sensors

MDPI

Communication

Disguised Full-Duplex Covert Communications

Jihwan Moon

Department of Mobile Convergence Engineering, Hanbat National University, Daejeon 34158, Republic of Korea; anschino@staff.hanbat.ac.kr

Abstract: Covert communications have arisen as an effective communications security measure that overcomes some of the limitations of cryptography and physical layer security. The main objective is to completely conceal from external devices the very existence of the link for exchanging confidential messages. In this paper, we take a step further and consider a scenario in which a covert communications node disguises itself as another functional entity for even more covertness. To be specific, we study a system where a source node communicates with a seemingly receive-only destination node which, in fact, is full-duplex (FD) and covertly delivers critical messages to another hidden receiver while evading the surveillance. Our aim is to identify the achievable covert rate at the hidden receiver by optimizing the public data rate and the transmit power of the FD destination node subject to the worst-case detection error probability (DEP) of the warden. Closed-form solutions are provided, and we investigate the effects of various system parameters on the covert rate through numerical results, one of which reveals that applying more (less) destination transmit power achieves a higher covert rate when the source transmit power is low (high). Since our work provides a performance guideline from the information-theoretic point of view, we conclude this paper with a discussion on possible future research such as analyses with practical modulations and imperfect channel state information.

Keywords: physical layer security; covert communications; low probability of detection; full duplex; covert rate; detection error probability

Citation: Moon, J. Disguised Full-Duplex Covert Communications. *Sensors* **2023**, *23*, 6515. https://doi.org/10.3390/s23146515

Academic Editor: Peter Chong

Received: 25 May 2023
Revised: 27 June 2023
Accepted: 12 July 2023
Published: 19 July 2023

1. Introduction

Wireless technology has revolutionized the way people live in various ways [1]. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage [2]. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys [3]. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security [4]. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) [5]. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Still, some applications require an even more strict level of confidentiality. A reconnaissance troop would require reporting its surroundings to the operation center without being detected by enemies in the middle of a military mission [6], or closed networks in security facilities need to make sure that any classified information over the air is concealed from any external party. An adequate technology for such situations is *covert communications* or *low-probability-of-detection* communications that hide the existence of a critical communications link [7].

Covert communications have also been extensively studied for full-duplex (FD) systems. A basic three-node system with a covert transmitter and an FD receiver that simulta-

neously emits AN was studied in [8]. The authors of [9,10] further treated specific channel properties where only channel distribution information of the transmitter-warden link is available, and where every link is non-coherent with channel distribution information for slow or fast fading, respectively. An antenna selection at the receiver was studied in [11], and a transmission time selection and power control strategy were presented by [12] based on channel state information (CSI). The authors in [13] also verified the effectiveness of a truncated channel inversion power control that ceases covert transmission when the channel of the transmitter–receiver is low. A delay-constrained covert communications with a fixed AN power was investigated in [14], and joint AN power and receiver position optimization problems were discussed in [15,16]. Uncertain locations of a warden node were also taken into consideration in [17]. On top of the AN, a random covert channel selection by the transmitter was studied in [18] to aggravate the confusion of the warden. The maximum detection error probability (DEP) subject to the age of information constraint was identified by [19].

As for more complex FD systems, an FD amplify-and-forward (AF) relay was considered by [20], and the authors in [21] designed an energy harvesting FD decode-and-forward (DF) relay-based covert communications protocol in which the relay forwards and harvests energy simultaneously. Moreover, for integrated satellite–terrestrial communications, an FD relay-aided covert communications from a satellite to a ground node was explored in [22].

For intelligent reflecting surface (IRS)-aided covert communications, a transmit beamforming vector and the reflecting coefficients are jointly optimized when an FD receiver broadcasts random AN to confuse the warden in [23]. An uplink covert communications with the aid of an IRS was also investigated by [24]. Utilizing an active IRS, which is naturally FD, for covert communications between a pair of users was discussed in [25]. The age of information was minimized in [26] when a receiver covertly transmits confidential messages to the transmitter, shielded under public transmissions from the transmitter to the receiver with the aid of an IRS.

For an FD unmanned aerial vehicle (UAV) that collects data from a scheduled user and interferes with unscheduled users with AN, the maximum lowest average covert rate was obtained in [27]. In [28], the location of a covert transmitter UAV was optimized with the help of an FD ground receiver that confuses the warden, and in [29], covert communications with a hovering FD UAV relay assuming Rician air–ground channel was studied. The authors of [30] considered an FD DF UAV relay to aid in covert communications where multiple sensors deliver messages to a remote base station in orthogonal time slots.

Moreover, in a cognitive radio system, covert communications between secondary users in the presence of FD eavesdroppers that interfere with the secondary receiver with AN were examined by [31]. The work in [32] studied covert rate maximization with a half-duplex (HD)/FD mode switching device-to-device (D2D) covert receiver in the presence of an uplink spectrum-sharing cellular network. Both secrecy and covert rates were optimized when an untrusted FD AF relay delivers the covert message to an FD base station that emits AN to the warden in [33].

In the IoT environment, the authors of [34] studied a covert transmitter with an optimized transmission probability, which is wirelessly charged by the AN from an FD receiver. Furthermore, covert uplink transmissions of devices towards FD IoT gateways were optimized based on the mean-field Stackelberg game approach in [35]. With an ambient backscatter system, a radio frequency tag modulates an ambient signal into a covert signal for an FD receiver that concurrently broadcasts AN [36].

Most of past works have assumed that the surveillance nodes have a perfect knowledge of the hardware specifications of covert nodes. However, the covert nodes could disguise themselves as other functional entities for even more covertness. For instance, an original FD node that secretly transmits confidential messages may disguise itself as a receive-only HD node. To the best of the author's knowledge, there are not enough studies on covert communications that consider such disguised tactics.

In this paper, we study a covert communications system where a source node communicates with a disguised FD destination node. Supposedly receive-only, the destination node covertly delivers critical messages with an invisible extra antenna to another hidden receiver while evading the surveillance of a warden node as much as possible. We identify the optimal public data rate and the transmit power of the FD destination node that maximizes the covert rate at the hidden receiver. Closed-form solutions are provided, and we investigate the effects of various system parameters on the covert rate through numerical results.

Our main contributions are summarized as follows:

- Different from past works which assume that the surveillance party is confident of the hardware specifications of covert nodes, we take a step further and consider a practical scenario in which a covert communications node disguises itself as another functional entity for even more covertness.
- The worst-case DEP is derived in the presence of noise uncertainty at the warden node.
- Noting that covert communications typically suffer from a low data rate due to the stringent DEP requirements, we focus on maximizing the covert rate at the hidden receiver by optimizing the public data rate and the transmit power of the FD destination node subject to the worst-case DEP of the warden.
- We investigate the effects of various system parameters on the covert rate through numerical results, one of which reveals that applying more (less) destination transmit power achieves a higher covert rate when the source transmit power is low (high).
- Since our work provides a performance guideline from the information-theoretic point of view, we suggest analyses with practical modulations and imperfect CSI as valuable future research topics.

2. System Model

2.1. Received Signals

Figure 1 illustrates the considered system model where the source node S sends a public message to the destination node D. In the meantime, the seemingly receive-only destination node executes a covert transmission via an invisible extra antenna to the hidden receiver R in an FD manner when the warden node W keeps monitoring the existence of any such unexpected communications.

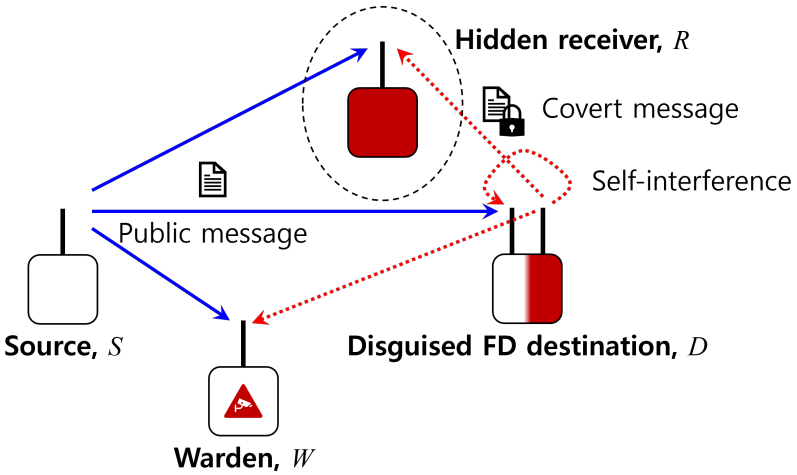

Figure 1. System model.

First, the received signal at the disguised FD destination node is expressed by

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

where h_{XY} stands for the channel coefficient between node X and Y for $X, Y \in \{S, D, R, W\}$, $\tilde{h}_{DD} \sim CN(0, \sigma_{SI}^2)$ specifies the residual self-interference channel after self-interference cancellation, $x_P \sim CN(0,1)$ and $x_C \sim CN(0,1)$ denote the public and covert messages, respectively, P_S and P_D indicate the transmit power at the source node and destination node, respectively, and $z_X \sim CN(0, \sigma_X^2)$ represents the additive noise at node X. Note that the destination node can keep the CSI of the source node h_{SD} since the covert transmission occurs internally under the normal *S*-*D* communications. The hidden receiver can also easily estimate the CSI of the source and destination nodes, h_{SR} and h_{DR}, during channel estimation duration if pilot sequences are informed from the destination node in advance. As for the availability of CSI on the warden node, we assume the worst-case covert communications scenario in this work, meaning that the warden has the perfect knowledge of the CSI from the destination and hidden receiver to identify the worst-case achievable covert rate as a performance guideline in practice.

The source node follows an adaptive transmission policy by which the public data rate $r_{P,D}$ is adjusted based on the feedback from the destination, and the achievable public data rate $\bar{r}_{P,D}$ at the destination can be written as [37]

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

The hidden receiver then receives both a public message through the direct link from the source node and a covert message from the destination node as

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

Therefore, the hidden receiver needs to successfully decode and eliminate public messages before retrieving covert messages. This implies that the public data rate is also limited by the achievable public data rate $\bar{r}_{P,R}$ at the hidden receiver as

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

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

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

2.2. Covert Message Detection

At the same time, the warden node receives

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

It first excludes public messages from y_W to obtain the effective residual signal $\tilde{z}_W \triangleq y_W - h_{SW}\sqrt{P_S}x_P$, assuming it perfectly knows h_{SW} and P_S [38]. We then have the following two hypotheses:

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

where the null hypothesis H_0 assumes that there does not exist a covert message, and the alternative hypothesis H_1 presumes that the source node did not send a covert message. This work considers a radiometer [39] as a detection means at the warden, and the sufficient

test statistic T for (7) after observing $N \to \infty$ number of signals reduces to the average residual power $\mathrm{E}[|\tilde{z}_W|^2]$ as [40]

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

The warden node makes a decision that a covert transmission exists when $T \geq \tau$ and otherwise when $T < \tau$ with some threshold τ.

We consider the uncertainty in the noise variance σ_W^2 at the warden node as in [39,41]. Concretely, $\sigma_{W,\mathrm{dB}}^2 \sim U(\bar{\sigma}_{W,\mathrm{dB}}^2 - \zeta_{\mathrm{dB}}, \bar{\sigma}_{W,\mathrm{dB}}^2 + \zeta_{\mathrm{dB}})$ in decibel scale with $\bar{\sigma}_{W,\mathrm{dB}}^2$ and $\zeta_{\mathrm{dB}} \geq 0$ set to the mean and bounded range, respectively. We then derive the DEP $\Pr(\mathrm{e})$ that consists of the false alarm and miss probabilities as

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

in which the warden node conjectures that the covert transmission randomly takes place with $\Pr(H_0) = \Pr(H_1) = 0.5$ [42]. Making use of the cumulative distribution function (CDF) of σ_W^2 (Appendix A),

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

the false alarm and miss probability are specifically written by

$$\Pr(T \geq \tau | H_0) = 1 - F_{\sigma_W^2}(\tau), \tau \in \mathcal{T}_1, \tag{11}$$

$$\Pr(T < \tau | H_1) = F_{\sigma_W^2}\left(\tau - |h_{DW}|^2 P_D \right), \tau \in \mathcal{T}_2, \tag{12}$$

respectively. Here, $\mathcal{T}_1 \triangleq [\bar{\sigma}_W^2/\zeta, \zeta \bar{\sigma}_W^2]$ and $\mathcal{T}_2 \triangleq [|h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta, |h_{DW}|^2 P_D + \zeta \bar{\sigma}_W^2]$.

We have two different cases depending on the value of $|h_{DW}|^2$ and P_D. If $\zeta \bar{\sigma}_W^2 < |h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta$,

$$\Pr(\mathrm{e}) = \begin{cases} \frac{1}{2} \Pr(T \geq \tau | H_0) & \tau \in \mathcal{T}_1, \\ 0 & \tau \in \mathcal{T}_3, \\ \frac{1}{2} \Pr(T < \tau | H_1) & \tau \in \mathcal{T}_2, \end{cases} \tag{13}$$

where $\mathcal{T}_3 \triangleq [\zeta \bar{\sigma}_W^2, |h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta]$. In contrast, if $\zeta \bar{\sigma}_W^2 \geq |h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta$,

$$\Pr(\mathrm{e}) = \begin{cases} \frac{1}{2} \Pr(T \geq \tau | H_0), & \tau \in \mathcal{T}_4, \\ \frac{1}{2} (\Pr(T \geq \tau | H_0) + \Pr(T < \tau | H_1)), & \tau \in \mathcal{T}_5, \\ \frac{1}{2} \Pr(T < \tau | H_1), & \tau \in \mathcal{T}_6, \end{cases} \tag{14}$$

with $\mathcal{T}_4 \triangleq [\bar{\sigma}_W^2/\zeta, |h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta]$, $\mathcal{T}_5 \triangleq [|h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta, \zeta \bar{\sigma}_W^2]$ and $\mathcal{T}_6 \triangleq [\zeta \bar{\sigma}_W^2, |h_{DW}|^2 P_D + \zeta \bar{\sigma}_W^2]$.

The warden node may desire a particular τ that can minimize the DEP. To this end, we first see that (11) and (12) are monotonic from 1 to 0 for $\tau \in \mathcal{T}_1$ and 0 to 1 for $\tau \in \mathcal{T}_2$, respectively. Moreover, the first derivative of $\Pr(T \geq \tau | H_0) + \Pr(T < \tau | H_1)$ is calculated as

$$\frac{1}{2 \ln \zeta} \frac{|h_{DW}|^2 P_D}{\tau \left(\tau - |h_{DW}|^2 P_D \right)}. \tag{15}$$

This is always positive for $\tau \in \mathcal{T}_5$; therefore, the optimal threshold $\tau^\star$ for the warden node in both (13) and (14) is determined by the boundary between $\mathcal{T}_3$ and $\mathcal{T}_2$, or $\mathcal{T}_4$ and $\mathcal{T}_5$ as

$$\tau^\star = |h_{DW}|^2 P_D + \frac{1}{\zeta}\bar{\sigma}_W^2. \tag{16}$$

Note that (16) provides the worst-case minimum DEP assuming that the warden node knows the exact value of P_D.

3. Problem Formulation

In this work, we aim to identify the optimal public data rate and transmit power of the FD destination node that maximizes the covert rate at the hidden receiver as

$$\text{(P1)}: \max_{P_D, r_P} \; r_{C,R}, \tag{17a}$$

$$\text{subject to: } r_P \leq \bar{r}_{P,R}, \tag{17b}$$

$$r_P \leq \bar{r}_{P,D}, \tag{17c}$$

$$r_P \geq \bar{r}_P, \tag{17d}$$

$$\Pr(\text{error})|_{\tau=\tau^\star} \geq \varepsilon, \tag{17e}$$

$$\zeta\bar{\sigma}_W^2 \geq |h_{DW}|^2 P_D + \frac{1}{\zeta}\bar{\sigma}_W^2, \tag{17f}$$

$$0 \leq P_D \leq \bar{P}_D. \tag{17g}$$

Constraint (17b) guarantees that the hidden receiver successfully decodes and eliminates a public message prior to decoding a covert message, and (17c) indicates the achievable public data rate up to which the destination node can notify the source node to adjust. A minimum quality of service $\bar{r}_P$ for the public transmission is considered in (17d), and (17e) with (17f) assures the non-zero minimum DEP for $0 \leq \varepsilon \leq 0.5$. Lastly, (17g) shows the power budget $\bar{P}_D$ at the disguised FD destination node.

4. Proposed Solutions

We first note that the covert rate in (17a) is an increasing function of P_D while the upper limits of r_P in (17b) and (17c) are decreasing functions of P_D. This means that the covert rate cannot exceed a value at which one of the upper limits becomes r_P, i.e., $r_P = \min(\bar{r}_{P,R}, \bar{r}_{P,D})$. Therefore, it is optimal for r_P to be as low as possible for the maximum covert rate as

$$r_P^\star = \bar{r}_P. \tag{18}$$

We now simplify (P1) using the monotonicity of logarithms as

$$\text{(P1.1)}: \max_{P_D} \; P_D, \tag{19a}$$

$$\text{subject to: } P_D \leq \frac{1}{|h_{DR}|^2}\left(\frac{|h_{SR}|^2 P_S}{2^{\bar{r}_P} - 1} - \sigma_R^2\right), \tag{19b}$$

$$P_D \leq \frac{1}{|\tilde{h}_{DD}|^2}\left(\frac{|h_{SD}|^2 P_S}{2^{\bar{r}_P} - 1} - \sigma_D^2\right), \tag{19c}$$

$$P_D \leq \left(\zeta^{(1-4\varepsilon)} - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_W^2}{|h_{DW}|^2}, \tag{19d}$$

$$P_D \leq \left(\zeta - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_W^2}{|h_{DW}|^2}, \tag{19e}$$

$$0 \leq P_D \leq \bar{P}_D. \tag{19f}$$

The right-hand side of (19d) is larger than or equal to that of (19e) for $0 \leq \varepsilon \leq 0.5$, implying that satisfying (19d) automatically fulfills (19e). Therefore, the optimal transmit power can be obtained by taking the minimum of the upper bounds from (19b)–(19d) and (19f) as

$$P_D^\star = \min\left\{ \frac{1}{|h_{DR}|^2}\left(\frac{|h_{SR}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_R^2\right), \frac{1}{|\tilde{h}_{DD}|^2}\left(\frac{|h_{SD}|^2 P_S}{2^{\bar{r}_P}-1} - \sigma_D^2\right), \left(\zeta^{(1-4\varepsilon)} - \frac{1}{\zeta}\right)\frac{\bar{\sigma}_W^2}{|h_{DW}|^2}, \bar{P}_D \right\}. \tag{20}$$

Remark 1. *When the D-R link is extremely strong, i.e.,* $|h_{DR}|^2 \to \infty$*, we have* $P_D^\star \to 0$ *since the hidden receiver cannot eliminate a source message in the presence of a dominant covert message, which is a prerequisite. When there exists excessive FD self-interference, i.e.,* $|\tilde{h}_{DD}|^2 \to \infty$*, we also have* $P_D^\star \to 0$ *for the public data rate, which cannot reach the given threshold* $\bar{r}_P$*. Lastly, when the channel gain of the D-W link is exceptionally high, i.e.,* $|h_{DW}|^2 \to \infty$*, we have* $P_D^\star \to 0$ *as well, since the absence and existence of covert transmission will cause a large difference in the received power at the warden, making it easier to detect any covert transmissions.*

5. Numerical Results

We evaluate the proposed solutions for covert communications with the disguised FD node through numerical results. The effects of various system parameters such as the source transmit power, disguised FD destination transmit power budget, noise uncertainty bound, and minimum DEP threshold on the achievable covert rate $r_{C,R}$ in (5) with the derived optimal destination transmit power $P_D^\star$ in (20) are examined in the upcoming figures. We also focus on verification that $P_D^\star$ fulfills the DEP requirements for any desired threshold ε in (17e) and compare with baseline schemes to stress the significance of $P_D^\star$.

The distance-dependent channel model is adopted for h_{XY} [43]. Concretely, we let $|h_{\mathsf{XY}}|^2 = L_{\mathsf{XY}}|\hat{h}_{\mathsf{XY}}|^2$, where $L_{\mathsf{XY}} \triangleq L_0(d_{\mathsf{XY}}/d_0)^{-\beta}$ indicates the path loss between X and Y. Here, L_0 stands for the path loss at a reference distance $d_0 = 1$ m, β represents the path loss exponent, and d_{XY} indicates the distance between X and Y. Also, the small-scale channel variable $\hat{h}_{\mathsf{XY}}$ follows $CN(0,1)$. The four nodes are placed with certain distances from the origin $O = (0,0)$ in a Cartesian coordinate system such that the coordinates of S, D, R, W are $(-d_{OS}, 0)$, $(d_{OD}, 0)$, $(0, d_{OR})$, $(0, -d_{OW})$, respectively (Figure 2). The overall system parameters are fixed as follows unless otherwise stated: the bandwidth $B = 20$ MHz, $d_{O\mathsf{X}} = 100$ m, source transmit power $P_S = 23$ dBm, destination transmit power budget $\bar{P}_D = 23$ 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 $\sigma_D^2 = \sigma_R^2 = -160$ dBm/Hz, residual self-interference $\sigma_{\mathrm{SI}}^2 = -100$ dB, minimum DEP threshold $\varepsilon = 0.45$, and pathloss exponent $\beta = 3.5$.

Figure 3 shows the average covert rate $r_{C,R}$ as the source transmit power P_S varies. Motivated by the fact that the destination transmit power P_D should be much lower than P_S for successful covert transmissions, we compare the optimal scheme with "α% P_S" in which P_D is fixed as $\min(\alpha\%$ of $P_S, \bar{P}_D)$. We notice that the proposed public data rate in (18) and destination transmit power in (20) result in the highest covert rate for every P_S value, indicating the importance of optimizing r_P and P_D.

We also observe from the "α% P_S" schemes that applying more P_D to a covert transmission induces a higher covert rate when P_S is low, while less P_D is preferred when P_S is high. First, when P_S is low, the public data rate constraints in (17b) and (17c) dominate determining $P_D^\star$ from (20). If $\nu \triangleq \min(\mathrm{E}[|h_{SR}|^2/(|h_{DR}|^2(2^{\bar{r}_P}-1))], \mathrm{E}[|h_{SD}|^2/(|\tilde{h}_{DD}|^2(2^{\bar{r}_P}-1))])$, then any "$\alpha$% P_S" schemes with $\alpha\% > \nu$ are likely to be infeasible on average. It can be inferred from Figure 3 that that $\nu \geq 5\%$ for our system setup since "5% P_S" performs the best among the other fixed P_D schemes.

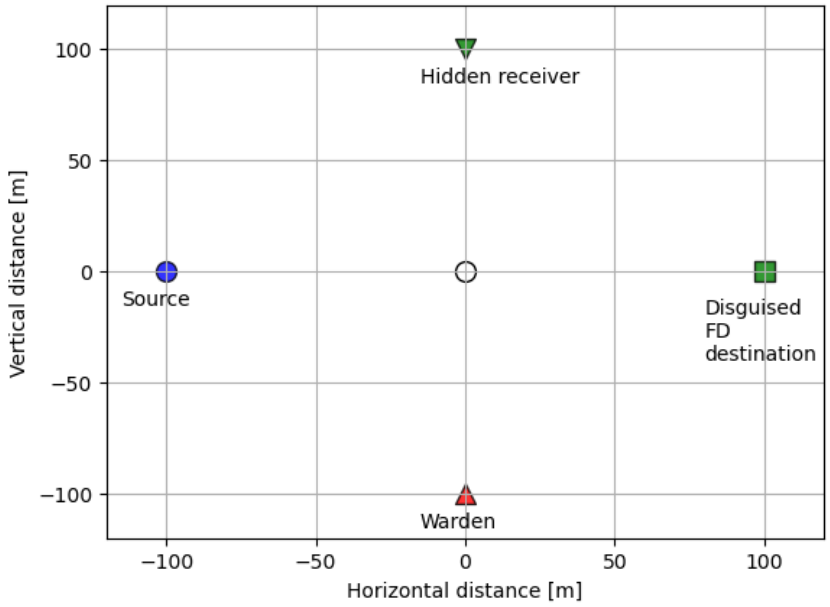

Figure 2. Node placements

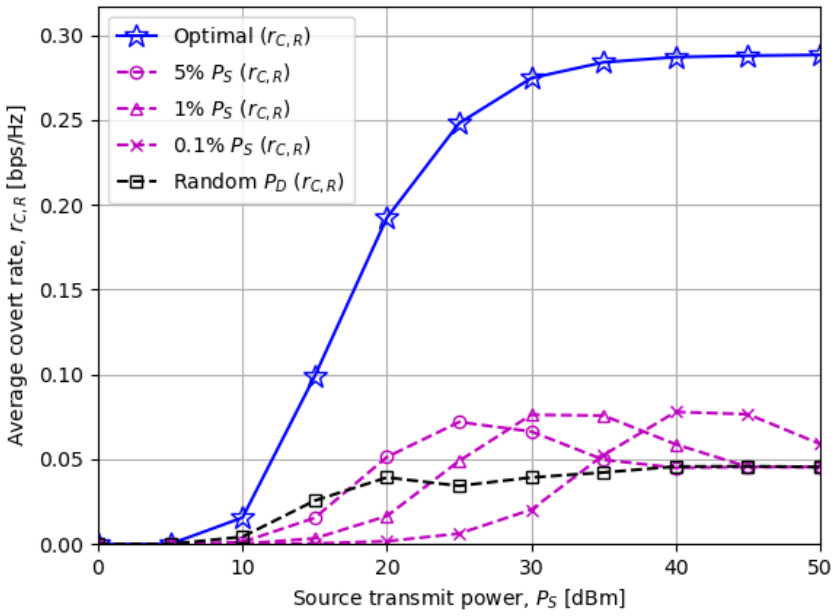

Figure 3. The average covert rate $r_{C,R}$ versus the source node power P_S: Applying more (less) P_D is preferred when P_S is low (high).

On the other hand, when P_S is high, the DEP constraint in (17e) and the power budget $\bar{P}_D$ dominate deciding $P_D^\star$. Hence, only the "α% P_S" schemes with sufficiently low α% can meet these requirements and be feasible on average. This explains the reason why "0.1% P_S" outperforms those with higher α% in Figure 3 in the high P_S region.

Figure 4 compares the average covert rate $r_{C,R}$ as the destination transmit power budget $\bar{P}_D$ changes. It can be seen that "5% P_S" and random P_D schemes perform close to the optimal scheme when $\bar{P}_D$ is low. The reasons are that $P_D^\star$ is dominated by $\bar{P}_D$ in this region and that fixed or randomly chosen P_D in the compared schemes is reduced to $\bar{P}_D$ if $P_D > \bar{P}_D$. For the rest of the $\bar{P}_D$ regions, our proposed solutions achieve the highest covert rate which once more highlights the necessity of optimizing the r_P and P_D.

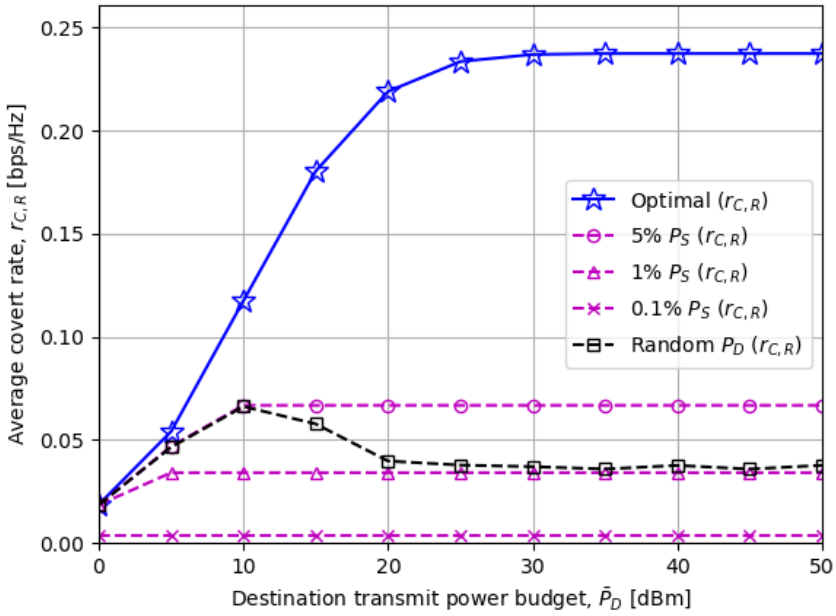

Figure 4. The average covert rate $r_{C,R}$ versus the destination node power budget $\bar{P}_D$: Close performance among the presented schemes for low $\bar{P}_D$ since the optimal P_D is dominantly limited by $\bar{P}_D$.

Figure 5 demonstrates the average covert rate $r_{C,R}$ for different noise uncertainty bounds ζ at the warden node. Quantitatively, a larger ζ widens the upper bound for $P_D^\star$ in (20) so that the covert rate, which is proportional to P_D, has more chance to be enhanced on average. Also, from the qualitative aspect, the larger ζ there is, the more confusion the warden node undergoes in deciding the existence of covert communications.

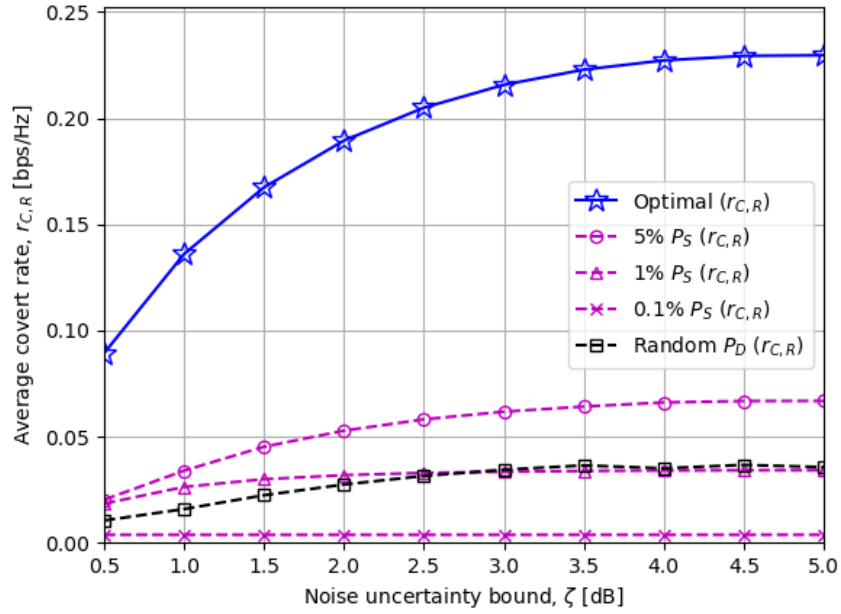

Figure 5. The average covert rate $r_{C,R}$ versus the noise uncertainty bound ζ [dB]: The more unsettled ζ is, the easier it is to perform covert transmissions.

Figures 6 and 7 illustrate the average covert rate $r_{C,R}$ and DEP, respectively, when the minimum DEP threshold ε changes. The covert rates decline in a monotonic manner as ε increases and eventually become zero when a perfect DEP of 0.5 is imposed on. Figure 7 also verifies that the proposed optimal solutions provide just enough DEP above the threshold ε

in general, while the other baseline schemes achieve unnecessarily high DEP by sacrificing the covert rate.

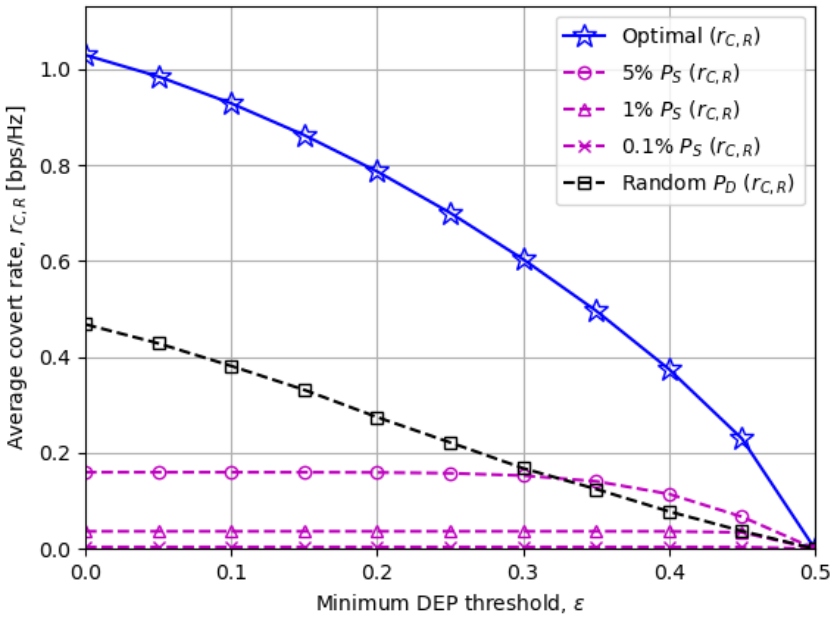

Figure 6. The average covert rate $r_{C,R}$ versus the minimum DEP threshold ε.

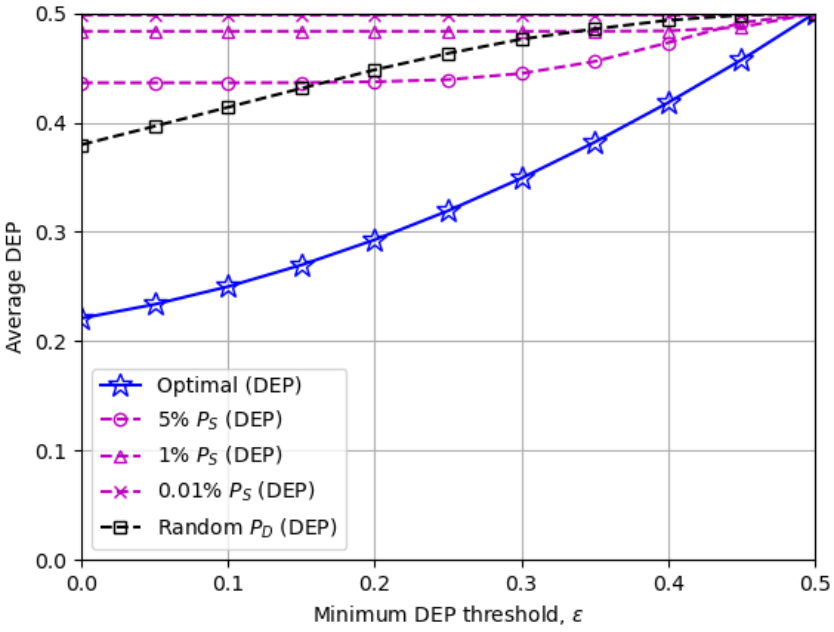

Figure 7. The average DEP versus the minimum DEP threshold ε: The optimal scheme benefits from the best trade-off between the covert rate and DEP for a given ε.

6. Discussion

6.1. Performance

The numerical results from Figures 3–7 confirmed that the optimized transmit power at the disguised FD destination node has a significant impact on the covert rate performance. Furthermore, Figure 3 revealed an interesting relationship between the source and destination transmit power, which is that applying more (less) destination transmit power achieves a higher covert rate when the source transmit power is low (high). Figure 7 also showed that the optimal destination transmits power exploits the best trade-off between the covert rate and minimum DEP threshold.

6.2. Applications

The considered system model and obtained solution may be used in various practical networks. In the military, a reconnaissance troop may place on the adversary side a counterfeit FD device that periodically reports situations while disguising itself as a typical half-duplex one. Moreover, the authors in [44] demonstrated the feasibility of FD on a low Earth orbit (LEO) satellite, and the future non-terrestrial military network would utilize the disguise tactic proposed in this paper for either defense or offense purposes. For surveillance, an IoT network administrator may exploit a disguised FD node to covertly monitor any suspicious users that misuse the network for prohibitive activities.

7. Conclusions

In this paper, we studied a covert communications system where a source node communicates with a disguised FD destination node. Supposedly receive-only, the destination node covertly delivers critical messages to another hidden receiver while evading the surveillance of a warden node as much as possible. We identified the optimal public data rate and the transmit power of the FD destination node that maximizes the covert rate at the hidden receiver.

The obtained closed-form solution exhibited the following: When the destination–receiver link is extremely strong, the optimal destination transmit power approaches zero since the hidden receiver cannot eliminate a source message prior to retrieving a covert message. If the self-interference is not sufficiently suppressed, the optimal destination transmit power approaches zero in this case as well since the public data rate cannot reach the required quality of service. In addition, when the destination–warden channel gain is exceptionally high, the optimal destination transmit power approaches zero since the large difference in the received power at the warden makes it easier to detect the covert link.

The extensive numerical results presented a phenomenon that applying more (less) destination transmit power achieves a higher covert rate when the source transmit power is low (high). It was also verified that the optimal destination transmits power yields the best balance between the covert rate and minimum DEP threshold.

Since our work provides a performance guideline from the information-theoretic point of view, we suggest analyses with practical modulations and imperfect CSI as valuable future research topics.

Funding: 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 Korean government (DAPA (Defense Acquisition Program Administration)) (21-106-A00-007, Space-Layer Intelligent Communication Network Laboratory, 2022).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A

First note that $\sigma^2_{W,\mathrm{dB}} = 10\log_{10}\sigma^2_W$. By the transformation of probability density functions (PDFs) $f_{\sigma^2_W}(\nu) = |J| f_{\sigma^2_{W,\mathrm{dB}}}(\nu)$ with the Jacobian J defined by [45]

$$J = \frac{\partial \sigma^2_{W,\mathrm{dB}}}{\partial \sigma^2_W} = \frac{10}{\sigma^2_W \ln 10}, \tag{A1}$$

the PDF of σ_W^2 becomes

$$f_{\sigma_W^2}(\nu) = \frac{10}{\nu \ln 10} \cdot \frac{1}{2\zeta_{\mathrm{dB}}} = \frac{10}{\nu \ln 10} \cdot \frac{1}{2 \cdot 10 \log_{10} \zeta} = \frac{1}{2 \ln \zeta \cdot \nu}. \tag{A2}$$

Accordingly, the CDF of σ_W^2 is obtained by

$$F_{\sigma_W^2}(\nu) = \int_{\frac{\sigma_W^2}{\zeta}}^{\nu} f_{\sigma_W^2}(\nu) d\nu, \tag{A3}$$

which yields (10).

References

1. Qazi, S.; Khawaja, B.A.; Farooq, Q.U. IoT-Equipped and AI-Enabled Next Generation Smart Agriculture: A Critical Review, Current Challenges and Future Trends. *IEEE Access* **2022**, *10*, 21219–21235. [CrossRef]
2. Zhang, J.; Yan, Z.; Fei, S.; Wang, M.; Li, T.; Wang, H. Is Today's End-to-End Communication Security Enough for 5G and Its Beyond? *IEEE Netw.* **2022**, *36*, 105–112. [CrossRef]
3. Forouzan, B.A. *Cryptography and Network Security*; McGraw-Hill: New York, NY, USA, 2007.
4. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
5. Angueira, P.; Val, I.; Montalbán, J.; Seijo, Ó.; Iradier, E.; Fontaneda, P.S.; Fanari, L.; Arriola, A. A Survey of Physical Layer Techniques for Secure Wireless Communications in Industry. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 810–838. [CrossRef]
6. Jiang, X.; Chen, X.; Tang, J.; Zhao, N.; Zhang, X. Y.; Niyato D.; Wong, K.-K. Covert Communication in UAV-Assisted Air-Ground Networks. *IEEE Wirel. Commun.* **2021**, *28*, 190–197. [CrossRef]
7. Bash, B.A.; Goeckel, D.; Towsley, D.; Guha, S. Hiding information in noise: Fundamental limits of covert wireless communication. *IEEE Commun. Mag.* **2015**, *53*, 26–31. [CrossRef]
8. Shahzad, K.; Zhou, X.; Yan, S.; Hu, J.; Shu, F.; Li, J. Achieving Covert Wireless Communications Using a Full-Duplex Receiver. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 8517–8530. [CrossRef]
9. Xu, T.; Xu, L.; Liu, X.; Lu, Z. Covert Communication with A Full-Duplex Receiver Based on Channel Distribution Information. In Proceedings of the 2018 12th International Symposium on Antennas, Propagation and EM Theory (ISAPE), Hangzhou, China, 3–6 December 2018; pp. 1–4.
10. Zheng, M.; Hamilton, A.; Ling, C. Covert Communications with a Full-Duplex Receiver in Non-Coherent Rayleigh Fading. *IEEE Trans. Commun.* **2021**, *69*, 1882–1895. [CrossRef]
11. Yang, L.; Yang, W.; Xu, S.; Tang, L.; He, Z. Achieving Covert Wireless Communications Using a Full-Duplex Multi-Antenna Receiver. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019; pp. 912–916.
12. Wang, J.; Li, Y.; Tang, W.; Li, X.; Li, S. Channel State Information Based Optimal Strategy for Covert Communication. In Proceedings of the 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), Xi'an, China, 23–25 December 2019; pp. 1–6.
13. Hu, J.; Yan, S.; Zhou, X.; Shu, F.; Li, J. Covert Wireless Communications With Channel Inversion Power Control in Rayleigh Fading. *IEEE Trans. Veh. Technol.* **2019**, *68*, 12135–12149. [CrossRef]
14. Shu, F.; Xu, T.; Hu, J.; Yan, S. Delay-Constrained Covert Communications With a Full-Duplex Receiver. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 813–816. [CrossRef]
15. Zhao, Y.; Li, Z.; Cheng, N.; Wang, D.; Quan, W.; Shen, X. Joint Power and Position Optimization for the Full-Duplex Receiver in Covert Communication. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 July 2020; pp. 1–6.
16. Xu, R.; Guan, L.; Zhao, Y.; Li, Z.; Wang, D. Robust Power and Position Optimization for the Full-Duplex Receiver in Covert Communication. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6.
17. Chen, X.; Sun, W.; Xing, C.; Zhao, N.; Chen, Y.; Yu, F.R.; Nallanathan, A. Multi-Antenna Covert Communication via Full-Duplex Jamming Against a Warden With Uncertain Locations. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 5467–5480. [CrossRef]
18. Che, B.; Yang, W.; Lu, X. Covert Communication for Multi-Channel Transmission with A Full-Duplex Receiver. In Proceedings of the 2021 13th International Conference on Wireless Communications and Signal Processing (WCSP), Changsha, China, 20–22 October 2021; pp. 1–5.
19. Wang, Y.; Yan, S.; Yang, W.; Cai, Y. Covert Communications With Constrained Age of Information. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 368–372. [CrossRef]
20. Sun, R.; Yang, B.; Ma, S.; Shen, Y.; Jiang, X. Covert Rate Maximization in Wireless Full-Duplex Relaying Systems With Power Control. *IEEE Trans. Commun.* **2021**, *69*, 6198–6212. [CrossRef]
21. Li, Y.; Zhao, R.; Deng, Y.; Shu, F.; Nie, Z.; Aghvami, A.H. Harvest-and-Opportunistically-Relay: Analyses on Transmission Outage and Covertness. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 7779–7795. [CrossRef]

22. Wu, Z.; Guo, K.; Zhu, S. Covert Communication for Integrated Satellite–Terrestrial Relay Networks with Cooperative Jamming. *Electronics* **2023**, *12*, 999. [CrossRef]
23. Wang, C.; Li, Z.; Shi, J.; Ng, D.W.K. Intelligent Reflecting Surface-Assisted Multi-Antenna Covert Communications: Joint Active and Passive Beamforming Optimization. *IEEE Trans. Commun.* **2021**, *69*, 3984–4000. [CrossRef]
24. Pejoski, S.; Hadzi-Velkov, Z.; Zlatanov, N. Full-Duplex Covert Communications Assisted by Intelligent Reflective Surfaces. *IEEE Commun. Lett.* **2022**, *26*, 2846–2850. [CrossRef]
25. Wang, M.; Xu, Z.; Xia, B.; Guo, Y. Active Intelligent Reflecting Surface Assisted Covert Communications. *IEEE Trans. Veh. Technol.* **2023**, *72*, 5401–5406. [CrossRef]
26. Wang, C.; Li, Z.; Zheng, T.-X.; Ng, D.W.K.; Al-Dhahir, N. Intelligent Reflecting Surface-Aided Full-Duplex Covert Communications: Information Freshness Optimization. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 3246–3263. [CrossRef]
27. Zhou, X.; Yan, S.; Shu, F.; Chen, R.; Li, J. UAV-Enabled Covert Wireless Data Collection. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 3348–3362. [CrossRef]
28. Guo, Z.; Zhao, S.; Wang, J.; Lit, H.; Shen, Y. Optimal Location Design for UAV Covert Communications with a Full-Duplex Receiver. In Proceedings of the 2022 International Conference on Networking and Network Applications (NaNA), Urumqi, China, 3–5 December 2022; pp. 35–40.
29. Zhang, R.; Chen, X.; Liu, M.; Zhao, N.; Wang, X.; Nallanathan, A. UAV Relay Assisted Cooperative Jamming for Covert Communications Over Rician Fading. *IEEE Trans. Veh. Technol.* **2022**, *71*, 7936–7941. [CrossRef]
30. Li, M.; Tao, X., Wu, H.; Li, N. Joint Trajectory and Resource Optimization for Covert Communication in UAV-Enabled Relaying Systems. *IEEE Trans. Veh. Technol.* **2023**, *72*, 5518–5523. [CrossRef]
31. Yang, J.; Zhou, H.; Chen, R.; Shi, J.; Li, Z. Covert Communication Against a Full-Duplex Adversary in Cognitive Radio Networks. In Proceedings of the GLOBECOM 2022-2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 3144–3149.
32. Yang, Y.; Yang, B.; Shen, S.; She, Y.; Taleb, T. Covert Rate Study for Full-Duplex D2D Communications Underlaid Cellular Networks. *IEEE Internet Things J.* **2023**. [CrossRef]
33. Sun, R.; Yang, B.; Shen, Y.; Jiang, X.; Taleb, T. Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks. *IEEE Internet Things J.* **2023**, *10*, 17–30. [CrossRef]
34. Wang, Y.; Yan, S.; Yang, W.; Zhong, C.; Ng, D.W.K. Probabilistic Accumulate-Then-Transmit in Wireless-Powered Covert Communications. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 10393–10406. [CrossRef]
35. Feng, S.; Lu, X.; Sun, S.; Niyato, D. Mean-Field Artificial Noise Assistance and Uplink Power Control in Covert IoT Systems. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 7358–7373. [CrossRef]
36. Liu, J.; Yu, J.; Chen, X.; Zhang, R.; Wang, S.; An, J. Covert Communication in Ambient Backscatter Systems With Uncontrollable RF Source. *IEEE Trans. Commun.* **2022**, *70*, 1971–1983. [CrossRef]
37. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; John Wiley & Sons, Inc.: New Jersey, NJ, USA, 2005.
38. Kim, S.W.; Ta, H.Q. Covert Communications Over Multiple Overt Channels. *IEEE Trans. Commun.* **2022**, *70*, 1112–1124. [CrossRef]
39. B. He and S. Yan and X. Zhou and V. K. N. Lau On Covert Communication With Noise Uncertainty. *IEEE Commun. Lett.* **2017**, *21*, 941–944. [CrossRef]
40. Sobers, T.V.; Bash, B.A.; Guha, S.; Towsley, D.; Goeckel, D. Covert Communication in the Presence of an Uninformed Jammer. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 6193–6206. [CrossRef]
41. Si, J.; Li, Z.; Zhao, Y.; Cheng, J.; Guan, L.; Shi, J.; Al-Dhahir, N. Covert Transmission Assisted by Intelligent Reflecting Surface. *IEEE Trans. Commun.* **2021**, *69*, 5394–5408. [CrossRef]
42. Liu, Z.; Liu, J.; Zeng, Y.; Ma, J. Covert Wireless Communications in IoT Systems: Hiding Information in Interference. *IEEE Wirel. Commun.* **2018**, *25*, 46–52. [CrossRef]
43. Moon, J.; Lee, S.H.; Lee, H.; Lee, I. Proactive Eavesdropping With Jamming and Eavesdropping Mode Selection. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 3726–3738. [CrossRef]
44. Grayver, E.; Keating, R.; Parower, A. Feasibility of full duplex communications for LEO satellite. In Proceedings of the 2015 IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2015, pp. 1–8.
45. Ross, S. *A First Course in Probability*, 10th ed.; Pearson: London, UK, 2019.