Ph.D. DISSERTATION

# Study on Physical-layer Security for Next-generation Communication Systems

## 차세대 통신 시스템을 위한 물리계층보안 연구

BY

YOON YOUNG-JUN

AUGUST 2023

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

Ph.D. DISSERTATION

# Study on Physical-layer Security for Next-generation Communication Systems

## 차세대 통신 시스템을 위한 물리계층보안 연구

BY

YOON YOUNG-JUN

AUGUST 2023

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

# Study on Physical-layer Security for Next-generation Communication Systems

차세대 통신 시스템을 위한 물리계층보안 연구

지도교수 김 성 철
이 논문을 공학박사 학위논문으로 제출함

2023년 8월

서울대학교 대학원

전기·정보공학부

윤 영 준

윤영준의 공학박사 학위 논문을 인준함

2023년 8월

| | | |
|---|---|---|
| 위 원 장: | 심 병 효 | (인) |
| 부위원장: | 김 성 철 | (인) |
| 위 원: | 최 완 | (인) |
| 위 원: | 이 종 호 | (인) |
| 위 원: | 김 용 화 | (인) |

# Abstract

With the emergence of infrastructure-free communication networks such as Internet of Things (IoT), the scale of a communication network grows increasingly due to its high connectivity. However, as the number of users within the network is larger, the probability that a security threat occurs is also higher. Thus, the confidential communication is an important issue to realize the massive networks such as smart factory, smart city, and smart grid. In response to this, on the dissertation, I study three subjects about securing confidentiality of those massive networks.

For the first subject, I study the physical-layer security (PLS) in the massive network. Particularly, the network includes the nodes assumed as a small device equipped with a single antenna and accordingly, it is very vulnerable to wiretapping due to the nature of omni-directivity from the single antenna. To obtain security, I propose the adaptive relay selection with cooperative jamming method for the network. In addition, I present jointly the optimal relay selection and the optimal power scheme for the proposed method.

In the second subject, I study the proactive eavesdropping method, can cope with a new kind of the security threat that occurs in the infrastructure-free network. I consider a general infrastructure-free communication network where the monitor node operates independently from other nodes. Moreover, the adaptive full-duplex jamming-helping method, in which the monitor node can select its own operation mode adaptively while eavesdropping the suspicious communication link, is proposed. The optimal power scheme of the monitor node for the proposed method is also studied together.

In succession to the second subject, for the three subject, I consider the negative effect of the imperfect self-interference cancellation problem in the full-duplex approach. To avoid this negative effect, I propose the proactive eavesdropping method using a half-duplex dual monitor node and the optimal power scheme for the proposed

method. Finally, through numerical analysis, it is verified that the proposed method with the optimal power scheme for the proposed can deal with effectively the imperfect self-interference cancellation problem.

**keywords**: Infrastructure-free networks, massive networks, optimal power scheme, physical-layer security, proactive Eavesdropping

**student number**: 2015-20953

# Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

With the development of ubiquitous systems such as Internet of Things (IoT), recent wireless communication systems are expected to build more accessible and user-friendly communication networks. Accordingly, it is no longer unusual that one device is connected to other numerous devices such as mobile, electronics, robots, vehicle and even unmanned aerial vehicle (UAV). In other words, massive users have been became a major characteristics of wireless communication systems. The massive network is regarded as a key role to realize many future-oriented applications such as health management, traffic monitoring, smart cities, smart farms, smart grids and so on. However, as the scale of a network become larger, there can be also larger exposures of the privacy or the confidential information within the network. Hence, a security is considered as a critical issue in the massive network.

In order to obtain the security, conventional communication systems have utilized the cryptography secure method [1] in which the transmitter and the receiver share a common secret key. However, it requires computations proportional to the number of users within the network. Moreover, the secret key should have higher computational complexity than the computation power of wiretappers to obtain security performance. For these reasons, the cryptography secure method is not suitable for the massive network, particularly, the network including many small devices which is not capable of

managing high computational complexity. As an alternative, the physical layer security (PLS), which does not require the secret key to users and its security performance does not depends on computation ability of wiretappers, has attracted attentions increasingly as a promising secure method. In response to this, on this dissertation, I deal with the PLS in the massive network as the first subject.

Especially, for the first subject, I consider a multi-node DF relay network where each node is assumed as a small device equipped with a single antenna. Since the device with the single antenna has no choice but to emit the signal toward omni-direction, the considered network is very vulnerable to wiretapping. To enhance the security performance, I propose an adaptive relay selection with cooperative jamming method for the network. Moreover, multi-carrier communication system such as orthogonal frequency division multiplexing (OFDM) is considered as a signal transmission method. I also present the optimization process to find an optimal power allocation scheme for the proposed method. In that process, it is shown that finding the optimal power allocation scheme is not straightforward. Then, as an alternative, I provide a sub-optimal power allocation scheme of which performance becomes almost identical to that of the optimal power allocation scheme as the number of sub-carriers goes to infinity. Nevertheless, it is verified that finding the sub-optimal power allocation scheme still requires the huge computations which a general system cannot afford. Hence, I also present another sub-optimal power allocation scheme to reduce the required computations. Finally, through numerical analysis, the security performance of the proposed method using the sub-optimal power allocation scheme with the reduced computation is validated.

Infrastructure-free communication networks also have been attractive as a promising technology since it can make coverage of a communication network larger at low cost. However, the infrastructure-free communication networks are highly vulnerable to security threats by malicious users who want to use those networks for harmful purposes [2]. For instance, the malicious user can actively exploit communication

links of the networks to commit crimes or terror. Unfortunately, conventional secure methods such as the cryptography or the PLS are not suitable for this kind of security attacks since they are mainly focused on blocking eavesdropping of illegitimate users. Accordingly, in order to prevent those security attacks, a need for new security approaches to constantly monitor and intervene in the communication networks increasingly grows. In response to this, the method, which is called proactive eavesdropping, has been researched in recent years. In the proactive eavesdropping method, the legitimate 'eavesdropper' is introduced to monitor the suspicious communication link. On this dissertation, I also address the proactive eavesdropping method for the infrastructure-free communication networks as the second subject.

For the second subject, I consider a general infrastructure-free communication network where the monitor node of the legitimate eavesdropper operates independently with other nodes. Moreover, to enhance the proactive eavesdropping performance, I propose the adaptive full-duplex jamming-helping method in which the legitimate eavesdropper node can select its own operation mode adaptively while eavesdropping the suspicious communication link. With the proposed method, the optimal power scheme for maximizing an eavesdropping rate is presented together. I also verify that the performance of the proposed method with the optimal power scheme is superior than that of conventional methods. Furthermore, in succession to the second subject, I consider a negative effect of the imperfect self-interference cancellation problem in full-duplex approach. To avoid this negative effect, I propose the proactive eavesdropping method using a half-duplex dual monitor node. Similarly to other subjects, the optimization process of the jamming power for the proposed method is provided. Finally, via the numerical analysis, it is verified that the proposed method outperforms the conventional method which uses the full-duplex monitor with the imperfect self-interference problem.

The remainder of this dissertation is organized as follows. Chapter 2 address the first subject, which is about the PLS in multi-carrier and multi-node DF relay networks.

In Chapter 3 and Chapter 4, the second subject and the third subject about the proactive eavesdropping method are discussed, respectively. Finally, I conclude the dissertation in Chapter 5.

# Chapter 2

# Efficient Power Allocation for Physical-Layer Security with Adaptive Transmission in Multi-Carrier and Multi-Node DF Relay Networks

## 2.1 Motivation

Physical layer security (PLS), which does not require secret key management, has attracted attention increasingly as a promising secure technique in the next generation communication networks[3]. The PLS is first introduced by Wyner[4, 5] and its basic concept is exploiting the physical characteristics of communication medium, which is so called the communication channel, to improve confidentiality of communications. In [4, 5], Wyner showed that the perfect security between the transmit node and the desirable receive node can be established as much as the achievable secrecy rate, which is defined as the rate at which information is perfect-confidentially delivered into a destination node.

In the PLS, a security performance fluctuates severely depending on channel states of the communication network. For instance, basic concept of the conventional PLS can obtain security only if the channel between the transmit node and the desirable receive node is better than that between the transmit node and the undesirable receive

node. However, due to a randomness nature of the wireless communication channel, there is no guarantee that the channel from the transmit node to the desirable node is frequently better than to the undesirable node. To overcome this randomness of the wireless channel, the PLS has been conducted together with techniques handling channel states such as cooperative transmission methods[6, 7, 8, 9]. In the cooperative transmission method, intermediate nodes in the network help the source node to transmit the secret signal confidentially into the desirable receive node by relaying the signal into the desirable node (cooperative relay) or jamming the undesirable node (cooperative jamming). By doing so, the intermediate nodes give their network more chances that the channel from the source node to the desirable node is better than that from the source node to the undesirable node. Moreover, there is generally more potential of performance improvements in the PLS as the number of intermediate nodes in the network increases gradually. For these reasons, the PLS is recognized as the promising security technique for the next generation multi-node communication network.

With cooperative transmission methods, there have been many PLS studies in multi-node networks [6, 7, 8, 9]. Dong et al.[6] studied PLS with three cooperative methods such as Decode-and-Forward (DF) relay, Amplify-and-Forward (AF) relay, and cooperative jamming (CJ). They found optimal relay weight of each cooperative method in the multi-node network in which multiple intermediate nodes are available for relays or jammers. Li et al.[7] also investigated PLS with cooperative DF relay and CJ methods in the multi-node network and proposed the sub-optimal solution to reduce difficulty of the optimization problem. In [8], Zheng et al. proposed the optimal CJ beamforming solution in the network where relay nodes are distributed spatially. Lee[9] considered the PLS in the wireless multi-hop multi-relay network and proposed the optimal power allocation into intermediate nodes at each-hop to maximize the achievable secrecy rate.

In recent years, a number of PLS researches with joint cooperative relay and co-

operative jamming, which means that the cooperative relay and cooperative jamming are both conducted in one multi-node network, were studied[10, 11, 12, 13, 14, 15]. In [10], Guo et al. considered the joint cooperative beamforming and cooperative jamming (JCBC) method in which a part of intermediate nodes in the multi-node network are used as relays and remains of those are utilized as jammers simultaneously. They derived the closed-form optimal power allocation for each relay set and determined the ultimate optimal power allocation by comparing the secrecy rate results for all possible relay sets. Jia et al.[11] proposed the novel relay selection method with artificial noise in the cognitive multi-node network. In their proposed method, one of intermediate nodes is selected for cooperative relay and the remains of intermediate nodes are utilized as cooperative jammers. In that system, they derived the optimal relay selection to maximize secrecy outage probability. Chen et al.[12] studied a joint cooperative relay and jammer selection method among a number of intermediate nodes in a two-way relay networks for enhancing security performance. Wang et al.[13] explored the hybrid cooperative beamforming and jamming method in which some intermediate nodes help to relay the signal into the desirable node and the remaining nodes jam the undesirable node at practical constraints. In [14], Feng et al. considered the novel joint user and relay selection method with the jamming signal in order to minimize the secrecy outage probability and maximize signal-to-interference-to-noise ratio (SINR) simultaneously. Wang et al.[15] studied hybrid opportunistic relaying and jamming method for the PLS based on practical assumption that only the channel distribution information of the eavesdropper user is known.

In the wireless communications, a multi-carrier system such as orthogonal frequency division multiplexing (OFDM) is a important technique since it can provide high data rate and reliability to the communication network. Thus, there have been some researches about the PLS with the multi-carrier system[16, 17, 18]. Jeong et al.[16] studied power allocation for maximizing sum secrecy rate in the multi-carrier DF relay network. They proposed three transmission modes which can be switched de-

pending on channel states at each sub-carrier and derived optimal power allocation for that system. In addition, they also suggested the sub-optimal power allocation whose performance is very close to that of the optimal power allocation but the required computation is relatively low. Bai et al.[17] proposed the quality-of-service (QoS) driven power allocation policy in the multi-carrier full-duplex (FD) relay communication network. In particular, they considered the imperfect CSI for deriving the proposed policy and showed that it is very robust to the channel uncertainty. In [18], Nawaz et al. presented the joint resource optimization framework for the optimal power loading and the efficient sub-carrier assignment in dual-hop multi-carrier DF relay networks. In addition, through simulation results, they showed that the optimization obtained from the framework is considerably better than other benchmark frameworks such as optimal power loading with random sub-carrier assignment and equal power allocation with efficient sub-carrier assignment.

However, to the best of my knowledge, there is still no study of the PLS for the multi-carrier and multi-node communication network with the joint cooperative relay and jamming. Moreover, in this chapter, I consider the adaptive cooperative transmission method in which all intermediate nodes change their purpose of use such as the cooperative relay and the cooperative jamming flexibly. With the adaptive cooperative transmission method, I jointly derive optimal power allocation of each sub-carrier and the best transmission strategy of each sub-carrier to maximize the sum secrecy rate, which is defined as a sum of achievable secrecy rates of all sub-carriers. The main contributions of this chapter can be summarized as follows;

1) I derive the optimal power distribution for each transmission strategy on the single sub-carrier and, using this, establish the optimization problem over all sub-carriers to maximize the sum secrecy rate.

2) I show that the optimization problem over all sub-carriers is not straightforward to be solved and, as the alternative, find the sub-optimal power allocation whose the security performance is asymptotically optimal when the number of the sub-

carriers or the intermediate nodes goes to a infinity.

3) I propose the efficient power allocation scheme which can derived by very little computation compared to the computation required for the sub-optimal power allocation. Furthermore, I slightly enhance the performance of the proposed power allocation by mitigating the approximation error in the process.

4) Through various numerical results, I prove that the proposed power allocation scheme is superior in the security performance than other benchmark power allocation schemes such as a random power allocation, a uniform power allocation and so on.

## 2.2 System Model

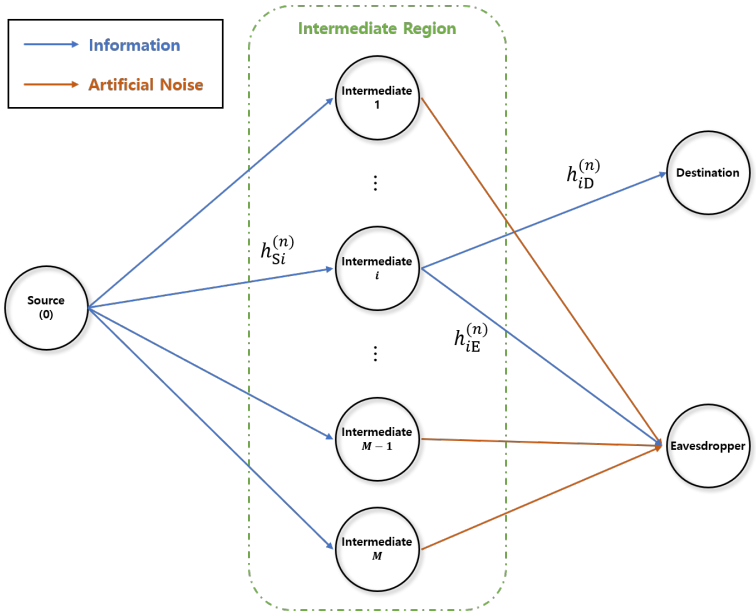



Figure 2.1: Description of the two-hop DF relay network topology

### 2.2.1 Network Topology

I consider the multi-node multi-carrier network where a source node, $M$ intermediate nodes, a destination node (desirable node) and a eavesdropper node (undesirable node) exist as shown in Fig.2.1. A signal transmission is conducted using the multi-carrier communications based on OFDM, which is the most commonly used in the communication system. In the multi-carrier system, there are a total of $N$ sub-carriers. All nodes are assumed to be small device. That is, they are equipped with only a single omni-directional antenna. Moreover, in our system model, the eavesdropper node is assumed to be a legitimate user in the network, but a low-level user who cannot access to the confidential signal. For convenience, I assign the index number 0 to the source node and the index number from 1 to $M$ to intermediate nodes. In Fig.2.1,

$h_{0j}^{(n)}$ denotes a channel coefficient of the link between the source node and $j$th intermediate node on the $n$th sub-carrier and $h_{i\mathrm{D}}^{(n)}$ and $h_{i\mathrm{E}}^{(n)}$ represents channel coefficients of the link between the $i$th node and the destination node, and between the $i$th node and the eavesdropper node, respectively, on the $n$th sub-carrier. Moreover, all links in the network are assumed to contain the additive white Gaussian noise (AWGN) with zero-mean and variance $\sigma^2$.

Table 2.1: Cooperative Transmission Process

| Phase | Source node | Relay node | Jamming node |
|---|---|---|---|
| 1 | Transmit | Receive / Decode | Rest |
| 2 | Rest | Forward | Jamming |

### 2.2.2 Adaptive Cooperative Transmission

In the cooperative transmission, only one among intermediate nodes performs a role as the relay node and help transmit the confidential message to the destination node successfully. Simultaneously, all remaining intermediate nodes do jamming the eavesdropper node using an artificial noise (AN), that is, they act as jamming nodes. At the relay node, the signal relaying is based on the DF relay method. The reason why I choose not multiple relay nodes but the single relay node is because it is generally best case in terms of the security performance to perform the signal relaying with the best one among relay nodes than together with multiple relay nodes for the DF relay method. The cooperative transmission method is conducted over two phases. This process is clearly described in Table 2.1. In the first phase, the source node transmits the confidential signal into intermediate nodes. At the same time, the intermediate node selected as the relay node receives and decodes the signal. In the second phase, the relay node forwards the re-encoded signal to the destination node and jamming nodes perform jamming by emitting AN into the network. On the one hand, the destination

node and the eavesdropper node both receive and try to decode the signal. All channel coefficients are assumed to be stationary during two phases, which it means that the time for the two phases is enough short relative to the channel coherence time. Furthermore, all channel state information are assumed to be known to the source node and all intermediate nodes. This is enough possible assumption in the situation that the eavesdropper node is actually another legitimate node of the network, but lower level node than the destination node.

Moreover, in the second phase, Zero-forcing (ZF) beamforming precoder is applied to the jamming nodes. ZF beamforming precoder is designed for the artificial noise not to interrupt the destination node. Thus, after applying ZF beamforming precoder to jamming nodes, the emitted AN is null-steered toward the destination node. That is, the AN does not have a effect on the destination node and affects as a noise at the eavesdropper node. Additionally, I assume that there are no direct links from the source node to the destination node and the eavesdropper node. It is because the channel state of the direct link are relatively harsher than channel states of other links. This implies that the strength of the signal transmitted from the source node can be ignored since it is very weak in comparison with that of the signal transmitted from the relay node. To sum up these assumptions, the received signal at the $m$th intermediate node on the $n$th sub-carrier in the first phase can be represented as

$$r_m^{(n)} = h_{\mathrm{S}m}^{(n)} \sqrt{p_{\mathrm{T}}^{(n)}} s^{(n)} + g, \tag{2.1}$$

where $r_m^{(n)}$ is the received signal at the $m$th intermediate node on the $n$th sub-carrier, $p_{\mathrm{T}}^{(n)}$ is the transmit power which the source node spends for transmitting the confidential signal, $s^{(n)}$ is the normalized confidential signal, and $g$ is AWGN with zero-mean and variance $\sigma^2$ In the case that the $m$th intermediate node is selected as the relay node, the received signal at the destination node and the eavesdropper node on the $n$th sub-carrier in the second phase can be given by

$$r_{\mathrm{D}_m}^{(n)} = h_{m\mathrm{D}}^{(n)} \sqrt{p_{\mathrm{R}}^{(n)}} s^{(n)} + g, \tag{2.2}$$

$$r_{\mathrm{E}_m}^{(n)} = h_{m\mathrm{E}}^{(n)} \sqrt{p_{\mathrm{R}}^{(n)}} s^{(n)} + \mathbf{h}_m^{(n)\mathrm{T}} \mathbf{w}_m^{(n)} \sqrt{p_{\mathrm{J}}^{(n)}} a^{(n)} + g, \tag{2.3}$$

where $r_{\mathrm{D}_m}^{(n)}$ and $r_{\mathrm{E}_m}^{(n)}$ are the received signals at the destination node and the eavesdropper node with aid of the relay node on the $n$th sub-carrier, respectively, $p_{\mathrm{R}}^{(n)}$ is the relay power which the relay node spends to forward the confidential signal, $p_{\mathrm{J}}^{(n)}$ is the jamming power which jamming nodes spend for transmitting AN, $a^{(n)}$ is the normalized AN, respectively, on the $n$th sub-carrier, and $(\cdot)^T$ is the transpose operator. $\mathbf{h}_m^{(n)}$ is ($M$-1) by 1 column vector whose elements are the channel coefficients between the jamming nodes and the eavesdropper node when the $m$th intermediate node is selected as the relay node on the $n$th sub-carrier and is given by

$$\mathbf{h}_m^{(n)} = \left[ h_{1\mathrm{E}}^{(n)}, \cdots, h_{(m-1)\mathrm{E}}^{(n)}, \; h_{(m+1)\mathrm{E}}^{(n)}, \cdots, h_{M\mathrm{E}}^{(n)} \right]^{\mathrm{T}}. \tag{2.4}$$

$\mathbf{w}_m^{(n)}$ is ($M$-1) by 1 column vector whose elements are the normalized ZF beamforming weights for jamming nodes when the $m$th intermediate node is selected as the relay node on the $n$th sub-carrier and is given by

$$\mathbf{w}_m^{(n)} = \left[ w_1^{(n)}, \cdots, w_{(m-1)}^{(n)}, \; w_{(m+1)}^{(n)}, \cdots, w_M^{(n)} \right], \tag{2.5}$$

where $w_i^{(n)}$ is the normalized ZF beamforming weight for the $i$th intermediate node on the $n$th sub-carrier and $\mathbf{w}_m^{(n)}$ satisfies

$$\left| \mathbf{w}_m^{(n)} \right|^2 = 1$$

Since the number of selecting the one as the relay node among the intermediate nodes is $M$, there are a total of $M$ different possible cooperative transmission strategies on each sub-carrier. At each sub-carrier, the optimal cooperative transmission scheme varies depending on the channel states and the available power. In order to enhance the security performance of the network, I consider an adaptive cooperative transmission scheme in which the cooperative transmission scheme is adaptively determined responding with the given channel states and the given available power. In the adaptive transmission scheme, the process of selecting optimal one among possible cooperative transmission schemes is performed individually on each sub-carrier.

That is, the cooperative transmission schemes of the sub-carriers can be different with one another. Consequently, depending on the given channel states and total system power, the cooperative transmission schemes of all sub-carriers are individually and adaptively decided to maximize the sum secrecy rate together with the optimal power distribution and the optimal power allocation.

### 2.2.3 Secrecy Rate

The secrecy rate is a quantitative measure of how well information transmission is conducted confidentially. It is defined as the difference between two channel capacities at the destination node and the eavesdropper node[4]. The secrecy rate R is given by

$$\mathcal{R} = [\mathcal{C}_{\mathrm{D}} - \mathcal{C}_{\mathrm{E}}]^{+}, \tag{2.6}$$

where $\mathcal{C}_{\mathrm{D}}$ and $\mathcal{C}_{\mathrm{E}}$ are the channel capacities at the destination node and the eavesdropper node, respectively. In addition, $[z]^{+}$ is a function operator same as $\max(z, 0)$, which it implies that there is no security if the eavesdropper node can receive higher information quantity than the destination node.

In the case of the Gaussian channel, the channel capacity is simply represented as a function of the signal-to-noise ratio (SNR)[4]. Therefore, (2.6) can be transformed as

$$\mathcal{R} = \left[\log_2\left(\frac{1+\mathcal{S}_{\mathrm{D}}}{1+\mathcal{S}_{\mathrm{E}}}\right)\right]^{+}, \tag{2.7}$$

where $\mathcal{S}_{\mathrm{D}}$ and $\mathcal{S}_{\mathrm{E}}$ are SNRs at the destination node and the eavesdropper node, respectively. If the $m$th intermediate node is utilized as the relay node, from (2.2) and (2.3), the secrecy rate on the $n$th sub-carrier $\mathcal{R}_m^{(n)}$ is given by

$$\mathcal{R}_m^{(n)}\left(\mathbf{p}^{(n)}\right) = \left[\log_2 \frac{\left(1+\alpha_m^{(n)} p_{\mathrm{R}}^{(n)}\right)\left(1+\gamma_m^{(n)} p_{\mathrm{J}}^{(n)}\right)}{\left(1+\beta_m^{(n)} p_{\mathrm{R}}^{(n)}+\gamma_m^{(n)} p_{\mathrm{J}}^{(n)}\right)}\right]^{+}, \quad \text{for } m = 1, 2, \cdots, M, \tag{2.8}$$

where $\alpha_m^{(n)} := \frac{\left|h_{m\mathrm{D}}^{(n)}\right|^2}{\sigma^2}$, $\beta_m^{(n)} := \frac{\left|h_{m\mathrm{E}}^{(n)}\right|^2}{\sigma^2}$, $\gamma_m^{(n)} := \frac{\left|\mathbf{h}_m^{(n)\mathrm{T}}\mathbf{w}_m^{(n)}\right|^2}{\sigma^2}$, and $\mathbf{p}^{(n)}$ is the power distribution vector defined as

$$\mathbf{p}^{(n)} = \left[p_{\mathrm{T}}^{(n)}, p_{\mathrm{R}}^{(n)}, p_{\mathrm{J}}^{(n)}\right] \text{ for } n = 1, \cdots, N.$$

Furthermore, the sum secrecy rate, which is defined as the sum of secrecy rates of all sub-carriers, is given by

$$\mathcal{R} = \sum_{n=1}^{N} \max_{m=1,2,\cdots,M} \left\{ \mathcal{R}_m^{(n)} \left( \mathbf{p}^{(n)} \right) \right\}. \tag{2.9}$$

## 2.3 Optimal Power Distribution

In this section, I derive the optimal power distribution of the individual cooperative transmission strategy to maximize the secrecy rate when the channel states and the available power are given on each sub-carrier. In addition, using the derived optimal power distribution, the achievable secrecy rate of the individual cooperative transmission strategy is defined as the function of the available power given on the sub-carrier. The achievable secrecy rate is utilized in order to formulate the optimal power allocation problem over all sub-carriers in the next section. Without loss of generality, throughout this section, I assume that the $m$th intermediate node is selected as the relay node on the $n$th sub-carrier. That is, the derived optimal power distribution can be extended to other cooperative transmission strategies and other sub-carriers.

If I let $p^{(n)}$ denote the available power on the $n$th sub-carrier, the power distribution vector must satisfies the following inequality.

$$p_{\mathrm{T}}^{(n)} + p_{\mathrm{R}}^{(n)} + p_{\mathrm{J}}^{(n)} \leq p^{(n)}, \tag{2.10}$$

Since the power distribution vector is the non-negative vector, each component of that vector is constrained by the positive condition represented as

$$p_{\mathrm{T}}^{(n)} \geq 0,\ p_{\mathrm{R}}^{(n)} \geq 0,\ p_{\mathrm{J}}^{(n)} \geq 0, \tag{2.11}$$

respectively. Moreover, for the DF relay method, the relay network must satisfy the DF relay constraint [5], which is given by

$$\left| h_{\mathrm{S}m}^{(n)} \right|^2 p_{\mathrm{T}}^{(n)} \geq \left| h_{m\mathrm{D}}^{(n)} \right|^2 p_{\mathrm{R}}^{(n)}. \tag{2.12}$$

The DF relay constraint is necessary condition for the relay node to forward the confidential message correctly to the destination node. Accordingly, the feasible set of the power distribution vector is determined as the three-dimensional space formed by (2.10), (2.11) and (2.12).

On the one hand, the first-order derivative of (2.8) with respect to the relay power, $p_{\mathrm{R}}^{(n)}$, is drawn as

$$\frac{\partial \mathcal{R}_m^{(n)}}{\partial p_{\mathrm{R}}^{(n)}} = \frac{\alpha_m^{(n)} \left(1 + \gamma_m^{(n)} p_{\mathrm{J}}^{(n)}\right) - \beta_m^{(n)}}{\left(1 + \alpha_m^{(n)} p_{\mathrm{R}}^{(n)}\right)\left(1 + \beta_m^{(n)} p_{\mathrm{R}}^{(n)} + \gamma_m^{(n)} p_{\mathrm{J}}^{(n)}\right)}. \tag{2.13}$$

In (2.13), the denominator of the derivative has always positive value inside the feasible set of the power distribution. Thus, the sign of the derivative in (2.13) depends on only the channel states and the jamming power. If the differentiate value is negative at the given channel states despite the fully maximum jamming power, $\mathcal{R}_m^{(n)}$ is decided a strictly decreasing function along $p_{\mathrm{R}}^{(n)}$ and accordingly, the optimal relay power is determined to be zero. Furthermore, the secrecy rate corresponding to the zero relay power is always determined as zero. This implies that it is impossible to obtain the security of the confidential communication at all costs because the channel states are terribly bad. On the other hand, if the differentiate value is positive at the given channel states and the given jamming power, $\mathcal{R}_m^{(n)}$ is decided a strictly increasing function along $p_{\mathrm{R}}^{(n)}$. In this case, the more the relay power is, the higher the secrecy rate is. Thus, the best choice for the relay power is utilizing as much power as possible.

On the other hand, the first-order derivative of (2.8) with respect to the jamming power, $p_{\mathrm{J}}^{(n)}$, is given as

$$\frac{\partial \mathcal{R}_m^{(n)}}{\partial p_{\mathrm{J}}^{(n)}} = \frac{\gamma_m^{(n)} \beta_m^{(n)} p_{\mathrm{R}}^{(n)}}{\left(1 + \gamma_m^{(n)} p_{\mathrm{J}}^{(n)}\right)\left(1 + \beta_m^{(n)} p_{\mathrm{R}}^{(n)} + \gamma_m^{(n)} p_{\mathrm{J}}^{(n)}\right)}. \tag{2.14}$$

Similar to the former case, the denominator of the right-hand side in (2.14) is always positive inside the feasible set of the power distribution. Thus, the sign of the right-hand side in (2.14) depends on only the relay power. If the relay power is given as

zero, the differentiate value also becomes zero and accordingly, $\mathcal{R}_m^{(n)}$ is given as zero-constant along $p_{\mathrm{J}}^{(n)}$. In this case, the optimal jamming power is determined to be zero since the jamming power does not affect the secrecy rate. In contrast, if the relay power is given as a non-zero value, the differentiate value is positive and $\mathcal{R}_m^{(n)}$ is decided the strictly increasing function along $p_{\mathrm{J}}^{(n)}$. Therefore, in this situation, the best choice for the jamming power is utilizing as much power as possible.

From (2.13) and (2.14), I can know that it is best that the available power of the sub-carrier is wholly distributed for the relay and the jamming both unless the optimal power is zero. Therefore, in the case of the non-zero relay power, the optimal power distribution must satisfy the equation version of (2.11) which is given by

$$p_{\mathrm{T}}^{(n)} + p_{\mathrm{R}}^{(n)} + p_{\mathrm{J}}^{(n)} = p^{(n)}. \tag{2.15}$$

In addition, the transmit power actually is independent term with the secrecy rate and only acts as a limit boundary of the relay power under the DF relay constraint. That is, the transmit power does not affect the value of $\mathcal{R}_m^{(n)}$ unlike the relay power and the jamming power Therefore, the best choice for the transmit power is distributing as low power as possible in order to spend more power for the relay power and the jamming power. Consequently, the optimal transmit power is simply determined by the equation version of the DF relay constraint which given as

$$p_{\mathrm{T}}^{(n)} = \epsilon_m^{(n)} p_{\mathrm{R}}^{(n)}, \tag{2.16}$$

where $\epsilon_m^{(n)} := \frac{\left|h_{m\mathrm{D}}^{(n)}\right|^2}{\left|h_{\mathrm{S}m}^{(n)}\right|^2}$. By introducing (2.16) to (2.15), the optimal jamming power also can be drawn as the equation of the relay power which is given by

$$p_{\mathrm{J}}^{(n)} = p^{(n)} - \left(1 + \epsilon_m^{(n)}\right) p_{\mathrm{R}}^{(n)}. \tag{2.17}$$

Using (2.16) and (2.17), I can transform (2.8) to the function of only the relay power which is given by

$$\mathcal{R}_m^{(n)}\left(p_{\mathrm{R}}^{(n)}\right) = \left[\log_2 \frac{\left(1 + \alpha_m^{(n)} p_{\mathrm{R}}^{(n)}\right)\left(1 + \gamma_m^{(n)} p^{(n)} - \lambda_m^{(n)} p_{\mathrm{R}}^{(n)}\right)}{\left(1 + \gamma_m^{(n)} p^{(n)} + \left(\beta_m^{(n)} - \lambda_m^{(n)}\right) p_{\mathrm{R}}^{(n)}\right)}\right]^+, \tag{2.18}$$

where $\lambda_m^{(n)} := \gamma_m^{(n)} \left(1 + \epsilon_m^{(n)}\right)$. From the first-order derivative of (2.18) with respect to the relay power, the optimal relay power can be derived and it is given by

$$p_{\mathrm{R}}^{\star(n)}\left(p^{(n)}, \mathbf{c}_m^{(n)}\right) = \begin{cases} \min\left(f\left(p^{(n)}, \mathbf{c}_m^{(n)}\right), \frac{\gamma_m^{(n)}}{\lambda_m^{(n)}} p^{(n)}\right), & \text{if } \alpha_m^{(n)} > \beta_m^{(n)}, \\ f\left(p^{(n)}, \mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)} \leq \beta_m^{(n)}, \end{cases} \tag{2.19}$$

where $p_{\mathrm{R}}^{\star(n)}$ is the optimal relay power on the $n$th sub-carrier, $\mathbf{c}_m^{(n)}$ is the vector which is defined as

$$\mathbf{c}_m^{(n)} := \left[\alpha_m^{(n)}, \beta_m^{(n)}, \gamma_m^{(n)}, \lambda_m^{(n)}\right] \text{ for } m = 1, \cdots, M \text{ and } n = 1, \cdots, N,$$

and $f(\cdot)$ is the function defined as

$$f(x, \mathbf{c}) := \frac{1 + \gamma x}{\beta - \lambda} \left(\sqrt{\frac{\beta}{\lambda}\left(1 - \frac{\beta - \lambda}{\alpha(1 + \gamma x)}\right)} - 1\right),$$

where $\mathbf{c} := [\alpha, \beta, \gamma, \lambda]$. Considering the case in which the optimal relay power is determined to be zero together with (2.19), the optimal relay power is extended to

$$p_{\mathrm{R}}^{\star(n)}\left(p^{(n)}, \mathbf{c}_m^{(n)}\right) = \begin{cases} \frac{\gamma_m^{(n)}}{\lambda_m^{(n)}} p^{(n)}, & \text{if } \alpha_m^{(n)} > \beta_m^{(n)} \text{ and } 0 \leq p^{(n)} < p_{m,1}^{(n)}, \\ f\left(p^{(n)}, \mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)} > \beta_m^{(n)} \text{ and } p^{(n)} \geq p_{m,1}^{(n)}, \\ 0, & \text{if } \alpha_m^{(n)} \leq \beta_m^{(n)} \text{ and } 0 \leq p^{(n)} < p_{m,2}^{(n)}, \\ f\left(p^{(n)}, \mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)} \leq \beta_m^{(n)} \text{ and } p^{(n)} \geq p_{m,2}^{(n)}, \end{cases} \tag{2.20}$$

where $p_{m,1}^{(n)}$ and $p_{m,2}^{(n)}$ are defined by

$$p_{m,1}^{(n)} := \frac{-\lambda_m^{(n)} + \sqrt{\left\{\lambda_m^{(n)}\right\}^2 + 4\alpha_m^{(n)}\gamma_m^{(n)}\left(\frac{\alpha_m^{(n)}}{\beta_m^{(n)}} - 1\right)}}{2\alpha_m^{(n)}\gamma_m^{(n)}}, \quad \text{for } m = 1, \cdots, M,$$

$$p_{m,2}^{(n)} := \frac{\beta_m^{(n)} - \alpha_m^{(n)}}{\alpha_m^{(n)}\gamma_m^{(n)}}, \quad \text{for } m = 1, \cdots, M.$$

From (2.20), the optimal transmit power and the optimal jamming power are deter-

mined as

$$p_{\mathrm{T}}^{\star(n)}\left(p^{(n)},\mathbf{c}_m^{(n)}\right)=\begin{cases}\frac{\epsilon_m^{(n)}\gamma_m^{(n)}}{\lambda_m^{(n)}}p^{(n)}, & \text{if } \alpha_m^{(n)}>\beta_m^{(n)} \text{ and } 0\le p^{(n)}<p_{m,1}^{(n)},\\ \epsilon_m^{(n)}f\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}>\beta_m^{(n)} \text{ and } p^{(n)}\ge p_{m,1}^{(n)},\\ 0, & \text{if } \alpha_m^{(n)}\le\beta_m^{(n)} \text{ and } 0\le p^{(n)}<p_{m,2}^{(n)},\\ \epsilon_m^{(n)}f\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}\le\beta_m^{(n)} \text{ and } p^{(n)}\ge p_{m,2}^{(n)},\end{cases} \tag{2.21}$$

$$p_{\mathrm{J}}^{\star(n)}\left(p^{(n)},\mathbf{c}_m^{(n)}\right)=\begin{cases}0, & \text{if } \alpha_m^{(n)}>\beta_m^{(n)} \text{ and } 0\le p^{(n)}<p_{m,1}^{(n)},\\ p^{(n)}-\frac{\lambda_m^{(n)}}{\gamma_m^{(n)}}f\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}>\beta_m^{(n)} \text{ and } p^{(n)}\ge p_{m,1}^{(n)},\\ 0, & \text{if } \alpha_m^{(n)}\le\beta_m^{(n)} \text{ and } 0\le p^{(n)}<p_{m,2}^{(n)},\\ p^{(n)}-\frac{\lambda_m^{(n)}}{\gamma_m^{(n)}}f\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}\le\beta_m^{(n)} \text{ and } p^{(n)}\ge p_{m,2}^{(n)},\end{cases} \tag{2.22}$$

where $p_{\mathrm{T}}^{\star(n)}$ is the optimal transmit power and $p_{\mathrm{J}}^{\star(n)}$ is the optimal jamming power on the $n$th sub-carrier, respectively.

By applying the optimal power distribution vector to (2.8), I define the achievable secrecy rate of the individual cooperative transmission strategy on the $n$th sub-carrier

as a function of the available power of the $n$th sub-carrier which is given by

$$\mathcal{R}_m^{\star(n)}\left(p^{(n)}\right)=\begin{cases}\mathcal{R}_1\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}>\beta_m^{(n)} \text{ and } 0\le p^{(n)}<p_{m,1}^{(n)},\\ \mathcal{R}_2\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}>\beta_m^{(n)} \text{ and } p^{(n)}\ge p_{m,1}^{(n)},\\ 0, & \text{if } \alpha_m^{(n)}\le\beta_m^{(n)} \text{ and } 0\le p^{(n)}<p_{m,2}^{(n)},\\ \mathcal{R}_2\left(p^{(n)},\mathbf{c}_m^{(n)}\right), & \text{if } \alpha_m^{(n)}\le\beta_m^{(n)} \text{ and } p^{(n)}\ge p_{m,2}^{(n)},\end{cases} \quad \text{for } m=1,\cdots,M, \tag{2.23}$$

where $\mathcal{R}_m^{\star(n)}$ is the achievable secrecy rate function when the $m$th intermediate node is used as the relay node on the $n$th sub-carrier, and $\mathcal{R}_1(\cdot)$ and $\mathcal{R}_2(\cdot)$ are its partial functions which are defined as

$$\mathcal{R}_1(x,\mathbf{c}):=\log_2\left(\frac{\lambda+\alpha\gamma x}{\lambda+\beta\gamma x}\right),$$

$$\mathcal{R}_2(x,\mathbf{c}):=\log_2\left(1+\alpha\lambda\frac{\{f(x,\mathbf{c})\}^2}{1+\gamma x}\right).$$

In addition, the maximum achievable secrecy rate on the $n$th sub-carrier is given by

$$\mathcal{R}^{\star(n)}\left(p^{(n)}\right)=\max_{\{m=1,2,\cdots,M\}}\mathcal{R}_m^{\star(n)}\left(p^{(n)}\right). \tag{2.24}$$

## 2.4 Optimal Power Allocation

In this section, I jointly find the optimal power allocation into each sub-carrier and the optimal cooperative transmission strategy of each sub-carrier to maximize the sum secrecy rate. Using the maximum achievable secrecy rate of each sub-carrier derived in the previous section, the optimization problem for finding the optimal power allocation can be set as

$$\begin{array}{cc}\max\limits_{\left\{p^{(n)}:n=1,2,\cdots,N\right\}} & \sum_{n=1}^{N}\mathcal{R}^{\star(n)}\left(p^{(n)}\right)\\ s.t. & \sum_{n=1}^{N}p^{(n)}\le p_{\text{tot}},\end{array} \tag{2.25}$$

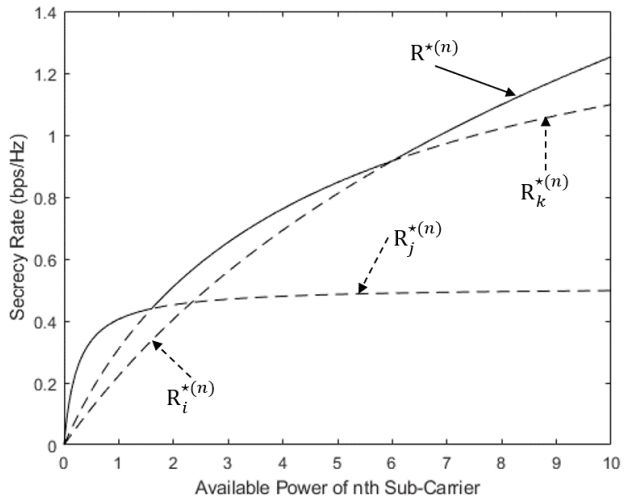



Figure 2.2: Illustration of non-convex shape of $\mathcal{R}^{\star(n)}$.

where $p_{\text{tot}}$ is a total system power. In general, the optimal cooperative strategy of the $n$th sub-carrier is not determined as the specific one among existing $M$ strategies and varies depending on how much the available power is given to that sub-carrier as shown in Fig. 2.2. This means that, before allocating the available power to the $n$th sub-carrier, I cannot specify the one as the optimal cooperative strategy among $M$ possible strategies. In addition, this also implies that $\mathcal{R}^{\star(n)}(\cdot)$ has a shape of the non-concave function at the discontinuity point where the optimal cooperative strategy changes as shown in Fig. 2.2. As a result, the objective function of (2.25) becomes the non-concave function. Thus, it is not straightforward to solve (2.25) since that problem is not the non-convex optimization problem. The typical method for solving (2.25) is considering the sub-problems derived from the original optimization problem instead of the original one. To eliminate the non-concavity resulted from the variation of the optimal cooperative strategy versus $p^{(n)}$, in the sub-problem, the specific one strategy is adopted arbitrarily among $M$ possible strategies on each sub-carrier regardless of whether they are really optimal strategies or not. By doing so, I can make a total of

$M^N$ different sub-problems from (2.25) assuming the number of total sub-carrier is $N$. If I index those sub-problems arbitrarily, the $i$th sub-problem can be represented as

$$\begin{array}{cc} \max\limits_{\{p^{(n)}:n=1,2,\cdots,N\}} & \sum_{n=1}^{N} \mathcal{R}_{n_i}^{\star(n)}\left(p^{(n)}\right) \\ s.t. & \sum_{n=1}^{N} p^{(n)} \leq p_{\text{tot}}, \end{array} \text{ for } i = 1, \cdots, M^N \tag{2.26}$$

where $n_i$ denotes the index number indicating the adopted cooperative transmission strategy among $M$ strategies on the $n$th sub-carrier for the $i$th sub-problem.

Consequently, the optimal available power and the optimal cooperative strategy of each sub-carrier is determined by comparing all sum secrecy rates corresponding to solutions of $M^N$ sub-problems. In other words, if the solution of the $i$th sub-problem is given by

$$p_i^{\star(n)} \quad \text{for } n = 1, 2, \cdots, N,$$

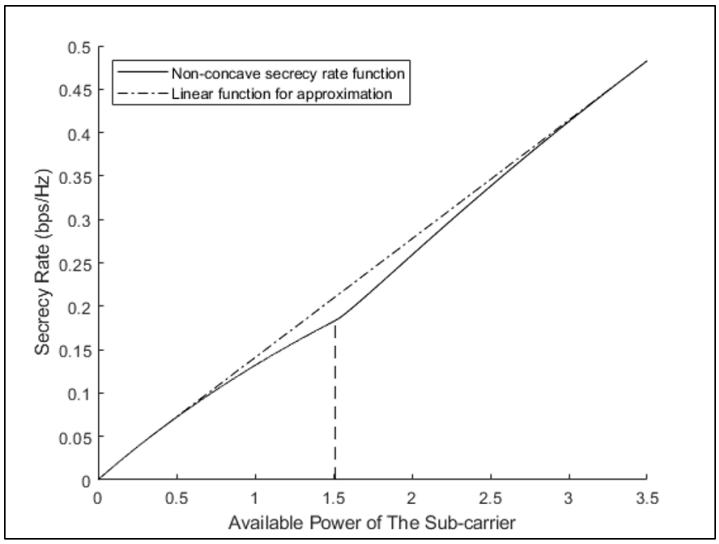
then, the solution of (2.25), the original problem, can be represented as

$$p^{\star(n)} = p_{i^*}^{\star(n)} \quad \text{for } n = 1, 2, \cdots, N,$$

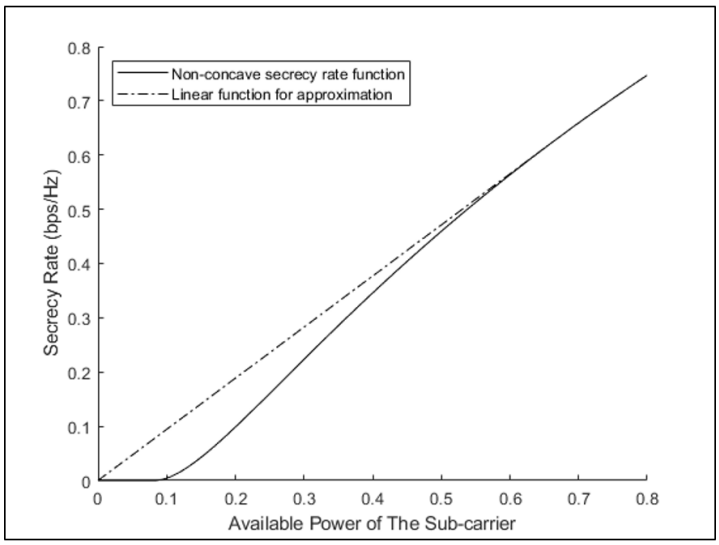
where $p^{\star(n)}$ is the optimal available power of the $n$th sub-carrier and $i^*$ denotes the index of the optimal cooperative transmission strategy on the $n$th sub-carrier which is determined as

$$i^* = \underset{\{i=1,2,\cdots,M^N\}}{\arg\max} \sum_{n=1}^{N} \mathcal{R}_{n_i}^{\star(n)}\left(p_i^{\star(n)}\right).$$

Even though, in each sub-problem, there does not exist the non-concavity caused from the variation of the optimal strategy on each sub-carrier, the objective functions of some sub-problem may be still the non-concave function depending on the channel states given on the sub-carrier. This is because that the achievable secrecy rate function of the individual strategy can be non-concave itself as shown in Fig. 2.3. It shows the cases in which the achievable secrecy rate function of the $n$th sub-carrier for the $i$th sub-problem has the shape of non-concave function at the two channel conditions; (a) $\alpha_{n_i}^{\star(n)} > \beta_{n_i}^{\star(n)}$ and (b) $\alpha_{n_i}^{\star(n)} \leq \beta_{n_i}^{\star(n)}$, respectively. Fortunately, in this case, the




(a)




(b)

Figure 2.3: Non-convex shape of $\mathcal{R}_{n_i}^{\star(n)}$ when (a) $\alpha_{n_i}^{\star(n)} > \beta_{n_i}^{\star(n)}$, (b) $\alpha_{n_i}^{\star(n)} \leq \beta_{n_i}^{\star(n)}$.

non-concave shape is relatively simple in comparison with that of the original problem and thus, the less number of computation may be required to obtain the solution of the sub-problem. Nevertheless, in general, the extremely tremendous computations which cannot be handled in normal systems are required to solve the non-concave optimization problem. Particularly, for the worst case where the objective functions of all sub-problems are non-concave functions, I have to solve a total of $M^N$ non-convex optimization problem in order to obtain the solution of (2.25). Due to this computation issue, the method of finding the sub-optimal solution rather than the optimal one is preferred for a realistic system. In this paper, I also derive the sub-optimal solution of the non-convex sub-problem which requires relatively very low computations and is asymptotically same as the optimal solution when the number of sub-carrier or intermediate nodes goes to infinity.

### 2.4.1 Sub-optimal power allocation

In order to obtain sub-optimal solution of each sub-problem, I utilize the method approximating the non-concave function to a concave function although the shape of the approximated one is not strictly concave. Actually, for all sub-problems, $\mathcal{R}_1(\cdot)$ is always the concave function among two partial functions of the achievable secrecy rate. Therefore, this implies that $\mathcal{R}_2$ causes the non-concavity of the achievable secrecy rate. In Fig. 2.3, it is shown that $\mathcal{R}_2(\cdot)$ has the convex shape during a certain interval from $p_{n_i,1}^{(n)}$ or $p_{n_i,2}^{(n)}$. However, since the second-order derivative of $\mathcal{R}_2$ is always the strictly decreasing function, $\mathcal{R}_2(\cdot)$ has the concave shape again when $p^{(n)}$ is greater than $p_{n_i,3}^{(n)}$ denoting the point in which the second-order derivative of $\mathcal{R}_2$ is zero as shown in Fig. 2.3.

To approximate the non-concave $\mathcal{R}_{n_i}^{\star(n)}(\cdot)$ to the concave function, I use the tangent line which is tangent to $\mathcal{R}_1(\cdot)$ and $\mathcal{R}_2(\cdot)$ simultaneously as shown in Fig. 2.3. Tangent points of two partial functions are denoted by $t_{n_i,1}^{(n)}$ and $t_{n_i,2}^{(n)}$, respectively. If I let $\mathcal{R}_{n_i,\text{app}}^{\star(n)}(\cdot)$ denote the approximated function in which the non-concave part

of $\mathcal{R}_{n_i}^{\star(n)}(\cdot)$ is replaced with the tangent line during the interval from $t_{n_i,1}^{(n)}$ to $t_{n_i,2}^{(n)}$, $\mathcal{R}_{n_i,\text{app}}^{(n)}(\cdot)$ is guaranteed surely to be the concave function. The slope of the tangent line is obtained from the following equation as

$$\frac{\mathcal{R}_2\left(t_{n_i,2}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) - \mathrm{I}_{n_i}^{(n)}\mathcal{R}_1\left(t_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right)}{t_{n_i,2}^{(n)} - \mathrm{I}_{n_i}^{(n)} t_{n_i,1}^{(n)}} = \mu_{n_i}^{(n)},$$

where $\mu_{n_i}^{(n)}$ denotes the slope of the tangent line for approximating the achievable secrecy rate of the $n$th sub-carrier for the $i$th sub-problem, and the two tangent points are given as

$$t_{n_i,1}^{(n)} = \mathcal{P}_1\left(\mu_{n_i}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right),$$

$$t_{n_i,2}^{(n)} = \mathcal{P}_2\left(\mu_{n_i}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right), \quad \text{s.t.} \quad t_{n_i,2}^{(n)} \geq p_{n_i,3}^{(n)}$$

where $\mathcal{P}_1(\cdot)$ and $\mathcal{P}_2(\cdot)$ are the functions same as the inverse functions of the first-order derivative functions of $\mathcal{R}_1$ and $\mathcal{R}_2$ with respect to $p^{(n)}$, which is defined as

$$\mathcal{P}_k(\mu, \mathbf{c}) := \{\mathcal{Q}_k(x, \mathbf{c})\}^{-1}, \quad \text{for } k = 1,\, 2,$$

$$\mathcal{Q}_k(x, \mathbf{c}) := \tfrac{\partial \mathcal{R}_k(x, \mathbf{c})}{\partial x}, \quad \text{for } k = 1,\, 2.$$

This means that $\mathcal{P}_k(\mu, \mathbf{c})$ equals to the point at which the tangent slope of $\mathcal{R}_k$ is $\mu$. For simplicity of equation expressions, the second-order derivative functions of $\mathcal{R}_1$ and $\mathcal{R}_2$ with respect to $p^{(n)}$ is also defined as

$$\mathcal{Q}_k'(x, \mathbf{c}) := \tfrac{\partial^2 \mathcal{R}_k(x, \mathbf{c})}{\partial x^2}, \quad \text{for } k = 1,\, 2,$$

and $p_{n_i,3}^{(n)}$ is determined such that $\mathcal{Q}_2'(p_{n_i,3}^{(n)}, \mathbf{c}_{n_i}^{(n)}) = 0$. Furthermore, $\mathcal{P}_1(\cdot)$ and $\mathcal{P}_2(\cdot)$ can be represented as the closed forms which are given as

$$\mathcal{P}_1(\mu, \mathbf{c}) := \frac{1}{2}\left\{\sqrt{\{y_1(\mathbf{c})\}^2 - y_2(\mathbf{c})\left(1 - \frac{y_3(\mathbf{c})}{\mu}\right)} - y_1(\mathbf{c})\right\},$$

$$\mathcal{P}_2(\mu, \mathbf{c}) := \frac{1}{2\alpha\gamma}\left\{\sqrt{2z_4(\mu, \mathbf{c}) - z_2(\mu, \mathbf{c})} - \frac{1}{2}z_1(\mu, \mathbf{c}) - \sqrt{-2z_4(\mu, \mathbf{c}) - z_2(\mu, \mathbf{c}) - 4\sqrt{\{z_4(\mu, \mathbf{c})\}^2 - z_3(\mu, \mathbf{c})}}\right\},$$

where $y_1(\mathbf{c}) := \frac{\lambda}{\alpha\gamma} + \frac{\lambda}{\beta\gamma}$, $y_2(\mathbf{c}) := \left(\frac{\lambda}{\gamma}\right)^2 \frac{4}{\alpha\beta}$, $y_3(\mathbf{c}) := \frac{\lambda}{\beta\gamma} - \frac{\lambda}{\alpha\gamma}$, and $z_1(\mu, \mathbf{c})$, $z_2(\mu, \mathbf{c})$, $z_3(\mu, \mathbf{c})$, $z_4(\mu, \mathbf{c})$ are the functions given by

$$z_1(\mu, \mathbf{c}) := 3\lambda - \beta - 4\alpha - \frac{2}{\mu},$$

$$z_2(\mu, \mathbf{c}) := \left(\frac{1}{\mu} - \lambda\right)\left(2\beta - 3\lambda + \frac{1}{\mu}\right) - \frac{3}{8}\left\{3\lambda - \beta - \frac{2}{\mu}\right\}^2,$$

$$z_3(\mu, \mathbf{c}) := -\frac{\beta\lambda}{\mu^2} + \frac{(\beta - \lambda)}{4}\left(\frac{1}{\mu} - \lambda\right)\left\{3\lambda - \beta - \frac{2}{\mu}\right\} + \left\{3\lambda - \beta - \frac{2}{\mu}\right\}^2 \frac{z_2(\mu, \mathbf{c})}{16} + \frac{3}{256}\left\{3\lambda - \beta - \frac{2}{\mu}\right\}^4,$$

$$z_4(\mu, \mathbf{c}) := 3\lambda - \beta - \frac{2}{\mu}$$

and $\mathrm{I}_{n_i}^{(n)}$ is the indicator function which is defined by

$$\mathrm{I}_{n_i}^{(n)} = \begin{cases} 0, & \text{if } \left\{\alpha_{n_i}^{(n)} \leq \beta_{n_i}^{(n)}\right\} \text{ or} \\ & \left\{\alpha_{n_i}^{(n)} > \beta_{n_i}^{(n)} \text{ and } \mathcal{D}\left(\mu_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) > 0\right\}, \\ 1, & \text{if } \alpha_{n_i}^{(n)} > \beta_{n_i}^{(n)} \text{ and } \mathcal{D}\left(\mu_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) \leq 0, \end{cases} \quad \begin{array}{c} \text{for } n = 1, \cdots, N; \\ i = 1, \cdots, M^N, \end{array}$$

where $\mu_{n_i,1}^{(n)} := \mathcal{Q}_1\left(0, \mathbf{c}_{n_i}^{(n)}\right)$ for all $n$ and all $i$, and $\mathcal{D}(\cdot)$ is the function defined as

$$\mathcal{D}(\mu, \mathbf{c}_1, \mathbf{c}_2) = \frac{\mathcal{R}_2(\mathcal{P}_2(\mu, \mathbf{c}_2), \mathbf{c}_2) - \mathcal{R}_1(\mathcal{P}_1(\mu, \mathbf{c}_1), \mathbf{c}_1)}{\mathcal{P}_2(\mu, \mathbf{c}_2) - \mathcal{P}_1(\mu, \mathbf{c}_1)} - \mu.$$

By doing so, the approximated achievable secrecy rate function on the $n$th sub-carrier for the $i$th sub-problem is given by

$$\mathcal{R}_{n_i,\text{app}}^{\star(n)}\left(p^{(n)}\right) = \begin{cases} \mathrm{I}_{n_i}^{(n)}\mathcal{R}_1\left(p^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) & \text{if } 0 \leq p^{(n)} \leq t_{n_i,1}^{(n)}, \\ \mu_{n_i}^{(n)}\left(p^{(n)} - t_{n_i,1}^{(n)}\right) + \mathrm{I}_{n_i}^{(n)}T_{n_i,1}^{(n)} & \text{if } t_{n_i,1}^{(n)} < p^{(n)} < t_{n_i,2}^{(n)}, \\ \mathcal{R}_2\left(p^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) & \text{if } p^{(n)} \geq t_{n_i,2}^{(n)}, \end{cases} \quad (2.27)$$

where $T_{n_i,1}^{(n)} := \mathcal{R}_1\left(t_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right)$ for all $n$ and all $i$.

Table 2.2: The Concavity of the Achievable Secrecy Rate Function on the $n$th Sub-carrier for the $i$th Sub-problem, $n = 1, \cdots, N$; $i = 1, \cdots, M^N$

| Conditions | | $\Omega_{n_i}^{(n)}$ |
|---|---|---|
| $\alpha_{n_i}^{(n)} > \beta_{n_i}^{(n)}$ | $\mathcal{Q}_2^{'}\left(p_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) < 0$ | 0 (concave) |
| | $\mathcal{Q}_2^{'}\left(p_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right) \geq 0$ | 1 (non-concave) |
| $\alpha_{n_i}^{(n)} \leq \beta_{n_i}^{(n)}$ | | |

For the sub-carrier of which the achievable secrecy rate is naturally the concave function, the approximating method is unnecessary. Thus, the achievable secrecy rates of all sub-carriers for the $i$th approximated sub-problem are given by

$$\mathcal{R}_{n_i,\text{sub}}^{\star(n)}\left(p^{(n)}\right) = \begin{cases} \mathcal{R}_{n_i}^{\star(n)}\left(p^{(n)}\right), & \text{if } \Omega_{n_i}^{(n)} = 0, \\ \mathcal{R}_{n_i,\text{app}}^{\star(n)}\left(p^{(n)}\right), & \text{if } \Omega_{n_i}^{(n)} = 1, \end{cases} \text{for } n = 1, \cdots, N, \tag{2.28}$$

where $\Omega_{n_i}^{(n)}$ is the number indicating the concavity of the achievable secrecy rate on the $n$th sub-carrier for the $i$th sub-problem based on the Table 2.2. As a result, the $i$th sub-problem can be considered as the convex optimization problem and be solved easily by the Karush-Kuhn-Tucker (KKT) conditions. The sub-optimal solution of each sub-

problem is given by

$$p_{i,\text{sub}}^{\star(n)}(\mu) = \begin{cases} 0, & \text{if } \mu > \mu_{n_i,1}^{(n)} \\ & \text{and } \Omega_{n_i}^{(n)} = 0, \\ \mathcal{P}_1\left(\mu, \mathbf{c}_{n_i}^{(n)}\right), & \text{if } \mu_{n_i,1}^{(n)} \geq \mu > \mu_{n_i,2}^{(n)} \\ & \text{and } \Omega_{n_i}^{(n)} = 0, \\ \mathcal{P}_2\left(\mu, \mathbf{c}_{n_i}^{(n)}\right), & \text{if } \mu \leq \mu_{n_i,2}^{(n)} \\ & \text{and } \Omega_{n_i}^{(n)} = 0, \\ 0, & \text{if } \mu > \mu_{n_i,3}^{(n)} \quad \text{for } n = 1, \cdots, N; \\ & \text{and } \Omega_{n_i}^{(n)} = 1, \quad i = 1, \cdots, M^N, \\ \mathbf{I}_{n_i}^{(n)}\mathcal{P}_1\left(\mu, \mathbf{c}_{n_i}^{(n)}\right), & \text{if } \mu_{n_i,3}^{(n)} \geq \mu > \mu_{n_i}^{(n)} \\ & \text{and } \Omega_{n_i}^{(n)} = 1, \\ p_{\text{tot}} - \sum_{l=1, l\neq n}^{N} p_{i,\text{sub}}^{\star(l)}\left(\mu_{n_i}^{(n)}\right), & \text{if } \mu = \mu_{n_i}^{(n)} \\ & \text{and } \Omega_{n_i}^{(n)} = 1, \\ \mathcal{P}_2\left(\mu, \mathbf{c}_{n_i}^{(n)}\right), & \text{if } \mu < \mu_{n_i}^{(n)} \\ & \text{and } \Omega_{n_i}^{(n)} = 1, \end{cases} \tag{2.29}$$

where $\mu_{n_i,2}^{(n)} := \mathcal{Q}_1\left(p_{n_i,1}^{(n)}, \mathbf{c}_{n_i}^{(n)}\right)$ for all $n$ and all $i$, $\mu_{n_i,3}^{(n)}$ is defined as

$$\mu_{n_i,3}^{(n)} = \begin{cases} \mathcal{Q}_1\left(0, \mathbf{c}_{n_i}^{(n)}\right), & \text{if } \alpha_{n_i}^{(n)} > \beta_{n_i}^{(n)}, \\ \infty, & \text{if } \alpha_{n_i}^{(n)} \leq \beta_{n_i}^{(n)}, \end{cases} \text{for } n = 1, \cdots, N;\ i = 1, \cdots, M^N,$$

and $\mu$ is determined such that $\sum_{n=1}^{N} p_{i,\text{sub}}^{(n)}(\mu) = p_{\text{tot}}$.

Consequently, the sub-optimal solution of (2.25) is given by

$$p_{\text{sub}}^{\star(n)} = p_{i^*,\text{sub}}^{\star(n)} \quad \text{for } n = 1, 2, \cdots, N,$$

where $p_{sub}^{\star(n)}$ is the sub-optimal power of the $n$th sub-carrier and $i^*$ is determined as

$$i^* = \underset{\{i=1,2,\cdots,M^N\}}{\arg\max} \sum_{n=1}^{N} \mathcal{R}_{n_i}^{\star(n)}\left(p_{i,\text{sub}}^{\star(n)}(\mu)\right).$$

Moreover, the sub-optimal cooperative transmission strategy on the $n$th sub-carrier is determined as

$$m_{\text{sub}}^{\star(n)} = n_{i^*} \quad \text{for } n = 1, 2, \cdots, N,$$

where $m_{\text{sub}}^{(n)}$ is the index indicating the sub-optimal cooperative transmission strategy among $M$ strategies on the $n$th sub-carrier.

Even though I have been avoid solving the non-concave optimization problem by deriving the sub-optimal solution instead of the optimal one of (2.25), there remains as the high computation issue as ever. This is because that the number of sub-problems is proportional to the number of intermediate nodes existing inside the network and even exponentially proportional to the number of sub-carriers of the system. Since, in the communication systems such as OFDM, the number of sub-carriers is usually from 64 to 128 or even more than 128, the required computation for solving $M^N$ sub-problems is generally extremely high even though the communication network includes low number of intermediate nodes. Thus, the normal communication systems cannot still afford to handle the computation required for deriving the sub-optimal solution of (2.25). To overcome this computation issue, I propose the efficient power allocation method which requires very low computation in comparison with finding the sub-optimal power allocation as well as the optimal one.

### 2.4.2 Proposed power allocation

At the very low available power of the sub-carrier including the zero available power, all achievable secrecy rate functions can be approximated to a linear function. Assuming that the $m$th strategy is adopted on the $n$th sub-carrier, the linear function for this approximation is given by

$$\mathcal{R}_m^{\star(n)}(x) \simeq \mathrm{I}_m^{(n)} \theta_m^{(n)} x, \tag{2.30}$$

where $\theta_m^{(n)} := \frac{\gamma_m^{(n)}}{\lambda_m^{(n)}}(\alpha_m^{(n)} - \beta_m^{(n)})$. This implies that the achievable secrecy rate function of the transmission strategy where the slope of the linear function is maximum is superior in the vicinity of the zero available power than the achievable secrecy rate

functions of other strategies. Thus, there always exists the positive number, $\delta_1^{(n)}$, satisfying the following equation as

$$\mathcal{R}^{\star(n)}(x) = \mathcal{R}_{v_n}^{\star(n)}(x) = \mathcal{R}_1\left(x, \mathbf{c}_{v_n}^{(n)}\right), \quad \text{if } 0 \leq x < \delta_1^{(n)}, \tag{2.31}$$

where $v_n$ is the index indicating the transmission strategy which corresponds to the optimal strategy at the very low available power and is given as

$$v_n = \underset{\{m=1,2,\cdots,M\}}{\arg\max}\ \theta_m^{(n)}.$$

On the one hand, at the very high available power of the sub-carrier, $f(\cdot)$ can be approximated to a linear function as follow

$$f\left(x, \mathbf{c}_m^{(n)}\right) \simeq \phi_m^{(n)}\left(1 + \gamma_m^{(n)} x\right), \tag{2.32}$$

where $\phi_m^{(n)} := \frac{1}{\beta_m^{(n)} - \lambda_m^{(n)}}\left(\left(\frac{\beta_m^{(n)}}{\lambda_m^{(n)}}\right)^{\frac{1}{2}} - 1\right)$. Using (2.32), at the very high available power, $\mathcal{R}_m^{\star(n)}(\cdot)$ is also approximated to the following equation as

$$\mathcal{R}_m^{\star(n)}(x) \simeq \log_2 x + \psi_m^{(n)}, \tag{2.33}$$

where $\psi_m^{(n)} := \log_2\{\alpha_m^{(n)}\gamma_m^{(n)}\lambda_m^{(n)}(\phi_m^{(n)})^2\}$. From (2.33), it is obvious that the optimal cooperative strategy is definitely determined by $\psi_m^{(n)}$ value as $x$ increases gradually. That is, at the enough high available power, the achievable secrecy rate corresponding to the strategy in which $\psi_m^{(n)}$ is the highest is most dominant than the achievable secrecy rate functions corresponding to other strategies. This implies that there always exists the positive number, $\delta_2^{(n)}$, satisfying the equation which is given by

$$\mathcal{R}^{\star(n)}(x) = \mathcal{R}_{w_n}^{\star(n)}(x) = \mathcal{R}_2\left(x, \mathbf{c}_{w_n}^{(n)}\right), \quad \text{for } x \geq \delta_2^{(n)}, \tag{2.34}$$

where $w_n$ is the index indicating the transmission strategy which corresponds to the optimal strategy at the very high available power and is given as

$$w_n = \underset{\{m=1,2,\cdots,M\}}{\arg\max}\ \psi_m^{(n)}.$$

Consequently, the shape of the maximum achievable secrecy rate of the $n$th sub-carrier, $\mathcal{R}^{\star(n)}$, necessarily includes the two achievable secrecy rate functions corresponding to the $v_n$th strategy and the $w_n$th strategy. For instance, in the case of Fig. 2.2, assuming that the shape of $\mathcal{R}^{\star(n)}$ is determined by only 3 functions such as $\mathcal{R}_i^{\star(n)}$, $\mathcal{R}_j^{\star(n)}$ and $\mathcal{R}_k^{\star(n)}$, $j$ and $i$ correspond to $v_n$ and $w_n$, respectively. From these results, similarly to the approximating method used in the sub-problem of (2.25), I propose the method which approximates $\mathcal{R}^{\star(n)}$ to a concave function at once using only two achievable secrecy rate functions of $\mathcal{R}_{v_n}^{\star(n)}$ and $\mathcal{R}_{w_n}^{\star(n)}$.

However, unlike the former approximating method, there may not exist the tangent line which is tangent to $\mathcal{R}_{v_n}^{\star(n)}$ and $\mathcal{R}_{w_n}^{\star(n)}$ simultaneously. This is because that, when $\delta_1^{(n)}$ is very small compared to $\delta_2^{(n)}$, the achievable secrecy rate function of the $v_n$th strategy may be much different with the maximum achievable secrecy rate at a majority of the interval from 0 to $\delta_2^{(n)}$. Thus, for preventing this case, I consider the additional strategy whose the achievable secrecy rate function may have the more similar shape to the maximum achievable secrecy rate. As a result, the transmission strategy utilized for the approximation of $\mathcal{R}^{\star(n)}$ is determined as

$$\acute{v}_n = \begin{cases} v_n, & \begin{array}{c} \text{if } \left\{\alpha_{v_n}^{(n)} \leq \beta_{v_n}^{(n)}\right\} \text{ or} \\ \left\{\alpha_{v_n}^{(n)} > \beta_{v_n}^{(n)} \text{ and } \mathcal{D}\left(\mu_0^{(n)}, \mathbf{c}_{v_n}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) > 0\right\}, \end{array} \\ \hat{v}_n, & \text{if } \alpha_{v_n}^{(n)} > \beta_{v_n}^{(n)} \text{ and } \mathcal{D}\left(\mu_0^{(n)}, \mathbf{c}_{v_n}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) \leq 0, \end{cases}$$

where $\mu_0^{(n)} := \mathcal{Q}_2(p_{w_n,3}^{(n)}, \mathbf{c}_{w_n}^{(n)})$, $\acute{v}_n$ is the index indicating the transmission strategy utilized for the approximation, and $\hat{v}_n$ denotes the index indicating the additional considered strategy which is given by

$$\hat{v}_n = \underset{\{m=1,2,\cdots,M\}}{\arg\max} \ \mathcal{R}_1\left(p_{w_n,1}^{(n)}, \mathbf{c}_{v_n}^{(n)}\right).$$

Similarly to the case of the sub-optimal power allocation, the slope of the tangent line for the approximation on the $n$th sub-carrier is obtained from the following

equation as

$$\frac{\mathcal{R}_2\left(t_{w_n}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) - \mathrm{I}^{(n)}\mathcal{R}_1\left(t_{\acute{v}_n}^{(n)}, \mathbf{c}_{\acute{v}_n}^{(n)}\right)}{t_{w_n}^{(n)} - \mathrm{I}^{(n)} t_{\acute{v}_n}^{(n)}} = \mu^{(n)},$$

where $\mu^{(n)}$ denotes the slope of the tangent line for approximating the achievable secrecy rate of the $n$th sub-carrier for the proposed method, and the two tangent points are given as

$$t_{\acute{v}_n}^{(n)} = \mathcal{P}_1\left(\mu^{(n)}, \mathbf{c}_{\acute{v}_n}^{(n)}\right),$$

$$t_{w_n}^{(n)} = \mathcal{P}_2\left(\mu^{(n)}, \mathbf{c}_{w_n}^{(n)}\right), \quad \text{s.t.} \quad t_{w_n}^{(n)} \geq p_{w_n,3}^{(n)}$$

and $\mathrm{I}^{(n)}$ is the indicator function which is defined as

$$\mathrm{I}^{(n)} = \begin{cases} 0, & \text{if } \left\{\alpha_{\acute{v}_n}^{(n)} \leq \beta_{\acute{v}_n}^{(n)}\right\} \text{ or} \\ & \left\{\alpha_{\acute{v}_n}^{(n)} > \beta_{\acute{v}_n}^{(n)} \text{ and } \mathcal{D}\left(\mu_1^{(n)}, \mathbf{c}_{\acute{v}_n}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) > 0\right\}, \quad \text{for } n = 1, \cdots, N. \\ 1, & \text{if } \alpha_{\acute{v}_n}^{(n)} > \beta_{\acute{v}_n}^{(n)} \text{ and } \mathcal{D}\left(\mu_1^{(n)}, \mathbf{c}_{\acute{v}_n}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) \leq 0, \end{cases}$$

where $\mu_1^{(n)} := \mathcal{Q}_1\left(0, \mathbf{c}_{\acute{v}_n}^{(n)}\right)$ for all $n$. In addition, the approximated achievable secrecy rate function of the $n$th sub-carrier is given by

$$\mathcal{R}_{\text{app}}^{\star(n)}\left(p^{(n)}\right) = \begin{cases} \mathrm{I}^{(n)}\mathcal{R}_1\left(p^{(n)}, \mathbf{c}_{\acute{v}_n}^{(n)}\right) & \text{if } 0 \leq p^{(n)} \leq t_{\acute{v}_n}^{(n)}, \\ \mu^{(n)}\left(p^{(n)} - t_{\acute{v}_n}^{(n)}\right) + \mathrm{I}^{(n)} T^{(n)} & \text{if } t_{\acute{v}_n}^{(n)} < p^{(n)} < t_{w_n}^{(n)}, \\ \mathcal{R}_2\left(p^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) & \text{if } p^{(n)} \geq t_{w_n}^{(n)}, \end{cases} \tag{2.35}$$

where $T^{(n)} := \mathcal{R}_1(t_{\acute{v}_n}^{(n)}, \mathbf{c}_{\acute{v}_n}^{(n)})$ for all $n$.

Since the approximating method is unnecessary for the sub-carrier of which the two achievable secrecy rate functions selected for the approximation forms the concave function shape already, the maximum achievable secrecy rate of each sub-carrier for the proposed method is given by

$$\mathcal{R}_{\text{prop}}^{\star(n)}\left(p^{(n)}\right) = \begin{cases} \mathcal{R}^{\star(n)}\left(p^{(n)}\right), & \text{if } \Omega^{(n)} = 0, \\ \mathcal{R}_{\text{app}}^{\star(n)}\left(p^{(n)}\right), & \text{if } \Omega^{(n)} = 1, \end{cases} \quad \text{for } n = 1, \cdots, N, \tag{2.36}$$

Table 2.3: The Concavity of the Maximum Achievable Secrecy Rate Function on the $n$th Sub-carrier, $n = 1, \cdots, N$

| Conditions | | | $\Omega^{(n)}$ |
|---|---|---|---|
| $\acute{v}_n = w_n$ | $\alpha_{w_n}^{(n)} > \beta_{w_n}^{(n)}$ | $\mathcal{Q}_2^{'}\left(p_{w_n,1}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) < 0$ | 0 (concave) |
| | | $\mathcal{Q}_2^{'}\left(p_{w_n,1}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right) \geq 0$ | 1 (non-concave) |
| | $\alpha_{w_n}^{(n)} \leq \beta_{w_n}^{(n)}$ | | |
| $\acute{v}_n \neq w_n$ | | | |

where $\Omega^{(n)}$ is the number indicating the concavity of the two achievable secrecy rate functions selected for the approximation on the $n$th sub-carrier based on the Table 2.3. Furthermore, using the KKT conditions, the proposed solution of (2.25) is given as

$$p_{\text{prop},1}^{\star(n)}(\mu) = \begin{cases} 0, & \text{if } \mu > \mu_1^{(n)} \\ & \text{and } \Omega^{(n)} = 0, \\ \mathcal{P}_1\left(\mu, \mathbf{c}_{w_n}^{(n)}\right), & \text{if } \mu_1^{(n)} \geq \mu > \mu_2^{(n)} \\ & \text{and } \Omega^{(n)} = 0, \\ \mathcal{P}_2\left(\mu, \mathbf{c}_{w_n}^{(n)}\right), & \text{if } \mu \leq \mu_2^{(n)} \\ & \text{and } \Omega^{(n)} = 0, \\ 0, & \text{if } \mu > \mu_3^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ \mathrm{I}^{(n)}\mathcal{P}_1\left(\mu, \mathbf{c}_{\acute{v}_n}^{(n)}\right), & \text{if } \mu_3^{(n)} \geq \mu > \mu^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ p_{\text{tot}} - \sum_{l=1, l\neq n}^{N} p_{prop,1}^{\star(l)}\left(\mu^{(n)}\right), & \text{if } \mu = \mu^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ \mathcal{P}_2\left(\mu, \mathbf{c}_{w_n}^{(n)}\right), & \text{if } \mu < \mu^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \end{cases} \quad \text{for } n = 1, \cdots, N, \tag{2.37}$$

where $\mu_2^{(n)} := \mathcal{Q}_1\left(p_{w_n,1}^{(n)}, \mathbf{c}_{w_n}^{(n)}\right)$ for all $n$, $\mu_3^{(n)}$ is defined as

$$\mu_3^{(n)} = \begin{cases} \mathcal{Q}_1\left(0, \mathbf{c}_{\acute{v}_n}^{(n)}\right), & \text{if } \alpha_{\acute{v}_n}^{(n)} > \beta_{\acute{v}_n}^{(n)}, \\ \infty, & \text{if } \alpha_{\acute{v}_n}^{(n)} \leq \beta_{\acute{v}_n}^{(n)}, \end{cases} \quad \text{for } n = 1, \cdots, N,$$

and $\mu$ is determined such that $\sum_{n=1}^{N} p_{\text{prop},1}^{\star(n)}(\mu) = p_{\text{tot}}$. Furthermore, the transmission strategy which is adopted on each sub-carrier for the proposed method is determined as

$$m_{\text{prop},1}^{\star(n)} = \underset{\{m=\acute{v}_n, w_n\}}{\arg\max}\ \mathcal{R}_m^{\star(n)}\left(p_{\text{prop},1}^{\star(n)}(\mu)\right), \quad \text{for } n = 1, \cdots, N,$$

where $m_{prop,1}^{\star(n)}$ is the index indicating the transmission strategy adopted on the $n$th sub-carrier for the proposed solution.

When all channel states from intermediate nodes to the destination node is worse than those from intermediate nodes to the eavesdropper node on the $n$th sub-carrier, the maximum achievable secrecy rate of the $n$th sub-carrier has the non-concave function shape as shown in Fig. 2.3 (b). In this case, the approximated function for the proposed method or for the sub-optimal method has a quite different function shape with the original function and accordingly, the security performance corresponding to the solutions of those methods deteriorates in comparison to the performance corresponding the optimal solution. Particularly, at the low available power, the different degree between the approximated function and the original function is relatively high.

To reduce this security performance deterioration, I consider another solution of (2.25) obtained by the method modifying (2.37). In this method, the solution corresponding to the approximated interval on the $n$th sub-carrier is determined by not the tangent line used for the approximation, but the achievable secrecy rate function of the

$\acute{v}_n$th strategy. By doing so, the other proposed solution of (2.25) is given by

$$p^{\star(n)}_{\text{prop},2}(\mu) = \begin{cases} 0, & \text{if } \mu > \mu_1^{(n)} \\ & \text{and } \Omega^{(n)} = 0, \\ \mathcal{P}_1\left(\mu, \mathbf{c}^{(n)}_{w_n}\right), & \text{if } \mu_1^{(n)} \geq \mu > \mu_2^{(n)} \\ & \text{and } \Omega^{(n)} = 0, \\ \mathcal{P}_2\left(\mu, \mathbf{c}^{(n)}_{w_n}\right), & \text{if } \mu \leq \mu_2^{(n)} \\ & \text{and } \Omega^{(n)} = 0, \\ 0, & \text{if } \mu \geq \mu_3^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ \mathrm{I}^{(n)}\mathcal{P}_1\left(\mu, \mathbf{c}^{(n)}_{\acute{v}_n}\right), & \text{if } \mu \in \mathrm{A}_1^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ \mathcal{P}_1\left(\tilde{\mu}, \mathbf{c}^{(n)}_{\acute{v}_n}\right), & \text{if } \mu \in \mathrm{A}_2^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ \mathcal{P}_2\left(\tilde{\mu}, \mathbf{c}^{(n)}_{w_n}\right), & \text{if } \mu \in \mathrm{A}_3^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \\ \mathcal{P}_2\left(\mu, \mathbf{c}^{(n)}_{w_n}\right), & \text{if } \mu \in \mathrm{A}_4^{(n)} \\ & \text{and } \Omega^{(n)} = 1, \end{cases} \quad \text{for } n = 1, \cdots, N, \quad (2.38)$$

where $\mu$ and $\tilde{\mu}$ are determined such that $\sum_{n=1}^{N} p^{\star(n)}_{\text{prop},2}(\mu) = p_{\text{tot}}$, and the sets $\mathrm{A}_1^{(n)}$, $\mathrm{A}_2^{(n)}$, $\mathrm{A}_3^{(n)}$ and $\mathrm{A}_4^{(n)}$ are defined as

$$\begin{aligned} \mathrm{A}_1^{(n)} &:= \left\{ \mu |\ \mu_3^{(n)} > \mu > \mu^{(n)},\ \mu \neq \mu^{(l)},\ l \in \mathrm{B}_1^{(n)} \right\}, \\ \mathrm{A}_2^{(n)} &:= \left\{ \mu |\ \mu = \mu^{(l)},\ l \in \mathrm{B}_1^{(n)} \right\}, \\ \mathrm{A}_3^{(n)} &:= \left\{ \mu |\ \mu = \mu^{(l)},\ l \in \mathrm{B}_2^{(n)} \right\}, \\ \mathrm{A}_4^{(n)} &:= \left\{ \mu |\ \mu < \mu^{(n)},\ \mu \neq \mu^{(l)},\ l \in \mathrm{B}_2^{(n)} \right\}, \end{aligned} \quad \text{for } n = 1, \cdots, N.$$

Moreover, the sets $\mathrm{B}_1^{(n)}$ and $\mathrm{B}_2^{(n)}$ are defined by

$$\begin{aligned} \mathrm{B}_1^{(n)} &:= \left\{ l |\ \mu^{(l)} \geq \mu^{(n)},\ \Omega^{(l)} = 1,\ 1 \leq l \leq N,\ l \in \mathbb{N} \right\}, \\ \mathrm{B}_2^{(n)} &:= \left\{ l |\ \mu^{(l)} < \mu^{(n)},\ \Omega^{(l)} = 1,\ 1 \leq l \leq N,\ l \in \mathbb{N} \right\}, \end{aligned} \quad \text{for } n = 1, \cdots, N,$$

where $\mathbb{N}$ is the set of natural numbers. In the other proposed solution, the transmission strategy which is adopted on each sub-carrier is given by

$$m_{\text{prop},2}^{\star(n)} = \begin{cases} \acute{v}_n, & \mu \geq \mu^{(n)}, \\ w_n, & \mu < \mu^{(n)}, \end{cases} \quad \text{for } n = 1, \cdots, N,$$

where $m_{\text{prop},2}^{\star(n)}$ is the index indicating the transmission strategy adopted on the $n$th sub-carrier for the other proposed solution.

Consequently, the ultimate proposed solution is determined as the one of which the sum secrecy rate is highest between the two proposed solutions. In other words, the ultimate proposed solution is represented as

$$p_{\text{prop}}^{\star(n)}(\mu) = p_{\text{prop},j^*}^{\star(n)}(\mu),$$

where $p_{\text{prop}}^{\star(n)}$ denotes the ultimate proposed solution of (2.25), and $j^*$ is determined by

$$j^* = \underset{\{j=1,2\}}{\arg\max}\, \mathcal{R}_{m_{\text{prop},j}^{\star(n)}}^{\star(n)} \left( p_{\text{prop},j}^{\star(n)}(\mu) \right).$$

The transmission strategy adopted on each sub-carrier for the ultimate proposed solution is denoted by the index which is given by

$$m_{\text{prop}}^{\star(n)} = m_{\text{prop},j^*}^{\star(n)}.$$

*Remark (Computational Complexity)* : In order to derive the sub-optimal solution of (2.25), a total of $M^N$ processes of solving the optimization problem with the KKT conditions is conducted. Furthermore, in the worst case, I need to implement the approximation method $M$ times for each solving process. On the other hand, to obtain the proposed solution of (2.25), it is required only two times to solve the optimization problem with the KKT conditions. In addition, the number of implementations of the approximation method is not proportional to the number of the solving the problem, but fixed by the number less than or equal to $M$. Although additional computations are necessary for deriving the proposed solution, they are very trivial in terms of the computational complexity in comparison with the solving the optimization problem

with the KKT conditions or the implementation of the approximation method. Thus, the required computational complexity for obtaining the proposed solution is much lower than that for obtaining the sub-optimal solution.

## 2.5 Numerical Results

In this section, I present the security performance of the proposed power allocation and the sub-optimal power allocation at various simulation settings. By doing so, it is verified that the security performance of the proposed power allocation is not much different with that of the sub-optimal power allocation. For additional comparisons, an uniform power allocation is considered together with three different power distributions. In the uniform power allocation, the total system power is equally allocated to all sub-carriers, that is, the available power of each sub-carrier is given by

$$p_{\text{unif}}^{(n)} = \tfrac{1}{N} p_{\text{tot}}, \quad \text{for } n = 1, \cdots, N.$$

As the first one of the three power distribution, the optimal power distribution derived in the previous section is taken into account. Therefore, the first power distribution for the uniform power allocation is given by

$$\begin{cases} p_{\text{T}}^{(n)} = p_{\text{T}}^{\star(n)} \left( p_{\text{unif}}^{(n)}, \mathbf{c}_{m_n^*}^{(n)} \right) \\ p_{\text{R}}^{(n)} = p_{\text{R}}^{\star(n)} \left( p_{\text{unif}}^{(n)}, \mathbf{c}_{m_n^*}^{(n)} \right) \\ p_{\text{J}}^{(n)} = p_{\text{J}}^{\star(n)} \left( p_{\text{unif}}^{(n)}, \mathbf{c}_{m_n^*}^{(n)} \right), \end{cases} \quad \text{for } n = 1, \cdots, N,$$

where $m_n^*$ is the index indicating the transmission strategy adopted on the $n$th sub-carrier for the uniform power allocation and is determined as

$$m_n^* = \underset{\{m=1,2,\cdots,M\}}{\arg\max} \; \mathcal{R}_m^{\star(n)} \left( p_{\text{unif}}^{(n)} \right).$$

The second one is a uniform power distribution in which the available power of the sub-carrier is distributed equally to the transmit power, the relay power and the jamming power. Thus, on each sub-carrier, the power distribution for the second power

distribution is represented as

$$p_{\mathrm{T}}^{(n)} = p_{\mathrm{R}}^{(n)} = p_{\mathrm{J}}^{(n)} = \tfrac{1}{3} p_{\mathrm{unif}}^{(n)}, \quad \text{for } n = 1, \cdots, N.$$

The last one is the uniform power distribution with no cooperative jamming. In this case, the available power of each sub-carrier is distributed equally to only the transmit power and the relay power and it is represented as

$$\begin{cases} p_{\mathrm{J}}^{(n)} = 0 \\ p_{\mathrm{T}}^{(n)} = p_{\mathrm{R}}^{(n)} = \tfrac{1}{2} p_{\mathrm{unif}}^{(n)}, \end{cases} \quad \text{for } n = 1, \cdots, N.$$

For the second and the last power distribution, the strategy adopted on each sub-carrier is determined the following equation as

$$m_n^* = \underset{\{m=1,2,\cdots,M\}}{\arg\max} \; \mathcal{R}_m^{(n)} \left( \mathbf{p}^{(n)} \right), \quad \text{for } n = 1, \cdots, N.$$

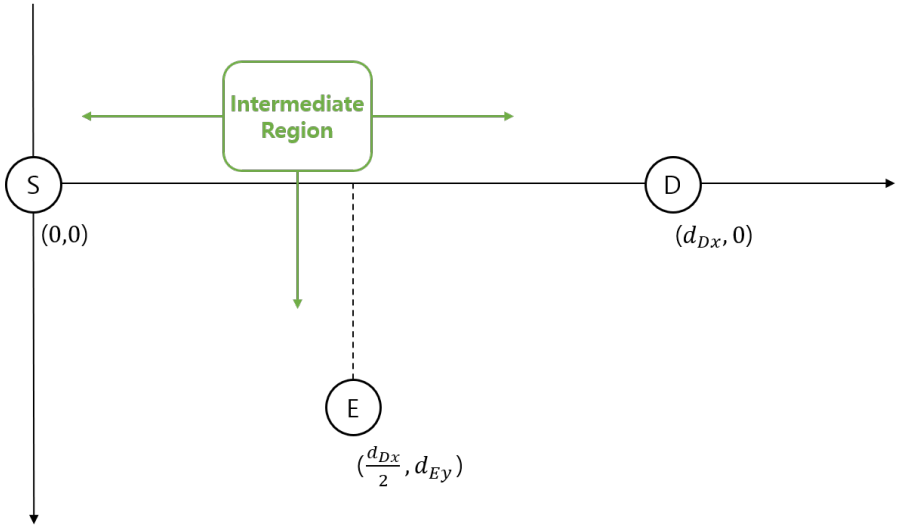



Figure 2.4: Illustration of the network topology in simulations.

The network topology used in the simulations is described in Fig.2.4. All nodes are deployed in a 2-Dimensional space while the source node is placed at the origin point of $(0, 0)$. The destination node and the eavesdropper node are positioned at

$(d_{\mathrm{D}_x}, 0)$ and $(\frac{d_{\mathrm{D}x}}{2}, d_{\mathrm{E}_y})$, respectively. The center of the intermediate region of which shape is the circle whose radius is $r_{\mathrm{I}}$ is placed at $(d_{\mathrm{I}_x}, d_{\mathrm{I}_y})$. For the fixed positions of the source node, the destination node, the eavesdropper node and the intermediate region, the simulation is iterated 10000 times. Moreover, for each iteration of the simulation, the intermediate nodes are placed randomly inside the intermediate region. All channel coefficients are generated based on the COST 207 Typical Urban channel model with 6 multi-path. The pathloss exponent of all channels is set as $4$. Delay and power information of 6 multi-path used for generating the channel coefficients is given by $\{0, 0.2, 0.5, 1.6, 2.3, 5.0\}$ and $\{0.189, 0.379, 0.239, 0.095, 0.061, 0.037\}$, respectively. In addition, the noise variance $\sigma^2$ is given by $\mathcal{N}_0 W$ where $\mathcal{N}_0$ is a noise spectral density and $W$ is a bandwidth of a single sub-carrier. Thus, the total noise power is determined by $N\sigma^2$. For all simulations, I assume that $W$ is 300kHz and the total system power and the total noise power are represented at once by the system SNR which is given by

$$p'_{\text{tot}} = \frac{p_{\text{tot}}}{N\sigma^2}$$

Fig.2.5 shows the security performance of each power allocation in the situation when the center of the intermediate region moves from $(\frac{d_{\mathrm{D}x}}{4}, 0)$ to $(\frac{3d_{\mathrm{D}x}}{4}, 0)$ with $d_{\mathrm{D}_x} = 1$, $d_{\mathrm{E}_y} = 0.5$, $r_{\mathrm{I}} = 0.05$, and $p'_{\text{tot}} = 0$dB. In Fig. 2.5, it is shown that the performance of the proposed power allocation is outstanding compared to other power allocations except for sub-optimal power allocation scheme. The performance gap between the proposed one and the sub-optimal one is very small. This performance gap between the two power allocations is relatively large when the intermediate node region is more far from the destination node than from the eavesdropper node. This is because the proposed power allocation experiences less the security deterioration than the sub-optimal one in the most cases in which the channel from the intermediate nodes to the destination node is worse than that to the eavesdropper node. In addition, it is noticeable that, in the uniform power allocation, the security performance of the optimal power distribution is maximum when the intermediate region is at seven of

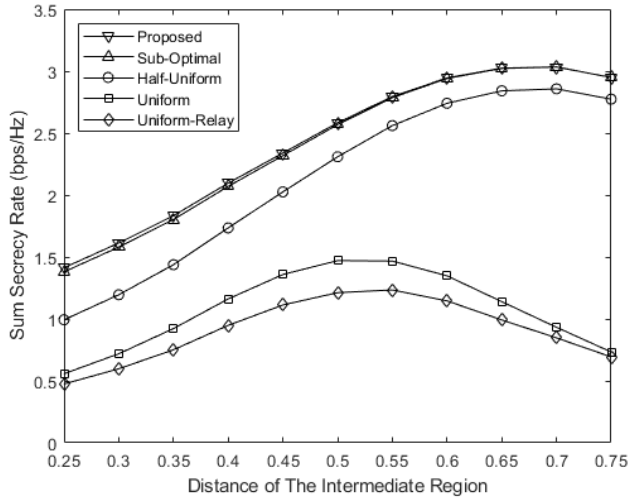



Figure 2.5: The sum secrecy rate when the center of intermediate region moves from $(\frac{d_{\mathrm{D}x}}{4}, 0)$ to $(\frac{3d_{\mathrm{D}x}}{4}, 0)$ with $d_{\mathrm{D}_x} = 1$, $d_{\mathrm{E}_y} = 0.5$, $p'_{\mathrm{tot}} = 0$dB.

tenths between the source node and the destination node. On the other hand, the uniform power distribution represents the maximum performance when the intermediate region is positioned in the vicinity of the middle between the source node and the destination node. From these results, I can know that the secrecy rate can be maximized at the position biased toward the destination node rather than the balanced position between the source node and the destination node.

Fig. 2.6 shows the security performance of each power allocation in the situation when the center of the intermediate region moves from $(\frac{d_{\mathrm{D}x}}{2}, 0)$ to $(\frac{d_{\mathrm{D}x}}{2}, \frac{d_{\mathrm{E}y}}{2})$ with $d_{\mathrm{D}_x} = 1$, $d_{\mathrm{E}_y} = 0.5$, $r_{\mathrm{I}} = 0.05$, and $p'_{tot} = 0$dB. Similar to Fig. 2.5, it is shown that the proposed power allocation represents the best performance compared to other power allocation schemes except for the sub-optimal power allocation. In addition, the performance gap between the proposed power allocation and the sub-optimal one is observed more clearly than in Fig. 2.5. This is because that the probability that the channel from the intermediate nodes to the destination node is worse than that

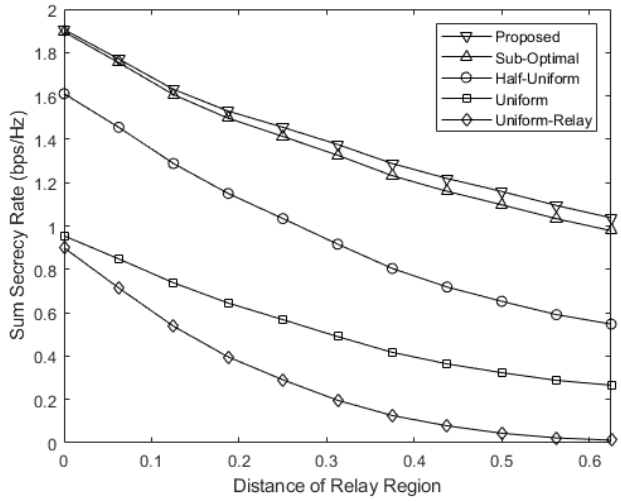



Figure 2.6: The sum secrecy rate when the center of intermediate region moves from $(\frac{d_{\mathrm{D}x}}{2}, 0)$ to $(\frac{d_{\mathrm{D}x}}{2}, \frac{d_{\mathrm{E}y}}{2})$ with $d_{\mathrm{D}x} = 1$, $d_{\mathrm{E}y} = 0.5$, $\mathrm{P}'_{tot} = 0$dB.

to the eavesdropper node is much higher than the former case as the intermediate region gets close to the eavesdropper node. Thus, there are many more cases in which the proposed power allocation outperforms the sub-optimal one in terms of the sum secrecy rate. Moreover, it is observed that the security performance of the uniform power distribution with no cooperative jamming is more rapidly decreasing than that of the uniform power distribution with the cooperative jamming as the intermediate region moves toward the eavesdropper node. This implies that the cooperative jamming affects significantly in the performance when the channel state from the relay node to the destination node is much harsher than that to the eavesdropper node.

In Fig. 2.7, it is shown that the security performance of each power allocation versus the system SNR in the situation where the center of the intermediate region is $(\frac{d_{\mathrm{D}x}}{2}, 0)$, $d_{\mathrm{D}x} = 1$, $d_{\mathrm{E}y} = 0.5$, and $r_{\mathrm{I}} = 0.05$. Fig. 2.7 shows that all security performances are increasing as the system SNR grows gradually. Like as the previous cases, the proposed power allocation and the sub-optimal power allocation represent almost

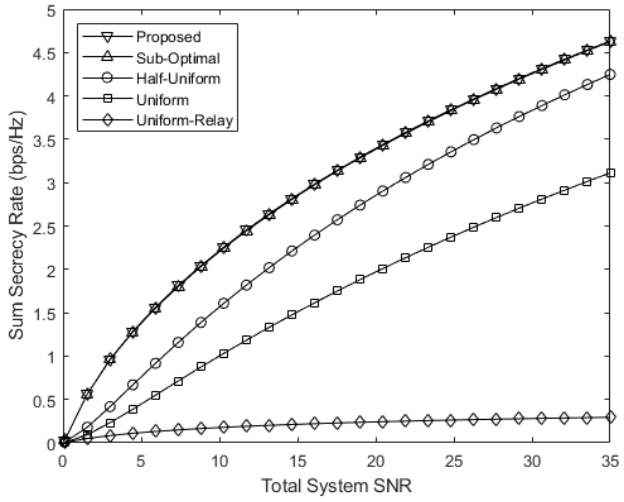



Figure 2.7: The sum secrecy rate versus the total system SNR where the center of the intermediate region is $(\frac{d_{\mathrm{D}x}}{2}, 0)$, $d_{\mathrm{D}x} = 1$, $d_{\mathrm{E}y} = 0.5$.

same security performances and they outperform other power allocations. On the one hand, it is shown that the performance of the uniform power allocation with the optimal power distribution is being close to that of the proposed power allocation decreases as the total SNR is increasing. This stems from that, at the high available power, all achievable secrecy rate functions have almost same function shapes as shown in (2.33). Thus, in the situation that a enough high power is allocated to each sub-carrier, the optimal power of each sub-carrier obtained by the KKT conditions is almost same as one another. In other words, the optimal power allocation converges into the uniform power allocation as the total system power grows increasingly.

Fig. 2.8 plots the security performance of each power allocation scheme corresponding to the number of the intermediate nodes. The total system SNR is given by 0dB and other simulation settings are same as the former one which used for representing Fig. 2.7. I can show that all security performances are getting higher as the total system SNR is increasing gradually. This implies that many number of the interme-

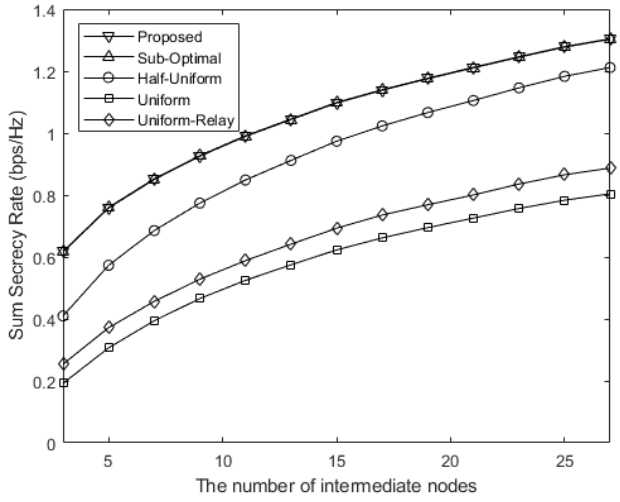



Figure 2.8: The sum secrecy rate ersus the number of intermediate nodes inside the intermediate region where the center of the intermediate region is $(\frac{d_{\mathrm{D}x}}{2}, 0)$, $d_{\mathrm{D}x} = 1$, $d_{\mathrm{E}y} = 0.5$.

diate nodes can provide a high probabilities to establish a good channel link between the relay node and the destination node and to form a fine ZF beamforming weight for the jamming nodes. Furthermore, in the situation of the good relay channel link and the fine ZF beamforming, each achievable secrecy rate function is approximated to (2.33) at the relatively low power. Therefore, similarly to Fig. 2.7, the performance of the uniform power allocation with the optimal power allocation approaches slowly to that of the proposed power allocation when the number of the intermediate nodes increases.

From Fig. 2.5-2.8, one can see that the proposed power allocation scheme outperforms other power allocation schemes except for the optimal power allocation scheme. Even though performances two schemes is not same exactly, in figure 5-8, it can be seen that the performance of the proposed power allocation scheme is very close to that of the optimal power allocation scheme and the performance gap between two

schemes is almost zero.

## 2.6 Summary

In this paper, I proposed the efficient power allocation scheme for multi-node the multi-carrier network. First, I suggested the adaptive cooperative transmission scheme and found optimal power distribution for the transmit power, the relay power and the jamming power at each sub-carrier. In next, I established the optimal power allocation problem over all sub-carriers. In the process, it was shown that the optimal power allocation problem was not straightforward to be solved and required unaffordable computation for finding solution. For this reason, instead of the optimal power allocation, I derived the sub-optimal power allocation whose security performance is asymptotically same as that of the optimal power allocation when the number of sub-carriers or intermediate nodes goes infinity. Nevertheless, since there is still high computational complexity to find the sub-optimal power allocation, I proposed the efficient power allocation whose required computation is relatively very low using the dominant shape approximation method. Furthermore, to mitigate performance drop by the dominant shape approximation method, I considered another power allocation obtained easily by modifying the efficient power allocation. Ultimately, the proposed power allocation was determined as better one among two power allocations. Through various numerical results, it is shown that the proposed power allocation is superior than other benchmark power allocation and some useful facts as follows; 1) when the intermediate region is closer to the eavesdropper node than to the destination node, the performance of the proposed power allocation is closer to that of the optimal power allocation than that of the sub-optimal power allocation; 2) when the system can provide a enough large power into each sub-carrier, the optimal power allocation is almost same as the uniform power allocation; 3) the more the number of intermediate nodes inside the intermediate region, the higher security performance of PLS is.

# Chapter 3

# Proactive Eavesdropping with Adaptive Full-duplex Jamming-Helping Method for Infrastructure-free Relay Networks

## 3.1 Motivation

The proactive eavesdropping method was first proposed by [19, 20] and [21]. In proactive eavesdropping, unlike conventional PLS, a legitimate "eavesdropper", authorized by legitimate organizations such as government agencies, is deployed and act as the supervisor of the network. Moreover, communication users are considered as suspicious users which have the potential to utilize communication links for malicious purpose. Therefore, for successful proactive eavesdropping, communication networks have to guarantee that the legitimate eavesdropper can always succeed in wiretapping suspicious users. This concept is directly contrary to the concept of conventional PLS in which communication networks have to prevent the eavesdropper from wiretapping communication users.

In order to achieve the goal of proactive eavesdropping, communication networks have to experience failure in terms of conventional PLS. In other words, the achievable rate at the legitimate eavesdropper must be larger than that at the suspicious user. This

implies that the performance of proactive eavesdropping highly depends on channel conditions of communication networks as conventional PLS was. For overcoming this channel dependency issue, in [20, 21], the legitimate eavesdropper used full-duplex jamming method to degrade the achievable rate for the suspicious user. In succession to [20, 21], many studies also proposed proactive eavesdropping approaches with the jamming method. References [22] and [23] extended the works of [20, 21] to multi-antenna scenarios from the scenario in which the legitimate eavesdropper is equipped with a single antenna. In addition, they designed beamforming vectors for minimizing the eavesdropping outage probability and for maximizing the eavesdropping rate, respectively. The work in [24] proposed the alternate-jamming-aided protocol where the two half-duplex monitor nodes operate cooperatively to imitate operation method of the full-duplex monitor node for avoiding the imperfect self-interference cancellation. Reference [25] designed the proactive eavesdropping system which improves the eavesdropping performance by using the secondary user as the jamming signal in cognitive radio networks. In [26], the proactive eavesdropping scenario where there exists multiple suspicious communication links was considered, and accordingly, the optimization problem for maximizing the average eavesdropping rate or the average successful eavesdropping probability over all suspicious links was introduced. Reference [27] is the first study considering the channel training phase in which the channel coefficient is estimated, and investigated the jamming strategy for two phases of the data transmission phase and the channel training phase. The work in [28] investigated the beamformer optimization and the antenna selection problem for the full-duplex multi-antenna monitor node, and analyzed the trade off between performance and complexity to provide design choice flexibility.

In [29, 30, 31, 32, 33, 34, 35, 36, 37], proactive eavesdropping via jamming approaches were studied in two-hop relay networks in which a relay node can support communications between suspicious users. The work in [29] presented the initial investigation of the proactive eavesdropping approach in the two-hop communication

network and proposed three eavesdropping methods from which the supervisor can adaptively choose depending on the channel conditions. In [30], a half-duplex eavesdropper, which can act as a jammer or a relay adaptively, was introduced and two strategies for maximizing the eavesdropping rate was proposed. Reference [31] considered the two-hop amplify-and-forward (AF) relay network and designed the jamming power for maximizing the average eavesdropping rate. The study in [32] introduced the scenario in which there are multiple full-duplex relays and a single cooperative jammer to help the legitimate eavesdropper intercept the signal exchanged between suspicious users and designed the combining vector and the relay precoders to maximize the eavesdropping rate. In [33], two half-duplex cooperative eavesdroppers were introduced to maximize the eavesdropping energy efficiency. Reference [34] considered the scenario where there are multiple intermediate nodes which can operate in either eavesdropping or jamming mode and optimized the mode selection and transmit power at each intermediate node to obtain the maximum eavesdropping rate. The work in [35] designed two proactive strategies and analyzed about which one between the two designed strategies is more preferable in the scenario where two suspicious nodes exchanges their data through the relay node. Reference [36] considered the multichannel decode-and-forward (DF) relay system and presented the fundamental trade-off between the given jamming power and the precondition probability for successful eavesdropping through numerical results. In [37], the problem of mode selection and the optimal power allocation for the monitor node were investigated in the multichannel DF relay network, and, to reduce complexity, a sub-optimal algorithm was proposed and verified via simulation results.

Further, recent proactive eavesdropping studies [38, 39] have considered characteristics of the infrastructure-free network in the general relay communication system model. In [38], the scenario where the monitor node eavesdrops suspicious multi-users in an UAV network was considered, and the optimization problem for maximizing the sum eavesdropping rate over all suspicious users was formulated and solved. The

work of [39] proposed the proactive eavesdropping method which exploits the two predetermined strategies for the UAV relay network, and investigated the optimal jamming power of the monitor node to maximize the eavesdropping rate. However, [38] lacks a consideration about relay communications which is a important property of the infrastructure-free network. The study of [39] also has limitations in that the monitor node could utilize only the two predetermined strategies and the direct link between the suspicious transmitter and the suspicious destination is ignored for simplicity of the optimization problem even though it cannot be in practice. Motivated by these, in this paper, I present a system model for the general infrastructure-free communication network scenario. Furthermore, to enhance the performance of proactive eavesdropping, I propose a novel adaptive full-duplex jamming-helping method and design an optimal power scheme for the proposed method. The main contributions of this paper are:

1) I consider the general infrastructure-free two-hop communication scenario where the legitimate eavesdropper is an independent node which operates separately with relay nodes, that is, the legitimate eavesdropper cannot cooperate with relay nodes. In our system model, to improve the proactive eavesdropping performance, I also propose the adaptive full-duplex jamming-helping method in which the legitimate eavesdropper node can select its own operation mode adaptively while eavesdropping the suspicious communication link.

2) I also design the optimal power scheme for the proposed method. The optimal power scheme is given by the solution of the optimization problem for maximizing the eavesdropping rate of the monitor node in the suspicious communication link under the successful proactive eavesdropping constraint. In order to make the optimization problem straightforward, I present five mutually exclusive cases by classifying channel conditions. Subsequently, for each case, I obtain the optimal power scheme in closed form by solving the simplified problem.

3) I introduce the additional optimization problem to minimize total power consumption of the monitor node since the optimal power scheme can be given by not an unique solution but a set of solutions. By solving the additional optimization problem, the optimal power scheme is determined as the unique solution which maximizes the eavesdropping rate while minimizing total power consumption.

4) Through various numerical results, I verify that the proposed method with the designed optimal power scheme is superior than the existing methods presented in conventional studies both in terms of the eavesdropping rate and the total power consumption.

## 3.2 System Model

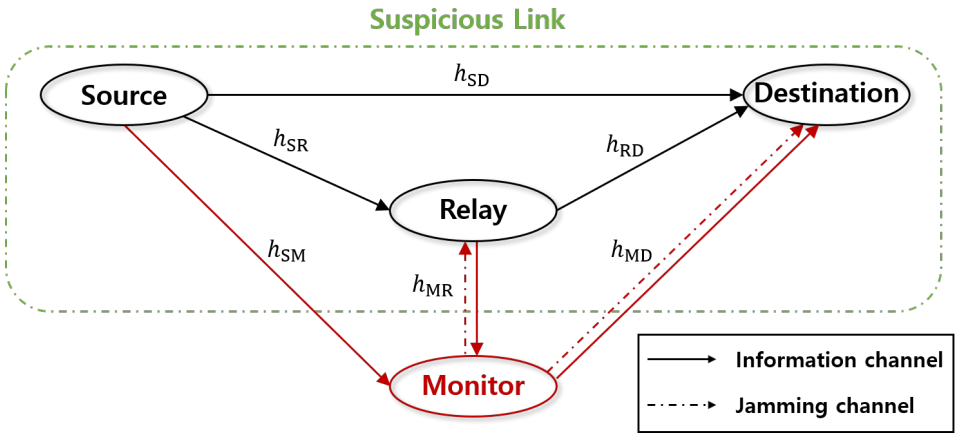



Figure 3.1: Description of the two-hop DF relay network topology

### 3.2.1 Network Topology

I consider a two-hop relay infrastructure-free network where a suspicious communication link exists as shown in Fig.3.1. The suspicious communication link consists of

a source node, a relay node, and a destination node. The relay node is driven by the source node and helps a signal transmission the source node by forwarding the transmitted signal to the destination node. All nodes in the suspicious link are assumed to be equipped with a single antenna. On the other hand, the monitor node M is equipped with two antennas to operate in full-duplex mode. In addition, I assume that all nodes in the suspicious link is not aware of the presence of the monitor node [29]. This assumption is practical because the monitor node is mainly used by a high-level user such as supervisors and government agencies. Thus, the monitor node can access the global channel state information (CSI) without being exposed to the suspicious nodes [30]. It is also assumed that all nodes have mobility, that is, they can move freely inside the network. In Fig.3.1, $h_{\mathrm{XY}}$ denotes the channel coefficient of the link between node X and node Y. For instance, $h_{\mathrm{SR}}$ means the channel coefficient of the link between a source node S and a relay node R in the suspicious communication link. All links of the network are assumed to involve additive white Gaussian noise (AWGN) and accordingly, the channel noise of each link is modeled as a zero-mean Gaussian random variable with variance $\sigma^2$ implying the noise power.

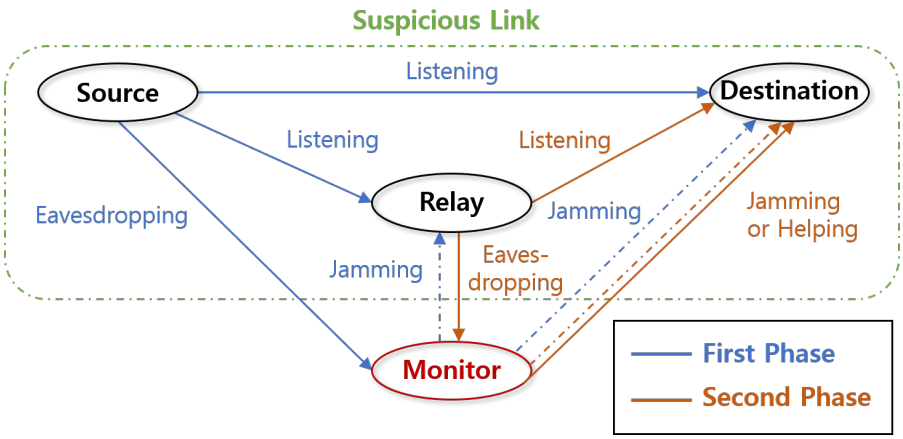



Figure 3.2: Graphical description of the time-sharing protocol

### 3.2.2 Time-sharing Protocol

In the suspicious communication link, the source node S transmits the signal to a destination node D with the aid of the relay node R which operates in DF method. Thus, the relay node receives and decodes the signal transmitted from the the source node and forwards that signal to the destination node. Meanwhile, the monitor node M eavesdrops the signal traveling from the source node to the destination node for surveillance purposes. In order to enhance surveillance performance, I introduce the monitor node operating in the adaptive full-duplex jamming-helping method. In that method, the monitor node can adaptively determine to either jam or help the signal transmission of the suspicious link while eavesdropping the signal. Moreover, I assume that a perfect self-interference cancellation method in the hardware domain is applied such that there is no self-interference at the monitor node. This whole process is conducted based on the time-sharing protocol [40], in which two time slots are spent for one signal to be transmitted to the destination node. This process is described graphically in Fig.3.2.

As shown in Fig.3.2, in the first phase, the source node S transmits the signal to the destination node D and the relay node R. Simultaneously, the monitor node M emits artificial noise to prevent the relay node and the destination node from receiving the signal while eavesdropping the signal transmitted at the source node. Next, in the second phase, the relay node forwards the signal to the destination node. At the same time, depending on the channel conditions, the monitor node selects adaptively its own operating mode between two modes: jamming mode and helping mode. If the monitor node obtains the perfect information of the signal in the first phase, there is no need for the monitor node to perform jamming in the second phase. In this case, it is best that the monitor node helps the signal transmission of the suspicious communication link so that the monitor node can eavesdrop more information. Therefore, the monitor node operates in the helping mode and forwards the received signal to the destination node as the relay node does. On the other hand, if the monitor node cannot get the whole information of the signal in the first phase, the monitor node needs to gather

more information by eavesdropping the signal forwarded from the relay node in the second time phase. In this case, it is the best decision that the monitor node eavesdrops the signal transmitted from the relay node while preventing the destination node from receiving the signal. Finally, the destination node and the monitor node obtain the signal information by combining the received signals during two phases, that is, using the maximum ratio combining (MRC) method.

### 3.2.3 Achievable Rate

The received signal at the relay node R in the first phase can be expressed as

$$r_{\mathrm{R}} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_t + \sqrt{q^{(1)}} h_{\mathrm{MR}} s_j + n_{\mathrm{R}}, \tag{3.1}$$

where $s_t$ and $s_j$ denote the normalized signal transmitted at the source node S and the normalized jamming signal emitted at the monitor node M, respectively. In addition, $P_{\mathrm{S}}$, $q^{(1)}$ and $n_{\mathrm{R}}$ denote the transmit power of the source node, the power which the monitor node spends for jamming in the first phase, and AWGN at the relay node, respectively. Therefore, the rate function of the relay node R is defined as

$$\mathcal{R}_{\mathrm{R}}(q^{(1)}) := \log_2 \left( 1 + \frac{\alpha_{\mathrm{SR}} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{MR}} q^{(1)}} \right), \tag{3.2}$$

where $\alpha_{\mathrm{XY}} := \frac{|h_{\mathrm{XY}}|^2}{\sigma^2}$.

The received signal at the monitor node M in the first phase can be expressed as

$$r_{\mathrm{M}}^{(1)} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SM}} s_t + n_{\mathrm{M}}^{(1)}, \tag{3.3}$$

where $n_{\mathrm{M}}^{(1)}$ denotes AWGN at the monitor node M in the first phase. Then, the rate of the monitor node M for the first phase is given by

$$\mathcal{R}_{\mathrm{M}} = \log_2 \left( 1 + \alpha_{\mathrm{SM}} P_{\mathrm{S}} \right), \tag{3.4}$$

Moreover, the received signal at the monitor node M in the second phase can be expressed as

$$r_{\mathrm{M}}^{(2)} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{MR}} s_t + n_{\mathrm{M}}^{(2)}, \tag{3.5}$$

where $P_{\mathrm{R}}$ and $n_{\mathrm{M}}^{(2)}$ denote the relay power of the relay node and AWGN at the monitor node M in the second phase. By the MRC method, the achievable rate of the monitor node M for two phases is given by

$$\mathcal{C}_{\mathrm{M}} = \log_2 \{1 + \lambda_{\mathrm{M}} P_{\mathrm{S}}\}. \tag{3.6}$$

where $\lambda_{\mathrm{M}} := \alpha_{\mathrm{SM}} + \rho\alpha_{\mathrm{MR}}$, and $\rho := \frac{P_{\mathrm{R}}}{P_{\mathrm{S}}}$.

Furthermore, the received signal at the destination node D in the first phase can be expressed as

$$r_{\mathrm{D}}^{(1)} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SD}} s_t + \sqrt{q^{(1)}} h_{\mathrm{MD}} s_j + n_{\mathrm{D}}^{(1)}, \tag{3.7}$$

where $n_{\mathrm{D}}^{(1)}$ denotes AWGN at the destination node in the first phase. The received signal at the destination node D in the second phase can also be expressed as

$$r_{\mathrm{D}}^{(2)} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{RD}} s_t + \sqrt{q^{(2)}} h_{\mathrm{MD}} s_{\mathrm{M}} + n_{\mathrm{D}}^{(2)}, \tag{3.8}$$

where $q^{(2)}$ and $n_{\mathrm{D}}^{(2)}$ denote the power which the monitor node spends for its operating mode in the second phase and AWGN at the destination node in the second phase, respectively. Moreover, $s_{\mathrm{M}}$ denotes the adaptive signal transmitted at the monitor node M in the second phase, which is given by

$$s_{\mathrm{M}} = \begin{cases} s_j, & \text{if } \mathcal{R}_{\mathrm{M}} < \mathcal{R}_{\mathrm{R}}(q^{(1)}), \\ s_t, & \text{if } \mathcal{R}_{\mathrm{M}} \geq \mathcal{R}_{\mathrm{R}}(q^{(1)}). \end{cases} \tag{3.9}$$

Equation (3.9) shows the helping mode condition in which the monitor node operates in the helping mode. This implies that, in the first phase, the monitor node can correctly decode the whole information of the received signal only if the rate of the monitor node is higher than the rate of the relay node. Then, the rate function of the destination node D for two phases is defined as

$$\mathcal{R}_{\mathrm{D}}(\boldsymbol{q}) := \begin{cases} \mathcal{R}_{\mathrm{DJ}}(\boldsymbol{q}), & \text{if } \mathcal{R}_{\mathrm{M}} < \mathcal{R}_{\mathrm{R}}(q^{(1)}), \\ \mathcal{R}_{\mathrm{DH}}(\boldsymbol{q}), & \text{if } \mathcal{R}_{\mathrm{M}} \geq \mathcal{R}_{\mathrm{R}}(q^{(1)}), \end{cases} \tag{3.10}$$

where $\boldsymbol{q} := (q^{(1)}, q^{(2)}) \in \mathbb{R}^2$, and $\mathbb{R}$ denotes the set of real numbers. In addition, $\mathcal{R}_{\mathrm{DJ}}(\cdot)$ and $\mathcal{R}_{\mathrm{DH}}(\cdot)$ are the rate functions of the destination node D for the jamming mode and the helping mode, respectively, and they are defined as

$$\mathcal{R}_{\mathrm{DJ}}(\boldsymbol{q}) := \log_2\left(1 + \frac{\alpha_{\mathrm{SD}} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{MD}} q^{(1)}} + \frac{\rho \alpha_{\mathrm{RD}} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{MD}} q^{(2)}}\right),$$

$$\mathcal{R}_{\mathrm{DH}}(\boldsymbol{q}) := \log_2\left(1 + \frac{\alpha_{\mathrm{SD}} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{MD}} q^{(1)}} + \mathcal{S}_{\mathrm{DH}}(q^{(2)})\right),$$

where $\mathcal{S}_{\mathrm{DH}}(\cdot)$ is the received signal power function at the destination node for the helping mode, which is defined as

$$\mathcal{S}_{\mathrm{DH}}(x) := \left|\sqrt{\rho \alpha_{\mathrm{RD}} P_{\mathrm{S}}} + \sqrt{\alpha_{\mathrm{MD}} x}\right|^2.$$

Consequently, the achievable rate function of the destination node D for two phases is given by [16]

$$\mathcal{C}_{\mathrm{D}}(\boldsymbol{q}) := \begin{cases} \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q}), & \text{if } \mathcal{R}_{\mathrm{M}} < \mathcal{R}_{\mathrm{R}}(q^{(1)}), \\ \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}), & \text{if } \mathcal{R}_{\mathrm{M}} \geq \mathcal{R}_{\mathrm{R}}(q^{(1)}), \end{cases} \tag{3.11}$$

where $\mathcal{C}_{\mathrm{DJ}}(\cdot)$ and $\mathcal{C}_{\mathrm{DH}}(\cdot)$ are the achievable rate function of the destination node D for the jamming mode and the helping mode, respectively, and they are defined as

$$\mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q}) := \min\Big(\mathcal{R}_{\mathrm{R}}(q^{(1)}), \mathcal{R}_{\mathrm{DJ}}(\boldsymbol{q})\Big),$$

$$\mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}) := \min\Big(\mathcal{R}_{\mathrm{R}}(q^{(1)}), \mathcal{R}_{\mathrm{DH}}(\boldsymbol{q})\Big).$$

## 3.3 Optimal Power Design

### 3.3.1 Maximizing Eavesdropping Rate

In this section, I design the optimal power allocation scheme for the monitor node M to maximize the eavesdropping rate. Under the successful eavesdropping condition in which the achievable rate of the monitor node is higher or equal to that of the destination node D, the monitor node can obtain perfect information of the signal transmitted at the source node S. Otherwise, if the successful eavesdropping condition

is not met, the monitor node cannot obtain any information from the received signals since it cannot decode the signals correctly, which is called "outage". Therefore, the eavesdropping rate function of the monitor node M during two phases is given by

$$\mathcal{E}_{\mathrm{M}}(\boldsymbol{q}) = \begin{cases} \mathcal{C}_{\mathrm{D}}(\boldsymbol{q}), & \text{if } \mathcal{C}_{\mathrm{M}} \geq \mathcal{C}_{\mathrm{D}}(\boldsymbol{q}), \\ 0, & \text{if } \mathcal{C}_{\mathrm{M}} < \mathcal{C}_{\mathrm{D}}(\boldsymbol{q}). \end{cases} \tag{3.12}$$

Then, the optimization problem for maximizing the eavesdropping rate is defined as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{E}_{\mathrm{M}}(\boldsymbol{q}) \\ \text{s.t.} \quad & q^{(1)} \geq 0,\ q^{(2)} \geq 0, \\ & q^{(1)} + q^{(2)} \leq Q_{\max}, \end{aligned} \tag{3.13}$$

where $Q_{\max}$ is the maximum available power for the monitor node.

Table 3.1: The five cases of channel conditions

| Channel Conditions | | | | *Case* # |
|---|---|---|---|---|
| $\alpha_{\mathrm{SM}} \geq \alpha_{\mathrm{SR}}$ | $\alpha_{\mathrm{SR}} < \alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}}$ | | | *Case* 1 |
| | $\alpha_{\mathrm{SR}} \geq \alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}}$ | | | *Case* 2 |
| $\alpha_{\mathrm{SM}} < \alpha_{\mathrm{SR}}$ | $\alpha_{\mathrm{SM}} \geq \alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}}$ | | | *Case* 3 |
| | $\alpha_{\mathrm{SM}} < \alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}}$ | $\alpha_{\mathrm{SM}} + \rho\alpha_{\mathrm{MR}} \geq \alpha_{\mathrm{SR}}$ | | *Case* 4 |
| | | $\alpha_{\mathrm{SM}} + \rho\alpha_{\mathrm{MR}} < \alpha_{\mathrm{SR}}$ | $\alpha_{\mathrm{SM}} + \rho\alpha_{\mathrm{MR}} \geq \alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}}$ | *Case* 4 |
| | | | $\alpha_{\mathrm{SM}} + \rho\alpha_{\mathrm{MR}} < \alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}}$ | *Case* 5 |

*Case* 1: The successful eavesdropping condition ($\mathcal{C}_{\mathrm{M}} \geq \mathcal{C}_{\mathrm{D}}(\boldsymbol{q})$) is always satisfied regardless of the values of $q^{(1)}$ and $q^{(2)}$. In addition, the helping mode condition ($\mathcal{R}_{\mathrm{M}} \geq \mathcal{R}_{\mathrm{R}}(q^{(1)})$) is always satisfied regardless of the value of $q^{(1)}$. Accordingly,

(3.13) can be transformed to

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}) \\ \text{s.t.} \quad & q^{(1)} \geq 0,\ q^{(2)} \geq 0, \\ & q^{(1)} + q^{(2)} \leq Q_{\max}. \end{aligned}$$

In *Case* 1, both $\mathcal{R}_{\mathrm{DH}}(\cdot)$ and $\mathcal{R}_{\mathrm{R}}(\cdot)$ are decreasing as $q^{(1)}$ increases. This implies that $\mathcal{C}_{\mathrm{DH}}(\cdot)$ is also decreasing when $q^{(1)}$ is increasing. Therefore, the optimal $q^{(1)}$ is determined as the smallest value, i.e. zero. Further, $\mathcal{R}_{\mathrm{R}}(0)$ is always smaller than $\mathcal{R}_{\mathrm{DH}}(0, q^{(2)})$ regardless of the value of $q^{(2)}$. Then, the solution set of (3.13) for *Case* 1 is just given by

$$T_1 := \left\{ \boldsymbol{q} \,|\, q^{(1)} = 0,\ 0 \leq q^{(2)} \leq Q_{\max} \right\}. \tag{3.14}$$

*Case* 2: For the same reason as *Case* 1, the monitor node operates in the helping mode and the optimal $q^{(1)}$ is determined as zero. Thus, (3.13) is transformed to

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}) \\ \text{s.t.} \quad & q^{(1)} = 0,\ 0 \leq q^{(2)} \leq Q_{\max}. \end{aligned}$$

Moreover, at $q^{(1)} = 0$, $\mathcal{C}_{\mathrm{DH}}(\cdot)$ is expressed as

$$\mathcal{C}_{\mathrm{DH}}(0, q^{(2)}) = \begin{cases} \mathcal{R}_{\mathrm{DH}}(0, q^{(2)}), & \text{if } 0 \leq q^{(2)} < Q_{2,\mathrm{thr}}, \\ \mathcal{R}_{\mathrm{R}}(0), & \text{if } q^{(2)} \geq Q_{2,\mathrm{thr}}, \end{cases}$$

where $Q_{2,\mathrm{thr}}$ is determined as $x$ such that $\mathcal{R}_{\mathrm{DH}}(0, x) = \mathcal{R}_{\mathrm{R}}(0)$ and is given by

$$Q_{2,\mathrm{thr}} = \frac{1}{\alpha_{\mathrm{MD}}} \left( \sqrt{(\alpha_{\mathrm{SR}} - \alpha_{\mathrm{SD}})} - \sqrt{(\rho \alpha_{\mathrm{RD}})} \right)^2 P_{\mathrm{S}}.$$

Since $\mathcal{R}_{\mathrm{DH}}(0, q^{(2)})$ is strictly increasing as $q^{(2)}$ increases, the solution set of (3.13) for *Case* 2 is given by

$$T_2 = \begin{cases} \{(0, Q_{\max})\}, & \text{if } 0 \leq Q_{\max} < Q_{2,\mathrm{thr}}, \\ \left\{ \boldsymbol{q} \,|\, q^{(1)} = 0, \right. \\ \left. Q_{2,\mathrm{thr}} \leq q^{(2)} \leq Q_{\max} \right\}, & \text{if } Q_{\max} \geq Q_{2,\mathrm{thr}}. \end{cases} \tag{3.15}$$

*Case* 3: The successful eavesdropping condition is always satisfied regardless of the values of $q^{(1)}$ and $q^{(2)}$. However, unlike *Case* 1 or *Case* 2, the monitor node can operate in the jamming mode as well as the helping mode depending on the value of $q^{(1)}$. That is, in *Case* 3, (3.11) can be transformed to

$$\mathcal{C}_{\mathrm{D}}(\boldsymbol{q}) := \begin{cases} \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q}), & \text{if } q^{(1)} < q_{\mathrm{thr}}^{(1)}, \\ \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}), & \text{if } q^{(1)} \geq q_{\mathrm{thr}}^{(1)}, \end{cases} \tag{3.16}$$

where $q_{\mathrm{thr}}^{(1)}$ denotes the threshold power for the monitor node to operate in the helping mode and is obtained by solving the equation of $\mathcal{R}_{\mathrm{M}} = \mathcal{R}_{\mathrm{R}}(q_{\mathrm{thr}}^{(1)})$. It is given by

$$q_{\mathrm{thr}}^{(1)} = \frac{1}{\alpha_{\mathrm{MR}}} \left( \frac{\alpha_{\mathrm{SR}}}{\alpha_{\mathrm{SM}}} - 1 \right).$$

Then, based on (3.16), I divide the optimization problem to two sub-problems by distinguishing its own feasible set into two mutually exclusive subsets. In other words, (3.13) separates into two individual optimization problems depending on the operating mode of the monitor node. The first sub-problem is expressed as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q}) \\ \text{s.t.} \quad & 0 \leq q^{(1)} < q_{\mathrm{thr}}^{(1)},\ q^{(2)} \geq 0, \\ & q^{(1)} + q^{(2)} \leq Q_{\max}. \end{aligned}$$

Under constraints of the first sub-problem, the monitor node operates in the jamming mode. From the fact that $\mathcal{C}_{\mathrm{DJ}}(\cdot)$ is strictly decreasing when either or both of $q^{(1)}$ and $q^{(2)}$ is increasing, I can easily know that the solution set of the first sub-problem is simply determined as

$$T_{3,\mathrm{sub1}} = \{(0,0)\}. \tag{3.17}$$

On the one hand, the second sub-problem is expressed as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}) \\ \text{s.t.} \quad & q^{(1)} \geq q_{\mathrm{thr}}^{(1)},\ q^{(2)} \geq 0, \\ & q^{(1)} + q^{(2)} \leq Q_{\max}. \end{aligned}$$

Contrary to the first sub-problem, the monitor node operates in the helping mode. Similarly as in *Case* 1 and *Case* 2, the optimal $q^{(1)}$ is easily determined as the smallest value, i.e. $q_{\text{thr}}^{(1)}$. At $q^{(1)} = q_{\text{thr}}^{(1)}$, $\mathcal{C}_{\text{DH}}(\cdot)$ is expressed as

$$\mathcal{C}_{\text{DH}}(q_{\text{thr}}^{(1)}, q^{(2)}) = \begin{cases} \mathcal{R}_{\text{DH}}(q_{\text{thr}}^{(1)}, q^{(2)}), & \text{if } 0 \le q^{(2)} \\ & \text{and } q^{(2)} < q_{3,\text{thr1}}^{(2)}, \\ \mathcal{R}_{\text{R}}(q_{\text{thr}}^{(1)}), & \text{if } q^{(2)} \ge q_{3,\text{thr1}}^{(2)}, \end{cases}$$

where $q_{3,\text{thr1}}^{(2)}$ is determined as $x$ such that $\mathcal{R}_{\text{DH}}(q_{\text{thr}}^{(1)}, x) = \mathcal{R}_{\text{R}}(q_{\text{thr}}^{(1)})$ and is given by

$$q_{3,\text{thr1}}^{(2)} = \frac{1}{\alpha_{\text{MD}}} \left( \sqrt{(\alpha_{\text{SM}} - \beta)} - \sqrt{(\rho \alpha_{\text{RD}})} \right)^2 P_{\text{S}},$$

where $\beta := \frac{\alpha_{\text{MR}} \alpha_{\text{SM}} \alpha_{\text{SD}}}{\alpha_{\text{MR}} \alpha_{\text{SM}} + \alpha_{\text{MD}} (\alpha_{\text{SR}} - \alpha_{\text{SM}})}$. Since $\mathcal{R}_{\text{DH}}(\cdot)$ is monotonically increasing as $q^{(2)}$ increases, the solution set of the second sub-problem is given as

$$T_{3,\text{sub2}} = \begin{cases} \emptyset, & \text{if } Q_{\max} < q_{\text{thr}}^{(1)}, \\ \left\{ (q_{\text{thr}}^{(1)},\ Q_{\max} - q_{\text{thr}}^{(1)}) \right\}, & \text{if } q_{\text{thr}}^{(1)} \le Q_{\max} \\ & \text{and } Q_{\max} < Q_{3,\text{thr1}} \\ \left\{ \boldsymbol{q} \mid q^{(1)} = q_{\text{thr}}^{(1)}, \right. & \\ \left. q_{3,\text{thr1}}^{(2)} \le q^{(2)} \le Q_{\max} - q_{\text{thr}}^{(1)} \right\}, & \text{if } Q_{\max} \ge Q_{3,\text{thr1}}, \end{cases} \tag{3.18}$$

where $Q_{3,\text{thr1}} := q_{\text{thr}}^{(1)} + q_{3,\text{thr1}}^{(2)}$. It is noticeable that, in the second sub-problem, the solution set exists only if $Q_{\max}$ is not smaller than $q_{\text{thr}}^{(1)}$. This implies that the monitor node necessarily jam the relay node on the first phase to operate in the helping mode. However, if the remain power after jamming is not enough to help the signal transmission, it is not guaranteed that the helping mode is optimal for *Case* 3. Therefore, the best operating mode is decided depending on the value of $Q_{\max}$. That is, at the given $Q_{\max}$, the solution set of (3.13) for *Case* 3 is determined to have a higher eavesdropping rate between (3.17) and (3.18). From the fact that $\mathcal{C}_{\text{DH}}(q_{\text{thr}}^{(1)}, q^{(2)})$ is a monotonically increasing function with respect to $q^{(2)}$, the solution set of (3.13) for *Case* 3 is given by

$$T_3 = \begin{cases} T_{3,\text{sub1}}, & \text{if } 0 \le Q_{\max} < Q_{3,\text{thr2}}, \\ T_{3,\text{sub2}}, & \text{if } Q_{\max} \ge Q_{3,\text{thr2}}, \end{cases}$$

where $Q_{3,\text{thr2}} := q_{\text{thr}}^{(1)} + q_{3,\text{thr2}}^{(2)}$, and $q_{3,\text{thr2}}^{(2)}$ is determined as $x$ such that $\mathcal{C}_{\text{DH}}(q_{\text{thr}}^{(1)}, x) = \mathcal{C}_{\text{DJ}}(0,0)$ and is given by

$$q_{3,\text{thr2}}^{(2)} = \frac{1}{\alpha_{\text{MD}}} \left( \sqrt{(\alpha_{\text{SD}} + t\alpha_{\text{RD}} - \beta)} - \sqrt{(\rho\alpha_{\text{RD}})} \right)^2 P_{\text{S}}.$$

Using (3.17) and (3.18), the solution set can be specifically expressed as

$$T_3 = \begin{cases} \{(0,0)\}, & \text{if } 0 \le Q_{\text{max}} < Q_{3,\text{thr2}}, \\ \left\{ (q_{\text{thr}}^{(1)},\ Q_{\text{max}} - q_{\text{thr}}^{(1)}) \right\}, & \text{if } Q_{3,\text{thr2}} \le Q_{\text{max}} \\ & \text{and } Q_{\text{max}} < Q_{3,\text{thr1}}, \\ \left\{ \boldsymbol{q} \mid q^{(1)} = q_{\text{thr}}^{(1)}, \right. & \\ \left. q_{3,\text{thr1}}^{(2)} \le q^{(2)} \le Q_{\text{max}} - q_{\text{thr}}^{(1)} \right\}, & \text{if } Q_{\text{max}} \ge Q_{3,\text{thr1}}. \end{cases} \tag{3.19}$$

*Case* 4: The same two sub-problems as in *Case* 3 are introduced. Accordingly, their solutions are also given exactly the same as (3.17) and (3.18). However, in *Case* 4, $\mathcal{C}_{\text{DH}}(\boldsymbol{q})$ is always smaller than $\mathcal{C}_{\text{DJ}}(0,0)$ under $\boldsymbol{q} \in T_{3,\text{sub2}}$ unlike *Case* 3. Thus, there is no need to consider the second sub-problem and the solution set of (3.13) for *Case* 4 is just given by

$$T_4 = T_{3,\text{sub1}} = \{(0,0)\}. \tag{3.20}$$

*Case* 5: Similarly to *Case* 3, the two sub-problems are considered by dividing the feasible set into two mutually exclusive subsets in accordance with the operating mode of the monitor node. However, unlike former *Case*s, the successful eavesdropping condition is not guaranteed in the first sub-problem of *Case* 5. Therefore, I once again divide the first sub-problem into two separate problems by splitting its feasible set into the two sets which are exclusive with each other. Thus, there are a total of three sub-problems in *Case* 5. Then, the first sub-problem of (3.13) for *Case* 5 can be expressed as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & 0 \\ \text{s.t.} \quad & 0 \le q^{(1)} < q_{\text{thr}}^{(1)},\ q^{(2)} \ge 0, \\ & q^{(1)} + q^{(2)} \le Q_{\text{max}},\ \mathcal{C}_{\text{M}} < \mathcal{C}_{\text{DJ}}(\boldsymbol{q}). \end{aligned}$$

In this case, the solution is just determined as its own feasible set since the objective function is a constant value. Thus, the solution set of the first sub-problem is given by

$$T_{5,\text{sub1}} := \Big\{ \boldsymbol{q} \,|\, 0 \le q^{(1)} < q^{(1)}_{\text{thr}},\ q^{(2)} \ge 0, \\ q^{(1)} + q^{(2)} \le Q_{\max},\ \mathcal{C}_{\text{M}} < \mathcal{C}_{\text{DJ}}(\boldsymbol{q}) \Big\}. \quad (3.21)$$

Meanwhile, the second sub-problem is expressed as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{C}_{\text{DJ}}(\boldsymbol{q}) \\ \text{s.t.} \quad & 0 \le q^{(1)} < q^{(1)}_{\text{thr}},\ q^{(2)} \ge 0, \\ & q^{(1)} + q^{(2)} \le Q_{\max},\ \mathcal{C}_{\text{M}} \ge \mathcal{C}_{\text{DJ}}(\boldsymbol{q}). \end{aligned}$$

From the fact that $\mathcal{C}_{\text{DJ}}(\cdot)$ is a monotonically decreasing continuous function for either $q^{(1)}$ or $q^{(2)}$, it is clear that the maximum value of $\mathcal{C}_{\text{DJ}}(\cdot)$ is determined as $\mathcal{C}_{\text{M}}$ due to the constraints of the second sub-problem. Thus, the solution is determined as a set of $\boldsymbol{q}$ satisfying $\mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q})$. Then, the solution set of the second sub-problem is equal to the solution set of the following problem as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{C}_{\text{M}} \\ \text{s.t.} \quad & 0 \le q^{(1)} < q^{(1)}_{\text{thr}},\ q^{(2)} \ge 0, \\ & q^{(1)} + q^{(2)} \le Q_{\max},\ \mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q}). \end{aligned}$$

Similarly to the first sub-problem, the solution set is determined as its own feasible set since the objective function is a constant value. That is, the solution set of the second sub-problem is given by

$$T_{5,\text{sub2}} := \Big\{ \boldsymbol{q} \,|\, 0 \le q^{(1)} < q^{(1)}_{\text{thr}},\ q^{(2)} \ge 0, \\ q^{(1)} + q^{(2)} \le Q_{\max},\ \mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q}) \Big\}. \quad (3.22)$$

Unfortunately, (3.22) cannot determined as an unique form because the set of $\boldsymbol{q}$ satisfying $\mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q})$ is defined using the parameters which vary depending on the channel conditions. Thus, I present Table 3.2, classifying the channel conditions

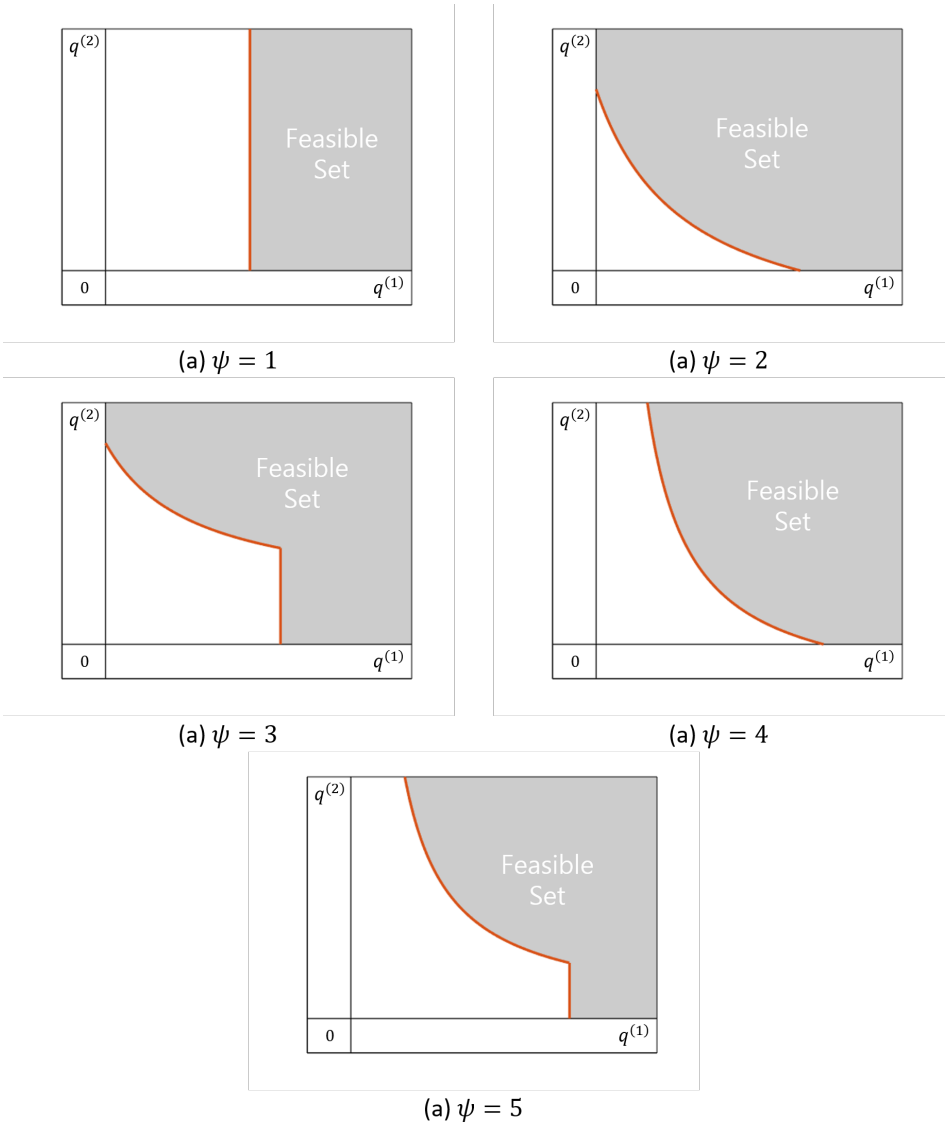



Figure 3.3: Description of the shape of $\mathcal{C} = \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q})$ and the area according to the feasible set in the $\psi$th sub-case of *Case* 5, i.e. *Case* $5_{\psi}$.

Table 3.2: The five sub-cases of channel conditions for *Case* 5

| Channel Conditions | | | $\psi$ |
|---|---|---|---|
| $\alpha_{\mathrm{SR}}\alpha_{\mathrm{MD}} - \alpha_{\mathrm{SD}}\alpha_{\mathrm{MR}} \leq \lambda_{\mathrm{M}}(\alpha_{\mathrm{MD}} - \alpha_{\mathrm{MR}})$ | | | 1 |
| $\alpha_{\mathrm{SR}}\alpha_{\mathrm{MD}} - \alpha_{\mathrm{SD}}\alpha_{\mathrm{MR}} > \lambda_{\mathrm{M}}(\alpha_{\mathrm{MD}} - \alpha_{\mathrm{MR}})$ | $\alpha_{\mathrm{SD}} < \lambda_{\mathrm{M}}$ | $\alpha_{\mathrm{MR}}\lambda_{\mathrm{M}}(\alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}} - \lambda_{\mathrm{M}})$ $\leq \alpha_{\mathrm{MD}}(\lambda_{\mathrm{M}} - \rho\alpha_{\mathrm{RD}})(\alpha_{\mathrm{SR}} - \lambda_{\mathrm{M}})$ | 2 |
| | | $\alpha_{\mathrm{MR}}\lambda_{\mathrm{M}}(\alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}} - \lambda_{\mathrm{M}})$ $> \alpha_{\mathrm{MD}}(\lambda_{\mathrm{M}} - \rho\alpha_{\mathrm{RD}})(\alpha_{\mathrm{SR}} - \lambda_{\mathrm{M}})$ | 3 |
| | $\alpha_{\mathrm{SD}} \geq \lambda_{\mathrm{M}}$ | $\alpha_{\mathrm{MR}}\lambda_{\mathrm{M}}(\alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}} - \lambda_{\mathrm{M}})$ $\leq \alpha_{\mathrm{MD}}(\lambda_{\mathrm{M}} - \rho\alpha_{\mathrm{RD}})(\alpha_{\mathrm{SR}} - \lambda_{\mathrm{M}})$ | 4 |
| | | $\alpha_{\mathrm{MR}}\lambda_{\mathrm{M}}(\alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}} - \lambda_{\mathrm{M}})$ $> \alpha_{\mathrm{MD}}(\lambda_{\mathrm{M}} - \rho\alpha_{\mathrm{RD}})(\alpha_{\mathrm{SR}} - \lambda_{\mathrm{M}})$ | 5 |

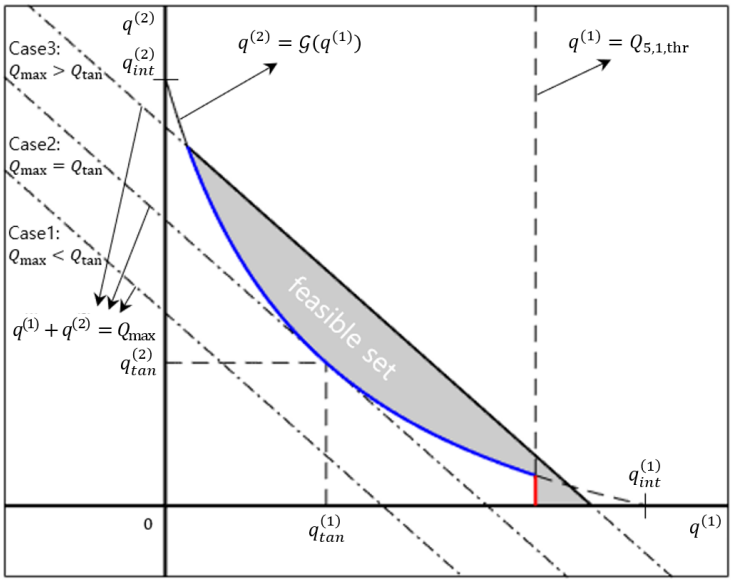



Figure 3.4: Description of how $Q_{\max}$ affects formation of the feasible set.

into five separate sub-cases in which $T_{5,\text{sub2}}$ is presented in different formula to one another. In Table 3.2, $\psi$ denotes the index number indicating each sub-case of *Case* 5. Furthermore, Fig.3.3 shows how the boundary line of $\mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q})$ is formed for each sub-case in the positive $\boldsymbol{q}$-domain where both $q^{(1)}$ and $q^{(2)}$ are positive values. In Fig.3.3, the orange line and the gray-colored area represents the boundary line satisfying $\mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q})$ and the feasible set of the second sub-problem, respectively, when $Q_{\text{max}}$ is given by an infinite number. I also provide Fig.3.4 to give an intuitive illustration of how the value of $Q_{\text{max}}$ affects the feasible set of the second sub-problem. In Fig.3.4, three cases where feasible sets are given as the empty set, a point, and an area respectively are considered and the gray-colored area represents the feasible set. From Fig.3.3 and Fig.3.4, I can define (3.22) as

$$T_{5,\text{sub2}} = \begin{cases} \emptyset, & \text{if } 0 \leq Q_{\text{max}} < Q_{5,\psi,\text{thr}} \\ V_\psi \cup W_\psi, & \text{if } Q_{\text{max}} \geq Q_{5,\psi,\text{thr}}, \end{cases} \tag{3.23}$$

where $Q_{5,\psi,\text{thr}}$ denotes the threshold value of $Q_{\text{max}}$ for the feasible set of the second sub-problem not to be the empty set in the $\psi$th sub-case of *Case* 5 and, in each sub-case, is given by

$$Q_{5,1,\text{thr}} := \frac{1}{\alpha_{\text{MR}}} \left( \frac{\alpha_{\text{SR}}}{\lambda_{\text{M}}} - 1 \right),$$

$$Q_{5,2,\text{thr}} := \begin{cases} Q_{\text{tan}}, & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} \geq 0, \\ \min\{q_{\text{int}}^{(1)}, q_{\text{int}}^{(2)}\}, & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} < 0, \end{cases}$$

$$Q_{5,3,\text{thr}} := \begin{cases} \min\{Q_{5,1,\text{thr}}, Q_{\text{tan}}\}, & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} \geq 0, \\ \min\{Q_{5,1,\text{thr}}, q_{\text{int}}^{(2)}\}, & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} < 0, \end{cases}$$

$$Q_{5,4,\text{thr}} := \begin{cases} Q_{\text{tan}}, & \text{if } q_{\text{tan}}^{(2)} \geq 0, \\ q_{\text{int}}^{(1)}, & \text{if } q_{\text{tan}}^{(2)} < 0, \end{cases}$$

$$Q_{5,5,\text{thr}} := \begin{cases} \min\{Q_{5,1,\text{thr}}, Q_{\text{tan}}\}, & \text{if } q_{\text{tan}}^{(2)} \geq 0, \\ Q_{5,1,\text{thr}}, & \text{if } q_{\text{tan}}^{(2)} < 0. \end{cases}$$

In addition, $q_{\text{int}}^{(1)}$ and $q_{\text{int}}^{(2)}$ denote $q^{(1)}$-intercept and $q^{(2)}$-intercept of $q^{(2)} = \mathcal{G}(q^{(1)})$ in the $\boldsymbol{q}$-domain, respectively, and $q_{\text{tan}}^{(1)}$ and $q_{\text{tan}}^{(2)}$ denote $q^{(1)}$ and $q^{(2)}$ of the point at which $\frac{\partial \mathcal{G}(q^{(1)})}{\partial q^{(1)}}$ is -1, respectively. $Q_{\text{tan}}$ denotes the sum of $q_{\text{tan}}^{(1)}$ and $q_{\text{tan}}^{(2)}$. They are described graphically in Fig.3.4 and are given by

$$
\begin{aligned}
q_{\text{int}}^{(1)} &= \frac{1}{\alpha_{\text{MD}}} \left( \frac{\alpha_{\text{SD}}}{\lambda_{\text{M}} - \rho\alpha_{\text{RD}}} - 1 \right), \\
q_{\text{int}}^{(2)} &= \frac{1}{\alpha_{\text{MD}}} \left( \frac{\rho\alpha_{\text{RD}}}{\lambda_{\text{M}} - \alpha_{\text{SD}}} - 1 \right), \\
q_{\text{tan}}^{(1)} &= \frac{1}{\alpha_{\text{MD}}} \left( \frac{\alpha_{\text{SD}} + \sqrt{\rho\alpha_{\text{SD}}\alpha_{\text{RD}}}}{\lambda_{\text{M}}} - 1 \right), \\
q_{\text{tan}}^{(2)} &= \frac{1}{\alpha_{\text{MD}}} \left( \frac{\rho\alpha_{\text{RD}} + \sqrt{\rho\alpha_{\text{SD}}\alpha_{\text{RD}}}}{\lambda_{\text{M}}} - 1 \right). \\
Q_{\text{tan}} &= q_{\text{tan}}^{(1)} + q_{\text{tan}}^{(2)}.
\end{aligned}
$$

Moreover, $\mathcal{G}(\cdot)$ is the function derived from the equation of $\mathcal{C}_{\text{M}} = \mathcal{C}_{\text{DJ}}(\boldsymbol{q})$ and it is defined as

$$
\mathcal{G}(x) := \frac{1}{\alpha_{\text{MD}}} \left( \frac{\rho\alpha_{\text{RD}}(1 + \alpha_{\text{MD}}x)}{\lambda_{\text{M}}(1 + \alpha_{\text{MD}}x) - \alpha_{\text{SD}}} - 1 \right).
$$

On the one hand, $V_\psi$ is given by

$$
V_\psi = \begin{cases}
\emptyset, & \text{if } \psi = 1, \\
\emptyset, & \text{if } \psi \in \{2,3,4,5\} \\
& \text{and } 0 \le Q_{\text{max}} < Q_{\text{tan}}, \\
\emptyset, & \text{if } \psi \in \{2,3,4,5\} \\
& \text{and } Q_{\text{max}} \ge Q_{\text{tan}} \\
& \text{and } q_{\text{L}}^{(1)} \ge Q_{5,1,\text{thr}}, \\
\{\boldsymbol{q} \mid q_{\text{L}}^{(1)} \le q^{(1)} \le q_{\text{U},\psi}^{(1)}, & \text{if } \psi \in \{2,3,4,5\} \\
\quad q^{(2)} = \mathcal{G}(q^{(1)})\}, & \text{and } Q_{\text{max}} \ge Q_{\text{tan}} \\
& \text{and } q_{\text{L}}^{(1)} < Q_{5,1,\text{thr}},
\end{cases}
$$

where $q_{\text{L}}^{(1)}$ and $q_{\text{U},\psi}^{(1)}$ are defined as

$$
q_{\text{L}}^{(1)} := \max\left\{0, q_{\text{l}}^{(1)}\right\},
$$

$$q_{\mathrm{U},\psi}^{(1)} := \begin{cases} \min\left\{q_{\mathrm{u}}^{(1)}, q_{\mathrm{int}}^{(1)}\right\}, & \text{if } \psi \in \{2,4\}, \\ \min\left\{q_{\mathrm{u}}^{(1)}, Q_{5,1,\mathrm{thr}}\right\}, & \text{if } \psi \in \{3,5\}, \end{cases}$$

where $q_{\mathrm{l}}^{(1)}$ and $q_{\mathrm{u}}^{(1)}$ are determined as the pair of $x$ such that $Q_{\max} - x = \mathcal{G}(x)$. On the other hand, $W_\psi$ is given by

$$W_\psi = \begin{cases} \emptyset, & \text{if } \psi \in \{1,3,5\}, \\ & \text{and } 0 \le Q_{\max} < Q_{5,1,\mathrm{thr}} \\ \{\boldsymbol{q} \mid q^{(1)} = Q_{5,1,\mathrm{thr}}, & \text{if } \psi \in \{1,3,5\} \\ \quad 0 \le q^{(2)} \le q_{\mathrm{U}}^{(2)}\} & \text{and } Q_{\max} \ge Q_{5,1,\mathrm{thr}}, \\ \emptyset, & \text{if } \psi \in \{2,4\}, \end{cases},$$

where $q_{\mathrm{U}}^{(2)}$ is defined as

$$q_{\mathrm{U}}^{(2)} := \min\left\{Q_{\max} - Q_{5,1,\mathrm{thr}},\ \mathcal{G}(Q_{5,1,\mathrm{thr}})\right\}.$$

Finally, the third sub-problem is expressed as

$$\begin{aligned} \max_{\boldsymbol{q}} \quad & \mathcal{E}_{\mathrm{M}}(\boldsymbol{q}) \\ \text{s.t.} \quad & q^{(1)} \ge q_{\mathrm{thr}}^{(1)},\ q^{(2)} \ge 0, \\ & q^{(1)} + q^{(2)} \le Q_{\max}. \end{aligned}$$

Under the constraint of $q^{(1)} \ge q_{\mathrm{thr}}^{(1)}$, it is enough to fulfill $\mathcal{C}_{\mathrm{M}} \ge \mathcal{C}_{\mathrm{D}}(\boldsymbol{q})$ because $\mathcal{C}_{\mathrm{M}} > \mathcal{R}_{\mathrm{M}} \ge \mathcal{R}_{\mathrm{R}}(q^{(1)})$ is always satisfied as long as $q^{(1)}$ is not smaller than $q_{\mathrm{thr}}^{(1)}$. Thus, the third sub-problem of *Case* 5 becomes identical to the second sub-problem of *Case* 3, and accordingly the solution set of the third sub-problem is just given by

$$T_{5,\mathrm{sub3}} = T_{3,\mathrm{sub2}}.$$

On the one hand, under the condition of $\boldsymbol{q} \in T_{5,\mathrm{sub3}}$, the maximum eavesdropping rate cannot exceed $\mathcal{R}_{\mathrm{M}}$ since the monitor node operates in the helping mode. On the other hand, the maximum eavesdropping rates under the conditions of $\boldsymbol{q} \in T_{5,\mathrm{sub1}}$ and $\boldsymbol{q} \in T_{5,\mathrm{sub2}}$ are determined as zero and $\mathcal{C}_{\mathrm{M}}$, respectively. Thus, as long as both $T_{5,\mathrm{sub2}}$

is not the empty set, it is obvious that the solution set of (3.13) for *Case* 5 is given as $T_{5,\text{sub2}}$. Furthermore, when $T_{5,\text{sub2}}$ is the empty set, $T_{5,\text{sub3}}$ is always determined as the empty set because $Q_{5,\psi,\text{thr}}$ is smaller than $q_{\text{thr}}^{(1)}$ for all $\psi$. Since $T_{5,\text{sub1}}$ is not always empty set, the solution set of (3.13) for *Case* 5 is given as

$$T_5 = \begin{cases} T_{5,\text{sub1}}, & \text{if } T_{5,\text{sub2}} = \emptyset, \\ T_{5,\text{sub2}}, & \text{if } T_{5,\text{sub2}} \neq \emptyset. \end{cases}$$

Using (3.21) and (3.23), this can be expressed as

$$T_5 = \begin{cases} \Big\{ \boldsymbol{q} \mid 0 \leq q^{(1)} < q_{\text{thr}}^{(1)}, \\ q^{(2)} \geq 0,\ \mathcal{C}_{\text{M}} < \mathcal{C}_{\text{DJ}}(\boldsymbol{q}),, & \text{if } 0 \leq Q_{\max} < Q_{5,\psi,\text{thr}}, \\ \quad q^{(1)} + q^{(2)} \leq Q_{\max} \Big\} \\ \qquad V_\psi \cup W_\psi, & \text{if } Q_{\max} \geq Q_{5,\psi,\text{thr}}. \end{cases} \tag{3.24}$$

To sum up, the final solution set of (3.13) is given as

$$T = \begin{cases} T_1, & \text{for Case } 1, \\ T_2, & \text{for Case } 2, \\ T_3, & \text{for Case } 3, \\ T_4, & \text{for Case } 4, \\ T_5, & \text{for Case } 5. \end{cases} \tag{3.25}$$

### 3.3.2 Minimizing Total Power Consumption

As long as $\boldsymbol{q}$ is included in $T$ which is the solution set of (3.13), it is guaranteed that the eavesdropping rate achieves maximum value under the successful eavesdropping condition. Nevertheless, all $\boldsymbol{q}$ in $T$ is not entirely equal. This is because the total power consumed at the monitor node is different depending on which $\boldsymbol{q}$ is selected as the optimal power scheme for the monitor node. While maintaining the maximum eavesdropping rate, in order to enhance the power efficiency simultaneously, I find $\boldsymbol{q}$ to minimize the total power consumption of the monitor node. This optimization problem

can be expressed as

$$\begin{aligned} \min_{\boldsymbol{q}} \quad & \textstyle\sum_{n=1}^{2} Q^{(n)} \\ \text{s.t.} \quad & \boldsymbol{q} \in T. \end{aligned} \tag{3.26}$$

For *Case* from 1 to 4, the solution of (3.26) is simply given by

$$\boldsymbol{q}_1^\star(Q_{\text{max}}) = (0,0),$$

$$\boldsymbol{q}_2^\star(Q_{\text{max}}) = \begin{cases} (0, Q_{\text{max}}), & \text{if } 0 \le Q_{\text{max}} < Q_{2,\text{thr}}, \\ (0, Q_{2,\text{thr}}), & \text{if } Q_{\text{max}} \ge Q_{2,\text{thr}}, \end{cases}$$

$$\boldsymbol{q}_3^\star(Q_{\text{max}}) = \begin{cases} (0,0), & \text{if } 0 \le Q_{\text{max}} < Q_{3,\text{thr2}}, \\ (q_{\text{thr}}^{(1)}, Q_{\text{max}} - q_{\text{thr}}^{(1)}), & \text{if } Q_{3,\text{thr2}} \le Q_{\text{max}} < Q_{3,\text{thr1}}, \\ (q_{\text{thr}}^{(1)}, q_{3,\text{thr1}}^{(2)}), & \text{if } Q_{\text{max}} \ge Q_{3,\text{thr1}}, \end{cases}$$

$$\boldsymbol{q}_4^\star(Q_{\text{max}}) = (0,0).$$

Furthermore, the solution of (3.26) for *Case* 5 is given by

$$\boldsymbol{q}_5^\star(Q_{\text{max}}) = \begin{cases} (0,0), & \text{if } 0 \le Q_{\text{max}} < Q_{5,\psi,\text{thr}}, \\ \boldsymbol{q}_{5,\psi}^\star, & \text{if } Q_{\text{max}} \ge Q_{5,\psi,\text{thr}}, \end{cases}$$

where $\boldsymbol{q}_{5,\psi}^\star$ denotes the solution of (3.26) for the $\psi$th sub-case of *Case* 5 and, for all $\psi$, is given as

$$\boldsymbol{q}_{5,1}^\star = (Q_{5,1,\text{thr}}, 0),$$

$$\boldsymbol{q}_{5,2}^\star = \begin{cases} (q_{\text{tan}}^{(1)}, q_{\text{tan}}^{(2)}), & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} \ge 0, \\ (0, q_{\text{int}}^{(2)}), & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} < 0 \\ & \text{and } q_{\text{tan}}^{(1)} < 0, \\ (q_{\text{int}}^{(1)}, 0), & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} < 0 \\ & \text{and } q_{\text{tan}}^{(1)} > 0, \end{cases}$$

$$\boldsymbol{q}_{5,3}^{\star} = \begin{cases} (q_{\text{tan}}^{(1)}, q_{\text{tan}}^{(2)}), & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} \geq 0 \\ & \text{and } Q_{\text{tan}} \leq Q_{5,1,\text{thr}}, \\ (0, q_{\text{int}}^{(2)}), & \text{if } q_{\text{tan}}^{(1)} q_{\text{tan}}^{(2)} < 0 \\ & \text{and } q_{\text{tan}}^{(1)} < 0 \\ & \text{and } q_{\text{int}}^{(2)} \leq Q_{5,1,\text{thr}}, \\ (Q_{5,1,\text{thr}}, 0), & \text{otherwise}, \end{cases}$$

$$\boldsymbol{q}_{5,4}^{\star} = \begin{cases} (q_{\text{tan}}^{(1)}, q_{\text{tan}}^{(2)}), & \text{if } q_{\text{tan}}^{(2)} \geq 0, \\ (q_{\text{int}}^{(1)}, 0), & \text{if } q_{\text{tan}}^{(2)} < 0, \end{cases}$$

$$\boldsymbol{q}_{5,5}^{\star} = \begin{cases} (q_{\text{tan}}^{(1)}, q_{\text{tan}}^{(2)}), & \text{if } q_{\text{tan}}^{(2)} \geq 0 \\ & \text{and } Q_{\text{tan}} \leq Q_{5,1,\text{thr}}, \\ (Q_{5,1,\text{thr}}, 0), & \text{otherwise}. \end{cases}$$

Consequently, the solution of (3.26) is given by

$$\boldsymbol{q}^{\star}(Q_{\text{max}}) = \begin{cases} \boldsymbol{q}_1^{\star}(Q_{\text{max}}), & \text{for Case } 1, \\ \boldsymbol{q}_2^{\star}(Q_{\text{max}}), & \text{for Case } 2, \\ \boldsymbol{q}_3^{\star}(Q_{\text{max}}), & \text{for Case } 3, \\ \boldsymbol{q}_4^{\star}(Q_{\text{max}}), & \text{for Case } 4, \\ \boldsymbol{q}_5^{\star}(Q_{\text{max}}), & \text{for Case } 5. \end{cases} \tag{3.27}$$

## 3.4 Numerical Results

In this section, I validate the performance of the proposed method with the optimal power strategy by simulation results. For simulation parameters, I set radio frequency as 5 GHz and bandwidth as 20 MHz. In addition, channel coefficients of all communication links are generated based on the COST207 Typical Urban 6-ray channel model [16, 41]. For the 6-ray channel model, the used path powers, $\{\gamma_z\}_{z=1}^{z=6}$, and the used path delays, $\{\delta_z\}_{z=1}^{z=6}$ are given as follows;

$$\{\gamma_z\}_{z=1}^{z=6} = \{0.189, 0.379, 0.239, 0.095, 0.061, 0.037\},$$

$$\{\delta_z\}_{z=1}^{z=6} = \{0.0, 0.2, 0.5, 1.6, 2.3, 5\} * 10^{-6}.$$

Then, the channel coefficient between node X and node Y can be expressed as

$$h_{\mathrm{XY}} = (d_{\mathrm{XY}})^{-2} \sum_{z=1}^{z=6} g_z e^{-j2\pi f \delta_z},$$

where $d_{\mathrm{XY}}$ denotes the Euclidean distance between node X and node Y, and $f$ is the radio frequency, and $g_z$ denotes the $z$th fading and is given by an independent complex Gaussian random variable with zero-mean and variance $\gamma_z$. Moreover, throughout this section, I use $\Gamma_{Q_{\max}}$, the ratio of $Q_{\max}$ to the power utilized for the suspicious communication, instead of $Q_{\max}$. That is, $\Gamma_{Q_{\max}}$ is defined as

$$\Gamma_{Q_{\max}} := \frac{Q_{\max}}{P_{\mathrm{tot}}},$$

where $P_{\mathrm{tot}}$ denotes the total power which the source node and the relay node consume for transmitting the signal to the destination node and is given by

$$P_{\mathrm{tot}} := P_{\mathrm{S}} + P_{\mathrm{R}}.$$

For comparison of performance, two conventional methods are introduced; one is the method where the monitor node is utilized as the jammer or the helper in the half-duplex mode [30] and the other is the half-duplex jamming method in which the monitor node acts as only the half-duplex jammer [37, 39]. I denote the first method [30] as 'Conv1' and the second method [37, 39] as 'Conv2' while denoting our proposed method as 'Prop' in each figure. Moreover, for more realistic and practical analysis, I consider two imperfect CSI cases as well as the perfect CSI case where there is noise-free CSI exploited by the monitor node. In the imperfect CSI cases, complex Gaussian noise is added to the channel coefficients at the monitor node. The ratios of each channel coefficient to noise are 0dB and 20dB in the two imperfect CSI cases, and is infinity in the perfect CSI case, respectively. To discriminate these cases, I mark the ratio of each channel coefficient to noise on each legend of all figures.

In order to examine the performance variation by the mobility of nodes in the infrastructure-free network, I consider three simulation scenarios. Fig.3.5 shows the

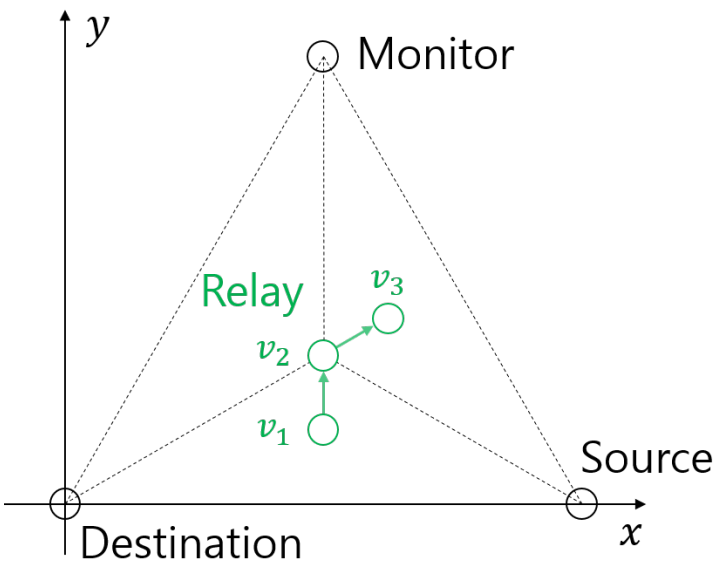
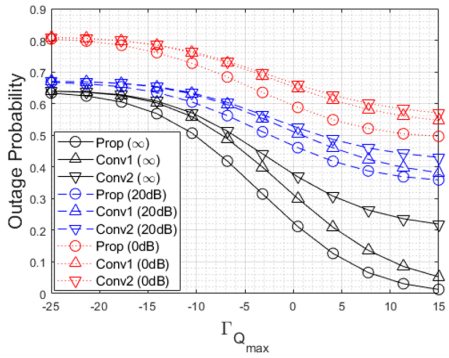


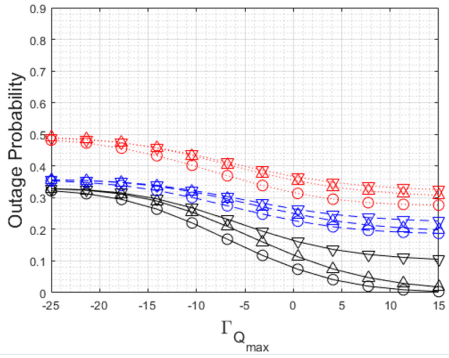

Figure 3.5: The network topology for the first simulation scenario.

network topology used for the first scenario. All nodes of the network are deployed in a 2-Dimensional space and, at the same time, the source node, the destination node, and the monitor node form an equilateral triangle. Coordinates of the three nodes are $(0, 2)$, $(0, 0)$, and $(1, \sqrt{3})$, respectively. Further, as shown in the figure, it is assumed that the relay node moves from the lower side of the triangle to the right side via the center. Therefore, simulations are carried out over three sub-cases where the relay node is positioned on $v_1$, $v_2$, and $v_3$. Coordinates of the three points are $(1, \frac{\sqrt{3}}{6})$, $(1, \frac{\sqrt{3}}{3})$, and $(\frac{5}{4}, \frac{\sqrt{3}}{2})$, respectively. All performances are averaged over a total of 500,000 simulation iterations.

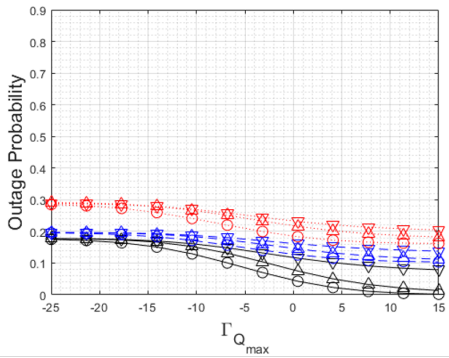
Fig.3.6 and Fig.3.7 shows the outage probabilities and the average eavesdropping rates for the three sub-cases in the first simulation scenario when $\Gamma_{Q_{\max}}$ is varying in the environment where $P_{\text{tot}}$ is 1, $\rho$ is 1, and $\sigma^2$ is $10^{-2}$. From the figures, it is clear that performances are enhanced regardless of the proactive eavesdropping method for all sub-cases when $\Gamma_{Q_{\max}}$ is increasing. I also identified that the proposed method outper-




(a) $v_1$

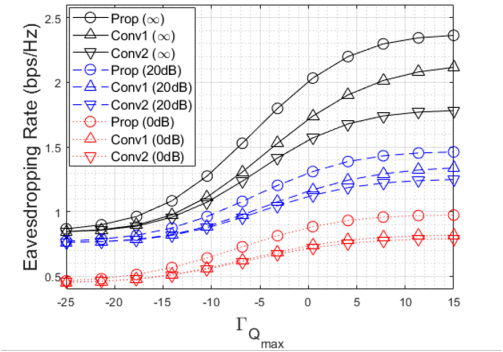



(b) $v_2$

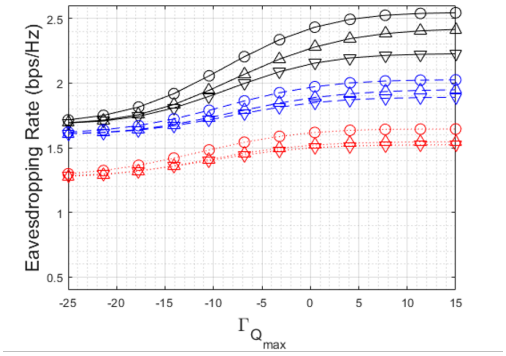



(c) $v_3$

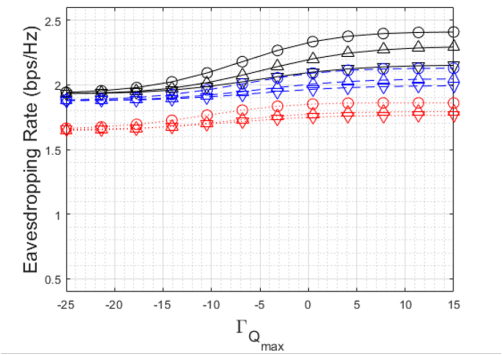
Figure 3.6: Outage probabilities for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the first simulation scenario.




(a) $v_1$




(b) $v_2$




(c) $v_3$

Figure 3.7: Average eavesdropping rates for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the first simulation scenario.

forms other benchmark methods over all $\Gamma_{Q_{\max}}$ both in terms of the outage probability and the eavesdropping rate. Particularly, performance differences are largest in the sub-case where the relay node is positioned at $v_1$. This is because the monitor node is on a more advantageous position to eavesdrop the suspicious communication link as the relay node moves from $v_1$ to $v_3$. In more detailed, this implies that the proposed method copes with adversarial situations to monitor networks more flexibly than other benchmark methods, since the full-duplex proposed method can eavesdrop the suspicious link throughout the transmission whereas other half-duplex benchmark methods could eavesdrop only one phase of the transmission. When the relay node moves from $v_1$ to $v_3$, the outage probability is improved over all $\Gamma_{Q_{\max}}$, but the average eavesdropping rate decreases during the high $\Gamma_{Q_{\max}}$ section. This result comes from that, at the high $\Gamma_{Q_{\max}}$ section, the achievable rate of the destination node decreases considerably compared to the enhancement of the outage probability. Moreover, it is shown that all performances deteriorate rapidly as the noise power is increasing on each channel coefficient. These results are reasonable since all methods are designed from the tight successful eavesdropping condition. Under this tight condition, even a small error on the CSI can lead to large increase in the probability that the successful eavesdropping condition is violated. Thus, in a practical communication network, a margin is needed in the successful eavesdropping condition for reliable performances.

Fig.3.8 shows the average eavesdropping rate of only the cases where all methods experience successful eavesdropping, i.e., no outage. Thus, the difference of the outage probabilities is ignored in Fig.3.8. From this, it is also verified that the proposed method does not merely enhance the number of no outage cases, but even improve the eavesdropping rate of the monitor node in no outage cases compared to other benchmark methods. This implies that the proposed method is still superior than other benchmark methods even if the outage scarcely occur because the monitor node is very advantageous to eavesdrop the suspicious communications.

In Fig.3.9, the network topology utilized for the second and the third simulation

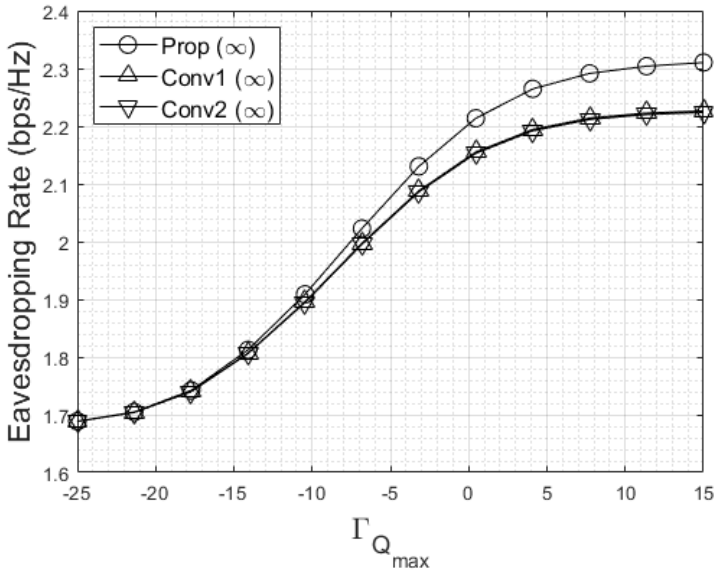
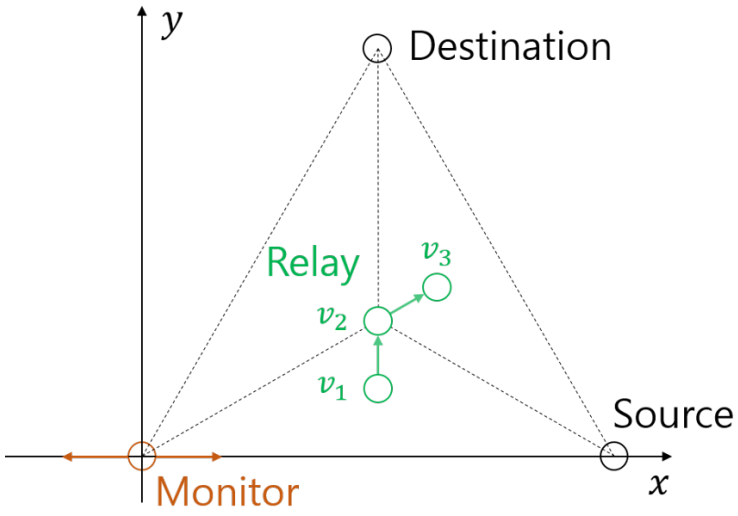


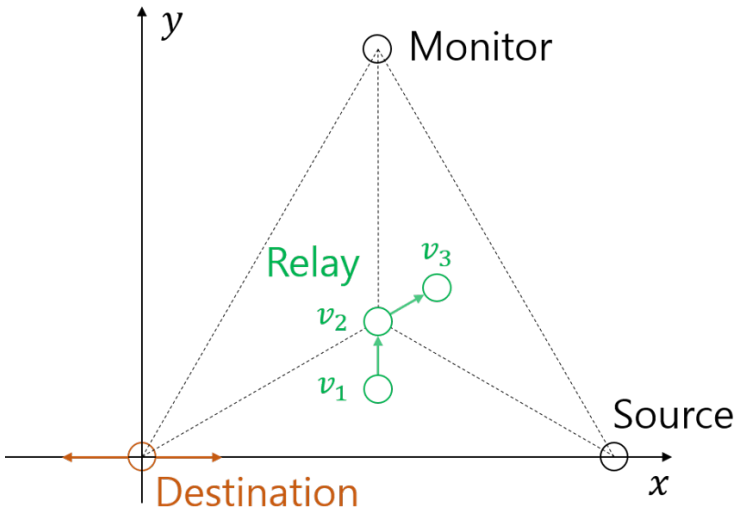

Figure 3.8: The average eavesdropping rate of the cases when the conventional method experiences no outage.

scenarios is graphically described. In the two scenarios, the source node, the destination node, and the monitor node form the equilateral triangle and the relay node is assumed to move from $v_1$ to $v_3$ via $v_2$ like the first simulation scenario. Coordinates of the source node, the destination node, and the monitor node are $(0, 2)$, $(1, \sqrt{3})$, and $(0, 0)$ for the second scenario and $(0, 2)$, $(0, 0)$, and $(1, \sqrt{3})$ for the third scenario. Further, in each scenario, simulations are carried out over three sub-cases where the relay node is positioned at $v_1$, $v_2$, and $v_3$. Coordinates of the three points are same as in the first simulation scenario. In addition, I assume that the monitor node for the second scenario and the destination node for the third scenario have lateral movements along the x-axis in 2-Dimensional space.

Fig.3.10 and Fig.3.11 show the outage probability and the average eavesdropping rate for the three sub-cases in the second simulation scenario when the monitor node moves from $(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$ in the environment where $P_{\text{tot}}$ is 1, $\Gamma_{Q_{\max}}$ is -10dB, $\rho$ is 1,

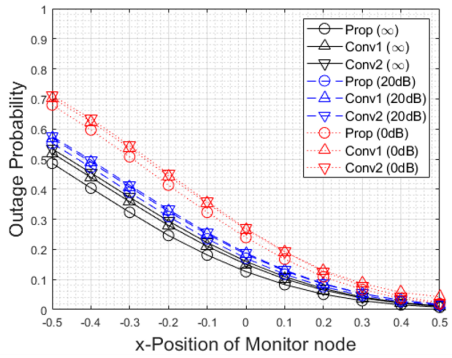



(a) The second simulation scenario

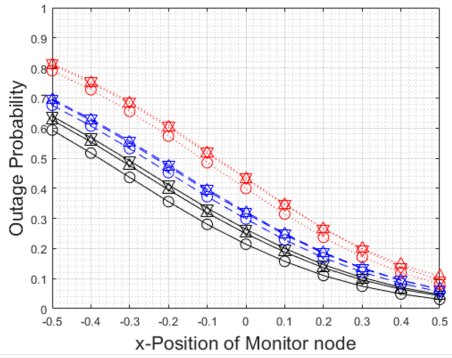



(b) The third simulation scenario

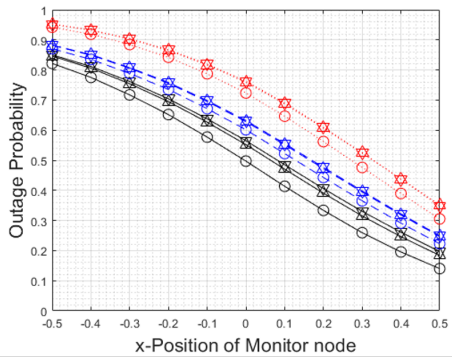
Figure 3.9: The network topology for (a) the second simulation scenario and (b) the third simulation scenario.




(a) $v_1$

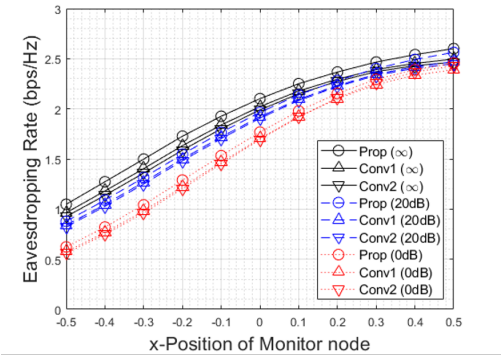



(b) $v_2$

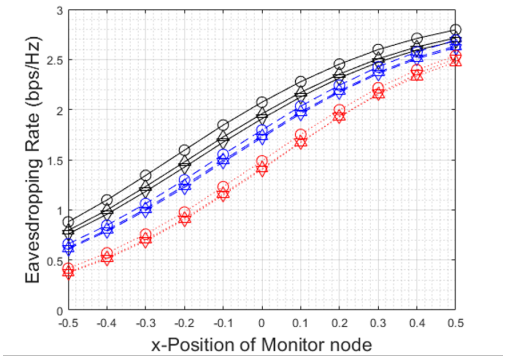



(c) $v_3$

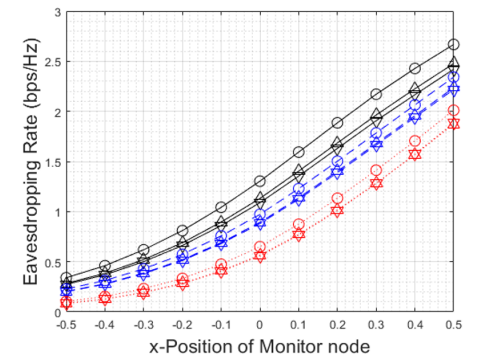
Figure 3.10: Outage probabilities for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the second simulation scenario.




(a) $v_1$




(b) $v_2$

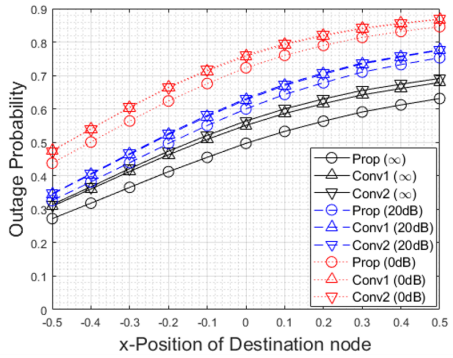



(c) $v_3$

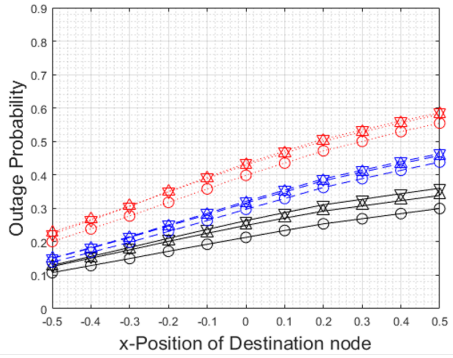
Figure 3.11: Average eavesdropping rates for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the second simulation scenario.

and $\sigma^2$ is $10^{-2}$. As shown in the two figures, it is verified that the proposed method is superior than other benchmark methods in both the outage probability and the average eavesdropping rate. For all sub-cases, all performances are improved as the monitor node moves from $(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$. This is because the channel states between the monitor node and the source node and between the monitor node and the relay node is getting more advantageous for eavesdropping. In other words, the monitor node is in more advantageous environment to eavesdrop the suspicious communication link when it moves in the positive direction on the x-axis. Further, unlike the first simulation scenario, the monitor node is in more adverse situation to eavesdrop the suspicious link as the relay node moves from $v_1$ to $v_3$. This is why moving the monitor node in the positive direction on the x-axis can maintain the outage probability performance when the relay node moves from $v_1$ to $v_3$. Nevertheless, from Fig.3.10, I can verify that the proposed method requires a relatively small movement of the monitor node compared to other benchmark methods to keep the same outage probability. This is because the proposed method using the full-duplex monitor node can obtain double channel gain than other benchmark method using the half-duplex monitor throughout the transmission. Therefore, the proposed method handles the situation when the monitor node is gradually harder to eavesdrop the suspicious link by movement of the relay node more efficiently. Meanwhile, from Fig.3.11, it is noticeable that, when the monitor node is in the vicinity of $(\frac{1}{2}, 0)$, the average eavesdropping rate is rather increasing as the relay node moves from $v_1$ to $v_2$. This effect comes from that the eavesdropping rate increment is relatively dominant compared with the drop in the outage probability because the monitor node already has a good channel state to eavesdrop the suspicious link. That is, if the monitor node is nearby the source node enough to eavesdrop the suspicious link, it may be better in terms of the eavesdropping rate that the relay node moves to increase the achievable rate of the suspicious link.

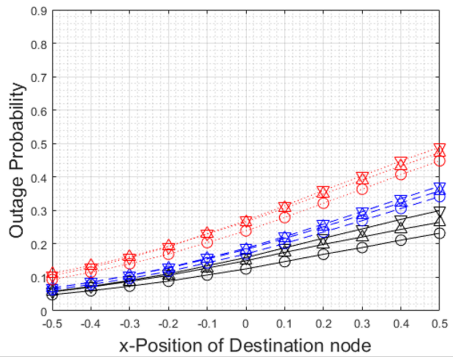
Fig.3.12 and Fig.3.13 show the outage probability and the average eavesdropping rate for the three sub-cases in the third simulation scenario when the destination node




(a) $v_1$

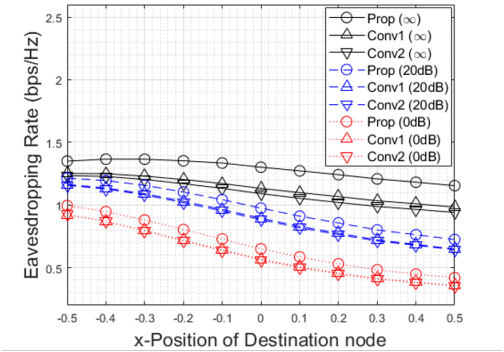



(b) $v_2$

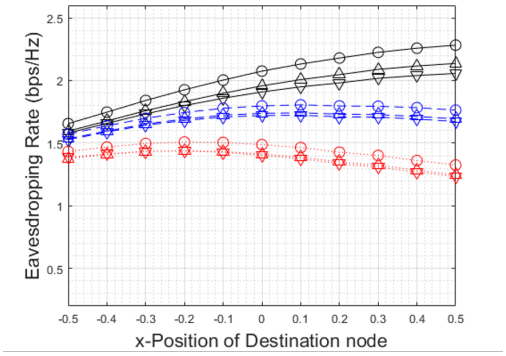



(c) $v_3$

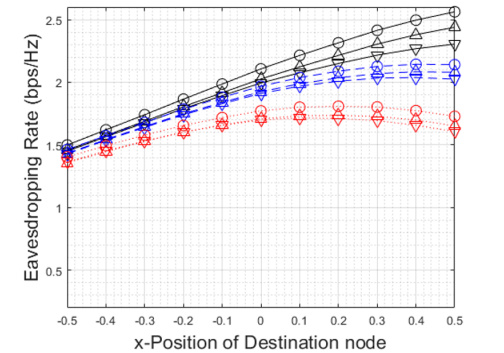
Figure 3.12: Outage probabilities for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the third simulation scenario.




(a) $v_1$




(b) $v_2$




(c) $v_3$

Figure 3.13: Average eavesdropping rates for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the third simulation scenario.

moves from $(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$ in the environment where $P_{\text{tot}}$ is 1, $\Gamma_{Q_{\max}}$ is -10dB, $\rho$ is 1, and $\sigma^2$ is $10^{-2}$. As shown in Fig.3.12, the outage probability performance is deteriorated for all sub-cases as the destination node moves from $(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$. This comes from the fact that the channel states between the destination node and the source node and between the destination node and the relay node become better as the destination node moves from $(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$. That is, when the destination node moves in the positive direction on the x-axis, the suspicious link becomes harder to eavesdrop. On the other hand, the monitor node becomes advantageous to eavesdropping the suspicious link when the relay node moves from $v_1$ to $v_3$. This is why the outage probability performance is gradually enhanced over all positions of the destination node as the position of the relay node is changed from $v_1$ to $v_3$. It is also identified that the performance differences between the proposed method and other benchmark methods become larger when the network circumstance becomes disadvantageous to eavesdropping the suspicious communication link. This implies that the proposed method is more tolerable to harsh network conditions, where the monitor node can hardly eavesdrop the suspicious link, than other benchmark methods. In Fig.3.13, it is noticeable that the average eavesdropping rates are slowly decreasing or even increasing as the destination node moves in the positive direction on the x-axis. This result comes from that both the eavesdropping rate corresponding to the successful eavesdropping case and the number of the outage cases increases together.

Although I assume that the ratio of the relay power to the transmit power, $\rho$, is known to the monitor node in the paper, the monitor node cannot know $\rho$ in practical communication scenarios. Fig.3.14 and Fig.3.15 show the outage probability and the average eavesdropping rate versus $\Gamma_{Q_{\max}}$, respectively, when $\rho$ used in the optimal power design is different with the real ratio of the relay power to the transmit power, $\rho_{\text{real}}$. Except for $\rho$, the simulation setting is same as in Fig.3.6 (b) and Fig.3.7 (b). I consider two cases in which $\rho$ and $\rho_{\text{real}}$ are different each other. In the first case, $\rho_{\text{real}}$

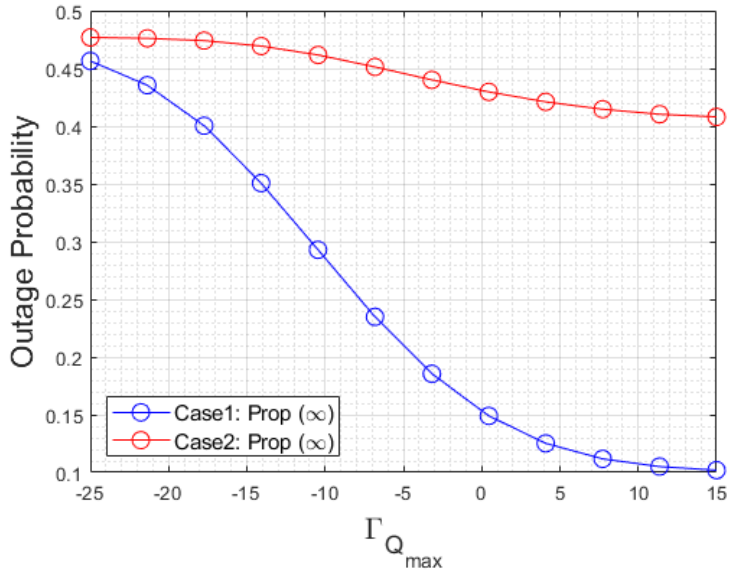



Figure 3.14: Average eavesdropping rates for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the third simulation scenario.

is given by 2 and $\rho$ is given by $\rho_{\text{opt}}$ which is defined as

$$\rho_{\text{opt}} := \frac{\alpha_{\text{SR}} - \alpha_{\text{SD}}}{\alpha_{\text{RD}}}.$$

Under the situation where there is no jamming or helping from the monitor node, $\rho_{\text{opt}}$ is the optimal ratio which maximizes the achievable rate of the destination node. Since all nodes in the suspicious communication link do not know the existence of the monitor node, $\rho_{\text{opt}}$ is a reasonable choice for the source node and the relay node. Whereas, in the second case, $\rho_{\text{real}}$ is given by $\rho_{\text{opt}}$ and $\rho$ is given by 2. In Fig.3.14 and Fig.3.15, the blue line and the red line represent the first case and the second case, respectively. From Fig.3.14, it is clearly shown that the first case is better than the second case in terms of the outage probability performance. This is because, in the second case, the monitor node underestimates the achievable rate of the destination node so that the probability that the monitor node does not jam the relay node and the destination node enough to eavesdrop the suspicious link successfully is relatively high. On the other

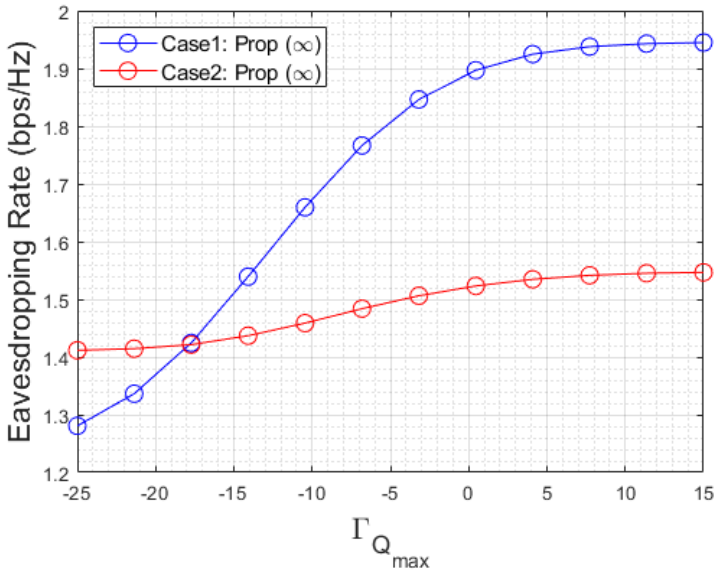



Figure 3.15: Average eavesdropping rates for the three sub-cases where the relay node is positioned at (a) , (b), and (c) in the third simulation scenario.

hand, the monitor node overestimates the achievable rate of the destination node in the first case. Thus, the monitor node is likely to jam the suspicious link even in the situation where it can eavesdrop successfully without the jamming. This is why the first case is worse than the second case in the eavesdropping rate performance when $Q_{\max}$ is very low as shown in Fig.3.15. Nevertheless, as $Q_{\max}$ increases, the eavesdropping rate performances of two cases become reversed because of an overwhelming difference of the outage probability performances. Consequently, it is inferred that, if $\rho_{\text{real}}$ is unknown to the monitor node, $\rho_{\text{opt}}$ is the best choice of $\rho$ in the optimal power design.

## 3.5 Summary

This chapter studied proactive eavesdropping in the general infrastructure-free communication network where all nodes have the mobility and the monitor node operates

independently from other nodes. In order to enhance the proactive eavesdropping performance of the network, I proposed the adaptive full-duplex jamming-helping method in which the monitor node can select its operating mode adaptively depending on the channel conditions. Furthermore, I designed the optimal power scheme for the proposed method to minimize the total power consumption of the monitor node while maximizing the eavesdropping rate. In the process, I first classified channel conditions into several cases to make the optimization problem straightforward. Then, for each classified case, I solved the simplified problem and presented the optimal power for the proposed method in closed form. In addition, I analyzed the numerical results came from the three simulation scenarios: 1) moving only the relay node, 2) moving the relay node and the destination node, and 3) moving the relay node and the monitor node. Through the numerical analysis, it was verified that the proposed method outperforms other benchmark methods both in the outage probability and the eavesdropping rate for all simulation scenarios. Particularly, in the situation where the relay node, the monitor node, or the destination node moves in the way that eavesdropping the suspicious communication link becomes harder, it is shown that performance differences between the proposed method and other benchmark methods becomes larger. I also identified that the outage probability performance becomes better regardless of the position of the destination node as the position of the monitor node is closer to the source node or the relay node, but the eavesdropping rate performance depends on the position of the destination node. From these results, it can be inferred that an optimal position of the monitor node can be different depending on which performance the system weights to.

# Chapter 4

# Proactive Eavesdropping using Half-Duplex Dual Monitor

## 4.1 Motivation

In proactive eavesdropping, the legitimate eavesdropper can monitor a suspicious communication link successfully only if it obtains whole information of the signal traveling in the suspicious link. From the viewpoint of information theory, the successful eavesdropping implies that achievable rate of the monitor node, which is managed by the legitimate eavesdropper, is greater than achievable rate of the destination node in the suspicious communication link. Unfortunately, a wireless communication medium has the nature of randomness and accordingly, it is not guaranteed that a channel from a source node to the monitor node is always better than to the destination node. Thus, in order to achieve the successful eavesdropping, the monitor node generally utilizes a jamming method to degrade achievable rate of the destination node in the suspicious link [42].

In general, there are two kinds of how the monitor node operates the jamming method; a half-duplex and a full-duplex. In the half-duplex jamming method, the monitor node conducts the eavesdropping and the jamming separately. That is, the monitor

node should select whether to eavesdrop or to jam the suspicious link at a given time duration. Whereas, in the full-duplex jamming method, the monitor node can fulfill the eavesdropping and the jamming simultaneously. Thus, the monitor node operating in the full-duplex jamming method has two antenna groups; the one is for eavesdropping and the other is for jamming. Since these two antenna groups have to be deployed nearby with each other, the jamming signal transmitted from the antenna group acts as an interference signal to the other antenna group, which is called a self-interference problem. To overcome this problem, the self-interference cancellation method is generally introduced both in software and hardware domain. If the self-interference can be perfectly removed, the full-duplex jamming method has great advantage over the half-duplex jamming method in terms of a time-efficiency.

For this advantage, studies about proactive eavesdropping have been carried out with the full-duplex jamming method [20, 21, 28, 42]. However, in [20, 21, 28], the self-interference problem is ignored with the assumption that the self-interference is perfectly cancelled by some methods. Authors in [42] considered the self-interference and proposed the mitigation method of that, but only under the condition the monitor node is equipped with multi-antennas. Motivated by that, in this chapter, I investigate the effect of imperfect self-interference cancellation in proactive eavesdropping using the full-duplex jamming method, and propose a half-duplex dual monitor method to overcome the self-interference problem efficiently even if monitor nodes are equipped with a single antenna. In the half-duplex dual monitor method, two distant monitor nodes are introduced to eavesdrop the suspicious communication link while getting spatial diversity and preventing self-interference simultaneously. I also design an adaptive transmission scheme for the proposed method to maximize the proactive eavesdropping performance. Finally, the proposed method with the adaptive transmission scheme is validated through numerical analysis.

## 4.2 System Model

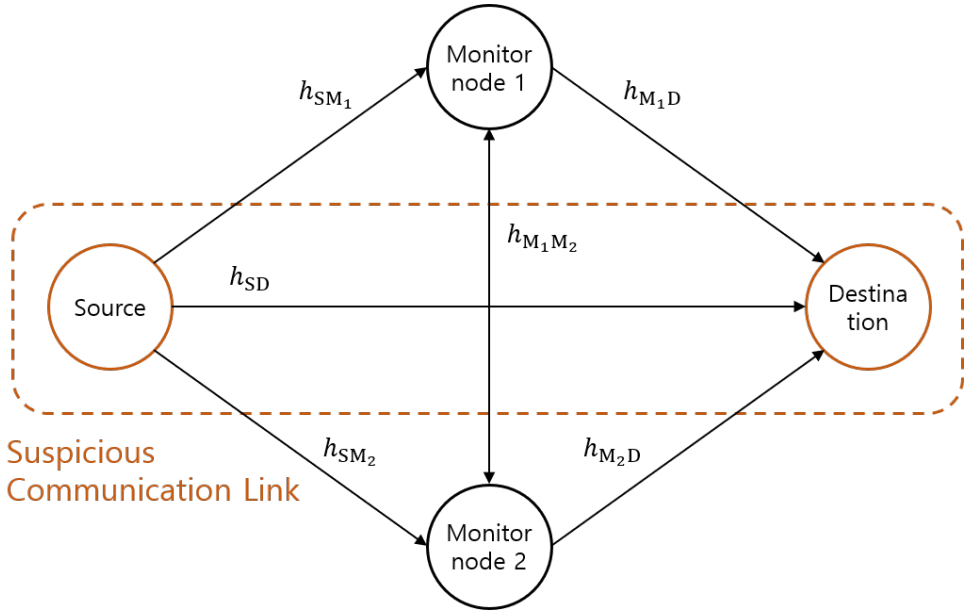



Figure 4.1: Description of the two-hop DF relay network topology

### 4.2.1 Network Topology

I consider a communication network where a suspicious source node and a suspicious destination node and a dual monitor exist as shown in Fig.4.1. The dual monitor consists of two half-duplex nodes; one is for eavesdropping and the other is for jamming. All nodes in the network assumed to be equipped with a single antenna. I assume that the the dual monitor is authorized to access the global channel state information (CSI) of the network by a central system and other nodes cannot know existence of the dual monitor node. These assumptions are realistic based on the fact that the monitor nodes are generally qualified as high-level users and accordingly, are empowered to access all information provided by the central system. The channel coefficient between of the link between node X and node Y is denoted by $h_{XY}$ as shown in Fig.4.1. All channel

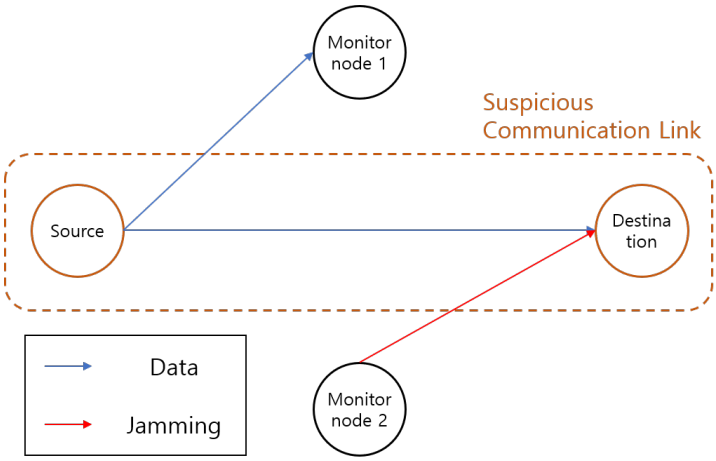
coefficients are reciprocal, that is, they satisfy the following equation;

$$h_{\mathrm{XY}} = h_{\mathrm{YX}}$$

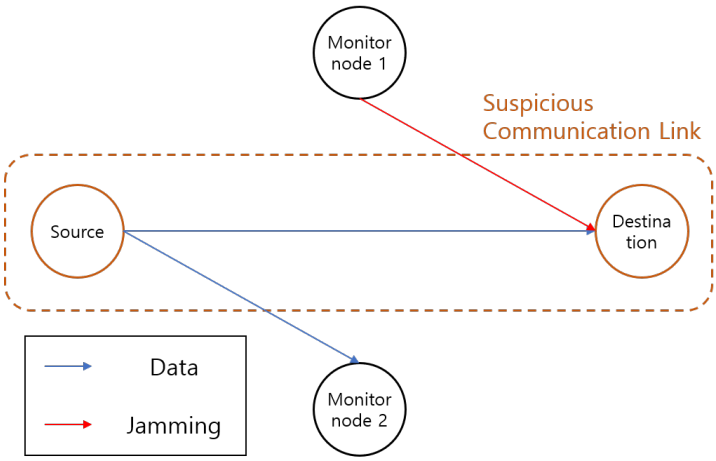
Furthermore, all channels of the network are assumed as Gaussian channels. In other words, a channel noise of each link can be modeled as a zero-mean Gaussian random variable with variance $\sigma^2$.

### 4.2.2 Transmission Protocol

The suspicious source node transmits a signal to the suspicious destination node. At the same time, one half-duplex node of the dual monitor eavesdrops the signal and the other half-duplex node jams the signal reception of the suspicious destination node. All channel coefficients are assumed to be stationary during the signal transmission. Although the half-duplex node for eavesdropping already knows this artificial noise via sharing information with the central system, it is assumed that the artificial noise cannot be removed entirely because of the limit in the software domain or the hardware domain. This implies that the residual artificial noise acts as a interference to the monitor node for eavesdropping. Moreover, since the two half-duplex monitor nodes can switch their roles with each other, the central system can select two options adaptively depending on the channel conditions of the network. The whole signal transmission process of each option is graphically described in Fig.4.2.




(a) 1st option




(b) 2nd option

Figure 4.2: Graphical illustration of the transmission protocol in the two options; (a) the 1st option and (b) the 2nd option.

### 4.2.3 Achievable Rate

As shown in Fig.4.2, for the $i$th option, the monitor node for eavesdropping is given by

$$\mathrm{E}_i = \begin{cases} \mathrm{M}_1, & \text{if } i = 1, \\ \mathrm{M}_2, & \text{if } i = 2. \end{cases}$$

At the same time, the monitor node for jamming is given by

$$\mathrm{J}_i := \begin{cases} \mathrm{M}_2, & \text{if } i = 1, \\ \mathrm{M}_1, & \text{if } i = 2. \end{cases}$$

Then, for the $i$th option, the received signal at the monitor node $\mathrm{E}_i$ is expressed as

$$r_{\mathrm{E},i} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SE}_i} s + \sqrt{Q} h_{\mathrm{J}_i\mathrm{E}_i} \sqrt{\Gamma_{\mathrm{res}}} a + n_{\mathrm{M}}, \tag{4.1}$$

where $s$, $a$, $P_{\mathrm{S}}$, $Q$, $n_{\mathrm{M}}$, and $\Gamma_{\mathrm{res}}$ denote the normalized transmit signal, the normalized artificial noise, the transmit power, the jamming power, the zero-mean AWGN with variance $\sigma^2$ at the monitor node for eavesdropping, and the ratio of the residual artificial noise power to the jamming power, respectively. In addition, the achievable rate function of the monitor node $\mathrm{E}_i$ is given by

$$\mathcal{C}_{\mathrm{E},i}(Q) = \log_2 \left\{ 1 + \frac{\alpha_{\mathrm{SE}_i} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{J}_i\mathrm{E}_i} \Gamma_{\mathrm{res}} Q} \right\}. \tag{4.2}$$

The received signal at the suspicious destination node D for the $i$th option can be expressed as

$$r_{\mathrm{D},i} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SD}} s + \sqrt{Q} h_{\mathrm{J}_i\mathrm{D}} a + n_{\mathrm{D}}, \tag{4.3}$$

where $n_{\mathrm{D}}$ denotes the zero-mean AWGN with variance $\sigma^2$ at the suspicious destination node D. Then, the achievable rate function of the suspicious destination node D for the $i$th option is given by

$$\mathcal{C}_{\mathrm{D},i}(Q) = \log_2 \left\{ 1 + \frac{\alpha_{\mathrm{SD}} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{J}_i\mathrm{D}} Q} \right\}. \tag{4.4}$$

## 4.3 Optimal Transmission Scheme

In this section, I aim to find the optimal transmission scheme for maximizing the proactive eavesdropping performance. To this end, I classify the channel conditions into separate cases based on Table 4.1.

Table 4.1: Channel conditions classification

| Channel conditions | | | Case |
|---|---|---|---|
| $\alpha_{\mathrm{SM}_1} \geq \alpha_{\mathrm{SM}_2}$ | $\alpha_{\mathrm{SM}_1} \geq \alpha_{\mathrm{SD}}$ | | 1 |
| | $\alpha_{\mathrm{SM}_1} < \alpha_{\mathrm{SD}}$ | $\frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 2 |
| | | $\frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 3 |
| $\alpha_{\mathrm{SM}_1} < \alpha_{\mathrm{SM}_2}$ | $\alpha_{\mathrm{SM}_2} \geq \alpha_{\mathrm{SD}}$ | | 4 |
| | $\alpha_{\mathrm{SM}_2} < \alpha_{\mathrm{SD}}$ | $\frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 5 |
| | | $\frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 6 |

In Case 1 or Case 4, the dual monitor can eavesdrop the suspicious communication link successfully without the jamming. Therefore, the optimal transmission scheme for Case 1 or Case 4 is no jamming while only eavesdropping. However, in other Cases, the optimal transmission scheme depends on the maximum available jamming power. That is, in Cases except Case 1 and Case 4, the optimal transmission scheme is determined by the jamming power conditions as shown in Table 4.2. In each optimal transmission scheme, actions of two monitor nodes are presented in Table 4.3

Table 4.2: Case classification

| Case Number | Conditions | | Scheme Number |
|---|---|---|---|
| 1 | | | 1 |
| 2 | $Q_{\max} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | | 2 |
| | $Q_{\max} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | | 3 |
| 3 | $Q_{\max} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | | 2 |
| | $Q_{\max} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | $Q_{\max} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 4 |
| | | $Q_{\max} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 3 |
| 4 | | | 5 |
| 5 | $Q_{\max} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | | 4 |
| | $Q_{\max} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | | 3 |
| 6 | $Q_{\max} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | | 4 |
| | $Q_{\max} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_2}}{\alpha_{\mathrm{SM}_2}\alpha_{\mathrm{M}_1\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | $Q_{\max} \geq \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 2 |
| | | $Q_{\max} < \frac{\alpha_{\mathrm{SD}}-\alpha_{\mathrm{SM}_1}}{\alpha_{\mathrm{SM}_1}\alpha_{\mathrm{M}_2\mathrm{D}}-\Gamma_{\mathrm{res}}\alpha_{\mathrm{SD}}\alpha_{\mathrm{M}_1\mathrm{M}_2}}$ | 3 |

Table 4.3: Optimal transmission scheme

| Scheme Number | Monitor Node 1 | Monitor Node 2 |
|---|---|---|
| 1 | Eavesdropping | Rest |
| 2 | Eavesdropping | Jamming |
| 3 | Rest | Rest |
| 4 | Jamming | Eavesdropping |
| 5 | Rest | Eavesdropping |

## 4.4 Numerical Results

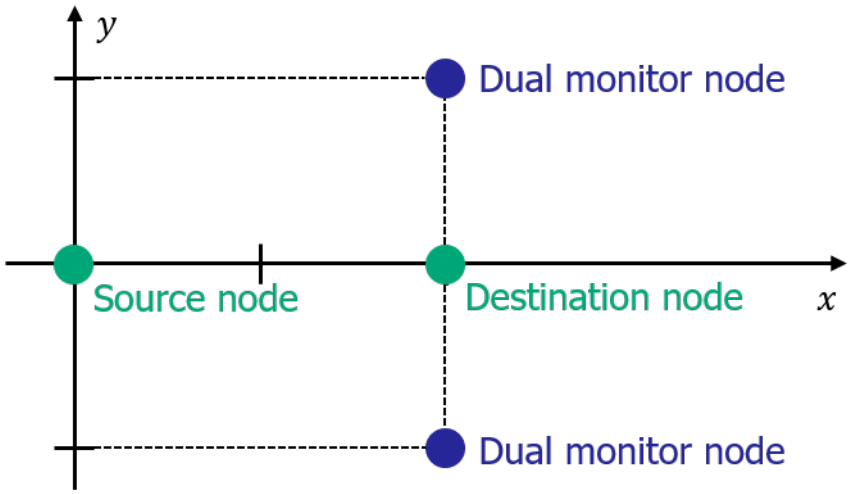



Figure 4.3: Graphical illustration of the network topology in the simulation.

In this section, I verify the proactive eavesdropping performance of the proposed method via the numerical simulation. First, the network topology used in the simulation is described in Fig.4.3. As shown in Fig.4.3, all nodes are coplanar points located in 2-dimensional x-y plane. The coordinates of the suspicious source node, the suspicious destination node and the two monitor nodes are $(0, 0)$, $(0, 2)$, and $(-2, 1)$, $(2, 1)$, respectively. Each channel coefficient between two arbitrary two nodes is generated based on the COST-207 Typical Urban 6-ray channel model. That is, channel coefficient between node A and node B is given by

$$h_{\mathrm{AB}} = (d_{\mathrm{AB}})^{-2} \sum_{z=1}^{z=6} g_z e^{-j2\pi f \delta_z},$$

where $d_{\mathrm{AB}} := \sqrt{(x_{\mathrm{X}} - x_{\mathrm{Y}})^2 + (y_{\mathrm{X}} - y_{\mathrm{Y}})^2}$, and $f$ is the radio frequency, and $g_z$ is the $z$th fading and is given by an independent complex Gaussian random variable with zero-mean and variance $\gamma_z$. In addition, the used path powers, $\{\gamma_z\}_{z=1}^{z=6}$, and the used

path delays, $\{\delta_z\}_{z=1}^{z=6}$ is given as follows;

$$\{\gamma_z\}_{z=1}^{z=6} = \{0.189, 0.379, 0.239, 0.095, 0.061, 0.037\},$$

$$\{\delta_z\}_{z=1}^{z=6} = \{0.0, 0.2, 0.5, 1.6, 2.3, 5\} * 10^{-6}.$$

Throughout the section, I use the ratio of the maximum available power for the monitor to the total power consumed for the suspicious communication link, $\Gamma_{Q_{\max}}$, instead of the maximum available power for the monitor, $Q_{\max}$. The ratio, $\Gamma_{Q_{\max}}$, is defined as

$$\Gamma_{Q_{\max}} := \frac{Q_{\max}}{P_{\mathrm{S}}}.$$

Fig.4.4 and Fig.4.5 shows the outage probability and eavesdropping rate performance versus the maximum available jamming power, respectively. For comparison, I also present the proactive performances of the conventional method using the full-duplex monitor node with the imperfect self-interference cancellation. Moreover, it is assumed that the self-interference is mitigated by a factor of $10^{-5}$. As shown in two figures, the proposed method with optimal transmission scheme is superior than the conventional method using the full-duplex node. This implies that the proposed method efficiently overcomes the self-interference caused by the full-duplex node. Even the eavesdropping rate performance of the conventional method using the full-duplex node decreases as the maximum available jamming power increases. This is because the self-interference quantity is also increasing as the jamming power is increasing. In other words, it is not guaranteed that the eavesdropping rate of the monitor node is enhanced when more jamming power is consumed.

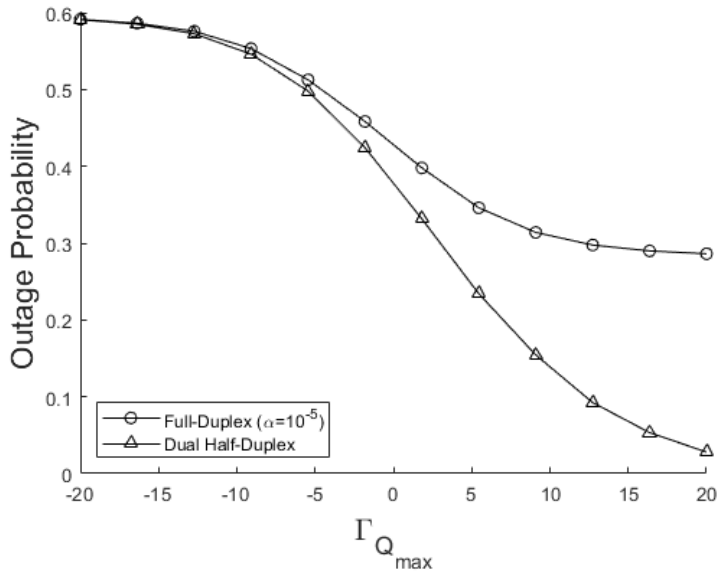



Figure 4.4: Outage probability versus the maximum available jamming power.

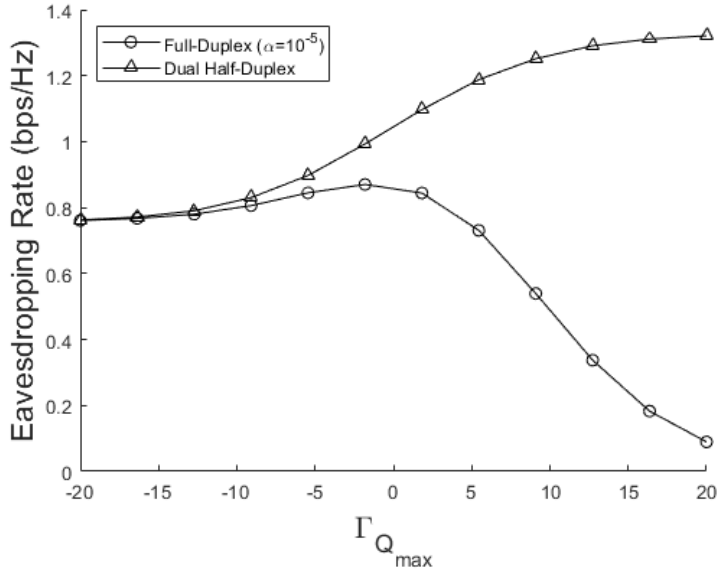



Figure 4.5: Eavesdropping rate versus the maximum available jamming power.

## 4.5 Summary

To overcome the self-interference problem, this chapter studied proactive eavesdropping using the half-duplex dual node which one of two monitor nodes is for eavesdropping and the other is for jamming. In addition, I proposed the adaptive transmission protocol for the half-duplex dual node and designed optimal transmission scheme for improving the proactive eavesdropping performance. Finally, through numerical analysis, it was verified that the proposed method with the optimal transmission scheme is superior both in terms of the eavesdropping rate and the outage probability than the conventional method with the self-interference problem caused by the full-duplex monitor node.

# Bibliography


[1] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC, FL, Boca Raton, 1996.

[2] J. Xu, L. Duan and R. Zhang, "Surveillance and Intervention of Infrastructure-Free Mobile Communications: A New Wireless Security Paradigm," *IEEE Wireless Communications*, vol. 24, no.4, pp. 152-159, Aug. 2017.

[3] R. Atat, L. Liu, J. Ashdown, M. J. Medley, J. D. Matyjas and Y. Yi, "A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems," *IEEE Internet of Things Journal*, vol. 5, no.1, pp. 295-309, Feb. 2018.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no.8, pp. 1355-1387, Oct. 1975.

[5] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, no.10, pp. 2135-2157, Dec. 1984.

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

[7] J. Li, A. P. Petropulu and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Transactions on Signal Processing*, vol. 59, no.10, pp. 4985-4997, Oct. 2011.

[8] G. Zheng, L. -C. Choo and K. -K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no.3, pp. 1317-1322, March 2011.

[9] J. -H. Lee, "Optimal Power Allocation for Physical Layer Security in Multi-Hop DF Relay Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no.1, pp. 28-38, Jan. 2016.

[10] H. Guo, Z. Yang, L. Zhang, J. Zhu and Y. Zou, "Joint Cooperative Beamforming and Jamming for Physical-Layer Security of Decode-and-Forward Relay Networks," *IEEE Access*, vol. 5, pp. 19620-19630, 2017.

[11] S. Jia, J. Zhang, H. Zhao, Y. Lou and Y. Xu, "Relay Selection for Improved Physical Layer Security in Cognitive Relay Networks Using Artificial Noise," *IEEE Access*, vol. 6, pp. 64836-64846, 2018.

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

[13] 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 Transactions on Information Forensics and Security*, vol. 8, no.12, pp. 2007-2020, Dec. 2013.

[14] Y. Feng, S. Yan, Z. Yang, N. Yang and J. Yuan, "User and Relay Selection With Artificial Noise to Enhance Physical Layer Security," *IEEE Transactions on Vehicular Technology*, vol. 67, no.11, pp. 10906-10920, Nov. 2018.

[15] C. Wang, H. -M. Wang and X. -G. Xia, "Hybrid Opportunistic Relaying and Jamming With Power Allocation for Secure Cooperative Networks," *IEEE Transactions on Wireless Communications*, vol. 14, no.2, pp. 589-605, Feb. 2015.

[16] C. Jeong and I. -M. Kim, "Optimal Power Allocation for Secure Multicarrier Relay Systems," *IEEE Transactions on Signal Processing*, vol. 59, no.11, pp. 5428-5442, Nov. 2011.

[17] Z. Bai, S. Liang, P. Ma, Y. Dong, H. Zhang and Y. Ma, "QoS Driven Power Allocation in Secure Multicarrier Full-Duplex Relay Systems," *IEEE Transactions on Wireless Communications*, vol. 19, no.2, pp. 929-941, Feb. 2020.

[18] M. Nawaz, W. U. Khan, Z. Ali, A. Ihsan, O. Waqar and G. A. S. Sidhu, "Resource Optimization Framework for Physical Layer Security of Dual-Hop Multi-Carrier Decode and Forward Relay Networks," *IEEE Open Journal of Antennas and Propagation*, vol. 2, pp. 634-645, 2021.

[19] J. Xu, L. Duan and R. Zhang, "Surveillance and Intervention of Infrastructure-Free Mobile Communications: A New Wireless Security Paradigm," *IEEE Wireless Communications*, vol. 24, no.4, pp. 152-159, Aug. 2017.

[20] J. Xu, L. Duan and R. Zhang, "Proactive Eavesdropping Via Jamming for Rate Maximization Over Rayleigh Fading Channels," *IEEE Wireless Communications Letters*, vol. 5, no.1, pp. 80-83, Feb. 2016.

[21] J. Xu, L. Duan and R. Zhang, "Proactive Eavesdropping via Cognitive Jamming in Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 16, no.5, pp. 2790-2806, May 2017.

[22] C. Zhong, X. Jiang, F. Qu and Z. Zhang, "Multi-Antenna Wireless Legitimate Surveillance Systems: Design and Performance Analysis," *IEEE Transactions on Wireless Communications*, vol. 16, no.7, pp. 4585-4599, July 2017.

[23] Y. Cai, C. Zhao, Q. Shi, G. Y. Li and B. Champagne, "Joint Beamforming and Jamming Design for mmWave Information Surveillance Systems," *IEEE Journal on Selected Areas in Communications*, vol. 36, no.7, pp. 1410-1425, July 2018.

[24] L. Sun, Y. Zhang and A. L. Swindlehurst, "Alternate-Jamming-Aided Wireless Physical-Layer Surveillance: Protocol Design and Performance Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1989-2003, 2021.

[25] Y. Ge and P. C. Ching, "Energy Efficiency for Proactive Eavesdropping in Cooperative Cognitive Radio Networks," *IEEE Internet of Things Journal*, vol. 9, no.15, pp. 13443-13457, Aug. 2022.

[26] D. Xu and H. Zhu, "Proactive Eavesdropping for Wireless Information Surveillance Under Suspicious Communication Quality-of-Service Constraint," *IEEE Transactions on Wireless Communications*, vol. 21, no.7, pp. 5220-5234, July 2022.

[27] G. Hu, F. Zhu, J. Si, Y. Cai and N. Al-Dhahir, "Proactive Eavesdropping With Jamming Power Allocation in Training-Based Suspicious Communications," *IEEE Signal Processing Letters*, vol. 29, pp. 667-671, Feb. 2022.

[28] F. Feizi, M. Mohammadi, Z. Mobini and C. Tellambura, "Proactive Eavesdropping via Jamming in Full-Duplex Multi-Antenna Systems: Beamforming Design and Antenna Selection," *IEEE Transactions on Communications*, vol. 68, no.12, pp. 7563-7577, Dec. 2020.

[29] G. Ma, J. Xu, L. Duan and R. Zhang, "Wireless surveillance of two-hop communications : (Invited paper)," *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Sapporo, Japan, July 2017, pp. 1-5.

[30] X. Jiang, H. Lin, C. Zhong, X. Chen and Z. Zhang, "Proactive Eavesdropping in Relaying Systems," *IEEE Signal Processing Letters*, vol. 24, no.6, pp. 917-921, June 2017.

[31] D. Hu, Q. Zhang, P. Yang and J. Qin, "Proactive Monitoring via Jamming in Amplify-and-Forward Relay Networks," *IEEE Signal Processing Letters*, vol. 24, no.11, pp. 1714-1718, Nov. 2017.

[32] J. Moon, H. Lee, C. Song, S. Lee and I. Lee, "Proactive Eavesdropping With Full-Duplex Relay and Cooperative Jamming," *IEEE Transactions on Wireless Communications*, vol. 17, no.10, pp. 6707-6719, Oct. 2018.

[33] B. Li, Y. Yao, H. Zhang and Y. Lv, "Energy Efficiency of Proactive Cooperative Eavesdropping Over Multiple Suspicious Communication Links," *IEEE Transactions on Vehicular Technology*, vol. 68, no.1, pp. 420-430, Jan. 2019.

[34] J. Moon, S. H. Lee, H. Lee and I. Lee, "Proactive Eavesdropping With Jamming and Eavesdropping Mode Selection," *IEEE Transactions on Wireless Communications*, vol. 18, no.7, pp. 3726-3738, July 2019.

[35] G. Hu, J. Ouyang, Y. Cai and Y. Cai, "Proactive Eavesdropping in Two-Way Amplify-and-Forward Relay Networks," *IEEE Systems Journal*, vol. 15, no.3, pp. 3415-3426, Sept. 2021.

[36] G. Hu, Y. Cai and J. Ouyang, "Proactive Eavesdropping via Jamming for Multichannel Decode-and-Forward Relay System," *IEEE Communications Letters*, vol. 24, no.3, pp. 491-495, March 2020.

[37] D. Xu, "Legitimate Surveillance of Suspicious Multichannel DF Relay Networks With Monitor Mode Selection," *IEEE Wireless Communications Letters*, vol. 10, no.2, pp. 401-405, Feb. 2021.

[38] G. Hu, J. Si, Y. Cai and F. Zhu, "Proactive Eavesdropping via Jamming in UAV-Enabled Suspicious Multiuser Communications," *IEEE Wireless Communications Letters*, vol. 11, no.1, pp. 3-7, Jan. 2022.

[39] G. Hu, J. Si, Y. Cai and N. Al-Dhahir, "Proactive Eavesdropping via Jamming in UAV-Enabled Relaying Systems With Statistical CSI," *IEEE Signal Processing Letters*, vol. 29, pp. 1267-1271, 2022.

[40] A. A. Nasir, X. Zhou, S. Durrani and R. A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing," *IEEE Transactions on Wireless Communications*, vol. 12, no.7, pp. 3622-3636, July 2013.

[41] European Commission and Directorate-General for the Information Society and Media, *COST 207: Digital Land Mobile Radio Communications*, Luxembourg City, Luxembourg:Publication Office of the European Union, 1990.

[42] L. Yang, J. Cui, R. Ma, H. Wu and J. Ou, "Proactive Eavesdropping Scheme via Decode-and-Forward Relay with Multiple Full-Duplex Antennas," *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, Chongqing, China, 2020, pp. 1232-1237.

# 초 록

사물인터넷 (Internet of Things)와 같은 높은 연결성을 지닌 무기반시설의 통신 네트워크가 등장함에 따라 통신망의 규모가 나날이 증가하고 있습니다. 하지만, 통신망의 규모가 커질수록 포함된 사용자의 수도 함께 높아지게 되는데 이는 통신 보안 위협의 발생 확률을 높이기도 합니다. 이러한 이유로 신뢰할 수 있는 통신의 보안성은 거대한 통신 네트워크를 구축하는 데 있어 아주 중요한 문제입니다. 이에 본 학위 논문은 거대한 통신 네트워크의 보안성을 확보하는 것을 목표로 크게 세 가지의 주제를 연구하고자 합니다.

첫 번째 주제로 저는 거대한 네트워크에서의 물리계층보안 (Physical-layer security)을 연구합니다. 특히, 하드웨어 제약으로 인해 단일 안테나가 장착될 수 밖에 없는 장치로 가정된 노드가 다수 분포되어 있는 통신 네트워크를 고려합니다. 이러한 통신 네트워크는 단일 안테나의 방사 특성으로 인해 도청 종류의 보안 공격에 매우 취약한 면모를 보입니다. 이에 대응하여 통신의 보안성을 확보하기 위해, 저는 적응적 중계 노드 선택과 협력적 재밍을 병행하는 기법을 제안합니다. 또한, 제안된 기법에 적합한 최적 중계 노드 선택 방안과 최적 전력 할당을 함께 도출하여 성능을 극대화하고자 합니다.

두 번째 주제로는 사전대응적 도청 (Proactive eavesdropping) 기법에 대해 연구합니다. 능동적 도청은 무기반시설 통신 네트워크에서 발생할 수 있는 새로운 유형의 통신 보안 위협에 대해 대처할 수 있는 기법입니다. 또한, 일반적인 무기반시설 통신 네트워크를 고려하기 위해 의심스러운 통신 링크와 독립적으로 동작하는 감시 노드를 상정합니다. 저는 이러한 시스템 모델에서 능동적 도청의 성능을 향상시킬 수 있는 적응형 전이중 재밍-도움 기법을 제안하고, 제안 기법의 성능을 극대화할

수 있는 전력 할당 방안을 최적화 문제를 통해 함께 도출합니다.

마지막 주제로 저는 능동적 도청 기법에서 전이중 방식이 갖는 부정적인 효과인 불완전한 자기간섭 완화 문제에 대해 연구합니다. 전이중 방식의 능동적 도청 기법에서는 불완전한 자기간섭 완화가 큰 성능 저하를 초래할 수 있습니다. 이를 극복하기 위해, 저는 반이중 방식의 감시 노드쌍 기반의 능동적 도청 방식을 제안합니다. 또한, 제안 기법의 성능을 극대화하기 위한 감시 노드쌍의 전력 할당을 도출하고 시뮬레이션을 통해 제안 기법이 효과적으로 전이중 방식의 불완전한 자기간섭 완화 문제를 회피할 수 있음을 보여주고자 합니다.

**주요어**: 무기반시설 통신 네트워크, 거대 네트워크, 최적 전력 할당, 물리계층보안, 능동적 도청

**학번**: 2015-20953