https://doi.org/10.7840/kics.2025.50.1.48

Detection Error Probability Maximization for Relay-Based Covert Communications

Md Sakil Hasan•, Jihwan Moon°

ABSTRACT

In this paper, we investigate the reliability of covert transmissions for a relay-based communications system. We specifically consider a scenario where a transmitter sends both public and covert messages to a receiver through a relay, while the detector embedded on the relay attempts to uncover covert messages. Considering the detection error probability (DEP) at the relay, we propose transmission strategies to confuse the detector as much as possible while maintaining a certain level of the reliability of covert transmissions. To this end, we first identify the worst-case DEP, i.e., the minimum possible DEP at the relay. We then solve optimization problems to obtain the optimal power ratio on between public and covert messages that simultaneously maximizes the worst-case DEP and guarantees a minimum covert rate threshold. Two well-known relay protocols, decode-and-forward (DF) and amplify-and-forward (AF), are studied by taking the processing delay difference into consideration. Hence, numerical results reveal not only how system parameters affect the DEP performance in general, but also instances in which DF or AF protocol outperforms each other.

Key Words : Physical layer security, covert communications, low probability of detection, decode-and-forward, amplify-and-forward, relay, false alarm, miss alarm

Ⅰ. Introduction

Advancements in wireless technology in recent times have provided opportunities to improve human life. These technologies have applications in fields such as earth observation satellites, vehicle-to-vehicle (V2V), and industrial internet of things (IIOT)[1].

Wireless communications, however, are becoming more exposed to dangers in several ways, such as data privacy, cybersecurity, and wireless jamming[2]. It is worth mentioning that the main objectives of the fifth-generation (5G) and the sixth-generation (6G) networks are to enhance communications by providing higher data rates, lower latency, and massive connectivity across diverse smart devices while ensuring strong user information security. Additionally, both generations focus on energy efficiency and sustainability, with 6G further integrating advanced artificial intelligence (AI) for optimized performance and expanding connectivity to more remote areas[3]. Moreover, the number of Mobile Internet of Things (MIoT) devices has increased dramatically for both 5G and the soon-to-be 6G networks to handle the risks posed to MIoT users[4]. Radio Access Network (RAN)

※ This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2021R1I1A3050126).
※ This research was partially supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-RS-2024-00437886) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).
※ This research was partially supported by the research fund of Hanbat National University in 2022.
• First Author : Hanbat National University, Department of Mobile Convergence Engineering, 30224028@o365.hanbat.ac.kr, 학생회원
° Corresponding Author : Hanbat National University, Department of Mobile Convergence Engineering, anschino@staff.hanbat.ac.kr, 정회원
논문번호 : 202407-147-B-RU, Received July 16, 2024; Revised August 22, 2024; Accepted August 23, 2024

is a method that connects individual devices to other parts of a network through radio connections. In the context of a 5G network, RAN includes advanced technologies and architectures designed to handle increased data traffic, support numerous connected devices, and provide higher data speeds with lower latency. However, in 5G networks, the concept of RAN has been enhanced with cloud-RAN (C-RAN) and open-RAN (O-RAN). Encryption algorithms, on the other hand, are used within the RAN to secure data transmission. In 5G networks, encryption algorithms like 128-EEA2 and 128-NEA2, based on the advanced encryption standard (AES), are implemented to protect user data at various layers. These algorithms ensure data confidentiality and integrity by encrypting it as it travels through the RAN, safeguarding against interception and eavesdropping[5]. These methods require a key exchange and incur a non-negligible computation load when encrypting or decrypting, which are specifically problematic for low-powered Internet of Things (IoT) devices nowadays.

Among some alternative security techniques, physical layer security (PLS) lately draws attention, which is a method of securing wireless communication by exploiting the unique characteristics of the physical channel through which the communication occurs. It specifically focuses on the inherent properties of the communication channel itself to prevent unauthorized access and eavesdropping[6]. Since cryptography methods ensure data confidentiality, integrity, and authenticity by encrypting and decrypting, combining them with physical layer security may provide comprehensive protection against a wide range of cyber threats and physical layer attacks.

Nonetheless, there is an increasing demand for security measures that not only prevent unauthorized entities from decoding information but also conceal the existence of the communication link[7]. For example, though the contents of phone conversations may be encrypted, adversaries can continue to be able to obtain information through traffic analysis, such as the duration of calls, the frequency and timing of communication between users, and the geographic locations from which calls are made[8]. Due to these reasons, researchers are now interested in *covert communication* or *low-probability-of-detection* (LPD). Covert communications aims to hide sensitive information from detectors, ensuring a higher level of secure information that is transferred from the transmitter to the receiver. This concept has recently been incorporated into various communications systems. One widely used technique is to hide user information within the environmental or artificial noise to transfer the receiver. Additional techniques, such as non-orthogonal multiple access (NOMA) or turbo encoding, are also utilized for covert communications[9].

Researchers have conducted many studies focused on covert communication in single-hop wireless system[10-15]. The authors demonstrated that the covert rate is achievable for the additive white Gaussian noise (AWGN) channels in [10], bosonic channel in [11], and discrete memoryless channel in [12]. Covert communications based on generating artificial noise in fullduplex (FD) mode was studied in [13]. The authors discussed in [14] how a covert transmitter adjusts its transmission power effectively by exploiting the unpredictable noise surrounding the detector. Using both bounded and unbounded noise uncertainty indicators, the researcher in [15] optimized the covert rate.

To combat the effects of channel fading and path loss, researchers studied covert transmissions on two-hop links as well. The authors in [16] investigated a system where a transmitter first sends the message to a relay, which then forwards the message to the receiver, such that the message transmission can be executed by a low transmit power with the help of the relay. The work[17] presented how to achieve a positive covert rate by leveraging relay and multi-channel uncertainty. In [18], the authors introduced two covert transmission methods for amplify-and-forward (AF) half-duplex (HD) relay. Studied in [19] is the covert rate of a two-hop wireless relaying system where the relay may choose to work in either the FD mode or the HD mode. The authors of [20] and [21] explored the use of power splitting and time switching for energy harvesting in an AF relay and a multi-antenna decodeand-forward (DF) relay, respectively. For covert communications aided by multi-antenna DF relays, [22] examined achievable covert rates, taking in-

Table 1. List of Abbreviations

Abbreviation	Full form
V2V	Vehicle-to-Vehicle
IIoT	Industrial Internet of Things
5G/6G	Fifth Generation/Sixth Generation
MIoT	Mobile Internet of Things
RAN	Radio Access Network
C-RAN	Cloud-RAN
O-RAN	Open-RAN
AES	Advanced Encryption standard
NOMA	Non-Orthogonal Multiple Access
IoT	Internet of Things
PLS	Physical Layer Security
LPD	Low Probability of Detection
AWGN	Additive White Gaussian noise
AF	Amplify-and-Forward
HD	Half Duplex
FD	Full Duplex
DF	Decode-and-Forward
DEP	Detection Error Probability
MD	Miss Detection
FA	False Alarm
QoS	Quality of Service

to account both direct and relay links.

In our past work[1], we previously investigated the maximum covert rate using optimal power and compared the maximum covert rates among DF, AF, and CF relays. Meanwhile, in some situations, e.g., covert operations in enemy territory, ensuring that covert communications between troops or command centers remain undetected is paramount. If enemy forces detect these communications, then their lives will be at risk. Therefore, ensuring high detection avoidance is more critical than enhancing the covert transmission rate in such a scenario. Motivated by this, we concentrated on identifying the maximum DEP by obtaining optimal power and compared performance between DF and AF relays in this work.

In this paper, we focus on a scenario in which a transmitter sends both public and covert messages to a receiver through a relay, while the detector embedded in the relay attempts to uncover covert messages. We investigate the maximum DEP across varying relay system types, specifically decode-and-forward (DF) and amplify-and-forward (AF). Considering the relay minimum DEP, i.e., the worst-case DEP from the perspective of covert communications, we strategically allocate power between the public and covert messages to obtain the highest possible worst-case DEP.

We further provide numerical results of a relay processing delay-ware comparison between DF and AF relay systems, as in [1]. We also include the effects of other system parameters, such as source and relay transmit power, noise uncertainty bound, and minimum required quality of service for both public and covert messages, on DEP performance on the DF and AF relay systems.

This paper is organized as follows: Section Ⅱ presents the system model and parameters used in our study. We formulate optimization problems in Section Ⅲ. In Section Ⅳ, we describe the technique and the algorithms employed. Section Ⅴ discusses the experimental setup and numerical results. Finally, Section Ⅵ concludes the paper.

Ⅱ. System Model

The considered scenario is illustrated in Figure 1. A transmitter node S sends both public and covert messages to a receiver node D through the relay R. A detector embedded in the relay makes an attempt to detect the presence of covert communication. Additionally, we presume the existence of messages at long distances (S, D, R). Therefore, D and R know when S is transmitting messages[17].

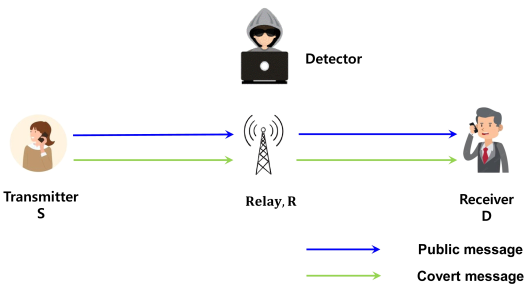

Fig. 1. System model

2.1 Received Signals

At the relay, the received signal is expressed as[1].

$$y_R = h_{SR}\sqrt{P_S}\left(\sqrt{\alpha}x_P + \sqrt{1-\alpha}x_C\right) + z_R. \quad (1)$$

Here, $x_P \sim CN(0, 1)$ and $x_C \sim CN(0, 1)$ represent the public and covert messages from the transmitting node, respectively, and $CN(0, 1)$ indicates a complex Gaussian distribution where the mean is 0 and the variance is 1[2]. The term P_S means the source transmit power, variables $\sqrt{\alpha}$ and $\sqrt{1-\alpha}$ denote the transmit power of public messages xP and covert messages x_C, respectively, and $z_R \sim CN(0, \sigma_R^2)$ represents the additive noise. [24] and [25], we consider that the noise σ_R^2, dB varies uncertainty such that the function $U(\bar{\sigma}_{R,\mathrm{dB}}^2 - \zeta_{\mathrm{dB}}, \bar{\sigma}_{R,\mathrm{dB}}^2 + \zeta_{\mathrm{dB}})$ operates within a decibel range where $\bar{\sigma}_{R,\mathrm{dB}}^2$ and ζ_{dB} are parameters representing the mean and bounded range respectively, both of which are non-negative. We proceed by examining two distinct relay types, namely DF and AF, and subsequently derive expressions for both the public and covert rates at the destination node.

2.1.1 DF Relay

First, we observe from (1) that the achievable rate for the combined message $x_S \triangleq \sqrt{\alpha}x_P + \sqrt{1-\alpha}x_C$ in the S-R node is expressed by

$$\bar{r}_S = \log_2\left(1 + \frac{|h_{SR}|^2 P_S}{\sigma_R^2}\right). \quad (2)$$

After successful decoding by the DF relay, the signal x_S is forwarded to the receiving node, where the received signal can be represented as

$$y_D = h_{RD}\sqrt{P_R}\left(\sqrt{\alpha}x_P + \sqrt{1-\alpha}x_C\right) + z_D, \quad (3)$$

where P_R stands for the transmission power of the relay and $z_D \sim CN(0, \sigma_D^2)$ represents the AWGN. The achievable rate for the combined message x_S in the R-D hop is denoted by

$$\bar{r}_R = \log_2\left(1 + \frac{|h_{RD}|^2 P_R}{\sigma_R^2}\right). \quad (4)$$

From (2) and (4), it is apparent that the effective data rate for x_S is bounded above by $\bar{r}_S$ and $\bar{r}_R$ for successful decoding at both the relay and receiving nodes. The receiver first decodes the public message by considering the covert message as interference, from which the achievable public message rate is obtained by [23]

$$r_{P,DF} = \log_2\left(1 + \frac{|h_{RD}|^2 P_R \alpha}{|h_{RD}|^2 P_R(1-\alpha) + \sigma_R^2}\right). \quad (5)$$

Secondly, the receiver D decodes the covert message by subtracting the decoded public message[3]. As a result, the achievable covert rate can be written by

$$r_{C,DF} = \log_2\left(1 + \frac{|h_{RD}|^2 P_R(1-\alpha)}{\sigma_R^2}\right). \quad (6)$$

It is clear that the actual public and covert rates are limited by $r_{P,DF}$ and $r_{C,DF}$, respectively for successfully decoding.

2.1.2 AF Relay

The AF relay transmits x_R to the receiver D, which is an amplified version of y_R, and the receiver D obtains

$$y_D = h_{RD}\sqrt{P_R}x_R + z_D. \quad (7)$$

Note that $x_R \triangleq y_R/\sqrt{|h_{SR}|^2 P_S + \sigma_R^2}$ denotes the normalized unit-power signal from the AF relay.

Similar to the DF case, if we assume that the receiver D adopts the successive decoding of public and covert messages in order, the achievable rates can be expressed as

1) The received signals at the relay and detector are the same since the detector is implemented on the relay.

2) The Gaussian distribution on x_P and x_C comes from the assumption of the Gaussian codebook to investigate the theoretically maximum covert and public rate performance [23].

3) The successive interference cancellation (SIC) is not performed on the modulation or signal wave level but on the digital symbol level.

$$r_{P,AF} = \log_2\left(1 + \frac{|h_{SR}|^2 P_S \alpha}{|h_{SR}|^2 P_S(1-\alpha) + \sigma_R^2 + \tilde{\sigma}_D^2}\right), \quad (8)$$

$$r_{C,AF} = \log_2\left(1 + \frac{|h_{SR}|^2 P_S(1-\alpha)}{\sigma_R^2 + \tilde{\sigma}_D^2}\right), \quad (9)$$

where $\tilde{\sigma}_D^2 \triangleq \left(|h_{SR}|^2 P_S + \sigma_R^2\right)\sigma_D^2 / \left(|h_{RD}|^2 P_R\right)$

2.2 Detection Performance at the Detector

The detector recognizes the received signal yR . To detect whether any covert messages exist, the detector at the relay first removes the public message portion form its receives signal as $\tilde{z}_R \triangleq y_R - h_{SR}\sqrt{P_S}x_P$ considering that the relay perfectly knows h_{SR} and P_S[26]. The detector then considers two hypotheses as

$$\begin{aligned} H_0: &\quad \tilde{z}_R = z_R, \\ H_1: &\quad \tilde{z}_R = h_{SR}\sqrt{P_S}\left((\sqrt{\alpha}-1)x_P + \sqrt{1-\alpha}x_C\right) + z_R. \end{aligned} \quad (10)$$

where H_0 indicates that no covert message was sent by the transmitting node, while H_1 indicates that a covert message is present. As [24], we also assume in this paper that the detector uses a radiometer to detect the signals after gathering $N \to \infty$ number of enough signals. Thus, the detector can apply test statistic T as

$$\begin{aligned} H_0: &\quad T = \sigma_R^2, \\ H_1: &\quad T = 2|h_{SR}|^2 P_S(1-\sqrt{\alpha}) + \sigma_R^2. \end{aligned} \quad (11)$$

Two kinds of detection errors are introduced by the hypothesis test. The first is called missed detection (MD), when the transmitter S and receiver D are in communication but the detector is unable to notice it. The second is called a false alarm (FM) when the detector incorrectly determines that there exists a covert transmission. Thus, the detection error probability (DEP), denoted by Pr (error/τ), is composed of the MD and FA probabilities[1,27]

$$\begin{aligned} &\Pr(\text{error}|\tau) = \\ &\Pr(T \geq \tau | H_0)\Pr(H_0) + \Pr(T < \tau | H_1)\Pr(H_1). \end{aligned} \quad (12)$$

Where Pr ($T \geq \tau / H_0$) and Pr ($T < \tau / H_1$) denote FA and MD probabilities, respectively for some threshold τ. Assuming that covert transmissions take place randomly, meaning that $\Pr(H_0) = \Pr(H_1) = 0.5$, according to [26], the optimal τ that minimizes the DEP can be derived

$$\tau^\star = 2|h_{SR}|^2 P_S(1-\sqrt{\alpha}) + \frac{1}{\zeta}\bar{\sigma}_R^2, \quad (13)$$

and the corresponding minimum DEP is calculated by [23]

$$\Pr(\text{error}|\tau^\star) = \frac{1}{2}\left(1 - \frac{1}{2\ln\zeta}\left(\ln\frac{\tau^\star}{\tau^\star - 2|h_{SR}|^2 P_S(1-\sqrt{\alpha})}\right)\right), \quad (14)$$

provided that $\zeta\bar{\sigma}_R^2 \geq 2|h_{SR}|^2 P_S(1-\sqrt{\alpha}) + \bar{\sigma}_R^2/\zeta$. We further make a conservative assumption that the detector knows the exact value of α , by which (13) leads to the worst-case minimum DEP.

Ⅲ. Problem Formulation

To achieve the maximum covert rate, the author[1] optimized the power allocation for the public and covert messages. In this section, we aim to determine the optimal power allocation between public and covert messages that maximizes the minimum DEP. We formulate optimization problems according to the type of relay in the next sections.

3.1 DF Relay

For DF, the optimization problem can be given by

$$\begin{aligned} \text{(P1)}: &\max_{\alpha, b_P, b_C} \Pr(\text{error}|\tau^\star), && (15a) \\ \text{subject to: } & b_P \geq \bar{r}_P, && (15b) \\ & b_P + b_C \leq \min\left(\bar{r}_S|_{\sigma_R^2 = \zeta\bar{\sigma}_R^2}, \bar{r}_R\right), && (15c) \\ & b_P \leq r_{P,DF}, && (15d) \\ & b_C \leq r_{C,DF}, && (15e) \\ & b_C \geq \bar{r}_C, && (15f) \\ & \zeta\bar{\sigma}_R^2 \geq 2|h_{SR}|^2 P_S(1-\sqrt{\alpha}) + \frac{1}{\zeta}\bar{\sigma}_R^2, && (15g) \\ & 0 \leq \alpha \leq 1, && (15h) \end{aligned}$$

where the actual rates for the public and covert messages are indicated by b_P and b_C, respectively. In (15b) and (15f), we set the minimum quality of service $\bar{r}_P$ on b_P and $\bar{r}_C$ on b_C for reliable public and covert communications. The upper constraints on bP and bC in (15c)-(15e) indicate conditions for successful decoding as discussed in section 2.1.1. By setting the noise variance $\sigma_R^2 = \zeta\bar{\sigma}_R^2$ at the DF relay, we consider the lowest feasible $\bar{r}_S$. Constraint (15g) ensures a positive minimum DEP, and (15h) sets a feasible region for α.

3.2 AF Relay

The optimization problem for the AF relay method can be expressed as

$$\text{(P2)}: \max_{\alpha} \Pr(\text{error}|\tau^{\star}), \tag{16a}$$

$$\text{subject to: } r_{P,AF}|_{\sigma_R^2=\zeta\bar{\sigma}_R^2} \geq \bar{r}_P, \tag{16b}$$

$$r_{C,AF}|_{\sigma_R^2=\zeta\bar{\sigma}_R^2} \geq \bar{r}_C, \tag{16c}$$

$$\zeta\bar{\sigma}_R^2 \geq 2|h_{SR}|^2 P_S(1-\sqrt{\alpha}) + \frac{1}{\zeta}\bar{\sigma}_R^2, \tag{16d}$$

$$0 \leq \alpha \leq 1, \tag{16e}$$

By setting the noise variance $\sigma_R^2 = \zeta\bar{\sigma}_R^2$ at AF relay, we consider the lowest possible $r_{P,AF}$ and $r_{C,AF}$ to guarantee the minimum reliable qualities of service $\bar{r}_P$ and $\bar{r}_C$ in (16b) and (16c), respectively. The constraints (16d) and (16e) correspond to (15g) and (15h) in (P1), respectively.

Ⅳ. Proposed Solutions

We provide the optimal solutions to the optimization problems (P1) and (P2).

4.1 DF Relay

In this subsection, we proceed our discussion with a feasible $\bar{r}_P$ that satisfies $\bar{r}_P \leq \min\left(\bar{r}_S|_{\sigma_R^2=\zeta\bar{\sigma}_R^2}, \bar{r}_R\right)$ from (15c). Next, we rewrite (15g) by

$$\sqrt{\alpha} \geq 1 - \left(\zeta - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_R^2}{2|h_{SR}|^2 P_S}. \tag{17}$$

This reduces to $\bar{\alpha} \leq \alpha \leq 1$ by merging (15g) and (15h) where

$$\bar{\alpha} \triangleq \left(\max\left(\sqrt{\alpha}, 0\right)\right)^2. \tag{18}$$

We also observe that b_C in (15c) and α in (15d) have larger feasible region when b_P is reduced. Hence, we can determine the optimal b_P to be the minimum required rate, as indicated in (15b), i.e.,

$$b_P^{\star} = \bar{r}_P, \tag{19}$$

without loss of generality. (P1) is then reformulated into

$$\text{(P1.1)}: \max_{\alpha, b_C} \Pr(\text{error}|\tau^{\star}), \tag{20a}$$

$$\text{subject to: } b_C \leq \min\left(\bar{r}_S|_{\sigma_R^2=\zeta\bar{\sigma}_R^2} - \bar{r}_P, \bar{r}_R - \bar{r}_P, r_{C,DF}\right), \tag{20b}$$

$$\alpha \geq \frac{\left(2^{\bar{r}_P}-1\right)|h_{RD}|^2 P_R + \left(2^{\bar{r}_P}-1\right)\sigma_D^2}{2^{\bar{r}_P}|h_{RD}|^2 P_R}, \tag{20c}$$

$$b_C \geq \bar{r}_C, \tag{20d}$$

$$\bar{\alpha} \leq \alpha \leq 1, \tag{20e}$$

where constraint (20b) comes from the combination of (15c) and (15e). Hence, (20d) and (20e) can be expressed by of $\tilde{\alpha}_{DF} \leq \alpha \leq 1$,

$$\tilde{\alpha}_{DF} \triangleq \max\left(\frac{\left(2^{\bar{r}_P}-1\right)\left(|h_{RD}|^2 P_R + \sigma_D^2\right)}{2^{\bar{r}_P}|h_{RD}|^2 P_R}, \bar{\alpha}\right). \tag{21}$$

It is worth noting from (P1.1) that in order to guarantee the feasibility, $\bar{r}_C \leq \min\left(\bar{r}_S|_{\sigma_R^2=\zeta\bar{\sigma}_R^2} - \bar{r}_P, \bar{r}_R - \bar{r}_P, r_{C,DF}\right)$ must hold. Furthermore, when b_C is declined, the feasible region in (20b) becomes larger. Consequently, we may set the optimal actual covert rate to $b_C^{\star} = \bar{r}_C$. (P1.1) then reduces to

$$\text{(P1.2)}: \max_{\alpha} \Pr(\text{error}|\tau^{\star}), \tag{22a}$$

$$\text{subject to: } \alpha \leq 1 - \frac{\left(2^{\bar{r}_C}-1\right)\sigma_D^2}{|h_{RD}|^2 P_R}, \tag{22b}$$

$$\tilde{\alpha}_{DF} \leq \alpha \leq 1, \tag{22c}$$

Noticing that the minimum DEP in (22a) is increas-

ing function of α, we can conclude that the optimal α should be as high as possible. That is,

$$\alpha_{DF}^{\star}=\min\left(1-\frac{\left(2^{\bar{r}_C}-1\right)\sigma_D^2}{|h_{RD}|^2 P_R},1\right), \tag{23}$$

as long as $\tilde{\alpha}_{DF}\le 1-\frac{\left(2^{\bar{r}_C}-1\right)\sigma_D^2}{|h_{RD}|^2 P_R}$.

4.2 AF Relay

From (16d) and (16e), we can derive the same value of $\bar{\alpha}$ that we obtained from (15g) and (15h). (P2) then reformulated into

$$\text{(P2.1)}: \max_{\alpha} \Pr(\text{error}|\tau^{\star}), \tag{24a}$$

$$\alpha \ge \frac{\left(2^{\bar{r}_P}-1\right)|h_{SR}|^2 P_S+\zeta\sigma_R^2+\tilde{\alpha}_D^2}{2^{\bar{r}_P}|h_{SR}|^2 P_S}, \tag{24b}$$

$$\alpha \le 1-\frac{\left(2^{\bar{r}_C}-1\right)\left(\zeta\sigma_R^2+\tilde{\alpha}_D^2\right)}{|h_{SR}|^2 P_S}, \tag{24c}$$

$$\bar{\alpha}\le\alpha\le 1, \tag{24d}$$

merging (24b) and (24d) leads to a single range of α as $\tilde{\alpha}_{AF}\le\alpha\le 1$ where

$$\tilde{\alpha}_{AF}\triangleq\max\left(\frac{\left(2^{\bar{r}_P}-1\right)|h_{SR}|^2 P_S+\zeta\sigma_R^2+\tilde{\alpha}_D^2}{2^{\bar{r}_P}|h_{SR}|^2 P_S},\bar{\alpha}\right). \tag{25}$$

Observing that the minimum DEP in (24a) is increasing function of α, we can deduce that the optimal α should be as high as possible as

$$\alpha_{AF}^{\star}=\min\left(1-\frac{\left(2^{\bar{r}_C}-1\right)\left(\zeta\sigma_R^2+\tilde{\alpha}_D^2\right)}{|h_{SR}|^2 P_S},\bar{\alpha}\right), \tag{26}$$

when $\tilde{\alpha}_{AF}\le 1-\frac{\left(2^{\bar{r}_C}-1\right)\left(\zeta\sigma_R^2+\tilde{\alpha}_D^2\right)}{|h_{SR}|^2 P_S}$ for feasibility.

4.3 Comparing Performance with Relay Processing Delay

Let us investigate the efffect of professing delay of DF and AF on covert rate to draw a fair performance comparsion. The relationship between the codeword lenghts of DF relay L_{DF} and AF relay L_{AF} which results in the same processing delay by, is given by [28].

$$L_{AF}\simeq\frac{2(1+\delta)}{2+\delta}L_{DF}, \tag{27}$$

in the high transmit power environment for a delay factor $\delta\ge 0$. When $\delta = 0$, there is no delay difference between the DF and AF relay systems; on the other hand, when $\delta = \infty$, there is a larger processing difference between the DF and AF relay systems. The public and covert rates between DF and AF are correlated with (27) as

$$r_{P,DF}=\frac{2+\delta}{2(1+\delta)}r_{P,AF} \quad \text{and} \quad r_{C,DF}=\frac{2+\delta}{2(1+\delta)}r_{C,AF}. \tag{28}$$

To conduct a delay-aware comparison, we can thus substitute $\frac{\bar{r}_P(2(1+\delta))}{2+\delta}$ and $\frac{\bar{r}_C(2(1+\delta))}{2+\delta}$ for $\bar{r}_P$ and $\bar{r}_C$ respec-tively for (P1).

V. Numerical Results

We evaluate and compare the covert communication performance of the considered relay systems by conducting numerical simulations. The channel coefficient designated as h_{XY} pertains to the connection between nodes X and Y for X, Y ∈ {*S*, *R*, *D*} is determined as a function of the distance d_{XY} between them. The nodes are lined up in a straight line, as illustrated in Fig. 2. Specifically, we let $h_{XY}=\sqrt{L_{XY}}\hat{h}_{XY}$ where path loss is indicated by $L_{XY}\triangleq L_0(d_{XY}/d_0)^{-\beta}$. L_0 signifies the path loss at regard distance $d_0 = 1$ m, where β is the exponent of the path loss, and the

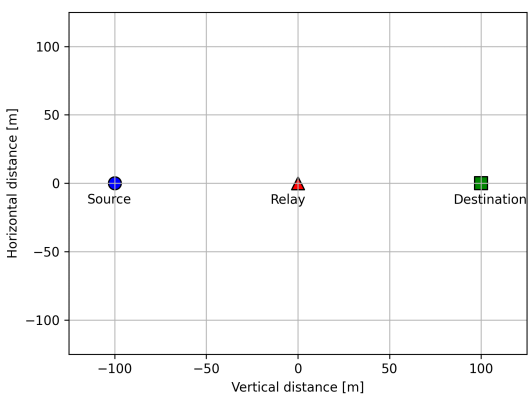

Fig. 2. Node placements

small-scale channel variable $\hat{h}_{XY}$ follows a complex normal distribution $\mathcal{CN}(0, 1)$[29].

5.1 System Setups

We analyze the system under the following configurations: the bandwidth W = 20 MHz, source-to-relay distance d_{SR} = 100 m, relay-to-destination distance d_{RD} = 100 m, source transmit power P_S = 24 dBm or 33 dBm, relay transmit power P_R = 24 dBm or 33 dBm, noise power at the relay $\bar{\sigma}_R^2$ = -160 dBm, noise uncertainty bound ζ = 5 dB, noise power at the destination node σ_D^2 = -160 dBm, path-loss exponent β = 3.5, minimum quality of service for public and covert messages $\bar{r}_P$ = 0.45 bps/Hz and $\bar{r}_C$ = 0.04 bps/ Hz, respectively, and processing delay factor δ = 5.0.

Fig. 3 illustrates the relationship between DEP and the source transmit power P_S. First, we note that DEP first rises until a certain P_S value and then decreases afterwards in every scheme. Observe that α is upper bounded by $1-\frac{\left(2^{\bar{r}_C}-1\right)\sigma_D^2}{|h_{RD}|^2 P_R}$ in (23) and $1-\frac{\left(2^{\bar{r}_C}-1\right)\left(\zeta\sigma_R^2+\bar{\alpha}_D^2\right)}{|h_{SR}|^2 P_S}$ in (26) for DF and AF relay, respectively. When P_S is low, it is likely that the system can not satisfy the minimum QoS constraints in (15e), (15f) for DF, and (16c) for AF, which results in low DEP on average since we set DEP zero for infeasible cases. On the other hand, when P_S increases to a certain level, there will be more feasible cases that fulfill the minimum covert rate QoS constraints for both DF and AF relay systems. If P_S increases further, (18) reveals that $\bar{\alpha}$ gradually reaches 1, which possibly exceeds the upper bound in (22b) for DF and (24b) for AF. As a result, there are more infeasible instances, and the average declines.

As for the comparison between DF and AF, the plot shows that AF is superior to DF when P_S is low. Particularly, the lower bound, $\tilde{\alpha}_{DF}$ in (21). This possibly leads to a larger average optimal solution $\alpha_{AF}^{\star}$ than $\alpha_{DF}^{\star}$, and the DEP for AF is correspondingly higher than DF on average as well.

Another interesting point for AF from the figure is that the fixed-α scheme with the largest α = 0.999 out-performs the other ones with a lower α. The reason for such a phenomenon stems from (26) in which the optimal $\alpha_{AF}^{\star}$ approaches 1 as P_S increases. The exact opposite is visible for the low-P_S region.

We also find that the DF is always preferred in terms of DEP to AF when δ = 0, which indicates a situation where the processing delay is equal. As δ increases alternatively, we observe that there are certain circumstances where AF may outperform DF, especially when P_S is either extremely low or high.

Fig. 4 shows the average DEP for different relays transmit power P_R. It is noteworthy that the DEP increases steadily as P_R increases. We can also observe that AF outperforms DF for low P_R and vice versa for high P_R. The reason lies in the difference in the upper bounds of α for DF and AF. For instance, the upper bound $1-\frac{\left(2^{\bar{r}_C}-1\right)\sigma_D^2}{|h_{RD}|^2 P_R}$ in (23) for DF increases with P_R, while the upper bound for AF in (26) is

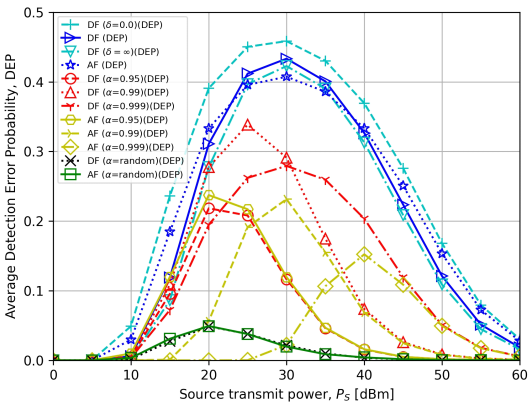

Fig. 3. Average DEP versus source transmit power with δ = 5.0

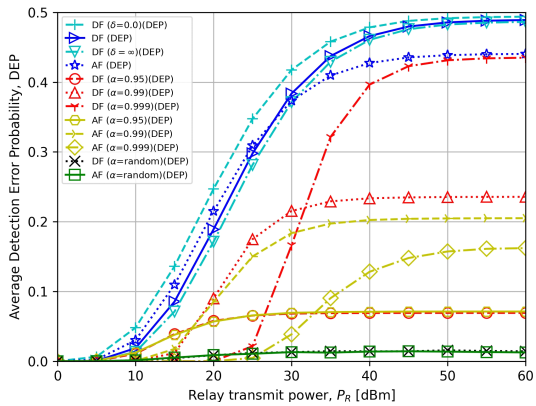

Fig. 4. Average DEP versus relay transmit power with δ = 5.0

unaffected. Therefore, when P_R is high, there is a higher probability for DF to take a larger $\alpha_{DF}^{\star} > \alpha_{AF}^{\star}\alpha$ which eventually results in a higher DEP.

For DF, comparison among the fixed-α schemes shows that higher α (e.g., 0.999) is preferred when P_R is high, while lower α (e.g., 0.95) is preferred when P_R is low. This is explained by (23) where the optimal $\alpha_{DF}^{\star}$ is nearly 1, when P_R is high. Thus, the fixed-α scheme with the highest α = 0.999 outperforms the other fixed-α schemes.

Fig. 5 presents the average DEP in the range of $\bar{r}_P$ for P_S = 33 dBm and P_R = 33 dBm. Every relay scheme experiences a decrease in the DEP since the optimal α in (23) and (26) are inversely related to $\bar{r}_P$. We also observe that when $\bar{r}_P$ is high, the gap between the DEP of AF and DF becomes dramatically large. We first highlight that $\tilde{\alpha}_{DF}$ in (21) and $\tilde{\alpha}_{AF}$ in (25) are the lower bounds of the optimal α for DF and AF, respectively. Then, for DF, (21) reveals that $\tilde{\alpha}_{DF}$ exceeds 1 when $\bar{r}_P$ becomes extremely large. (25), on the other hand, shows that $\tilde{\alpha}_{AF}$ reduces $\bar{\alpha}$ in this case. Therefore, there will be relatively more infeasible instances due to (21) in DF, leading to a lower DEP on average.

Fig. 6 depicts the average DEP corresponding to various $\bar{r}_C$. $\bar{r}_C$ is inversely related to the optimal α values in (23) and (26), and both relay schemes accordingly exhibit a decline in DEP as $\bar{r}_C$ increases. When $\bar{r}_C$ is high, we also note that the DEP of DF is significantly higher than that of AF. We clearly see that $\tilde{\sigma}_D^2$ is larger than σ_D^2 due to our simulation parameters,

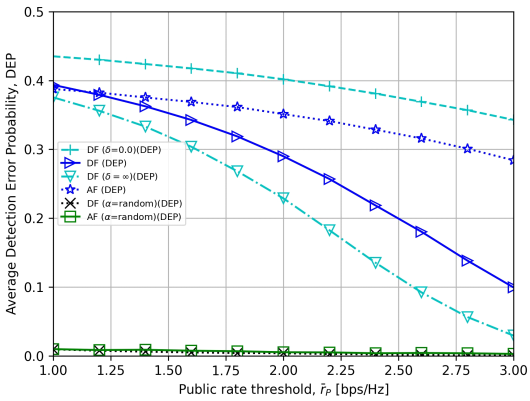

Fig. 5. Average DEP versus minimum quality of service for public messages with δ = 5.0

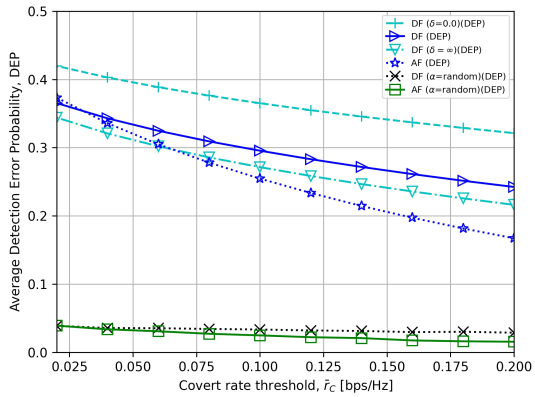

Fig. 6. Average DEP versus minimum quality of service for covert messages with δ = 5.0

where $P_S = P_R$ and $|h_{SR}|^2$ is nearly equal to $|h_{RD}|^2$ since there is the same pathloss and distance between *S*-*R* and *R*-*D*. As a result, the optimal $\alpha_{DF}^{\star}$ in (23) is higher than the optimal $\alpha_{AF}^{\star}$ in (26).

Fig. 7 displays the average DEP for different processing delay factors δ with public message $\bar{r}_P$ = 0.45 bps/ Hz, covert message $\bar{r}_C$ = 0.04 pbs/Hz, P_S = 24 dBm, and P_R = 24 dBm. If δ = 0, we see from equation (28) that the covert rate delay process for the DF relay is comparable to the AF relay. Since the relay performance of DF is generally higher than that of AF, the covert rate constraint will also be more easily satisfied for DF. This explains why DF shows a higher DEP when δ is 0. When δ ≥ 5.0, AF begins to outperform DF since the relay processing delay becomes non-negligible for DF.

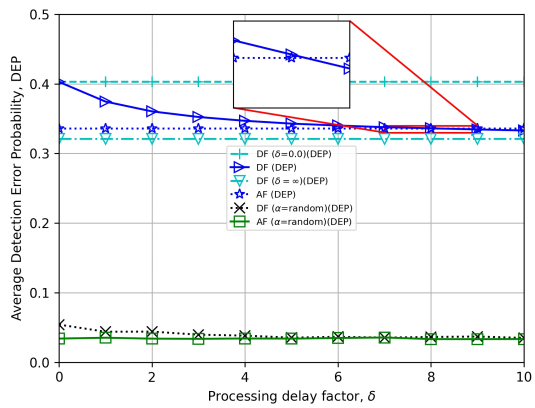

Fig. 7. Average DEP versus processing delay factor

Ⅵ. Conclusion

This paper investigated the comparison of DEP for covert communications between DF and AF relay systems by taking the relay processing delay into consideration. We optimized the transmission power ratio between the public and covert messages, aming for maximum DEP in both relay systems. Through numerical results, we provided a thorough explanation and analyses on the DEP performance, including coparisons between the two different relay protocols from a covert communicaton perspective. The effects of various system parameters such as source and relay transmit power, noise uncertainty bound, and minimum required quality of service for both public and covert messages were studied. The results of this paper can provide helpful guidance in various real-world scenarios, such as when military covert communication is used to exchange sensitive information. The maximum probability that the enemy force can incorrectly identify that sensitive information can be determined through the analysis of this paper. Similarly, the findings of this study can be utilized to evaluate the likelihood that unauthorized entities intercept important information in the banking sector, where covert communication may be employed to transfer important information.

References

[1] J. Moon, “Performance comparison of relay-based covert communication: Df, cf and af,” *Sensors*, Oct. 2023.

[2] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, “5g security threat assessment in real networks,” *Commun. Security in Wireless and Mobile Netw.*, Aug. 2021.

[3] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, and S. Mandal “Wireless communications and applications above 100 ghz: Opportunities and challenges for 6g and beyond,” *IEEE Access*, vol. 7, pp. 78729-78757, Jan. 2019.

[4] M. Pons, E. Valenzuela, B. Rdoriguez, J. A. Nolazco-Flores, and C. Del-valle-Soto, “Utilization of 5g technologies in IoT applications: Current limitations by interference and network optimization difficulties,” *Appl. Internet of Things Netw. in 5G and Beyond*, Apr. 2023.

[5] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, “A systematic survey on 5g and 6g security considerations, challenges, trends, and research areas,” *5G Security: Challenges, Opportunities, and the Road Ahead*, Feb. 2024.

[6] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, “An overview of key technologies in physical layer security,” *Entropy Rev.*, Nov. 2020.

[7] X. Jiang, X. Chen, J. Tang, and N. Zhao, et al., “Covert communication in uav-assisted airground networks,” *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 1-6, Aug. 2021.

[8] B. A. Forouzan, *Introduction of Cryptography and Network Security,* New York, NY, USA: McGraw-Hill, 2007.

[9] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, “Covert communications: A comprehensive survey,” *IEEE Commun. Surv. and Tuts.*, vol. 25, no. 2, pp. 1173-1198, Apr. 2023.

[10] B. A. Bash, D. Goeckel, and D. Towsley, “Limits of reliable communication with low probability of detection on awgn channels,” *IEEE J. Sel. Areas in Commun.*, vol. 31, no. 9, pp. 1921-1930, Sep. 2013.

[11] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, “Fundamental limits of quantum-secure covert communication over bosonic channels,” *IEEE J. Sel. Areas in Commun.*, vol. 38, no. 3, pp. 56-63, Mar. 2020.

[12] M. Ahmadipour, S. Salehkalaibar, M. H. Yassaee, and V. Y. F. Tan, “Covert communication over a compound discrete memoryless channel,” *2019 IEEE ISIT*, pp. 982-986, Sep. 2019.

[13] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, “Achieving covert wireless

communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517-8530, Dec. 2018.

[14] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 236-239, Feb. 2016.

[15] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communications with interference uncertainty," *IEEE Int. Conf. Commun.*, vol. 8, no. 1, pp. 1-6, 2018.

[16] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," *GLOBECOM 2017-2017 IEEE Global Commun. Conf.*, pp. 1-6, Jan. 2018.

[17] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 317-320, Feb. 2019.

[18] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *GLOBECOM 2017-2017 IEEE Global Commun. Conf.*, vol. 17, no. 7, pp. 4766-4779, Jul. 2018.

[19] R. Sun, B. Yang, S. Ma, Y. Shen, and X. Jiang, "Covert rate maximization in wireless full-duplex relaying systems with power control," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6198-6212, Sep. 2021.

[20] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Inf. Forensics and Secur.*, vol. 17, pp. 760-773, Feb. 2022.

[21] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Trans. Wireless Commun.*, vol. 18, pp. 4089-4102, Aug. 2019.

[22] M. Wang, Z. Xu, B. Xia, Y. Guo, and Z. Chen, "Df relay assisted covert communication: Analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 4073-4078, Mar. 2023.

[23] H. Q. Ta, K. Ho-Van, D. B. da Costa, S. W. Kim, and H. Oh, "Covert communications over non-orthogonal multiple overt channels," *IEEE Access*, vol. 10, pp. 122361-122375, 2022.

[24] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941-944, Apr. 2017.

[25] J. Si, Z. Li, Y. Zhao, J. Cheng, L. Guan, J. Shi, and N. Al-Dhahir, "Covert transmission assisted by intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394-5408, Aug. 2021.

[26] S. W. Kim and H. Q. Ta, "Covert communications over multiple overt channels," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1112-1124, Feb. 2022.

[27] J. Moon, "The channel uncertainty of warden on disguised full-duplex covert communications," *J. KICS*, vol. 48, no. 11, pp. 1365-1373, Nov. 2023.

[28] B. Makki and M. S. Alouini, "End-to-end performance analysis of delay-sensitive multirelay networks," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2159-2163, Dec. 2019.

[29] J. Moon, O. Simeone, S. H. Park and I. Lee, "Online reinforcement learning of X-haul content delivery model in fog radio access networks," *IEEE Signal Process. Lett.*, vol. 26, no. 10, pp. 1451-1455, Oct. 2019.

Md Sakil Hasan

Aug. 2016 : B.Sc., Computer Science & Engineering, Primeasia University, Bangladesh

Aug. 2024: M.Eng., Department of Mobile Convergence Engineering, Hanbat National University, the Republic of Korea

Sept. 2024-Current: Ph.D. student, Department of Mobile Convergence Engineering, Hanbat National University, the Republic of Korea

<Research Interest> Wireless communications, physical layer security, wireless security, machine learning

[ORCID:0009-0009-9958-3579]

Jihwan Moon

Feb. 2014 : B.Eng., Departmet of Electrical Engineering, Korea University, the Republic of Korea

Feb. 2019 : Ph.D., Department of Electrical Engineering, Korea University, the Republic of Korea

Jan. 2018-Mar. 2018 : Visiting research student, King's College London

Mar. 2019-Jul. 2019: Postdoctoral research associate, Research Institute for Information and Communication Technology (RICT), Korea University, the Republic of Korea

Jul. 2019-Aug. 2020: Researcher, The Affiliated Institute of Electronics and Telecommunications Research Institute (ETRI), the Republic of Korea

Sept. 2020-Feb. 2022: Assistant professor, Department of Information and Communication Engineering, Chosun University, the Republic of Korea

Mar. 2022-Current : Assistant professor, Department of Mobile Convergence Engineering, Hanbat National University, the Republic of Korea

<Research Interest> Optimization techniques, energy harvesting, physical-layer security, wireless surveillance, covert communications, and machine learning for wireless communications.

[ORCID:0000-0002-9812-7768]