https://doi.org/10.7840/kics.2023.48.11.1365

The Channel Uncertainty of Warden on Disguised Full-Duplex Covert Communications

Jihwan Moon◆°

ABSTRACT

In this paper, we investigate a covert communications system that consists of a source node communicating with a disguised full-duplex (FD) destination node. Supposedly receive-only, the destination node covertly transmits confidential messages to a hidden receiver while avoiding the surveillance of a warden node. Our specific focus is on the impact of the channel uncertainty of the warden node from the perspective of the destination node on covert communications. We take the expected minimum detection error probability (DEP) at the warden node into consideration and obtain the optimal public data rate and transmit power to maximize the covert rate. Numerical results verify that the covert rate increases as the availability of the channel state information (CSI) improves and highlight the importance of optimization regardless of the level of CSI based on comparisons with baseline schemes.

Key Words : Physical layer security, covert communications, low probability of detection, full duplex, channel uncertainty.

Ⅰ. Introduction

Cryptography has long been applied to a variety of communications systems to protect critical information from adversaries[1]. Limitations such as high complexity of secret key generation and vulnerability to eavesdroppers with higher computational ability, however, motivated security engineers to consider the possibility of utilizing physical layer security[2]. This technology blocks a wireless link from legitimate entities to eavesdroppers by beamforming with multiple antennas, or by broadcasting artificial noise (AN)[3] without the need of sharing secret keys and avoiding high-powered eavesdroppers.

Meanwhile, many applications nowadays, e.g., reconnaissance operation and bank transactions, require even more secure transmissions such that any unauthorized entities cannot recognize the existence of such *covert communications* or *low-probability-of-detection* communications[4].

Covert communications for full-duplex (FD) systems has been investigated in depth by a number of past works, ranging from a fundamental system including a covert transmitter, an FD receiver that simultaneously emits AN to a warden node[5-7] to more complex configurations such as FD relays[8,9], time-division multiple access (TDMA)[10], integrated satellite-terrestrial communications[11], intelligent reflecting surface (IRS) systems[12-15], unmanned aerial

※ 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 work was partially supported by Korea Research Institute for defense Technology planning and advancement(KRIT) grant funded by the Korea government(DAPA(Defense Acquisition Program Administration)) (21-106-A00-007, Space-Layer Intelligent Communication Network Laboratory, 2022).
This research was partially supported by the research fund of Hanbat National University in 2022.
◆° First and Corresponding Author : Hanbat National University, Department of Mobile Convergence Engineering; anschino@staff.hanbat.ac.kr, 정회원
논문번호 : 202308-056-A-RU, Received August 22, 2023; Revised August 28, 2023; Accepted August 28, 2023

vehicle (UAV) based covert transmissions[16-19], and Internet-of-Things (IoT)[20,21].

It is worth noting that many past works have assumed that monitoring nodes are perfectly aware of the hardware specifications of covert communications devices. However, the covert nodes may disguise themselves as other functional entities to increase confusion at the monitoring nodes.Our previous work[22] first addressed such a scenario where an originally FD node that secretly transmits confidential messages disguises itself as a receive-only HD node under the assumption of perfect channel state information (CSI) at every node.

In this paper, we focus on the impact of the channel uncertainty of the warden node from the perspective of the destination node on covert communications in the system model developed by [22]. We take the expected minimum detection error probability (DEP) at the warden node into consideration and obtain the optimal public data rate and transmit power to maximize the covert rate. Numerical results verify that the covert rate increases as the availability of the CSI improves and highlight the importance of optimization regardless of the level of CSI based on comparisons with baseline schemes.

Ⅱ. System Model

2.1 Received Signals

Fig. 1 [22] depicts our considered system model where the source node S delivers a public message to the destination node D. At the same time, the seemingly receive-only destination node carries out a covert transmission through an unseen antenna to the hidden receiver R in FD while the warden node W surveils any suspicious communications links.

The received signal at the disguised FD destination node can be written as

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

Here, $x_P \sim \mathcal{CN}(0,1)$ and $x_C \sim \mathcal{CN}(0,1)$ specify the public and covert messages, respectively, P_D and P_S stand for the transmit power at the destination node and source node, respectively, $\tilde{h}_{DD} \sim \mathcal{CN}(0,\sigma_{\mathrm{SI}}^2)$

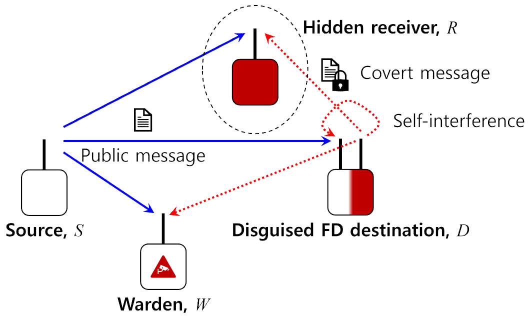

Fig. 1. System model [22]

denotes the residual self-interference channel after self-interference cancellation, and $z_X \sim \mathcal{CN}(0,\sigma_X^2)$ means the additive noise at node X.

The distance-dependent channel model is adopted for the channel coefficient h_{XY} between node X and Y for X, Y $\in \{S,D,R,W\}$[23]. To be specific, we let $|h_{XY}|^2 = L_{XY}|\hat{h}_{XY}|^2$, where $L_{XY} \triangleq L_0(d_{XY}/d_0)^{-\beta}$ denotes the path loss between X and Y. The pathloss is denoted by L_0 at a reference distance d_0 =1 m, β signifies the path loss exponent, and d_{XY} represents the distance between X and Y. Moreover, the small-scale channel variable $\hat{h}_{XY}$ follows $\mathcal{CN}(0,1)$.

We assume in this work that the destination node has access to the CSI of the source node h_{SD} since the covert communications occurs during ordinary S-D communications. The hidden receiver is also able to readily estimate the CSI of the destination and source nodes, h_{DR} and h_{SR} , during channel estimation if pilot sequences are informed by the destination node in advance.

On the other hand, different from the previous work[22], we consider the channel uncertainty of the warden node from the perspective of the destination node. The D-W channel can be modelled as [24]

$$h_{DW} = \sqrt{\rho}\bar{h}_{DW} + \sqrt{1-\rho}\tilde{h}_{DW}, \quad (2)$$

in which h_{DW}, $\bar{h}_{DW}$ and $\tilde{h}_{DW} \sim \mathcal{CN}(0, L_{DW})$ represent the ground-truth channel, estimated channel and estimation error, respectively, with $\rho \in [0, 1]$ denoting the level of estimation correctness. That is, $\rho = 1$ means the channel is perfectly estimated by the covert communication party, while $\rho = 0$ indicates that only the channel distribution information (CDI) is available.

By an adaptive transmission policy at the source node, the public data rate $r_{P,D}$ is controlled with the feedback from the destination node. Accordingly, the achievable public data rate $\bar{r}_{P,D}$ is calculated as [25]

$$\bar{r}_{P,D} = \log_2\left(1+\frac{|h_{SD}|^2 P_S}{|\tilde{h}_{DD}|^2 P_D + \sigma_D^2}\right). \quad (3)$$

As for the hidden receiver, both a direct-link public message from the source node and a covert message from the destination node are received as

$$y_R = h_{SR}\sqrt{P_S}x_P + h_{DR}\sqrt{P_D}x_C + z_R. \quad (4)$$

The hidden receiver then decodes and eliminate public messages in prior to recovering covert messages. For successful decoding of public messages, it is required that the public data rate be limited by its achievable amount $\bar{r}_{P,R}$ as

$$\bar{r}_{P,R} = \log_2\left(1+\frac{|h_{SR}|^2 P_S}{|h_{DR}|^2 P_D + \sigma_R^2}\right). \quad (5)$$

Therefore, the achievable covert rate after removing x_P from y_R is expressed by

$$r_{C,R} = \log_2\left(1+\frac{|h_{DR}|^2 P_D}{\sigma_R^2}\right). \quad (6)$$

2.2 Covert Message Detection

During communications, the warden node receives

$$y_W = h_{SW}\sqrt{P_S}x_P + h_{DW}\sqrt{P_D}x_C + z_W. \quad (7)$$

In this work, we take a conservative assumption from the perspective of the covert communications party that the warden node is assumed to perfectly know necessary parameters such as h_{SW}, h_{WD} and P_S. Upon this worst-case presumption, the warden node first removes public messages from y_W and obtain the effective residual signal $\tilde{z}_W \triangleq y_W - h_{SW}\sqrt{P_S}x_P$z. We then have null and alternative hypotheses as

$$\begin{aligned} H_0 &: \quad \tilde{z}_W = z_W, \\ H_1 &: \quad \tilde{z}_W = h_{DW}\sqrt{P_D}x_C + z_W. \end{aligned} \quad (8)$$

The null hypothesis H_0 represents an event that a covert message is not transmitted, and the alternative hypothesis H_1 indicates the other event where the disguised FD destination node sent a covert message. Using a radiometer[26] as a detection measure, the sufficient test statistic T for (8) after observing N $\rightarrow \infty$ number of transmissions becomes $\mathrm{E}[|\tilde{z}_W|^2]$ as [27]

$$\begin{aligned} H_0 &: \quad T = \sigma_W^2, \\ H_1 &: \quad T = |h_{DW}|^2 P_D + \sigma_W^2. \end{aligned} \quad (9)$$

The warden node decides that a covert link exists if $T \geq \tau$ and otherwise when $T < \tau$ for some threshold τ.

We consider the noise uncertainty on σ_W^2 at the warden node as in [26] and [28]. Hence, $\sigma_{W,\mathrm{dB}}^2 \sim U(\bar{\sigma}_{W,\mathrm{dB}}^2 - \zeta_{\mathrm{dB}}, \bar{\sigma}_{W,\mathrm{dB}}^2 + \zeta_{\mathrm{dB}})$ in decibel scale with $\bar{\sigma}_{W,\mathrm{dB}}^2$ and $\zeta_{\mathrm{dB}} \geq 0$ representing the mean and maximum range, respectively. The resulting DEP $\Pr(\mathrm{e})$ is then calculated by summing the miss detection and false alarm probabilities as

$$\Pr(\mathrm{e}) = \underbrace{\Pr(T \geq \tau | H_0)}_{\text{False alarm}} \Pr(H_0) + \underbrace{\Pr(T < \tau | H_1)}_{\text{Miss}} \Pr(H_1), \quad (10)$$

with random covert transmission as $\Pr(H_0) = \Pr(H_1) = 0.5$[29].

The optimal τ that minimizes the DEP is obtained from [22] as

$$\tau^\star = |h_{DW}|^2 P_D + \frac{\bar{\sigma}_W^2}{\zeta}. \quad (11)$$

and the corresponding minimum DEP is also derived from [22] as

$$\Pr(\mathrm{e})|_{\tau=\tau^\star} = \frac{1}{2}\left(1-\frac{1}{2\ln\zeta}\left(\ln\frac{\tau^\star}{\tau^\star - |h_{DW}|^2 P_D}\right)\right), \quad (12)$$

as long as $\zeta\bar{\sigma}_W^2 \geq |h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta$. Note that (12) provides the worst-case minimum DEP assuming that the warden node knows the exact value of P_D.

Ⅲ. Problem Formulation

In this work, we aim to optimize the transmit power of the FD destination node and public data rate in the presence of the channel uncertainty on h_{DW} from the destination node point of view. We thus formulate an optimization problem as

$$\text{(P1)}: \max_{P_D, r_P} \; r_{C,R}, \tag{13a}$$
$$\text{subject to: } r_P \leq \bar{r}_{P,R}, \tag{13b}$$
$$r_P \leq \bar{r}_{P,D}, \tag{13c}$$
$$r_P \geq \bar{r}_P, \tag{13d}$$
$$\mathrm{E}_{h_{DW}}\left[\Pr(\mathrm{e}|h_{DW})|_{\tau=\tau^\star}\right] \geq \varepsilon, \tag{13e}$$
$$\zeta\bar{\sigma}_W^2 \geq |h_{DW}|^2 P_D + \frac{\bar{\sigma}_W^2}{\zeta}, \tag{13f}$$
$$0 \leq P_D \leq \bar{P}_D. \tag{13g}$$

Constraint (13b) ensures that the hidden receiver successfully decodes and removes a public message to retrieve a covert message, and (13c) sets an upper bound on the public data rate to which the destination node can tolerate. A restraint on the minimum quality of service $\bar{r}_P$ for the public message delivery is included in (13d). Also, (13e) and (13f) guarantee a non-zero expected minimum DEP for $0 \leq \varepsilon \leq 0.5$ with respect to the imperfectly estimated channel h_{DW}. (13g) in the end adds the power budget $\bar{P}_D$ at the disguised FD destination node.

Ⅳ. Proposed Solutions

First, it can be easily shown that (13e) automatically fulfills (13f) such that (13f) can be omitted from (P1). Next, expanding (13e) results in

$$\frac{1}{2}\left(1-\frac{1}{2\ln\zeta}\left(\mathrm{E}_{h_{DW}}\left[\ln\left(|h_{DW}|^2 P_D+\frac{\bar{\sigma}_W^2}{\zeta}\right)\right]-\ln\frac{\bar{\sigma}_W^2}{\zeta}\right)\right), \tag{14}$$

in which $|h_{DW}|^2$ inside the expectation can further be expressed as

$$\rho\left|\bar{h}_{DW}\right|^2+2\mathrm{Re}\left\{\sqrt{\rho(1-\rho)}\bar{h}_{DW}\tilde{h}_{DW}^*\right\}+(1-\rho)\left|\tilde{h}_{DW}\right|^2. \tag{15}$$

It is analytically intractable to find the exact expectation of the logarithm of terms involving the random channel estimation error variables $\tilde{h}_{DW}^*$ and $\left|\tilde{h}_{DW}\right|^2$ in (15). In the mean time, Jensen's inequality[25] by noting the concavity of the logarithm reveals that

$$\begin{aligned}&\mathrm{E}_{h_{DW}}\left[\ln\left(|h_{DW}|^2 P_D+\frac{\bar{\sigma}_W^2}{\zeta}\right)\right]\\ &\leq \ln\left(\mathrm{E}_{h_{DW}}\left[|h_{DW}|^2 P_D+\frac{\bar{\sigma}_W^2}{\zeta}\right]\right)\\ &= \ln\left(\left(\rho\left|\bar{h}_{DW}\right|^2+(1-\rho)L_{DW}\right)P_D+\frac{\bar{\sigma}_W^2}{\zeta}\right).\end{aligned} \tag{16}$$

This leads to a lower bound of the expected minimum DEP in (13e) as

$$\begin{aligned}&\mathrm{E}_{h_{DW}}\left[\Pr(\mathrm{e}|h_{DW})|_{\tau=\tau^\star}\right]\\ &\geq \frac{1}{2}\left(1-\frac{1}{2\ln\zeta}\left(\ln\frac{\left(\rho\left|\bar{h}_{DW}\right|^2+(1-\rho)L_{DW}\right)P_D\zeta+\bar{\sigma}_W^2}{\bar{\sigma}_W^2}\right)\right)\end{aligned} \tag{18}$$

Hence, we propose to solve the following alternative problem:

$$\text{(P1.1)}: \max_{P_D, r_P} \; r_{C,R}, \tag{18a}$$
$$\text{subject to: } r_P \leq \bar{r}_{P,R}, \tag{18b}$$
$$r_P \leq \bar{r}_{P,D}, \tag{18c}$$
$$r_P \geq \bar{r}_P, \tag{18d}$$
$$\mathrm{DEP}_{\mathrm{LB}} \geq \varepsilon, \tag{18e}$$
$$0 \leq P_D \leq \bar{P}_D, \tag{18f}$$

where $\mathrm{DEP}_{\mathrm{LB}}$ is the right hand side of (17). We emphasize that satisfying (18e) guarantees (13e) in the original problem (P1).

Now, we note that the covet rate in (18a) is an increasing function of P_D while the upper limits of r_P in (18b) and (18c) are decreasing functions of P_D. This indicates that the covert rate must be less than a value at which one of the upper limits equals to r_P, i.e., $r_P = \min(\bar{r}_{P,R}, \bar{r}_{P,D})$. Thus, the optimal r_P should be set as low as possible for the highest covert rate as

$$r_P^\star = \bar{r}_P. \tag{19}$$

Let us simplify (P1.1) using the monotonicity of logarithms as

$$\text{(P1.2)}: \max_{P_D} P_D, \tag{20a}$$

$$\text{subject to: } P_D \le \frac{1}{|h_{DR}|^2}\left(\frac{|h_{SR}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_R^2\right), \tag{20b}$$

$$P_D \le \frac{1}{|\tilde{h}_{DD}|^2}\left(\frac{|h_{SD}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_D^2\right), \tag{20c}$$

$$P_D \le \left(\zeta^{(1-4\varepsilon)} - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_W^2}{\rho\,|\bar{h}_{DW}|^2 + (1-\rho)L_{DW}}, \tag{20d}$$

$$0 \le P_D \le \bar{P}_D. \tag{20e}$$

As a result, the optimal transmit power becomes the minimum of the upper bounds from (20b)-(20e) as

$$P_D^\star = \min\left\{\frac{1}{|h_{DR}|^2}\left(\frac{|h_{SR}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_R^2\right), \frac{1}{|\tilde{h}_{DD}|^2}\left(\frac{|h_{SD}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_D^2\right), \left(\zeta^{(1-4\varepsilon)} - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_W^2}{\rho\,|\bar{h}_{DW}|^2 + (1-\rho)L_{DW}}, \bar{P}_D\right\}. \tag{21}$$

V. Numerical Results

We evaluate the impact of the channel uncertainty of the warden node on covert communications through numerical results. The four nodes are located with respect to the origin $O = (0,0)$ in a cartesian coordinate system in a way that the coordinates of S, D, R, W are $(-d_{OS}, 0)$, $(d_{OD}, 0)$, $(0, d_{OR})$, $(0, -d_{OW})$, respectively (Fig. 2). Unless otherwise stated, the system parameters are set to as follows: the bandwidth B = 20 MHz, d_{OX} = 100 m, $\forall X$, source transmission power P_S = 23 dBm, destination transmission power budget $\bar{P}_D$ = 23 dBm, quality of service for public messages $\bar{r}_{P,D}$ = 0.1 bps/Hz, mean noise power at the warden node $\bar{\sigma}_W^2$ = -160 dBm/Hz, noise uncertainty bound ζ = 5 dB, noise power at the hidden receiver and destination node $\sigma_R^2 = \sigma_D^2$ = -160 dBm/Hz, residual selfinterference σ_{SI}^2 = -100 dB, minimum DEP threshold ε = 0.45, pathloss exponent β = 3.5, and ρ = 0.75.

Fig. 3 presents the average covert rate $r_{C,R}$ as the source transmit power P_S varies for ρ = 0.75. Noting that the destination transmit power P_D is in general much smaller than P_S to realize covert transmissions, we make a comparison with "α% P_S" where P_D is set to min(α% of P_S, $\bar{P}_D$). We first observe that the optimal public data rate in (19) and destination transmit power in (21) yield the best covert rate for all P_S regime, highlighting the necessity of carefully choosing r_P and P_D. Two additional schemes with the perfect CSI (ρ = 1.0) and without the CSI (ρ = 0.0) are also plotted in the figure, and each of them clearly marks the performance bound. Interestingly, even if only the CDI of the warden node is available at the FD destination node, the optimization leads to higher covert rate compared to the naive power allocation schemes.

Fig. 4 shows the average covert rate $r_{C,R}$ as the channel estimation correctness ρ varies. We can notice that the performance rapidly increases as ρ approaches 1, or equivalently, the perfect CSI of the warden. Also, the covert rate with the perfect CSI is remarkably higher than that without the CSI.

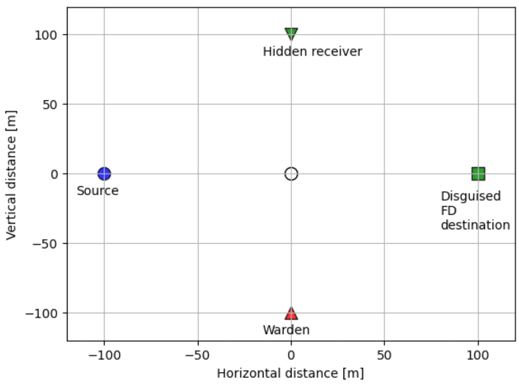

Fig. 2. Node placements

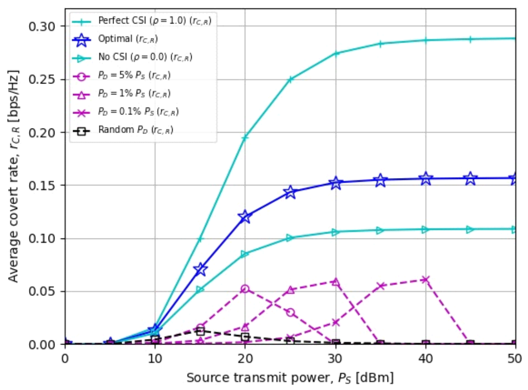

Fig. 3. Average covert rate versus source transmit power with ρ = 0.75

Nevertheless, since considerably imperfect CSI with low ρ still helps providing meaningful covert rate that is higher than the naive power allocation schemes, we can once again recognize the importance of optimizing r_P and P_D.

Fig. 5 provides the average DEP and the obtained lower bound $\mathrm{DEP_{LB}}$ in (17) as the minimum DEP threshold ε varies. It is confirmed that the average DEP is strictly larger than $\mathrm{DEP_{LB}}$ for every scheme in all ε regime. Meanwhile, since the gap between them is relatively small especially when ε is higher, which is a preferred requirement in practice, we may assess the obtained lower bound as a tight approximation. The figure also verifies that the proposed optimal solutions yield a just enough DEP above the threshold ε in general while the other baseline schemes achieve unnecessarily high DEP by

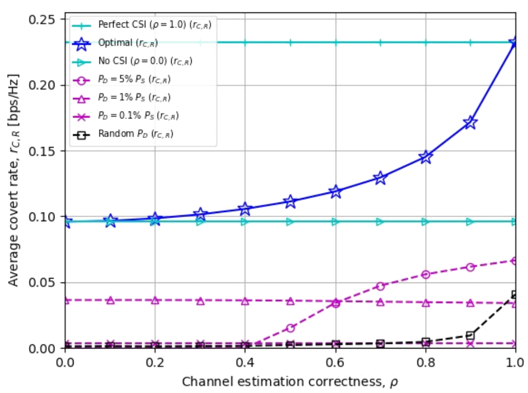

Fig. 4. Average covert rate versus channel estimatino correctness

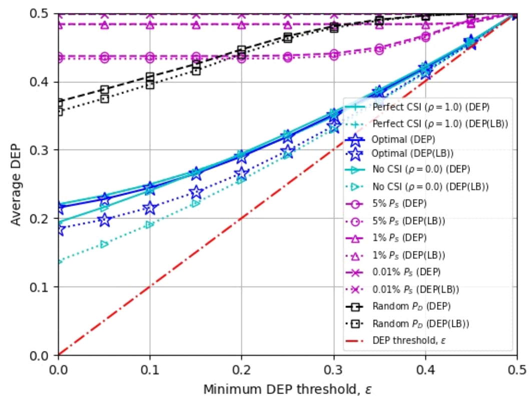

Fig. 5. Average DEP versus minimum DEP threshold with ρ = 0.75

sacrificing the covert rate.

Ⅵ. Conclusion

In this paper, we re-examined a covert communications system that consists of a source node communicating with a disguised FD destination node in [22]. Particularly, we took a step further to study the impact of the channel uncertainty of the warden node from the perspective of the destination node on covert communications. With the imperfect CSI of the warden node, we assumed the FD destination operates based on the expected minimum DEP at the warden node. Since the exact value is difficult to obtain, we made use of its lower bound to solve the covert rate maximization problem. Numerical results confirmed the tightness of the proposed lower bound, and we observed that the covert rate increases as the availability of the CSI improves. Furthermore, the results highlighted the importance of optimization regardless of the level of CSI based on comparisons with baseline schemes.

References

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

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

Oct. 1975. DOI: 10.1002/j.1538-7305.1975.tb02040.x.

[3] P. Angueira, I. Val, J. Montalbán, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 810-838, Secondquarter 2022. (https://doi.org/10.1109/COMST.2022.3148857)

[4] 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, Dec. 2015. (https://doi.org/10.1109/ MCOM.2015.7355562)

[5] 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. (https://doi.org/10.1109/TWC.2018.2878014)

[6] 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* (*IS- APE*), pp. 1-4, Hangzhou, China, Dec. 2018. (https://doi.org/10.1109/ISAPE.2018.8634312)

[7] M. Zheng, A. Hamilton, and C. Ling, "Covert communications with a full-duplex receiver in non-coherent rayleigh fading," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1882-1895, Mar. 2021. (https://doi.org/10.1109/TCOMM.2020.3041353)

[8] 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. (https://doi.org/10.1109/TCOMM.2021.3089694)

[9] 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, Dec. 2020. (https://doi.org/10.1109/TWC.2020.3015816)

[10] J. Moon, "Covert communications in time division multiple access networks," *J. KICS*, vol. 46, no. 9, pp. 1407-1410, 2021. (https://doi.org/10.7840/kics.2021.46.9.1407)

[11] Z. Wu, K. Guo, and S. Zhu, "Covert communication for integrated satellite–terrestrial relay networks with cooperative jamming," *Electronics*, vol. 12, no. 4, p. 999, Feb. 2023. (https://doi.org/10.3390/electronics12040999)

[12] 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, Jun. 2021. (https://doi.org/10.1109/TCOMM.2021.3062376)

[13] S. Pejoski, Z. Hadzi-Velkov, and N. Zlatanov, "Full-duplex covert communications assisted by intelligent reflective surfaces," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 2846-2850, Dec. 2022. (https://doi.org/10.1109/LCOMM.2022.3206962)

[14] M. Wang, Z. Xu, B. Xia, and Y. Guo, "Active intelligent reflecting surface assisted covert communications," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5401-5406, Apr. 2023. (https://doi.org/10.1109/TVT.2022.3224024)

[15] 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, May 2023. (https://doi.org/10.1109/TWC.2022.3217041)

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

[17] Z. Guo, S. Zhao, J. Wang, H. Lit, and Y. Shen, "Optimal location design for uav covert

communications with a full-duplex receiver," in *2022 Int. Conf. Networking and Network Applications* (*NaNA*), pp. 35-40, Urumqi, China, Dec. 2022. (https://doi.org/10.1109/NaNA56854.2022.00014)

[18] R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang, and A. Nallanathan, "Uav relay assisted cooperative jamming for covert communications over rician fading," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7936-7941, Jul. 2022. (https://doi.org/10.1109/TVT.2022.3164051)

[19] 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, Apr. 2023. (https://doi.org/10.1109/TVT.2022.3225508)

[20] 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. 10 393-10 406, Dec. 2022. (https://doi.org/10.1109/TWC.2022.3183892)

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

[22] J. Moon, "Disguised full-duplex covert communications," *Sensors*, vol. 23, no. 14, p. 6515, Jul. 2023. (https://doi.org/10.3390/s23146515)

[23] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3726-3738, Jul. 2019. (https://doi.org/10.1109/TWC.2019.2918452)

[24] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale mimo relaying techniques for physical layer security: Af or df?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135-5146, Sep. 2015. (https://doi.org/10.1109/TWC.2015.2433291)

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

[26] 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. (https://doi.org/10.1109 / LCOMM.2016.2647716)

[27] 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, Sep. 2017. (https://doi.org/10.1109/TWC.2017.2720736)

[28] 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. (https://doi.org/10.1109/TCOMM.2021.3082779)

[29] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in iot systems: Hiding information in interference," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 46-52, Dec. 2018. (https://doi.org/10.1109/MWC.2017.1800070)

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

Sep. 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]