https://doi.org/10.7840/kics.2024.49.12.1715

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

Refat Khan◆, Jihwan Moon°

ABSTRACT

This paper delves into reliable covert communications with a disguised full-duplex (FD) node. Seemingly half-duplex receive-only, this node in our considered system simultaneously listens to a transmitter and secretly transmits covert mes- sages to another hidden receiver. In the meantime, a warden attempts to detect this covert link. We first study the detection error probability (DEP) and identify the minimum DEP from the perspective of the warden. After that, we derive the optimal transmit power of the disguised FD node that concurrently maximizes the minimum DEP and guarantees a given reliability of the covert rate. Numerical results validate the effectiveness of our proposed solution and present how dif- ferent system parameters affect DEP performance. In conclusion, we provide valuable guidance for the design of secure communication systems and suggest future research directions in this critical domain.

Key Words : Physical layer security, covert communications, low probability of detection, full duplex, detection error probability

Ⅰ. Introduction

Wireless technology has transformed numerous facets of human existence, including connectivity, healthcare,education, and economic systems, reshaping the very fabric of daily life[1,2]. The widespread adoption of wireless communications, on the other hand, is accompanied by cyberattacks that expose users to the risk of information disclosure[3]. In response to this challenge, cryptography has become extensively utilized, employing secret keys to encode and decode data[4]. Besides, a number of foundational studies Traditional cryptography and physical layer security hold profound importance in fortifying information. Security against unauthorized interception, paving the way for advancements in safeguarding sensitive data[5,6]. Nonetheless, even though these technologies keep our messages safe from eavesdroppers, communication links might still be at privacy risk. For instance, the electromagnetic signals from a commander on the battlefield may expose his position to nearby enemies. Communicating in the presence of an authoritarian government that may want to curtail any organization by certain entities[7]. A suitable solution for such scenarios involves covert or low-probability detection. communications, which conceals the presence of crucial communication links[8].

※ 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-2024-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, 30224029@o365.hanbat.ac.kr, 학생회원
° Corresponding Author : Hanbat National University, Department of Mobile Convergence Engineering, anschino@staff.hanbat.ac.kr, 정회원
논문번호 : 202407-144-B-RU, Received July 13, 2024; Revised August 21, 2024; Accepted Augst 27, 2024

Extensive research has also been conducted on covert communications within full duplex (FD) systems. The authors in [9] investigated covert communication using an FD receiver under limited channel information and demonstrated that random noise improves performance. By optimizing transmit and artificial noise (AN) power to minimize outage probability at Bob, the authors observed a non-linear relationship between AN power and performance. Additionally, the numerical results in [10] presented some performance differences between circumstances with and without channel state information (CSI). In [11], a constrained muliti objective optimization problem (MOP) was formulated to maximize two conflicting objectives: the transmission rate between legitimate transceivers and the average covert probability (ACP) for eavesdroppers.

In complex FD systems, the exhibition of covert communications fluctuates across diverse relay systems: decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF). The study in [12] compares DF, CF, and AF systems,accounting for system parameters such as processing delay, quality of service, and detection error probability (DEP) threshold, revealing performance variations under different conditions. In [13], the authors devised a protocol for energy harvesting FD DF relay-based covert communications. Additionally, [14] scrutinized FD relay-aided covert communications from a satellite to a ground node in the context of integrated satellite - terrestrial communications. The optimization of both secrecy and covert rates was performed in [15], where an untrusted FD AF relay transmits the covert message to an FD base station. The base station then emits artificial noise (AN) to deceive the warden. In the Internet of Things (IoT) domain, [16] investigated a covert transmitter with optimized transmission probability, powered wirelessly by artificial noise (AN) from an FD receiver. Moreover, [17] optimized covert uplink transmissions of devices to FD IoT gateways using a mean-field Stackelberg game approach. Additionally, [18] utilized an ambient backscatter system, in which artificial noise (AN) is concurrently broadcast by an FD receiver, and an ambient signal is modulated into a covert signal by a radio frequency tag.

Recently, the research community has given significant attention to possibilities of covert communications in intelligent reflecting surfaces (IRS)[19,20]. The authors of [21] and [22] collectively contribute to advancing the field of covert communication within IRS aided communication systems. They focus on optimizing transmission power, phase shifts, and beamforming vectors to maximize secrecy while leveraging IRS technology. Additionally, they propose novel algorithms to address the optimization challenges posed by imperfect channel state information (CSI), offering practical solutions to enhance covert communication performance. By exploring the potential of IRS in multi-antenna systems and tackling non-convex optimization problems using penalty dual decomposition (PDD) and successive convex approximation (SCA) methods, these papers provide valuable insights and techniques for improving covert communication in the presence of surveillance. The authors of [23] examined an IRS communication scenario where a covert user possesses full control over the IRS and remains concealed from the warden. In [22], the optimization of a transmit beamforming vector and reflecting coefficients is conducted for IRS-aided covert communications, where an FD receiver emits random artificial noise (AN) to confuse the warden.

Moreover, covert communications have been briefly studied in unmanned aerial vehicle (UAV) systems. In [24], the authors concentrated on a covert communication setup utilizing UAVs equipped with FD receivers. In [25], UAVs were employed to help the transmission and confuse the warden. The maximum of the lowest average covert rate was achieved in the case of an FD UAV collecting data from a scheduled user and interfering with unscheduled users using AN[26]. In [27], the authors explored an FD DF UAV relay to facilitate covert communications, where multiple sensors transmit messages to a remote base station in separate time slots.

Some literature has investigated covert communications in cognative radio (CR) networks. Chen et al.[28] analyzed user scheduling performance in covert CR Networks. In [29], the authors addressed the problem of power allocation with the aid of generative adversarial networks in covert CR networks. The authors of

[30] considered covert communications by exploiting cognitive jammers to counter an intelligent eavesdropper, thereby enhancing physical layer security within cooperative cognitive radio networks. In [31] the authors discussed the dilemmas, balancing covertness and secrecy. On one hand, the goal is to prevent detection by the Device to Device (D2D) communications, while on the other hand, the untrusted relay poses a threat of eavesdropping on the user equipment (UE) message. Another dilemma arises in determining the optimal power control strategy at the UE, relay, and base station (BS) to maximize the average covert rate while ensuring covertness and security requirements are met.

Although numerous communications systems have been analyzed from various perspectives of covertness as such, it is worth pointing out that many studies have presumed that surveillance nodes possess complete knowledge about the hardware specifications of covert nodes. However, covert nodes have the potential to enhance their concealment by masquerading as different functional entities. For example, an FD node secretly transmitting sensitive messages might masquerade as a receiver-only HD node. To the author's knowledge, there has not been sufficient work on covert communications that incorporates such deceptive strategies besides our initial result in [32].

In our covert communication system, the setup involves a source node transmitting a public message to a seemingly receive-only destination node. This destination then secretly transmits a covert message to a hidden receiver using an unseen antenna in an FD manner. Our focus is on ensuring secure and undetectable transmission from the destination to the hidden node, all while under the surveillance of the warden node. In contrast to [32], which focuses on maximizing the covert rate with equal probabilities for covert and public messages, our work prioritizes the maximization of the worst-case detection error probability (DEP) while maintaining a guaranteed covert rate. This is more suitable for scenarios where ensuring detection avoidance is more critical than the mere covert transmission rate, such as military communication, intelligence operations, and critical infrastructure protection. The contributions of our research can be outlined as follows:

- Unlike previous studies which assume that the surveillance party is sure of covert node hardware specifications, we consider a practical scenario where a covert communication node disguises itself as a different functional entity to enhance its stealth further.
- The worst-case DEP is derived by considering an arbitrary covert transmission probability, which generalizes the previous result in [32] where only an equally probabilistic covert transmission was handled.
- Our focus lies in improving the minimum DEP at the warden node by optimizing both the public data rate as well as the FD destination node of the transmit power. Additionally, we prioritize maintaining a minimum covert rate within the system.
- We explore the impact of diverse system parameters on the worst-case DEP using numerical analysis.
- Given that our study offers insights from an information-theoretic standpoint, we propose exploring practical modulation techniques and the implications of imperfect CSI as promising for future research.

In Section II, we will go over the system concept and quickly review received signals and covert message identification. In Section III, we will formulate the problem by considering several important constraints. In Section IV, we will propose a solution to maximize the worst-case DEP while meeting all constraints. Lastly, we will provide the numerical outcomes of our suggested plan in Section V.

Ⅱ. System Model

2.1 Received Signals

Fig. 1 depicts the system model we are considering. There is a source node S that sends a public message to a destination node D which appears to be a half-duplex receive-only, but in fact, secretly sends a covert message to a hidden receiver node R using a concealed extra antenna. Meanwhile, a warden node W, monitors for any unexpected communications i.e.,

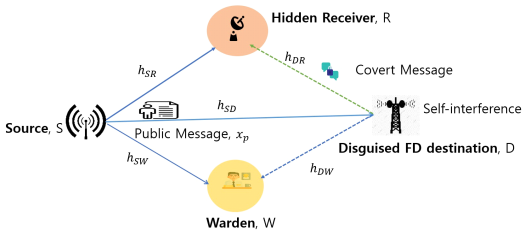

Fig. 1. System model

covert messages. At the FD destination node that is disguised the received signal can be stated as

$$y_D = h_{SD}\sqrt{P_S}x_P + \tilde{h}_{DD}\sqrt{P_D}x_C + z_D. \quad (1)$$

In this system model, the channel coefficient *h*XY represents communication links between different nodes X, Y ∈ {*S, D, R, W*}. The residual self-interference channel $\tilde{h}_{DD} \sim CN(0, \sigma_{SI}^2)$ accounts for leftover signals after self-interference cancellation. Public messages $x_P \sim CN(0, 1)$ and covert messages $x_C \sim CN(0, 1)$ are transmitted. The transmit power is denoted by P_S and P_D for the source and destination nodes, respectively. Additive noise $z_X \sim CN(0, \sigma_X^2)$ is present at each node, and we assume that the destination node can estimate the *hSD* while the hidden receiver can estimate *hSR* and *hDR* if provided with pilot sequences[33]. The warden is assumed to have perfect knowledge of all CSI for the worst-case scenario analysis. We also consider that the source adopts its data rate based on destination feedback and the achievable data rate at the destination is denoted by $\bar{r}_{P,D}$ as [34]

$$\bar{r}_{P,D} = \log_2\left(1 + \frac{|h_{SD}|^2 P_S}{|\tilde{h}_{DD}|^2 P_D + \sigma_D^2}\right). \quad (2)$$

Next, consider a direct message from the source node to the public, along with a hidden message from the destination node. Accordingly, the received signal at the hidden receiver can be written as:

$$y_R = h_{SR}\sqrt{P_S}x_P + h_{DR}\sqrt{P_D}x_C + z_R. \quad (3)$$

The hidden receiver first decodes and removes the public message before accessing the covert message. Consequently, the achievable public data rate, denoted by $\bar{r}_{P,R}$ at the hidden receiver is given by

$$\bar{r}_{P,R} = \log_2\left(1 + \frac{|h_{SR}|^2 P_S}{|h_{DR}|^2 P_D + \sigma_R^2}\right). \quad (4)$$

The achievable covert rate resulting after removing x_P from y_R can also be evaluated as

$$r_{C,R} = \log_2\left(1 + \frac{|h_{DR}|^2 P_D}{\sigma_R^2}\right). \quad (5)$$

2.2 Covert Message Detection

The received signal at the warden is expressed by

$$y_W = h_{SW}\sqrt{P_S}x_P + h_{DW}\sqrt{P_D}x_C + z_W. \quad (6)$$

It first excludes public messages from *yW* to calculate the effective residual signal $\tilde{z}_W \triangleq y_W - h_{SW}\sqrt{P_S}x_P$, presuming that is fully aware of h_{SW} and P_S[33]. The warden can then take into account these two hypothesis:

$$\begin{aligned} H_0 &: \ \tilde{z}_W = z_W, \\ H_1 &: \ \tilde{z}_W = h_{DW}\sqrt{P_D}x_C + z_W. \end{aligned} \quad (7)$$

The null hypothesis H_0 indicates a case that there are no covert messages, the alternative hypothesis H_1 presumes that the destination node transmits a covert message.

In this study, a radiometer is utilized as a detection method at the warden[35]. The test statistic *T* for equation (7), after observing $N \to \infty$ number of symbols leads to the average residual power $\mathrm{E}[|\tilde{z}_W|^2]$ as [7]

$$\begin{aligned} H_0 &: \ T = \sigma_W^2, \\ H_1 &: \ T = |h_{DW}|^2 P_D + \sigma_W^2. \end{aligned} \quad (8)$$

The warden node determines the presence of a covert transmission if *T* surpasses a predefined threshold τ. In this paper, we consider uncertainty in the noise variance σ_W^2 at the warden, similar to [35], [7], and [21]. Specifically, we model the noise variance σ_W^2 in decibels as $\sigma_{W,\mathrm{dB}}^2 \sim U(\bar{\sigma}_{W,\mathrm{dB}}^2 - \zeta_{\mathrm{dB}}, \bar{\sigma}_{W,\mathrm{dB}}^2 + \zeta_{\mathrm{dB}})$ where

$\sigma^2_{W,\mathrm{dB}}$ represents the mean and $\zeta_{\mathrm{dB}} \geq 0$ denotes the bounded range. The resulting DEP Pr(e), that encompasses both false alarm and miss detection probabilities is then expressed by

$$\Pr(\mathrm{e}) = \underbrace{\Pr(T \geq \tau | H_0)}_{\text{False alarm}} \Pr(H_0) + \underbrace{\Pr(T < \tau | H_1)}_{\text{Miss}} \Pr(H_1), \tag{9}$$

By leveraging the CDF of σ^2_W as [36]

$$F_{\sigma^2_W}(\nu) = \frac{1}{2\ln\zeta}\left[\ln\nu - \frac{\ln\overline{\sigma}^2_W}{\zeta}\right] \text{for} \nu \in \left(\frac{\overline{\sigma}^2_W}{\zeta}, \zeta\overline{\sigma}^2_W\right), \tag{10}$$

the false alarm and miss probability are calculated by

$$\Pr(T \geq \tau | H_0) = 1 - F_{\sigma^2_W}(\tau) \quad \text{for} \quad \tau \in T_1, \tag{11}$$

$$\Pr(T < \tau | H_1) = 1 - F_{\sigma^2_W}\left(\tau - |h_{DW}|^2 P_D\right) \quad \text{for} \quad \tau \in T_2. \tag{12}$$

respectively, where $T_1 \triangleq [\frac{\overline{\sigma}^2_W}{\zeta}, \zeta\overline{\sigma}^2_W]$ and $T_2 \triangleq [|h_{DW}|^2 P_D + \frac{\overline{\sigma}^2_W}{\zeta}, |h_{DW}|^2 P_D + \zeta\overline{\sigma}^2_w]$. We encounter two distinct scenarios depending on the magnitude of $|h_{DW}|^2$ and P_D. If $\zeta\overline{\sigma}^2_W < |h_{DW}|^2 P_D + \frac{\overline{\sigma}^2_W}{\zeta}$,

$$\Pr(\mathrm{e}) = \begin{cases} (1-p)\Pr(T \geq \tau \mid H_0), & \tau \in T_1, \\ 0, & \tau \in T_3, \\ p\Pr(T < \tau \mid H_1), & \tau \in T_2, \end{cases} \tag{13}$$

where $\Pr(H_0) = 1 - p$, $\Pr(H_1) = p$, and $T_3 \triangleq [\zeta\overline{\sigma}^2_W, |h_{DW}|^2 P_D + \frac{\overline{\sigma}^2_W}{\zeta}]$. On the other hand, if $\zeta\overline{\sigma}^2_W \geq |h_{DW}|^2 P_D + \frac{\overline{\sigma}^2_W}{\zeta}$,

$$\Pr(\mathrm{e}) = \begin{cases} (1-p)\Pr(T \geq \tau \mid H_0), & \tau \in T_4, \\ (1-p)\big(\Pr(T \geq \tau \mid H_0) & \\ \quad + p\Pr(T < \tau \mid H_1)\big), & \tau \in T_5, \\ p\Pr(T < \tau \mid H_1), & \tau \in T_6, \end{cases} \tag{14}$$

with $T_4 \triangleq [\frac{\overline{\sigma}^2_W}{\zeta}, |h_{DW}|^2 P_D + \frac{\overline{\sigma}^2_W}{\zeta}]$, $T_5 \triangleq [|h_{DW}|^2 P_D + \frac{\overline{\sigma}^2_W}{\zeta}, \zeta\overline{\sigma}^2_W]$, and $T_6 \triangleq [\zeta\overline{\sigma}^2_W, |h_{DW}|^2 P_D + \zeta\overline{\sigma}^2_W]$.

It is evident that the warden aims to set the threshold τ to minimize the DEP. We see from (13) that the worst-case DEP is 0 regardless of p if τ is set to any value from T_3 when $\zeta\bar{\sigma}^2_W < |h_{DW}|^2 P_D + \frac{\bar{\sigma}^2_W}{\zeta}$ from (13). Therefore, we now focus on the second case when $\zeta\bar{\sigma}^2_W \geq |h_{DW}|^2 P_D + \frac{\bar{\sigma}^2_W}{\zeta}$. Particularly, the DEP for $\tau \in T_5$ in (14) can be re-expressed by

$$\begin{aligned} \Pr(\mathrm{e}) &= (1-p)\Pr(T \geq \tau \mid H_0) + p\Pr(T < \tau \mid H_1) \\ &= 1 - p - \frac{1}{2\ln\zeta}\Big(\ln(\tau) - p\ln\big(\tau(\tau - |h_{DW}|^2 P_D)\big) \\ &\quad - (1-2p)\ln\left(\frac{\overline{\sigma}^2_w}{\zeta}\right)\Big). \end{aligned} \tag{15}$$

The first derivative for $p = 0.5$ then becomes

$$\begin{aligned} &\frac{\partial}{\partial\tau}\left(\frac{1}{2}\Pr(T \geq \tau \mid H_0) + \frac{1}{2}\Pr(T < \tau \mid H_1)\right) \\ &= \frac{1}{2}\frac{1}{2\ln\zeta}\frac{|h_{DW}|^2 P_D}{\tau(\tau - |h_{DW}|^2 P_D)}, \end{aligned} \tag{16}$$

which is an increasing function for $\tau \geq |h_{DW}|^2 P_D$. On the other hand, if $p \neq \frac{1}{2}$,

$$\begin{aligned} &\frac{\partial}{\partial\tau}\left(\frac{1}{2}\Pr(T \geq \tau \mid H_0) + \frac{1}{2}\Pr(T < \tau \mid H_1)\right) \\ &= -\frac{1-2p}{2\ln\zeta}\left(\frac{\tau - \frac{1-p}{(1-2p)}|h_{DW}|^2 P_D}{\tau(\tau - |h_{DW}|^2 P_D)}\right). \end{aligned} \tag{17}$$

The expression reveals the existence of a unique extreme point at $\tau_{ext} = \frac{1-p}{(1-2p)}|h_{DW}|^2 P_D$. Since $\frac{\partial}{\partial p}\left(\frac{1-p}{1-2p}\right) = \frac{1}{(1-2p)^2} > 0$, τ_{ext} increases with p. Furthermore, $\tau_{ext} \in [|h_{DW}|^2 P_D, +\infty)$ if $p \in [0,\ 0.5)$, and $\tau_{ext} \in (-\infty,\ 0]$ if $p \in [0,\ 0.5)$ as shown in Fig. 2. Let us inves-tigate the shape of the DEP function in the two different regions of p as follows.

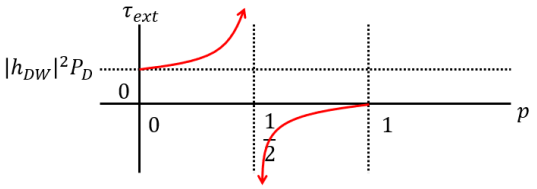

Fig. 2. Variation of extremum point τ_{ext} with respect to p

2.2.1 Case 1: $p \in [0,\ 0.5)$

Note that $\frac{1-p}{1-2p} \in [1, +\infty)$ since $1-2p \in (0,\ 1]$ in this case. Based on this, the first derivative of the DEP can be drawn as Fig. 3.

Therefore, the DEP in (14) for all regions of τ will exhibit the shape in Fig. 4. The following lemma then proves that the DEP is lower at $\tau = |h_{DW}|^2P_D + \frac{1}{\zeta}\bar{\sigma}_W^2$ compared to that at $\tau = \zeta\bar{\sigma}_W^2$.

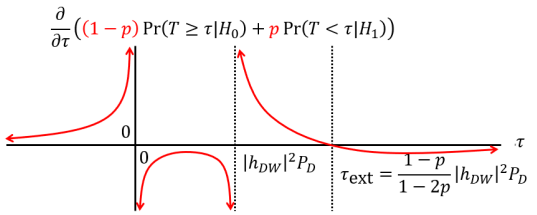

Fig. 3. Shape of the first derivative of the DEP as a function of τ for $p \in [0,\ 0.5)$

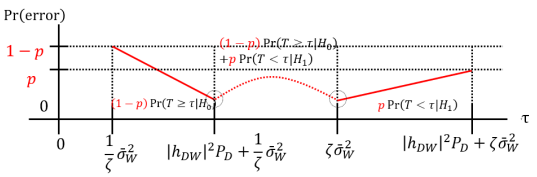

Fig. 4. The shape of DEP as a function of τ

Lemma 1. *For* $\zeta\bar{\sigma}_w^2 \geq |h_{DW}|^2P_D + \frac{\bar{\sigma}_w^2}{\zeta}$ *and* $p \in \left[0, \frac{1}{2}\right)$, $Pr(error)\big|_{\tau=|h_{DW}|^2P_D+\frac{\bar{\sigma}_w^2}{\zeta}} < Pr(error)\big|_{\tau=\zeta\bar{\sigma}_w^2}$.

Proof. First note that

$$\Pr(\text{error})\big|_{\tau=\zeta\bar{\sigma}_w^2} - \Pr(\text{error})\big|_{\tau=|h_{DW}|^2P_D+\frac{\bar{\sigma}_w^2}{\zeta}}$$
$$= \frac{1}{2\ln\zeta}\ln\left(\frac{\left(|h_{DW}|^2P_D+\frac{\bar{\sigma}_w^2}{\zeta}\right)^{1-p}\left(\zeta\bar{\sigma}_w^2-|h_{DW}|^2P_D\right)^p}{\left(\zeta\bar{\sigma}_w^2\right)^{1-p}\left(\frac{\bar{\sigma}_w^2}{\zeta}\right)^p}\right) \geq 0$$

if

$$\ln\left(\frac{\left(|h_{DW}|^2P_D+\frac{\bar{\sigma}_w^2}{\zeta}\right)^{1-p}\left(\zeta\bar{\sigma}_w^2-|h_{DW}|^2P_D\right)^p}{\left(\zeta\bar{\sigma}_w^2\right)^{1-p}\left(\frac{\bar{\sigma}_w^2}{\zeta}\right)^p}\right) \geq 0 \tag{18}$$

This implies that

$$\left(\frac{|h_{DW}|^2P_D+\frac{\bar{\sigma}_w^2}{\zeta}}{\zeta\bar{\sigma}_w^2}\right)^{1-p} \geq \left(\frac{\frac{\bar{\sigma}_w^2}{\zeta}}{\zeta\bar{\sigma}_w^2-|h_{DW}|^2P_D}\right)^p \tag{19}$$

To verify this, let us define $\nu_1 \triangleq |h_{DW}|^2P_D + \frac{\bar{\sigma}_W^2}{\zeta}$, $\nu_2 \triangleq \zeta\bar{\sigma}_w^2$, and $a \triangleq |h_{DW}|^2$, P_D such that

$$\frac{|h_{DW}|^2P_D+\frac{\bar{\sigma}_W^2}{\zeta}}{\zeta\bar{\sigma}_w^2} = \frac{\nu_1}{\nu_2} \text{ and } \frac{\frac{\bar{\sigma}_w^2}{\zeta}}{\zeta\bar{\sigma}_w^2-|h_{DW}|^2P_D} = \frac{\nu_1-a}{\nu_2-a}. \tag{20}$$

Taking the derivative of $\frac{\nu_1-a}{\nu_2-a}$ with respect to a, and noting that $\nu_2 \geq \nu_1$ from our assumption, we can see that

$$\frac{\partial}{\partial a}\left(\frac{\nu_1-a}{\nu_2-a}\right) = \frac{\nu_a-a}{(\nu_2-a)^2} \leq 0. \tag{21}$$

This confirms that the function is an increasing of a, leading to $\frac{\nu_1}{\nu_2} \geq \frac{\nu_1-a}{\nu_2-a}$.

Furthermore since $p \in [0,\ 0.5)$,

$$\left(\frac{\nu_1}{\nu_2}\right)^{1-p} \geq \left(\frac{\nu_1-a}{\nu_2-a}\right)^p. \tag{22}$$

This completes the proof. □

The rest is to compare τ_{ext} and $\zeta\bar{\sigma}_W^2$. IF $\tau_{ext} < \zeta\bar{\sigma}_W^2$, the rough shape of the DEP in (14) can be shown as Fig. 5. Otherwise, the function will have the shape in Fig. 6.

Consequently, we can conclude that the worst-case DEP occurs at $\tau = |h_{DW}|^2P_D + \frac{1}{\zeta}\bar{\sigma}_W^2$, and the corresponding DEP value is $(1-p)\Pr(T \geq \tau\,|\,H_0)$.

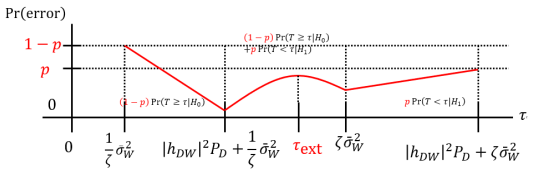

Fig. 5. The shape of DEP as a function of τ

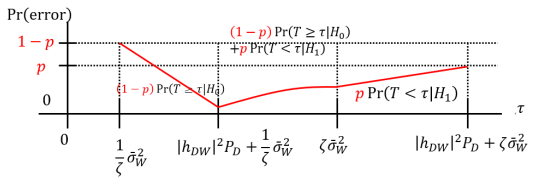

Fig. 6. The shape of DEP for $\tau_{ext} < \zeta\bar{\sigma}_w^2$ and $p \in [0, 1)$

2.2.2 Case 2: $p \in (0.5, 1]$

In this case, we have $1-2p \in [-1, 0)$ and $\frac{1-p}{1-2p} \in (-\infty, 0)$, which yields the shape of the first derivative of the DEP as Fig. 7.

Observing from Fig. 7 that the DEP is an increasing function for $\tau > |h_{DW}|^2P_D$, Fig. 8 shows a sketch of the DEP in (14). Similar to Case 1, it can be seen that the worst-case DEP occurs at $\tau = |h_{DW}|^2P_D + \frac{1}{\zeta}\bar{\sigma}_W^2$, and the corresponding DEP value is also $(1-p)\Pr(T \geq \tau \mid H_0)$.

Thus, the optimal threshold τ^* for the warden node in both(13) and (14) is obtained by

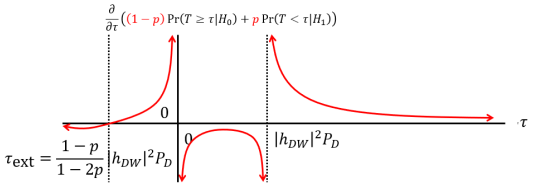

Fig. 7. Shape of the first derivative of the DEP as a function of τ for $p \in (\frac{1}{2}, 1)$

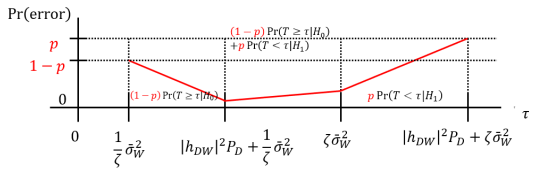

Fig. 8. The shape of DEP for $p \in (\frac{1}{2}, 1]$

$$\tau^* = |h_{DW}|^2 + \frac{1}{\zeta}\bar{\sigma}_W^2, \tag{23}$$

and the worst-case DEP is calculated by

$$\min \Pr(\mathrm{e}) = \begin{cases} 0, & \zeta\bar{\sigma}_W^2 \\ & < |h_{DW}|^2P_D + \frac{\bar{\sigma}_W^2}{\zeta}, \\ (1-p) & \zeta\bar{\sigma}_W^2 \\ \cdot\left(1-\frac{1}{2\ln\zeta}\left(\ln\tau^*-\ln\left(\frac{\bar{\sigma}_W^2}{\zeta}\right)\right)\right), & \geq |h_{DW}|^2P_D + \frac{\bar{\sigma}_W^2}{\zeta}. \end{cases} \tag{24}$$

Remark 1. *The worst-case DEP monotonically decreases with p, implying that the more the disguised FD node transmits, the more probable the warden will detect it.*

It is important to note that we operate under the conservative assumption that the warden is fully aware of the true value of P_D. This represents the worst-case scenario in terms of clandestine communications.

Ⅲ. Problem Formulation

In this study, we aim to optimize the public data rate and transmission power at the disguised FD destination node that maximizes the minimum error probability at the warden node as

$$\text{(P1)}: \max_{P_D, r_P} \min \Pr(\mathrm{e}), \tag{25a}$$

$$\text{subject to: } r_P \leq \bar{r}_{P,R}, \tag{25b}$$

$$r_P \leq \bar{r}_{P,D}, \tag{25c}$$

$$r_P \geq \bar{r}_P, \tag{25d}$$

$$r_P \geq \bar{r}_C, \tag{25e}$$

$$\zeta\bar{\sigma}_W^2 \geq |h_{DW}|^2P_D + \frac{\bar{\sigma}_W^2}{\zeta}, \tag{25f}$$

$$0 \leq P_D \leq \bar{P}_D. \tag{25g}$$

Constraint (25b) ensures that the hidden receiver can successfully decode and remove the public message before decoding the covert message. Constraint

Table 1. Notation

Notation	Description
r_p	Public data rate
P_s	Source transmit power
P_D	Destination transmit power
$\bar{r}_{P,D}$	Public message QoS at D
$\bar{r}_{P,R}$	Public data rate at hidden receiver
$\bar{r}_P$	Minimum quality of service
$\bar{r}_c$	Threshold of covert data rate

(25c) specifies the maximum achievable public data rate, allowing the destination node to inform the source node for adjustment. In (25d), a minimum quality of services $\bar{r}_P$ for public transmission is considered. (25e) specifies a minimum threshold $\bar{r}_c$ for the covert data rate for reliable covert transmission and (25f) ensures a non-zero DEP. Finally, constraint (25g) indicates the power budget $\bar{P}_D$ for the disguised FD destination node.

Ⅳ. Proposed Solutions

This chapter discusses the solution for (P1) that maximizes the worst-case DEP in (25a). First, it is important to note that DEP is a decreasing function of P_D(i.e., the derivative of DEP equation (15) is negative with respect to P_D). Similarly, the upper limits of the public data rate (25b) and (25c) also decrease as P_D increases (P_D is denominator at equation (2) and (4)). This implies that the public rate cannot surpass a certain threshold, which is defined by the minimum of two upper limits, namely r_P, i.e. $r_P = \min(r_{P,R}, r_{P,D})$. Consequently, it's advantageous for r_P to remain at its lowest feasible level to consistently uphold a minimum public rate, as given by

$$r_P^* = \bar{r}_P, \tag{26}$$

However, the covert rate in (25e) increases with an increase P_D . Therefore, in order to maximize the worstcase DEP, we can easily see that the covert rate should be set to the minimum possible value, which is the required threshold $\bar{r}_C$. Given these trade-offs, (P1) reduces to the following:

$$\text{(P1.2)}: \min_{P_D} P_D, \tag{27a}$$

$$\text{subject to: } P_D \le \frac{1}{|h_{DR}|^2}\left(\frac{|h_{SR}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_R^2\right), \tag{27b}$$

$$P_D \le \frac{1}{|\tilde{h}_{DD}|^2}\left(\frac{|h_{SD}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_D^2\right), \tag{27c}$$

$$P_D \ge \frac{\sigma_R^2}{|h_{DR}|^2}\left(2^{\bar{r}_C}-1\right), \tag{27d}$$

$$P_D \le \left(\zeta - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_W^2}{|h_{DW}|^2}, \tag{27e}$$

$$0 \le P_D \le \bar{P}_D. \tag{27f}$$

Therefore, this leads to the optimal P_D as

$$P_D^* = \min\left(\frac{1}{|h_{DR}|^2}\left(\frac{|h_{SR}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_R^2\right), \frac{1}{|\tilde{h}_{DD}|^2}\left(\frac{|h_{SD}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_D^2\right), \frac{\sigma_R^2}{|h_{DR}|^2}\left(2^{\bar{r}_C}-1\right), \bar{P}_D\right), \tag{28}$$

The analytical solution we derived revealed several key insights:

Remark 2. *In certain scenarios, the upper bound may be lower than the lower bound. In such infeasible cases, the transmit power P_D can be simply set to 0 in an effort to evade from detection.*

Remark 3. *When the link between the destination and receiver is exceptionally strong, the optimal transmit power for the destination node tends towards zero. This occurs because the hidden receiver cannot effectively filter out source messages before receiving covert messages. In such a case, the hidden receiver may consider directly decoding the covert message instead of first decoding and subtracting the public message.*

Remark 4. *Insufficient suppression of self-interference also leads to an optimal transmit power close to zero, as the public data rate cannot maintain the required quality of service.*

Remark 5. *In scenarios where the channel gain between the destination and warden node is significantly high, the optimal transmit power for the destination node approaches zero, as the warden node can more easily detect the covert link due to the large power difference.*

V. Numerical Results

We assess the maximum achievable worst-case DEP with the disguised FD node through numerical analysis. We investigate the impacts of different system parameters, including source transmit power, disguised FD destination transmit power budget, noise ambiguity bound, and minimal quality of service r_P, along with the derived optimal destination transmit power P_D^* from (28).

We adopt the distance-dependent channel model from [37], where $|h_{XY}|^2 = L_{XY}|\hat{h}_{XY}|^2$, $L_{XY} = L_0\left(\frac{d_{XY}}{d_0}\right)^{-b}$, represents the path loss between nodes X and Y, L_0, denotes the path loss at a reference distance $d_0 = 1$ m, b signifies the path loss exponent, and d_{XY}, reveals the distance between nodes X together with Y. Additionally, the small-scale channel variable $\hat{h}_{XY}$, follows the complex normal distribution $\mathcal{CN}(0, 1)$. The four nodes are positioned at certain distance from the origin $O = (0, 0)$, in the cartesian coordinate system, with coordinates for S, D, R and W, denoted by $(-d_{OS}, 0)$, $(d_{OD}, 0)$, $(0, d_{OR})$, and $(0, d_{OW})$, respectively (Fig. 1). The overall system parameters are predefined as follows, unless otherwise stated: bandwidth $B = 20$MHz, $d_{Ox} = 100$m, source transmit power $\bar{P}_S = 23$dBm, destination transmit power budget $P_D = 23$dBm, public message quality of service $\bar{r}_{P,D} = 0.1$bps/Hz, mean noise power at the warden node $\bar{\sigma}_W^2 = -160$dBm/Hz, noise uncertainty bound $\zeta = 5$dB, noise power at the destination node and hidden receiver $\bar{\sigma}_D^2 = \bar{\sigma}_R^2 = -160$dBm/Hz, residual self-interference $\bar{\sigma}_{SI}^2 = -160$dB, minimum DEP threshold $\varepsilon = 0.45$, path loss exponent $b = 3.5$ and covert transmission probability $p = 0.5$.

Fig. 10 illustrates how the worst-case DEP changes with the source transmit power P_S. Since it is necessary for the destination transmit power P_D to be significantly lower than P_S to ensure covertness, we compare the optimal solution with fixed power schemes "α% P_S" in which P_D is set to min ($\alpha\%P_S$, $\bar{P}_D$). Putting greater P_D to a covert transmission results in a worse-case DEP percentage when P_S is low, but implementing less P_D is recommended when P_S is high, while less P_D is preferred when P_S is high. First, the public data rate limitations in (25b) and (25c) predominate over the final P_D^* expression (28) while P_S is low. If $\nu \triangleq \min\left(E\left[\frac{|h_{SR}|^2}{|h_{DR}|^2(2^{\bar{r}_P}-1)}\right], E\left[\frac{|h_{SD}|^2}{|\tilde{h}_{DD}|^2(\bar{r}_P-1)}\right]\right)$ "α%P_S" schemes with $\alpha\% > \nu$ are likely to be infeasible on average. From Fig. 10, one can deduce that $\nu \geq 5\%$ for our system configuration because "5%P_S" works the greatest fixed P_D scheme out of all of them. Conversely, when P_S is high, P_D^* is mostly determined by the power budget $\bar{P}_D$. Therefore, only the "α%P_S" schemes that may satisfy these require-

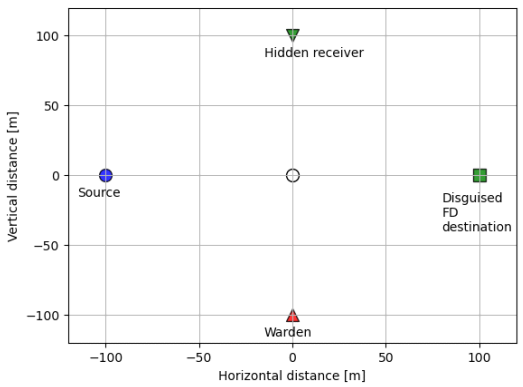

Fig. 9. Node placements

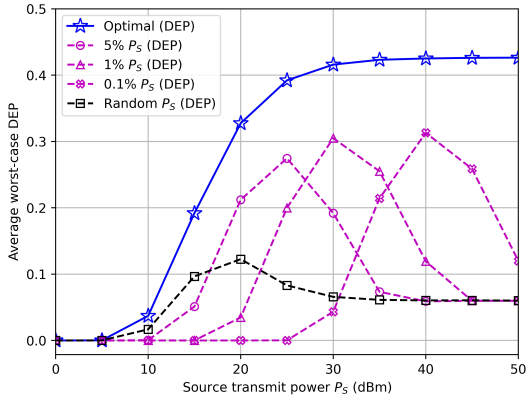

Fig. 10. Worst-case DEP versus source power

ments and be generally feasible are those with a low enough α%. This explains the reason why "0.1%P_S" overtakes those with higher α% in Fig. 10 in the high P_S region. The figure also indicates that the proposed strategy, incorporating the public data rate optimization from equation (26) and the destination transmit power optimization from equation (28), consistently yields the highest worst-case DEP rate across various P_S values. This underscores the critical importance of optimizing both r_P and P_D.

Fig. 11 presents the average worst-case DEP with changes in the covert rate threshold $\bar{r}_C$. It is evident that the worst-case DEP exhibits a monotonically decreasing trend as the guaranteed covet rate increases. This observation stems from the fact that higher $\bar{r}_C$ requires higher transmit power P_D which, in turn, decreases the DEP since DEP is decreasing function of P_D . In terms of average worst-case DEP, it is evident that "5%P_S " and random P_D schemes outperform the other fixed powerschemes. To maintain the covert rate, a certain minimum power P_D must be provided. As the covert rate increases, higher P_D is required, and this explains why "5%P_S " scheme exhibits higher DEP than the other fixed power strategies.

Fig. 12 illustrates the average worst-case DEP for different minimum quality of services for public message $\bar{r}_P$. The average worst-case DEP decline in monotonic manner as $\bar{r}_P$ increases as expected.

Fig. 13 shows the average worst-case DEP for different destination transmits power budget $\bar{P}_D$. Notably, when $\bar{P}_D$ is low, both the "5%P_S" and random P_D

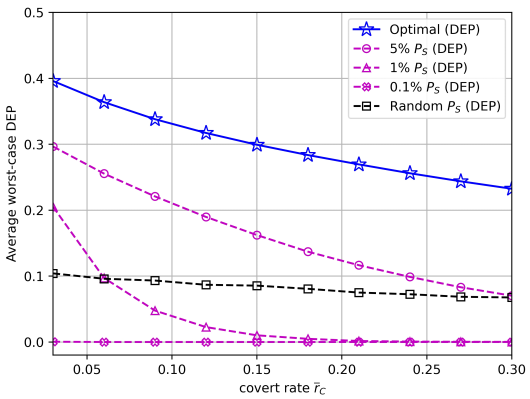

Fig. 11. DEP versus covert rate

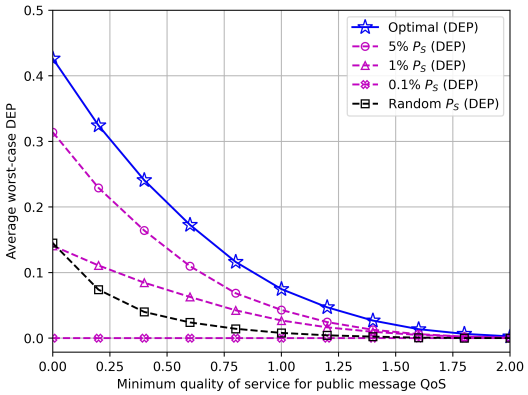

Fig. 12. DEP versus minimum quality of service for public message QoS

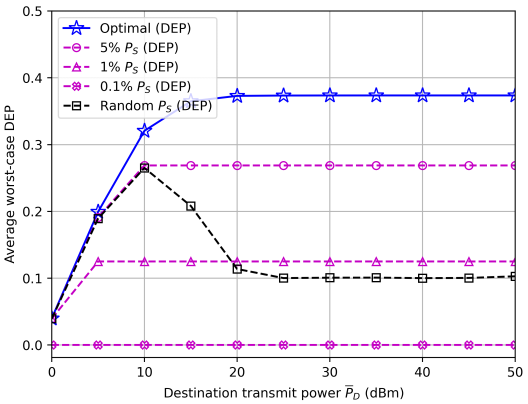

Fig. 13. DEP versus destination transmit power budget

schemes demonstrate performance close to the optimal scheme. This closeness in performance arises because P_D^* is dominantly determined by $\bar{P}_D$ from (28), and the P_D of the compared schemes with fixed or randomly chosen P_D converges to $\bar{P}_D$. This figure also clarifies that increasing $\bar{P}_D$ cannot further improve DEP because it does not affect P_D^* in (28). As a result, the DEP saturates beyond a certain $\bar{P}_D$ in the figure. We would also like to highlight that our proposed solution consistently achieves the highest worst-case DEP once again underscores the importance of optimizing both r_P and P_D

Fig. 14 represents how the worst-case DEP changes when covert transmission probability p veries and it is monotonically decreasing with respect of p increasing implying that the more the disguised FD node transmits, the more probable the warden will detect it.

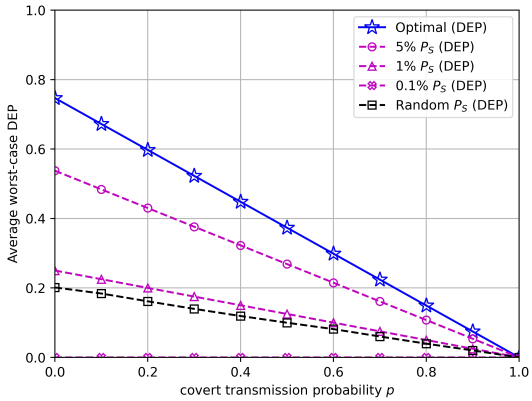

Fig. 14. DEP versus covert trasmission probability p

Ⅵ. Conclusion

In this study, we explored a covert communication setup where a source node communicates with a FD destination node. Despite appearing as a receiver-only node, the destination secretly transmits crucial messages to a hidden receiver while evading detection by a monitoring warden node. Our focus was on determining the optimal public data rate and transmit power for the FD destination node, aiming to maximize the worscase DEP at the warden node. In some situations, the upper bound might fall below the lower bound. When such cases arise, the transmit power P_D can be set to 0 as a strategy to avoid detection.

When the connection between the destination and the receiver is particularly strong, the best transmit power for the destination node tends to decrease toward zero. This is because the hidden receiver struggles to properly filter out the source messages before receiving the covert messages. In this scenario, the hidden receiver might opt to decode the covert message directly, bypassing the need to first decode and subtract the public message.

Similarly, if self-interference is not sufficiently suppressed, the optimal transmit power will also be low, as the public data rate cannot sustain the necessary quality of service.

Moreover, when the channel gain between the destination and the warden node is considerably high, the optimal transmit power for the destination node also trends toward zero. This is because the warden node can more easily detect the covert communication due to the significant power difference.

References

[1] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, “A comprehensive review of the covid-19 pandemic and the role of Iot, drones, ai, blockchain, and 5g in managing its impact,” *IEEE Access*, vol. 8, pp. 90225-90265, 2020. (http://dx.doi.org/10.1109/ACCESS.2020.2992341)

[2] S. Revathi, A. Shrivastava, A. Yussupova, A. N. Hidayatulloh, D. Saltanat, and A. Mishra, “Role of wireless communications in digital economy in the present context,” in *2022 6th Int. Conf. Trends in Electr. and Inf.* (*ICOEI*), pp. 703-709, 2022. (http://dx.doi.org/10.1109/ICOEI53556.2022.9777115)

[3] J. Zhang, Z. Yan, S. Fei, M. Wang, T. Li, and H. Wang, “Is today’s end-to-end communication security enough for 5g and its beyond?” *IEEE Netw.*, vol. 36, no. 1, pp. 105-112, 2022. (http://dx.doi.org/10.1109/MNET.101.2100189)

[4] B. A. Forouzan, *Cryptography and Netw. Security,* New York, NY, USA: McGraw-Hill, 2007.

[5] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, “Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286-8297, 2016. (http://dx.doi.org/10.1109/TWC.2016.2613860)

[6] H.-M. Wang, B.-Q. Zhao, and T.-X. Zheng, “Adaptive full-duplex jamming receiver for secure d2d links in random networks,” *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254-1267, 2019. (http://dx.doi.org/10.1109/TCOMM.2018.2880216)

[7] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, “Covert

communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193-6206, 2017. (http://dx.doi.org/10.1109/TWC.2017.2720736)

[8] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26-31, 2015. (http://dx.doi.org/10.1109/MCOM.2015.7355562)

[9] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 813-816, 2019. (http://dx.doi.org/10.1109/LWC.2019.2894617)

[10] T. Xu, L. Xu, X. Liu, and Z. Lu, "Covert communication with a full-duplex receiver based on channel distribution information," in *2018 12th Int. Symp. Ant., Propag. and EM Theory* (*ISAPE*), pp. 1-4, 2018. (http://dx.doi.org/10.1109/ISAPE.2018.8634312)

[11] Y. Zhao, Z. Li, N. Cheng, D. Wang, W. Quan, and X. Shen, "Joint power and position optimization for the full-duplex receiver in covert communication," in *ICC 2020-2020*, pp. 1-6, 2020. (http://dx.doi.org/10.1109/ICC40277.2020.9148663)

[12] J. Moon, "Covert communications in a compress-and-forward relay system," *ICT Express*, vol. 10, no. 2, pp. 412-417, ISSN: 2405-9595, Apr. 2024. (http://dx.doi.org/10.1016/j.icte.2023.08.005)

[13] Y. Li, R. Zhao, Y. Deng, F. Shu, Z. Nie, and A. H. Aghvami, "Harvest-and-opportunistically-relay: Analyses on transmission outage and covertness," *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 7779-7795, 2020. (http://dx.doi.org/10.1109/TWC.2020.3015816)

[14] E. Björnson and L. Sanguinetti, "Power scaling laws and near-field behaviors of massive mimo and intelligent reflecting surfaces," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1306-1324, 2020. (http://dx.doi.org/10.1109/OJCOMS.2020.3020925)

[15] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678-1690, 2014. (http://dx.doi.org/10.1109/TVT.2013.2285244)

[16] Y. Wang, S. Yan, W. Yang, C. Zhong, and D. W. K. Ng, "Probabilistic accumulate-then-transmit in wireless-powered covert communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 12, pp. 10393-10406, 2022. (http://dx.doi.org/10.1109/TWC.2022.3183892)

[17] S. Feng, X. Lu, S. Sun, and D. Niyato, "Meanfield artificial noise assistance and uplink power control in covert Iot systems," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7358-7373, 2022. (http://dx.doi.org/10.1109/TWC.2022.3157885)

[18] J. Liu, J. Yu, X. Chen, R. Zhang, S. Wang, and J. An, "Covert communication in ambient backscatter systems with uncontrollable rf source," *IEEE Trans Commun.*, vol. 70, no. 3, pp. 1971-1983, 2022. (http://dx.doi.org/10.1109/TCOMM.2022.3144447)

[19] Z. Wu, K. Guo, and S. Zhu, "Covert communication for integrated satellite-terrestrial relay networks with cooperative jamming," *Electr.*, vol. 12, p. 999, Feb. 2023. (http://dx.doi.org/10.3390/electronics12040999)

[20] S. Zhang and R. Zhang, "Capacity characterization for intelligent reflecting surface aided mimo communication," *IEEE J. Sel. Areas in Commun.*, vol. 38, no. 8, pp. 1823-1838, 2020. (http://dx.doi.org/10.1109/JSAC.2020.3000814)

[21] J. Si, Z. Li, Y. Zhao, et al., "Covert transmission assisted by intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394-5408, 2021.

(http://dx.doi.org/10.1109/TCOMM.2021.3082779)

[22] C. Wang, Z. Li, J. Shi, and D. W. K. Ng, "Intelligent reflecting surface-assisted multi-antenna covert communications: Joint active and passive beamforming optimization," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3984-4000, 2021. (http://dx.doi.org/10.1109/TCOMM.2021.3062376)

[23] C. Wang, Z. Li, T.-X. Zheng, D. W. K. Ng, and N. Al-Dhahir, "Intelligent reflecting surface-aided full-duplex covert communications: Information freshness optimization," *IEEE Trans. Wireless Commun.*, vol. 22, no. 5, pp. 3246-3263, 2023. (http://dx.doi.org/10.1109/TWC.2022.3217041)

[24] X. Xu, L. Hu, S. Wei, et al., *On Irsassisted Covert Communication with a Friendly UAV*, May 2023. (http://dx.doi.org/10.20944/preprints202305.2156.v1)

[25] X. Jiang, X. Chen, J. Tang, et al., "Covert communication in UAV-assisted air-ground networks," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 190-197, 2021. (http://dx.doi.org/10.1109/MWC.001.2000454)

[26] X. Zhou, S. Yan, F. Shu, R. Chen, and J. Li, "Uav-enabled covert wireless data collection," *IEEE J. Sel. Areas in Commun.*, vol. 39, no. 11, pp. 3348-3362, 2021. (http://dx.doi.org/10.1109/JSAC.2021.3088688)

[27] M. Li, X. Tao, H. Wu, and N. Li, "Joint trajectory and resource optimization for covert communication in UAV-enabled relaying systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5518-5523, 2023. (http://dx.doi.org/10.1109/TVT.2022.3225508)

[28] R. Chen, J. Shi, L. Yang, et al., "Performance analysis for user scheduling in covert cognitive radio networks," in *2020 IEEE 31st Annual Int. Symp. Personal, Indoor and Mobile Radio Commun.*, pp. 1-6, 2020. (http://dx.doi.org/10.1109/PIMRC48278.2020.9217377)

[29] X. Liao, J. Si, J. Shi, Z. Li, and H. Ding, "Generative adversarial network assisted power allocation for cooperative cognitive covert communication system," *IEEE Commun. Lett.*, vol. 24, no. 7, pp. 1463-1467, 2020. (http://dx.doi.org/10.1109/LCOMM.2020.2988384)

[30] Y. Wen, L. Liu, J. Li, et al., "A covert jamming scheme against an intelligent eavesdropper in cooperative cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13243-13254, 2023. (http://dx.doi.org/1109/TVT.2023.3277457)

[31] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "Covertness and secrecy study in untrusted relay-assisted d2d networks," *IEEE Int. Things J.*, vol. 10, no. 1, pp. 17-30, 2023. (http://dx.doi.org/10.1109/JIOT.2022.3201021)

[32] J. Moon, "Disguised full-duplex covert communications," *Sensors*, vol. 23, p. 6515, Jul. 2023. (http://dx.doi.org/10.3390/s23146515)

[33] S. W. Kim and H. Q. Ta, "Covert communications over multiple overt channels," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1112-1124, 2022. (http://dx.doi.org/10.1109/TCOMM.2021.3127532)

[34] T. M. Cover and J. A. Thomas, *Elements of Information Theory,* New Jersey, NJ, USA: John Wiley & Sons, Inc., 2005.

[35] 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, 2017. (http://dx.doi.org/10.1109/LCOMM.2016.2647716)

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

[37] 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, 2019.
(http://dx.doi.org/10.1109/TWC.2019.2918452)

Refat Khan

2019-2020 : Software Developer, SP Wave, Dhaka, 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 Uni- versity, the Republic of Korea

<Research Interest> Wireless Network Security, Machine/ Deep Learning, Natural Language Process- ing(NLP), Data/Text Mining.

[ORCID:0009-0000-4934-6270]

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 surveil- lance, covert communications, and machine learning for wireless communications.

[ORCID:0000-0002-9812-7768]