IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 26 May 2023, accepted 30 May 2023, date of publication 2 June 2023, date of current version 12 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3282222

RESEARCH ARTICLE

Proactive Eavesdropping With Adaptive Full-Duplex Jamming-Helping Method for Infrastructure-Free Relay Networks

YOUNG-JUN YOON[1,2], (Member, IEEE), WANJEI CHO[1,2], SEONGWOOK LEE[3], (Member, IEEE), JONG-HO LEE[4], (Member, IEEE), JIHO SONG[5], (Member, IEEE), AND SEONG-CHEOL KIM[1,2], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Seoul National University, Seoul 08826, South Korea
[2]INMC, Seoul National University, Seoul 08826, South Korea
[3]School of Electrical and Electronics Engineering, College of ICT Engineering, Chung-Ang University, Dongjak-gu, Seoul 06974, South Korea
[4]School of Electronic Engineering, Soongsil University, Seoul 06978, South Korea
[5]Department of Electrical and Electronic Engineering, Hanyang University, ERICA, Ansan 15588, South Korea

Corresponding author: Seong-Cheol Kim (sckim@maxwell.snu.ac.kr)

This work was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-2021-0-02048) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) and in part by Samsung Electronics Co., Ltd (IO-210202-08366-01).

ABSTRACT With the emergence of advanced communication technologies such as infrastructure-free communication networks, the need for proactive eavesdropping which can constantly monitor and intervene in the communication network is growing. In response to those demands, we study proactive eavesdropping in the general infrastructure-free communication scenario where the legitimate eavesdropper has to monitor a suspicious communication link without the aid of other nodes. Particularly, to enhance proactive eavesdropping performances, we propose the adaptive full-duplex jamming-helping method in which the legitimate eavesdropper selects the best operating mode adaptively depending on the channel conditions unlike conventional studies where the behavior of the monitor node was predetermined. Moreover, we design the optimal power scheme for the proposed method to maximize the eavesdropping rate while minimizing total power consumption of the legitimate eavesdropper simultaneously. In the process, we classify the channel conditions into several mutual exclusive cases to simplify the optimization problem, and present the optimal solution in closed form for each case. Finally, it is verified through simulation results that the proposed method is superior in terms of both the eavesdropping rate and the outage probability than other benchmark methods.

INDEX TERMS Adaptive, full-duplex, infrastructure-free, jamming, power allocation, proactive eavesdropping, relay networks.

I. INTRODUCTION

With the development of ubiquitous systems such as Internet of Things (IoT), recent wireless communication systems are expected to realize more accessible and user-friendly communication networks. In particular, the infrastructure-free communication networks have been more attractive technology since it can allow the communication networks to include more diverse type of users such as mobiles, robots, unmanned aerial vehicle (UAV) and so on. Nevertheless, infrastructure-free communication networks are highly vulnerable to security threats by malicious users who want to use those networks for harmful purposes [1]. For instance, the malicious user can actively exploit communication links of the networks to commit crimes or acts of terror. Unfortunately, conventional security approaches such as cryptography [2] and physical layer security (PLS) [3], [4], [5], [6], [7], [8] are not suitable for those 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

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

security approaches to constantly monitor and intervene in the communication networks increasingly grows [1], [9], [10].

In response to this, a method, which is called proactive eavesdropping, was first proposed by [1], [9], and [10]. 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 [9] and [10], the legitimate eavesdropper used full-duplex jamming method to degrade the achievable rate for the suspicious user. In succession to [9] and [10], many studies also proposed proactive eavesdropping approaches with the jamming method. References [11] and [12] extended the works of [9] and [10] 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 [13] 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 [14] designed the proactive eavesdropping system which improves the eavesdropping performance by using the secondary user as the jamming signal in cognitive radio networks. In [15], 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 [16] 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 [17] 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 [18], [19], [20], [21], [22], [23], [24], [25], and [26], 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 [18] 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 [19], 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 [20] considered the two-hop amplify-and-forward (AF) relay network and designed the jamming power for maximizing the average eavesdropping rate. The study in [21] 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 [22], two half-duplex cooperative eavesdroppers were introduced to maximize the eavesdropping energy efficiency. Reference [23] 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 [24] 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 [25] 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 [26], 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 [27], [28] have considered characteristics of the infrastructure-free network in the general relay communication system model. In [27], 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 [28] 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, [27] lacks a consideration about relay communications which is a important property of the infrastructure-free network. The study of [28] 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, we present a system model for the general infrastructure-free communication network scenario. Furthermore, to enhance the performance of proactive eavesdropping, we 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) We 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, we 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) We 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, we present five mutually exclusive cases by classifying channel conditions. Subsequently, for each case, we obtain the optimal power scheme in closed form by solving the simplified problem.
3) We 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, we 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.

The remainder of the paper is organized as follows. In Section II, we describe the system model such as the network topology, the communication protocol, and the maximum achievable rate. In Section III, the optimal power for achieving our goal is derived. In Section IV, the numerical results are presented. Lastly, we conclude the paper in Section V.

II. SYSTEM MODEL

We consider a two-hop relay infrastructure-free network where a suspicious communication link exists as shown in Fig. 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

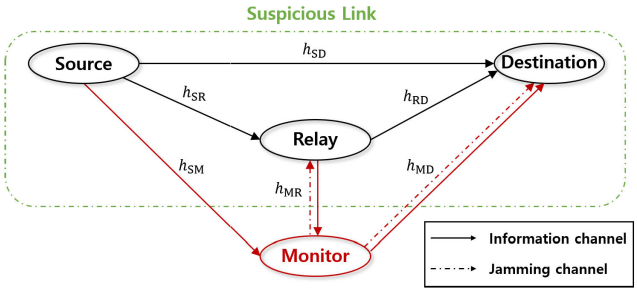


FIGURE 1. The network topology in the system model.

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, we assume that all nodes in the suspicious link is not aware of the presence of the monitor node [18]. 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 [19]. It is also assumed that all nodes have mobility, that is, they can move freely inside the network. In Fig. 1, h_{XY} denotes the channel coefficient of the link between node X and node Y. For instance, h_{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 σ^2 implying the noise power.

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, we 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, we 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 [29], in which two time slots are spent for one signal to be transmitted to the destination node. This process is described graphically in Fig. 2.

As shown in Fig. 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

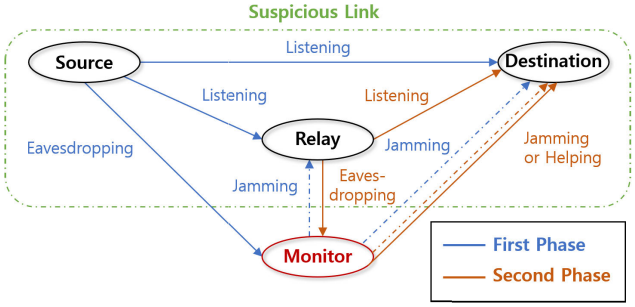


FIGURE 2. The communication protocol in the system model.

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.

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

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

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_{S}, $q^{(1)}$ and n_{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

$$\mathcal{R}_{\mathrm{R}}(q^{(1)}) := \log_2\left(1 + \frac{\alpha_{\mathrm{SR}} P_{\mathrm{S}}}{1 + \alpha_{\mathrm{MR}} q^{(1)}}\right), \tag{2}$$

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

$$r_{\mathrm{M}}^{(1)} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SM}} s_t + n_{\mathrm{M}}^{(1)}, \tag{3}$$

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

$$\mathcal{R}_{\mathrm{M}} = \log_2\left(1 + \alpha_{\mathrm{SM}} P_{\mathrm{S}}\right), \tag{4}$$

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

$$r_{\mathrm{M}}^{(2)} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{MR}} s_t + n_{\mathrm{M}}^{(2)}, \tag{5}$$

where P_{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

$$\mathcal{C}_{\mathrm{M}} = \log_2\left\{1 + \lambda_{\mathrm{M}} P_{\mathrm{S}}\right\}. \tag{6}$$

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

$$r_{\mathrm{D}}^{(1)} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SD}} s_t + \sqrt{q^{(1)}} h_{\mathrm{MD}} s_j + n_{\mathrm{D}}^{(1)}, \tag{7}$$

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

$$r_{\mathrm{D}}^{(2)} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{RD}} s_t + \sqrt{q^{(2)}} h_{\mathrm{MD}} s_{\mathrm{M}} + n_{\mathrm{D}}^{(2)}, \tag{8}$$

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_{M} denotes the adaptive signal transmitted at the monitor node M in the second phase, which is given by

$$s_{\mathrm{M}} = \begin{cases} s_j, & \text{if } \mathcal{R}_{\mathrm{M}} < \mathcal{R}_{\mathrm{R}}(q^{(1)}), \\ s_t, & \text{if } \mathcal{R}_{\mathrm{M}} \geq \mathcal{R}_{\mathrm{R}}(q^{(1)}). \end{cases} \tag{9}$$

Equation (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

$$\mathcal{R}_{\mathrm{D}}(\boldsymbol{q}) := \begin{cases} \mathcal{R}_{\mathrm{DJ}}(\boldsymbol{q}), & \text{if } \mathcal{R}_{\mathrm{M}} < \mathcal{R}_{\mathrm{R}}(q^{(1)}), \\ \mathcal{R}_{\mathrm{DH}}(\boldsymbol{q}), & \text{if } \mathcal{R}_{\mathrm{M}} \geq \mathcal{R}_{\mathrm{R}}(q^{(1)}), \end{cases} \tag{10}$$

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

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

TABLE 1. The five cases of channel conditions.

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

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

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

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

Consequently, the achievable rate function of the destination node D for two phases is given by [8]

$$\mathcal{C}_D(\boldsymbol{q}) := \begin{cases} \mathcal{C}_{DJ}(\boldsymbol{q}), & \text{if } \mathcal{R}_M < \mathcal{R}_R(q^{(1)}), \\ \mathcal{C}_{DH}(\boldsymbol{q}), & \text{if } \mathcal{R}_M \geq \mathcal{R}_R(q^{(1)}), \end{cases} \tag{11}$$

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

$$\mathcal{C}_{DJ}(\boldsymbol{q}) := \min\left(\mathcal{R}_R(q^{(1)}), \mathcal{R}_{DJ}(\boldsymbol{q})\right),$$
$$\mathcal{C}_{DH}(\boldsymbol{q}) := \min\left(\mathcal{R}_R(q^{(1)}), \mathcal{R}_{DH}(\boldsymbol{q})\right).$$

III. OPTIMAL POWER DESIGN

A. MAXIMIZING EAVESDROPPING RATE

In this section, we 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

$$\mathcal{E}_M(\boldsymbol{q}) = \begin{cases} \mathcal{C}_D(\boldsymbol{q}), & \text{if } \mathcal{C}_M \geq \mathcal{C}_D(\boldsymbol{q}), \\ 0, & \text{if } \mathcal{C}_M < \mathcal{C}_D(\boldsymbol{q}). \end{cases} \tag{12}$$

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

$$\begin{aligned} &\max_{\boldsymbol{q}} \ \mathcal{E}_M(\boldsymbol{q}) \\ &\text{s.t. } q^{(1)} \geq 0, \quad q^{(2)} \geq 0, \\ &\quad q^{(1)} + q^{(2)} \leq Q_{max}, \end{aligned} \tag{13}$$

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

The objective function of the optimization problem has different forms depending on the channel conditions of the suspicious network involving the monitor node. Thus, to solve the optimization problem, we first decide the form of the objective function in accordance with the channel conditions. Table 1 presents five mutually exclusive cases obtained by classifying the channel conditions based on the form of the objective function. Next, in each case, we solve the optimization problem in which the decided objective function is introduced.

Case 1: The successful eavesdropping condition ($\mathcal{C}_M \geq \mathcal{C}_D(\boldsymbol{q})$) is always satisfied regardless of the values of $q^{(1)}$ and $q^{(2)}$. In addition, the helping mode condition ($\mathcal{R}_M \geq \mathcal{R}_R(q^{(1)})$) is always satisfied regardless of the value of $q^{(1)}$. Accordingly, (13) can be transformed to

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

In *Case* 1, both $\mathcal{R}_{DH}(\cdot)$ and $\mathcal{R}_R(\cdot)$ are decreasing as $q^{(1)}$ increases. This implies that $\mathcal{C}_{DH}(\cdot)$ is also decreasing when $q^{(1)}$ is increasing. Therefore, the optimal $q^{(1)}$ is determined as the smallest value, i.e. zero. Further, $\mathcal{R}_R(0)$ is always smaller than $\mathcal{R}_{DH}(0, q^{(2)})$ regardless of the value of $q^{(2)}$. Then, the solution set of (13) for *Case* 1 is just given by

$$T_1 := \left\{\boldsymbol{q} \mid q^{(1)} = 0, \ 0 \leq q^{(2)} \leq Q_{max}\right\}. \tag{14}$$

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, (13) is transformed to

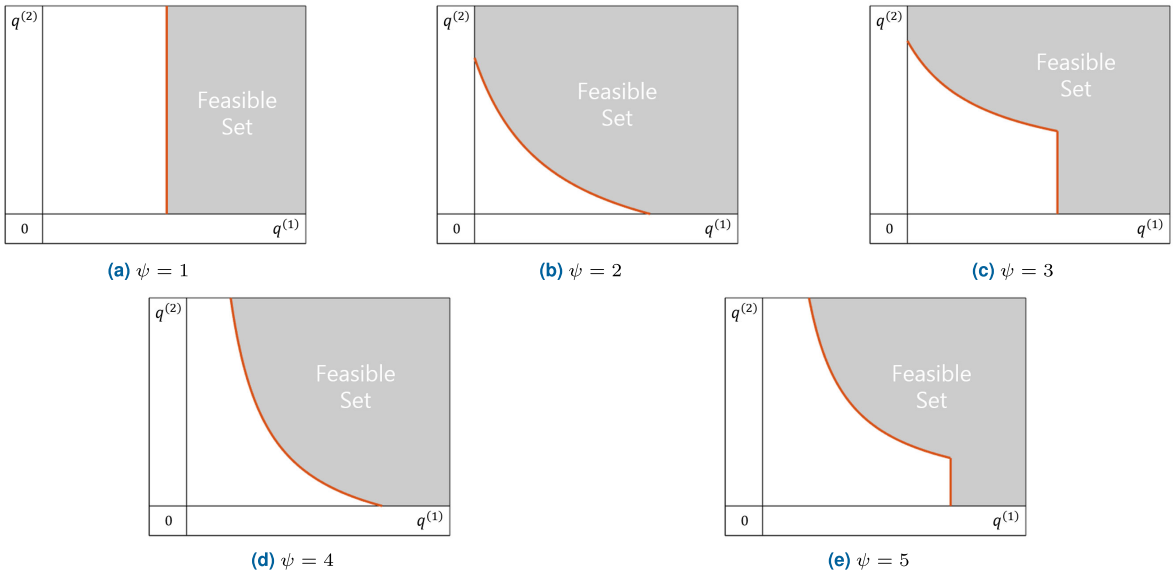
$$\begin{aligned} &\max_{\boldsymbol{q}} \ \mathcal{C}_{DH}(\boldsymbol{q}) \\ &\text{s.t. } q^{(1)} = 0, \quad 0 \leq q^{(2)} \leq Q_{max}. \end{aligned}$$

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

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

TABLE 2. The five sub-cases of channel conditions for *Case* 5.

Channel Conditions			ψ
$\alpha_{\mathrm{SR}}\alpha_{\mathrm{MD}} - \alpha_{\mathrm{SD}}\alpha_{\mathrm{MR}} \le \lambda_{\mathrm{M}}(\alpha_{\mathrm{MD}} - \alpha_{\mathrm{MR}})$			1
$\alpha_{\mathrm{SR}}\alpha_{\mathrm{MD}} - \alpha_{\mathrm{SD}}\alpha_{\mathrm{MR}} > \lambda_{\mathrm{M}}(\alpha_{\mathrm{MD}} - \alpha_{\mathrm{MR}})$	$\alpha_{\mathrm{SD}} < \lambda_{\mathrm{M}}$	$\alpha_{\mathrm{MR}}\lambda_{\mathrm{M}}(\alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}} - \lambda_{\mathrm{M}}) \le \alpha_{\mathrm{MD}}(\lambda_{\mathrm{M}} - \rho\alpha_{\mathrm{RD}})(\alpha_{\mathrm{SR}} - \lambda_{\mathrm{M}})$	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
	$\alpha_{\mathrm{SD}} \ge \lambda_{\mathrm{M}}$	$\alpha_{\mathrm{MR}}\lambda_{\mathrm{M}}(\alpha_{\mathrm{SD}} + \rho\alpha_{\mathrm{RD}} - \lambda_{\mathrm{M}}) \le \alpha_{\mathrm{MD}}(\lambda_{\mathrm{M}} - \rho\alpha_{\mathrm{RD}})(\alpha_{\mathrm{SR}} - \lambda_{\mathrm{M}})$	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



(a) $\psi = 1$ (b) $\psi = 2$ (c) $\psi = 3$

(d) $\psi = 4$ (e) $\psi = 5$

FIGURE 3. Description of the shape of $C_{\mathrm{M}} = C_{\mathrm{DJ}}(q)$ and the area according to the feasible set in the ψth sub-case of *Case* 5, i.e. *Case* 5_{ψ}.

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 (13) for *Case* 2 is given by

$$T_2 = \begin{cases} \{(0, Q_{\max})\}, & \text{if } 0 \le Q_{\max} < Q_{2,\mathrm{thr}}, \\ \left\{\boldsymbol{q} \mid q^{(1)} = 0, \right. & \\ \left. Q_{2,\mathrm{thr}} \le q^{(2)} \le Q_{\max}\right\}, & \text{if } Q_{\max} \ge Q_{2,\mathrm{thr}}. \end{cases} \tag{15}$$

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, (11) can be transformed to

$$\mathcal{C}_{\mathrm{D}}(\boldsymbol{q}) := \begin{cases} \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q}), & \text{if } q^{(1)} < q^{(1)}_{\mathrm{thr}}, \\ \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q}), & \text{if } q^{(1)} \ge q^{(1)}_{\mathrm{thr}}, \end{cases} \tag{16}$$

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

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

Then, based on (16), we divide the optimization problem to two sub-problems by distinguishing its own feasible set into two mutually exclusive subsets. In other words, (13) separates into two individual optimization problems depending on the operating mode of the monitor node. The first sub-problem is expressed as

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

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, we can easily know that the solution set of the first sub-problem is simply determined as

$$T_{3,\mathrm{sub1}} = \{(0, 0)\}. \tag{17}$$

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

$$\max_{\boldsymbol{q}} \mathcal{C}_{\mathrm{DH}}(\boldsymbol{q})$$

$$\text{s.t. } q^{(1)} \geq q_{\text{thr}}^{(1)}, \quad q^{(2)} \geq 0,$$
$$q^{(1)} + q^{(2)} \leq Q_{\max}.$$

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

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

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

$$T_{3,\text{sub2}} = \begin{cases} \emptyset, & \text{if } Q_{\max} < q_{\text{thr}}^{(1)}, \\ \left\{ (q_{\text{thr}}^{(1)}, \ Q_{\max} - q_{\text{thr}}^{(1)}) \right\}, & \text{if } q_{\text{thr}}^{(1)} \leq Q_{\max} \\ & \text{and } Q_{\max} < Q_{3,\text{thr1}}, \\ \left\{ \boldsymbol{q} \mid q^{(1)} = q_{\text{thr}}^{(1)}, \right. & \\ \left. q_{3,\text{thr1}}^{(2)} \leq q^{(2)} \leq Q_{\max} - q_{\text{thr}}^{(1)} \right\}, & \text{if } Q_{\max} \geq Q_{3,\text{thr1}}, \end{cases} \tag{18}$$

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 (13) for *Case* 3 is determined to have a higher eavesdropping rate between (17) and (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 (13) for *Case* 3 is given by

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

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 (17) and (18), the solution set can be specifically expressed as

$$T_3 = \begin{cases} \{(0, 0)\}, & \text{if } 0 \leq Q_{\max} < Q_{3,\text{thr2}}, \\ \left\{ (q_{\text{thr}}^{(1)}, \ Q_{\max} - q_{\text{thr}}^{(1)}) \right\}, & \text{if } Q_{3,\text{thr2}} \leq Q_{\max} \\ & \text{and } Q_{\max} < Q_{3,\text{thr1}}, \\ \left\{ \boldsymbol{q} \mid q^{(1)} = q_{\text{thr}}^{(1)}, \right. & \\ \left. q_{3,\text{thr1}}^{(2)} \leq q^{(2)} \leq Q_{\max} - q_{\text{thr}}^{(1)} \right\}, & \text{if } Q_{\max} \geq Q_{3,\text{thr1}}. \end{cases} \tag{19}$$

Case 4: The same two sub-problems as in *Case* 3 are introduced. Accordingly, their solutions are also given exactly the same as (17) and (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 (13) for *Case* 4 is just given by

$$T_4 = T_{3,\text{sub1}} = \{(0, 0)\}. \tag{20}$$

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, we 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 (13) for *Case* 5 can be expressed as

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

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

$$T_{5,\text{sub1}} := \left\{ \boldsymbol{q} \mid 0 \leq q^{(1)} < q_{\text{thr}}^{(1)}, \ q^{(2)} \geq 0, \right. \\ \left. q^{(1)} + q^{(2)} \leq Q_{\max}, \ \mathcal{C}_{\text{M}} < \mathcal{C}_{\text{DJ}}(\boldsymbol{q}) \right\}. \tag{21}$$

Meanwhile, the second sub-problem is expressed as

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

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

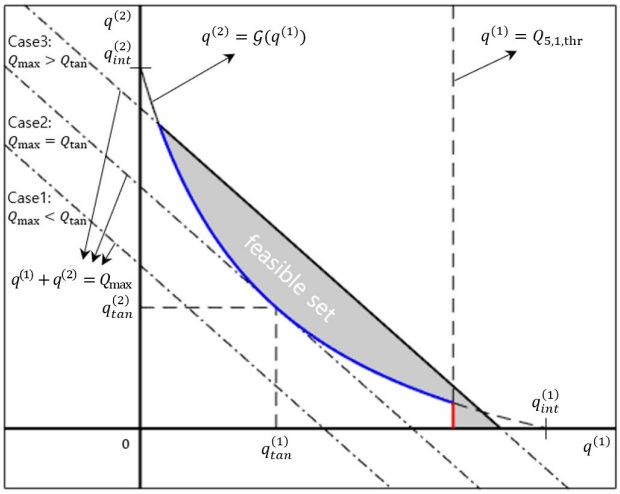


FIGURE 4. Description of how $Q_{\max}$ affects formation of the feasible set.

solution set of the second sub-problem is equal to the solution set of the following problem as

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

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

$$\begin{aligned}T_{5,\mathrm{sub2}} := \Big\{\boldsymbol{q} \mid 0 \le q^{(1)} < q^{(1)}_{\mathrm{thr}},\ q^{(2)} \ge 0,\\ q^{(1)} + q^{(2)} \le Q_{\max},\ \mathcal{C}_{\mathrm{M}} = \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q})\Big\}. \quad (22)\end{aligned}$$

Unfortunately, (22) cannot determined as an unique form because the set of $\boldsymbol{q}$ satisfying $\mathcal{C}_{\mathrm{M}} = \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q})$ is defined using the parameters which vary depending on the channel conditions. Thus, we present Table 2, classifying the channel conditions into five separate sub-cases in which $T_{5,\mathrm{sub2}}$ is presented in different formula to one another. In Table 2, ψ denotes the index number indicating each sub-case of *Case* 5. Furthermore, Fig. 3 shows how the boundary line of $\mathcal{C}_{\mathrm{M}} = \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q})$ 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, the orange line and the gray-colored area represents the boundary line satisfying $\mathcal{C}_{\mathrm{M}} = \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q})$ and the feasible set of the second sub-problem, respectively, when $Q_{\max}$ is given by an infinite number. We also provide Fig. 4 to give an intuitive illustration of how the value of $Q_{\max}$ affects the feasible set of the second sub-problem. In Fig. 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 and Fig. 4, we can define (22) as

$$T_{5,\mathrm{sub2}} = \begin{cases}\emptyset, & \text{if } 0 \le Q_{\max} < Q_{5,\psi,\mathrm{thr}}\\ V_\psi \cup W_\psi, & \text{if } Q_{\max} \ge Q_{5,\psi,\mathrm{thr}},\end{cases} \quad (23)$$

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

$$\begin{aligned}Q_{5,1,\mathrm{thr}} &:= \frac{1}{\alpha_{\mathrm{MR}}}\left(\frac{\alpha_{\mathrm{SR}}}{\lambda_{\mathrm{M}}} - 1\right),\\ Q_{5,2,\mathrm{thr}} &:= \begin{cases}Q_{\mathrm{tan}}, & \text{if } q^{(1)}_{\mathrm{tan}} q^{(2)}_{\mathrm{tan}} \ge 0,\\ \min\{q^{(1)}_{\mathrm{int}}, q^{(2)}_{\mathrm{int}}\}, & \text{if } q^{(1)}_{\mathrm{tan}} q^{(2)}_{\mathrm{tan}} < 0,\end{cases}\\ Q_{5,3,\mathrm{thr}} &:= \begin{cases}\min\{Q_{5,1,\mathrm{thr}}, Q_{\mathrm{tan}}\}, & \text{if } q^{(1)}_{\mathrm{tan}} q^{(2)}_{\mathrm{tan}} \ge 0,\\ \min\{Q_{5,1,\mathrm{thr}}, q^{(2)}_{\mathrm{int}}\}, & \text{if } q^{(1)}_{\mathrm{tan}} q^{(2)}_{\mathrm{tan}} < 0,\end{cases}\\ Q_{5,4,\mathrm{thr}} &:= \begin{cases}Q_{\mathrm{tan}}, & \text{if } q^{(2)}_{\mathrm{tan}} \ge 0,\\ q^{(1)}_{\mathrm{int}}, & \text{if } q^{(2)}_{\mathrm{tan}} < 0,\end{cases}\\ Q_{5,5,\mathrm{thr}} &:= \begin{cases}\min\{Q_{5,1,\mathrm{thr}}, Q_{\mathrm{tan}}\}, & \text{if } q^{(2)}_{\mathrm{tan}} \ge 0,\\ Q_{5,1,\mathrm{thr}}, & \text{if } q^{(2)}_{\mathrm{tan}} < 0.\end{cases}\end{aligned}$$

In addition, $q^{(1)}_{\mathrm{int}}$ and $q^{(2)}_{\mathrm{int}}$ denote $q^{(1)}$-intercept and $q^{(2)}$-intercept of $q^{(2)} = \mathcal{G}(q^{(1)})$ in the $\boldsymbol{q}$-domain, respectively, and $q^{(1)}_{\mathrm{tan}}$ and $q^{(2)}_{\mathrm{tan}}$ denote $q^{(1)}$ and $q^{(2)}$ of the point at which $\frac{\partial \mathcal{G}(q^{(1)})}{\partial q^{(1)}}$ is -1, respectively. Q_{tan} denotes the sum of $q^{(1)}_{\mathrm{tan}}$ and $q^{(2)}_{\mathrm{tan}}$. They are described graphically in Fig. 4 and are given by

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

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

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

On the one hand, V_ψ is given by

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

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

$$q_{\mathrm{L}}^{(1)} := \max\left\{0, q_{\mathrm{l}}^{(1)}\right\},$$
$$q_{\mathrm{U},\psi}^{(1)} := \begin{cases} \min\left\{q_{\mathrm{u}}^{(1)}, q_{\mathrm{int}}^{(1)}\right\}, & \text{if } \psi \in \{2,4\}, \\ \min\left\{q_{\mathrm{u}}^{(1)}, Q_{5,1,\mathrm{thr}}\right\}, & \text{if } \psi \in \{3,5\}, \end{cases}$$

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_ψ is given by

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

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

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

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 (13) for *Case* 5 is given as $T_{5,\mathrm{sub2}}$. Furthermore, when $T_{5,\mathrm{sub2}}$ is the empty set, $T_{5,\mathrm{sub3}}$ is always determined as the empty set because $Q_{5,\psi,\mathrm{thr}}$ is smaller than $q_{\mathrm{thr}}^{(1)}$ for all ψ. Since $T_{5,\mathrm{sub1}}$ is not always empty set, the solution set of (13) for *Case* 5 is given as

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

Using (21) and (23), this can be expressed as

$$T_5 = \begin{cases} \left\{\boldsymbol{q} \mid 0 \le q^{(1)} < q_{\mathrm{thr}}^{(1)}, \right. & \\ q^{(2)} \ge 0,\ \mathcal{C}_{\mathrm{M}} < \mathcal{C}_{\mathrm{DJ}}(\boldsymbol{q}), & \\ \left. q^{(1)} + q^{(2)} \le Q_{\max}\right\}, & \text{if } 0 \le Q_{\max} < Q_{5,\psi,\mathrm{thr}}, \\ V_\psi \cup W_\psi, & \text{if } Q_{\max} \ge Q_{5,\psi,\mathrm{thr}}. \end{cases} \tag{24}$$

To sum up, the final solution set of (13) is given as

$$T = \begin{cases} T_1, & \text{for Case 1}, \\ T_2, & \text{for Case 2}, \\ T_3, & \text{for Case 3}, \\ T_4, & \text{for Case 4}, \\ T_5, & \text{for Case 5}. \end{cases} \tag{25}$$

B. MINIMIZING TOTAL POWER CONSUMPTION

As long as $\boldsymbol{q}$ is included in T which is the solution set of (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, we find $\boldsymbol{q}$ to minimize the total power consumption of the monitor node. This optimization problem can be expressed as

$$\min_{\boldsymbol{q}} \sum_{n=1}^{2} Q^{(n)}$$
$$\text{s.t. } \boldsymbol{q} \in T. \tag{26}$$

For *Case* from 1 to 4, the solution of (26) is simply given by

$$\boldsymbol{q}_1^\star(Q_{\max}) = (0,0),$$
$$\boldsymbol{q}_2^\star(Q_{\max}) = \begin{cases} (0, Q_{\max}), & \text{if } 0 \le Q_{\max} < Q_{2,\mathrm{thr}}, \\ (0, Q_{2,\mathrm{thr}}), & \text{if } Q_{\max} \ge Q_{2,\mathrm{thr}}, \end{cases}$$
$$\boldsymbol{q}_3^\star(Q_{\max}) = \begin{cases} (0,0), & \text{if } 0 \le Q_{\max} < Q_{3,\mathrm{thr2}}, \\ (q_{\mathrm{thr}}^{(1)}, Q_{\max} - q_{\mathrm{thr}}^{(1)}), & \text{if } Q_{3,\mathrm{thr2}} \le Q_{\max} < Q_{3,\mathrm{thr1}}, \\ (q_{\mathrm{thr}}^{(1)}, q_{3,\mathrm{thr1}}^{(2)}), & \text{if } Q_{\max} \ge Q_{3,\mathrm{thr1}}, \end{cases}$$
$$\boldsymbol{q}_4^\star(Q_{\max}) = (0,0).$$

Furthermore, the solution of (26) for *Case* 5 is given by

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

where $\boldsymbol{q}_{5,\psi}^\star$ denotes the solution of (26) for the ψth sub-case of *Case* 5 and, for all ψ, is given as

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

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

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

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

Consequently, the solution of (26) is given by

$$\boldsymbol{q}^{\star}(Q_{\max}) = \begin{cases} \boldsymbol{q}^{\star}_1(Q_{\max}), & \text{for Case 1}, \\ \boldsymbol{q}^{\star}_2(Q_{\max}), & \text{for Case 2}, \\ \boldsymbol{q}^{\star}_3(Q_{\max}), & \text{for Case 3}, \\ \boldsymbol{q}^{\star}_4(Q_{\max}), & \text{for Case 4}, \\ \boldsymbol{q}^{\star}_5(Q_{\max}), & \text{for Case 5}. \end{cases} \tag{27}$$

IV. NUMERICAL RESULTS

In this section, we validate the performance of the proposed method with the optimal power strategy by simulation results. For simulation parameters, we 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 [8], [30]. 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

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

where d_{XY} denotes the Euclidean distance between node X and node Y, and f is the radio frequency, and g_z denotes the zth fading and is given by an independent complex Gaussian random variable with zero-mean and variance γ_z. Moreover, throughout this section, we 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

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

where P_{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

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

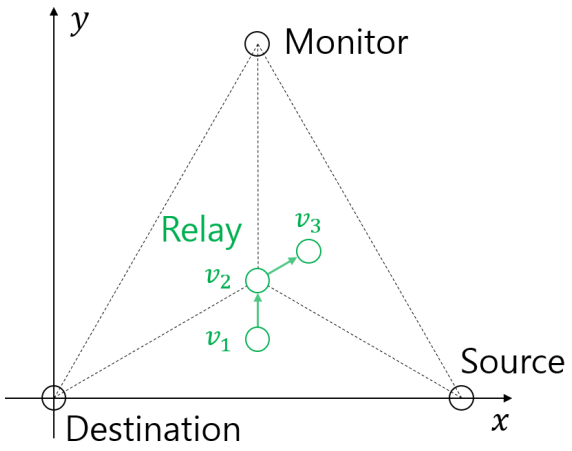
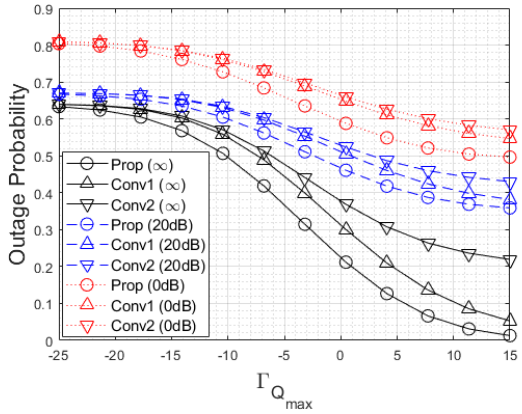


FIGURE 5. The network topology for the first simulation scenario.

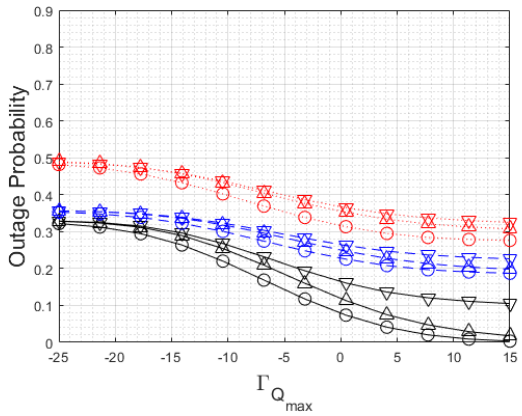
For comparison of performance, two conventional methods are introduced; one is the method where the monitor node is utilized as the jammer or the helper in the half-duplex mode [19] and the other is the half-duplex jamming method in which the monitor node acts as only the half-duplex jammer [26], [28]. We denote the first method [19] as 'Conv1' and the second method [26], [28] as 'Conv2' while denoting our proposed method as 'Prop' in each figure. Moreover, for more realistic and practical analysis, we 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, we 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, we consider three simulation scenarios. Fig. 5 shows the 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.

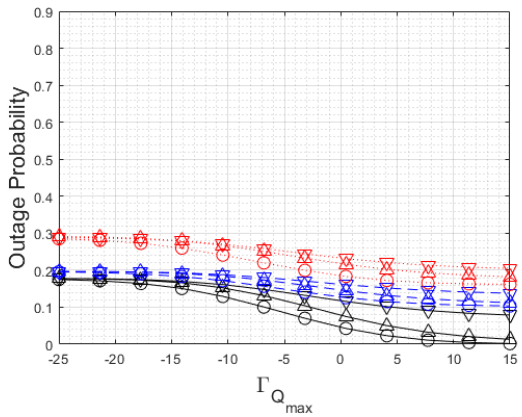
Fig. 6 and Fig. 7 shows the outage probabilities and the average eavesdropping rates for the three sub-cases in the first simulation scenario when $\Gamma_{Q_{\max}}$ is varying in the environment where P_{tot} is 1, ρ is 1, and σ^2 is 10^{-2}. From the figures, it is clear that performances are enhanced regardless of the proactive eavesdropping method for all sub-cases when $\Gamma_{Q_{\max}}$



(a) v_1

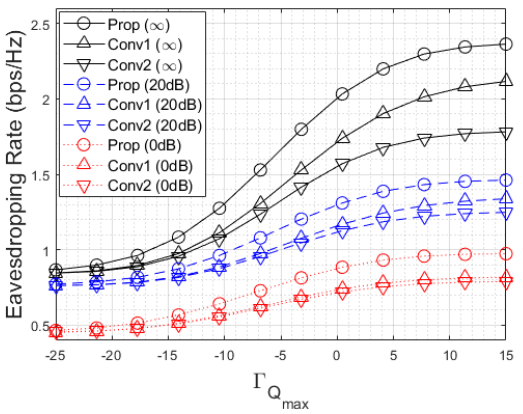


(b) v_2

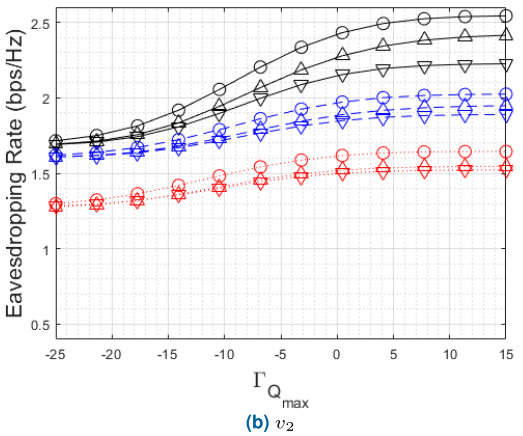


(c) v_3

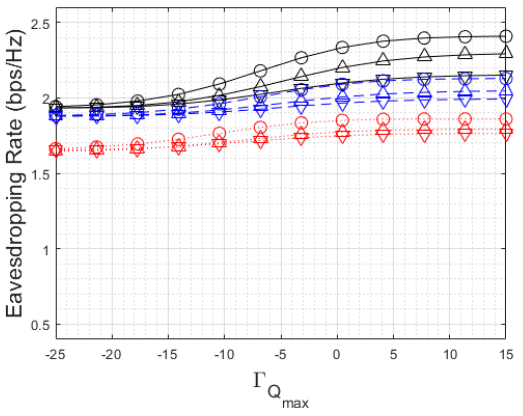
FIGURE 6. Outage probabilities for the three sub-cases where the relay node is positioned at (a), (b), and (c) in the first simulation scenario.



(a) v_1



(b) v_2



(c) v_3

FIGURE 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.

is increasing. We also identified that the proposed method outperforms 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

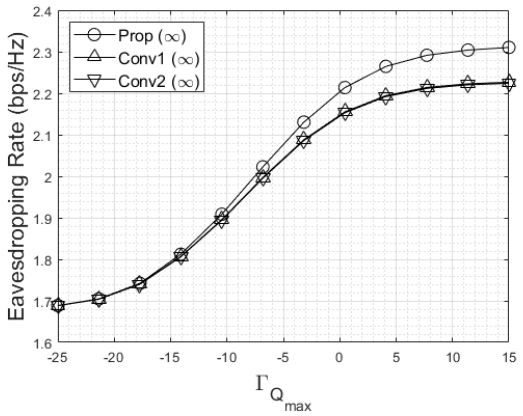


FIGURE 8. The average eavesdropping rate of the cases when the conventional method experiences no outage.

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. 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. 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. 9, the network topology utilized for the second and the third simulation 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, we 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. 10 and Fig. 11 show the outage probability and the average eavesdropping rate for the three sub-cases in the

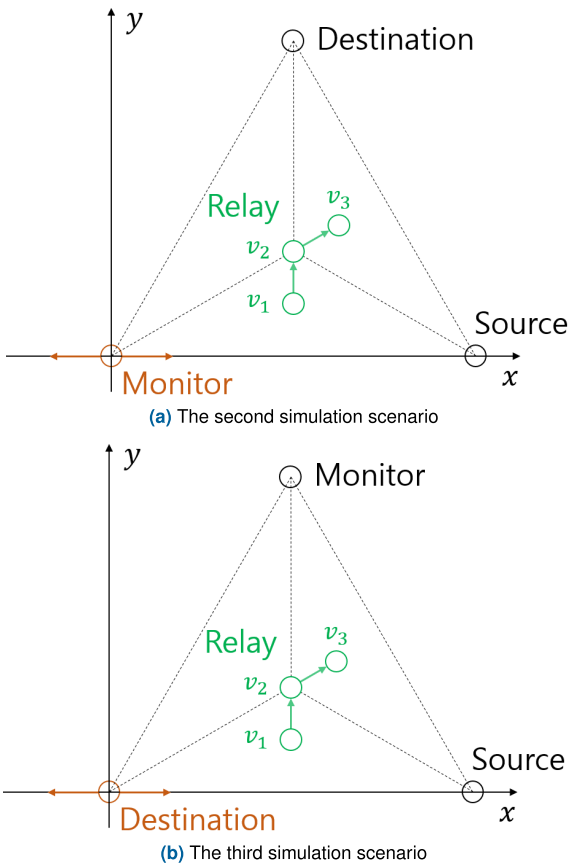
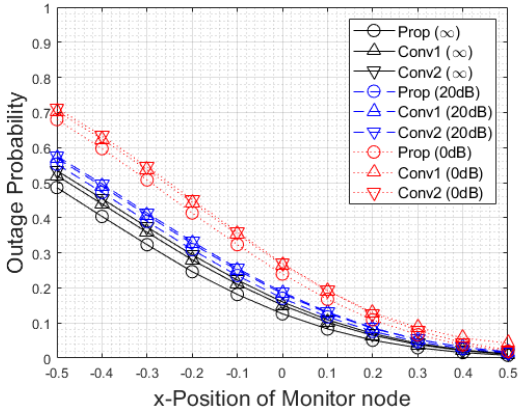
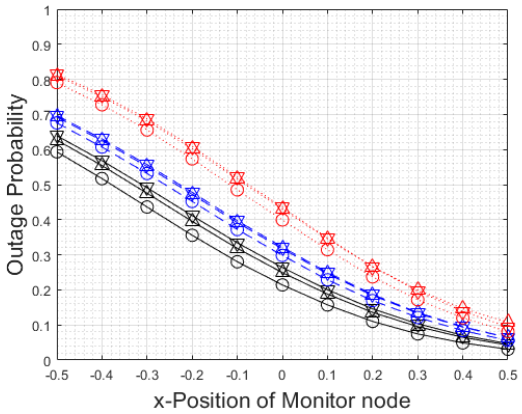


FIGURE 9. The network topology for (a) the second simulation scenario and (b) the third simulation scenario.

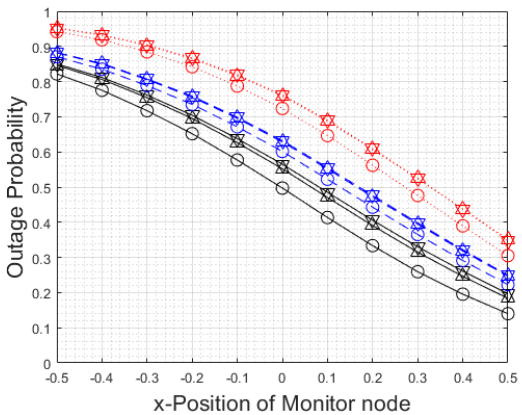
second simulation scenario when the monitor node moves from $(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$ in the environment where P_{tot} is 1, $\Gamma_{Q_{\max}}$ is -10dB, ρ is 1, and σ^2 is 10^{-2}. As shown in the two figures, it is verified that the proposed method is superior than other benchmark methods in both the outage probability and the average eavesdropping rate. For all subcases, 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. 10, we 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



(a) v_1

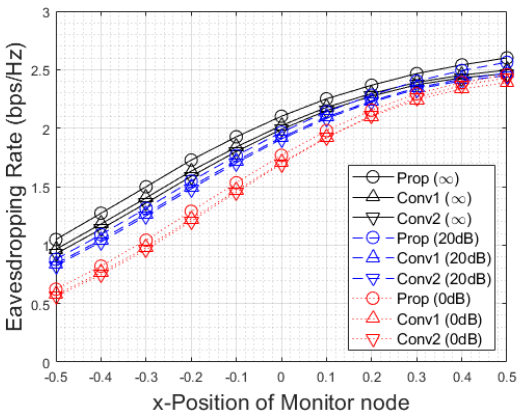


(b) v_2

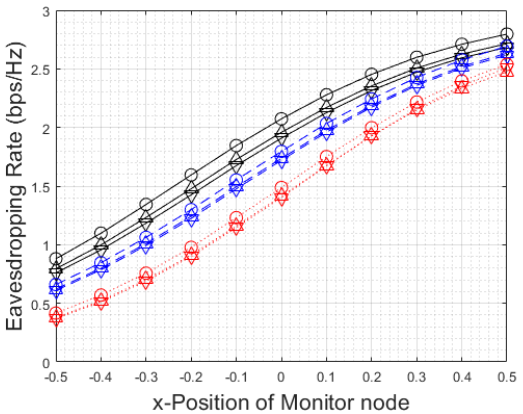


(c) v_3

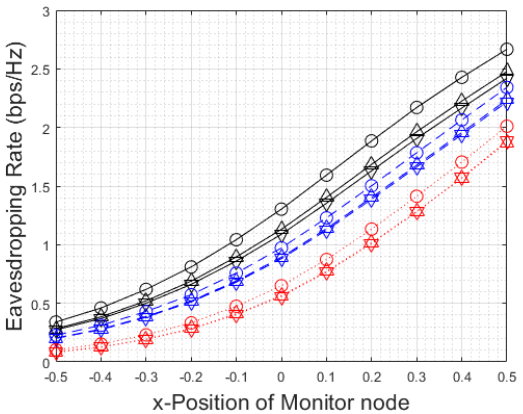
FIGURE 10. Outage probabilities for the three sub-cases where the relay node is positioned at (a), (b), and (c) in the first simulation scenario.



(a) v_1



(b) v_2



(c) v_3

FIGURE 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.

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. 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. 12 and Fig. 13 show the outage probability and the average eavesdropping rate for the three sub-cases in the third simulation scenario when the destination node moves from

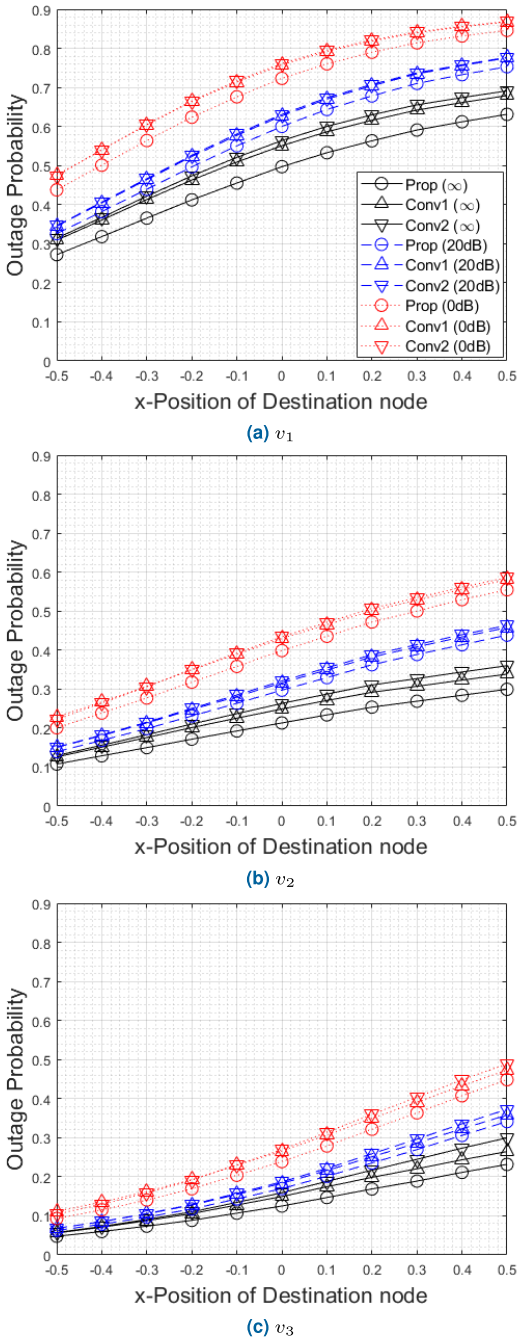


FIGURE 12. Outage probabilities for the three sub-cases where the relay node is positioned at (a), (b), and (c) in the second simulation scenario.

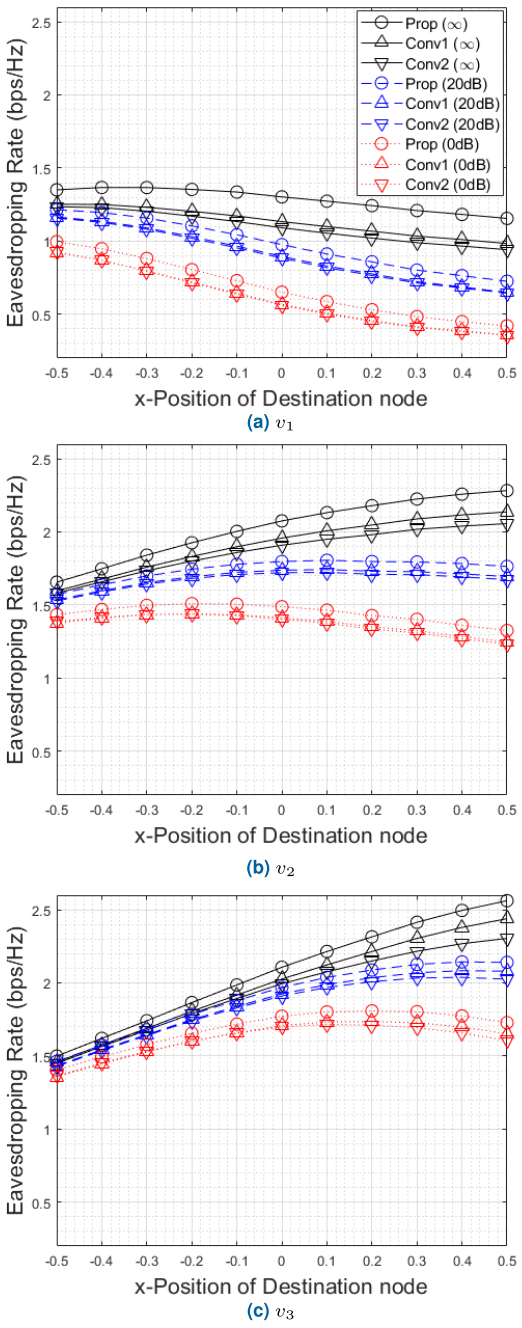


FIGURE 13. Average eavesdropping rates for the three sub-cases where the relay node is positioned at (a), (b), and (c) in the third simulation scenario.

$(-\frac{1}{2}, 0)$ to $(\frac{1}{2}, 0)$ in the environment where P_{tot} is 1, $\Gamma_{Q_{\max}}$ is -10dB, ρ is 1, and σ^2 is 10^{-2}. As shown in Fig. 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 disadvanta-

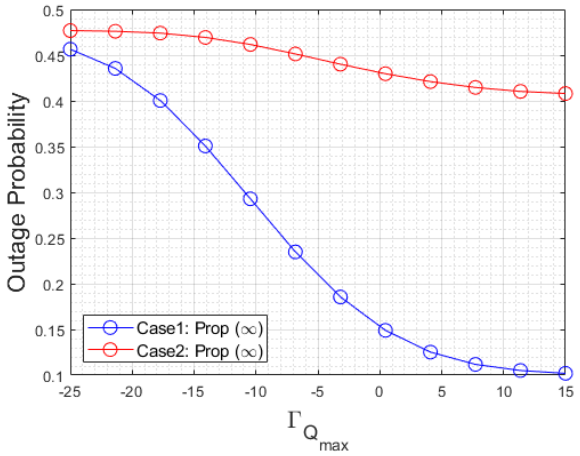


FIGURE 14. Outage probability of the two cases where ρ and ρ_{real} are different versus $\Gamma_{Q_{\max}}$.

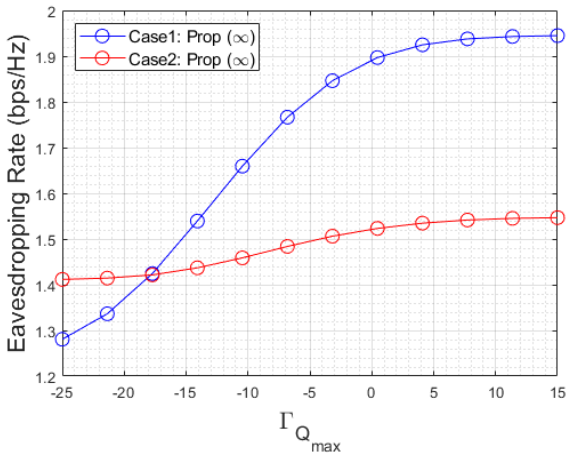


FIGURE 15. Average eavesdropping rate of the two cases where ρ and ρ_{real} are different versus $\Gamma_{Q_{\max}}$.

geous 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. 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 we assume that the ratio of the relay power to the transmit power, ρ, is known to the monitor node in the paper, the monitor node cannot know ρ in practical communication scenarios. Fig. 14 and Fig. 15 show the outage probability and the average eavesdropping rate versus $\Gamma_{Q_{\max}}$, respectively, when ρ used in the optimal power design is different with the real ratio of the relay power to the transmit power, ρ_{real}. Except for ρ, the simulation setting is same as in Fig. 6 (b) and Fig. 7 (b). We consider two cases in which ρ and ρ_{real} are different each other. In the first case, ρ_{real} is given by 2 and ρ is given by ρ_{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, ρ_{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, ρ_{opt} is a reasonable choice for the source node and the relay node. Whereas, in the second case, ρ_{real} is given by ρ_{opt} and ρ is given by 2. In Fig. 14 and Fig. 15, the blue line and the red line represent the first case and the second case, respectively. From Fig. 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 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. 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 ρ_{real} is unknown to the monitor node, ρ_{opt} is the best choice of ρ in the optimal power design.

V. CONCLUSION

This paper 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, we 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, we 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, we first classified channel conditions into several cases to make the optimization problem straightforward. Then, for each classified case, we solved the simplified problem and presented the optimal power for the proposed method in closed form. In addition, we 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. We 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. In addition, we plan to extend this work to a more realistic communication scenario where the monitor node knows only the statistical CSI, not the perfect instantaneous CSI of the network. For further studies, we will also consider the beamforming design or the beam scheduling problem in the multi-antenna scenario or the multi-monitor scenario.

REFERENCES

[1] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[2] A. Menezes, J. Katz, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography* (Discrete Mathematics and Its Applications). Boca Raton, FL, USA: CRC Press, 1996. [Online]. Available: https://books.google.co.kr/books?id=nSzoG72E93MC

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

[4] J. Lee, "Confidential multicasting assisted by multi-hop multi-antenna DF relays in the presence of multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 64, no. 10, pp. 4295–4304, Oct. 2016.

[5] Q. Li, W. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1359–1374, Dec. 2016.

[6] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[7] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[8] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[9] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[10] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790–2806, May 2017.

[11] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.

[12] Y. Cai, C. Zhao, Q. Shi, G. Y. Li, and B. Champagne, "Joint beamforming and jamming design for mmWave information surveillance systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1410–1425, Jul. 2018.

[13] L. Sun, Y. Zhang, and A. L. Swindlehurst, "Alternate-jamming-aided wireless physical-layer surveillance: Protocol design and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1989–2003, 2021.

[14] Y. Ge and P. C. Ching, "Energy efficiency for proactive eavesdropping in cooperative cognitive radio networks," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13443–13457, Aug. 2022.

[15] D. Xu and H. Zhu, "Proactive eavesdropping for wireless information surveillance under suspicious communication quality-of-service constraint," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 5220–5234, Jul. 2022.

[16] 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 Process. Lett.*, vol. 29, pp. 667–671, 2022.

[17] 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 Trans. Commun.*, vol. 68, no. 12, pp. 7563–7577, Dec. 2020.

[18] G. Ma, J. Xu, L. Duan, and R. Zhang, "Wireless surveillance of two-hop communications (invited paper)," in *Proc. IEEE 18th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jul. 2017, pp. 1–5.

[19] X. Jiang, H. Lin, C. Zhong, X. Chen, and Z. Zhang, "Proactive eavesdropping in relaying systems," *IEEE Signal Process. Lett.*, vol. 24, no. 6, pp. 917–921, Jun. 2017.

[20] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1714–1718, Nov. 2017.

[21] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6707–6719, Oct. 2018.

[22] B. Li, Y. Yao, H. Zhang, and Y. Lv, "Energy efficiency of proactive cooperative eavesdropping over multiple suspicious communication links," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 420–430, Jan. 2019.

[23] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3726–3738, Jul. 2019.

[24] G. Hu, J. Ouyang, Y. Cai, and Y. Cai, "Proactive eavesdropping in two-way amplify-and-forward relay networks," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3415–3426, Sep. 2021.

[25] G. Hu, Y. Cai, and J. Ouyang, "Proactive eavesdropping via jamming for multichannel decode-and-forward relay system," *IEEE Commun. Lett.*, vol. 24, no. 3, pp. 491–495, Mar. 2020.

[26] D. Xu, "Legitimate surveillance of suspicious multichannel DF relay networks with monitor mode selection," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 401–405, Feb. 2021.

[27] G. Hu, J. Si, Y. Cai, and F. Zhu, "Proactive eavesdropping via jamming in UAV-enabled suspicious multiuser communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 1, pp. 3–7, Jan. 2022.

[28] G. Hu, J. Si, Y. Cai, and N. Al-Dhahir, "Proactive eavesdropping via jamming in UAV-enabled relaying systems with statistical CSI," *IEEE Signal Process. Lett.*, vol. 29, pp. 1267–1271, 2022.

[29] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[30] 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.

YOUNG-JUN YOON (Member, IEEE) received the B.S. degree in electrical and computer engineering from the University of Seoul, Seoul, Republic of Korea, in February 2015. He is currently pursuing the integrated Ph.D. degree with Seoul National University, Seoul. His research interests include the physical layer of communications systems, such as physical-layer security and proactive eavesdropping, communications channel modeling, radar signal processing, and deep learning applications.

WANJEI CHO received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2019, where he is currently pursuing the Ph.D. degree. His current research interests include radar signal processing, wireless channel modeling, acoustic channel modeling, and DNN applications.

SEONGWOOK LEE (Member, IEEE) received the B.S. and Ph.D. degrees in electrical and computer engineering from Seoul National University (SNU), Seoul, Republic of Korea, in February 2013 and August 2018, respectively. From September 2018 to February 2020, he was a Staff Researcher with the Machine Learning Laboratory, AI & SW Research Center, Samsung Advanced Institute of Technology (SAIT), Gyeonggi-do, Republic of Korea. He was an Assistant Professor with the School of Electronics and Information Engineering, College of Engineering, Korea Aerospace University (KAU), Gyeonggi-do, from March 2020 to February 2023. Since March 2023, he has been an Assistant Professor with the School of Electrical and Electronics Engineering, College of ICT Engineering, Chung-Ang University (CAU), Seoul. He published more than 90 articles on signal processing for radar systems. His research interests include radar signal processing techniques, such as enhanced target detection and tracking, target recognition and classification, clutter suppression and mutual interference mitigation, and artificial intelligence algorithms for radar systems.

JONG-HO LEE (Member, IEEE) received the B.S. degree in electrical engineering and the M.S. and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, South Korea, in 1999, 2001, and 2006, respectively. From 2006 to 2008, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2008 to 2009, he was a Postdoctoral Researcher with the Georgia Institute of Technology, Atlanta, GA, USA. From 2009 to 2012, he was an Assistant Professor with the Division of Electrical, Electronic, and Control Engineering, Kongju National University, Cheonan, South Korea. From 2012 to 2018, he was an Associate Professor with the Department of Electronic Engineering, Gachon University, Seongnam, South Korea. Since 2018, he has been a Faculty Member with the School of Electronic Engineering, Soongsil University, Seoul. His research interests include wireless communication systems and signal processing for communication, with an emphasis on multiple-antenna techniques, multi-hop relay networks, physical-layer security, and full-duplex wireless communications.

JIHO SONG (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, South Korea, in 2009 and 2011, respectively, and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2017. He is currently an Assistant Professor with the Department of Electrical and Electronic Engineering, Hanyang University, Ansan, South Korea. Before joining Hanyang University, he was a Senior Researcher with Motorola Mobility, Chicago, IL, USA, from 2017 to 2018, and an Assistant Professor with the School of Electrical Engineering, University of Ulsan, Ulsan, South Korea, from 2018 to 2022. His research interests include the design and analysis of millimeter-wave, sub-THz, and vehicular communication systems. He received the Bronze Prize in Samsung Electronics' 23rd Humantech Paper Contest, in 2017.

SEONG-CHEOL KIM (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, South Korea, in 1984 and 1987, respectively, and the Ph.D. degree in electrical engineering from the Polytechnic Institute of NYU, Brooklyn, NY, USA, in 1995. From 1995 to 1999, he was with the Wireless Communications Systems Engineering Department, AT&T Bell Laboratories, Holmdel, NJ, USA. Since 1999, he has been a Professor with the Department of Electrical and Computer Engineering, Seoul National University. His current research interests include system engineering of wireless communications, including millimeter wave channel modeling, localization algorithms, power line communications, and automotive radar signal processing.