Ph.D. DISSERTATION

Optimization and Allocation for Secure Communication in Two-hop Relay Network with Cooperative Jamming

협력 재밍을 이용한 중계 네트워크의 보안 통신을 위한 최적화 및 할당 기법

BY

Yongyun Choi

FEBRUARY 2019

DEPARTMENT OF ELECTRICAL AND
COMPUTER ENGINEERING
COLLEGE OF ENGINEERING
SEOUL NATIONAL UNIVERSITY

Optimization and Allocation for Secure Communication in Two-hop Relay Network with Cooperative Jamming

Doctoral Dissertation

Submitted in February of 2019 to the Graduate School

of Seoul National University

in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy

in

Electrical and Computer Engineering

by

Yongyun Choi

Department of Electrical and Computer Engineering

College of Engineering

Seoul National University

Abstract

Physical layer security is a promising technology in the upcoming fifth generation (5G) wireless communication because the wireless communication is vulnerable to eavesdrop and it is complex to encrypt a data signal. In physical layer security, secure transmission is satisfied by using the physical characteristics of the wireless channel. Cooperative jamming is one of the efficient techniques to enhance secrecy performance in physical layer security. In cooperative jamming, a cooperating node transmits a jamming signal to interfere the eavesdropper. However, this jamming signal effects not only the eavesdropper but also the destination, which degrades the secrecy performance and causes waste of transmit power. It means the jamming signal transmission needs to be designed properly with optimization and power allocation to enhance security.

The dissertation consists of two main results. First, we investigate a two-hop relay network consists of a source, an AF relay, a destination, and an eavesdropper. In this network, cooperative jamming is utilized in which the destination and the source transmit jamming signals in phase 1 and 2, respectively. At the destination, its own jamming signal transmitted in phase 1 is perfectly cancelled, and the jamming signal

from the source has negligible strength due to the weak channel condition from the source to destination. We propose an optimal source power allocation for the network to enhance the secrecy performance based on the channel knowledge available at the source. Simulation results show that the proposed source power allocation scheme achieves higher secrecy rate and lower secrecy outage probability than the fixed power allocation schemes.

Second, we investigate a two-hop relay network consists of a source, multiple AF relays, a destination, and an eavesdropper. In this network, one relay is selected out of the relays to forwards the data signals. Also, cooperative jamming is utilized in which the destination and the source transmit jamming signals in phase 1 and 2, respectively. We propose power allocation and relay selection scheme to minimize secrecy outage probability with the total power constraint and the power constraints for each phases, respectively. In total power constraint case, power allocation and relay selection problem is formulated and it is divided into a master problem and a subproblem by using the primal decomposition method. Simulation results show that the proposed scheme achieves lower secrecy outage probability than the conventional jamming power allocation scheme as well as without jamming scheme.

Keywords: Physical layer security, cooperative jamming, secrecy rate, secrecy outage probability, relay network, amplify-and-forward, power allocation, relay selection, primal decomposition

Student Number: 2013-20895

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Secure communication is an important issue due to the broadcast nature of radio propagation in wireless communications. The purpose of the secure communication is to transmit source data to the legitimate destination while the eavesdroppers are not able to interpret this information. As one of the attractive approach, physical layer security has been studied widely because it does not need any encryption methods. The main concept of the physical layer security is to exploit the physical characteristics of the wireless channel in order to transmit the source data securely.

In this chapter, Section 1.1 provides the background of the physical layer security in wireless communication. Section 1.2 describes the outline of this dissertation. In Section 1.3, we provide the notations, the list of the abbreviations, and some mathematical definitions and functions used throughout the dissertation.

1.1 Background and Related Work

1.1.1 Physical Layer Security

Due to the vulnerability to eavesdropping in wireless communications, secure communication is an important issue, especially in military and homeland security applications. To satisfy secure communication, many encryption methods are investigated, in which a specific key cryptosystem or key protocols are needed [1, 2]. In [1], public key protocols are considered and in [2], a new signature scheme is designed that achieves a public key cryptosystem.

Meanwhile, the physical layer security is appealing because it does not need any higher-layer encryption methods [3]. In [3], the source and destination can exchange perfectly secure messages at a non-zero rate, while the eavesdropper earn nothing about the messages. A rate at which information can be transmitted secretly from the source to destination is termed an achievable secrecy rate.

Many early works on physical layer security considers different version of wiretap channel conditions [4–6]. In [4], the channel condition is considered in which the main channel is noiseless and the wiretap channel is a binary symmetric channel. In [5], more general version of wiretap channel is considered to obtain an achievable rate. In [6], the main channel is noiseless but the wiretapper has access to an arbitrary subset of the main coded bits. However, when the main channel is weaker than the wiretap channel, it is hard to achieve positive secrecy performance.

Artificial noise transmission, where an artificially generated noise is transmitted

from the source to interrupt the eavesdropper, is considered as a candidate technique to physical layer security [7–12]. In [7], an achievable rate of the network with artificial noise transmission is obtained. In [8], a transmit beamforming is designed to enhance the secrecy performance. In [9], an outage secrecy region is introduced to evaluate the secrecy performance from a geometrical perspective. In [10], artificial noise transmission in multiple eavesdropper case is investigated. In [11], the design of artificial noise aided transmission is investigated in slow fading channel. In [12], more generalized beamforming is considered in which the secrecy rate is maximized. However, all of these works have to assume multiple antennas at the transmitter in order to use the beamforming technique to interrupt the eavesdropper, not the destination.

1.1.2 Cooperative Jamming

Cooperative jamming is first introduced in 2008 as one of the efficient technique to enhance secrecy performances [13]. In cooperative jamming, a non-transmitting user helps to increase the secrecy performance by transmitting a jamming signal [14–17]. In [13], users whose secrecy rate constraints are not satisfied transmit a jamming signal to help the other users. In [14], two user interference channel is considered and the two users transmit their own data signal as well as the jamming signal.

Also, there are some works in which a friendly jammer exists to transmit a jamming signal [15–20]. In [18], a new security metrics, jamming coverage and jamming efficiency, are introduted to evaluate the performance of the cooperative jamming. In [19], a feasible conditions on the positiveness of the secrecy rate are provided with

cooperative jamming technique. In [15], a Gaussian MIMO wiretap channel with cooperative jammer is considered. In [17], an external jammer transmits a jamming signal to help the source transmission and get resources for its own signal transmission as a rewards. In [16], a multiuser broadcast channel is investigated in which a multiple antenna friendly jammer transmits a jamming signal. In [20], an energy efficiency is considered in cooperative jamming with multiple friendly jammer

As a natural extension, cooperative relay has been applied in cooperative jamming recently. Existing works on cooperative jamming with cooperative relay are categorized into two cases: One is the untrusted relay case and the other is the trusted relay case.

In untrusted relay case, the relay is considered as a potential eavesdropper so that the signal has not to be decoded at the relay [21–24]. In [21], it is indicated that cooperative transmission, even with an untrusted relay, could be beneficial in relay channels with orthogonal components. In [22], three-node MIMO untrusted relay network is considered with secure beamforming design. In [23, 24], these works are extended to the two-way communication scenario.

In trusted relay case, the cooperative relays can help the signal transmission from the source to destination, and for some cases, transmits a jamming signal [25–32]. In [25, 26], a new cooperative jamming scheme is proposed in which all relay nodes transmits a jamming signal instead of forwarding data signal. In [27, 28], one of the relays transmits a jamming signal while all other relays forwards the signal from the source. In this networks, cooperative beamforming is designed with the power

allocation. In [29, 30], one of the relays forwards the signal from the source while all other relays transmits a jamming signal with beamforming. In [31], a problem is formulated whether the relay forwards the data signal or the relay transmits a jamming signal. In [32], an ergodic achievable secrecy rate is derived in cooperative jamming network with one relays which transmits a jamming signal.

Recently, some works focus on the idea that the source or the destination could transmit a jamming signal in the two-hop relay communication. In [33], the source and relay transmit a jamming signal with the assumption that the destination exactly knows the jamming signal. In [34, 35], the destination transmits a jamming signal in the dual-hop relay network.

1.2 Outline of Dissertation

In this dissertation, we consider the physical layer security with cooperative jamming in two-hop relay network.

In Chapter 2, we consider a two-hop relay network with cooperative jamming in which the source as well as destination transmits a jamming signal. The destination cancels its own jamming signal and the jamming signal from the source is negligible at the destination due to their weak channel strength. An optimal source power allocation problem is formulated based on the available channel state information at the source. Simulation results on the secrecy rate and the secrecy outage probability show that the proposed power allocation scheme achieves higher secrecy rate and lower secrecy outage probability than conventional schemes.

In Chapter 3, we consider a two-hop relay network with cooperative jamming in which the source and destination transmit jamming signals in the presence of multiple relays. We analyze the secrecy outage probability and propose a joint power allocation and relay selection scheme to minimize the secrecy outage probability. A joint problem is formulated in which the transmit power of the transmitting nodes and which relay to select is determined, and it is divided into a master problem and a subproblem by using the primal decomposition method to obtain the solution. Simulation results show that the proposed joint power allocation and relay selection scheme provides lower secrecy outage probability than the conventional jamming power allocation scheme as well as the scheme without jamming.

Finally, in Chapter 4, conclusions are drawn and future works about cooperative jamming are provided.

1.3 Notations

Table 1.1 and Table 1.2 list the abbreviations and symbols used throughout the dissertation, respectively.

Table 1.1. List of abbreviations

Abbreviation	Stands for
5G	Fifth Generation
AWGN	Additive White Gaussian Noise
CDF	Cumulative Distribution Function
CSI	Channel State Information
dB	Decibels, $10\log_{10}(\cdot)$
dBm	Decibels relative to one milliwatt, $10\log_{10}(\frac{\cdot}{1\text{ mW}})$
DF	Decode-and-Forward
i.i.d.	Independent and Identically Distributed
i.ni.d.	Independent and Not Identically Distributed
LTE	Long Term Evolution
NP-Hard	Non-deterministic Polynomial-time Hard
PDF	Probability Density Function
SIR	Signal-to-Interference Ratio
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
QoS	Quality of Service

Table 1.2. List of symbols

Symbol	Meaning
$\in$	Is an element of
$\notin$	Is not an element of
$[\cdot]$	Closed interval
$\{x_n\}_{n=1}^{N}$	Set of elements $x_1, x_2, \cdots, x_N$
$\arg(\cdot)$	Argument
$e^{(\cdot)}$	Exponential function
$\exp(\cdot)$	Exponential function
$O(\cdot)$	Big O notation
$\max\{x_1, x_2\}$	Maximum of x_1 and x_2
$\min\{x_1, x_2\}$	Minimum of x_1 and x_2
$\Pr[\cdot]$	Probability
∞	Infinity
$\int_a^b (\cdot) dx$	Definite integral from a to b
$\int_{\mathcal{S}} (\cdot) dx$	Definite integral over the set $\mathcal{S}$
$\prod_{n=1}^{N}$	Multiple product
$\sum_{n=1}^{N}$	Multiple sum
$n!$	Factorial
$\lvert \cdot \rvert$	Absolute value / Cardinality of a set
$=$	Equal
$\neq$	Not equal
$\approx$	Approximately equal
$\geq$	Greater than or equal to
$\leq$	Less than or equal to
$>$	Strictly greater than
$<$	Strictly less than

Chapter 2

Source Power Allocation for Cooperative Jamming in Amplify-and-Forward Relay Network with Eavesdropper

Secure communication is an important issue in wireless networks due to their vulnerability to eavesdropping [3]. The physical-layer security is appealing because it does not need any encryption methods. Based on Shannon's notion of perfect secrecy [36], the secrecy rate and the secrecy outage probability are characterized to ensure the wireless information-theoretic security.

Cooperative relay network improves the reliability of communications by using one or multiple relays to aid the signal transmission from the source to destination [37,38].

In cooperative relay network with an eavesdropper, cooperative jamming is an efficient way to improve the secrecy rate [39–45]. In cooperative jamming, cooperating node transmits the jamming signal to confuse the eavesdropper. In [39, 40], the relay is selected out of multiple relays to transmit the jamming signal. In [41–43], multiple relays helps the signal transmission as well as transmit a jammming signal with cooperation. In [44, 45], the destination transmits the jamming signal. However, most previous works consider a jamming signal only from either the relay or the destination.

In this Chapter, we consider a two-hop relay network in which the source as well as destination transmits a jamming signal. An optimal source power allocation problem is formulated based on the available channel state information (CSI) at the source. An effect of the source power allocation on the secrecy rate is investigated.

The remainder of this Chapter is organized as follows. We describe the system model in Section 2.1. We formulate a source power allocation problem for a two-hop relay network and obtain its solution in Section 2.2. Simulation results are provided by computer simulations in Section 2.3. Finally, this Chapter is summarized in Section 2.4.

2.1 System Model

Consider a two-hop relay network which consists of a source s, an amplify-and-forward (AF) relay r, a destination d, and an eavesdropper e, as shown in Fig. 2.1. Assume that there is no direct link between the source and destination, while there is a direct link between the source and eavesdropper. Assume that the channel coefficient between

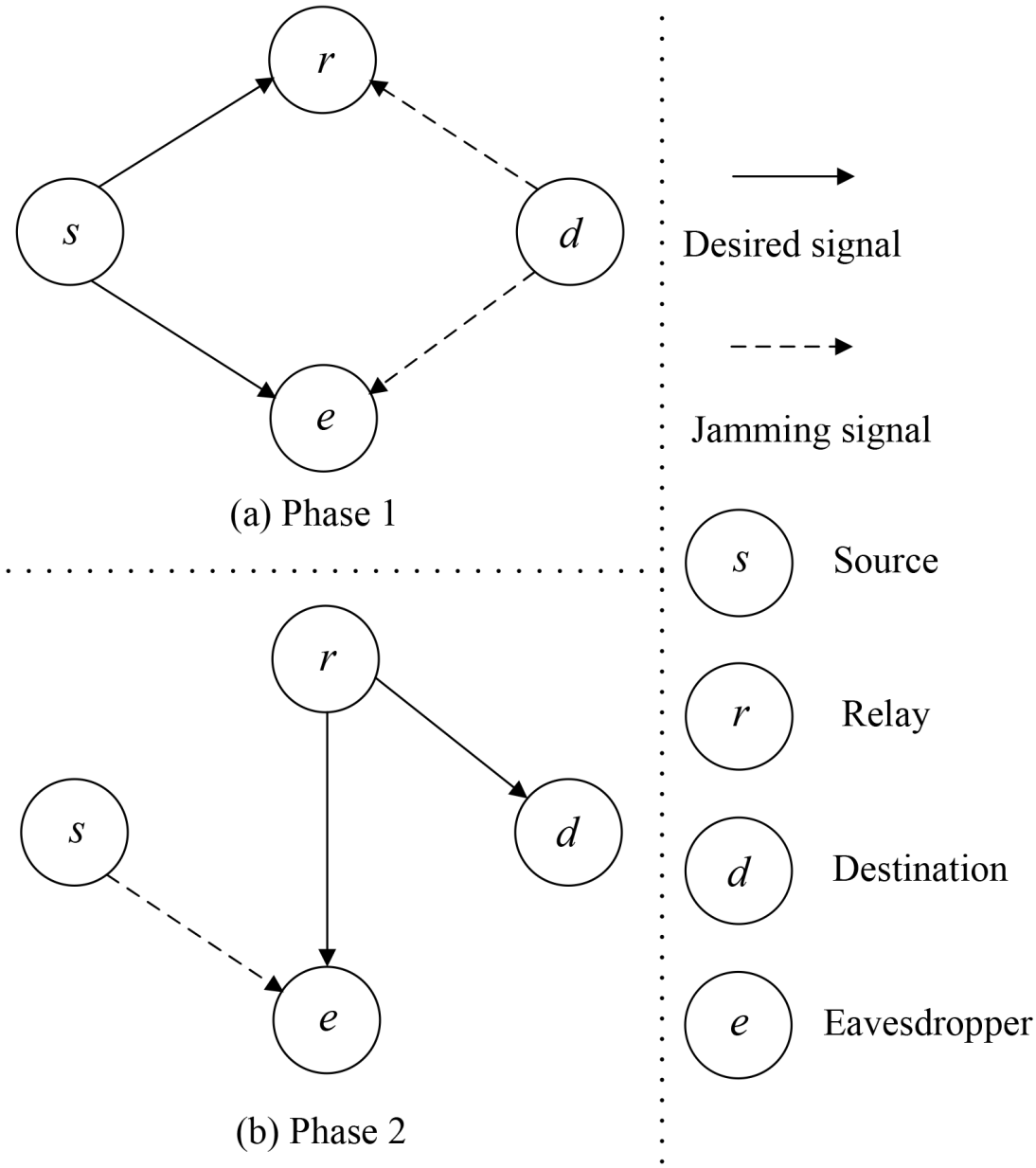


Figure 2.1. System model for a two-hop relay network.

node a and node b, h_{ab}, $a, b \in \{s, r, d, e\}$, is an independent zero-mean circularly symmetric complex Gaussian random variable with variance σ_{ab}^2. Assume that all channels are reciprocal and have an additive white Gaussian noise (AWGN) with zero mean and variance N_0.

The source transmits its signal to the destination through two phases each of which duration is normalized to one. In the first phase, the source transmits signal x with power $P_s^{(1)}$. Since the direct link between the source and the eavesdropper exists, the eavesdropper could receive the signal. In order to degrade the received signal at the eavesdropper, the destination simultaneously transmits jamming signal z_d with transmit power P_d. Assume that the jamming signal z_d is modeled as complex Gaussian random variable which is independent to the data signal x.

The received signal at the relay is given by

$$y_r = h_{sr}x + h_{dr}z_d + n_r \tag{2.1}$$

where n_r is an AWGN. The received signal at the eavesdropper is given by

$$y_e = h_{se}x + h_{de}z_d + n_e^{(1)} \tag{2.2}$$

where $n_e^{(1)}$ is an AWGN.

In the second phase, the relay amplifies and forwards the received signal with

variable gain g_r, which is given by

$$g_r = \sqrt{\frac{P_r}{|h_{sr}|^2 P_s^{(1)} + |h_{dr}|^2 P_d + N_0}} \tag{2.3}$$

where P_r is transmit power of the relay. During the relay transmission, the source transmits a jamming signal z_s with power $P_s^{(2)}$. Assume that the jamming signal z_s is modeled as complex Gaussian random variable which is independent to the other signals. As the direct link between the source and the destination does not exist, z_s does not interrupt the destination.It does not interrupt the destination, because of the negligible strength of direct link between the source and the destination.

The received signal at the destination is given by

$$\begin{aligned} y_d &= h_{rd} g_r y_r + n_d \\ &= h_{rd} g_r h_{sr} x + h_{rd} g_r h_{dr} z_d + h_{rd} g_r n_r + n_d \end{aligned} \tag{2.4}$$

where n_d is an AWGN. Assume that the destination perfectly cancels its own jamming signal, z_d, which is transmitted in the first phase. After cancellation, the received signal at the destination becomes

$$\hat{y}_d = h_{rd} g_r h_{sr} x + h_{rd} g_r n_r + n_d. \tag{2.5}$$

The received signal at the eavesdropper is given by

$$\begin{aligned} y_e &= h_{re} g_r y_r + h_{se} z_s + n_e^{(2)} \\ &= h_{re} g_r h_{sr} x + h_{re} g_r h_{dr} z_d + h_{re} g_r n_r + h_{se} z_s + n_e^{(2)} \end{aligned} \tag{2.6}$$

where $n_e^{(2)}$ is an AWGN.

From (2.5), the received signal-to-noise ratio (SNR) at the destination is given by

$$\gamma_d = \frac{P_s^{(1)} P_r |h_{sr}|^2 |h_{rd}|^2}{N_0 \left\{ (P_r + P_d)|h_{rd}|^2 + P_s^{(1)} |h_{sr}|^2 + N_0 \right\}}. \tag{2.7}$$

From (2.2), the received SNR at the eavesdropper in the first phase is given by

$$\gamma_e^{(1)} = \frac{P_s^{(1)} |h_{se}|^2}{P_d |h_{de}|^2 + N_0}. \tag{2.8}$$

From (2.6), the received SNR at the eavesdropper in the second phase is given by

$$\gamma_e^{(2)} = \frac{P_s^{(1)} P_r |h_{sr}|^2 |h_{re}|^2}{P_r |h_{re}|^2 (P_d |h_{rd}|^2 + N_0) + (P_s^{(2)} |h_{se}|^2 + N_0)(P_d |h_{rd}|^2 + P_s^{(1)} |h_{sr}|^2 + N_0)}, \tag{2.9}$$

Suppose that the available energy of each node for transmission is P. Since the duration of each phase is normalized to one, the transmit power of the destination in the first phase $P_d = P$ and the transmit power of the relay in the second phase $P_r = P$, while the transmit power of the source is splitted in the first phase and the second phase, so that $P_s^{(1)} = \alpha P,\ P_s^{(2)} = (1 - \alpha)P$, where $0 \leq \alpha \leq 1$. (2.7), (2.8), (2.9) are

rewritten as

$$\gamma_d = \frac{\alpha\gamma_{sr}\gamma_{rd}}{\alpha\gamma_{sr} + 2\gamma_{rd} + 1}, \tag{2.10}$$

$$\gamma_e^{(1)} = \frac{\alpha\gamma_{se}}{\gamma_{de} + 1}, \tag{2.11}$$

and

$$\gamma_e^{(2)} = \frac{\alpha\gamma_{re}\gamma_{sr}}{\gamma_{re}\gamma_{rd} + \gamma_{re} + \{(1-\alpha)\gamma_{se} + 1\}(\alpha\gamma_{sr} + \gamma_{rd} + 1)}, \tag{2.12}$$

respectively, where $\gamma_{ab} = P|h_{ab}|^2/N_0,\ \ a, b \in \{s, r, d, e\}$. As the channel coefficient is a complex Gaussian random variable, the probability density function (PDF) of γ_{ab} is given by

$$f_{\gamma_{ab}}(x) = \frac{1}{\bar{\gamma}_{ab}} e^{-\frac{x}{\bar{\gamma}_{ab}}} \tag{2.13}$$

where $\bar{\gamma}_{ab} = P\sigma_{ab}^2/N_0$. The secrecy rate of the network is given by [46]

$$\begin{aligned} R &= \left[\frac{1}{2}\left\{\log_2(1+\gamma_d) - \log_2\left(1 + \max\{\gamma_e^{(1)}, \gamma_e^{(2)}\}\right)\right\}\right] \\ &= \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_d}{1+\max\{\gamma_e^{(1)}, \gamma_e^{(2)}\}}\right)\right]^+ \end{aligned} \tag{2.14}$$

where $[x]^+ = \max\{0, x\}$. In the information theoretic view, the secrecy rate is the achievable rate that the source could transmit a data to the destination with perfect secrecy. A secrecy outage occurs when the secrecy rate is below the threshold, R_t. The secrecy outage probability of the network is given by [47]

$$P_o = \Pr\left[\frac{1}{2}\log_2\left(\frac{1+\gamma_d}{1+\max\{\gamma_e^{(1)}, \gamma_e^{(2)}\}}\right) < R_t\right]. \tag{2.15}$$

2.2 Source Power Allocation

In this section, we find the optimal power allocation factor of the source to minimize the secrecy outage probability based on the channel knowledge available at the source. When the source knows CSI of all links, the secrecy outage probability is minimized by maximizing the secrecy rate. When the source does not know the CSI of the eavesdropper links, maximizing the secrecy rate is impossible. In this case, optimal source power is allocated to minimize the secrecy outage probability.

2.2.1 Full CSI for All Links

When the source knows the CSI of all links, the optimal source power allocation problem is formulated as

$$\alpha_{opt} = \arg \max_{0 \le \alpha \le 1} \left\{ \frac{1}{2} \log_2 \left(\frac{1+\gamma_d}{1+\max\{\gamma_e^{(1)}, \gamma_e^{(2)}\}} \right) \right\}. \tag{2.16}$$

To find α_{opt}, we define the sets of α which satisfies $\gamma_e^{(1)} > \gamma_e^{(2)}$ and $\gamma_e^{(1)} \le \gamma_e^{(2)}$, respectively, which are given by Let R_1 and R_2 denote the set of α which satisfies $\gamma_e^{(1)} > \gamma_e^{(2)}$ and $\gamma_e^{(1)} \le \gamma_e^{(2)}$, respectively. Then, R_1 and R_2 are given by

$$R_1 = \left\{ \alpha \;\middle|\; 0 \le \alpha \le 1,\ \gamma_e^{(1)} > \gamma_e^{(2)} \right\} \tag{2.17}$$

and

$$R_2 = \left\{ \alpha \;\middle|\; 0 \le \alpha \le 1,\ \gamma_e^{(1)} \le \gamma_e^{(2)} \right\}, \tag{2.18}$$

respectively. From (2.11) and (2.12), $\gamma_e^{(1)} > \gamma_e^{(2)}$ is equivalent to

$$X_2\alpha^2 + X_1\alpha + X_0 < 0 \tag{2.19}$$

where

$$X_0 = \frac{\gamma_{re}\gamma_{sr}\left(\gamma_{de}+1\right)}{\gamma_{se}} - \left(\gamma_{se}+\gamma_{re}+1\right)\left(\gamma_{rd}+1\right), \tag{2.20}$$

$$X_1 = \gamma_{se}\left(\gamma_{rd}+1\right) - \gamma_{sr}\left(\gamma_{se}+1\right), \tag{2.21}$$

and

$$X_2 = \gamma_{se}\gamma_{sr}. \tag{2.22}$$

When $X_1^2 - 4X_2X_0 > 0$, (2.19) becomes

$$X_2(\alpha-\alpha_1)(\alpha-\alpha_2) < 0 \tag{2.23}$$

where

$$\alpha_1 = \frac{-X_1 - \sqrt{X_1^2 - 4X_2X_0}}{2X_2}, \tag{2.24}$$

and

$$\alpha_2 = \frac{-X_1 + \sqrt{X_1^2 - 4X_2X_0}}{2X_2}. \tag{2.25}$$

By using (2.23), (2.17) is rewritten as

$$R_1 = \left\{\alpha \;\middle|\; 0 \le \alpha \le 1,\ \alpha_1 < \alpha < \alpha_2\right\}. \tag{2.26}$$

When $X_1^2 - 4X_2X_0 \leq 0$, (2.19) has no solution and $R_1 = \emptyset$. Because R_1 and R_2 are disjoint, we obtain R_2.

The details of obtaining the optimal values of α in R_1, $\alpha_{opt}^{(1)}$, and R_2, $\alpha_{opt}^{(2)}$, are offered in Appendix. Finally, between $\alpha_{opt}^{(1)}$ and $\alpha_{opt}^{(2)}$, α_{opt} is selected such that the secrecy rate is maximized.

2.2.2 Full CSI for Desired Links only

When the source does not know the CSI of the eavesdropper links, the optimal source power allocation problem is formulated as

$$\begin{aligned}\alpha_{opt} &= \arg\min_{0\leq\alpha\leq 1} P_o \\ &= \arg\min_{0\leq\alpha\leq 1} \Pr\left[\frac{1}{2}\log_2(1+\gamma_d) - \frac{1}{2}\log_2(1+\max\{\gamma_e^{(1)}, \gamma_e^{(2)}\}) < R_t\right]. \end{aligned} \quad (2.27)$$

If $\bar{\gamma} \gg 1$, we utilize the high SNR approximation for $\gamma_e^{(1)}$ and $\gamma_e^{(2)}$. Then, it is approximated as $\gamma_e^{(1)} \approx \alpha \triangleq f_1(\alpha)$ and $\gamma_e^{(2)} \approx \alpha/(2-\alpha^2) \triangleq f_2(\alpha)$, respectively. From the shapes of these two functions as shown in Fig. 2.2, we approximate $\max\{\gamma_e^{(1)}, \gamma_e^{(2)}\} \approx$

$\gamma_e^{(1)}$ in $0 \leq \alpha \leq 1$ and the secrecy outage probability is also approximated as

$$\begin{aligned} P_o &\approx \Pr\left[\frac{1}{2}\log_2(1+\gamma_d) - \frac{1}{2}\log_2(1+\gamma_e^{(1)}) < R_t\right] \\ &= \Pr\left[\gamma_e^{(1)} > g(\alpha)\right] \\ &= \Pr\left[\frac{\alpha\gamma_{se}}{\gamma_{de}+1} > g(\alpha)\right] \\ &\triangleq P_o^{(1)}(\alpha) \end{aligned} \tag{2.28}$$

where

$$g(\alpha) = 2^{-2R_t}(1+\gamma_d) - 1. \tag{2.29}$$

Using the PDF of γ_{se} and γ_{de}, $P_o^{(1)}(\alpha)$ is given by

$$\begin{aligned} P_o^{(1)}(\alpha) &= \Pr\left[\gamma_{se} > \frac{g(\alpha)}{\alpha}(\gamma_{de}+1)\right] \\ &= \int_0^\infty \int_{\frac{g(\alpha)}{\alpha}(u+1)}^\infty f_{\gamma_{se}}(v) f_{\gamma_{de}}(u) dv du \\ &= \int_0^\infty \exp\left(-\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}(x+1)\right)\frac{1}{\bar{\gamma}_{de}} e^{-\frac{x}{\bar{\gamma}_{de}}} dx \\ &= \exp\left(-\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}\right)\frac{1}{\bar{\gamma}_{de}}\int_0^\infty \exp\left(-\left(\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}+\frac{1}{\bar{\gamma}_{de}}\right)x\right)dx \\ &= \exp\left(-\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}\right)\left(\frac{\bar{\gamma}_{se}\alpha}{\bar{\gamma}_{de}g(\alpha)+\bar{\gamma}_{se}\alpha}\right). \end{aligned} \tag{2.30}$$

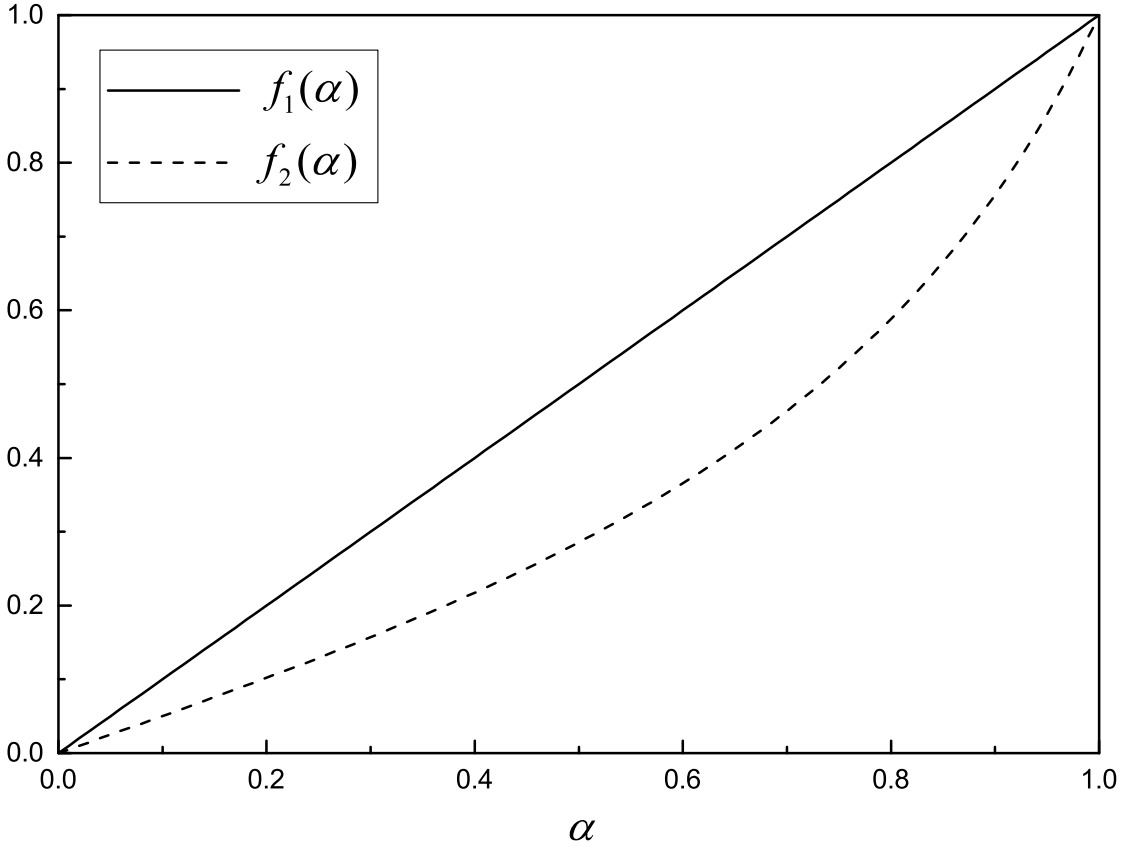


Figure 2.2. Shapes of the two functions for α.

The first order derivative of $P_o^{(1)}(\alpha)$ with respect to α is given by

$$\begin{aligned}\frac{\partial P_o^{(1)}(\alpha)}{\partial \alpha} &= \frac{\partial \exp\left(-\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}\right)}{\partial \alpha}\left(\frac{\bar{\gamma}_{se}\alpha}{\bar{\gamma}_{de}g(\alpha)+\bar{\gamma}_{se}\alpha}\right)+\exp\left(-\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}\right)\frac{\partial\left(\frac{\bar{\gamma}_{se}\alpha}{\bar{\gamma}_{de}g(\alpha)+\bar{\gamma}_{se}\alpha}\right)}{\partial \alpha} \\ &= \exp\left(-\frac{g(\alpha)}{\bar{\gamma}_{se}\alpha}\right)\left(\frac{g(\alpha)-\alpha g'(\alpha)}{\bar{\gamma}_{de}g(\alpha)+\bar{\gamma}_{se}\alpha}\right)\left(\frac{\bar{\gamma}_{se}\bar{\gamma}_{de}}{\bar{\gamma}_{de}g(\alpha)+\bar{\gamma}_{se}\alpha}+\frac{1}{\alpha}\right) \qquad (2.31)\end{aligned}$$

where

$$\begin{aligned}g'(\alpha) &= \frac{\partial g(\alpha)}{\partial \alpha} \\ &= 2^{-2R_t}\frac{\partial \gamma_d}{\partial \alpha} \\ &= 2^{-2R_t}\frac{\gamma_{sr}\gamma_{rd}\left(2\gamma_{rd}+1\right)}{\left(\alpha\gamma_{sr}+2\gamma_{rd}+1\right)^2}. \qquad (2.32)\end{aligned}$$

From (2.31), it is easily shown that the first term, the denominator of the second term, and the third term of (2.31) are strictly greater than 0, so that finding a solution of $\frac{\partial P_o^{(1)}(\alpha)}{\partial \alpha}=0$ is equivalent to finding a solution of the equation:

$$g(\alpha)-\alpha g'(\alpha)=0. \qquad (2.33)$$

By substituting (2.29) and (2.32) into (2.33), we have

$$(1+\gamma_d)-2^{2R_t}-\alpha\frac{\gamma_{sr}\gamma_{rd}\left(2\gamma_{rd}+1\right)}{\left(\alpha\gamma_{sr}+2\gamma_{rd}+1\right)^2}=0 \qquad (2.34)$$

With some mathematical manipulations, we have

$$Y_2\alpha^2 + Y_1\alpha + Y_0 = 0 \tag{2.35}$$

where

$$Y_0 = (2\gamma_{rd} + 1)^2\eta, \tag{2.36}$$

$$Y_1 = 2\gamma_{sr}(2\gamma_{rd} + 1)\eta, \tag{2.37}$$

$$Y_2 = \gamma_{sr}^2\left(\gamma_{rd} + \eta\right), \tag{2.38}$$

and $\eta = 1 - 2^{2R_t}$. When $Y_1^2 - 4Y_2Y_0 > 0$, (2.35) has two solutions, which are given by

$$\alpha_3 = \frac{-Y_1 - \sqrt{Y_1^2 - 4Y_2Y_0}}{2Y_2}, \tag{2.39}$$

and

$$\alpha_4 = \frac{-Y_1 + \sqrt{Y_1^2 - 4Y_2Y_0}}{2Y_2}, \tag{2.40}$$

respectively. Since $\alpha_3 < 0$, $\alpha_4 > 0$, and $P_o^{(1)}(\alpha)$ is decreasing function of α, $\alpha \in [\alpha_3,\ \alpha_4]$, the optimum value of α is $\min\{\alpha_4,\ 1\}$.

When $Y_1^2 - 4Y_2Y_0 \leq 0$, LHS of (2.35) is always negative in the range of α from 0 to 1, i.e. $P_o^{(1)}(\alpha)$ is decreasing function of α, $\alpha \in [0,\ 1]$. Thus, the optimum value of α is 1.

Hence, optimum value of α is given by

$$\alpha_{opt} = \begin{cases} \min\{\alpha_4,\ 1\}, & Y_1^2 - 4Y_2Y_0 > 0, \\ 1, & Y_1^2 - 4Y_2Y_0 \leq 0. \end{cases} \tag{2.41}$$

2.3 Simulation Results

Consider a two-hop relay network which consists of a source, an AF relay, a destination, and an eavesdropper. We assume that the noise variance, N_0 is normalized to 1. Two fixed power allocation schemes are also presented to compare the secrecy performances. For fair comparison, total energy spent by the source in these two compared schemes are same as that of the proposed scheme. In the first compared scheme, total energy spent by the source is equally divided in each phases, i.e., $\alpha = 0.5$. In the second compared scheme, all energy spent by the source is allocated to the data transmission in the first phase, i.e., $\alpha = 1$.

2.3.1 Identical Channel Condition

In this subsection, we assume that the variances of all channel coefficients are equal to 1.

Fig. 2.3 shows the ergodic secrecy rate versus average SNR for the proposed scheme and the compared schemes. It is shown that the proposed source power allocation scheme achieves higher ergodic secrecy rate than those of compared fixed power allocation schemes. Proposed scheme needs nearly 20% less power to achieve same secrecy

rate of the compared fixed power allocation scheme with $\alpha = 0.5$. It is shown that the ergodic secrecy rate increases as the average SNR increases for all schemes.

Fig. 2.4 shows the probability of the non-zero secrecy rate versus average SNR for the proposed scheme and the compared schemes. This probability is equivalent to the probability of satisfying secure communiation in the network [48, 49]. It is shown that the proposed scheme achieves higher probability to satisfy secure communication than those of compared schemes. It is shown that the probability increases as the average SNR increases for all three schemes.

Fig. 2.5 shows the secrecy outage probability versus average SNR for the proposed scheme and the compared schemes. It is shown that the proposed scheme achieves lower secrecy outage probability than those of compared schemes. It is shown that the secrecy outage probability decreases as the average SNR increases and it increases as the threshold R_t increases for all schemes. It is also shown that the slopes of secrecy outage probability of the proposed scheme as well as the fixed power allocation scheme with $\alpha = 0.5$ decrease steeper than that of fixed power allocation scheme with $\alpha = 1$.

Fig. 2.6 shows the secrecy performances versus various values of α. It is shown that the optimal value of α maximizes ergodic secrecy rate is around 0.7, and the optimal value of α maximizes secrecy outage probability is around 0.5. It is also shown that this tendency retains as the average SNR varies from 25dB to 30dB.

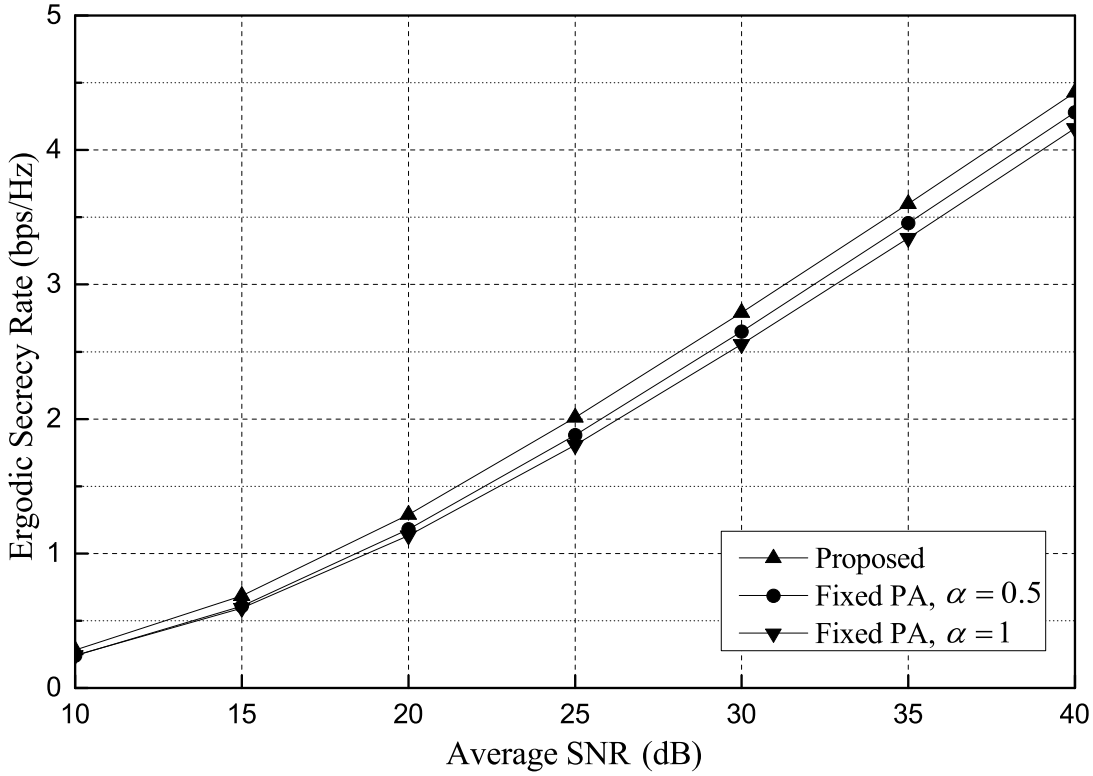


Figure 2.3. Ergodic secrecy rate versus average SNR.

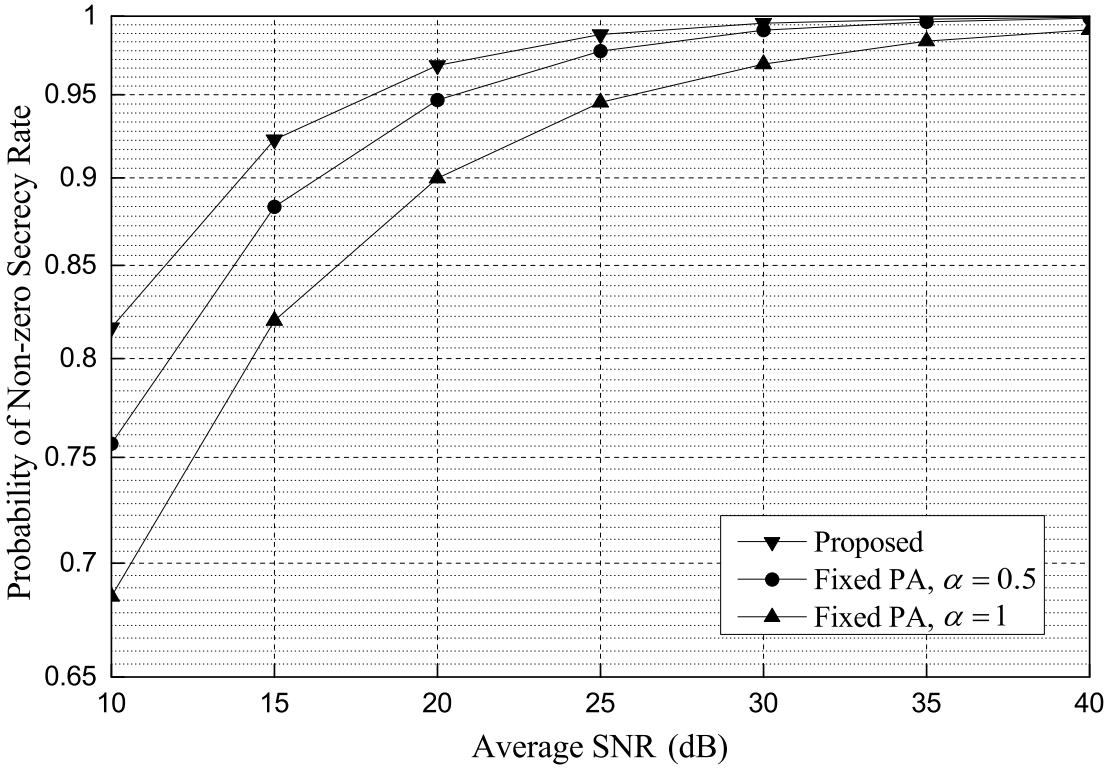
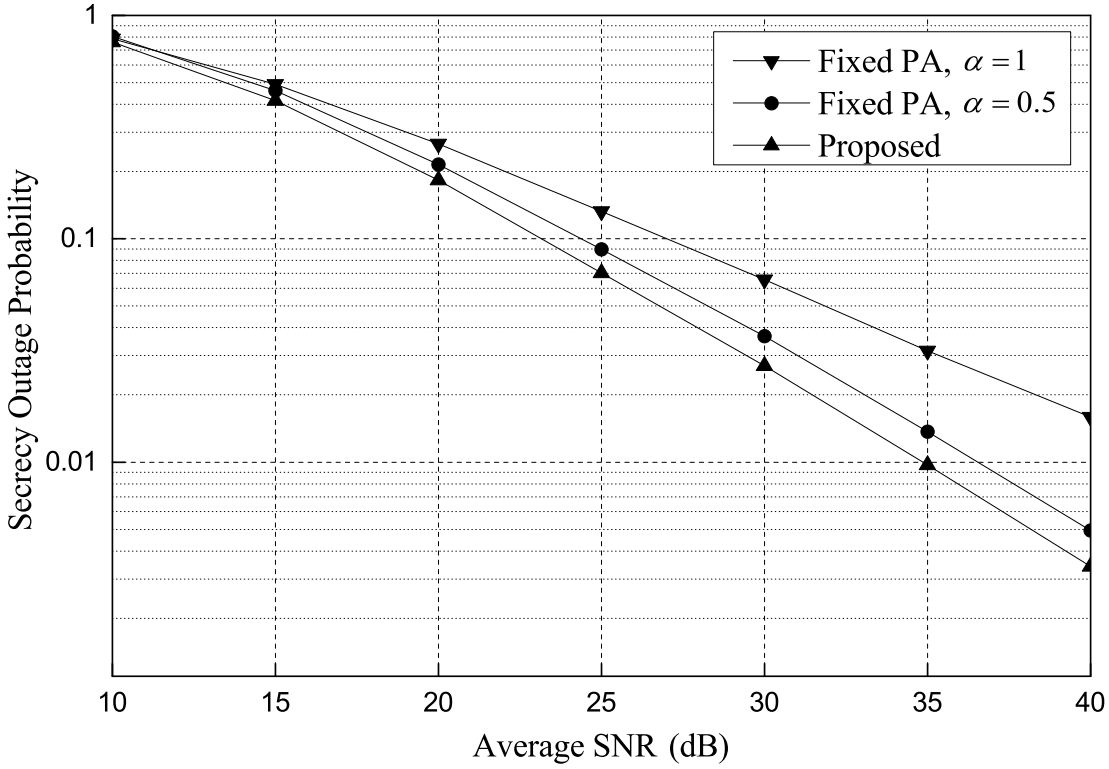
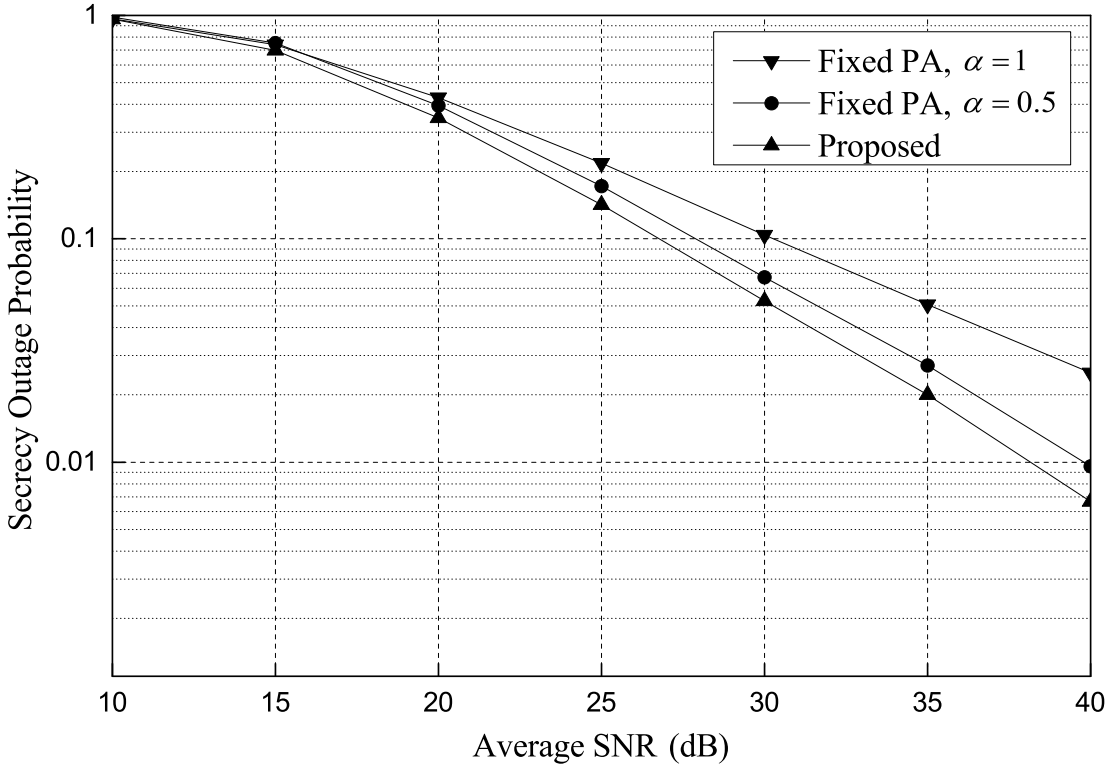


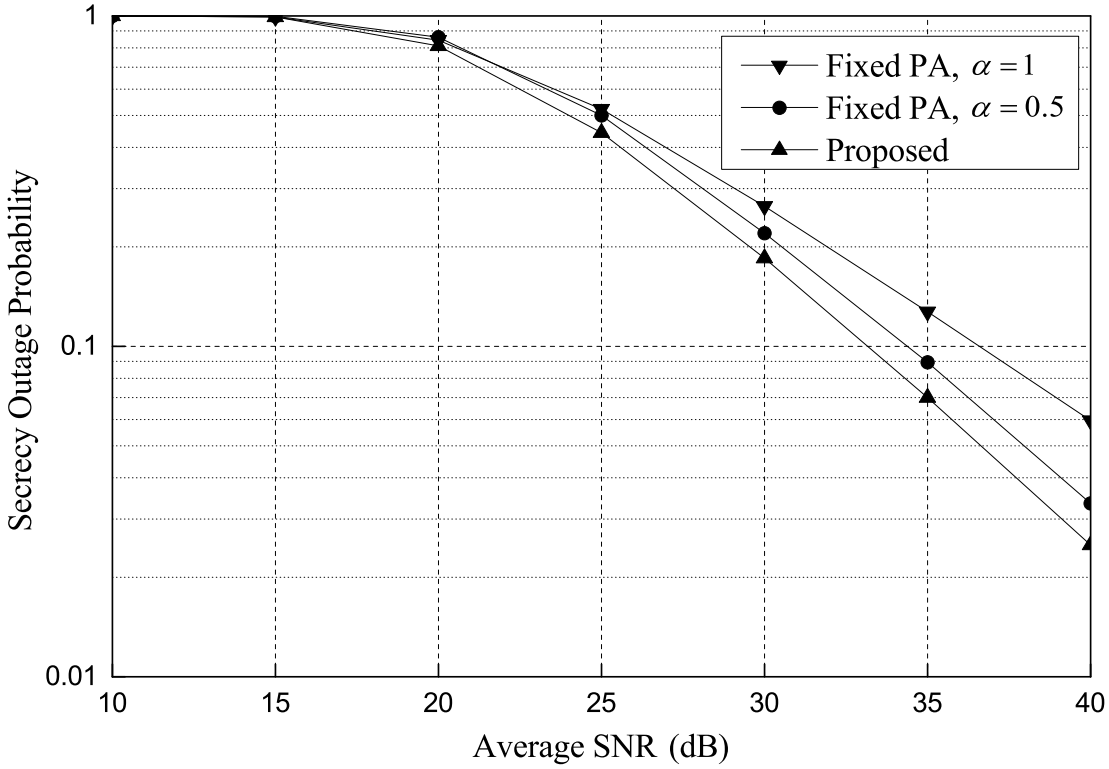
Figure 2.4. Probability of the non-zero secrecy rate versus average SNR.


Secrecy Outage Probability
1
0.1
0.01
10
15
20
25
30
35
40
Average SNR (dB)
Fixed PA, $\alpha = 1$
Fixed PA, $\alpha = 0.5$
Proposed

(a) $R_t = 0.5$ bps/Hz

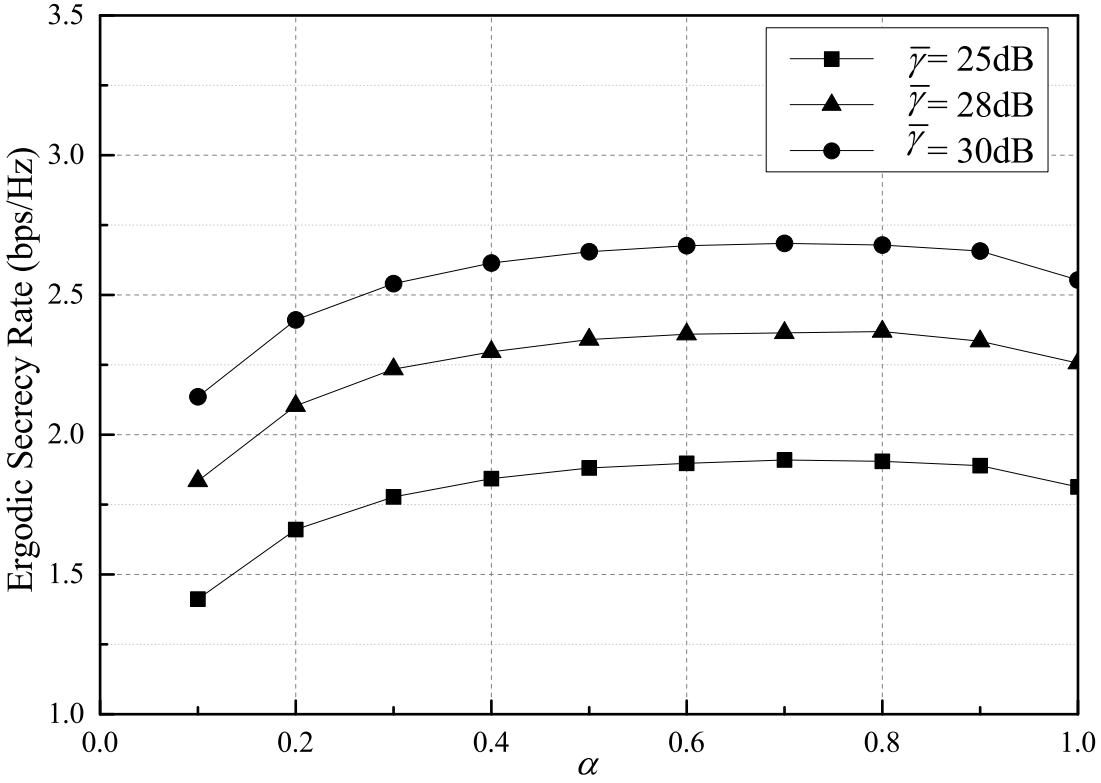

Secrecy Outage Probability
1
0.1
0.01
10
15
20
25
30
35
40
Average SNR (dB)
Fixed PA, $\alpha = 1$
Fixed PA, $\alpha = 0.5$
Proposed

(b) $R_t = 1.0$ bps/Hz

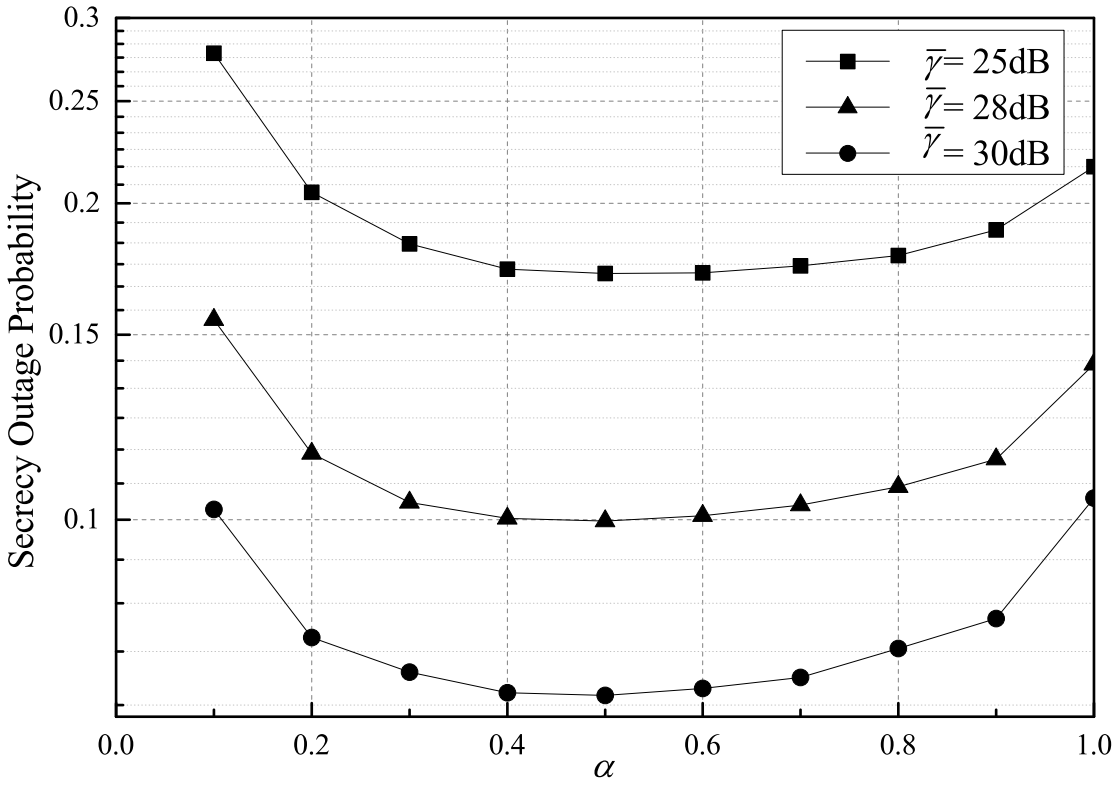


(c) $R_t = 2.0$ bps/Hz

Figure 2.5. Secrecy outage probability versus average SNR.



(a) Ergodic secrecy rate versus α



(b) Secrecy outage probability versus α, $R_t = 1.0$ bps/Hz

Figure 2.6. Secrecy performances versus α.

2.3.2 Non-identical Channel Condition

In this subsection, we assume that the variances of all channel coefficients are not equal. Three cases are considered as follows:

1. The eavesdropper is close to the source. In this case, we suppose $\sigma_{se}^2 = 2$ and $\sigma_{de}^2 = 0.5$.

2. The eavesdropper is close to the relay. In this case, we suppose $\sigma_{re}^2 = 2$.

3. The eavesdropper is close to the destination. In this case, we suppose $\sigma_{de}^2 = 2$ and $\sigma_{se}^2 = 0.5$.

In these three cases, all other variances of channel are normalized to 1.

Simulation results of the first case is shown from Fig. 2.7 to Fig. 2.9. Fig. 2.7 shows the ergodic secrecy rate versus average SNR for the proposed scheme and the compared schemes. It is shown that the ergodic secrecy rate is slightly lower than that of identical channel condition case, because the eavesdropper could overhear the data signal from the source easily. It is also shown that all other tendencies are equal to previous identical channel condition case.

Fig. 2.8 shows the secrecy outage probability versus average SNR for the proposed scheme and the compared schemes. Similar to the ergodic secrecy rate performance, secrecy outage probability is slightly higher than that of identical channel condition case for all schemes. It is also shown that the gap of the secrecy outage probabilities between the proposed scheme and other schemes decreases proportional to their decreased value.

Fig. 2.9 shows the secrecy performances versus various values of α. Different from the identical channel condition case, it is shown that the optimal value of α maximizes ergodic secrecy rate is around 0.6, and the optimal value of α maximizes secrecy outage probability is around 0.3 and 0.4. It means that more power is allocated to transmit jamming signal, which is a natural result with the condition of high σ_{se}^2.

Simulation results of the second case is shown from Fig. 2.10 to Fig. 2.12. Fig. 2.10 shows the ergodic secrecy rate versus average SNR for the proposed scheme and the compared schemes. It is shown that the ergodic secrecy rate is almost same for that of identical channel condition case. This is because the transmitted signal from the eavesdropper already contains a jamming signal from the destination, so that the eavesdropper couldn't increase its received SINR with high σ_{re}^2.

Fig. 2.11 shows the secrecy outage probability versus average SNR for the proposed scheme and the compared schemes. Similar to the ergodic secrecy rate performance, secrecy outage probability is almost same for that of identical channel condition case for all schemes.

Fig. 2.12 shows the secrecy performances versus various values of α. It is shown that the optimal value of α is same for that of identical channel condition case, and it is independent of the values of σ_{re}^2.

Finally, simulation results of the third case is shown from Fig. 2.13 to Fig. 2.15. Fig. 2.13 shows the ergodic secrecy rate versus average SNR for the proposed scheme and the compared schemes. It is shown that the ergodic secrecy rate is slightly higher than that of identical channel condition case, because the eavesdropper receives decreased

data signal form the source and increased jamming signal from the destination in this case. It is also shown that all other tendencies are equal to previous identical channel condition case.

Fig. 2.14 shows the secrecy outage probability versus average SNR for the proposed scheme and the compared schemes. Similar to the ergodic secrecy rate performance, secrecy outage probability is slightly lower than that of identical channel condition case for all schemes. It is also shown that the gap of the secrecy outage probabilities between the proposed scheme and other schemes increases proportional to their decreased value.

Fig. 2.15 shows the secrecy performances versus various values of α. Different from the identical channel condition case, it is shown that the optimal value of α maximizes ergodic secrecy rate is around 0.8, and the optimal value of α maximizes secrecy outage probability is around 0.5 and 0.6. It means that less power is allocated to transmit jamming signal, which is a natural result with the condition of low σ_{se}^2.

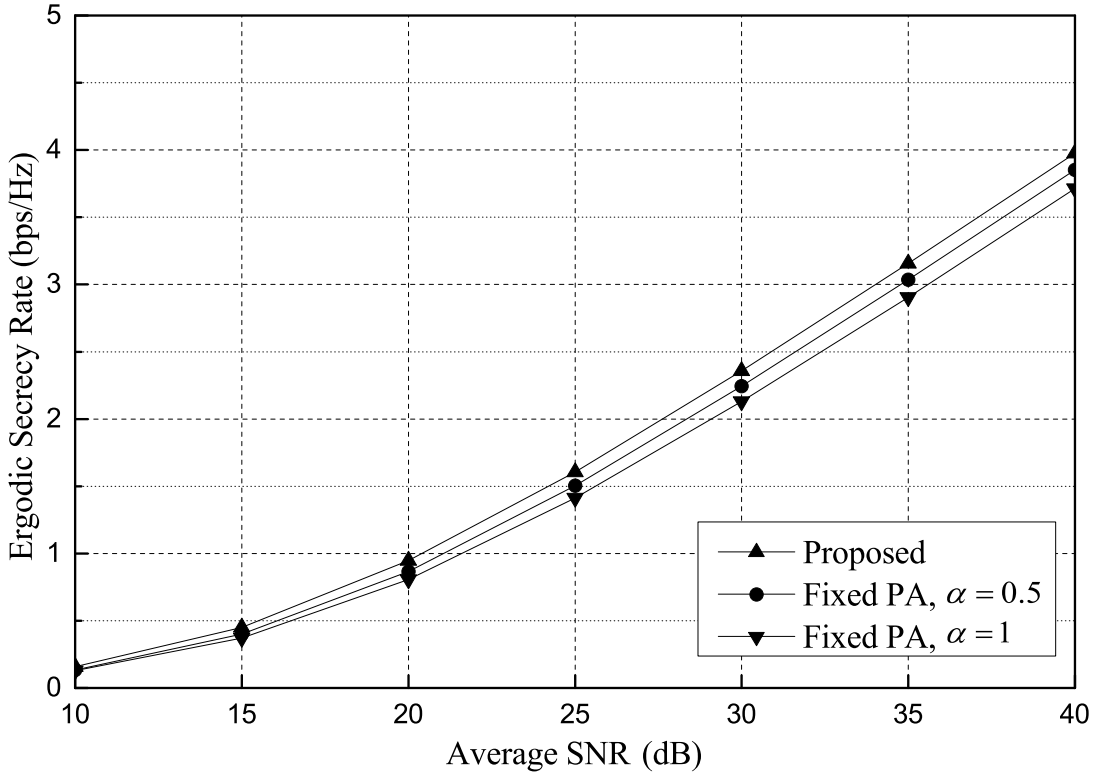
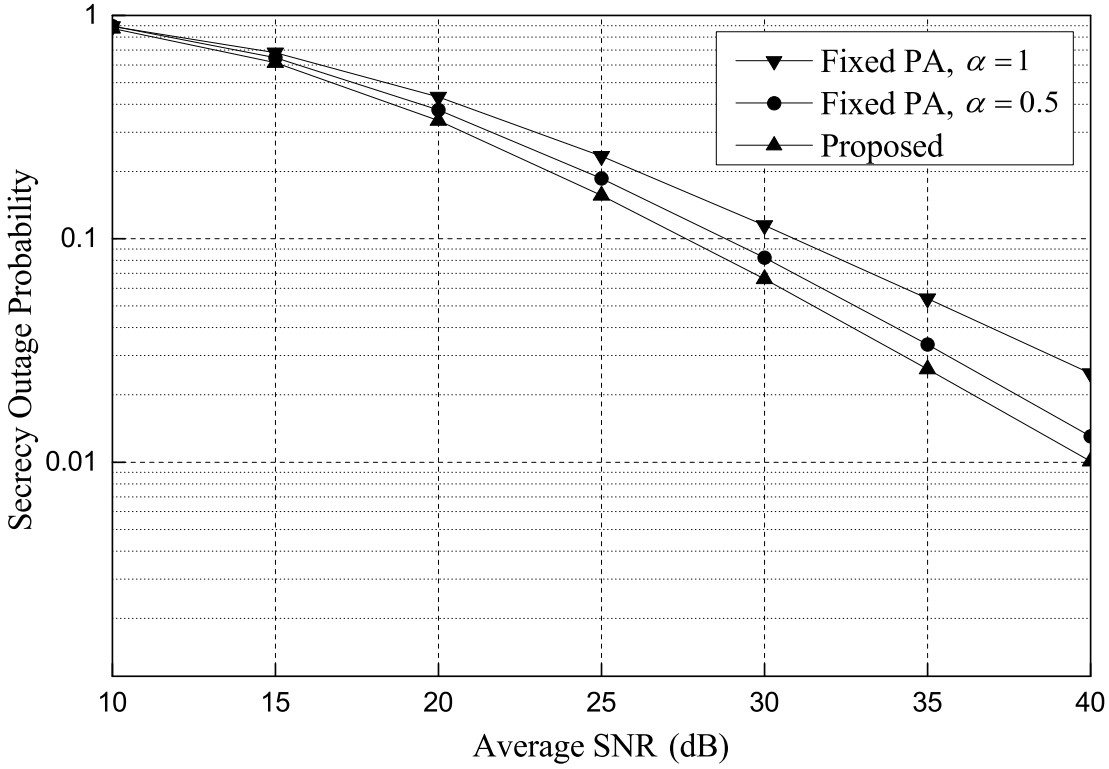
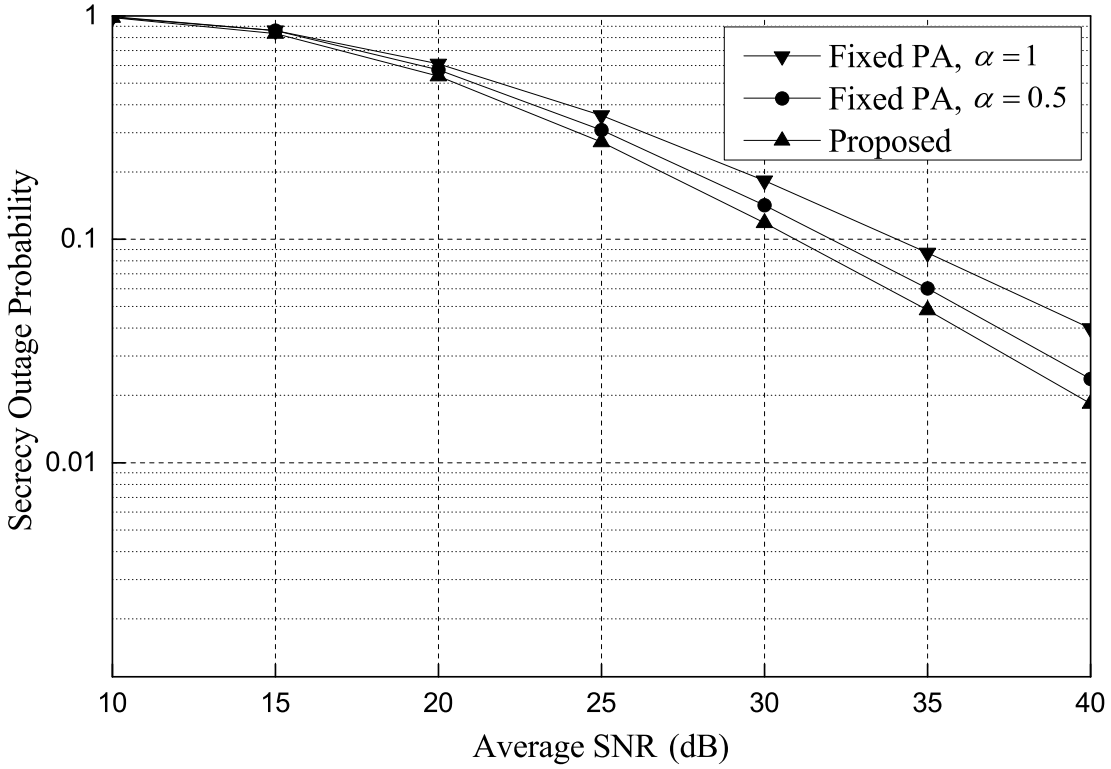


Figure 2.7. Ergodic secrecy rate versus average SNR, $\sigma_{se}^2 = 2$ and $\sigma_{de}^2 = 0.5$.

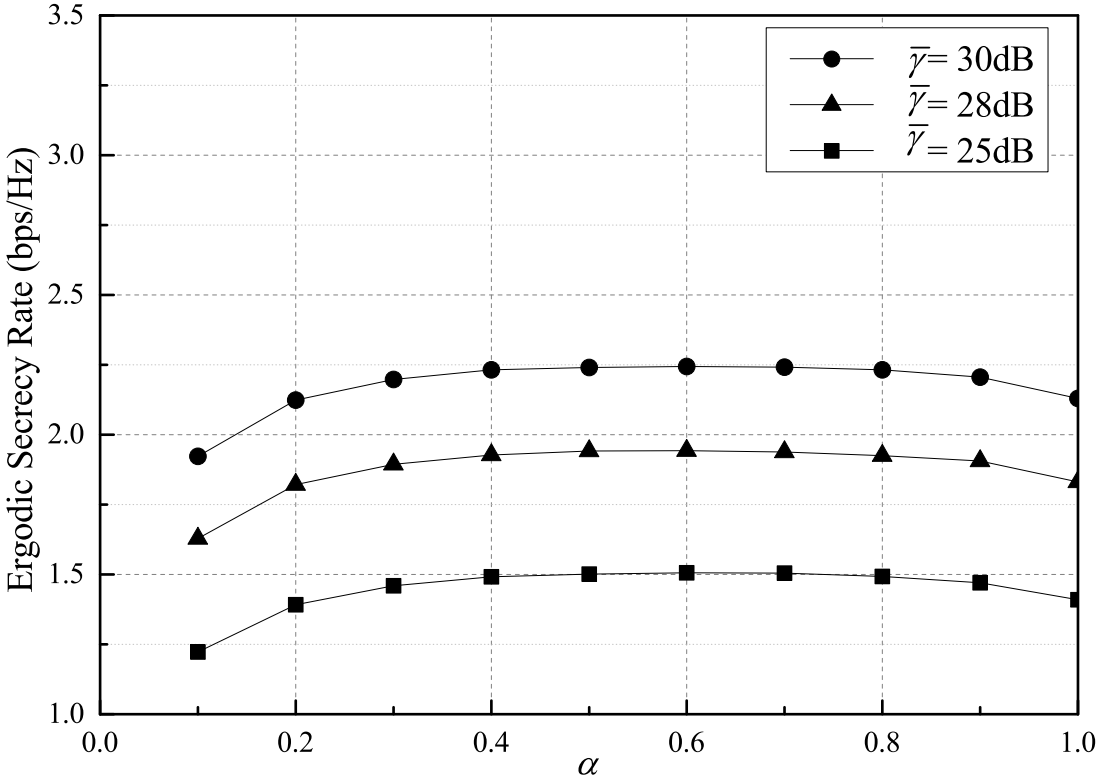

Secrecy Outage Probability
1
0.1
0.01
10
15
20
25
30
35
40
Average SNR (dB)
Fixed PA, $\alpha = 1$
Fixed PA, $\alpha = 0.5$
Proposed

(a) $R_t = 0.5$ bps/Hz

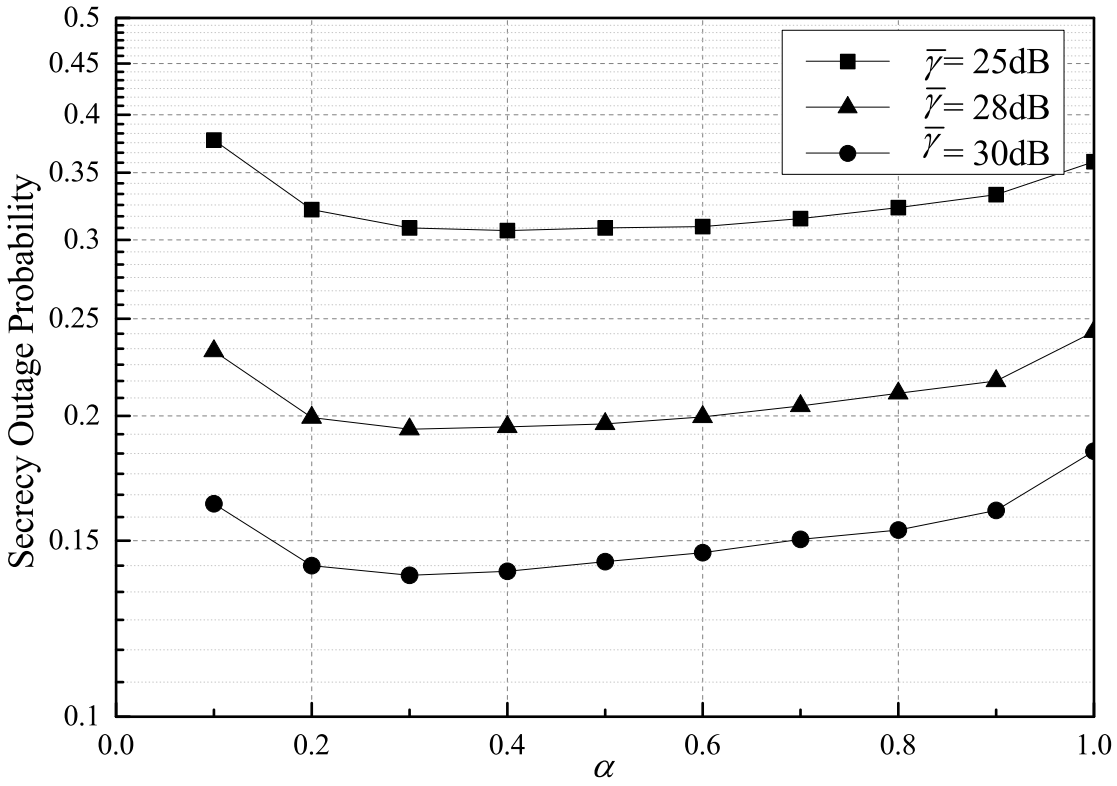


(b) $R_t = 1.0$ bps/Hz

Figure 2.8. Secrecy outage probability versus average SNR, $\sigma_{se}^2 = 2$ and $\sigma_{de}^2 = 0.5$.



(a) Ergodic secrecy rate versus α



(b) Secrecy outage probability versus α, $R_t = 1.0$ bps/Hz

Figure 2.9. Secrecy performances versus α, $\sigma_{se}^2 = 2$ and $\sigma_{de}^2 = 0.5$.

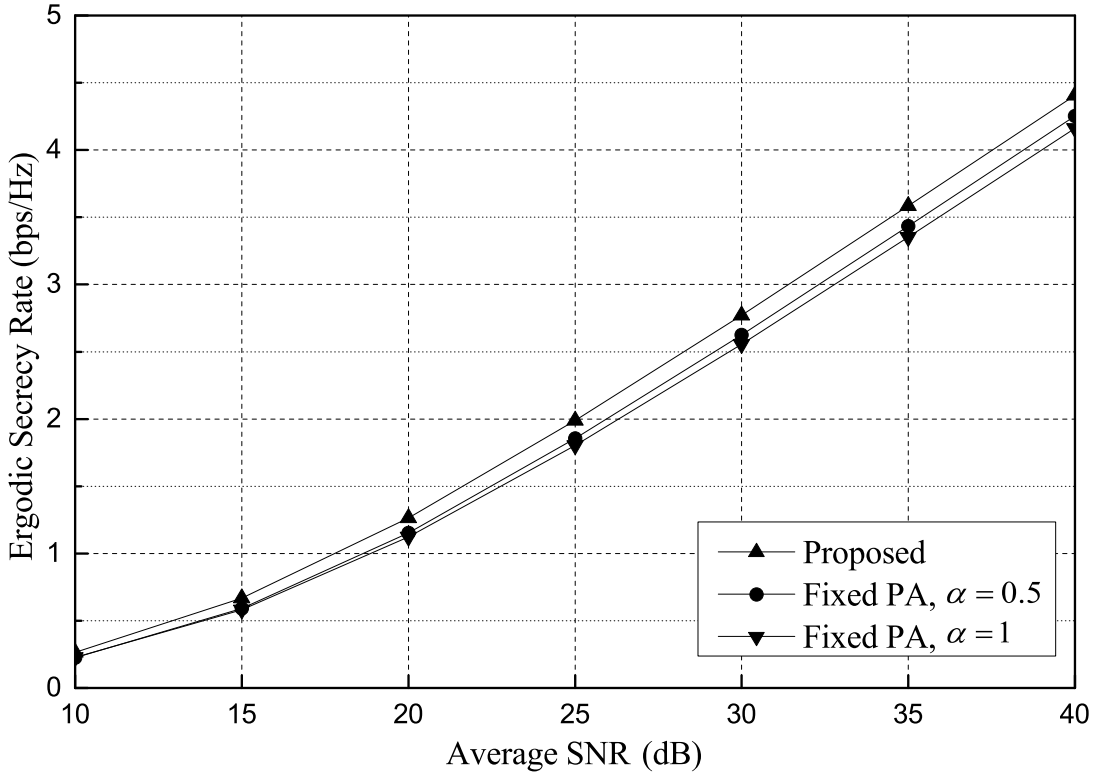
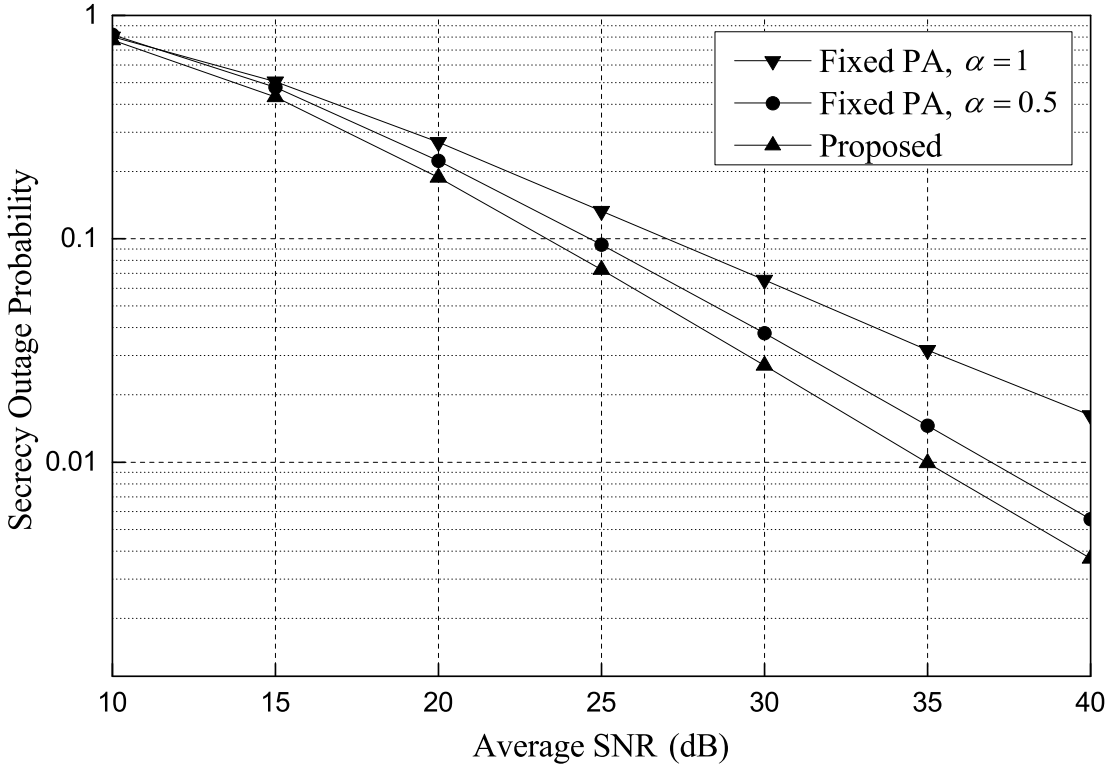
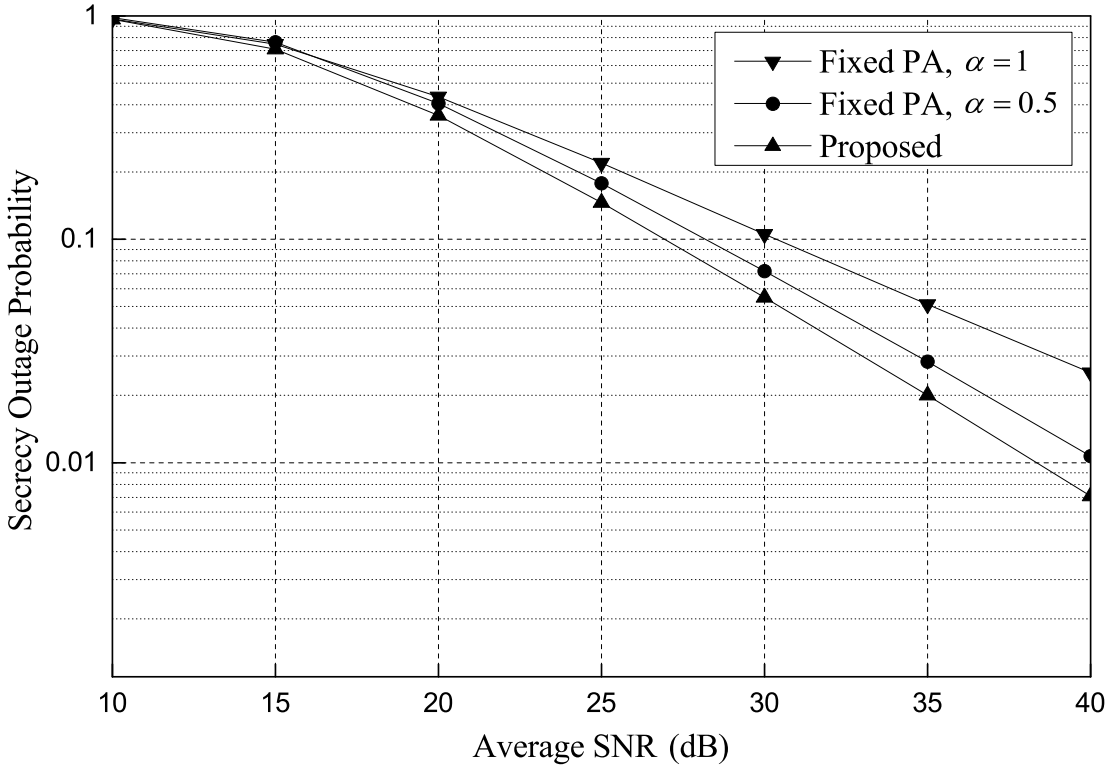


Figure 2.10. Ergodic secrecy rate versus average SNR, $\sigma_{re}^2 = 2$.

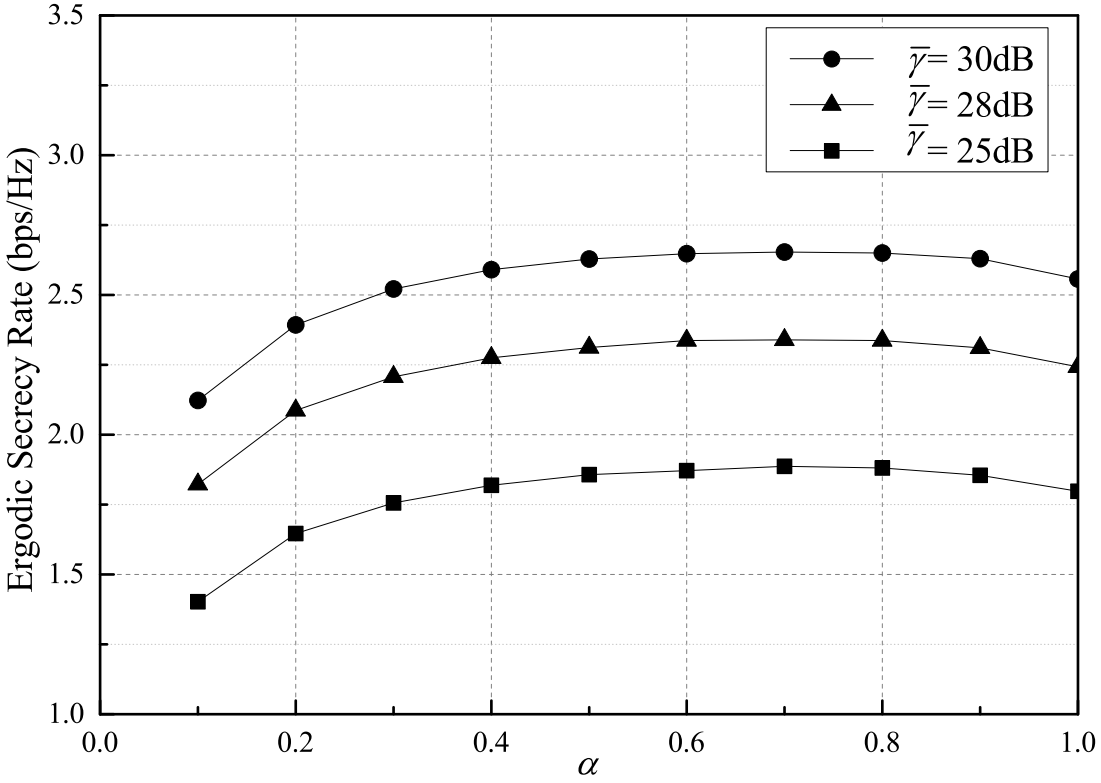

Secrecy Outage Probability
1
0.1
0.01
10
15
20
25
30
35
40
Average SNR (dB)
Fixed PA, $\alpha = 1$
Fixed PA, $\alpha = 0.5$
Proposed

(a) $R_t = 0.5$ bps/Hz

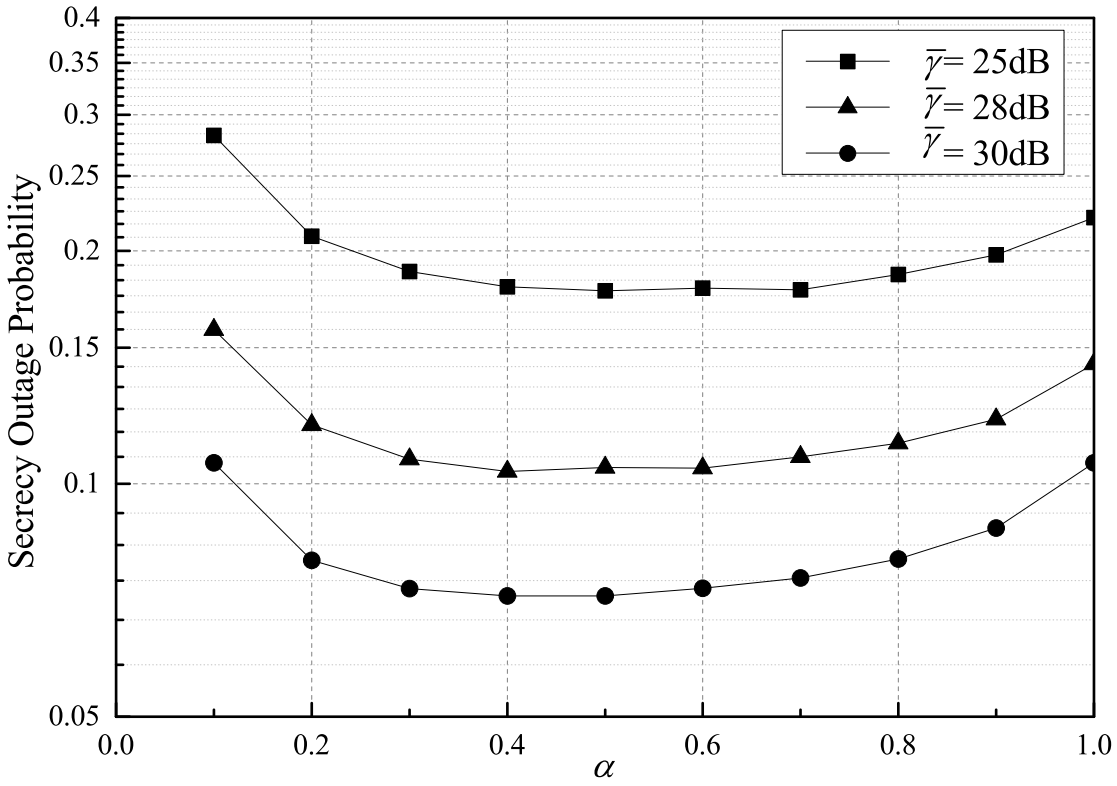


(b) $R_t = 1.0$ bps/Hz

Figure 2.11. Secrecy outage probability versus average SNR, $\sigma_{re}^2 = 2$.



(a) Ergodic secrecy rate versus α



(b) Secrecy outage probability versus α, $R_t = 1.0$ bps/Hz

Figure 2.12. Secrecy performances versus α, $\sigma_{re}^2 = 2$.

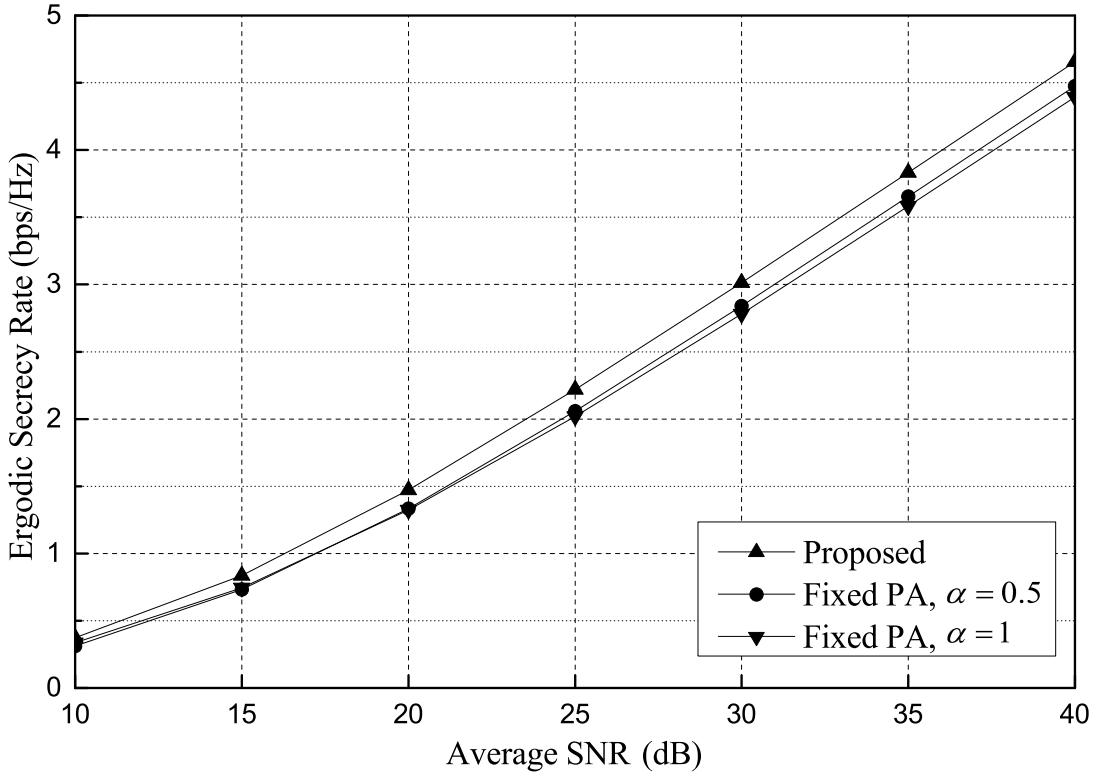
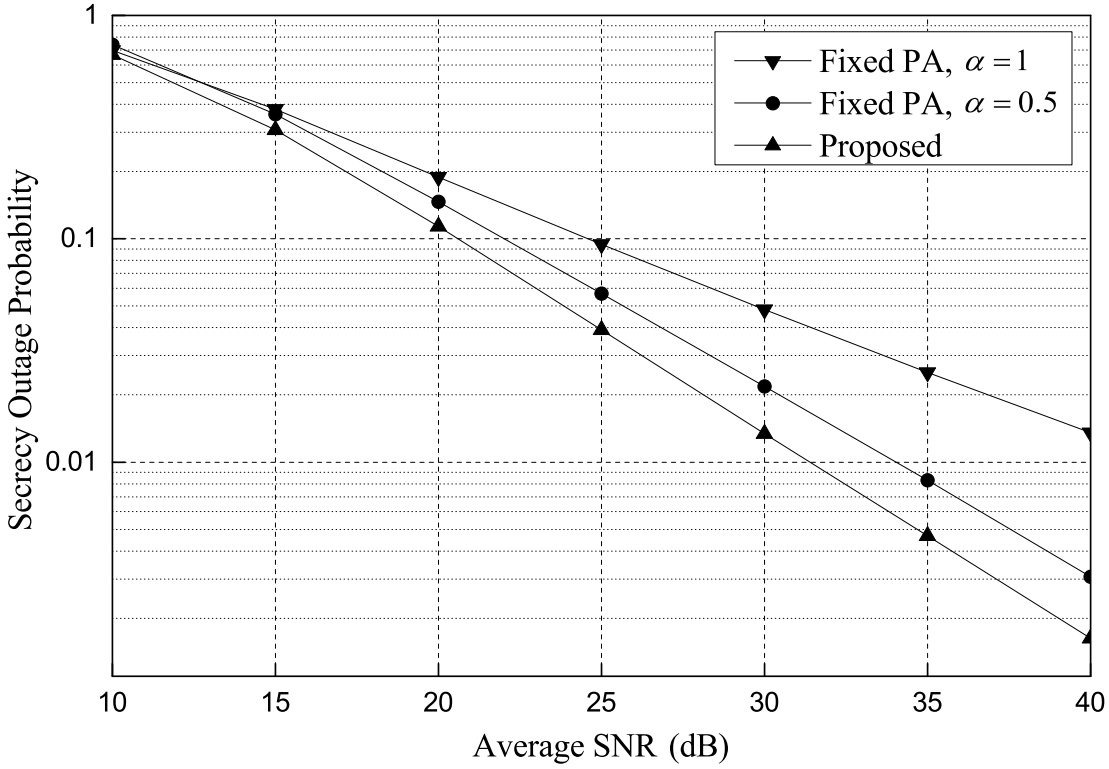
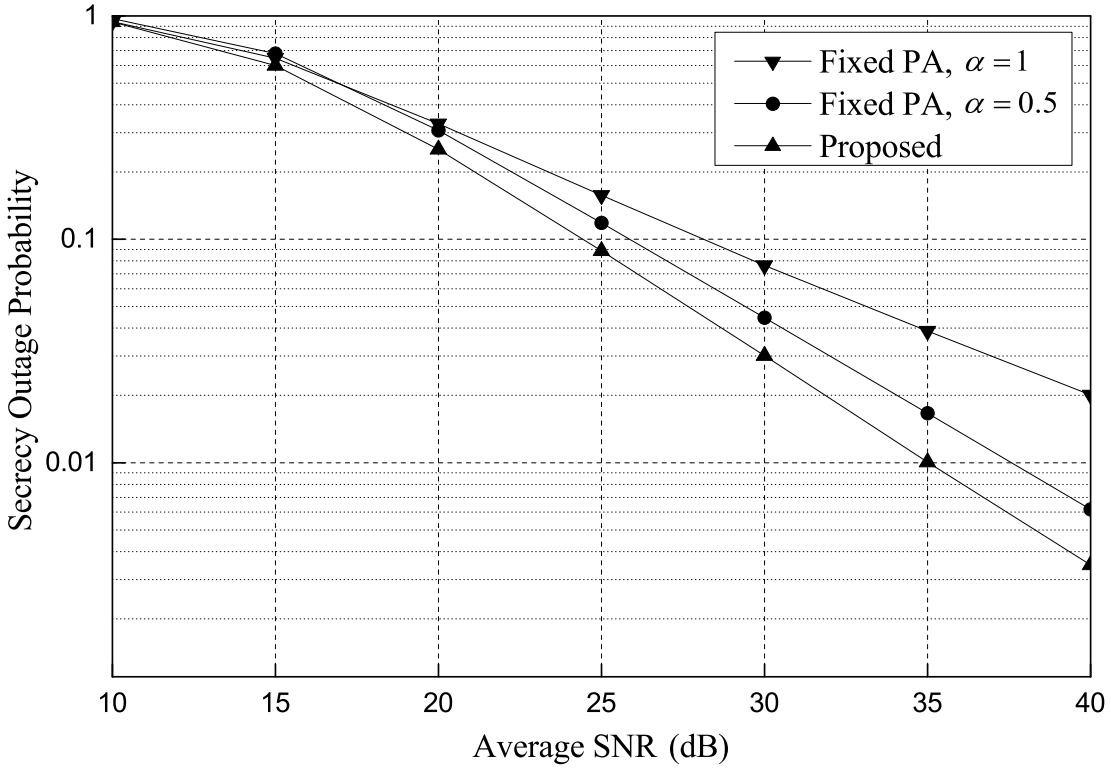


Figure 2.13. Secrecy rate versus average SNR, $\sigma_{de}^2 = 2$ and $\sigma_{se}^2 = 0.5$.

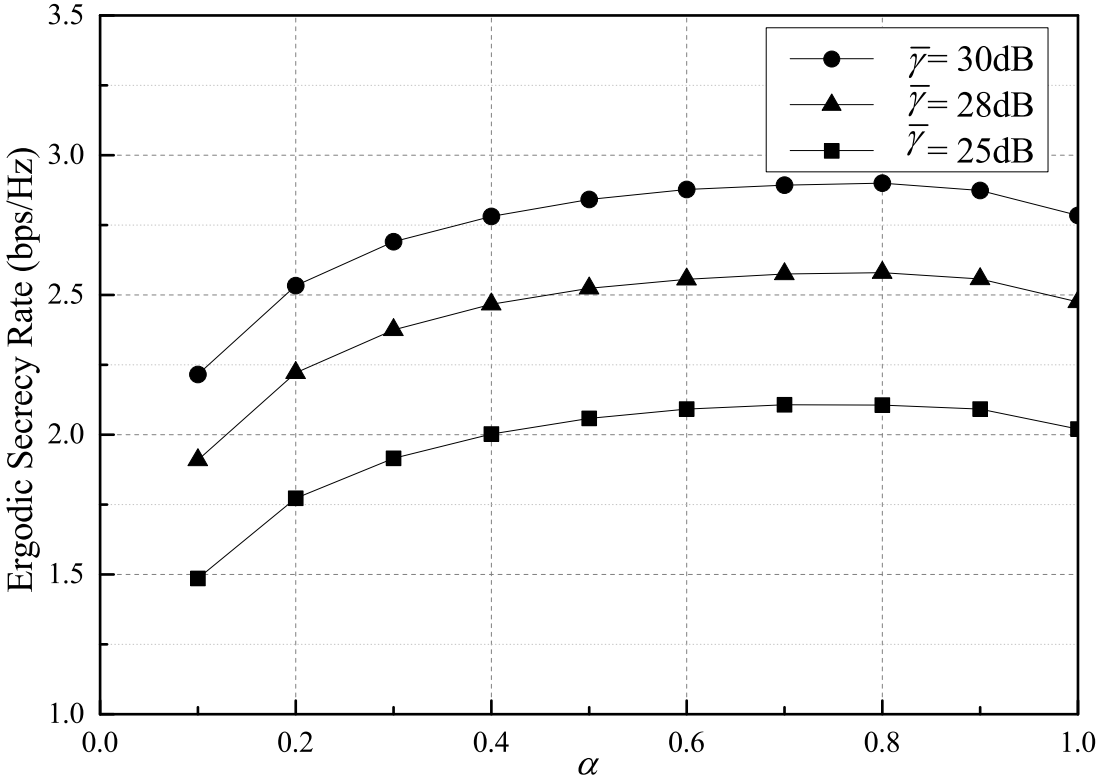

Secrecy Outage Probability
1
0.1
0.01
10
15
20
25
30
35
40
Average SNR (dB)
Fixed PA, $\alpha = 1$
Fixed PA, $\alpha = 0.5$
Proposed

(a) $R_t = 0.5$ bps/Hz

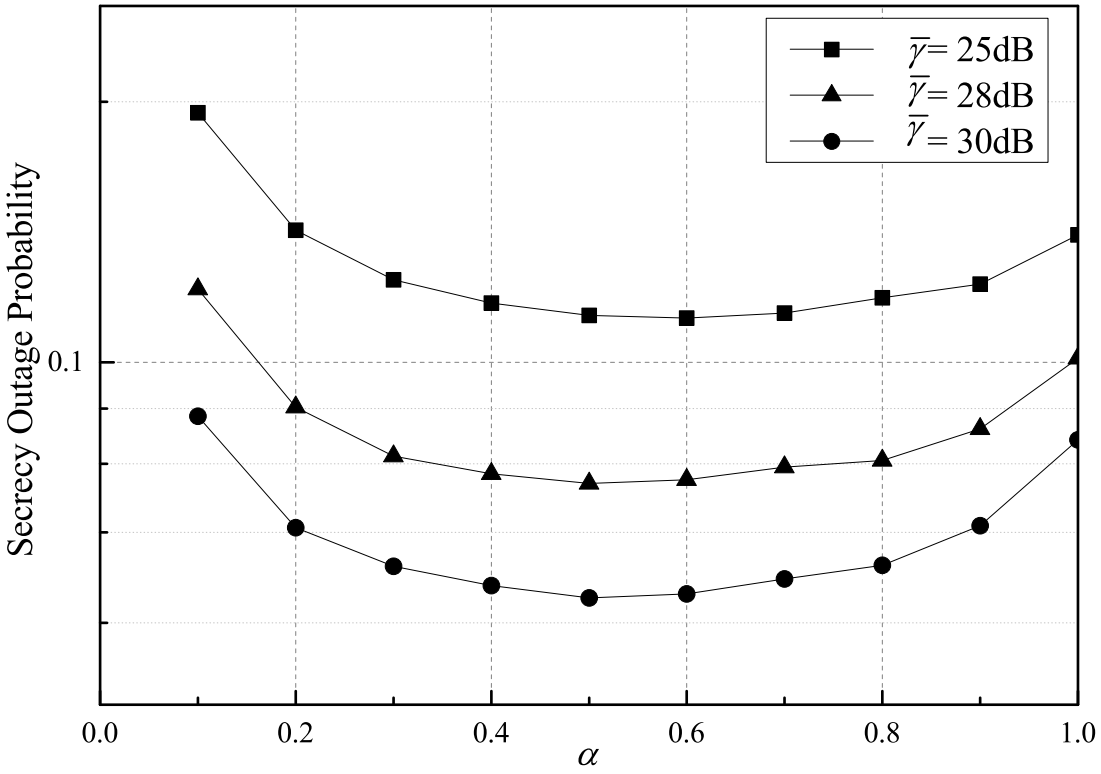


(b) $R_t = 1.0$ bps/Hz

Figure 2.14. Secrecy outage probability versus average SNR, $\sigma_{de}^2 = 2$ and $\sigma_{se}^2 = 0.5$.



(a) Ergodic secrecy rate versus α



(b) Secrecy outage probability versus α, $R_t = 1.0$ bps/Hz

Figure 2.15. Secrecy performances versus α, $\sigma_{de}^2 = 2$ and $\sigma_{se}^2 = 0.5$.

2.3.3 Multiple Antenna Eavesdropper

In wireless communication network, an eavesdropper is usually an unintended, uncontrollable node in the network. Since the purpose of the eavesdropper is to overhere the data signal from the source, it is possible that the eavesdropper has multiple antennas. This multiple antenna eavesdropper utilizes beamforming technique to enhance its signal reception. A new source power allocation is needed to deal with this multiple antenna eavesdropper, which will be considered in future works.

Consider a two-hop relay network which consists of a source, an AF relay, a destination, and an eavesdropper. Assume that the eavesdropper has N antennas, while all other nodes have single antenna, respectively. All other parameters are same as previous case with identical channel condition.

Fig. 2.16 shows the secrecy performances versus various values of N with $R_t = 1$ bps/Hz. It is shown that the proposed source power allocation scheme achieves lower secrecy outage probability than those of compared schemes even when the eavesdropper has 4 antennas. It is shown that the secrecy outage probability decreases as the number of antennas at the eavesdropper increases in all three schemes.

2.4 Summary

In this chapter, we propose a new source power allocation scheme for a two-hop relay network with cooperative jamming where the source and destination transmit jamming signals. When the full CSI of all links are available, an optimal source power allocation problem is formulated to maximize the secrecy rate. When the CSI

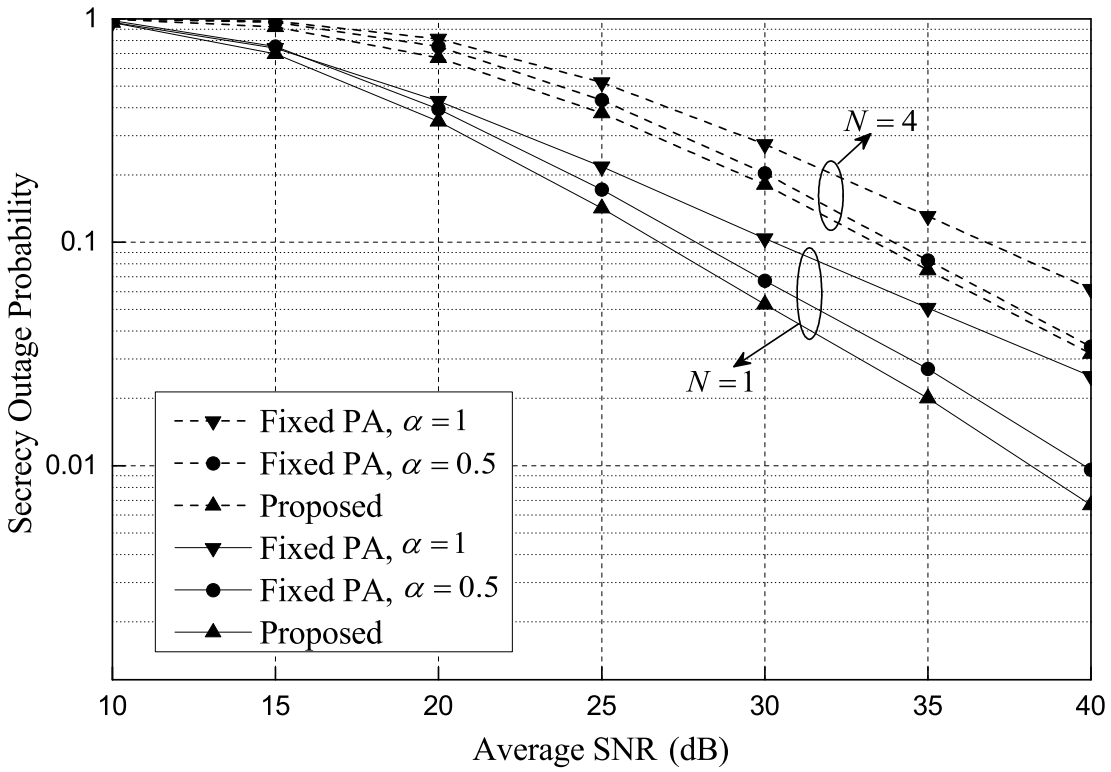


Figure 2.16. Secrecy outage probability for different number of antennas at the eavesdropper, N, $R_t = 1$ bps/Hz.

for desired links are only available, an optimal source power allocation problem is formulated to minimize the secrecy outage probability and the solution is obtained. Simulation results show that the proposed power allocation scheme achieves higher secrecy rate and lower secrecy outage probability than compared two fixed power allocation schemes.

Chapter 3

Power Allocation and Relay Selection for Cooperative Jamming in AF Relay Network with Multiple Relays and an Eavesdropper

Physical-layer security provides secure communication for a wireless network in which an eavesdropper attempts to intercept a data signal [3, 50, 51]. In a wireless relay network with physical layer security, its secrecy performance is improved by cooperative jamming or relay selection [25, 39, 52].

In cooperative jamming, a jamming signal is transmitted by a cooperating node to

interfere an eavesdropper. Most of previous works on cooperative jamming techniques focus on networks in which a single cooperating node transmits a jamming signal [45, 53]. In [45], a destination act as cooperating node to transmit a jamming signal. In [53], a relay and a cooperating node are selected among multiple intermediate nodes to minimize the secrecy outage probability (SOP).

Recently, cooperative jamming from multiple cooperating nodes is proposed to improve the secrecy performance more [40, 43, 54–56]. In [40, 43, 54, 55], multiple cooperating nodes are selected among relays which are not selected to forward the data signal. In [56], the network in which a source and destination serves as a cooperating node is studied, but this work considers single decode-and-forward (DF) relay which needs to decode its received signal first.

Utilizing cooperative jamming in DF relay network has some problems as follows, compared to that in amplify-and-forward (AF) relay network. First, when the jamming signal is transmitted from the cooperating node in the first phase, additional technique such as beamforming must be needed to help the relay decode its received signal. Second, transmitted signal from the DF relay is more vulnerable from eavesdropping than that from the AF relay which contains jamming signal received in the first phase. In AF relay network with cooperative jamming, of course, the destination also receives the signal which contains jamming signal from the relay. For this case, an efficient cooperative jamming technique is needed to improve the secrecy performance, which has not been investigated yet.

In this Chapter, we propose a new cooperative jamming technique in which the

source and destination transmit jamming signals for an AF relay network with multiple relays. By using AF relay protocol, the single antenna destination transmit a jamming signal without using any beamforming technique since the signal decoding at the relay does not needed. Also, the destination cancel its own jamming signal conveyed from the AF relay. Since the source node is idle during the second phase in conventional relay network, it transmit another jamming signal in the proposed cooperative jamming technique to further interfere the eavesdropper. We also propose a joint power allocation and relay selection scheme to minimize the SOP for the proposed cooperative jamming technique. A joint problem is formulated in which the transmit power of the transmitting nodes and which relay to select is determined, and it is divided into a master problem and a subproblem by using the primal decomposition method to obtain the solution.

The remainder of this Chapter is organized as follows. We describe the system model in Section 3.1. We derive the secrecy outage probability of the network in Section 3.2. We propose a joint power allocation and relay selection scheme for the network in Section 3.3. We present numerical results in Section 3.4. In Section 3.5, we extend the proposed scheme to multiple relay selection with power allocation. Finally, this Chapter is summarized in Section 3.6.

3.1 System Model

Consider a two-hop relay network consisting of a source S, M AF relays R_1, $R_2, \cdots$, R_M, a destination D, and an eavesdropper E, as shown in Fig. 3.1. Assume the direct

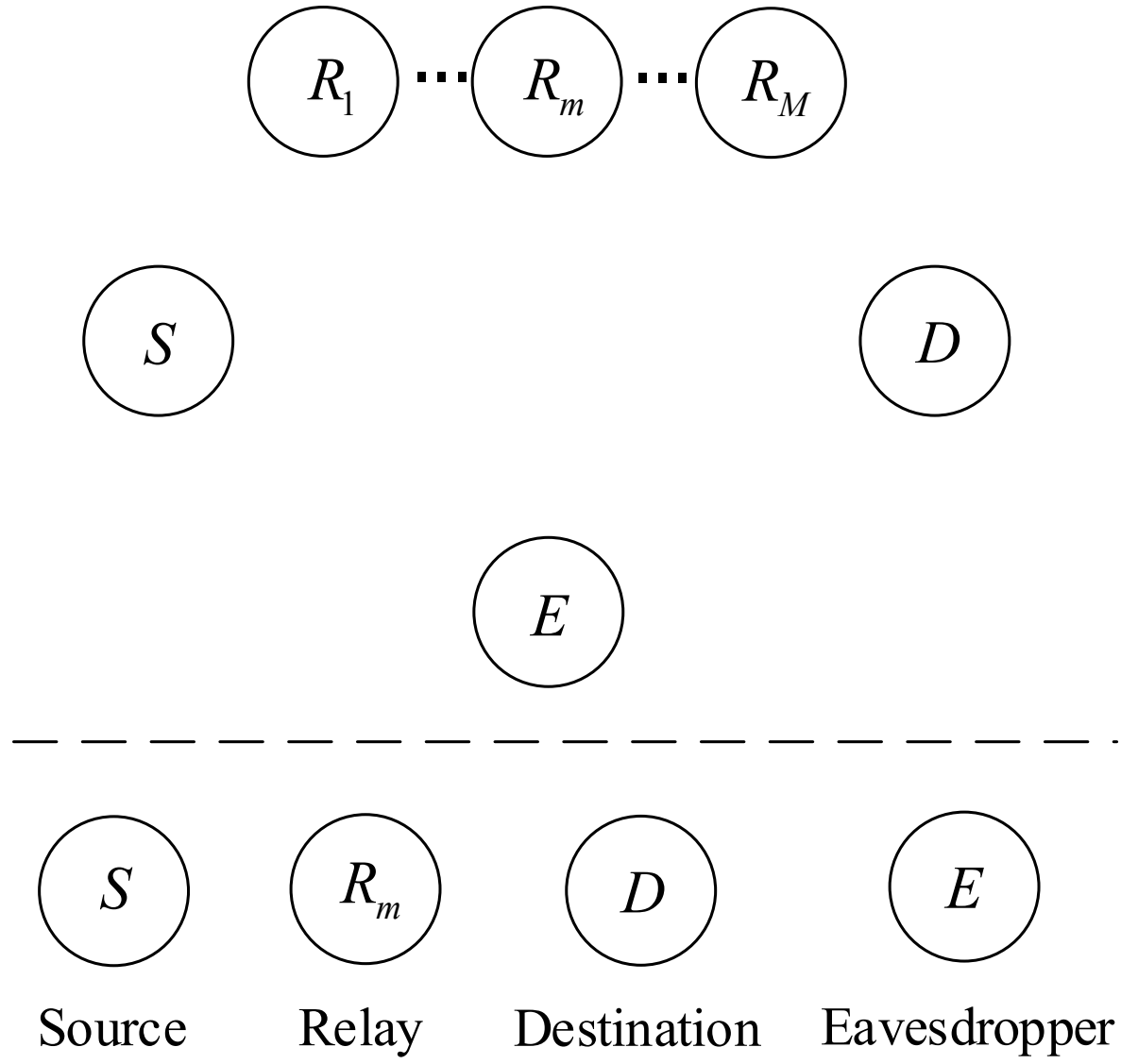


Figure 3.1. System model for a two-hop relay network with multiple AF relays.

link between the source and destination is negligible because of the high path loss, while the direct link between the source and eavesdropper exists.

Assume that all channels are reciprocal and the coefficient of the channel between node a and node b, h_{ab}, $(a,b) \in \{(S,R_m),(R_m,D),(R_m,E),(S,E),(D,E),$ $m=1,2,\cdots,M\}$, is an independent circularly symmetric complex Gaussian random variable with variance σ_{ab}^2. Assume that all channels have an additive white Gaussian noise (AWGN) with zero mean and variance N_0.

We propose a new cooperative jamming technique for the two-hop relay network in which the destination and source transmit jamming signals in two phases to interfere the eavesdropper, as shown in Fig. 3.2. In phase 1, the source transmits a data signal $x^{(1)}$ with transmit power $P_S^{(1)}$ while the destination transmits a jamming signal $z_D^{(1)}$ with transmit power $P_D^{(1)}$. Assume that the jamming signal $z_D^{(1)}$ is modeled as complex Gaussian random variable which is independent to the data signal $x^{(1)}$. The signal received at the m-th relay is given by

$$y_{R_m}^{(1)} = h_{SR_m}x^{(1)} + h_{R_mD}z_D^{(1)} + n_{R_m}^{(1)}, \tag{3.1}$$

for $m=1,\ 2,\cdots,M$, where $n_{R_m}^{(1)}$ is an AWGN. The signal received at the eavesdropper is given by

$$y_E^{(1)} = h_{SE}x^{(1)} + h_{DE}z_D^{(1)} + n_E^{(1)} \tag{3.2}$$

where $n_E^{(1)}$ is an AWGN. Suppose that m^*-th relay is selected out of M relays at the end of phase 1.

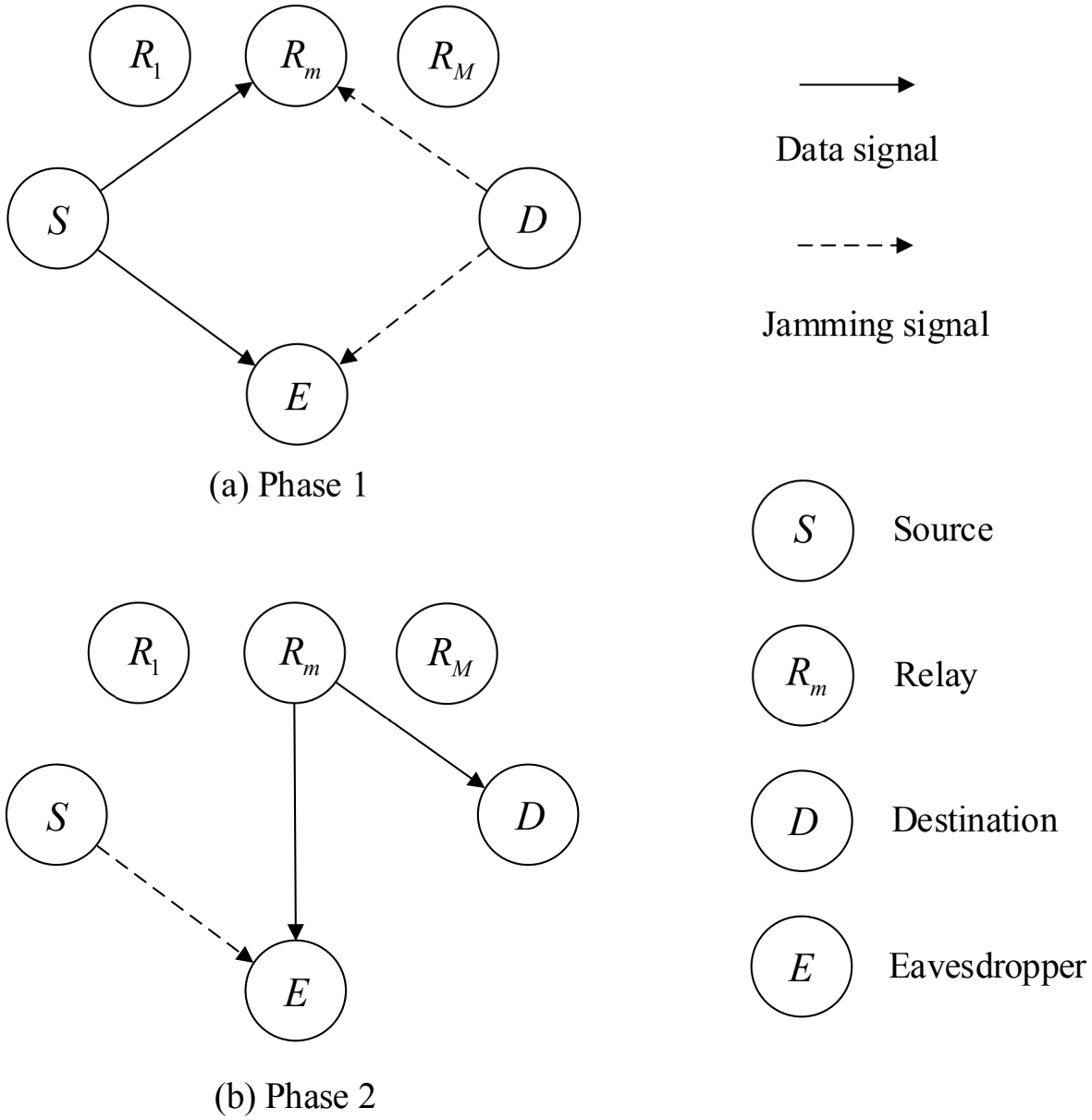


Figure 3.2. Signal transmission of the proposed cooperative jamming technique.

In phase 2, the selected m^*-th relay amplifies and forwards its received signal to the destination while the source transmits a jamming signal $z_S^{(2)}$ with transmit power $P_S^{(2)}$. Assume that the jamming signal $z_S^{(2)}$ is modeled as complex Gaussian random variable which is independent to the other signals. The amplification factor of the m^*-th relay is given by [57]

$$\beta_{R_{m^*}} = \sqrt{\frac{P_{R_{m^*}}^{(2)}}{|h_{SR_{m^*}}|^2 P_S^{(1)} + |h_{R_{m^*}D}|^2 P_D^{(1)} + N_0}} \tag{3.3}$$

where $P_{R_{m^*}}^{(2)}$ is the transmit power of the m^*-th relay. Since the jamming signal from the source is neglected at the destination because of its negligible strength, the signal received at the destination is given by

$$\begin{aligned} y_D^{(2)} &= h_{R_{m^*}D}\beta_{R_{m^*}} y_{R_{m^*}}^{(1)} + n_D^{(2)} \\ &= h_{R_{m^*}D}\beta_{R_{m^*}} h_{SR_{m^*}} x^{(1)} + h_{R_{m^*}D}\beta_{R_{m^*}} h_{R_{m^*}D} z_D^{(1)} \\ &\quad + h_{R_{m^*}D}\beta_{R_{m^*}} n_{R_{m^*}}^{(1)} + n_D^{(2)} \end{aligned} \tag{3.4}$$

where $n_D^{(2)}$ is an AWGN. Since the destination knows its own jamming signal $z_D^{(1)}$ assume that the destination perfectly cancels out $z_D^{(1)}$ from the received signal $y_D^{(2)}$. After the cancellation, the signal received at the destination is given by

$$\hat{y}_D^{(2)} = h_{R_{m^*}D}\beta_{R_{m^*}} h_{SR_{m^*}} x^{(1)} + h_{R_{m^*}D}\beta_{R_{m^*}} n_{R_{m^*}}^{(1)} + n_D^{(2)}. \tag{3.5}$$

From (3.3) and (3.5), the received signal-to-interference-plus-noise ratio (SINR) at

the destination is given by

$$\gamma_D = \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}D}|^2 |\beta_{R_{m^*}}|^2}{\left(|h_{R_{m^*}D}|^2 |\beta_{R_{m^*}}|^2 + 1\right) N_0}$$

$$= \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}D}|^2 P_{R_{m^*}}^{(2)}}{\left\{|h_{SR_{m^*}}|^2 P_S^{(1)} + |h_{R_{m^*}D}|^2 \left(P_{R_{m^*}}^{(2)} + P_D^{(1)}\right) + N_0\right\} N_0}. \tag{3.6}$$

The signal received at the eavesdropper is given by

$$\begin{aligned} y_E^{(2)} &= h_{R_{m^*}E} \beta_{R_{m^*}} y_{R_{m^*}}^{(1)} + h_{SE} z_S^{(2)} + n_E^{(2)} \\ &= h_{R_{m^*}E} \beta_{R_{m^*}} h_{SR_{m^*}} x^{(1)} + h_{R_{m^*}E} \beta_{R_{m^*}} h_{R_{m^*}D} z_D^{(1)} \\ &\quad + h_{R_{m^*}E} \beta_{R_{m^*}} n_{R_{m^*}}^{(1)} + h_{SE} z_S^{(2)} + n_E^{(2)} \end{aligned} \tag{3.7}$$

where $n_E^{(2)}$ is an AWGN. The eavesdropper employs selection combining on the two signals received in phase 1 and 2. After selection combining, the received SINR at the eavesdropper is given by

$$\gamma_E = \max \left\{ \frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)} + N_0}, \right.$$

$$\left. \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)} (|h_{R_{m^*}D}|^2 P_D^{(1)} + N_0) + (|h_{SE}|^2 P_S^{(2)} + N_0)(|h_{R_{m^*}D}|^2 P_D^{(1)} + |h_{SR_{m^*}}|^2 P_S^{(1)} + N_0)} \right\}$$

$$= \max \left\{ \frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)} + N_0}, \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (|h_{SE}|^2 P_S^{(2)} + N_0) B} \right\}. \tag{3.8}$$

where $A = P_{R_{m^*}}^{(2)} (|h_{R_{m^*}D}|^2 P_D^{(1)} + N_0)$ and $B = |h_{R_{m^*}D}|^2 P_D^{(1)} + |h_{SR_{m^*}}|^2 P_S^{(1)} + N_0$.

The secrecy rate of the network is given by [46]

$$C = \left[\frac{1}{2}\log_2(1+\gamma_D) - \frac{1}{2}\log_2(1+\gamma_E)\right]^+ \tag{3.9}$$

where $[x]^+ = \max\{0, x\}$.

3.2 Secrecy Outage Probability Analysis

A secrecy outage event occurs when the secrecy rate is less than a rate threshold, C_{th}. The secrecy outage probability of the network is defined as [47]

$$\begin{aligned} p_{out} &\triangleq \Pr\left[C < C_{th}\right] \\ &= \Pr\left[\frac{1}{2}\log_2(1+\gamma_D) - \frac{1}{2}\log_2(1+\gamma_E) < C_{th}\right]. \end{aligned} \tag{3.10}$$

Assume that the destination knows the exact coefficients of the channels between S and R_m and between R_m and D as well as the variances of the coefficients of all other channels. This assumption is common in many works considering physical layer security [25], and these coefficients of the channels could be obtained by channel estimation technique. From (3.7), (3.8), and (3.10), the SOP of the network is given

by

$$
\begin{aligned}
p_{out} &= \Pr\left[\max\left\{\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)} + N_0}, \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (|h_{SE}|^2 P_S^{(2)} + N_0)B}\right\} > \eta\right] \\
&= \Pr\left[\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)} + N_0} > \eta\right] \\
&\quad + \Pr\left[\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)} + N_0} \leq \eta,\ \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (|h_{SE}|^2 P_S^{(2)} + N_0)B} > \eta\right].
\end{aligned}
\tag{3.11}
$$

where $\eta \triangleq (1+\gamma_D)2^{-2C_{th}} - 1$.

The first term on the right-hand side of (3.11) is given by

$$
\begin{aligned}
&\Pr\left[\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)} + N_0} > \eta\right] \\
&= \int \Pr\left[|h_{SE}|^2 > \frac{\eta(|h_{DE}|^2 P_D^{(1)} + N_0)}{P_S^{(1)}} \,\middle|\, |h_{DE}|^2 = x\right] \cdot f_{|h_{DE}|^2}(x)\, dx \\
&= \int_0^\infty \exp\left(-\frac{\eta(xP_D^{(1)} + N_0)}{\sigma_{SE}^2 P_S^{(1)}}\right) \frac{1}{\sigma_{DE}^2} \exp\left(-\frac{x}{\sigma_{DE}^2}\right) dx \\
&= \frac{1}{\sigma_{DE}^2} \exp\left(-\frac{\eta N_0}{\sigma_{SE}^2 P_S^{(1)}}\right) \int_0^\infty \exp\left(-\frac{\eta x P_D^{(1)}}{\sigma_{SE}^2 P_S^{(1)}} - \frac{x}{\sigma_{DE}^2}\right) dx \\
&= \frac{1}{\sigma_{DE}^2} \exp\left(-\frac{\eta N_0}{\sigma_{SE}^2 P_S^{(1)}}\right) \frac{1}{\frac{\eta P_D^{(1)}}{\sigma_{SE}^2 P_S^{(1)}} + \frac{1}{\sigma_{DE}^2}}.
\end{aligned}
\tag{3.12}
$$

The second term on the right-hand side of (3.11) is given by

$$\Pr\left[\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)}+N_0} \le \eta,\ \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (|h_{SE}|^2 P_S^{(2)}+N_0)B} > \eta\right]$$

$$= \int_0^\infty \Pr\left[\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)}+N_0} \le \eta,\ \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (|h_{SE}|^2 P_S^{(2)}+N_0)B} > \eta \,\middle|\, |h_{SE}|^2 = x\right] \cdot \frac{1}{\sigma_{SE}^2}\exp\left(-\frac{x}{\sigma_{SE}^2}\right) dx$$

$$= \frac{1}{\sigma_{SE}^2}\int_0^\infty \Pr\left[\frac{xP_S^{(1)}}{|h_{DE}|^2 P_D^{(1)}+N_0} \le \eta,\ \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (xP_S^{(2)}+N_0)B} > \eta\right] \cdot \exp\left(-\frac{x}{\sigma_{SE}^2}\right) dx$$

$$= \frac{1}{\sigma_{SE}^2}\int_0^\infty \Pr\left[\frac{xP_S^{(1)}}{|h_{DE}|^2 P_D^{(1)}+N_0} \le \eta\right] \cdot \Pr\left[\frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (xP_S^{(2)}+N_0)B} > \eta\right] \cdot \exp\left(-\frac{x}{\sigma_{SE}^2}\right) dx$$

$$= \int_0^\infty p_1(x)\cdot p_2(x)\cdot \frac{1}{\sigma_{SE}^2}\exp\left(-\frac{x}{\sigma_{SE}^2}\right) dx \tag{3.13}$$

where

$$p_1(x) = \Pr\left[\frac{xP_S^{(1)}}{|h_{DE}|^2 P_D^{(1)}+N_0} \le \eta\right] \tag{3.14}$$

and

$$p_2(x) = \Pr\left[\frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (xP_S^{(2)}+N_0)B} > \eta\right]. \tag{3.15}$$

Since $|h_{DE}|^2$ is exponentially distributed from the assumption of the coefficient of the

channel, (3.14) is rewritten as

$$p_1(x) = \Pr\left[|h_{DE}|^2 \geq \frac{1}{P_D^{(1)}}\left(\frac{xP_S^{(1)}}{\eta} - N_0\right)\right]$$
$$= \begin{cases} \exp\left(-\frac{1}{\sigma_{DE}^2 P_D^{(1)}}\left(\frac{xP_S^{(1)}}{\eta} - N_0\right)\right), & \text{if } x \geq \frac{N_0\eta}{P_S^{(1)}}, \\ 1, & \text{otherwise.} \end{cases} \tag{3.16}$$

Similarly, (3.15) is rewritten as

$$p_2(x) = \Pr\left[|h_{R_{m^*}E}|^2\left(|h_{SR_{m^*}}|^2 P_S^{(1)} P_{R_{m^*}}^{(2)} - \eta A\right) > \eta(xP_S^{(2)} + N_0)B\right]$$
$$= \begin{cases} \exp\left(-\frac{\eta(P_S^{(2)}x + N_0)B}{\xi\sigma_{R_{m^*}E}^2}\right), & \text{if } \xi \geq 0, \\ 0, & \text{otherwise} \end{cases} \tag{3.17}$$

where $\xi \triangleq |h_{SR_{m^*}}|^2 P_S^{(1)} P_{R_{m^*}}^{(2)} - \eta A$. From (3.13), (3.16), and (3.17), The second term

on the right-hand side of (3.11) is given by

$$\Pr\left[\frac{|h_{SE}|^2 P_S^{(1)}}{|h_{DE}|^2 P_D^{(1)}+N_0} \le \eta,\ \frac{|h_{SR_{m^*}}|^2 P_S^{(1)} |h_{R_{m^*}E}|^2 P_{R_{m^*}}^{(2)}}{|h_{R_{m^*}E}|^2 A + (|h_{SE}|^2 P_S^{(2)}+N_0)B} > \eta\right]$$

$$= \frac{1}{\sigma_{SE}^2}\exp\left(-\frac{\eta A N_0 B}{\xi \sigma_{R_{m^*}E}^2}\right)\cdot\left\{\frac{1}{\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}+\frac{1}{\sigma_{SE}^2}}\left(1-\exp\left(-\left(\frac{1}{\sigma_{SE}^2}+\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}\right)\frac{N_0\eta}{P_S^{(1)}}\right)\right)\right.$$

$$\left.+\frac{1}{\frac{P_S^{(1)}}{\sigma_{DE}^2 P_D^{(1)}\eta}+\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}+\frac{1}{\sigma_{SE}^2}}\exp\left(\frac{N_0}{\sigma_{DE}^2 P_D^{(1)}}-\left(\frac{P_S^{(1)}}{\sigma_{DE}^2 P_D^{(1)}\eta}+\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}+\frac{1}{\sigma_{SE}^2}\right)\frac{N_0\eta}{P_S^{(1)}}\right)\right\}. \tag{3.18}$$

From (3.11), (3.12), and (3.18), the SOP of the network is given by

$$p_{out} = \frac{1}{\sigma_{DE}^2}\exp\left(-\frac{\eta N_0}{\sigma_{SE}^2 P_S^{(1)}}\right)\frac{1}{\frac{\eta P_D^{(1)}}{\sigma_{SE}^2 P_S^{(1)}}+\frac{1}{\sigma_{DE}^2}}$$

$$+\frac{1}{\sigma_{SE}^2}\exp\left(-\frac{\eta A N_0 B}{\xi\sigma_{R_{m^*}E}^2}\right)\cdot\left\{\frac{1}{\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}+\frac{1}{\sigma_{SE}^2}}\left(1-\exp\left(-\frac{N_0\eta}{P_S^{(1)}}\left(\frac{1}{\sigma_{SE}^2}+\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}\right)\right)\right)\right.$$

$$\left.+\frac{1}{\frac{P_S^{(1)}}{\sigma_{DE}^2 P_D^{(1)}\eta}+\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}+\frac{1}{\sigma_{SE}^2}}\cdot\exp\left(\frac{N_0}{\sigma_{DE}^2 P_D^{(1)}}-\left(\frac{P_S^{(1)}}{\sigma_{DE}^2 P_D^{(1)}\eta}+\frac{\eta A P_S^{(2)} B}{\xi\sigma_{R_{m^*}E}^2}+\frac{1}{\sigma_{SE}^2}\right)\frac{N_0\eta}{P_S^{(1)}}\right)\right\}. \tag{3.19}$$

3.3 Power Allocation and Relay Selection

The SOP obtained in the previous section depends on the transmit power of the source, relay and destination as well as selected relay, that is, m^*. With limited available power of the network, we need to determine the transmit power of these nodes and which relay to select to minimize the SOP. We propose joint power allocation and relay selection scheme for the network with the proposed cooperative jamming technique.

3.3.1 Total Power Constraint

Let $\mathbf{P} = \left(P_S^{(1)},\ P_D^{(1)},\ P_{R_m}^{(2)},\ P_S^{(2)}\right)$ denote a 4-tuple of transmit powers and P_{tot} denote the maximum available power of the network. Then, the set of feasible $\mathbf{P}$ is given by

$$\mathcal{P}_f = \left\{ \left(P_S^{(1)},\ P_D^{(1)},\ P_{R_m}^{(2)},\ P_S^{(2)}\right) \middle|\ 0 \leq P \leq P_{tot}, \right. \\ \left. P \in \{P_S^{(1)}, P_D^{(1)}, P_{R_m}^{(2)}, P_S^{(2)}\} \right\}. \tag{3.20}$$

A joint power allocation and relay selection problem to minimize the SOP is formulated as

$$\{\mathbf{P}^*, m^*\} = \underset{\substack{\mathbf{P} \in \mathcal{P}_f \\ m \in \{1,\cdots,M\}}}{\arg\min} \quad p_{out} \tag{3.21}$$

subject to

$$P_S^{(1)} + P_D^{(1)} + P_{R_m}^{(2)} + P_S^{(2)} = P_{tot}. \tag{3.22}$$

Since the problem (3.21) is non-convex, we divide it into a master problem and a subproblem by using the primal decomposition method [58]. The master problem determines total transmit power in each phase, and the subproblem determines transmitting relay and each node's transmit power in each phase, respectively with fixed total transmit power of each phase. The details of proposed master problem and subproblem are as follows. Let $P_{tot}^{(1)}$ and $P_{tot}^{(2)}$ denote available power in phase 1 and that in phase 2, respectively. Then the constraint in (3.22) is divided into two: one for phase 1 and the other for phase 2, which are given by

$$P_S^{(1)} + P_D^{(1)} = P_{tot}^{(1)}, \tag{3.23}$$

and

$$P_{R_m}^{(2)} + P_S^{(2)} = P_{tot}^{(2)}, \tag{3.24}$$

respectively.

With these constraints, we formulate a master problem and a subproblem. In the subproblem, $P_{tot}^{(1)}$ and $P_{tot}^{(2)}$ are fixed and $\mathbf{P}$ is optimized with constraints (3.23) and (3.24), along with the relay selection, and in the master problem, $P_{tot}^{(1)}$ and $P_{tot}^{(2)}$ are optimized by using the results of the subproblem.

The master problem is formulated as

$$\min_{P_{tot}^{(1)},\, P_{tot}^{(2)}} \quad p_{out} \tag{3.25}$$

subject to

$$P_{tot}^{(1)} + P_{tot}^{(2)} = P_{tot}, \tag{3.26}$$

which is easily solved by one-dimensional line search. Then for the fixed $P_{tot}^{(1)}$ and $P_{tot}^{(2)}$, the subproblem is formulated as

$$\{\mathbf{P}^*, m^*\} = \underset{\substack{\mathbf{P} \in \mathcal{P}_f \\ m \in \{1,\cdots,M\}}}{\arg\min} \quad p_{out} \tag{3.27}$$

subject to (3.23) and (3.24), which is also solved easily by one-dimensional line search for each variable. Optimal relay is selected by iterating this power allocation procedure about each relay.

3.3.2 Power Constraints for Each Phases

Let $P^{(1)}$ and $P^{(2)}$ denote the power constraints for phase 1 and that for phase 2, respectively. Then, a joint power allocation and relay selection problem to minimize the SOP is formulated as

$$\{\mathbf{P}^*, m^*\} = \underset{\substack{\mathbf{P} \\ m \in \{1,\cdots,M\}}}{\arg\min} \quad p_{out} \tag{3.28}$$

subject to

$$P_S^{(1)} + P_D^{(1)} \leq P^{(1)}, \tag{3.29}$$

$$P_{R_m}^{(2)} + P_S^{(2)} \leq P^{(2)}. \tag{3.30}$$

To find the optimal values of the transmit powers, these following Theorems are given.

Theorem 1. *Given $P_S^{(1)}$ fixed, p_{out} decreases monotonically with $P_D^{(1)}$ increasing.*

Proof. $P_D^{(1)}$ is the power of the jamming signal from the destination. Because of the assumption that the destination perfectly cancels its own jamming signal, the jamming signal from the destination has more effects on the eavesdropper. Thus, the secrecy rate, C, increases monotonically with $P_D^{(1)}$ increasing and the secrecy outage probability, p_{out}, decreases monotonically with $P_D^{(1)}$ increasing. ■

Theorem 2. *Given $P_{R_m}^{(2)}$ fixed, p_{out} decreases monotonically with $P_S^{(2)}$ increasing.*

Proof. $P_S^{(2)}$ is the power of the jamming signal from the source. Because of the assumption that there is no direct link between the source and destination, the jamming signal from the source affects the eavesdropper only. Thus, the secrecy rate, C, increases monotonically with $P_S^{(2)}$ increasing and the secrecy outage probability, p_{out}, decreases monotonically with $P_S^{(2)}$ increasing. ■

Theorem 3. *Optimal solution of the problem (3.28) is obtained when the constraints are satisfied in equality, i.e., $P_S^{(1)} + P_D^{(1)} = P^{(1)}$ and $P_{R_m}^{(2)} + P_S^{(2)} = P^{(2)}$.*

Proof. Suppose that $\mathbf{P}^* = (P_S^{(1)}, P_D^{(1)}, P_S^{(2)}, P_{R_m}^{(2)})$ which satisfies $P_S^{(1)} + P_D^{(1)} = \hat{P}^{(1)} < P^{(1)}$ and $P_S^{(2)} + P_{R_m}^{(2)} = \hat{P}^{(2)} < P^{(2)}$ is optimal solution of the problem (3.28). Then, for $P^{**} = (P_S^{(1)}, P_D^{(1)} + P^{(1)} - \hat{P}^{(1)}, P_S^{(2)} + P^{(2)} - \hat{P}^{(2)}, P_{R_m}^{(2)})$, it satisfies the constraint of the problem (3.28) and $p_{out}|_{\mathbf{P}=\mathbf{P}^{**}} < p_{out}|_{\mathbf{P}=\mathbf{P}^*}$ because of Theorem 1 and Theorem 2, This contradicts the supposition that $\mathbf{P}^*$ is optimal solution of the problem (3.28).

Thus, an optimal solution of the problem (3.28) is obtained when the constraints are satisfied in equality. ■

Thus, problem (3.28) is reformulated as

$$\{\mathbf{P}^*, m^*\} = \underset{\substack{\mathbf{P} \\ m \in \{1,\cdots,M\}}}{\arg\min} \quad p_{out} \tag{3.31}$$

subject to

$$P_S^{(1)} + P_D^{(1)} = P^{(1)}, \tag{3.32}$$

$$P_{R_m}^{(2)} + P_S^{(2)} = P^{(2)}. \tag{3.33}$$

This optimization problem can be solved by exhaustive search. After the power vector $\mathbf{P}$ is determined by exhaustive search, optimal relay can be easily obtained.

3.4 Numerical Results

Consider a two-hop AF relay network with a source, M relays, a destination, and an eavesdropper. We assume that the noise variance, N_0, and the variances of all channel coefficients, σ_{ab}^2, are normalized to 1 [45]. With this assumption, we can handle the average SNR value by determining the total transmit power P_{tot}.

Fig. 3.3 shows the probability of the non-zero secrecy rate versus average SNR with various cooperative jamming schemes. For comparison, we show the SOP of a conventional jamming power allocation (JPA) scheme for the network with a conventional cooperative jamming technique in which only the destination transmits a

jamming signal [45]. It is shown that the proposed scheme for the network with the proposed technique achieves higher probability to satisfy secure communication than a conventional JPA scheme for the network with a conventional technique as well as the proposed scheme for the network without cooperative jamming. It is shown that the probability increases as the average SNR increases for all schemes.

Fig. 3.4 shows the secrecy outage probability for the network with various cooperative jamming schemes. It is shown that the proposed scheme for the network with the proposed technique provides lower SOP than a conventional JPA scheme for the network with a conventional technique as well as the proposed scheme for the network without cooperative jamming, especially in high average SNR region. This is because when the average SNR increases, more power is allocated to the jamming signal from the source, result in decrease of the SOP. It is shown that the proposed scheme has lower SOP as the number of relays increases. It is shown that the SOP increases as the rate threshold increases.

Fig. 3.5 shows the secrecy outage probability for the network versus the number of relays when the average SNR is 20dB and 30dB. It is shown that the SOP of all schemes decrease as the number of relay increases. It is shown that for each average SNR value, SOP saturates in its final value as the number of relay increases.

Fig. 3.6 shows the secrecy outage probability for the network when the eavesdropper is close to the source. To directly apply this case, suppose that $\sigma_{SE}^2 = 2$ and $\sigma_{DE}^2 = 0.5$, while variances of all other channel coefficients are normalized to 1. It is shown that the SOP is higher than the case when the variances of all channel

coefficients are equal.

Fig. 3.7 shows the secrecy outage probability for the network when the eavesdropper is close to the relays. To directly apply this case, suppose that $\sigma^2_{R_mE} = 2$, while variances of all other channel coefficients are normalized to 1. It is shown that the SOP is almost same as the case when the variances of all channel coefficients are equal.

Fig. 3.8 shows the secrecy outage probability for the network when the eavesdropper is close to the destination. To directly apply this case, suppose that $\sigma^2_{DE} = 2$ and $\sigma^2_{SE} = 0.5$, while variances of all other channel coefficients are normalized to 1. It is shown that the SOP is lower than the case when the variances of all channel coefficients are equal.

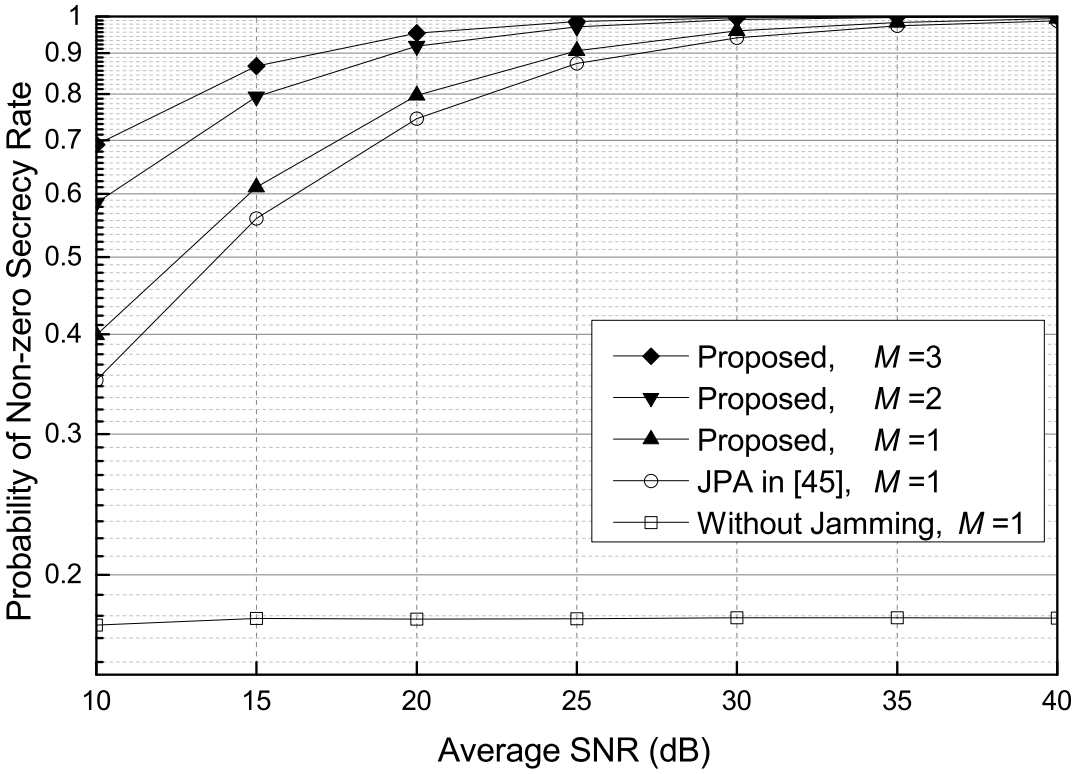
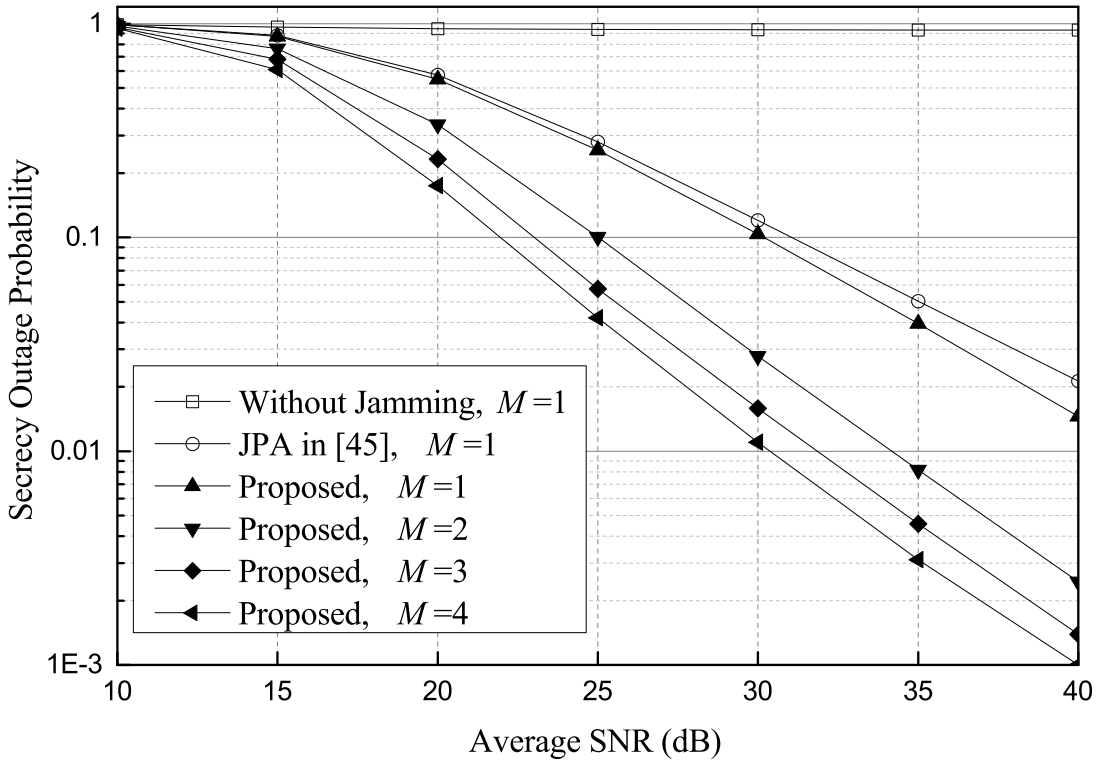
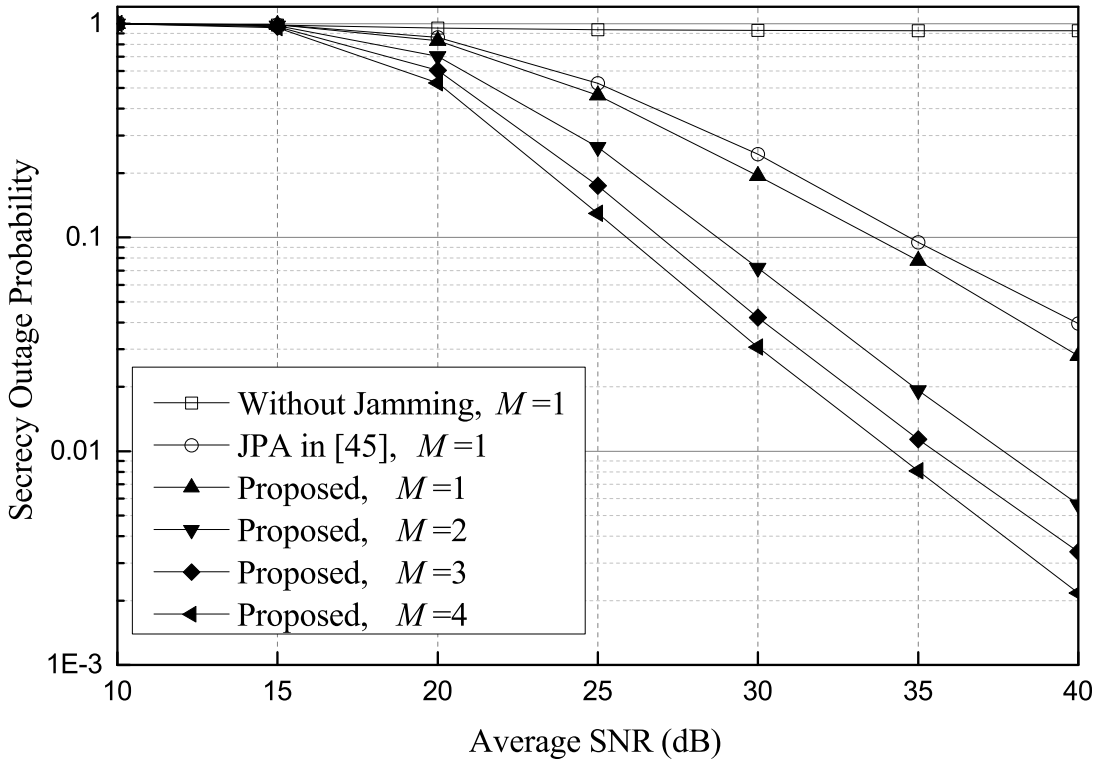


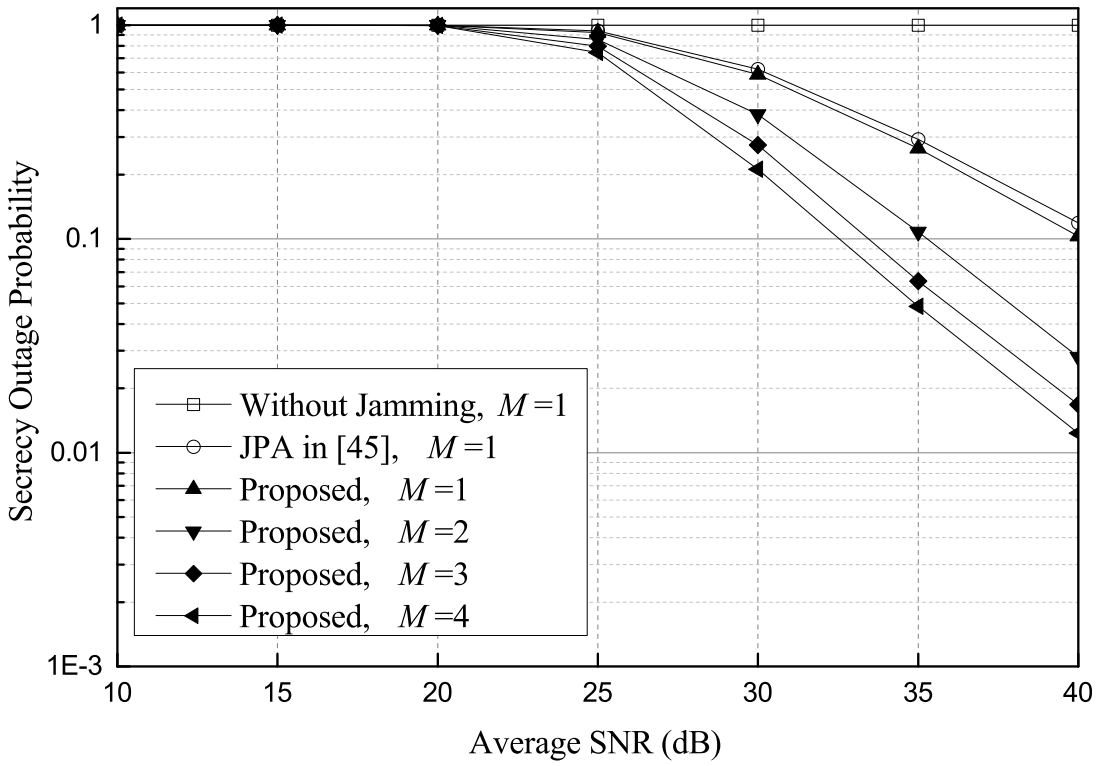
Figure 3.3. Probability of the non-zero secrecy rate versus average SNR.



(a) $C_{th} = 0.5$ bps/Hz

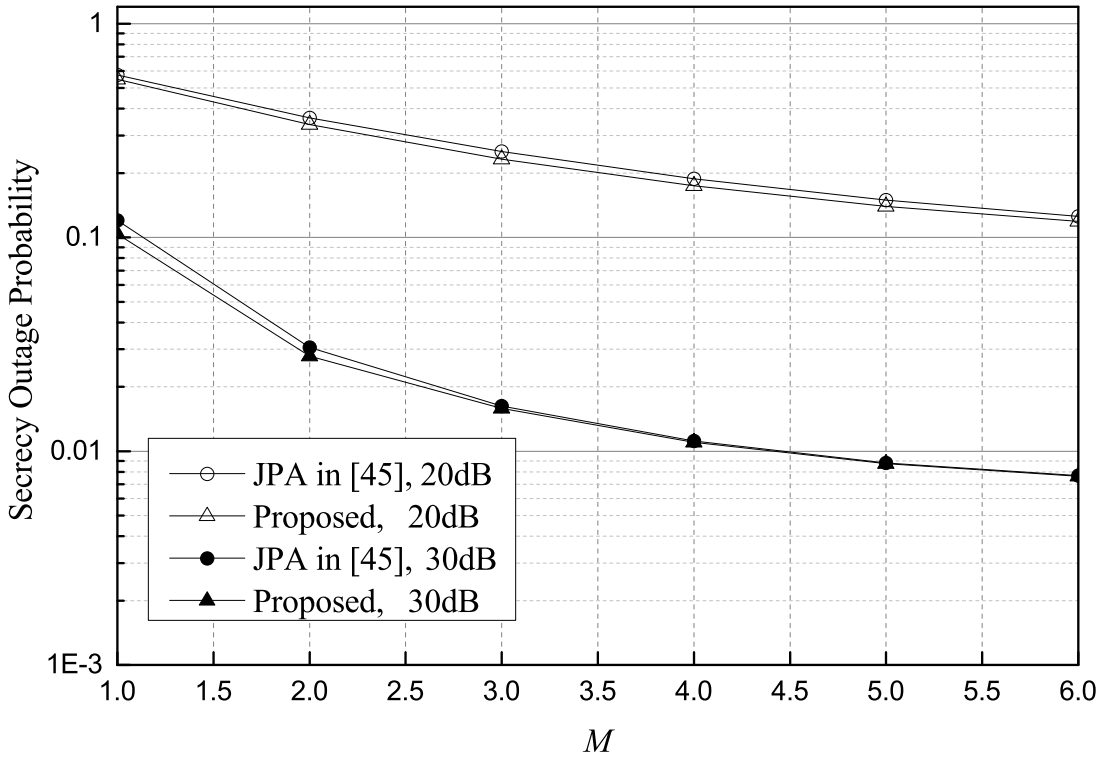


(b) $C_{th} = 1.0$ bps/Hz

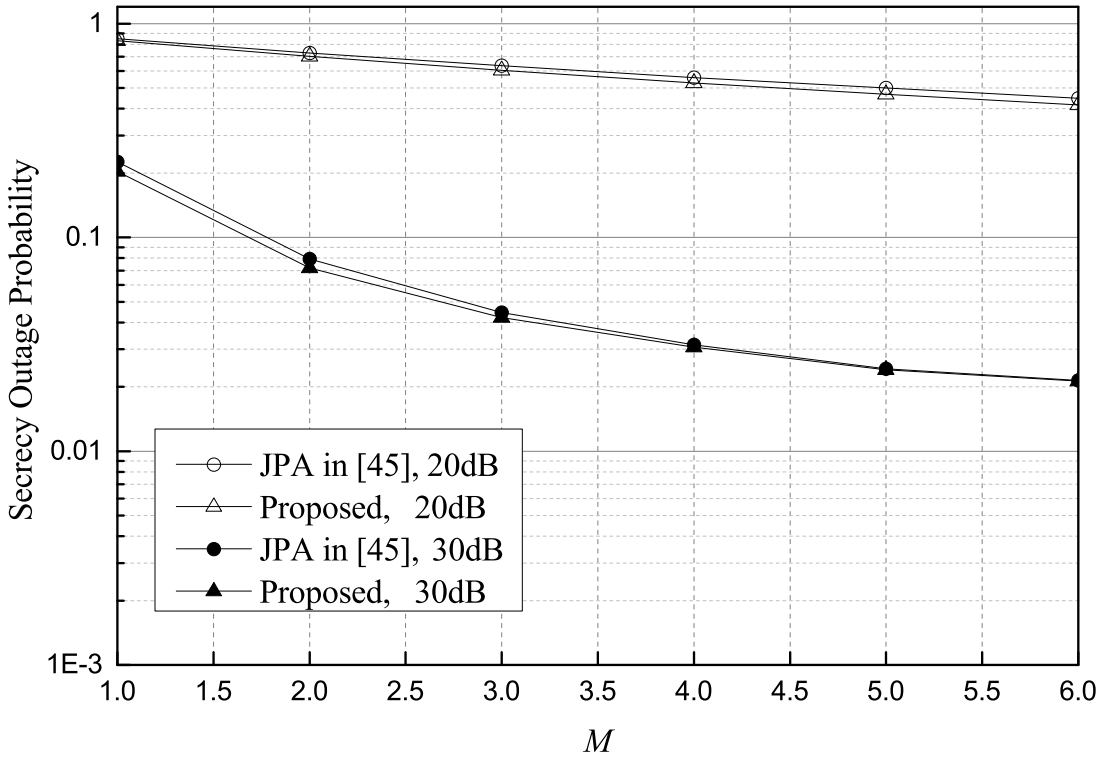


(c) $C_{th} = 2.0$ bps/Hz

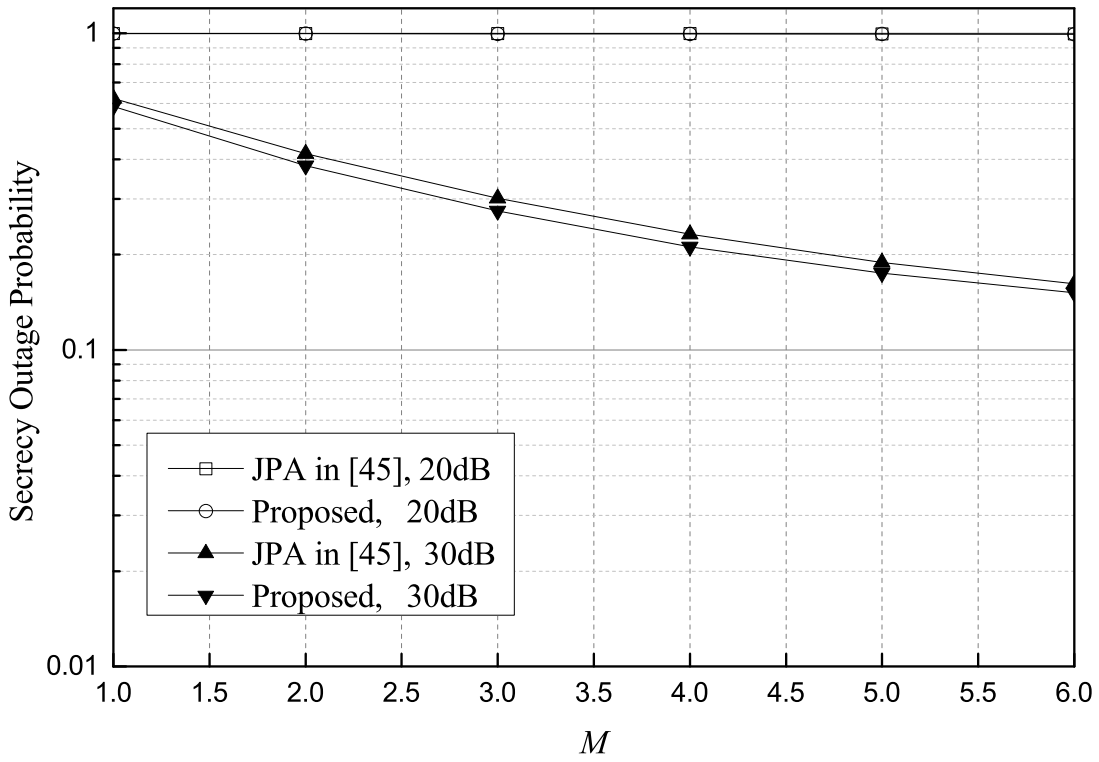
Figure 3.4. Secrecy outage probability with various cooperative jamming schemes.



(a) $C_{th} = 0.5$ bps/Hz

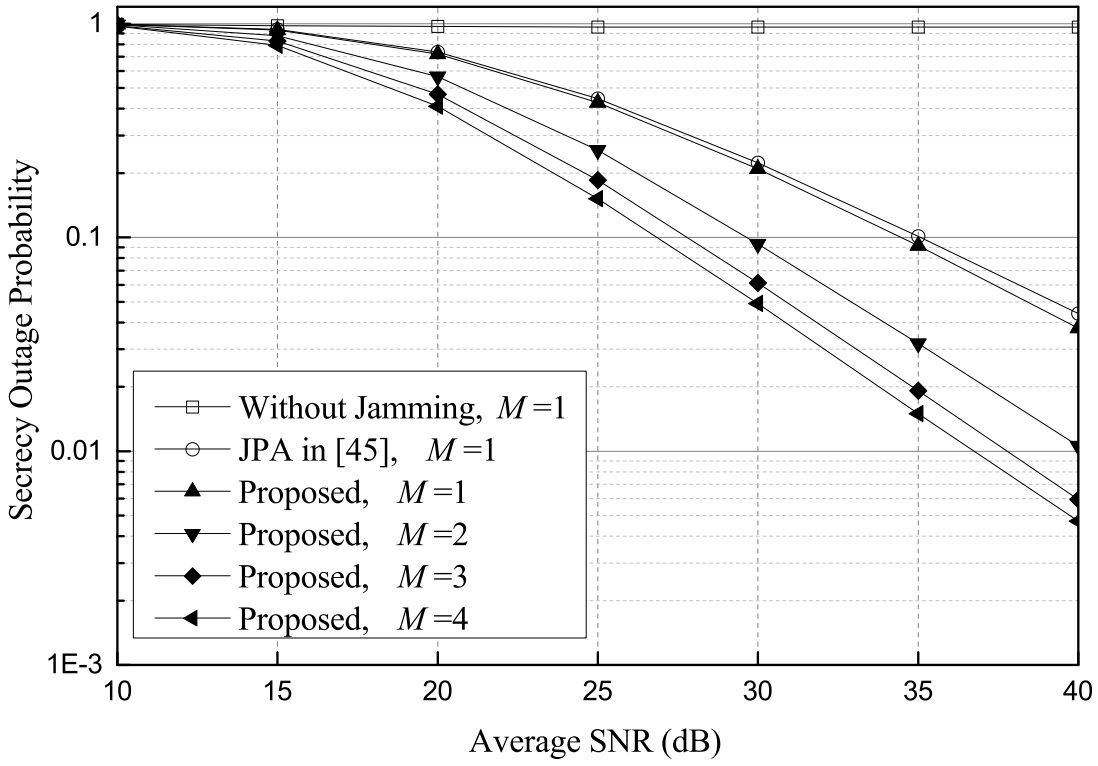


(b) $C_{th} = 1.0$ bps/Hz

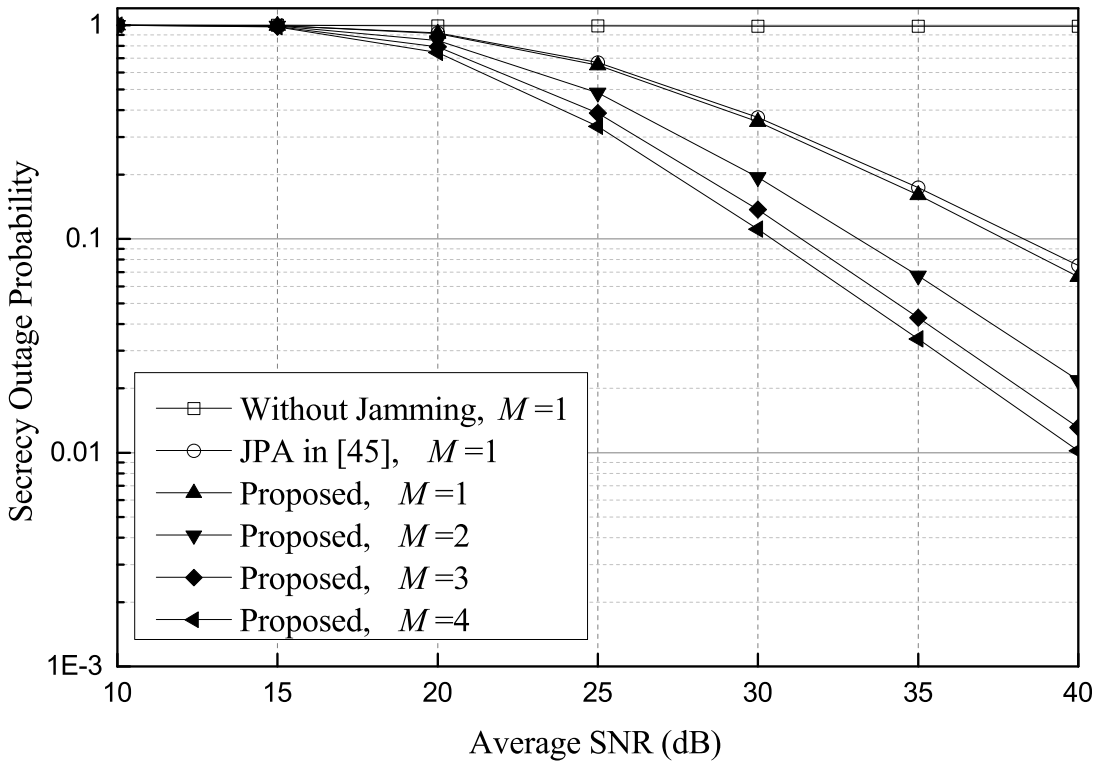


(c) $C_{th} = 2.0$ bps/Hz

Figure 3.5. Secrecy outage probability versus the number of relays.

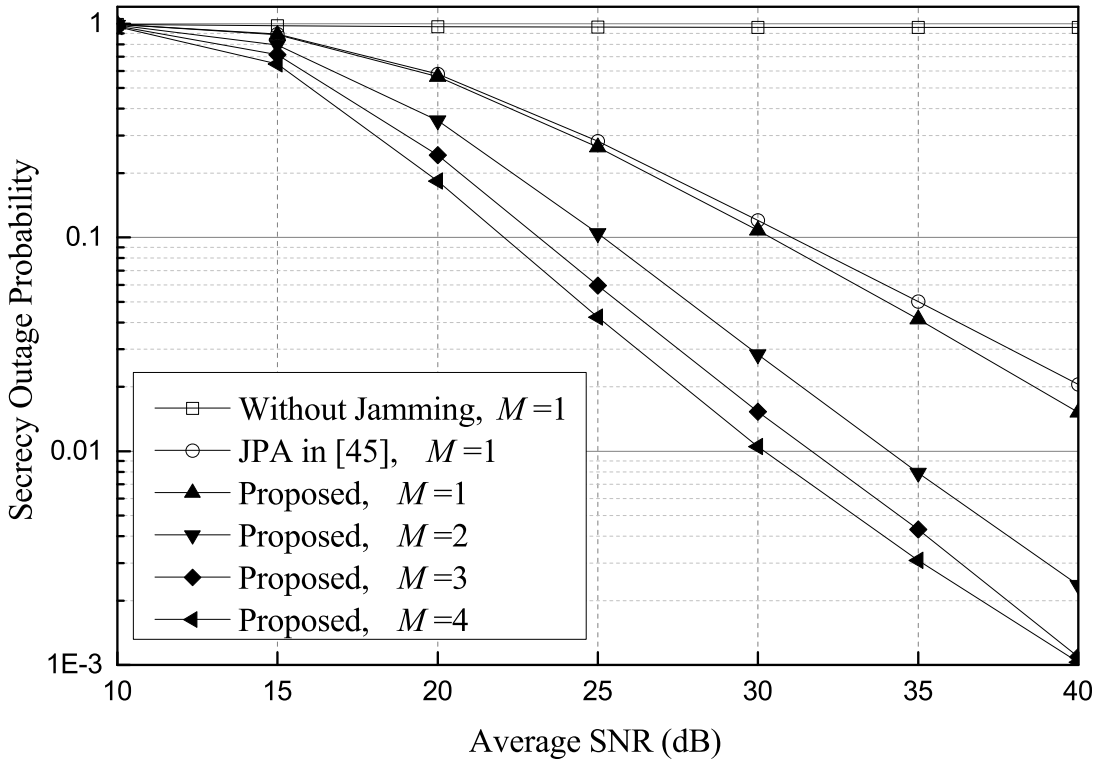


(a) $C_{th} = 0.5$ bps/Hz

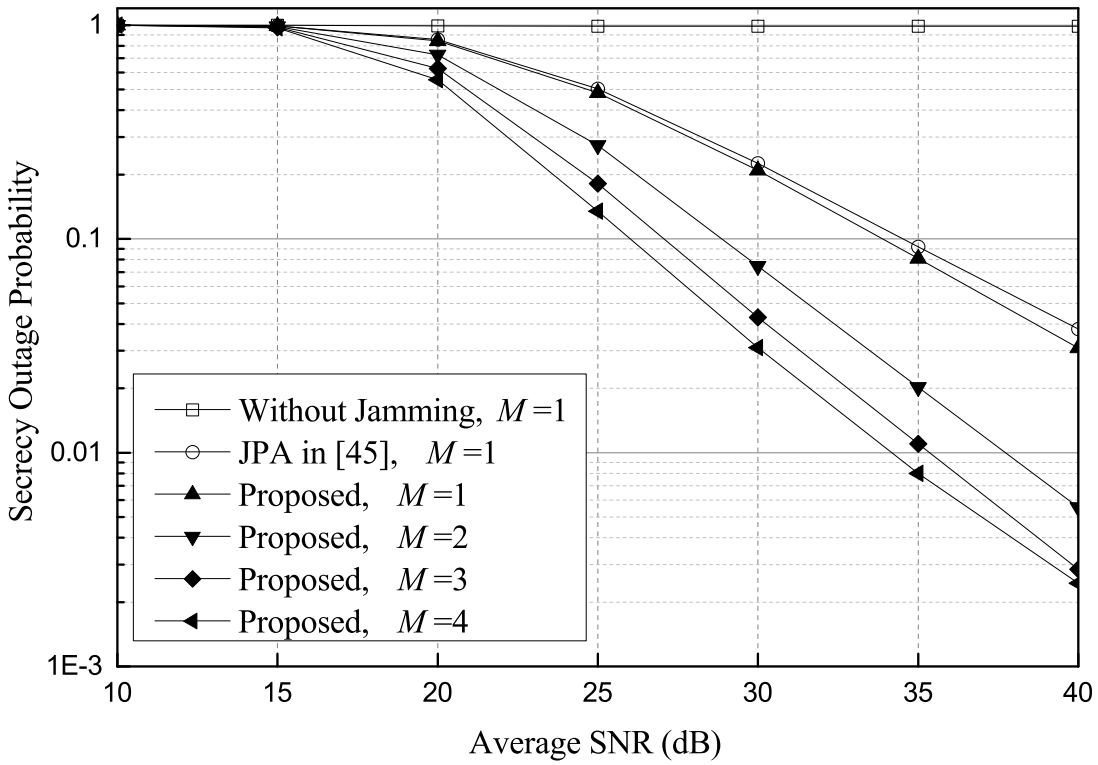


(b) $C_{th} = 1.0$ bps/Hz

Figure 3.6. Secrecy outage probability versus average SNR, $\sigma^2_{SE} = 2$ and $\sigma^2_{DE} = 0.5$.

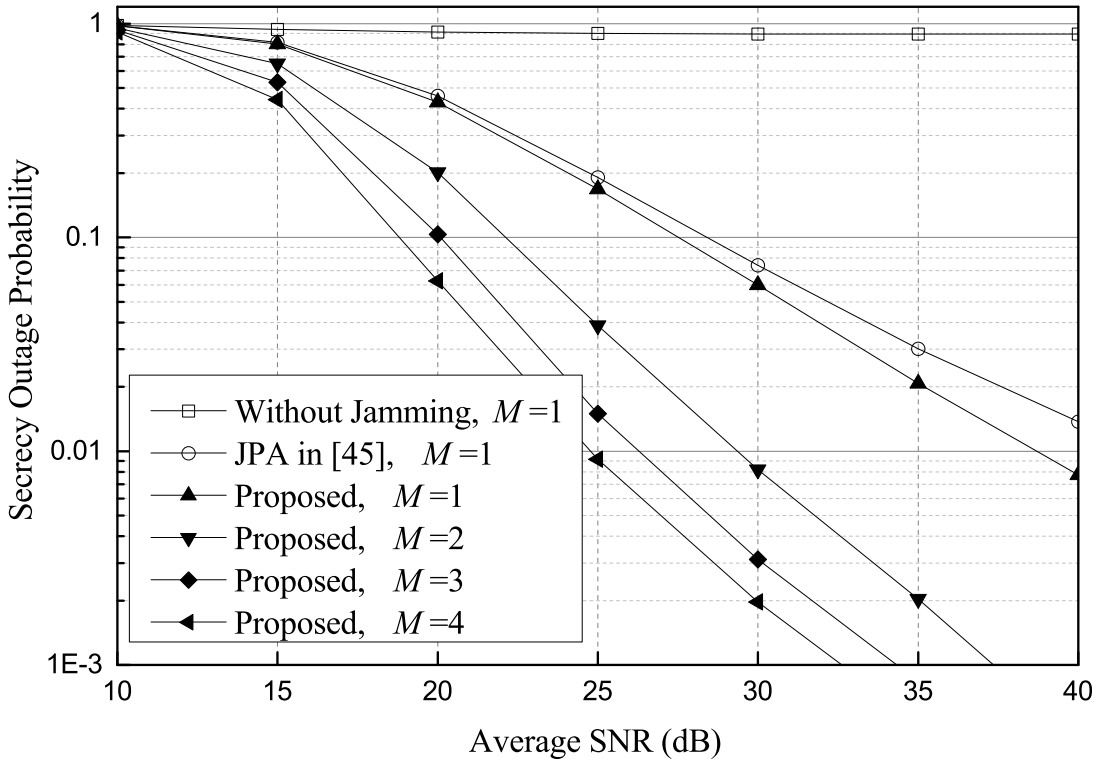


(a) $C_{th} = 0.5$ bps/Hz

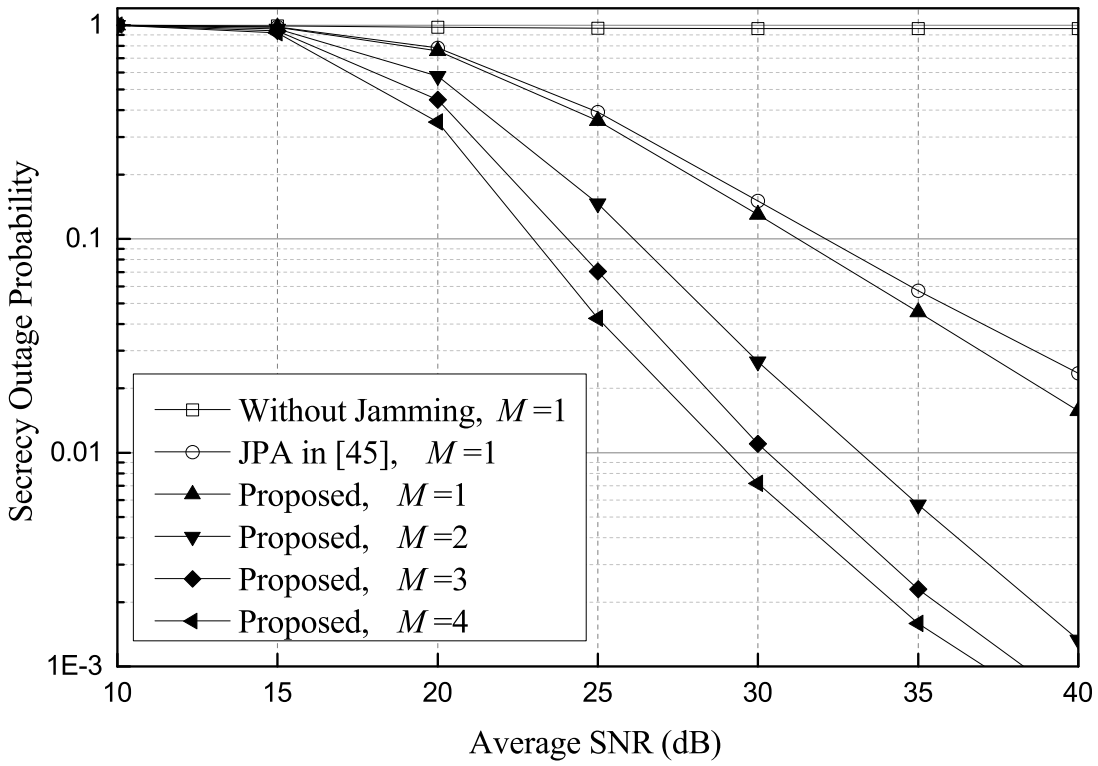


(b) $C_{th} = 1.0$ bps/Hz

Figure 3.7. Secrecy outage probability versus average SNR, $\sigma^2_{R_mE} = 2$.



(a) $C_{th} = 0.5$ bps/Hz



(b) $C_{th} = 1.0$ bps/Hz

Figure 3.8. Secrecy outage probability versus average SNR, $\sigma_{DE}^2 = 2$ and $\sigma_{SE}^2 = 0.5$.

3.4.1 Multiple Antenna Eavesdropper

Consider a two-hop AF relay network with a source, M relays, a destination, and an eavesdropper. Assume that the eavesdropper has N antennas, while all other nodes have single antenna, respectively. All other parameters are same as previous ones.

Fig. 3.9 shows the secrecy performances versus various values of N with $C_t h = 1$ bps/Hz. It is shown that the proposed scheme for the network with the proposed technique provides lower SOP than a conventional JPA scheme for the network with a conventional technique even when the eavesdropper has 4 antennas. It is shown that the secrecy outage probability decreases as the number of antennas at the eavesdropper increases in all schemes.

3.5 Extension to Multiple Relay Selection

In the proposed power allocation and relay selection scheme, single best relay is selected to forwards the signal. As a natural extension, if we utilizes multiple relays with power allocation to forwards the signal, we achieve lower secrecy outage probability of the network.

Let $\mathbf{P} = \left(P_S^{(1)}, P_D^{(1)}, P_S^{(2)}, P_{R_1}^{(2)}, \cdots, P_{R_M}^{(2)}\right)$ denote a $M+3$-tuple of transmit powers. If we determine this $\mathbf{P}$, all relays which assigned non-zero transmit power are the selected relays, and these relays do a cooperative beamforming, i.e., the i-th selected relay, $i \in \mathbf{M}$, multiplies its received signal by a weight β_{R_i} and then re-transmits its obtained signal. Different to the single relay selection, joint power allocation and

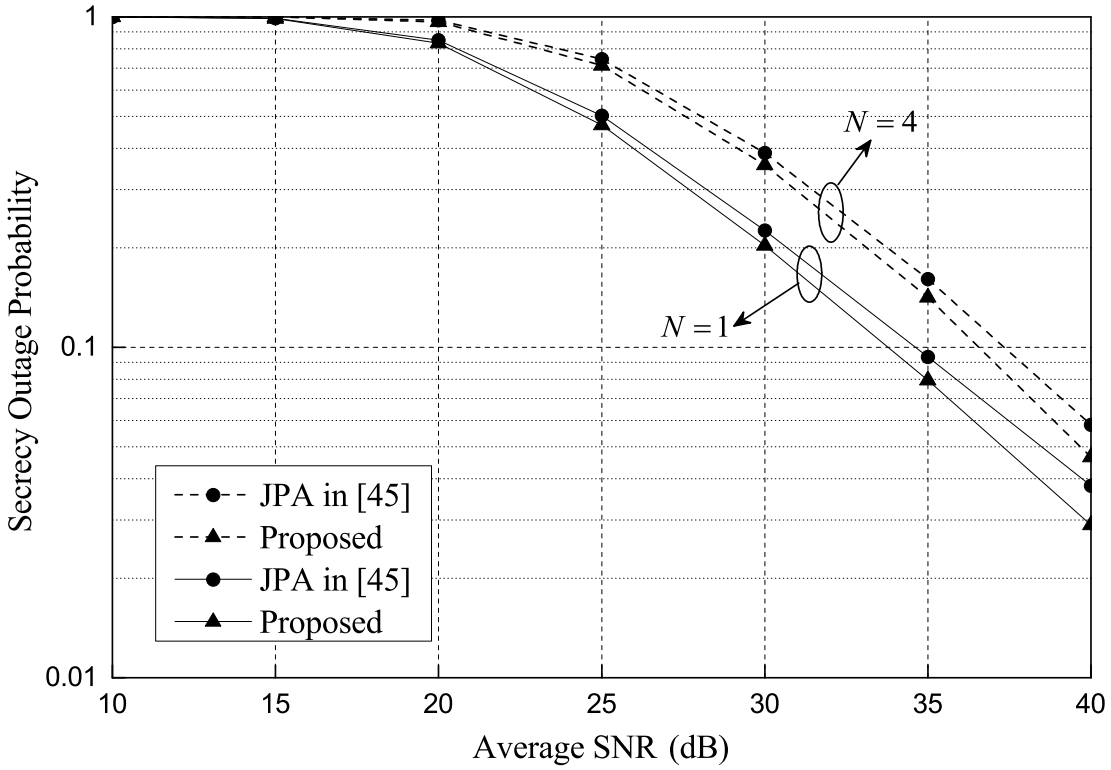


Figure 3.9. Secrecy outage probability for different number of antennas at the eavesdropper, N, with $C_{th} = 1$ bps/Hz.

relay selection scheme is reformulated as

$$\mathbf{P}^* = \arg\min p_{out} \tag{3.34}$$

subject to

$$P_S^{(1)} + P_D^{(1)} + P_S^{(2)} + \sum_{m=1}^{M} P_{R_m}^{(2)} = P_{tot}, \tag{3.35}$$

It is shown that this problem is non-convex. Solving this problem is an extension of our works, which will be briefly mentioned in future works.

3.6 Summary

In this chapter, we propose a joint power allocation and relay selection scheme for an AF relay network with multiple relays where the destination and source transmit jamming signals in phase 1 and 2, respectively. The SOP of the network is derived when the destination knows the exact coefficients of the main channels as well as the variances of the coefficients of the eavesdropper channels. We formulate a joint power allocation and relay selection problem to minimize the SOP. By using the primal decomposition method, we divide this problem into a master problem and a subproblem each of which solution is obtained by one-dimensional line search. Simulation results show that the proposed joint power allocation and relay selection scheme provides lower SOP than the conventional JPA scheme as well as the scheme without jamming.

Chapter 4

Conclusion

4.1 Summary

In this dissertation, we have investigated the physical layer security and cooperative jamming in two-hop relay network with single relay and multiple relays.

In Chapter 1, we introduce the basic concept, history, and related works of the physical layer security and especially, cooperative jamming. In addition, we describe the outline of this dissertation and present the notation, abbreviations, and functions used in this dissertation.

In Chapter 2, we propose a source power allocation problem for a two-hop relay network with single AF relay and an eavesdropper. Cooperative jamming is utilized in which a destination and source transmit jamming signals. Depends on the available CSI, secrecy rate and secrecy outage probability are optimized with source power allocation. In simulation results, it is shown that the proposed source power allocation

scheme achieves higher secrecy rate and lower secrecy outage probability than fixed power allocation schemes with various channel conditions.

In Chapter 3, we propose a power allocation and relay selection scheme for a two-hop relay network with multiple AF relays and an eavesdropper. Cooperative jamming is also utilized in which a destination and source transmit jamming signals. In the network, secrecy outage probability is analyzed in closed form. We formulate a power allocation and relay selection problem to minimize the secrecy outage probability with two different power constraints. In numerical results, it is shown that the proposed scheme achieves lower secrecy outage probability than the conventional jamming power allocation scheme as well as without jamming scheme.

4.2 Future Works

The enormous potential of cooperative jamming technique for future 5G wireless communications has been studied in extensive literatures. However, there are still some research topics on this technique which are important but have not been investigated yet.

In this dissertation, only one eavesdropper with single antenna is considered in both Chapter 2 and 3. As a natural extension, possible future works on this topic include:

1. A multiple antenna eavesdropper with beamforming

2. Multiple eavesdroppers cooperating each other

Considering these cases, new optimization and allocation needs to be studied to deal with these new types of eavesdropper(s). In Chapter 3, we propose single relay selection scheme with power allocation. As a natural extension, multiple relay could be selected, which will cause more complex problem to solve.

Since the secure communication could be applied in various wireless communication scenarios, more works on cooperative jamming technique are still challenging for various communication scenarios. For instance, energy harvesting, which gains an increasing attention with the concept of green communiation, is a good scenario to apply the cooperative jamming. For the wireless power transfer in energy harvesting, the jamming signal is also considered as the power transferring signal, and vice versa. The future works on this topic include:

1. Wireless energy harvesting from the jamming signal

2. Cooperative jamming with an energy harvesting relay

3. Jamming signal transmission from the energy harvesting jammer

Appendix A

Obtainment of Optimal Values of α in R_1 and R_2

In R_1, the optimal source power allocation problem is formulated as

$$\alpha_{opt}^{(1)} = \arg\max_{\alpha \in R_1} \left\{ \frac{1}{2}\log_2(1+\gamma_d) - \frac{1}{2}\log_2(1+\gamma_e^{(1)}) \right\}. \tag{A.1}$$

Due to the monotonicity of the log function, (A.1) is simplified as

$$\alpha_{opt}^{(1)} = \arg\max_{\alpha \in R_1} \frac{1+\gamma_d}{1+\gamma_e^{(1)}} \tag{A.2}$$

For convenience, define

$$K_1(\alpha) \triangleq \frac{1+\gamma_d}{1+\gamma_e^{(1)}} = \frac{1+\frac{\alpha\gamma_{sr}\gamma_{rd}}{\alpha\gamma_{sr}+2\gamma_{rd}+1}}{1+\frac{\alpha\gamma_{se}}{\gamma_{de}+1}} \tag{A.3}$$

The first order derivative of $K_1(\alpha)$ with respective to α is given by

$$\frac{\partial K_1(\alpha)}{\partial \alpha} = \frac{(\gamma_{de}+1)c(\alpha)}{(\alpha\gamma_{se}+\gamma_{de}+1)^2(\alpha\gamma_{sr}+2\gamma_{rd}+1)^2} \tag{A.4}$$

where

$$\begin{aligned} c(\alpha) = &-\gamma_{se}\gamma_{sr}^2(\gamma_{rd}+1)\alpha^2 - 2\gamma_{se}\gamma_{sr}(2\gamma_{rd}+1)\alpha \\ &+ (2\gamma_{rd}+1)\left\{(\gamma_{de}+1)\gamma_{sr}\gamma_{rd} - \gamma_{se}(2\gamma_{rd}+1)\right\}. \end{aligned} \tag{A.5}$$

Let S_1 denote the set of the solutions of $c(\alpha) = 0$. Among elements of S_1, $\alpha_{opt}^{(1)}$ is selected such that $K_1(\alpha)$ is maximized.

Similarly, in R_2, the optimal source power allocation problem is formulated as

$$\alpha_{opt}^{(2)} = \arg\max_{\alpha\in R_2}\left\{\frac{1}{2}\log_2(1+\gamma_d) - \frac{1}{2}\log_2(1+\gamma_e^{(2)})\right\}. \tag{A.6}$$

For convenience, define

$$K_2(\alpha) \triangleq \frac{1}{2}\log_2(1+\gamma_d) - \frac{1}{2}\log_2(1+\gamma_e^{(2)}). \tag{A.7}$$

The first order derivative of $K_2(\alpha)$ with respective to α is given by

$$\frac{\partial K_2(\alpha)}{\partial \alpha} = \frac{1}{2\ln 2}\left\{\frac{\gamma_{sr}\gamma_{rd}(\gamma_{rd}+1)}{A(\alpha)\left(A(\alpha)+\alpha\gamma_{sr}\gamma_{rd}\right)} - \frac{\gamma_{sr}\gamma_{re}\left(\alpha^2\gamma_{sr}\gamma_{se}+(\gamma_{rd}+1)(\gamma_{se}+\gamma_{re}+1)\right)}{B(\alpha)\left(B(\alpha)+\alpha\gamma_{sr}\gamma_{re}\right)}\right\} \tag{A.8}$$

where

$$A(\alpha) = \alpha\gamma_{sr} + 2\gamma_{rd} + 1 \tag{A.9}$$

and

$$B(\alpha) = \gamma_{re}(\gamma_{rd}+1) + \left\{(1-\alpha)\gamma_{se}+1\right\}\left(\alpha\gamma_{sr}+\gamma_{rd}+1\right). \tag{A.10}$$

Let S_2 denote the set of the solutions of $\frac{\partial K_2(\alpha)}{\partial \alpha} = 0$. Among elements of S_2, $\alpha_{opt}^{(2)}$ is selected such that $K_2(\alpha)$ is maximized.

Bibliography

[1] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[2] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, July 1985.

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

[4] A. B. Carleial and M. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Inf. Theory*, vol. 23, no. 5, pp. 625–627, May 1977.

[5] I. Csiszar and J. Korner, "Broadcast channel swith confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[8] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[9] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[10] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[11] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, June 2013.

[12] P.-S. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[13] 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. 2735–2751, June 2008.

[14] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[15] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[16] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, June 2013.

[17] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[18] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, June 2011.

[19] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to ehhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[20] M. Dehghan, D. L. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3025–3029, Sep. 2012.

[21] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[22] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[23] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[24] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[25] 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.

[26] J. 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.

[27] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[28] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[29] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[30] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for WANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1117–1128, Apr. 2015.

[31] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: to relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[32] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic achivable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2537–2551, Apr. 2016.

[33] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *Proc. IEEE ICC 2011*, Kyoto, Japan, June 2011.

[34] Y. Liu, J. Li, A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[35] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7274–7284, Sep. 2016.

[36] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[37] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.

[38] D. Lee and J. H. Lee, "Outage probability for dual-hop relaying systems with multiple interferers over Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 333–338, Jan. 2011.

[39] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Nov. 2009.

[40] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, July 2012.

[41] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC 2005-Fall*, Dallas, TX, USA, Sep. 2005.

[42] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[43] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[44] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: a case for cooperative jamming," in *Proc. IEEE GLOBECOM 2008*, New Orleans, LA, USA, Dec. 2008.

[45] K. H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[46] M. 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.

[47] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[48] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE ISIT 2007*, Nice, France, June 2007.

[49] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Proc. 2009 ACSSC*, Pacific Grove, CA, USA, Nov. 2009.

[50] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun. Mag.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[51] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[52] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. CISS 2010*, Princeton, NJ, USA, Mar. 2010.

[53] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[54] J. Chen, R. Zhang, L. Song, Z. Han, B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[55] Y. Zou, X. Wang, W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[56] 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.

[57] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[58] D. P. Palomar and M. Chiang, "A tutorial on decomposition methods for network utility maximization," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1439–1451, Aug. 2006.

Korean Abstract

물리 계층 보안은 무선통신의 보안에 대한 취약점과 암호화의 복잡성이라는 특징으로 인하여, 5세대(5G) 이동통신을 위한 핵심 기술로 간주되고 있다. 물리 계층 보안은 무선 채널의 물리적 특성을 이용하여 보안 통신을 가능하게 한다. 협력 재밍(cooperative jamming)은 물리 계층 보안에서의 보안 성능을 향상시키는 효과적인 기술로, 협력 노드가 재밍 신호를 전송함으로써 도청자를 방해하고, 보안을 달성한다. 그러나, 이러한 재밍 신호는 도청자 뿐 아니라 수신단 역시 방해하게 되므로 과도한 재밍 신호 전송은 보안 성능 향상에 지장을 주고 전력을 낭비하게 된다. 따라서 보안 성능을 향상시키기 위해서는 재밍 신호의 전력 할당 및 최적화를 하는 것이 필수적이다.

본 논문에서의 두 가지 주요한 연구 결과는 다음과 같다. 첫째, 하나의 송신단, 증폭 후 재전송 중계기, 수신단 및 도청자가 존재하는 중계 네트워크를 분석한다. 이 때 수신단 및 송신단이 협력 재밍을 통해 각각 첫 번째 및 두 번째 페이즈에서 재밍 신호를 전송하도록 한다. 수신단이 첫 번째 페이즈에 전송한 재밍 신호는 중계기를 통해 증폭되지만 수신단이 제거할 수 있으며, 송신단의 재밍 신호는 송신단과 수신단 사이의 채널이 약하기 때문에 수신단에 미치지 못한다. 이 때 본 네트워크에서 네트워크의 보안 전송률(secrecy rate) 및 보안 불능 확률(secrecy outage probability)을 향상시키는

송신단의 각 페이즈 별 전송 전력을 송신단이 가진 채널 정보를 통해 최적화한다. 모의 실험을 통해 제안한 전력 할당 기법이 다른 고정 전력 할당 기법에 비해 높은 보안 전송률과 낮은 보안 불능 확률을 달성함을 확인한다.

둘째, 하나의 송신단, 다수의 증폭 후 재전송 중계기들, 하나의 수신단 및 도청자가 존재하는 중계 네트워크를 분석한다. 다수의 중계기 중 하나의 중계기가 선택되어 신호를 전송하게 되며, 협력 재밍을 통해 수신단 및 송신단이 재밍 신호를 전송한다. 이 때 네트워크의 보안 불능 확률을 최소화하기 위한 중계기 선택 및 전력 할당 기법을 다양한 전력 제한에 맞게 분석한다. 네트워크 전체 전력이 제한된 경우에서는 중계기 선택 및 전력 할당 문제를 풀기 위해 두 개의 부문제(subproblem) 로 분할한다. 모의 실험을 통해 제안한 기법이 기존의 기법 및 재밍 신호를 전송하지 않는 기법에 비해 낮은 보안 불능 확률을 달성함을 확인한다.

주요어: 물리 계층 보안, 협력 재밍, 보안 전송률, 보안 불능 확률,
전력 할당, 중계기 선택

학번: 2013-20895