frac{1+P_a||h_{\text{AB}}||^2}{1+\frac{P_a||h_{\text{AE}}||^2}{P_r||\mathbf{h}_{\text{RE}}^H\mathbf{w}_{\text{CJ}}||^2+1}} \right\}, \tag{4.60}$$

which, together with (4.53), are the ergodic secrecy rates by using DF, CJ and RJ, respectively. We consider two power budget situations: 1) fixing P_a and let P_r vary from small to large (e.g., $0 \to \infty$). This situation refers to that the relay node holds adaptive power budget and chooses a relay scheme to assist a certain user holding the fixed power; and 2) fixing P_r and let P_a vary from small to large. This situation refers to that the relay node has a non-adaptive power budget while the users may have a very different power condition, e.g., $0 \leq P_a \leq \infty$.

4.4.1 Fixed Power Budget at Alice, Varied Power Budget at Relay

When P_r is small, the achievable ergodic secrecy rate by using DF approaches zero. However, when P_r increases, due to the advantage of the multiple-antennas, the legitimate channel rate increases faster than that of the illegitimate channel which leads to a positive $C_{\text{s-DF}}$. Note that when $P_r \to \infty$, (4.59) converges to a value related to N:

$$\lim_{P_r\to\infty} C_{\text{s-DF}} \approx \frac{1}{2}E\left\{ \log_2 \left[\frac{||\mathbf{h}_{\text{RB}}||^2}{||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{DF}}||^2} \right] \right\}$$

$$= \frac{1}{2\ln 2}\big[\psi(N)\big], \tag{4.61}$$

where $\psi(\cdot)$ is the digamma function [47].

For the CJ scheme, the communication system is similar to a point-to-point single-antenna transmission model when P_r is small. Thus, the achievable ergodic secrecy rate is low. When P_r gets larger, higher ergodic secrecy rate $C_{\text{s-CJ}}$ is achieved as Eve experiences stronger interference while Bob gets no jamming signal. However, with $P_r \to \infty$, $C_{\text{s-CJ}}$ asymptotically approaches the limiting value dependent on P_a:

$$\begin{aligned}\lim_{P_r\to\infty} C_{\text{s-CJ}} &\approx E\Big\{\log_2(1+P_a||h_{\text{AB}}||^2)\Big\} \\ &= -\frac{e^{\frac{1}{P_a}}\,\text{Ei}(\text{-}\frac{1}{P_a})}{\ln 2},\end{aligned} \tag{4.62}$$

which indicates that the achievable ergodic secrecy rate for the CJ scheme is restricted by the power budget at the transmitter. Actually, the result matches the intuitive thought that the eavesdropper will be fully confounded by the strong jamming signal, and the secrecy rate reduces to the rate of Alice-Bob channel.

Similar to the DF and CJ schemes, the RJ scheme could only obtain small ergodic secrecy rate when $P_r \to 0$. However, for large P_r, $C_{\text{s-RJ}}(\rho_{opt})$ is still proportion to P_r:

$$\begin{aligned}&\lim_{P_r\to\infty} C_{\text{s-RJ}}(\rho_{opt}) \\ &\quad\approx \frac{1}{2}E\left\{\log_2\left[\frac{\rho_{opt}P_r||\mathbf{h}_{\text{RB}}||^2}{1+P_a||\text{h}_{\text{AE}}||^2+\frac{\rho_{opt}||\mathbf{h}_{\text{RE}}^H\mathbf{s}_{\text{RJ}}||^2}{\frac{(1-\rho_{opt})}{N-1}||\mathbf{h}_{\text{RE}}^H\mathbf{Z}||^2}}\right]\right\},\end{aligned} \tag{4.63}$$

which implies that $C_{\text{s-RJ}}(\rho_{opt})$ could go to infinity if P_r keeps increasing.

These results show that RJ with optimal power allocation ratio is the optimal relay scheme when the relay node has relatively larger power than that of Alice. When P_r is relatively small, the CJ scheme is a preferred solution.

4.4.2 Varied Power Budget at Alice, Fixed Power Budget at Relay

When the DF scheme is in use and P_a is small, $C_{\text{s-DF}}$ depends more on the portion of P_r and positive $C_{\text{s-DF}}$ is achieved according to (4.59). However, when P_a gets larger, the difference between the rates of the legitimate channel and the illegitimate channel becomes smaller and $C_{\text{s-DF}}$ approaches zero. Note that the maximal $C_{\text{s-DF}}$ is also confined by the number of antennas mounted at the relay node based on (4.61).

By using the CJ scheme, the ergodic secrecy rate gets higher when P_a increases. Similar to the performance in the last case, $C_{\text{s-CJ}}$ is limited when $P_a \to \infty$. Hence, the difference is the limit dependent on P_r and N, which is

$$\lim_{P_a \to \infty} C_{\text{s-CJ}} \approx E\Big\{ \log_2 \left(\frac{||h_{\text{AB}}||^2}{||h_{\text{AE}}||^2} \right) \Big\} + E\Big\{ \log_2(1 + P_r ||\mathbf{h}_{\text{RE}}^H \mathbf{w}_{\text{CJ}}||^2) \Big\} \tag{4.64}$$

$$= \frac{1}{\ln 2} e^{\frac{1}{P_r}} \sum_{k=1}^{N-1} E_k \left(\frac{1}{P_r} \right), \tag{4.65}$$

where $E_k(\cdot)$ is the generalized exponential integral. The first part of (4.64) is zero and (4.65) is obtained due to $||\mathbf{h}_{\text{RE}}^H \mathbf{w}_{\text{CJ}}||^2 \sim \Gamma(N-1, 1)$.

We now consider the RJ scheme with optimal power allocation ratio. Similar to the DF scheme, when P_a increases, the rate difference between legitimate and illegitimate channels gets smaller. The achievable ergodic secrecy rate is getting smaller in this situation. When $P_a \to \infty$, the RJ scheme is almost the same as the DF scheme. Our numerical results also prove that.

Therefore, in this case, we could conclude that when P_a is relatively small, the optimal scheme for the relay node is the RJ scheme. To the user with large transmission power, the relay node should apply the CJ scheme instead.

4.5 Numerical Results and Discussions

Figure 4.1: The ergodic secrecy rates achieved by DF, CJ and RJ: theoretical results vs simulation results.

In this section, numerical results are presented to illustrate the performance of DF, CJ and the proposed RJ scheme. The channel $h_{\mathrm{AB}}, h_{\mathrm{AE}}, \mathbf{h}_{\mathrm{RB}}$ and $\mathbf{h}_{\mathrm{RE}}$ are generated from CSCG independent random variables with zero mean and unit variance. The settlements of P_a, P_r and the number of antennas N are given in specific situations.

First, we design a simulation to verify the accuracy of the theoretical (analytical) expressions of the ergodic secrecy rate for different schemes, i.e., (4.30), (4.39) and (4.51). To this end, we set $N = 3$ and choose $P_a = P_r$ changing from -5 dB to 20 dB. In Fig. 4.1, the achievable ergodic secrecy rates for all three schemes are shown. It can be observed that the theoretical results and the simulation results are overlapping.

In the region of -5dB to 0dB, the overlapping dashed line and solid line in the lower position represent the theoretical result and simulation result for CJ. While the lines in the higher position represent the theoretical results and simulation results for both RJ and DF. With Fig. 4.2, in the region of -5dB to 0dB, the optimal power ratio is close to 1. This suggests that most power in relay is assign to information signal, which indicates the RJ becomes DF. This also verifies the overlapping of RJ and DF in the region of -5dB to 0dB.

Note that the slightly non-overlapping part in Fig. 4.2 is due to the minimum step size of one-dimension search of ρ_{opt}. To illustrate this, we have Table 4.1 showing the values of ρ_{opt} in Fig. 4.2. It is observed that the largest difference between ρ_{simu} and ρ_{theo} is 0.01, i.e., the minimum step size of one-dimension search. Therefore, our theoretical expressions about the ergodic secrecy rate are confirmed to be accurate.

Figure 4.2: The optimal power allocation ratio ρ for the RJ scheme: theoretical result vs simulation result.

Table 4.1: Values of ρ_{opt} in Fig. 4.2.

ρ_{simu}	1.00	0.97	0.80	0.75	0.81	0.85
ρ_{theo}	1.00	0.98	0.79	0.76	0.80	0.85

In Fig. 4.2, when P_a and P_r are small, more power needs to be assigned to the information signal, i.e., $\rho_{opt} \to 1$. When the power increases, ρ_{opt} decreases which suggests that more power needs to be allocated to the jamming signal. When both P_a and P_r become very large, ρ_{opt} approaches 1 as discussed in Section 4.3.2.

Figure 4.3: The ergodic secrecy rate achieved by DF, CJ and RJ when $P_a = 10$ dB and $N = 6, 15$.

Now, we fix $P_a = 10$ dB, and let P_r change from -10 dB to 30 dB. The number of antennas is chosen to be 6 and 15. In Fig. 4.3, the maximal ergodic secrecy rate is limited by a value related to N. For CJ, when $P_r \ll P_a$, higher ergodic secrecy rate could be obtained than that by using RJ with optimal ρ. However, when P_r grows large, $C_{\text{s-RJ}}(\rho_{opt})$ can keep increasing while $C_{\text{s-CJ}}$ gets bounded by an asymptotic value related to P_a only. Therefore, when P_r is larger than a certain threshold, e.g., 15 dB when $N = 15$ in this case, the RJ scheme could outperform the CJ scheme.

Figure 4.4: Optimal power allocation ratio for RJ when $P_a = 60$ dB and $N = 6, 15$.

In Fig. 4.4, when $P_r \ll P_a$, e.g., $P_r = -5$ dB, the optimal power allocation ratio approaches zero, which indicates the relay node should assign most of the available power to the jamming signal. With $P_r \to \infty$, ρ_{opt} eventually converges to a constant which is dependent on N as proven in [38, 76].

We then consider the second power design by fixing P_r, e.g., $P_r = 10$ dB and let P_a change from -10 dB to 30 dB. The number of antennas at the relay node remains to be 6 and 15. In Figs. 4.5 and 4.6, the ergodic secrecy rates achieved by using DF, CJ and RJ and the optimal ρ in this case are illustrated, respectively. In Fig. 4.5, it shows that the achievable ergodic secrecy rate by using DF is lower if the transmitter holds

Figure 4.5: The ergodic secrecy rate achieved by DF, CJ and RJ when $P_r = 10$ dB and $N = 6, 15$.

Figure 4.6: Optimal power allocation ratio for RJ when $P_r = 10$ dB and $N = 6, 15$.

larger power supplying. Similar to Fig. 4.3, the maximal $C_{\text{s-DF}}$ gets limited. By using the CJ scheme, it can obtain higher ergodic secrecy rate when P_a increases, and $C_{\text{s-CJ}}$ then reaches the asymptotic limit which is related to P_r and N, as shown in (4.65). By using the RJ scheme, $C_{\text{s-RJ}}(\rho_{opt})$ decreases when P_a gets larger. When $P_a \to \infty$, $C_{\text{s-RJ}}(\rho_{opt})$ approaches $C_{\text{s-DF}}$.

It may be counter-intuitive to have the secrecy rate dropping with increasing P_a. The reason is given as follows. The secrecy rate is defined as the channel rate difference between legitimate channel and illegitimate channel. So simply using more power may not obtain larger secrecy rate. In this simulation result, when P_r is fixed at 10 dB and P_a increases, this scenario represents the variation from Case 2 to Case 3. When power of Alice becomes large, the ergodic channel rate difference between legitimate channel and illegitimate channel actually decreases. That is why when P_a is large, the achievable ergodic secrecy rate becomes small.

In Fig. 4.6, when P_a is relatively small, e.g., $P_a \leq 10$ dB, it is beneficial for the relay node to split its power to both the information signal and the jamming signal. However, if the transmitter has a larger power budget, the relay node needs to spend most power on the information signal to achieve maximal ergodic secrecy rate.

4.6 Conclusion

In this chapter, we have studied the secure transmission between the single-antenna users with the assistance of a multiple-antenna relay node. The eavesdropper's channel was only statistically known and the relay node and the transmitter had individual power constraints. A new hybrid relay scheme, relaying-and-jamming, has been intro-

duced together with two existing schemes: DF and CJ. The power ratio ρ between the information signal and the jamming signal is the key parameter to maximize the achievable ergodic secrecy rate for RJ, which has been found by a one-dimension search method. The expressions of ergodic secrecy rates by using all three schemes have been derived in order to find the optimal relay scheme. With the numerical results, we conclude that the proposed RJ scheme could achieve higher ergodic secrecy rate than those of DF and CJ when the relay node has relatively larger power. In other cases, the RJ scheme will assign all the power to jamming signal which simplifies the relay scheme to the CJ scheme.

Chapter 5

Pilot Spoofing Attack Detection: Energy Ratio Detector

In the previous two chapters, the problem of passive eavesdropping is discussed in MISO and relay wiretap channel model. However, as reviewed in Chapter 2, the adversary could conduct the active attack, e.g., the pilot spoofing attack. In a practical multiple-antenna communication system, a training phase is needed to estimate the channels first. For example, in the time-division-duplex (TDD) system, the legitimate receiver will send the pre-assigned pilot signal (training signal) to the transmitter through uplink channel. These pilot signals are repeatedly used by the system and are usually publicly known. Therefore, an intelligent eavesdropper attacks the training phase by sending the same pilot signal as that of the legal receiver and acts as a normal receiver during the data transmission phase. Such a pilot spoofing attack could lead to the information leakage to the active eavesdropper and also decrease the legitimate channel rate considerably.

The pilot spoofing attack (pilot contamination attack) was first mentioned in [102], where the authors got the idea from the pilot contamination phenomenon. However, reference [102] mainly focused on illustrating the impact brought by the pilot spoofing attack, and studying the optimal energy allocation for the eavesdropper with

full-duplex transmission ability to either jam the legitimate receiver or listen to the information signal. Note that references [104, 105] also studied the choice of the eavesdropper being active (jamming) or passive. Due to all the serious damages this attack could cause, it is important for the legal system to be able to at least detect such an attack. In the literature, there are few works concentrating on solving this pilot spoofing attack [106, 107]. The authors in [106] proposed a random training method, which suggested to use phase-shift keying (PSK) symbols to replace the current pilot signals and detected the pilot spoofing attack by randomly sending two PSK symbols and examining the phase of received signal at the legitimate transmitter. Furthermore, with the assumption of a large number of antennas, the random training method could also work with the consideration of noise. In [107], the authors proposed a two-way training method based on discriminatory channel estimation, claiming that the method could diminish the impact of the pilot spoofing attack by randomly choosing the new designed stochastic pilot signals at the legitimate receiver. However, both methods require to fundamentally change the set of pilot signal designs as well as the channel estimation process, which is not always preferable because the current pilot signal design is not only functioning for the channel estimation but also having other purposes. For example, the orthogonality of pilot signals is used to discriminate legitimate users who transmit at the same time.

Motivated by the fact that the pilot spoofing attack can decrease the signal reception at the legitimate receiver, we propose the energy ratio detector (ERD) by exploring the asymmetry of received signal power levels at the transmitter and the legitimate receiver. Our detection method mainly includes two phases. First, the legitimate receiver (Bob) sends the assigned pilot signal to the transmitter (Alice) via uplink channel, and Alice estimates the channel based on the samples of the signal. Second, Alice calculates the received signal power, modulates that as a data signal and broadcasts it via downlink channel. Bob demodulates the data and calculates the power of his received signal. Bob

then decides whether the system is under pilot spoofing attack or not by comparing the two power levels. Note that Alice utilizes the same power to broadcast the data as that of Bob used for sending the pilot signal. The main feature of our method is to provide high detection performance without any major modifications to the current channel estimation design.

The rest of the chapter is organized as follows. In Section 5.1, the system model utilized in this chapter and related assumptions are introduced. Furthermore, the problems caused by pilot spoofing attack are also included. In Section 5.2, the detailed process of deriving the ERD is given under the general situation, i.e., considering the noise and estimation error. Some insightful results are given in Section 5.3 by considering several special cases. Section 5.4 contains the simulation set-up and results as well as the related discussions. The conclusion and the future work are finally drawn in Section 5.5.

5.1 System Model and Problem Formulation

Figure 5.1: The communication system model used in this chapter. Alice is equipped with multiple antennas, Bob and Eve are single-antenna users.

As illustrated in Fig. 5.1, a three-component system model is considered: one transmitter (Alice), one legitimate receiver (Bob) and one active eavesdropper (Eve). Alice is equipped with M ($M \geq 2$) antennas and both Bob and Eve are single-antenna users. All the antennas are assumed to be omnidirectional and working in half-duplex mode. We consider a TDD communication system, where the downlink channels and the uplink channels are assumed to be reciprocal. The channel training phase is necessary for Alice to gain the CSI in order to apply beamforming for data transmission. This is achieved by having Bob send the pilot signals (denoted as $x_p(n)$) to Alice. Since the pilot signals are repeatedly used and publicly known, it allows the smart

eavesdropper Eve to transmit the same pilot signals to confound Alice[2]. Next we will briefly review the pilot spoofing attack and analyze the damage caused by this attack to the legitimate communication system.

Figure 5.2: The illustration of R_B, R_E changing vs the power of Eve $\mathcal{P}_E$ with $M = 4, 16, 64$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

The received uplink signal at Alice is denoted as

$$\mathbf{y}(n) = (\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)x_p(n) + \mathbf{u}(n), \tag{5.1}$$

where $n = 1, \ldots, N_1$ and N_1 is the number of pilot samples at Alice. The terms $\mathcal{P}_B$ and $\mathcal{P}_E$ are the powers utilized to send the pilot signal by Bob and Eve, respectively. We denote the legitimate channel and illegitimate channel as $\mathbf{h}_B \in \mathbb{C}^{M\times 1}$ and $\mathbf{h}_E \in \mathbb{C}^{M\times 1}$, respectively. In particular,

$$\mathbf{h}_B = \sqrt{\beta_B}\tilde{\mathbf{h}}_B, \tag{5.2}$$

$$\mathbf{h}_E = \sqrt{\beta_E}\tilde{\mathbf{h}}_E, \tag{5.3}$$

where β_B and β_E represent the large-scale fading (e.g., path loss) coefficients for the legitimate channel and illegitimate channel, respectively. The terms $\tilde{\mathbf{h}}_B \in \mathbb{C}^{M\times 1}$ and $\tilde{\mathbf{h}}_E \in \mathbb{C}^{M\times 1}$ then denote the small-scale fading (e.g., multiple path effect) vectors for these two channels, respectively, where each element in $\tilde{\mathbf{h}}_B, \tilde{\mathbf{h}}_E$ is independent and identically distributed (i.i.d) CSCG random variable with zero mean and unit variance, i.e., $\tilde{\mathbf{h}}_B \sim \mathcal{CN}(0, \mathbf{I}_{M\times M}), \tilde{\mathbf{h}}_E \sim \mathcal{CN}(0, \mathbf{I}_{M\times M})$. We assume that the elements in noise vector $\mathbf{u}(n)$ are i.i.d CSCG random variables with zero mean and variance σ^2, i.e., $\mathbf{u}(n) \sim \mathcal{CN}(0, \sigma^2\mathbf{I}_{M\times M})$. We also assume the channels remain stationary in every time slot and independent of each other for different time slots.

[2]The synchronization of transmission from Bob and Eve is assumed, which is related to the transmission frequency, their distances to Alice and etc. The detailed processes on how the synchronization is achieved are beyond the scope of this work.

The channel estimate $\hat{\mathbf{h}}_B$ based on the least square (LS) method [108] of $\mathbf{y}(n)$ is

$$\hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E + \tilde{\mathbf{e}}, \tag{5.4}$$

where $\tilde{\mathbf{e}}$ is the estimation error, i.e., $\tilde{\mathbf{e}} \sim \mathcal{CN}(0, \frac{\sigma^2}{N_1}\mathbf{I}_{M\times M})$. Note that the major interference is the spoofing pilot signal from Eve rather than the channel estimation error caused by noise. Thereafter, in the downlink data transmission phase, Alice utilizes the MRT scheme and the beamformer $\mathbf{w}$ becomes

$$\mathbf{w} = \frac{\hat{\mathbf{h}}_B}{\|\hat{\mathbf{h}}_B\|}, \tag{5.5}$$

and the received signals at Bob and Eve are

$$y_b(n) = \sqrt{\mathcal{P}_A}\mathbf{h}_B^H\mathbf{w}x_d(n) + v_b(n), \tag{5.6}$$

$$y_e(n) = \sqrt{\mathcal{P}_A}\mathbf{h}_E^H\mathbf{w}x_d(n) + v_e(n), \tag{5.7}$$

where $n = 1, \ldots, N_2$ and N_2 is the number of received signal samples at Bob/Eve. Alice sends the data signal $x_d(n)$ with power $\mathcal{P}_A$. Without loss of generality, we could let $\mathcal{P}_A = \mathcal{P}_B$. $v_b(n)$ and $v_e(n)$ are the white Gaussian noise components at Bob and Eve, respectively, i.e., $v_b(n) \sim \mathcal{CN}(0, \sigma^2)$ and $v_e(n) \sim \mathcal{CN}(0, \sigma^2)$. Then the average signal-to-noise-ratios (SNRs) at Bob and Eve are given by

$$\mathrm{SNR}_B = \frac{\mathcal{P}_A}{\sigma^2}|\mathbf{h}_B^H\mathbf{w}|^2, \tag{5.8}$$

$$\mathrm{SNR}_E = \frac{\mathcal{P}_A}{\sigma^2}|\mathbf{h}_E^H\mathbf{w}|^2, \tag{5.9}$$

respectively. If there is no pilot spoofing attack, the beamformer $\mathbf{w}$ will be basically in the same direction of $\mathbf{h}_B$ and generate the largest SNR at Bob (based on the MRT property). Thus, with the interference (contamination) caused by $\mathbf{h}_E$, the SNR at Bob

becomes smaller unless $\mathbf{h}_E$ is also in the same direction of $\mathbf{h}_B$:

$$|\mathbf{h}_B^H \mathbf{w}|^2 \leq \|\mathbf{h}_B\|^2. \tag{5.10}$$

The equality in (5.10) is achieved when $\mathbf{h}_E = \alpha \mathbf{h}_B, (\alpha \geq 0)$. However, given that $\mathbf{h}_E$ and $\mathbf{h}_B$ are independent of each other, the probability of equality is rather low.

Furthermore, in Fig. 5.2, the simulation results show that by spending more power in the pilot signal, Eve could gain much more information rate from its channel. Consequently, the legitimate receiver has less information rate, where the achievable information rate is proportional to the SNR, e.g., $R_B \propto \text{SINR}_B$ and $R_E \propto \text{SINR}_E$. Note that when $\mathcal{P}_B = \mathcal{P}_E$, e.g., at 10 dB, the ergodic information rate $R_B = R_E$ as Bob and Eve contribute equally to the channel estimate. When $\mathcal{P}_E$ becomes larger, R_E will exceed R_B.

In order to illustrate the detriment more clearly, we consider two special cases in the following: A) Alice is equipped with a very large number of antennas (a.k.a Massive MIMO); B) Eve utilizes very large power to send the pilot signal.

5.1.1 Large Number of Antennas

In this case, we first introduce a lemma as follows.

Lemma 5. If $\mathbf{a}, \mathbf{b} \in \mathbb{C}^{M \times 1}$ are two i.i.d. vectors with distribution $\mathcal{CN}(0, c\mathbf{I}_{M \times M})$, where c is a constant, we then have [110]:

$$\lim_{M \to \infty} \frac{\mathbf{a}^H \mathbf{b}}{M} \to 0, \tag{5.11}$$

$$\lim_{M \to \infty} \frac{\mathbf{a}^H \mathbf{a}}{M} \to c. \tag{5.12}$$

Applying the above lemma to independent channels $\mathbf{h}_B$ and $\mathbf{h}_E$, we have the SNRs

of Bob and Eve for large M given by

$$\mathrm{SNR}_B \overset{\text{asym}}{=\!=} \frac{\mathcal{P}_A}{\sigma^2} \cdot \frac{\mathcal{P}_B M \beta_B^2}{\mathcal{P}_B \beta_B + \mathcal{P}_E \beta_E}, \tag{5.13}$$

$$\mathrm{SNR}_E \overset{\text{asym}}{=\!=} \frac{\mathcal{P}_A}{\sigma^2} \cdot \frac{\mathcal{P}_E M \beta_E^2}{\mathcal{P}_B \beta_B + \mathcal{P}_E \beta_E}, \tag{5.14}$$

where $\overset{\text{asym}}{=\!=}$ denotes "asymptotically equals". Based on (5.13) and (5.14), the pilot spoofing attack diminishes the SNR_B by injecting $\mathcal{P}_E \beta_E$ to the denominator. On the other hand, the eavesdropper could obtain the SNR of (5.14) rather than 0 due to the attack. Clearly, this shows that as an active eavesdropper, Eve could gain much more than being a passive secret listener.

5.1.2 Large Power at Eavesdropper

In this case, we assume that Eve becomes very aggressive and utilizes very large power to send the pilot signal. Then the asymptotic results of the SNRs at Bob and Eve become

$$\mathrm{SNR}_B \overset{\text{asym}}{=\!=} \frac{\mathcal{P}_A}{\sigma^2} \cdot \frac{|\mathbf{h}_B^H \mathbf{h}_E|^2}{\|\mathbf{h}_E\|^2}, \tag{5.15}$$

$$\mathrm{SNR}_E \overset{\text{asym}}{=\!=} \frac{\mathcal{P}_A}{\sigma^2} \cdot \|\mathbf{h}_E\|^2. \tag{5.16}$$

Based on (5.15) and (5.16), with large power used by Eve, the designed beamformer at Alice is dominated by the illegitimate channel and the majority of the signal power seems to shift toward Eve. If we combine the results in the case of large M, the SNR at Bob will become rather small.

Moreover, even when the system uses a particular encoding-decoding process to achieve the perfect secrecy [3], the pilot spoofing attack could also cause serious damage. The perfect secrecy rate is defined as the difference of information rates between legitimate channel and illegitimate channel [3]. Due to the decrease in the legitimate

channel rate and increase in the illegitimate channel rate under the pilot spoofing attack, it is easily to lead to a non-positive secrecy rate.

Therefore, it is essential for the legitimate parts (Alice and Bob) to be able to detect such a pilot spoofing attack. In the next section, we will introduce the energy ratio detector based on the asymmetry between the received power levels of Alice and Bob when the attack happens.

5.2 Energy Ratio Detector

According to the analysis in the above section, it is understood that the pilot spoofing attack could cause certain decrease in SNR at Bob. This phenomenon motivates the idea of exploring the power difference between Alice and Bob to detect the existence of the pilot spoofing attack.

Firstly, we define two events, H_0 and H_1, i.e., H_0: there exists no active eavesdropper who conducts the pilot spoofing attack; and H_1: the active eavesdropper conducts the pilot spoofing attack trying to steal the information from the transmitter.

In the uplink phase of a given time slot, Bob transmits the assigned pilot signal to Alice and the smart eavesdropper broadcasts the same pilot signal to spoof Alice as well. Then the received signal at Alice is

$$H_0 : \mathbf{y}(n) = \sqrt{\mathcal{P}_B}\mathbf{h}_B x_p(n) + \mathbf{u}(n), \tag{5.17}$$

$$H_1 : \mathbf{y}(n) = (\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)x_p(n) + \mathbf{u}(n). \tag{5.18}$$

Based on $\mathbf{y}(n)$, the channel estimation result is derived as

$$H_0 : \hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \tilde{\mathbf{e}}, \tag{5.19}$$

$$H_1 : \hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E + \tilde{\mathbf{e}}. \tag{5.20}$$

In this chapter, we will prove that the detection threshold has no relation to the channels even with consideration of the estimation error.

Alice then applies the maximum-ratio combining (MRC) to process the received signal, yielding

$$H_0{:}y_a(n) = \frac{\hat{\mathbf{h}}_B^H}{\|\hat{\mathbf{h}}_B\|}[\sqrt{\mathcal{P}_B}\mathbf{h}_B x_p(n) + u(n)], \tag{5.21}$$

$$H_1{:}y_a(n) = \frac{\hat{\mathbf{h}}_B^H}{\|\hat{\mathbf{h}}_B\|}[(\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)x_p(n) + u(n)]. \tag{5.22}$$

Based on $y_a(n)$, we can obtain the average power of received signal in the uplink phase at Alice, which is denoted as

$$Q_1 = \frac{1}{N_1}\sum_{n=1}^{N_1}|y_a(n)|^2. \tag{5.23}$$

Based on the central limit theorem (CLT), if N_1 is large enough, Q_1 can be approximated by a Gaussian distributed random variable with mean μ_1 and variance σ_1^2 [113], i.e., $Q_1 \sim \mathcal{N}(\mu_1, \sigma_1^2)$, where

$$\mu_1 = \begin{cases} \left|\frac{\hat{\mathbf{h}}_B^H \mathbf{h}_B}{\|\hat{\mathbf{h}}_B\|}\right|^2 \mathcal{P}_B + \sigma^2 & \to H_0 \\ \left|\frac{\hat{\mathbf{h}}_B^H(\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)}{\|\hat{\mathbf{h}}_B\|}\right|^2 + \sigma^2 & \to H_1 \end{cases}, \tag{5.24}$$

and

$$\sigma_1^2 = \frac{1}{N_1}\mu_1^2. \tag{5.25}$$

Note that $\hat{\mathbf{h}}_B$ is different under H_0 and H_1 as indicated by (5.19) and (5.20), respectively.

Thereafter, we modulate Q_1 as the data signal[3] $x_q(n)$ and send $x_q(n)$ to Bob through downlink channel by power $\mathcal{P}_A$. We assume Bob could successfully demodulate the signal and obtain the value of Q_1.

Note that there is a possibility that the eavesdropper might be aware of the Q_1 transmission and send the jamming signal to Bob to interfere the reception of Q_1. To prevent such jamming attack, one possible countermeasure is that Alice transmits a variable length of non-confidential message to Bob before Q_1 data and the confidential message are transmitted. By doing so, Eve then cannot determine the position of Q_1 data transmission so it cannot conduct the jamming attack specifically to Q_1 without jeopardizing the possible reception of the confidential information. Otherwise, Eve will become a pure jammer that is against its objective to conduct the pilot spoofing attack, which is to eavesdrop the confidential information between Alice and Bob. Indeed, further study on how to detect a super intelligent eavesdropper who could conduct both the pilot spoofing attack and the jamming attack is an interesting topic for future research direction.

We apply the MRT to the downlink transmission and the received signal at Bob is

$$y_b(n) = \frac{\mathbf{h}_B^H \hat{\mathbf{h}}_B}{\|\hat{\mathbf{h}}_B\|} \sqrt{\mathcal{P}_A} x_q(n) + v(n), \tag{5.26}$$

where $n = 1, \ldots, N_2$ and N_2 is the number of received signal samples at Bob. $v(n)$ is white complex Gaussian noise. Then we derive the average energy of the received signal at Bob as

$$Q_2 = \frac{1}{N_2} \sum_{n=1}^{N_2} |y_b(n)|^2. \tag{5.27}$$

Again based on the CLT, if N_2 is sufficiently large, Q_2 can be approximated by a

[3]If necessary we could apply certain encoding technology to ensure the Bob could decode the value of Q_1. Some redundant data may be needed to fulfil the sequence length.

Gaussian distribution with mean μ_2 and variance σ_2^2, i.e., $Q_2 \sim \mathcal{N}(\mu_2, \sigma_2^2)$, where

$$\mu_2 = \left| \frac{\mathbf{h}_B^H \hat{\mathbf{h}}_B}{\|\hat{\mathbf{h}}_B\|} \right|^2 \mathcal{P}_A + \sigma^2, \tag{5.28}$$

$$\sigma_2^2 = \frac{1}{N_2} \mu_2^2. \tag{5.29}$$

Note that for H_0 and H_1, the expressions of μ_2 appear the same where the difference is in $\hat{\mathbf{h}}_B$.

From (5.24) and (5.28), we can observe that when there is no pilot spoofing attack (under H_0), $\mu_1 = \mu_2$ and $\sigma_1^2 = \sigma_2^2$ if we set $\mathcal{P}_A = \mathcal{P}_B$, which shows Q_1 and Q_2 have the same distributions. However, when the active eavesdropper conducts the pilot spoofing attack (under H_1), based on the analysis in the last section, $\mu_1 \neq \mu_2$ and given the channels are independent, μ_1 is larger than μ_2 for most cases.

According to this observation, we design the detecting mechanism at Bob and let Bob explore the difference between Q_1 and Q_2 by setting the test statistic as $T = Q_2/Q_1$. First, we give the following lemma.

Lemma 6. Let x and y be two independent Gaussian random variables: $x \sim \mathcal{N}(\mu_x, \sigma_x^2)$ and $y \sim \mathcal{N}(\mu_y, \sigma_y^2)$. According to [114], the pdf of $z = x/y$ is given by

$$\begin{aligned} f(z) \;=\; & \frac{b(z)c(z)}{\sqrt{2\pi}\sigma_x\sigma_y a^3(z)} \left[2\Phi\left(\frac{b(z)}{a(z)} \right) - 1 \right] \\ & + \frac{1}{a^2(z)\pi\sigma_x\sigma_y} e^{-\frac{1}{2}(\mu_x^2/\sigma_x^2 + \mu_y^2/\sigma_y^2)}, \end{aligned} \tag{5.30}$$

where

$$a(z) = \sqrt{\frac{z^2}{\sigma_x^2} + \frac{1}{\sigma_y^2}}, \tag{5.31}$$

$$b(z) = \frac{\mu_x}{\sigma_x^2} z + \frac{\mu_y}{\sigma_y^2}, \tag{5.32}$$

and

$$c(z) = e^{\frac{1}{2}\left[b^2(z)/a^2(z) - (\mu_x^2/\sigma_x^2 + \mu_y^2/\sigma_y^2)\right]}. \tag{5.33}$$

Under H_0, based on Lemma 6, let $T = Q_2/Q_1$ where $Q_1 \sim \mathcal{N}(\mu_1, \sigma_1^2 = \frac{1}{N_1}\mu_1^2)$ and $Q_2 \sim \mathcal{N}(\mu_2, \sigma_2^2 = \frac{1}{N_2}\mu_2^2)$. We have $\mu_1 = \mu_2$, and

$$\frac{b(T)}{a(T)} = \frac{N_2 T + N_1}{\sqrt{N_2 T^2 + N_1}}, \tag{5.34}$$

$$\sigma_1 \sigma_2 a(T)^2 = \sqrt{N_1 N_2}(N_2 T^2 + N_1), \tag{5.35}$$

and

$$c(T) = e^{\frac{1}{2}\left[b(t)^2/a(T)^2 - N_1 - N_2\right]}. \tag{5.36}$$

For a sufficiently large N_1 and N_2, the test statistic T under H_0 could be approximated as a random variable with the PDF of $f_0(T)$, where $f_0(T)$ is not related to legitimate channel $\mathbf{h}_B$ or illegitimate channel $\mathbf{h}_E$ but is dependent on the numbers of samples N_1 and N_2. To be specific,

$$\begin{aligned} f_0(T) &= \frac{(N_2 T + N_1)\sqrt{N_1 N_2}}{\sqrt{2\pi}(N_2 T^2 + N_1)^{\frac{3}{2}}} e^{\frac{1}{2}\left[\frac{(N_2 T + N_1)^2}{N_2 T^2 + N_1} - N_1 - N_2\right]} \\ &\left[2\Phi\left(\frac{N_2 T + N_1}{\sqrt{N_2 T^2 + N_1}}\right) - 1\right] + \frac{\sqrt{N_1 N_2}}{\pi(N_2 T^2 + N_1)} e^{-\frac{1}{2}(N_1 + N_2)}, \end{aligned} \tag{5.37}$$

where

$$\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}u^2} du. \tag{5.38}$$

Under H_1, the PDF of T becomes $f_1(T)$:

$$\begin{aligned} f_1(T) &= \frac{\sqrt{N_1N_2}b(T)c(T)}{\sqrt{2\pi}\mu_1\mu_2a^3(T)}\left[2\Phi\left(\frac{b(T)}{a(T)}\right)-1\right] \\ &\quad + \frac{\sqrt{N_1N_2}}{a^2(T)\pi\mu_1\mu_2}e^{-\frac{1}{2}(N_1+N_2)}, \end{aligned} \tag{5.39}$$

where

$$a(T) = \sqrt{\frac{N_2T^2}{\mu_2^2}+\frac{N_1}{\mu_1^2}}, \tag{5.40}$$

$$b(T) = \frac{N_2T}{\mu_2}+\frac{N_1}{\mu_1}, \tag{5.41}$$

and

$$c(T) = e^{\frac{1}{2}\left[b^2(T)/a^2(T)-N_1-N_2\right]}. \tag{5.42}$$

Note that $\Phi(x)$ has been given in (5.38). Moreover, $f_1(T)$ is dependent on μ_1 and μ_2, which indicates the PDF of the test statistic under H_1 is related to the channel realizations of $\mathbf{h}_B$ and $\mathbf{h}_E$.

Based on the PDFs of the test statistic, we can illustrate the probability of false alarm P_{fa} as

$$\begin{aligned} P_{fa} &= \Pr(T<\gamma|H_0;\mathbf{h}_B,\mathbf{h}_E) = \Pr(T<\gamma|H_0) \\ &= \int_{-\infty}^{\gamma} f_0(x)dx. \end{aligned} \tag{5.43}$$

With a given target of P_{fa}, we could calculate a corresponding detection threshold γ [109]. As shown in (5.43), one advantage of our detection method is that we do not require the CSI to obtain the detection threshold. Then the probability of detection P_d is expressed as

$$P_d = \Pr(T < \gamma | H_1; \mathbf{h}_B, \mathbf{h}_E) = \int_{-\infty}^{\gamma} f_1(x)dx. \tag{5.44}$$

Clearly, the performance of the ERD is relying on the channel realizations. In some special occasion, e.g., $\mathbf{h}_E = \alpha \mathbf{h}_E$ ($\alpha \geq 0$), it is difficult for the ERD to detect the existence of the pilot spoofing attack. However, given the condition that two channels are independent, the possibility that the two channels are in the same direction is quite low. When the eavesdropper spends only small power in sending the pilot signal, it is observed that the ERD also face more difficulty to successfully detect the attack. However, if $\mathcal{P}_E$ becomes small, the impact of the pilot spoofing attack will be much weaker as well.

Since the CSI of the legitimate channel and illegitimate channel is unknown, we consider the ergodic probability of detection $\bar{P}_d$

$$\bar{P}_d = E_{\mathbf{h}_B, \mathbf{h}_E}\big[\Pr(T < \gamma | H_1)\big] = E_{\mathbf{h}_B, \mathbf{h}_E}\left[\int_{-\infty}^{\gamma} f_1(x)\right]. \tag{5.45}$$

It is generally complicated to derive the closed-form expression of detection threshold γ and the ergodic probability of detection $\bar{P}_d$, but they can be obtained numerically by mathematical software like MatLab.

5.3 Performance Analysis

In the previous section, the ERD has been introduced for the general situation. Here we study the performance of the ERD in two special cases, e.g., large N_1 and large antenna numbers M, in order to obtain more insightful results.

5.3.1 Detection Performance in Two Special Cases

First, we assume that the sample numbers at Alice, N_1, approaches very large, i.e., $N_1 \to \infty$. The estimation error $\tilde{\mathbf{e}}$ becomes very small and negligible, i.e., $\tilde{\mathbf{e}} \to \mathbf{0}$, results in the channel estimation outcomes

$$H_0 : \hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B, \tag{5.46}$$

$$H_1 : \hat{\mathbf{h}}_B = \sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E. \tag{5.47}$$

Accordingly, the mean value of Q_1 becomes

$$\mu_1 = \begin{cases} \|\mathbf{h}_B\|^2\mathcal{P}_B + \sigma^2 & \to H_0 \\ \|\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E\|^2 + \sigma^2 & \to H_1 \end{cases}, \tag{5.48}$$

and the mean value of Q_2 becomes

$$\mu_2 = \begin{cases} \|\mathbf{h}_B\|^2\mathcal{P}_A + \sigma^2 & \to H_0 \\ \left|\dfrac{\mathbf{h}_B^H(\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)}{\|\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E\|}\right|^2 \mathcal{P}_A + \sigma^2 & \to H_1 \end{cases}. \tag{5.49}$$

When N_1 is very large, we could regard Q_1 as stationary, i.e., $Q_1 \to \mu_1$, as the variance σ_1^2 approaches zero. Therefore, the test statistic T could be simplified to

$$H_0 : T = \frac{Q_2}{\mu_1} \sim \mathcal{N}\left(\mu_{1,0} = 1, \sigma_{1,0}^2 = \frac{1}{N_2}\right), \tag{5.50}$$

$$H_1 : T = \frac{Q_2}{\mu_1} \sim \mathcal{N}\left(\mu_{1,1} = \frac{\mu_2}{\mu_1}, \sigma_{1,1}^2 = \frac{\mu_2^2}{N_2\mu_1^2}\right), \tag{5.51}$$

where

$$\frac{\mu_2}{\mu_1} = \frac{\left|\frac{\mathbf{h}_B^H(\sqrt{\mathcal{P}_A}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E)}{\|\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E\|}\right|^2 \mathcal{P}_B + \sigma^2}{\|\sqrt{\mathcal{P}_B}\mathbf{h}_B + \sqrt{\mathcal{P}_E}\mathbf{h}_E\|^2 + \sigma^2}. \tag{5.52}$$

Now the test statistic is a common Gaussian random variable. Then a simple expression of the detection threshold γ can be derived based on a given probability of false alarm. From (5.43), we get

$$P_{fa} = \Phi\left(\frac{\gamma - \mu_{1,0}}{\sigma_{1,0}}\right) = \Phi\left[\sqrt{N_2}(\gamma - 1)\right], \tag{5.53}$$

and the threshold is

$$\gamma_0 = \frac{\Phi^{-1}(P_{fa})}{\sqrt{N_2}} + 1. \tag{5.54}$$

Based on the derived threshold γ_0, we could obtain the probability of detection P_d as

$$P_d = \Phi\left(\frac{\gamma_0 - \mu_{1,1}}{\sigma_{1,1}}\right) = \Phi\left[\sqrt{N_2}(\frac{\mu_1}{\mu_2}\gamma - 1)\right]. \tag{5.55}$$

Compared with the integrals in (5.37) and (5.39), the expressions of γ_0 and P_d are much easier to calculate.

For the ergodic probability of detection $\bar{P}_d$, it is still complicated to derive due to the double integral over $\mathbf{h}_B$ and $\mathbf{h}_E$. Therefore, we consider another special case that Alice is mounted with a large number of antennas, i.e., $M \to \infty$.

According to Lemma 5, μ_1 in (5.48) becomes

$$\mu_1 = \begin{cases} M\mathcal{P}_B\beta_B + \sigma^2 & \to H_0 \\ M\mathcal{P}_B\beta_B + M\mathcal{P}_E\beta_E + \sigma^2 & \to H_1 \end{cases}, \tag{5.56}$$

and μ_2 in (5.49) becomes

$$\mu_2 = \begin{cases} M\mathcal{P}_A\beta_B + \sigma^2 & \to H_0 \\ \dfrac{\mathcal{P}_A\mathcal{P}_B\beta_B^2 M}{\mathcal{P}_B\beta_B + \mathcal{P}_E\beta_E} + \sigma^2 & \to H_1 \end{cases}. \tag{5.57}$$

We can observe that μ_1 still equals μ_2 in this case and expression (5.50) still holds as well. However, μ_2/μ_1 becomes

$$\frac{\mu_2}{\mu_1} = \frac{\mathcal{P}_A\mathcal{P}_B\beta_B^2 M + (\mathcal{P}_B\beta_B + \mathcal{P}_E\beta_E)\sigma^2}{(\mathcal{P}_B\beta_B + \mathcal{P}_E\beta_E)(\mathcal{P}_B\beta_B M + \mathcal{P}_E\beta_E M + \sigma^2)} \tag{5.58}$$

From (5.58), the test statistic under H_1 is no longer dependent on the instant channel realization $\mathbf{h}_B$ and $\mathbf{h}_B$, but related to the large-scale fading coefficients β_B and β_E. Thus, we obtain

$$\bar{P}_d = P_d = \Phi\left(\frac{\gamma_0 - \mu_{1,1}}{\sigma_{1,1}}\right) = \Phi\left[\sqrt{N_2}\left(\frac{\mu_1}{\mu_2}\gamma - 1\right)\right]. \tag{5.59}$$

5.3.2 Ergodic Information Leakage

In this subsection, we study how much information will be leaked to Eve after implementing the ERD. Based on Fig. 5.2, if Eve utilizes larger power to attack Alice and Bob, it could obtain higher information rate from the illegitimate channel and further decrease the information rate of the legitimate channel. However, using larger $\mathcal{P}_E$ highly increases Eve's risk of being detected by Bob. Obviously, there exists a trade-off between the achieved information rate and probability of being detected. Therefore, we formulate the following problem to examine the maximal achievable ergodic information rate C_E for Eve, which is also the maximal ergodic information leakage from the legitimate system.

$$\begin{aligned} \max_{\mathcal{P}_E} \quad & C_E = (1 - \bar{P}_d)\bar{R}_E \\ \text{s.t.} \quad & \text{given} \quad P_{fa}, 1 \geq P_{fa} \geq 0, \\ & P_0 \geq \mathcal{P}_E \geq 0. \end{aligned} \tag{5.60}$$

This problem illustrates that only when the miss of detection happens, the eavesdropper could have the information rate gain. The achievable ergodic information rate for Eve

is then defined in (5.60). Based on a given probability of false alarm P_{fa}, which leads to a threshold γ, we could calculate the overall miss of detection probability. $\bar{R}_E$ is the ergodic information rate of the illegitimate channel, e.g., $\bar{R}_E = E_{\mathbf{h}_B,\mathbf{h}_E}[\log_2(1+\text{SINR}_E)]$, and $\bar{P}_d$ is given by (5.45). Meanwhile, the eavesdropper holds a certain power budget limit, P_0. When $\mathcal{P}_E$ becomes very large, the detection probability is approaching 1.

In order to find the optimal $\mathcal{P}_E$ that maximizes (5.60), the conventional method is setting the first order of derivative of (5.60) as zero. However, since the expression of (5.60) is almost intractable in the closed-form by utilizing the conventional method, we apply a numerical method to exhaustingly search for the optimal $\mathcal{P}_E$ that achieves the largest ergodic information leakage. The brief description of this method is simple. We set $\mathcal{P}_E$ starting with a small value, e.g., -10 dB, and calculate the corresponding C_E. In next step, we increase the $\mathcal{P}_E$ by a fixed step size and conduct the calculation again until $\mathcal{P}_E$ reaches the power budget. The optimal $\mathcal{P}_E$ is the power level that obtain the largest C_E. Note that $1-\bar{P}_d$ monotonically decreases with $\mathcal{P}_E$ while $\bar{R}_E$ monotonically increases with $\mathcal{P}_E$, which shows there exists only one optimal $\mathcal{P}_E$ and the accuracy of the numerical search is based on the minimum step size.

As will be shown in subsequent numerical results, the ergodic information leakage after implementing the ERD is very low especially compared with that before using ERD as shown in Fig. 5.2. It proves that our ERD could efficiently prevent the legitimate transmission from being eavesdropped.

5.3.3 Post-Detection Action

We have proposed the ERD to detect the pilot spoofing attack. One other important question for the legal system is how to act after the detection process. If the detection result shows no pilot spoofing attack, the transmitter shall proceed the data transmission. However, if the result shows the legal system is under pilot spoofing attack, the legal system may take the opportunity to find out where the eavesdropper is, or still

get the estimations of $\mathbf{h}_B$ and $\mathbf{h}_E$ by having several more handshake communication between Alice and Bob. Since in this chapter, we concentrate on the detection against the pilot spoofing attack, and the discussion of post-detection operation design will be provided in next chapter.

5.4 Numerical Results

Figure 5.3: The comparison of thresholds obtained by theoretical analysis and simulation results. $P_{fa} = 0.1, M = 4$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

In this section, we provide numerical results to validate our proposed ERD. We will show the results under different sample numbers, different power budgets used by Eve, different number of antennas used by Alice, etc. The simulation results are derived from 100000 times of Monte-Carlo experiments. The power budgets at Bob and Alice are 10 dB, e.g., $\mathcal{P}_A = \mathcal{P}_B = 10$ dB. We normalize the noise power as 1, i.e., $\sigma^2 = 1$. The path loss will indeed affect the performance. Basically, we could merge the path loss value and power value and study their effect together. If given other conditions are the same, when the path loss for illegitimate channel is small, like Eve is closer to Alice than Bob does, this indicates that Eves channel will have larger ratio in the estimated channel. This shows that given other conditions are the same, being closer to the transmitter will let Eve easier to be detected by our method. Without loss of generality, we set the large-scale fading coefficients to be one, e.g., $\beta_B = \beta_E = 1$.

Figure 5.4: The probability of detection (P_d) versus different given probability of false alarm (P_{fa}) under $N_1 = N_2 = 1000$ and $N_1 = N_2 = 100$. $M = 4$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

As shown in Fig. 5.3, the simulation thresholds are overlapping with the thresholds obtained from (5.43) for the case of both large sample numbers, e.g., $N_1 = N_2 = 1000$, and small sample numbers, e.g., $N_1 = N_2 = 100$. Note that the latter case is close

to the set-up in a practical system where the sample numbers are usually of several hundreds. Therefore, the overlapping results demonstrate the validity of our theoretical analysis. Moreover, it is observed that with even larger N_1 and N_2, the variance of the test statistic T becomes smaller, which leads the threshold approaching 1. In Fig. 5.4, the detection performance of our proposed ERD is shown under different requirements of P_{fa} and different power budgets at Eve. We also consider both large sample numbers ($N_1 = N_2 = 1000$) and small sample numbers ($N_1 = N_2 = 100$). For the theoretical results, the threshold and the detection probability are obtained based on (5.43) and (5.45), respectively.

We can observe that a larger $\mathcal{P}_E$, a higher required P_{fa} or larger sample numbers can all lead to a higher $\bar{P}_d$. In order to make the ergodic secrecy rate to be zero, the eavesdropper needs to spend at least equal power as that of Bob. In that case, the ERD's detection probability approaches one for different sizes of N_1 and N_2. Furthermore, we test the actual probability of false alarm P_{fa} when we utilize the theoretical threshold derived from (5.43). The results are shown in Table 5.1. The actual P_{fa} levels are all smaller than the require values, which satisfies the demand of the system.

Figure 5.5: The probability of detection (P_d) versus different number of antennas (M). $M = 4, 16, 64$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

The detection performance under different number of antennas, e.g., $M = 4, 16, 64$, is shown in Fig. 5.5. We could observe some interesting phenomenon: when $\mathcal{P}_E$ is large, more antennas could generate higher probability of detection; however, when $\mathcal{P}_E$ is small, e.g., $\mathcal{P}_E < -5$ dB, larger M would lower the detection probability. We could use (5.58) to explain this. Considering $M \to \infty$, we have $\mu_{1,0} = 1$ and $\mu_{1,1} = \mu_2/\mu_1$. In order to achieve high P_d, we need the gap between $\mu_{1,0}$ and $\mu_{1,0}$ to be large enough. Therefore, when $\mathcal{P}_E$ is small, e.g., $\mathcal{P}_E \to 0$, we have (5.58) asymptotically approaches one.

Table 5.1: Comparison of required P_{fa} and actual P_{fa}.

N_1, N_2	1000	1000	100	100
Required P_{fa}	0.10	0.01	0.10	0.01
Actual P_{fa}	0.0999	0.0096	0.0988	0.0087

Figure 5.6: The ergodic information leakage to eavesdropper versus different power at Eve. $P_{fa} = 0.01, M = 4, 16, 64$ and $\mathcal{P}_A = \mathcal{P}_B = 10$ dB.

If M becomes large, the asymptotic value will approach $\mu_{1,0}$. Therefore, in the low $\mathcal{P}_E$ region, more antennas actually reduce the performance of the ERD. However, in the high $\mathcal{P}_E$ region, we the have (5.58) asymptotically approaches $(\mathcal{P}_B/(\mathcal{P}_B + \mathcal{P}_E))^2$. When $\mathcal{P}_E$ is non-negligible, the asymptotic value is apparently smaller than 1, leading to a high detection probability as shown in the figure. Note that if Eve only spends small power, the impact of the pilot spoofing attack will also be very small.

In Fig. 5.6, the ergodic information leakage to Eve is shown under different power budgets and different number of antennas. As explained in Fig. 5.5, more antennas at Alice would have small detection probability in low $\mathcal{P}_E$ region, which means Eve could have a large chance to eavesdrop the communication. Therefore, we can observe in Fig. 5.6 that the optimal $\mathcal{P}_E$ for $M = 64$ is smaller than that for $M = 4$. Moreover, we can see that under $M = 4$, Eve can actually obtain a larger ergodic rate with optimal $\mathcal{P}_E$ than that under $M = 16$. This is because for the optimal $\mathcal{P}_E$ under $M = 4$, it achieves a larger information rate even the probability of successfully eavesdropping is lower. Overall, we could see that the best achievable ergodic rate for Eve is smaller than 0.5 bit/s/Hz, which is not comparable with the rate that Eve can achieve when there is no detection. This shows that our proposed energy ratio detector could efficiently protect the legitimate communication.

5.5 Conclusion

In this chapter, we have studied an active eavesdropping problem, i.e., pilot spoofing attack. The smart eavesdropper sent the identical pilot signal as that of the legitimate receiver to spoof the transmitter, which gained higher data rates in return. Since this attack could cause a lot of damages, we have proposed the energy ratio detector to help the legitimate users to detect such attacks. The ERD is working based on exploring the asymmetry of received signals' power levels at Alice and Eve if there exists the pilot spoofing attack. Our detector does not require to change the design of current pilot signal and drastically redesign the process of current channel estimation process. Finally, numerical results validated the accuracy of our theoretical analysis on the ERD and also proved that the ERD could protect the legitimate users from the pilot spoofing attack efficiently.

Chapter 6

Secure Transmission against Pilot Spoofing Attack

The detection of pilot spoofing attack has been discussed in Chapter 5. With the intention of incurring as less modifications as possible to the current pilot-assisted channel estimation process, the energy ratio detector (ERD) [115] was proposed by exploiting the power imbalance between the transmitter side and the receiver side when they are under attack. Although the ERD provides good detection performance, it is a lack of backup plans to recover the data transmission, which is important when the pilot spoofing attack is detected.

Motivated by this demand, we propose a two-way training based scheme to achieve the goals of detecting the pilot spoofing attack and securely re-transmitting the data signal. As shown in Fig. 6.1, the basic process is that the reverse training is still operating as usual to allow the transmitter to estimate the CSI. Before starting confidential data transmission in the downlink phase, the transmitter first sends the channel estimation results to the receiver, and then conducts the traditional downlink training by having each antenna transmit the pilot signal to the receiver. Therefore, both uplink and downlink channel estimations are available at the receiver, which allows it to make a test based on the difference between two estimation results. The detection

outcome will be fed back to the transmitter together with the downlink channel estimation if needed. The simulation performance shows that our detector, named as two-way training detector (TWTD), could obtain an even higher detection rate than that of ERD. More importantly, if the detection result indicates the existence of pilot spoofing attack, the transmitter could derive the estimations of both legitimate and illegitimate channels. Thus, by applying secure beamforming, the transmitter is able to immediately recover the data transmission while keeping it secret from the adversary.

Figure 6.1: The wiretap channel model with a two-way training based scheme. Alice is equipped with multiple antennas and Bob and Eve are single-antenna users.

The main contributions of our work are summarized as follows. First, the TWTD could achieve even higher detection probability than that of the ERD. Similar to the ERD, our proposed scheme needs no drastic modification to the current transmission structure. Second, unlike the ERD, our scheme is able to estimate both channels, switch to secure beamforming almost immediately and finally achieve positive secrecy rate within the same time frame. Third, even without any prior information about Eve, our scheme is able to obtain the maximal secrecy rate as that of using optimal channel estimation or perfect channel information.

The rest of the chapter is organized as follows. In Section 6.1, we introduce the system model utilized in this chapter and related assumptions. Moreover, the negative impacts caused by pilot spoofing attack are also discussed. In Section 6.2, the detailed detection process of the two-way training detector is given, including the derivation of test threshold and evaluation of detection probability. Section 6.3 illustrates how to recover the secure transmission when the detection result suggests the pilot spoofing attack. Section 6.4 contains the simulation set-up and results as well as the related discussions, which verifies our theoretical analysis. The conclusion is finally drawn in Section 6.5.

6.1 System Model and Problem Formulation

Figure 6.2: The time frame structure with the two-way training based scheme.

We adopt a typical wiretap channel model, in which the transmitter Alice has multiple antennas and both the receiver Bob and the eavesdropper Eve are equipped with a single antenna. In a TDD system, Bob sends the assigned pilot signal to let Alice estimate the channel. Meantime, Eve conducts the pilot spoofing attack by sending the same pilot signal to Alice. In this work, we assume that the channels are block fading, i.e., the CSI remains constant during a given time frame length (denoted as N) and changes independently among different time frames. As shown in Fig. 6.2, the coherence time length N is mainly spitting into three parts: uplink training with N_1, downlink training with N_2 and data transmission for N_d. D_1 indicates the data information of the channel estimation result from Alice. The length of D_1 and resulting feedback are assumed to be short enough and negligible.

The legitimate channel $\mathbf{h}_B \in \mathbb{C}^{M\times 1}$ and illegitimate channel $\mathbf{h}_E \in \mathbb{C}^{M\times 1}$ are

$$\mathbf{h}_B = \sqrt{\beta_B}\bar{\mathbf{h}}_B, \tag{6.1}$$

$$\mathbf{h}_E = \sqrt{\beta_E}\bar{\mathbf{h}}_E, \tag{6.2}$$

where M ($M \geq 2$) is the number of antennas at Alice. β_B and β_E represent the long-term fading components (e.g., shadowing and path-loss) for Bob and Eve, respectively. The vectors $\bar{\mathbf{h}}_B, \bar{\mathbf{h}}_E \in \mathbb{C}^{M\times 1}$ denote the short-term fading coefficients (e.g., multi-path effect), where each element of $\bar{\mathbf{h}}_B, \bar{\mathbf{h}}_E$ is CSCG distributed with zero mean and unit variance. The power budgets at Alice, Bob and Eve are denoted as $\mathcal{P}_A, \mathcal{P}_B$ and $\mathcal{P}_E$, separately. We assume that the power for pilot signal and data signal is the same unless particularly specified.

The received signal at Alice, denoted as $\mathbf{Y}_a$, becomes

$$\mathbf{Y}_a = \sqrt{\mathcal{P}_B}\left(\mathbf{h}_B + \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\mathbf{h}_E\right)\mathbf{x}_{up} + \mathbf{U}, \tag{6.3}$$

where $\mathbf{Y}_a, \mathbf{U} \in \mathbb{C}^{M\times N_1}, \mathbf{x}_{up} \in \mathbb{C}^{1\times N_1}$, and we design $\mathbf{x}_{up}\mathbf{x}_{up}^H = N_1$. $\mathbf{U}$ is the additive Gaussian noise matrix at Alice and each element of $\mathbf{U}$ is independent and identically and distributed (i.i.d) with zero mean and variance σ^2.

Using the linear minimum mean square error (LMMSE) channel estimation method [108], we obtain the uplink channel estimation $\hat{\mathbf{h}}_B$, which is

$$\hat{\mathbf{h}}_B = \mathbf{Y}_a\mathbf{A} = \sqrt{\mathcal{P}_B}\mathbf{h}_B\mathbf{x}_{up}\mathbf{A} + \sqrt{\mathcal{P}_E}\mathbf{h}_E\mathbf{x}_{up}\mathbf{A} + \mathbf{U}\mathbf{A}, \tag{6.4}$$

$$\mathbf{A} = \frac{\mathbf{x}_{up}^H}{\sqrt{\mathcal{P}_B}\sigma^2}\left(\frac{1}{\mathcal{P}_B\beta_B} + \frac{\mathbf{x}_{up}\mathbf{x}_{up}^H}{\sigma^2}\right)^{-1}, \tag{6.5}$$

where $\mathbf{A}$ is pre-designed and (6.5) is obtained based on Matrix Inversion Lemma [116]. Then we could have

$$\hat{\mathbf{h}}_B = \hat{\mathbf{h}}'_B + \mathbf{h}'_E = \mathbf{h}_B + \mathbf{h}'_E + \boldsymbol{\varepsilon}_u, \tag{6.6}$$

where $\mathbf{h}'_E = \sqrt{\mathcal{P}_E}\mathbf{h}_E\mathbf{x}_{up}\mathbf{A}$, and $\boldsymbol{\varepsilon_u}$ is the Gaussian estimation error vector with zero mean and covariance matrix $\sigma^2_{\boldsymbol{\varepsilon}_u}\mathbf{I}_M$. Note that $\mathbf{A}$ is designed to estimate $\mathbf{h}_B$ without knowing the existence of $\mathbf{h}_E$. According to the property of LMMSE, $\hat{\mathbf{h}}'_B$ and $\boldsymbol{\varepsilon}_u$ are two uncorrelated Gaussian random vectors that are also independent from $\mathbf{h}'_E$. Based on the orthogonality principle, ergodically we have $E\{\|\mathbf{h}_B\|^2\} = E\{\|\hat{\mathbf{h}}'_B\|^2\} + E\{\|\boldsymbol{\varepsilon}_u\|^2\}$. Because $\mathbf{h}_B$ and $\boldsymbol{\varepsilon}_u$ are mutually independent, the derived $\sigma^2_{\boldsymbol{\varepsilon}_u}$ is also applicable in a particular time frame. With the Matrix Inversion Lemma again, it yields

$$\sigma^2_{\boldsymbol{\varepsilon}_u} = \frac{\beta_B\sigma^2}{\sigma^2 + \mathcal{P}_B\beta_B N_1}. \tag{6.7}$$

We can see that $\hat{\mathbf{h}}_B$ is now contaminated by the intrusive component $\mathbf{h}'_E$. With no more verifying, Alice utilizes this $\hat{\mathbf{h}}_B$ to design the beamformer $\mathbf{w}$ for the downlink data transmission, e.g., MRT. We express the signal-to-noise ratio (SNR) at Bob and Eve as

$$SNR_B = \frac{\mathcal{P}_A \|\mathbf{h}_B^H \mathbf{w}\|^2}{\sigma^2}, \tag{6.8}$$

$$SNR_E = \frac{\mathcal{P}_A \|\mathbf{h}_E^H \mathbf{w}\|^2}{\sigma^2}, \tag{6.9}$$

respectively, where $\mathbf{w} = \hat{\mathbf{h}}_B / \|\hat{\mathbf{h}}_B\|$. By observing (6.4), we can see that if there is no pilot spoofing attack, e.g., $\mathcal{P}_E = 0$, $\mathbf{w}$ will basically follow the direction to Bob. However, as the attack happens, the direction of $\mathbf{w}$ swings towards Eve. Especially when $\mathcal{P}_E > \mathcal{P}_B$, the portion of $\mathbf{h}_E$ in $\hat{\mathbf{h}}_B$ is larger than that of $\mathbf{h}_B$, which leads to the situation that the beamformer is mainly towards the attacker. In this case, Alice and Bob then cannot achieve any positive secrecy rate, defined as $R_s = \log_2(1 + SNR_B) - \log_2(1 + SNR_E)$ [4].

According to Fig. 6.3, with increasing $\mathcal{P}_E$, the achievable channel rate of Bob is decreasing while that of Eve is increasing. When $\mathcal{P}_E$ reaches the same level as $\mathcal{P}_B$, the achievable secrecy rate will be no longer positive. The simulation results match our analysis. That is, in order to generate non-positive ergodic R_s, the adversary needs to spend at least equal power of a legitimate receiver.

Figure 6.3: The impact to the achievable channel rate when getting pilot spoofing attack. $\mathcal{P}_B = 10$ dB

Since the serious damages could be caused by pilot spoofing attack, it is important for Alice and Bob to have the ability to detect such an attack and also recover secure transmission. Motivated by these requirements, a two-way training based scheme is proposed, where in addition to the reverse training, a downlink training session is implemented to allow the channel estimation at Bob. The TWTD exploits the unbal-

ance of the estimation results at Alice and Bob to decide whether they are under pilot spoofing attack or not. When the attack is indicated by the detection results, Alice and Bob can immediately generate the estimation for both legitimate and illegitimate channels and perform the secure beamforming to re-achieve a positive secrecy rate.

Note that Eve may also attack the downlink training session and interfere with the estimation result at Bob. However, in this case, the most serious damage Eve could create is to jam the channel estimation $\tilde{\mathbf{h}}_B$ at Bob, meaning that Eve could not benefit much from such an attack. Therefore, we focus on the case that Eve attacks Alice only. Moreover, we can show that our TWTD could also successfully detect the pilot spoofing attack to Bob if there is any.

6.2 Two-way Training based Detector

In this section, the detailed process of TWTD is introduced. Firstly, we define two hypothesises: H_0 denotes that there is no pilot spoofing attack; H_1 indicates that Alice is under pilot spoofing attack. The two-way training based channel estimation phase consists of the following two sessions:

6.2.1 Channel Estimation

Uplink Training Session

In this session, Bob transmits the assigned pilot signals to Alice and under H_1, Eve transmits the identical pilot signals to spoof Alice. The received signals become

$$H_0: \quad \mathbf{Y}_a = \sqrt{\mathcal{P}_B}\mathbf{h}_B\mathbf{x}_{up} + \mathbf{U}, \tag{6.10}$$

$$H_1: \quad \mathbf{Y}_a = \sqrt{\mathcal{P}_B}\left(\mathbf{h}_B + \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\mathbf{h}_E\right)\mathbf{x}_{up} + \mathbf{U}. \tag{6.11}$$

As discussed in Section 6.1, Alice utilizes the pre-designed LMMSE estimator to handle the incoming signal $\mathbf{Y}_a$ and obtains

$$H_0: \quad \hat{\mathbf{h}}_B = \mathbf{h}_B + \boldsymbol{\varepsilon}_u, \tag{6.12}$$

$$H_1: \quad \hat{\mathbf{h}}_B = \hat{\mathbf{h}}'_B + \mathbf{h}'_E = \mathbf{h}_B + \mathbf{h}'_E + \boldsymbol{\varepsilon}_u, \tag{6.13}$$

where the variance of estimation error $\boldsymbol{\varepsilon}_u$ is given in (6.7). Note that $\hat{\mathbf{h}}'_B$ under H_1 actually has the same property as $\hat{\mathbf{h}}_B$ under H_0, e.g., $\hat{\mathbf{h}}'_B$ is uncorrelated to $\boldsymbol{\varepsilon}_u$.

Downlink Training Session

We apply traditional downlink training method in this session, i.e., each antenna at Alice transmits the assigned pilot signal (denoted as $\mathbf{x}_{dn} \in \mathbb{C}^{1\times N'_2}, N_2 = MN'_2$), and Bob then estimates every channel between that antenna of Alice and the antenna of Bob. First, we have

$$\mathbf{Y}_{b,i} = \sqrt{\mathcal{P}_A} h^H_{B,i} \mathbf{x}_{dn} + \mathbf{v}, \tag{6.14}$$

where $h_{B,i}$ represents the channel between i_{th} ($i \in \{1, 2 \cdots M\}$) antenna at Alice to Bob, and $\mathbf{Y}_{b,i}, \mathbf{v} \in \mathbb{C}^{1\times N'_2}$ denote the received signal and white noise at Bob, respectively. Similarly, we design $\mathbf{x}_{dn}\mathbf{x}^H_{dn} = N'_2$. Therefore, the estimation result by utilizing LMMSE estimator is

$$\tilde{h}_{B,i} = A_b \mathbf{Y}^H_{b,i}, \tag{6.15}$$

$$A_b = \frac{1}{\sqrt{\mathcal{P}_A}\sigma^2}\left(\frac{1}{\mathcal{P}_A\beta_B} + \frac{\mathbf{x}_{dn}\mathbf{x}^H_{dn}}{\sigma^2}\right)^{-1}\mathbf{x}_{dn}, \tag{6.16}$$

and

$$\tilde{h}_{B,i} = h_{B,i} + \varepsilon_{d,i}, \tag{6.17}$$

where $\varepsilon_{d,i}$ is the i_{th} channel estimation error. Similarly to (6.7), we obtain

$$\sigma^2_{\varepsilon_{d,i}} = \frac{\beta_B \sigma^2}{\sigma^2 + \mathcal{P}_A \beta_B N_2'}. \tag{6.18}$$

We formate $\tilde{\mathbf{h}}_B = [\tilde{h}_{B,1}, \tilde{h}_{B,2} \cdots \tilde{h}_{B,M}]^T$ and get

$$\tilde{\mathbf{h}}_B = \mathbf{h}_B + \boldsymbol{\varepsilon}_d. \tag{6.19}$$

The noise terms among different channels are independent, in which $\boldsymbol{\varepsilon}_d \sim \mathcal{CN}(0, \sigma^2_{\boldsymbol{\varepsilon}_d} \mathbf{I}_M)$, where $\sigma^2_{\boldsymbol{\varepsilon}_d} = \sigma^2_{\varepsilon_{d,i}}$.

6.2.2 Detection Statistic Design

By observing the estimation results, we can find that under H_0, (6.12) and (6.19) have similar formations but under H_1, (6.13) has an extra component $\mathbf{h}_E'$. This gives Alice and Bob an opportunity to detect the attack's existence.

In a given time frame, the channel conditions $\mathbf{h}_B$ and $\mathbf{h}_E$ are considered to be stationary. Therefore, we can obtain that $\hat{\mathbf{h}}_B \sim \mathcal{CN}(\mathbf{h}_B, \sigma^2_{\boldsymbol{\varepsilon}_u} \mathbf{I}_M)$ under H_0, $\hat{\mathbf{h}}_B \sim \mathcal{CN}(\mathbf{h}_B + \mathbf{h}_E', \sigma^2_{\boldsymbol{\varepsilon}_u} \mathbf{I}_M)$ under H_1, and $\tilde{\mathbf{h}}_B \sim \mathcal{CN}(\mathbf{h}_B, \sigma^2_{\boldsymbol{\varepsilon}_d} \mathbf{I}_M)$. We then have

$$(\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B) \sim \begin{cases} \mathcal{CN}(0, \sigma_1^2 \mathbf{I}_M) & \to H_0 \\ \mathcal{CN}(\mathbf{h}_E', \sigma_1^2 \mathbf{I}_M) & \to H_1 \end{cases}, \tag{6.20}$$

where $\sigma_1^2 = \sigma^2_{\boldsymbol{\varepsilon}_u} + \sigma^2_{\boldsymbol{\varepsilon}_d}$. In real transmission, $\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B$ could be achieved by having Alice encode $\hat{\mathbf{h}}_B$ as data information and send it to Bob before the downlink training session. The problem of detecting Eve based on (6.20) becomes similar to detecting an unknown deterministic signal within the received Gaussian signals [109], while here the "unknown deterministic signal" is actually the illegitimate channel.

In order to differentiate H_0 and H_1, the test statistic T is designed as $T = \|\hat{\mathbf{h}}_B -$

$\tilde{\mathbf{h}}_B\|^2$ inspired by the classic energy detector. The hypothesis test problem is

$$T = \|\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B\|^2 \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma, \tag{6.21}$$

and γ is the test threshold to be determined.

Under H_0, we have

$$T = \frac{\sigma_1^2}{2}\left\|\frac{\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B}{\sigma_1/\sqrt{2}}\right\|^2 \sim \Gamma(M, \sigma_1^2), \tag{6.22}$$

and under H_1, the test statistic becomes

$$T = \frac{\sigma_1^2}{2}\left\|\frac{\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B}{\sigma_1/\sqrt{2}}\right\|^2 = \frac{\sigma_1^2}{2}T', \tag{6.23}$$

$$T' \sim \chi^2_{2M}(\lambda), \tag{6.24}$$

where $\Gamma(k, \theta)$ represents the gamma distribution with a shape parameter k and a scale parameter θ, and $\chi^2_k(\lambda)$ denotes the non-central chi-squared distribution with k degrees of freedom and non-centrality parameter λ. Here λ in (6.24) is

$$\lambda = \frac{2}{\sigma_1^2}\|\mathbf{h}'_E\|^2 = \frac{2\mathcal{P}_E}{\sigma_1^2\mathcal{P}_B}(\|\mathbf{h}_E\|\mathbf{x}_{up}\mathbf{A})^2. \tag{6.25}$$

Given the distribution of T under H_0 and the requirement of probability of false alarming, we could derive the threshold γ of the test statistic:

$$\begin{aligned} P_{fa} &= \Pr\{T > \gamma, |\mathbf{h}_B, \mathbf{h}_E; H_0\} = \Pr\{T > \gamma, |H_0\}, & (6.26)\\ &= \int_{\gamma}^{+\infty} f_0(t)dt = 1 - F_0(\gamma), & (6.27) \end{aligned}$$

where $f_0(t)$ and $F_0(t)$ are the probability density function (PDF) and corresponding cumulative density function (CDF) of T under H_0, respectively. Note that the test threshold derived is not related to the instantaneous channel conditions $\mathbf{h}_B$ or $\mathbf{h}_E$.

Based on the gamma distribution, we obtain

$$F_0(\gamma) = \frac{1}{\Gamma(M)} r\left(M, \frac{\gamma}{\sigma_1^2}\right), \tag{6.28}$$

where $r(a, b)$ is the lower incomplete gamma function. Therefore, the test threshold γ is obtained by performing an inverse operation on $F_0(\gamma)$. Based on the threshold, we can evaluate the performance the TWTD by examining the probability of detection P_d, which is

$$\begin{aligned} P_d &= \Pr\{T > \gamma, |\mathbf{h}_B, \mathbf{h}_E; H_1\} && (6.29)\\ &= \Pr\left\{T' > \frac{2\gamma}{\sigma_1^2}, |\mathbf{h}_E; H_1\right\} = \int_{\frac{2\gamma}{\sigma_1^2}}^{+\infty} f_1(t)dt && (6.30)\\ &= 1 - F_1\left(\frac{2\gamma}{\sigma_1^2}\right), && (6.31) \end{aligned}$$

where $f_1(t)$ and $F_1(t)$ are the PDF and corresponding CDF of T' under H_0, respectively. According to the property of non-central chi-squared distribution, P_d could be rewritten as

$$P_d = 1 - \left[1 - Q_M\left(\sqrt{\lambda}, \sqrt{\frac{2\gamma}{\sigma_1^2}}\right)\right] = Q_M\left(\sqrt{\lambda}, \sqrt{\frac{2\gamma}{\sigma_1^2}}\right), \tag{6.32}$$

where $Q_M(a, b)$ is the Marcum Q-function and λ is given in (6.25). P_d represents the possibility that Alice-Bob could detect the pilot spoofing attack in a particular time frame. Note that this detection performance is related to the channel condition $\mathbf{h}_E$. To evaluate the detection probability of TWTD through the average perspective, $\bar{P}_d$ is introduced, which is the ergodic detection probability

$$\bar{P}_d = E_{\mathbf{h}_E}\{P_d\} = E_{\mathbf{h}_E}\left\{Q_M\left(\sqrt{\lambda}, \sqrt{\frac{2\gamma}{\sigma_1^2}}\right)\right\}, \tag{6.33}$$

where λ is related to $\mathbf{h}_E$.

As aforementioned, the adversary might also conduct pilot spoofing attack to Bob in the downlink as the pilot signals are not re-designed, which may generate another two attacking cases: 1) only Bob is getting attack and 2) both Alice and Bob are attacked. Next, We will succinctly explain that our TWTD could also successfully detect the attack in these cases.

Case 1: Only Bob is attacked

In this case, we consider that only Bob is under attack. Therefore, the uplink training result becomes

$$\hat{\mathbf{h}}_B = \mathbf{h}_B + \boldsymbol{\varepsilon}_u, \tag{6.34}$$

and the downlink training results become

$$H_0: \quad \tilde{h}_{B,i} = h_{B,i} + \varepsilon_{d,i}, \tag{6.35}$$

$$H_1: \quad \tilde{h}_{B,i} = h_{B,i} + h'_{EB} + \varepsilon_{d,i}, \tag{6.36}$$

where h'_{EB} is the Bob-Eve channel component and remains stationary in the same time frame. Then we have

$$H_0: \quad \tilde{\mathbf{h}}_B = \mathbf{h}_B + \boldsymbol{\varepsilon}_d, \tag{6.37}$$

$$H_1: \quad \tilde{\mathbf{h}}_B = \mathbf{h}_B + h'_{EB}\mathbf{1} + \boldsymbol{\varepsilon}_d, \tag{6.38}$$

in which $\mathbf{1} \in \mathbb{C}^{M\times 1}$ represents a vector with every element is one. According to TWTD, $(\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B)$ becomes

$$(\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B) \sim \begin{cases} \mathcal{CN}(0, \sigma_1^2\mathbf{I}_M) & \to H_0 \\ \mathcal{CN}(-h'_{EB}\mathbf{1}, \sigma_1^2\mathbf{I}_M) & \to H_1 \end{cases}, \tag{6.39}$$

We can easily observe that (6.39) is similar to (6.20). The negative sign is negligible in calculating λ. Without too much difficulty, it is shown that our TWTD is still effective.

Case 2: Both Alice and Bob are attacked

We consider that Alice and Bob are both under the pilot spoofing attack. According to (6.12), (6.13), (6.37) and (6.38), we could directly rewrite $(\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B)$ as

$$(\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B) \sim \begin{cases} \mathcal{CN}(0, \sigma_1^2 \mathbf{I}_M) & \rightarrow H_0 \\ \mathcal{CN}(\mathbf{h}'_E - h'_{EB}\mathbf{1}, \sigma_1^2 \mathbf{I}_M) & \rightarrow H_1 \end{cases}, \tag{6.40}$$

With the similar proof given in Case 1, our TWTD is still valid in this attacking situation.

In fact, λ is dependent on the norm of $\mathbf{h}'_E$ in (6.20) and $(\mathbf{h}'_E - h'_{EB}\mathbf{1})$ in this case. As $\mathbf{h}'_E$ and $h'_{EB}\mathbf{1}$ are two i.i.d. Gaussian random vetctors ergodically, so λ is on average even larger in this case, which indicates Eve could more easily be detected. This matches the intuitive thought that if the adversary is more active (attacking both Alice and Bob), it will take higher risk to be caught. Due to this reason and the fact that Eve actually could not benefit much from attacking Bob, we stay put the case that only Alice is attacked.

After detection, Bob will feed back the result to Alice. It is then important for Alice to know how to react to the detection result. If it shows no pilot spoofing attack, Alice can continue MRT in data transmission. When the result indicates the attack, Alice should have a backup plan to recover the secure transmission.

6.3 Secure Transmission

In this section, the procedure of re-achieving the secure data transmission is introduced.

6.3.1 Estimation of Illegitimate Channels

Firstly, Bob feeds the detection result back to Alice along with $\tilde{\mathbf{h}}_B$ when the result implies the pilot spoofing attack. Alice then utilizes $\tilde{\mathbf{h}}_B$ as the correct estimation of $\mathbf{h}_B$, and without loss of generality, we could rewrite

$$\mathbf{h}_B = \tilde{\mathbf{h}}_B + \boldsymbol{\varepsilon}_d. \tag{6.41}$$

Next, Alice intends to obtain the estimation of $\mathbf{h}_E$. According to $\mathbf{h}'_E = \sqrt{\mathcal{P}_E}\mathbf{h}_E\mathbf{x}_{up}\mathbf{A}$, we formate two estimations on $\mathbf{h}_E$, which are

$$\hat{\mathbf{h}}_E = \frac{\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B}{\sqrt{\mathcal{P}_E}\mathbf{x}_{up}\mathbf{A}} = \mathbf{h}_E + \boldsymbol{\varepsilon}_{\hat{e}}, \tag{6.42}$$

$$\tilde{\mathbf{h}}_E = \frac{\hat{\mathbf{h}}_B - \tilde{\mathbf{h}}_B}{\sqrt{\mathcal{P}_B}\mathbf{x}_{up}\mathbf{A}} = \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\mathbf{h}_E + \boldsymbol{\varepsilon}_{\tilde{e}}, \tag{6.43}$$

where $\boldsymbol{\varepsilon}_{\hat{e}}$ and $\boldsymbol{\varepsilon}_{\tilde{e}}$, are the estimation error vectors with Gaussian distribution, respectively, i.e., $\boldsymbol{\varepsilon}_{\hat{e}} = \frac{\boldsymbol{\varepsilon}_u - \boldsymbol{\varepsilon}_d}{\sqrt{\mathcal{P}_E}\mathbf{x}_{up}\mathbf{A}} \sim \mathcal{CN}(0, \sigma^2_{\boldsymbol{\varepsilon}_{\hat{e}}}\mathbf{I}_M)$ and $\boldsymbol{\varepsilon}_{\tilde{e}} = \frac{\boldsymbol{\varepsilon}_u - \boldsymbol{\varepsilon}_d}{\sqrt{\mathcal{P}_B}\mathbf{x}_{up}\mathbf{A}} \sim \mathcal{CN}(0, \sigma^2_{\boldsymbol{\varepsilon}_{\tilde{e}}}\mathbf{I}_M)$. As $\mathcal{P}_E$ is usually unknown in realistic situations, we regard $\hat{\mathbf{h}}_E$ is the optimal estimation and $\tilde{\mathbf{h}}_E$ is the practical estimation result, which we have $\tilde{\mathbf{h}}_E = \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\hat{\mathbf{h}}_E$. Clearly, $\hat{\mathbf{h}}_E$ is more accurate than $\tilde{\mathbf{h}}_E$ as the channel estimation. With the knowledge of $\tilde{\mathbf{h}}_B$ and $\hat{\mathbf{h}}_E$ (or $\tilde{\mathbf{h}}_E$), Alice could apply secure beamforming that can maximize the achievable secrecy rate denoted as R_s [34]. Let $\mathbf{s}_d \in \mathbb{C}^{1\times N_d}$ and $\mathbf{X}_d \in \mathbb{C}^{M\times N_d}$ represent the data signal before and after precoding, respectively.

$$\mathbf{X}_d = \mathbf{w}\mathbf{s}_d. \tag{6.44}$$

The received signals at Bob and Eve are

$$\mathbf{y}_b = \sqrt{\mathcal{P}_A}{\mathbf{h}_B}^H\mathbf{X}_d + \mathbf{v}_b, \tag{6.45}$$

$$\mathbf{y}_e = \sqrt{\mathcal{P}_A}{\mathbf{h}_E}^H\mathbf{X}_d + \mathbf{v}_e, \tag{6.46}$$

where $\mathbf{v}_b$ and $\mathbf{v}_e$ represent the Gaussian noise at Bob and Eve with zero mean and variance σ^2, respectively. Given (6.41) and (6.42), we may then rewrite

$$\begin{aligned} \mathbf{y}_b &= \sqrt{\mathcal{P}_A}(\tilde{\mathbf{h}}_B + \boldsymbol{\varepsilon}_d)^H \mathbf{X}_d + \mathbf{v}_b \\ &= \sqrt{\mathcal{P}_A}\tilde{\mathbf{h}}_B^H \mathbf{X}_d + (\sqrt{\mathcal{P}_A}\boldsymbol{\varepsilon}_d^H \mathbf{X}_d + \mathbf{v}_b) \\ &= \sqrt{\mathcal{P}_A}\tilde{\mathbf{h}}_B^H \mathbf{X}_d + \mathbf{v}_b', \end{aligned} \tag{6.47}$$

and

$$\begin{aligned} \mathbf{y}_e &= \sqrt{\mathcal{P}_A}(\hat{\mathbf{h}}_E + \boldsymbol{\varepsilon}_{\hat{e}})^H \mathbf{X}_d + \mathbf{v}_e \\ &= \sqrt{\mathcal{P}_A}\hat{\mathbf{h}}_E^H \mathbf{X}_d + (\sqrt{\mathcal{P}_A}\boldsymbol{\varepsilon}_{\hat{e}}^H \mathbf{X}_d + \mathbf{v}_e) \\ &= \sqrt{\mathcal{P}_A}\hat{\mathbf{h}}_E^H \mathbf{X}_d + \mathbf{v}_e', \end{aligned} \tag{6.48}$$

where $\boldsymbol{\varepsilon}_{\hat{e}} = \sqrt{\frac{\mathcal{P}_B}{\mathcal{P}_E}}\boldsymbol{\varepsilon}_{\tilde{e}}$. Based on the orthogonality principle of LMMSE, $\tilde{\mathbf{h}}_B$ is uncorrelated with $\boldsymbol{\varepsilon}_d$ and the instantaneous SNR at Bob could be written as

$$SNR_B = \frac{\mathcal{P}_A \|\mathbf{w}^H \tilde{\mathbf{h}}_B\|^2}{\mathcal{P}_A \|\mathbf{w}^H \boldsymbol{\varepsilon}_d\|^2 + \sigma^2}. \tag{6.49}$$

To Eve, we have following lemma.

Lemma 7. Given (6.13), (6.19), (6.42) and (6.43), $\hat{\mathbf{h}}_E$ and $\tilde{\mathbf{h}}_E$ are uncorrelated with $\boldsymbol{\varepsilon}_{\hat{e}}$ and $\boldsymbol{\varepsilon}_{\tilde{e}}$, respectively.

To prove Lemma 7, it is equivalent to prove both $\hat{\mathbf{h}}_B$ and $\tilde{\mathbf{h}}_B$ are uncorrelated with $\boldsymbol{\varepsilon}_u$ and $\boldsymbol{\varepsilon}_d$. According to

1. $\mathbf{h}_E'$ is independent from $\boldsymbol{\varepsilon}_u$ and $\boldsymbol{\varepsilon}_d$,

2. $\hat{\mathbf{h}}_B'$ is independent from $\boldsymbol{\varepsilon}_d$ and uncorrelated with $\boldsymbol{\varepsilon}_u$,

3. $\tilde{\mathbf{h}}_B$ is independent from $\boldsymbol{\varepsilon}_u$ and uncorrelated with $\boldsymbol{\varepsilon}_d$.

Based on 1), 2) and (6.13), we can see that $\hat{\mathbf{h}}_B$ is uncorrelated with $\boldsymbol{\varepsilon}_u$ and $\boldsymbol{\varepsilon}_d$. Based on 3), $\tilde{\mathbf{h}}_B$ is proved to be uncorrelated with $\boldsymbol{\varepsilon}_u$ and $\boldsymbol{\varepsilon}_d$. Due to the fact that $\sqrt{\mathcal{P}_E}\mathbf{x}_{up}\mathbf{A}$ is a scalar value which does not affect the non-correlation, so the proof of Lemma 7 is completed.

Therefore, we could represent the SNR of Eve as

$$SNR_E = \frac{\mathcal{P}_A \|\mathbf{w}^H \hat{\mathbf{h}}_E\|^2}{\mathcal{P}_A \|\mathbf{w}^H \boldsymbol{\varepsilon}_{\hat{e}}\|^2 + \sigma^2}. \tag{6.50}$$

6.3.2 Secure Beamformer Design

Based on Lemma 7 in [117] and [118], the achievable secrecy rate $R_s(\mathbf{w})$ could be approximated as

$$R_s(\mathbf{w}) = \log_2\left(\frac{1+SNR_B}{1+SNR_E}\right) \approx R'_s(\mathbf{w}), \tag{6.51}$$

$$R'_s(\mathbf{w}) = \log_2\left(\frac{1+\alpha\|\mathbf{w}^H\tilde{\mathbf{h}}_B\|^2}{1+\hat{\beta}\|\mathbf{w}^H\hat{\mathbf{h}}_E\|^2}\right), \tag{6.52}$$

where $\alpha = \mathcal{P}_A/(\mathcal{P}_A\sigma^2_{\boldsymbol{\varepsilon}_d} + \sigma^2)$ and $\hat{\beta} = \mathcal{P}_A/(\mathcal{P}_A\sigma^2_{\boldsymbol{\varepsilon}_{\hat{e}}} + \sigma^2)$. For the tractable reason, we target on maximizing $R'_s(\mathbf{w})$ by designing the secure beamformer $\mathbf{w}$. $R'_s(\mathbf{w})$ could be expressed as

$$R'_s(\mathbf{w}) = \log_2\left[\frac{\mathbf{w}^H(\mathbf{I}_M + \alpha\tilde{\mathbf{h}}_B\tilde{\mathbf{h}}_B^H)\mathbf{w}}{\mathbf{w}^H(\mathbf{I}_M + \hat{\beta}\hat{\mathbf{h}}_E\hat{\mathbf{h}}_E^H)\mathbf{w}}\right]. \tag{6.53}$$

Due to the monotonicity of the log function, maximizing (6.53) is equivalent to the following optimizing problem:

$$\begin{aligned} \max_{\mathbf{w}} \quad & \frac{\mathbf{w}^H(\mathbf{I}_M + \alpha\tilde{\mathbf{h}}_B\tilde{\mathbf{h}}_B^H)\mathbf{w}}{\mathbf{w}^H(\mathbf{I}_M + \hat{\beta}\hat{\mathbf{h}}_E\hat{\mathbf{h}}_E^H)\mathbf{w}} = \frac{\mathbf{w}^H\mathbf{M}\mathbf{w}}{\mathbf{w}^H\mathbf{N}\mathbf{w}} \\ s.t. \quad & \|\mathbf{w}\|^2 = 1, \\ & \mathbf{M}, \mathbf{N} > 0. \end{aligned} \tag{6.54}$$

Note that (6.54) is a generalized Rayleigh quotient (GRQ) problem. In order to find the optimal beamformer (denoted as $\mathbf{w}^o$) that maximizes the value of (6.54), we recall the Lemma 1 introduced in Chapter 3.

Based on Lemma 1, we could easily find that the optimal secure beamformer which achieves the largest R'_s is the unit-norm generalized eigenvector corresponding to the largest generalized eigenvalue of matrix pencil $(\mathbf{M}, \mathbf{N})$, i.e., $\mathbf{w}^o = \mathbf{e}_{\max}$ and $R'_{s-\max} = R'_s(\mathbf{w}^o) = \log_2(\lambda_{\max})$.

Recall the fact that $\hat{\mathbf{h}}_E$ is our optimal estimation and $\tilde{\mathbf{h}}_E$ is the practical channel estimation, due to unknown $\mathcal{P}_E$. We could have $R''_s(\mathbf{w})$ by replacing $\hat{\mathbf{h}}_E, \boldsymbol{\varepsilon}_{\hat{e}}$ with $\tilde{\mathbf{h}}_E, \boldsymbol{\varepsilon}_{\tilde{e}}$ in (6.48), it then yields

$$R''_s(\mathbf{w}) = \log_2 \left[\frac{\mathbf{w}^H(\mathbf{I}_M + \alpha \tilde{\mathbf{h}}_B \tilde{\mathbf{h}}_B^H)\mathbf{w}}{\mathbf{w}^H(\mathbf{I}_M + \tilde{\beta} \tilde{\mathbf{h}}_E \tilde{\mathbf{h}}_E^H)\mathbf{w}} \right], \tag{6.55}$$

where $\tilde{\beta} = \mathcal{P}_A/(\mathcal{P}_A \sigma^2_{\boldsymbol{\varepsilon}_{\tilde{e}}} + \sigma^2)$. Therefore, in practical situations, we first obtain the beamformer $\mathbf{w}^*$ that maxinzes $R''_s(\mathbf{w})$, and substitute it into (6.53) to evaluate the actual achieved secrecy rate $R'(\mathbf{w}^*)$. According to Lemma 1, it is easy to observe that $\mathbf{w}^*$ is the unit-norm generalized eigenvector corresponding to the largest generalized eigenvalue of matrix pencil $(\mathbf{M}, \mathbf{N}')$, where $\mathbf{N}' = \mathbf{I}_M + \tilde{\beta} \tilde{\mathbf{h}}_E \tilde{\mathbf{h}}_E^H$. Moreover, $R'(\mathbf{w}^*)$ could be written as

$$R'(\mathbf{w}^*) = \log_2 \left[\frac{(\mathbf{w}^*)^H(\mathbf{I}_M + \alpha \tilde{\mathbf{h}}_B \tilde{\mathbf{h}}_B^H)\mathbf{w}^*}{(\mathbf{w}^*)^H(\mathbf{I}_M + \hat{\beta} \hat{\mathbf{h}}_E \hat{\mathbf{h}}_E^H)\mathbf{w}^*} \right]. \tag{6.56}$$

We can conclude that

$$R'(\mathbf{w}^o) \geq R'(\mathbf{w}^*). \tag{6.57}$$

6.3.3 Discussions

The bound in (6.57) illustrates that $R'(\mathbf{w}^o)$ could be regarded as an upper bound to the achievable secrecy rate. So the remaining question is: under what condition that we can achieve the equality in (6.57), or in another word, $\mathbf{w}^* = \mathbf{w}^o$?

First, note that $\tilde{\mathbf{h}}_E = \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\hat{\mathbf{h}}_E$ and $\boldsymbol{\varepsilon}_{\tilde{e}} = \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\boldsymbol{\varepsilon}_{\hat{e}}$. We can expand $\mathbf{N}$ and $\mathbf{N}'$ as

$$\begin{aligned}
\mathbf{N} &= \mathbf{I}_M + \hat{\beta}\hat{\mathbf{h}}_E\hat{\mathbf{h}}_E^H, && (6.58)\\
&= \mathbf{I}_M + \hat{\beta}\frac{\mathcal{P}_B}{\mathcal{P}_E}\tilde{\mathbf{h}}_E\tilde{\mathbf{h}}_E^H, && (6.59)\\
&= \mathbf{I}_M + \frac{\mathcal{P}_A}{\mathcal{P}_A\frac{\mathcal{P}_E}{\mathcal{P}_B}\sigma^2_{\boldsymbol{\varepsilon}_{\hat{e}}} + \frac{\mathcal{P}_E}{\mathcal{P}_B}\sigma^2}\tilde{\mathbf{h}}_E\tilde{\mathbf{h}}_E^H, && (6.60)\\
&= \mathbf{I}_M + \frac{\mathcal{P}_A}{\mathcal{P}_A\sigma^2_{\boldsymbol{\varepsilon}_{\tilde{e}}} + \frac{\mathcal{P}_E}{\mathcal{P}_B}\sigma^2}\tilde{\mathbf{h}}_E\tilde{\mathbf{h}}_E^H, && (6.61)
\end{aligned}$$

and

$$\begin{aligned}
\mathbf{N}' &= \mathbf{I}_M + \tilde{\beta}\tilde{\mathbf{h}}_E\tilde{\mathbf{h}}_E^H, && (6.62)\\
&= \mathbf{I}_M + \frac{\mathcal{P}_A}{\mathcal{P}_A\sigma^2_{\boldsymbol{\varepsilon}_{\tilde{e}}} + \sigma^2}\tilde{\mathbf{h}}_E\tilde{\mathbf{h}}_E^H. && (6.63)
\end{aligned}$$

It is obvious that $\mathbf{N} = \mathbf{N}'$ only if $\mathcal{P}_B = \mathcal{P}_E$. In this case, we can achieve $\mathbf{w}^o = \mathbf{w}^*$. However, what about the situation that $\mathcal{P}_E \neq \mathcal{P}_B$?

As $\mathbf{w}$ is generally unable to be written in the explicit expression, we will discuss the design of $\mathbf{w}$ for two special cases: small $\mathcal{P}_E$ (i.e., $\frac{\mathcal{P}_E}{\mathcal{P}_B} \to 0$) case and large $\mathcal{P}_E$ (i.e., $\frac{\mathcal{P}_E}{\mathcal{P}_B} \to \infty$) case. In the former case, we first generate

$$\mathbf{N}' = \mathbf{I}_M + \tilde{\beta}\frac{\mathcal{P}_E}{\mathcal{P}_B}\hat{\mathbf{h}}_E\hat{\mathbf{h}}_E^H \approx \mathbf{I}_M, \tag{6.64}$$

given that $\tilde{\beta}$ is a constant scalar value with fixed $\mathcal{P}_A$, N_1 and N_2'. By observing (6.55), the design of $\mathbf{w}^*$ reduces to the MRT beamforming over $\tilde{\mathbf{h}}_B$, i.e., $\mathbf{w}^* = \tilde{\mathbf{h}}_B/\|\tilde{\mathbf{h}}_B\|$. Apparently, such $\mathbf{w}^*$ is not the optimal beamformer for (6.53), meaning that $\mathbf{w}^o \neq \mathbf{w}^*$

and $R'(\mathbf{w}^o) > R'(\mathbf{w}^*)$. It shows that in this case, we may not achieve the maximized secrecy rate without knowing $\mathcal{P}_E$. However, according to Fig. 6.3, $\mathcal{P}_E = \mathcal{P}_B$ is the moment when Eve begins to generate a zero ergodic secrecy rate if there is no detection. This implies that from the adversary's perspective, $\mathcal{P}_E$ should not be very small; otherwise, the adversary could not benefit much from the attack.

In the latter case of large $\mathcal{P}_E$, $\tilde{\beta}\frac{\mathcal{P}_E}{\mathcal{P}_B}$ becomes very large. Based on (6.64) again, the design of $\mathbf{w}^*$ is basicly the zero-forcing (ZF) beamformer over $\hat{\mathbf{h}}_E$, i.e., $|\hat{\mathbf{h}}_E^H \mathbf{w}^*| = 0$, and we derive $\mathbf{w}^*$ from following problem

$$\begin{aligned} \max_{\mathbf{w}} \quad & \mathbf{w}^H \mathbf{M} \mathbf{w} \\ s.t. \quad & \|\mathbf{w}\|^2 = 1, \mathbf{M}, \mathbf{N} > 0, \\ & |\hat{\mathbf{h}}_E^H \mathbf{w}^*| = 0. \end{aligned} \tag{6.65}$$

Moreover, $\hat{\beta} = \mathcal{P}_A/(\mathcal{P}_A \sigma^2_{\boldsymbol{\varepsilon}_{\tilde{e}}} \frac{\mathcal{P}_B}{\mathcal{P}_E} + \sigma^2)$ is also very large in this case. For the same reason, the optimization problem (6.54) is equivalent to the above problem (6.65), suggesting that $\mathbf{w}^* = \mathbf{w}^o$ and $R'_s(\mathbf{w}^*) = R'_s(\mathbf{w}^o)$.

Therefore, we can conclude that the equality in (6.57) is achieved under two cases: one is when $\mathcal{P}_B = \mathcal{P}_E$ and the other is in the large $\mathcal{P}_E$ region. It means that we can achieve the optimal ergodic secrecy rate in these two cases even without the knowledge of $\mathcal{P}_E$.

Finally, we could obtain the effective ergodic achievable secrecy rate, denoted as $\bar{C}_s$, is

$$\bar{C}_s = \frac{N - N_1 - N_2}{N} E\{P_d R'_s(\mathbf{w}^*)\}, \tag{6.66}$$

$$= \frac{N - N_1 - N_2}{N} E_{\mathbf{h}_E}\{P_d\} E_{\tilde{\mathbf{h}}_B, \hat{\mathbf{h}}_E}\{R'_s(\mathbf{w}^*)\}, \tag{6.67}$$

where P_d and $R'_s(\mathbf{w}^*)$ are given in (6.32) and (6.55), respectively. We assume that Eve conducts the pilot spoofing attack during all the time frames, and positive secrecy rate

is achieved only when the attack has been detected. We have $\mathbf{h}_E \sim \mathcal{CN}(0, \beta_E \mathbf{I}_M)$, and due to the orthogonality principle of MMSE, we also have $\tilde{\mathbf{h}}_B \sim \mathcal{CN}(0, (\beta_B - \sigma^2_{\boldsymbol{\varepsilon}_d})\mathbf{I}_M)$ and $\hat{\mathbf{h}}_E \sim \mathcal{CN}(0, (\beta_E - \sigma^2_{\boldsymbol{\varepsilon}_{\hat{e}}})\mathbf{I}_M)$. If Alice and Bob spend more time to estimate the channel, i.e., larger N_1, N_2, it is easy to see that we could obtain more accurate $\hat{\mathbf{h}}_B$, $\tilde{\mathbf{h}}_B$ and $\tilde{\mathbf{h}}_E$. Due to the smaller estimation error, we are able to achieve higher detection probability P_d and larger secrecy rate $R'_s(\mathbf{w}^*)$. However, it is also obvious that longer channel training phase will shrink the time for data transmission N_d. Therefore, there exists a trade-off over N_1 and N_2, which is

$$\begin{aligned} \max_{N_1,N_2} \quad & \bar{C}_s \\ s.t. \quad & N_1, N_2 > 0, \\ & N_{\max} > N_1 + N_2 > 0, \end{aligned} \tag{6.68}$$

where $N_{\max}$ is the constraint for the total training length, and $N_{max} \leq N$. Due to the complexity of P_d and $R'_s(\mathbf{w}^*)$, it is difficult to obtain the explicit expressions of optimal N_1, N_2 that optimizes the effective ergodic secrecy rate $\bar{C}_s$. Thus, in Section 6.4, we provide a numerical method to explore and find the optimal N_1, N_2. Certainly, designing a more effective approach to obtain the optimal N_1, N_2 is an interesting problem for the future study.

6.4 Numerical Results

We conduct several computer simulations to verify our theoretical analysis and the corresponding results are presented in this section. Every simulation result is obtained by 10^4 times Monto Carlo experiments. Without loss of generality, the long-term fading coefficients are set to be one, i.e., $\beta_B = \beta_E = 1$, and the power budgets at Alice and Bob are 10 dB, i.e., $\mathcal{P}_A = \mathcal{P}_B = 10$ dB. The antenna number $M = 4$ if there is no other specification. In the simulation, we will verify the impact of different power of

Eve $\mathcal{P}_E$, different lengths (N_1, N_2) of uplink and downlink training.

Figure 6.4: Thresholds derived by simulation and theoretical analysis, $\mathcal{P}_A = \mathcal{P}_B = \mathcal{P}_E = 10$ dB, $M = 4$.

As shown in Fig. 6.4, the threshold values based on simulation and theoretical results are presented under different N_1, N_2 when $\mathcal{P}_E = 10$ dB. It is easy to observe that both results are almost overlapping, which validates the accuracy of our theoretical analysis. Moreover, the overlapping level when $N_1 = 100$ is lower than that when $N_1 = 500$, which is understandable that the threshold will be more accurate with longer training length. As N_1 or N_2 get larger, the threshold gets smaller. This is because a larger training length will generate more accurate channel estimation results, and the test statistic T under H_0 will approach its mean value 0. Therefore, with a given P_{fa}, the derived threshold becomes smaller.

Figure 6.5: Detection probability versus variable $\mathcal{P}_E$ and different requirement of P_{fa}. $\mathcal{P}_A = \mathcal{P}_B = 10$ dB, $M = 4$ and $N_1 = 100$, $N_2 = 400$.

The detection performance of our TWTD is given in Fig. 6.5, in which we present three types of detection probability: 1) P_d obtained by simulations based on simulation threshold; 2) P_d obtained by simulations based on theoretical threshold; 3) P_d derived by theoretical analysis based on theoretical threshold. Given the false alarm probabilities $P_{fa} = 0.01$, 0.001, the three detection probabilities are nearly overlapping. When $\mathcal{P}_E$ is larger than 0 dB, our detection probability is almost 1 which implies that our TWTD could almost detect all the pilot spoofing attacks. Even when $\mathcal{P}_E$ is small, like $\mathcal{P}_E = -10$ dB, the detection probability is still over 90% and 80%, respectively.

Observe that the P_d achieved by simulations based on simulation threshold is usually the smallest, it is because the simulation threshold is slightly larger than the theoretical one (as seen in Fig. 6.4) which generates a relatively smaller detection probability. Due to the same reason, the actual P_{fa} is also slightly larger than the required P_{fa}, e.g., $P_{fa} = 0.011$ when required one is 0.01 and $P_{fa} = 0.0011$ when required one is 0.001.

Figure 6.6: Achievable Secrecy rate versus variable $\mathcal{P}_E$ under different channel estimation cases. $\mathcal{P}_A = \mathcal{P}_B = 10$ dB, $M = 4$ and $N_1 = 100$, $N_2 = 400$.

The performances of achievable secrecy rate by using our proposed two-way training based scheme under practical channel estimation, optimal channel estimation and perfect CSI are illustrated in Fig. 6.6, and the one without detection is also presented as a comparison. Clearly, we can achieve much higher secrecy rate by using the detection and secure beamforming. More accurate channel conditions we have, the larger secrecy rate we could obtain. This phenomenon is more obvious in the low $\mathcal{P}_E$ region, e.g., when $\mathcal{P}_E = 0$ dB, the detection probability approaches 1 according to Fig. 6.5, and the achievable secrecy rate with optimal channel estimation is larger than that with practical channel estimation. However, when $\mathcal{P}_E$ is large, e.g., $\mathcal{P}_E > 10$ dB, utilizing the practical channel estimation could generate as large secrecy rate as that of optimal channel estimation or perfect CSI. This validates our analysis in (6.65). Therefore, we are able to achieve the maximal secrecy rate without knowing exact $\mathcal{P}_E$ in this case.

Figure 6.7: Effective Secrecy rate versus different N_1, N_2. $\mathcal{P}_A = \mathcal{P}_B = \mathcal{P}_E = 10$ dB and $M = 4$.

Figure 6.7 shows the effective secrecy rate achieved by different training length N_1, N_2. We utilize a numerical method to solve the intractable problem in (6.68). We first set the overall length of the time frame to be $N = 15000$, and the maximal allowed length $N_{\max}$ for training session is 600, i.e., $N_1 + N_2 \leq 600$. N_1 starts with a minimal value 20 and increases by a fixed step size $\Delta N_1 = 20$ until it reaches its maximal value $N_{1m} = 200$. N_2 follows a similar process only the step size become $\Delta N_2 = \Delta N_1 \times M$ and its maximal value becomes $N_{2m} = N_{\max} - N_{1m}$. For each pair of (N_1, N_2), we calculate the corresponding effective secrecy rate and we are able to find the largest effective secrecy rate and the optimal training length denoted as (N_1^*, N_2^*). Obviously, the accuracy of this numerical method is dependent on the step size, and a smaller step size may improve the accuracy but consume more computational resources. In

Fig. 6.7, it shows that the optimal $N_1^* = 80, N_2^* = 120$ and the largest $\bar{C}_s = 4.6407$ bits/s/Hz. We could observe that it does not consume all the available training length, which suggests that a long training session is not necessary for achieving the maximal effective secrecy rate.

6.5 Conclusion

In this chapter, we have studied an active eavesdropping problem, i.e., pilot spoofing attack. A two-way training based scheme has been proposed to defend such attack. The scheme first detects the attack by the unbalance of channel estimations at Alice and Bob, and then formats the secure beamforming based on the estimations of legitimate and illegitimate channels. It is shown that the proposed scheme could achieve a high detection probability and recover the secure transmission at the same time. With the further validation of numerical results, our two-way training based scheme has been proven to be able to protect the confidential communication against the pilot spoofing attack.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

Achieving physical layer security in multiple-antenna wiretap channels is highly dependent on the availability of the channel state information. With full knowledge of the legitimate and illegitimate channels, the transmitter is able to design secure beamformer to achieve the largest secrecy rate. However, the eavesdropper could deploy intelligent attacks and steal the information rather than just using passive eavesdropping. In this thesis, the problems of achieving physical layer security have been considered in both the MISO wiretap channels and the cooperative relay wiretap channels when eavesdropper's CSI is only statistically known. In addition, the pilot spoofing attack issue has also been investigated due to its destructive impact to the secure transmission.

The physical layer security problem in MISO fading wiretap channels was first studied by using precoding with artificial noise. For the case that the Eve's channel is available at Alice, the optimal ANaP strategy was proved to be reduced to the conventional precoding strategy, i.e., all the transmit power should be utilized to the information signal. While in the other case when the Eve's channel is unknown at Alice, we derived the optimal power allocation ratio between the information signal and the artificial noise. Our analytical derivations have shown that this power ratio depends

on the number of antennas and the transmit power at the transmitter. In particular, when the available transmit power at Alice increases or the number of antennas at Alice decreases, more power should be allocated to the artificial noise.

Furthermore, we have studied the secure transmission between the single-antenna users with the assistance of a multiple-antenna relay node. The illegitimate channels (from the transmitter or the relay node to the eavesdropper) were assumed only statistically known and the relay node and the transmitter had individual power constraints. Therefore, the ergodic secrecy rate was utilized as the optimizing objective. We have introduced a new hybrid relay scheme, called relaying-and-jamming, together with two other existing schemes: DF and CJ. The power splitting ratio ρ at the relay node between the information signal and the artificial noise is the key parameter to optimize to achieve the maximal achievable ergodic secrecy rate for RJ, which could be found by a one-dimension search method. The expressions of ergodic secrecy rates by using all three schemes have been derived to do the comparison in order to find the optimal relay scheme. With the numerical results, we showed that the proposed RJ scheme could achieve higher ergodic secrecy rate than that of DF or CJ when the relay node has relatively larger energy. In other cases, the CJ scheme might provide better performance.

In addition to the passive eavesdropping discussed in Chapters 3 and 4, we have studied an active eavesdropping problem, i.e., pilot spoofing attack. The intelligent eavesdropper could transmit the identical pilot signal as that of a legitimate receiver to spoof the transmitter, gaining higher data rates in downlink transmission. Due to the serious damages caused by such attacks, we first proposed the energy ratio detector to help the legitimate users to detect such attacks. The ERD explores the asymmetry of received signals' power levels at Alice and Eve if there exists the pilot spoofing attack. We showed that our proposed detector requires no significant modifications to the existing pilot signal pattern or drastically revision of channel estimation process.

Numerical results have validated that our ERD could detect the pilot spoofing attack efficiently.

However, it is not enough to only detect of the pilot spoofing attack. The design should also have the capability to recover secure transmission. Therefore, a two-way training based scheme was proposed to fully defend such attack. The scheme first detects the pilot spoofing attack based on the difference of channel estimation variations at Alice and Bob. With the forward and reverse channel estimation results, it is able to generate the estimation of the legitimate and illegitimate channels and further format the secure beamforming based on such estimations. We have shown that the proposed scheme could not only achieve a high detection probability but recover the secure transmission at the same time.

7.2 Future Work

Among the issues studied in previous chapters, we have considered the case that the receiver and the adversary are equipped with one antenna. The single-antenna deployment allows us to investigate the problem in a tractable way; otherwise it may become extremely complicated. Due to similar reasons, in the relay wiretap channel model, the single antenna set-up is normally applied to the legitimate and illegitimate receiver. However, the multiple antennas deployment in the mobile users becomes common in recent years. Moreover, the malicious eavesdropper is more powerful than a regular receiver in some cases, especially when it is prepared to conduct certain kinds of active attacks. Therefore, the multiple-antenna eavesdropper case is worth studying. Note that the MIMO case has been studied like the secrecy capacity for a MIMO broadcast channel model derived in [10] and the capacity for a Gaussian MIMO channel model was derived [12]. Yet many problems are still open to address, e.g., designing the beamformer for a MIMO fading wiretap channel, or how to quantify the achievable secrecy rate under unknown illegitimate channel.

Another future direction that is worth investigating is to address the physical layer security in the future 5G networks [111]. Secure transmission is always needed in every generation of wireless communication systems. Here we take three potential techniques that may be applied in 5G wireless systems as examples: heterogeneous networks (HetNet), massive MIMO and millimeter wave. The HetNet creates a multi-tier topology where multiple nodes are deployed with dissimilar characteristics such as transmit power budgets, coverage areas, and radio access technologies. Therefore, utilizing the opportunities offered by the multi-tier topology, such as spatial modelling of nodes, association of mobile users, and direct connection between devices, could be an important part in the design of physical layer security. While in the massive MIMO [110], by deploying a very large number of antennas (e.g. a few hundred) at base stations to serve a huge number of users at the same time, massive MIMO keeps all the benefits offered by traditional MIMO systems, but on a much larger scale. With the consideration of applying physical layer security in massive MIMO, some challenges like pilot contamination, power management, channel reciprocity and eavesdropper-resistant signal processing, need to be tackled during the design process. With the above discussion, we believe that the evolution to 5G is unstoppable and it will impose a profound impact on how to achieve physical layer security.

Recently, practical design of physical layer design has been done [119], where the first time a secure prototype is built based on the information theoretical secrecy. As a researcher in this area, promoting the theory to practical is always a alluring direction for future study.

List of Publications

Journal papers

1. Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357-360, Aug. 2014.

2. Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An Energy-Ratio Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932-940, May. 2015.

3. Q. Xiong, Y.-C. Liang, K. H. Li, Y. Gong, and S. Y. Han, "Secure Transmission Against Pilot Spoofing Attack: A Two-Way Training Based Scheme," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1017-1026, May. 2016.

Conference papers

1. Q. Xiong, Y. Gong, and Y.-C. Liang, "Achieving Secrecy Capacity of MISO Fading Wiretap Channels with Artificial Noise," in *IEEE WCNC*, Apr. 2013, pp. 2452-2456.

2. Q. Xiong, K. H. Li, Y.-C. Liang, and Y. Gong, "Secure Transmission with Hybrid Relay Scheme: Relaying and Jamming," *European Modelling Symposium (EMS)*, PP. 220-224, Manchester, Nov. 2013.

3. Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "Detection of Pilot Spoofing Attack in Multi-Antenna systems via Energy-Ratio Comparison," *2015 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, South Brisbane, QLD, 2015, pp. 1747-1751.

4. Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "A Two-Way Training Method for Defending Against Pilot Spoofing Attack in MISO Systems," *2015 IEEE International Conference on Communication (ICC)*, London, 2015, pp. 1880-1885.

Bibliography

[1] W. Stallings, *Cryptography and Network Security Principles and Practices*. Upper Saddle River, NJ: Prentice Hall, 3rd ed., 2003.

[2] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell Syst. Tech. J., vol.28, no.8, pp. 656-715, Oct. 1949.

[3] A. Wyner, "The wiretap channel," Bell Syst. Tech. J., vol.54, no.8, pp. 1355-1387, Oct. 1975.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[5] Y. B. Liang, H. V. Poor, and S. Shamai, "Information Theoretic Security," Foundations and Trends in *Communications and Information Theory*, vol. 5, no. 4-5, pp. 355-580, 2009.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[7] S. K. Leung-Yan-Cheong, "On a special class of wiretap channels," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 5, pp.625 -627, 1977.

[8] Y. B. Liang, H. V. Poor, and S. Shamai(Shitz) "Secure communication over fading channels," *IEEE Trans. Inf. Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2470-2492, June 2008.

[9] A.O. Hero. "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235-3249, Dec. 2013.

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[11] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas - Part I: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.

[12] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas - Part II: The MIMOME Wiretap Channel". *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, July 2010.

[13] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conf. on Inf. Sciences and Syst.(CISS'07)*, Mar. 2007, pp. 905-910.

[14] Z. Li, R. Yates, and W. Traggpe. "Secure Communication with a fading eavesdropper channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, June 2007, pp. 1296-1300.

[15] H. Sato, "An outer bound on the capacity region of broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 374377, May 1978.

[16] H.D. Ly, T. Liu, and Y. B. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477-5487, Nov. 2010.

[17] T. H. Chang, W. C. Chaing, Y. W. P. Hong, and C. Y. Chi, "Joint training and beamforming design for performance discrimination using artificial noise," in *Proc IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, June 5-9, 2011.

[18] S. H. Lai, P. H. Lin, S. C. Lin and H. J. Su, "On Optimal Artificial-Noise Assisted Secure Beamforming for the Fading Eavesdropper Channel," IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) , Sep. 2011.

[19] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, March, 2010, pp. 25622565.

[20] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 12021216, Mar. 2011.

[21] H. H. Qin, X. Chen, Y. Sun, M. Zhao, and J. Wang, "Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications," in *Proc IEEE Int. Conf. Commun. (ICC)*, June 2011, pp. 1-5.

[22] Q. Li and W. K. Ma, "A robust artificial noise aided transmit design for MISO secrecy," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, May 2011, pp. 34363439.

[23] Y. L. Liang, Y. S. Wang, T. H. Chang, Hong, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," in *IEEE International Symposium on Information Theory (ISIT)*, June, 2009, pp.2351,2355.

[24] S. C. Lin, T. H. Chang, Y. L. Liang, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901915, Mar. 2011.

[25] P. K. Gopala, L. F. Lai, and H. E. Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[26] Y. L. Chen and A. J. H. Vinck, "Wiretap Channel With Side Information," in *IEEE International Symposium on Information Theory (ISIT)*, July 2006, pp. 2607-2611.

[27] C. C. Mitrpant, A. J. H. Vinck, and L. Yuan, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181-2190, May 2006.

[28] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 439-441, 1983.

[29] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 12351249, Mar. 2009.

[30] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, vol.55, no.6, pp. 2547-2553, June 2009.

[31] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding," *IEEE Trans. Comm*, vol. 60, no. 11, pp. 3472-3482, Nov. 2012.

[32] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 27352751, Jun. 2008.

[33] M. R. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008.

[34] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, June 2007, pp. 2466–2470.

[35] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. VTC Fall*, vol. 3, Sept. 2005, pp. 1906-1910.

[36] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Tran. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[37] X. Zhou and M. R. McKay, "Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation", in *Proc Int. Conf. on Signal Processing and Commun. Syst. (ICSPCS)*, Omaha, NE, Sept. 2009, pp. 1-5.

[38] X. Zhou and M. R. McKay, "Secret communication with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technology*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

[39] X. Zhang, X. Y. Zhou, and M.R. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Trans. Veh. Technology*, vol. 62, no. 5, pp. 2170-2181, Jun. 2013.

[40] X. Zhou, M. R. McKay, B. Maham, and A. Hjrungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302304, Mar. 2011.

[41] G. Strang, *Linear Algebra and Its Applications*, Wellesley-Cambridge Univ. Press, 1998

[42] Y. Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Tran. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[43] Q. Li and W. K. Ma, "Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799-3812, Aug. 2011.

[44] David A. Harville, *Matrix Algebra From A Statistician's Perspective*, Springer, 1997.

[45] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimizaton Methods and Softw.*, pp. 625-653, 1999.

[46] CVX Research, Inc. *CVX: Matlab software for disciplined convex programming,* version 2.0 beta. http://cvxr.com/cvx, September 2012.

[47] M. Abramowitz and I. A. Stegun, (Eds.) *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, Dover, 1972.

[48] G. Alfano, A. Lozano, A. M. Tulino, and S. Verd, "Mutual information and eigenvalue distribution of MIMO Ricean channels," in *Proc. ISITA*, Parma, Italy, Oct. 2004.

[49] H. Gao, P.J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666-672, May 1998.

[50] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products,* 7th ed. New York: Academic, 2007.

[51] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Beamforming for secrecy rate maximization under outage constraints and partial CSI," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov. 2011, pp. 193-197.

[52] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704-716, Mar. 2012.

[53] S. Gerbracht, A. Wolf, and E. Jorswieck, "Beamforming for Fading Wiretap Channels with Partial Channel Information, in *Proc. of International ITG Workshop on Smart Antennas (WSA)*, Bremen, Germany, Feb. 2010, pp. 394-401.

[54] Y. Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683-1693, Apr. 2011.

[55] P. H. Lin, S. C. Lin, S. H. Lai, and H. J. Su, "On secure beamforming for wiretap channels with partial channel state information at the transmitter," in *Proc. APSIPA ASC*, Hollywood, CA, Dec 2012, pp. 15.

[56] S. Luo, J. Y. Li, and A. P. Petropulu, "Physical Layer Security with Uncoordinated Helpers Implementing Cooperative Jamming," in *IEEE 7th Sensor Array and Multichannel Signal Processing Workshop*, 2012, pp. 97-100.

[57] H.-T. Chiang and J. S. Lehnert, "Optimal cooperative jamming for security," in *MILCOM 2011*, Nov. 2011, pp. 125130.

[58] R. Zhang, L. Song, Z. Han, B. Jiaa, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE GLOBECOM*, Miami, FL, 2010, pp. 1-6.

[59] A. Chorti and H. Y. Poor, "Achievable secrecy rates in physical layer secure systems with a helping interferer," in *IEEE Int. Conference on Computing, Networking and Communications*, Maui, HI, Feb. 2012, pp. 18-22.

[60] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proceedings of the IEEE Workshop on Statistical Signal Processing*, Cardiff, Wales, UK, Aug.-Sept. 2009, pp. 417-420.

[61] J. C. Chen, R. Q. Zhang, L. Y. Song, Z. Han, and B. L. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310320, Feb. 2012.

[62] J. Kim, A. Ikhlef and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Journal of communications and networks*, Vol. 14, no. 4, pp. 364-373. Aug. 2012.

[63] F.S.A. Qahtani, C. J. Zhong, H. M. Alnuweiri, "Opportunistic Relay Selection for Secrecy Enhancement in Cooperative Networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756-1770, May 2015.

[64] Hui Hui; Swindlehurst, A.L.; Guobing Li; Junli Liang, "Secure Relay and Jammer Selection for Physical Layer Security," *IEEE Signal Processing Letters*, vol.22, no.8, pp.1147,1151, Aug. 2015.

[65] Y. L. Zou, X. B. Wang, and W. M. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 20992111, Oct. 2013.

[66] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 50035011, Oct. 2009.

[67] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 60766085, Dec. 2013.

[68] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 34503460, June 2007.

[69] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 17871791, Oct. 2010.

[70] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks." *IEEE, Trans. Signal Process.*, vol.61, no. 6, pp. 1544-1554, Mar. 2013.

[71] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.* vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[72] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1132-138.

[73] J. Y. Li, A. P. Petropulu, and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[74] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317-1322, Mar. 2011.

[75] J. Mo, M. Tao, and Y. Liu, "Relay Placement for Physical Layer Security: A Secure Connection Perspective", *IEEE Communication Letter*, vol. 16, no. 6, pp. 878881, June 2012.

[76] Q. Xiong, Y. Gong, and Y.-C. Liang, "Achieving Secrecy Capacity of MISO Fading Wiretap Channels with Artificial Noise," in *IEEE WCNC*, Apr. 2013, pp. 2452-2456.

[77] R. Q. Zhang, L. Y. Song, Z. Han, and B. L. Jiao, "Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers," *IEEE Trans. Veh. Technology*, vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[78] Z. G. Ding, M. Xu, J. H. Lu, and F. Liu, "Improving Wireless Security for Bidirectional Communication Scenarios," *IEEE Trans. Veh. Technology*, vol. 61, no. 6, pp. 2842-2848, July 2012.

[79] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. ICC*, Jun. 2010, pp. 1-5.

[80] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. 44th Annu. Conf. Inform. Sci. Syst. (CISS)*, Syndeney, Australia, Mar. 2010, pp. 16.

[81] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Princeton, NJ, Apr. 2010, pp. 16.

[82] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 35323545, Jul. 2012.

[83] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[84] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528-3540, Oct. 2011.

[85] X. Wang, K. Wang, and X. D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technology*, vol. 62, no. 5, pp. 2140-2155, Jun. 2013.

[86] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The gaussian wiretap channel with a helping interferer," in *Proc. IEEE Int. Symp. Information Theory(ISIT)*, Toronto, Canada, July 2008, pp. 389393.

[87] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696-1707, Apr. 2012.

[88] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011.

[89] J. Li and A. P. Petropulu, "Explicit solution of worst-case secrecy rate for MISO wiretap channels with spherical uncertainty," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3892-3895, Jul. 2012.

[90] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176-1187, Apr. 2011.

[91] J. Y. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels With Rician fading". *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861-867, Sept. 2011.

[92] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357-360, Aug. 2014.

[93] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 793-808, Dec. 2007.

[94] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948-5956, Dec. 2009.

[95] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492-503, Sept. 2009.

[96] L. Xiao, A. Reznik, W. Trappe, C. X. Ye, Y. Shah, L. J. Greenstein, and N. B. Mandayam, "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. GLOBECOM*, Dec. 2010, pp. 1-6.

[97] F. J. Liu, X. B. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. MILCOM*, Nov. 2011, pp. 538-542.

[98] J. Yang, Y. Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44-58, Jan. 2013.

[99] V. Aggarwal, L. Lai, R. Calderbank, and H. V. Poor, "Wiretap channel type II with an active eavesdropper," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 19441948.

[100] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 8291, Jan. 2013.

[101] V. Guruswami and P. Indyk, "Efficiently decodable low-rate codes meeting Gilbert Varshamov bound," in *Proc. 41st Annual Allerton Conference on Communication, Control and Computing*, Sept. 2003, pp. 7982-7989.

[102] X. Y. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903-907, Mar. 2012.

[103] S. Shahbazpanahi, A. Gershman, and J. Manton, "Closed-form blind MIMO channel estimation for orthogonal space-time block codes," *IEEE Trans. Signal Process.*, vol. 53, no. 12, pp. 4506-4517, Dec. 2005.

[104] A. Garnaev and W. Trappe, "The eavesdropping and jamming dilemma in multi-channel communications," in *Proc. ICC*, June 2013, pp. 2160-2164.

[105] S. M. Perlaza, A. Chorti, H. V. Poor, and Z. Han, "On the impact of network-state knowledge on the feasibility of secrecy," in *Proc.IEEE ISIT*, July 2013. pp. 2960-2964.

[106] D. Kapetanovi, G. Zheng, K. K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. PIMRC*, Sept. 2013, pp. 13-18.

[107] J. J. Yang, S. L. Xie, X. Y. Zhou, R. Yu, and Y. Zhang, "A semiblind two-way training method for discriminatory channel estimation in MIMO systems," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2400-2410, July 2014.

[108] S. M. Kay, *Fundamentals of Statistical Signal Processing: Volume 1 Estimation Theory*, New Jersey: Prentice Hall international, 1998.

[109] S. M. Kay, *Fundamentals of Statistical Signal Processing: Volume 2 Detection Theory*, New Jersey: Prentice Hall international, 1998.

[110] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Proces. Mag.*, vol. 30, no. 1, pp. 40-46, Jan. 2013.

[111] J.G. Andrews, S. Buzzi, Wan Choi, S.V. Hanly, A. Lozano, A.C.K. Soong, and J.C. Zhang,"What Will 5G Be?," *Selected Areas in Communications, IEEE Journal on*, vol.32, no.6, pp. 1065-1082, June 2014.

[112] N. Yang, L. F. Wang, G. Geraci, M. Elkashlan, J. H. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Comm. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[113] Y.-C. Liang, Y. H. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[114] D. V. Hinkley, "On the ratio of two correlated normal random variables". *Biometrika*, vol. 56, no. 3, pp. 635-639, Dec. 1969.

[115] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An Energy-Ratio Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932-940, May. 2015.

[116] D. J. Tylavsky and G. R. L. Sohie, "Generalization of the matrix inversion lemma," *Proceedings of the IEEE*, vol. 74, no. 7, pp. 1050-1052, July 1986.

[117] T.-Y. Liu, S.-C. Lin, T.-H. Chang and Y. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. ICC*, 10-15 June 2012, pp. 4782-4787.

[118] T. Yoo and A. Goldsmith , "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203-2214, May 2006.

[119] Q. Wang, K. Ren, G. Li, C. Xia, X. Chen and Z. Wang et al. "Walls Have Ears! Opportunistically Communicating Secret Messages Over the Wiretap Channel: from Theory to Practice," *The 22nd ACM Sigsac Conference on Computer and Communications Security*, pp. 376-387, 2015.