sensors

Article

Hiding Messages in Secure Connection Transmissions with Full-Duplex Overt Receiver

Lap Luat Nguyen [1,2], Tien-Tung Nguyen [3], Anthony Fiche [4], Roland Gautier [4] and Hien Q. Ta [1,2,*]

[1] School of Electrical Engineering, International University, Ho Chi Minh City 700000, Vietnam; nlluat@hcmiu.edu.vn
[2] Vietnam National University, Ho Chi Minh City 700000, Vietnam
[3] Telecommunication Division, Industrial University of Ho Chi Minh City, Ho Chi Minh City 700000, Vietnam; nguyentientung@iuh.edu.vn
[4] Univ Brest, CNRS, Lab-STICC, CS 93837, 6 Avenue Le Gorgeu, CEDEX 3, 29238 Brest, France; anthony.fiche@univ-brest.fr (A.F.); roland.gautier@univ-brest.fr (R.G.)
* Correspondence: tqhien@hcmiu.edu.vn

Abstract: This paper considers hiding messages in overt transmissions with a full-duplex receiver, which emits artificial noise to secure its transmission connection while a transmitter opportunistically sends a covert message to a covert user. The warden's uncertainties in decoding the overt message and artificial-noise-received power are exploited to hide messages. Then, the covert throughput accompanied with the warden's average detection error probability are determined. The results show that increasing the transmit power of artificial noise or improving secure connection at the overt user will improve the covert performance. The results also show that the covert performance is improved when the self-interference cancellation is improved at the full-duplex receiver or when the warden is located close to the full-duplex receiver, indicating the positive impact of the overt performance on the covert performance.

Keywords: covert communication; reliable deniable communication; covert throughput

Citation: Nguyen, L.L.; Nguyen, T.-T.; Fiche, A.; Gautier, R.; Ta, H.Q. Hiding Messages in Secure Connection Transmissions with Full-Duplex Overt Receiver. *Sensors* **2022**, *22*, 5812. https://doi.org/10.3390/s22155812

Academic Editor: Changchuan Yin

Received: 3 June 2022
Accepted: 1 August 2022
Published: 3 August 2022

1. Introduction

In wireless transmissions, the security and privacy of their broadcast nature become a critical issue as it operates not only in the civil area but also in the military. For example, privacy information in health care, the journey or location of vehicles in transportation and the position or confidential information of the targets need to be protected. Regarding security protection for wireless communications, several conventional approaches, such as cryptography [1] or physical layer security [2–4], have been implemented. These methods only target preventing the confidential content of messages from being stolen by eavesdroppers. Nevertheless, some scenarios are dedicated to avoiding being attacked, such as jamming when the existence (privacy) of transmissions is revealed. For example, in the case of a self-driving car, the controlling signals need to be completely secured or hidden from the adversary. Moreover, the location or itinerary of vehicles needs to be kept private. Their revelations to the attacker may cause security issues or accidents. Therefore, covert communication has emerged as a potential solution for dealing with the issue of privacy.

Covert or low-probability-of-detection communication refers to scenarios where the transmitter sends its message to the receiver such that the warden cannot detect (or can detect at a low probability) the existence of transmissions [5]. The square root law (SRL) for covert communication was firstly introduced in additive white Gaussian noise (AWGN) channels for covert or low-probability-of-detection communication with two important measures: the warden's detection error probability ξ, defined as the sum of the probabilities of a false alarm when the transmitter is not sending and missed the detection when the transmitter is sending, and the covert throughput, defined by the number of bits transmitted reliably over N channels subject to the constraint of $\xi \geq 1-\epsilon$ for covert requirement $\epsilon \geq 0$ [5]. Then, SRL can be used to preside the covert communication, in which, the $\mathcal{O}(\sqrt{N})$ bits can be transmitted over N channels covertly and reliably. After proving the SRL in additive white Gaussian noise (AWGN) channels [5], it was developed to discrete memoryless channels (DMCs) [6–8], in which, the Big-O notation characterizes the constant hidden. Then, [9] extended the study to covert communication in DMCs under some constraints related to the covertness. In [10], the authors showed that the Gaussian signalling can be optimal under only a covertness constraint. Thus, the Kullback–Leibler divergence asymmetry property can optimize the Gaussian signalling with other constraints to [10]. However, SRL has a weakness, as a positive covert rate cannot be guaranteed when the number of channels tends to infinity. This means that the covert rate $\mathcal{O}(N)$ tends to 0 when N tends to infinity. This problem of SRL was later addressed and solved by [11–13]. In [11], the study pointed out that a signal-to-noise ratio (SNR) threshold will impact the detection of the transmitted signal if the received signal power is less than this threshold. Thus, it can be seen as a noise uncertainty when the noise power estimation does not match the actual noise power. Hence, the noise uncertainty is useful in covert communication since it could be a medium to hide a message. The study in [12] proved that there will be a positive covert rate even for an infinite number of channels if the legitimate has noise uncertainty. Thus, the covert throughput was analyzed in [13] based on two noise uncertainty practical models under AWGN channels.

In general, two well-known approaches adopted for covert communications have been widely investigated in the literature. The key idea of the first approach is to take advantage of various sources of the adversary's uncertainty to guarantee the covertness, e.g., adversary's noise uncertainty in [12,13], uncertainties of transmission time [14], channel state information [15] and transmit power [16]. Later, the noise uncertainty was extended to uninformed jamming [17] and artificial noise (AN) from a friendly jammer [18] or from a full-duplex receiver [19–21]. Using AN at the FD receiver, the receiver receives the covert message while jamming the warden to make it harder to detect the covert message [19–21]. However, two critical questions arise: (1) in the case of the covert receiver being a low cost-device, i.e., IoT users with hardware that is not complex and does not have enough energy to simultaneously carry out two such roles, and (2) jamming by the covert receiver, which receives the covert message, may help the adversary to detect the presence of covert transmission. Hence, jamming while receiving the covert information by the covert receiver may not be practical in a real scenario. For the second approach, other works considered superimposing the covert message into another message of existing transmissions, termed as hiding messages into overt transmissions, and exploited transmit power control [22] and random transmit power [23]. The basic idea of the second approach is to guarantee covertness by enlarging the dynamic range of the adversary's uncertainties via the existing transmission. Most recently, [24] showed, for the first time, that the warden cannot detect the covert message if the overt message where the covert message is superimposed onto is not decoded. This finding can be referred to as *decoding uncertainty* at the warden.

Inspired by [24] and the full-duplex receiver scheme in [19–21], we introduce a novel scheme of hiding messages into existing overt transmissions with a FD overt receiver. Different from [19–21], the artificial noise jamming signal is transmitted by the overt receiver with just naive intention to secure its connection with the transmitter [25] and, thus, the presence of the covert transmission will not be detected via artificial noise jamming. More specifically, the superposition signal of the covert and overt messages is transmitted at a fixed transmit power while the overt receiver emits the AN to secure its connection. With this setting, we find that, in order to detect the covert message, it is necessary for the warden to decode the overt message and, even if the overt message is decoded, the covertness still can be guaranteed due to the adversary's uncertainty in receiving AN powers. Then, an efficient AN and the improved performance of the secure connection of the overt transmission leads to an improvement in the covertness. In this paper, performances were evaluated by using three metrics: the adversary's average detection error probability ξ, the covert throughput

η_u and the overt throughput loss $\eta_{v,\text{loss}}$. The main contributions of the paper are listed as follows:

- We propose a scheme to hide the covert information by exploiting the existing secure connection transmission with the aid of artificial noise generated by a full-duplex overt receiver, which has not been considered in literature.
- The artificial noise used for improving the secure connection transmission can also be exploited for improving covert transmissions.
- The artificial noise can be further improved if the channel state information between the over receiver and the warden is unknown at the warden, which is also known as the uncertainty of artificial noise power.

This paper is organized as follows. Section 2 will describe the system model with one transmitter and two receivers, as well as a warden. Section 3 presents the optimum detection of the warden. The covert throughput and the overt throughput loss are examined in Sections 4 and 5, respectively. The numerical results will be shown in Section 6.

2. System Model

We considered one transmitter (Alice) and two receivers—one (Carol) to receive overt messages, $\mathbf{v} = (v_1, ..., v_n)$, and one (Bob) to receive covert messages, $\mathbf{u} = (u_1, ..., u_n)$—and a warden (Willie) to detect the presence of covert transmission. The proposed system is illustrated in Figure 1, where Carol equipped with two antennas operates at full-duplex mode to secure its connection to the warden [19], whereas other nodes employ a half-duplex mode with a single antenna. The proposed scheme is under practical consideration of uplink transmissions, in which, the transmitter (an IoT device) opportunistically sends its covert message on top of the overt message as a camouflage while the overt receiver (a base station with an advanced receiver architecture) secures its connection. Here, the artificial noise is naively exploited to secure the connection for the overt user and, then, is opportunistically used to provide covertness for the covert user.

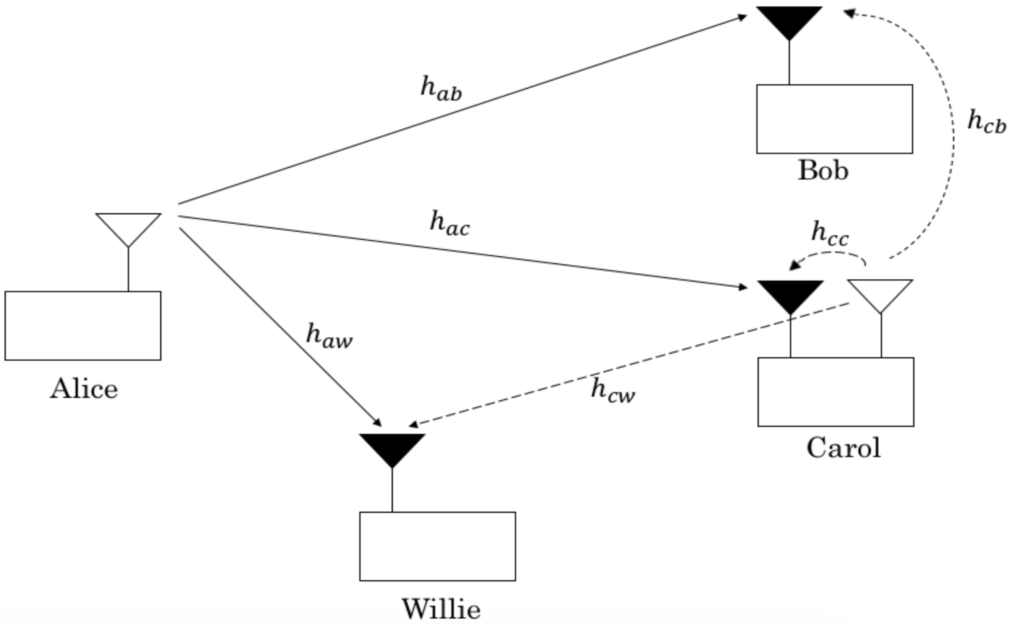

Figure 1. Alice tries to hide a covert message to Bob within overt transmissions to Carol toward Willie; a warden looks for covert message.

Considering the random coding used to generate codewords [26], the codewords $\mathbf{u}$ and $\mathbf{v}$ are independently generated by random selection symbols from a complex normal distribution. To guarantee the covertness, the codebook of $\mathbf{u}$ is a share secret between

Alice and Bob, whereas that of **v** is assumed as known to all users, including Willie. The transmitted signal from Alice, from Willie's perspective, is given by

$$\mathbf{x} = \begin{cases} \sqrt{P_a}\mathbf{v}, & H_0, \\ \sqrt{P_a}(\sqrt{\alpha}\mathbf{v} + \sqrt{1-\alpha}\mathbf{u}), & H_1, \end{cases} \tag{1}$$

where H_0 and H_1 denote the null hypothesis that **u** has not been sent by Alice and the alternative hypothesis, respectively, $\alpha \in [0,1]$ is the ratio of power allocated to the overt message and P_a is Alice's total transmit power, which is always constant regardless of the covert transmission.

The quasi-static Rayleigh block fading channels is considered, where the channel gain is constant inside an n symbols block and changes from one block to another independently [22,24]. Let the channel gain be h_{ij} between nodes i and j, where $i \in \{a, c\}$ and $j \in \{b, c, w\}$, in which nodes a, b, c and w represent Alice, Bob, Carol and Willie, respectively, and have a Gaussian distribution with mean 0 and variance σ_{ij}^2. A high value of σ_{ij}^2 means that the two users are close. Assuming that Alice sends pilot symbols for channel estimations before data transmissions, and assuming perfect channel estimation at all receiver nodes, node j perfectly knows h_{aj}. We further denote $\mathbf{n}_j$, $j \in \{b, c, w\}$ as the background noise vector at node j and assume that $\mathbf{n}_j$ has a complex Gaussian distribution with mean 0 and variance σ_n^2, i.e., $\mathbf{n}_j \sim CN(0, \sigma_n^2)$. It should be noted that Carol does not send their channel estimate to Alice. In addition, Bob will not send their channel estimate to Alice in order to avoid being detected by Willie. Hence, Alice does not know the channel information from them to other nodes and designs fixed transmission rates to Bob and Carol. This design is suitable for IoT applications with a requirement of strict latency as it does not require channel information feedback. For convenience, the parameter and metric notations are provided in Table 1.

Table 1. Table of parameter and metric notations.

Parameter	Notation
Alice's transmit power	P_a
Carol's transmit power or the transmit AN power	P_c
The power allocation ratio	α
The cancellation coefficient at Carol	ϕ
The channel gain between nodes i and j	h_{ij}
The channel gain variance between nodes i and j	σ_{ij}^2
The background noise variance	σ_n^2
The transmission rate of the overt message, **v**	R_v
The transmission rate of the covert message, **u**	R_u
Covertness requirement	ϵ
Average detection error probability	ξ
Covert throughput	η_u
Maximum covert throughput	$\eta_{u,\max}$
Overt throughput	η_v
Overt throughput loss	$\eta_{v,\text{loss}}$
Received signal at Bob	$\mathbf{y}_b$
Received signal at Carol	$\mathbf{y}_c$
Received signal at Willie	$\mathbf{y}_w$

3. Warden's Optimum Detection

After receiving the transmitted signal from Alice and artificial noise from Carol, the signal to be received at Willie is expressed as

$$\mathbf{y}_w = \begin{cases} \sqrt{P_a} h_{aw} \mathbf{v} + \sqrt{P_c} h_{cw} \mathbf{z} + \mathbf{n}_w, & H_0, \\ \sqrt{P_a} h_{aw} (\sqrt{\alpha} \mathbf{v} + \sqrt{1-\alpha} \mathbf{u}) + \sqrt{P_c} h_{cw} \mathbf{z} + \mathbf{n}_w, & H_1, \end{cases} \tag{2}$$

where $\mathbf{z} \sim CN(0,1)$ is the AN signal transmitted by Carol and P_c is the transmit AN power. It will be proven that the distribution of $\mathbf{y}_w = \{y_{w,1}, \ldots, y_{w,n}\}$ is identical under H_0 and H_1 if $\mathbf{v}$ is not decoded, and different if $\mathbf{v}$ is decoded. This means that Willie cannot detect the covert message $\mathbf{u}$ if the overt message $\mathbf{v}$ cannot be decoded. Moreover, since Willie has uncertainty in the received AN power, $|h_{cw}|^2 P_c$, the covertness can still be guaranteed if $\mathbf{v}$ is decoded. In this section, the average total detection error probability, estimated over the event of Willie's success and failure to decode $\mathbf{v}$, is calculated. In detail, we considered two cases: Willie fails to decode $\mathbf{v}$ and Willie succeeds in decoding $\mathbf{v}$, as follows.

3.1. Willie Fails to Decode $\mathbf{v}$

When Willie fails to decode $\mathbf{v}$, they will perform the marginalized likelihood ratio test (LRT), i.e., averaging unknown $\mathbf{v}$ in the likelihood functions, as its optimum detection [27], is

$$\Lambda := \frac{\mathrm{E}_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_1)]}{\mathrm{E}_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_0)]} \underset{H_1}{\overset{H_0}{\lesseqgtr}} \lambda, \tag{3}$$

where ($E_X[f(X)]$ denotes the expectation of the function $f(X)$ with respect to the random variable X), under H_1, by treating $\mathbf{u} = \{u_1, ..., u_n\}$ in (2) as noise since Willie does not know the codebook of $\mathbf{u}$, we have

$$\begin{aligned} \Pr(\mathbf{y}_w|\mathbf{v}, H_1) &= \prod_{i=1}^{n} \Pr(y_{w,i}|v_i, H_1) \\ &= \prod_{i=1}^{n} \frac{\exp\left(-\frac{|y_{w,i} - h_{aw}\sqrt{\alpha P_a} v_i|^2}{\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha) P_a |h_{aw}|^2}\right)}{\pi(\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a)} \\ &= \frac{\exp\left(-\frac{\left\|\mathbf{y}_w - h_{aw}\sqrt{\alpha P_a}\mathbf{v}\right\|^2}{\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha) P_a |h_{aw}|^2}\right)}{(\pi(\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a))^n}, \end{aligned} \tag{4}$$

and, under H_0, we similarly have

$$\Pr(\mathbf{y}_w|\mathbf{v}, H_0) = \frac{\exp\left(-\frac{||\mathbf{y}_w - h_{aw}\sqrt{P_a}\mathbf{v}||^2}{\sigma_n^2 + |h_{cw}|^2 P_c}\right)}{(\pi(\sigma_n^2 + |h_{cw}|^2 P_c))^n}. \tag{5}$$

Then, we obtain from (4) and (5) that

$$\mathrm{E}_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_0)] = \mathrm{E}_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_1)]. \tag{6}$$

The proof of (6) is provided in Appendix A. Hence, $\Lambda = 1$.

Let $I(\mathbf{v};\mathbf{y}_w)$ denote the mutual information between $\mathbf{v}$ and $\mathbf{y}_w$, and R_v denote the transmission rate of the overt message. The design value of R_v will be determined in Section 5. It follows from [28] (Equation (1)) that the event of $I(\mathbf{v};\mathbf{y}_w) < R_v$ is a subset of the event that Willie fails to decode $\mathbf{v}$. Then, the lower bound of the false alarm and missed detection probabilities, in the case that Willie fails to decode $\mathbf{v}$, are given by

$$\begin{aligned} P_f &= \Pr(\lambda < 1, I(\mathbf{v};\mathbf{y}_w) < R_v | H_0), \\ P_m &= \Pr(\lambda \geq 1, I(\mathbf{v};\mathbf{y}_w) < R_v | H_1), \end{aligned} \tag{7}$$

respectively, where

$$I(\mathbf{v};\mathbf{y}_w) = \begin{cases} \log_2\left(1 + \frac{|h_{aw}|^2 P_a}{\sigma_n^2 + |h_{cw}|^2 P_c}\right), & H_0, \\ \log_2\left(1 + \frac{\alpha |h_{aw}|^2 P_a}{\sigma_n^2 + (1-\alpha)|h_{aw}|^2 P_a + |h_{cw}|^2 P_c}\right), & H_1. \end{cases} \tag{8}$$

To achieve a high detection performance, the strategy of the warden Willie is to minimize the sum of the false alarm and missed detection probabilities ($P_f + P_m$) by choosing λ properly. Since $I(\mathbf{v};\mathbf{y}_w)$ under H_0 is larger than that under H_1, Willie may choose $\lambda < 1$ to obtain the minimum

$$\begin{aligned} P_f + P_m &= \Pr(I(\mathbf{v};\mathbf{y}_w) < R_v | H_0) \\ &= 1 - \Pr\left(|h_{aw}|^2 \geq \frac{(2^{R_v} - 1)(\sigma_n^2 + |h_{cw}|^2 P_c)}{P_a}\right), \end{aligned} \tag{9}$$

which, since $|h_{ij}|^2$ is distributed exponentially with a scale of $1/\sigma_{ij}^2$, yields

$$\begin{aligned} P_f + P_m &= 1 - \int_0^\infty \exp\left(-\frac{(2^{R_v} - 1)(\sigma_n^2 + x P_c)}{\sigma_{aw}^2 P_a}\right) \times \frac{\exp(-x/\sigma_{cw}^2)}{\sigma_{cw}^2} dx \\ &= 1 - \frac{\exp(-(2^{R_v} - 1)\sigma_n^2 / (\sigma_{aw}^2 P_a))}{1 + (2^{R_v} - 1)\sigma_{cw}^2 P_c / (\sigma_{aw}^2 P_a)}. \end{aligned} \tag{10}$$

Remark 1. *One can see from (9) that $(P_f + P_m)$ also represents the secure connection probability and increases as the AN transmit power P_c increases. This means that the AN helps to not only secure the connection for the overt user but also to hide the message for the covert user.*

3.2. Willie Succeeds in Decoding v

When Willie succeeds in decoding $\mathbf{v}$, they will perform the LRT of

$$\begin{aligned} \Lambda' &:= \frac{1}{n} \ln\left(\frac{\Pr(\mathbf{y}_w | \mathbf{v}, H_1)}{\Pr(\mathbf{y}_w | \mathbf{v}, H_0)}\right) - \ln\left(\frac{\sigma_n^2 + |h_{cw}|^2 P_c}{\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a}\right) \\ &= \frac{||\mathbf{y}_w - h_{aw}\sqrt{P_a}\mathbf{v}||^2}{n(\sigma_n^2 + |h_{cw}|^2 P_c)} - \frac{||\mathbf{y}_w - h_{aw}\sqrt{\alpha P_a}\mathbf{v}||^2}{n(\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a)} \underset{H_1}{\overset{H_0}{\lesseqgtr}} \lambda', \end{aligned} \tag{11}$$

where (11) is derived from (4) and (5). As $n \to \infty$ (the best scenario for Willie's detection), Λ' converges to

$$\Lambda' \to \begin{cases} \frac{2\sqrt{\alpha}(1-\sqrt{\alpha})|h_{aw}|^2 P_a}{\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a}, & H_0, \\ \frac{2(1-\sqrt{\alpha})|h_{aw}|^2 P_a}{\sigma_n^2 + |h_{cw}|^2 P_c}, & H_1. \end{cases} \tag{12}$$

Remark 2. *One can see that, if Willie perfectly knows the channel gain h_{cw} via channel information feedback at Carol or perfectly knows their received AN power of $|h_{cw}|^2P_c$, Willie can choose the detection threshold*

$$\lambda' \in \left[\frac{2\sqrt{\alpha}(1-\sqrt{\alpha})|h_{aw}|^2P_a}{\sigma_n^2+|h_{cw}|^2P_c+(1-\alpha)|h_{aw}|^2P_a}, \frac{2(1-\sqrt{\alpha})|h_{aw}|^2P_a}{\sigma_n^2+|h_{cw}|^2P_c}\right] \tag{13}$$

such that, from (12), the false alarm probability and missed detection probability are zero, i.e., $P_f'(h_{aw}) = P_m'(h_{aw}) = 0$, i.e., Willie can always detect the presence of the covert transmission if the overt message **v** *is decoded and removed. However, this channel information feedback is not considered in our system model and, hence, Willie has uncertainty in the received AN power, which still guarantees a certain covertness even if the overt message* **v** *is decoded and removed.*

Since $|h_{cw}|^2$ has an exponential distribution with a mean of σ_{cw}^2, the false alarm and missed detection probabilities for decoding **u** at Willie, by assuming that Willie succeeds in decoding **v**, based on (8) and (12), are given by

$$\begin{aligned} P_f'(h_{aw}) &= \Pr(\Lambda' > \lambda', I(\mathbf{v};\mathbf{y}_w) \geq R_v|H_0) \\ &= \Pr(|h_{cw}|^2/\sigma_{cw}^2 < \min\{r_0/\lambda' - s_0, \delta_0\}) \\ &= 1 - \exp\big(-\min\{r_0/\lambda' - s_0, \delta_0\}\big), \end{aligned} \tag{14}$$

$$\begin{aligned} P_m'(h_{aw}) &= \Pr(\Lambda' \leq \lambda', I(\mathbf{v};\mathbf{y}_w) \geq R_v|H_1) \\ &= \Pr\Big(r_1/\lambda' - s_1 \leq |h_{cw}|^2/\sigma_{cw}^2 \leq \delta_1\Big) \\ &= (\exp(-(r_1/\lambda' - s_1)) - \exp(-\delta_1))^+, \end{aligned} \tag{15}$$

where $(x)^+ = \max(x, 0)$, and

$$\begin{aligned} r_0 &= 2\sqrt{\alpha}(1-\sqrt{\alpha})|h_{aw}|^2P_a/(\sigma_{cw}^2P_c), \\ s_0 &= (\sigma_n^2 + (1-\alpha)|h_{aw}|^2P_a)/(\sigma_{cw}^2P_c), \\ r_1 &= 2(1-\sqrt{\alpha})|h_{aw}|^2P_a/(\sigma_{cw}^2P_c), \\ s_1 &= \sigma_n^2/(\sigma_{cw}^2P_c), \\ \delta_0 &= |h_{aw}|^2P_a/((2^{R_v}-1)\sigma_{cw}^2P_c) - \sigma_n^2/(\sigma_{cw}^2P_c), \\ \delta_1 &= |h_{aw}|^2P_a(\alpha(1-\alpha)2^{R_v})^+/((2^{R_v}-1)\sigma_{cw}^2P_c) - \sigma_n^2/(\sigma_{cw}^2P_c). \end{aligned} \tag{16}$$

Willie attempts to minimize $(P_f'(h_{aw}) + P_m'(h_{aw}))$ by properly choosing λ' equal to

$$\lambda' = \left[\min\left\{\frac{\ln(r_1/r_0) - (s_0 - s_1)}{r_1 - r_0}, \frac{s_1 + \delta_1}{r_1}\right\}\right]^{-1}, \tag{17}$$

where its proof is provided in Appendix B, and then

$$P_f'(h_{aw}) + P_m'(h_{aw}) = 1 - \exp\big(s_0 - r_0/\lambda'\big) + \exp(s_1 - r_1/\lambda')) - \exp(-\delta_1). \tag{18}$$

3.3. Average Total Detection Error Probability

In summary, the average total detection error probability, estimated over the event of Willie's success and failure to decode $\mathbf{v}$ regardless of the number of symbols n, can be determined as

$$\xi = (P_f + P_m) + \mathrm{E}_{h_{aw}}[P'_f(h_{aw}) + P'_m(h_{aw})], \tag{19}$$

which can be computed from (10) and (18). Here, we emphasize that the total detection error probability in (19) is the lower bound obtained from (10) and (18) and that it is necessary to consider (19) as the covertness measure, which is independent of the number of symbols under practical considerations.

Covert requirement: A covert communication can be achieved if $\xi \geq 1 - \epsilon$ for any covertness requirement $\epsilon > 0$. This means that the detection is ineffective, i.e., $\xi \to 1$, at a sufficiently small $\epsilon \to 0$.

4. Covert Throughput at the Covert User Bob

In this section, the covert throughput will be determined. The covert throughput of $\mathbf{u}$ between Alice and Bob is the average rate correctly received over many transmission bursts, i.e., $R_u \times (1 - P_{\mathrm{out},B})$, because the message is only correctly received on $(1 - P_{\mathrm{out},B})$ transmissions [15], with $P_{\mathrm{out},B}$ being the decoding outage probability. Since Alice does not know h_{ab}, they will transmit $\mathbf{u}$ at a fixed rate R_u. The received signal at Bob is given by

$$\boldsymbol{y}_b = \sqrt{(1-\alpha)P_a}h_{ab}\mathbf{u} + \sqrt{\alpha P_a}h_{ab}\mathbf{v} + \sqrt{P_c}h_{cb}\mathbf{z} + \mathbf{n}_b. \tag{20}$$

Assuming successive interference cancellation receiver type at Bob [29], the covert message maximum rate is given by

$$I(\mathbf{u};\mathbf{y}_b)_0 = \log_2\left(1 + \frac{(1-\alpha)|h_{ab}|^2 P_a}{\sigma_n^2 + \alpha|h_{ab}|^2 P_a + |h_{cb}|^2 P_c}\right) \tag{21}$$

if Bob cannot decode $\mathbf{v}$, i.e., $I(\mathbf{v};\mathbf{y}_b) < R_v$ or, equivalently,

$$|h_{ab}|^2 < \frac{(2^{R_v} - 1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v} - 1))^+ P_a}, \tag{22}$$

and, otherwise,

$$I(\mathbf{u};\mathbf{y}_b)_1 = \log_2\left(1 + \frac{(1-\alpha)|h_{ab}|^2 P_a}{\sigma_n^2 + |h_{cb}|^2 P_c}\right). \tag{23}$$

Since $|h_{ab}|^2$ has an exponential distribution with a mean of σ_{ab}^2 with its cumulative distribution function (CDF) of

$$\Pr(|h_{ab}|^2 < x) = 1 - \exp(-x/\sigma_{ab}^2) \tag{24}$$

and $|h_{cb}|^2$ has an exponential distribution with a mean of σ_{cb}^2 with its probability density function (PDF) of

$$p_{|h_{cb}|^2}(x) = \exp(-x/\sigma_{cb}^2)/\sigma_{cb}^2. \tag{25}$$

The decoding outage probability, denoted as $P_{\mathrm{out},B}(P_a)$, of the covert message $\mathbf{u}$ can be derived in a closed-form expression as

$$\begin{aligned}
P_{\text{out},B}(P_a) &= \Pr\left(I(\mathbf{u};\mathbf{y}_b)_0 < R_u, |h_{ab}|^2 < \frac{(2^{R_v}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^+ P_a} \right) \\
&\quad + \Pr\left(I(\mathbf{u};\mathbf{y}_b)_1 < R_u, |h_{ab}|^2 \geq \frac{(2^{R_v}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^+ P_a} \right) \\
&= \Pr\left(|h_{ab}|^2 < \min\left\{ \frac{(2^{R_v}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^+ P_a}, \frac{(2^{R_u}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(1-\alpha 2^{R_u})^+ P_a} \right\} \right) \\
&\quad + \Pr\left(\frac{(2^{R_v}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^+ P_a} \leq |h_{ab}|^2 \leq \frac{(2^{R_u}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(1-\alpha) P_a} \right) \\
&= 1 - \int_0^\infty \exp\left(-\min\left\{ \frac{(2^{R_v}-1)(\sigma_n^2 + x P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^+ \sigma_{ab}^2 P_a}, \frac{(2^{R_u}-1)(\sigma_n^2 + x P_c)}{(1-\alpha 2^{R_u})^+ \sigma_{ab}^2 P_a} \right\} \right) \\
&\qquad \times p_{|h_{cb}|^2}(x) dx \\
&\quad + \int_0^\infty \left(\exp\left(-\frac{(2^{R_v}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^+ \sigma_{ab}^2 P_a} \right) \right. \\
&\qquad \left. - \exp\left(-\frac{(2^{R_u}-1)(\sigma_n^2 + |h_{cb}|^2 P_c)}{(1-\alpha)\sigma_{ab}^2 P_a} \right) \right) p_{|h_{cb}|^2}(x) dx \\
&= 1 - \max\left\{ \frac{e^{-\frac{(2^{R_v}-1)\sigma_n^2}{(\alpha-(1-\alpha)(2^{R_v}-1))^+ \sigma_{ab}^2 P_a}}}{1 + \frac{(2^{R_v}-1)\sigma_{cb}^2 P_c}{(\alpha-(1-\alpha)(2^{R_v}-1))^+ \sigma_{ab}^2 P_a}}, \frac{e^{-\frac{(2^{R_u}-1)\sigma_n^2}{(1-\alpha 2^{R_u})^+ \sigma_{ab}^2 P_a}}}{1 + \frac{(2^{R_u}-1)\sigma_{cb}^2 P_c}{(1-\alpha 2^{R_u})^+ \sigma_{ab}^2 P_a}} \right\} \\
&\quad + \left(\frac{e^{-\frac{(2^{R_v}-1)\sigma_n^2}{(\alpha-(1-\alpha)(2^{R_v}-1))^+ \sigma_{ab}^2 P_a}}}{1 + \frac{(2^{R_v}-1)\sigma_{cb}^2 P_c}{(\alpha-(1-\alpha)(2^{R_v}-1))^+ \sigma_{ab}^2 P_a}} - \frac{e^{-\frac{(2^{R_u}-1)\sigma_n^2}{\sigma_{ab}^2 P_a}}}{1 + \frac{(2^{R_u}-1)\sigma_{cb}^2 P_c}{\sigma_{ab}^2 P_a}} \right)^+ .
\end{aligned} \tag{26}$$

As in [24], the covert throughput (bits/Hz/s) is expressed as $R_u \times (1 - P_{\text{out},B}(P_a))$. In this paper, the covert throughput maximization problem is formulated as

$$\begin{aligned}
\eta_u = \max_{P_a} \quad & R_u \times (1 - P_{\text{out},B}(P_a)) \\
\text{s.t.} \quad & \xi \geq 1 - \epsilon,
\end{aligned} \tag{27}$$

where ϵ represents the covertness requirement. Since $P_{\text{out},B}(P_a)$ is a decreasing function of P_a (see Figure 2), $R_u(1 - P_{\text{out},B}(P_a))$ is an increasing function of P_a. Also, since ξ is a decreasing function of P_a (see Figure 3), the constraint of $\xi \geq 1 - \epsilon$ requires P_a less than a threshold P_a^*, where P_a^* is the solution of $\xi = 1 - \epsilon$. Hence, $R_u(1 - P_{\text{out},B}(P_a))$ is maximized when $P_a = P_a^*$. Therefore, the covert throughput (bits/Hz/s) is given by

$$\eta_u = R_u \times (1 - P_{\text{out},B}(P_a^*)). \tag{28}$$

and its resulting maximum covert throughput is given by

$$\eta_{u,max} = \max_{R_u} \ \eta_u \tag{29}$$

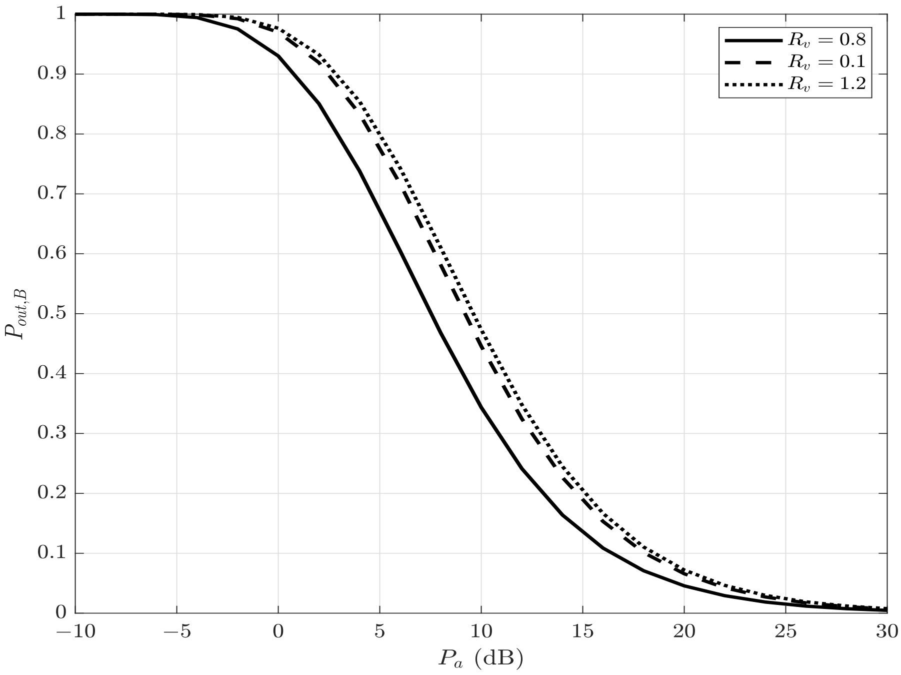

Figure 2. Bob's decoding outage probability, $P_{\text{out},B}(P_a)$, versus Alice's transmit power P_a, for different values of R_v; $\alpha = 0.8$ and $P_c = 5$ dB.

To enable a positive covert throughput, the overt user needs to sacrifice its throughput for the covert message. Consequently, the next section presents the overt throughput loss.

5. Overt Throughput Loss at the Overt User Carol

In this section, the loss of the overt throughput traded for the covert throughput is characterized. Under H_1, the received signal at Carol is given by

$$\boldsymbol{y}_c = \sqrt{\alpha P_a} h_{ac} \mathbf{v} + \sqrt{(1-\alpha)P_a} h_{ac} \mathbf{u} + \sqrt{\phi P_c} h_{cc} \mathbf{z} + \mathbf{n}_c, \tag{30}$$

where ϕ denotes the cancellation coefficient. Although the AN is known to Carol, it cannot be absolutely cancelled and, in practice, can be eliminated with a cancellation coefficient, ϕ, where $0 < \phi \le 1$ [30]. A low value of cancellation coefficient ϕ indicates that the self-interference has nearly been cancelled ($\phi \to 0$: total cancellation; $\phi = 1$: no cancellation). Since Carol does not know the presence of $\mathbf{u}$, the capacity of $\mathbf{v}$ considering $\mathbf{u}$ as noise is given by

$$I(\mathbf{v}; \mathbf{y}_c) = \log_2\left(1 + \frac{\alpha |h_{ac}|^2 P_a}{\sigma_n^2 + (1-\alpha)|h_{ac}|^2 P_a + \phi |h_{cc}|^2 P_c}\right). \tag{31}$$

Alice considers transmitting the overt message at a fixed rate R_v due to unknown h_{ac}. Since $|h_{ac}|^2$ has an exponential distribution with a mean of σ_{ac}^2 with its cumulative distribution function (CDF) of

$$\Pr(|h_{ac}|^2 < x) = 1 - \exp(-x/\sigma_{ac}^2) \tag{32}$$

and $|h_{cc}|^2$ has an exponential distribution with a mean of σ_{cc}^2 with its probability density function (PDF) of

$$p_{|h_{cc}|^2}(x) = \exp(-x/\sigma_{cc}^2)/\sigma_{cc}^2, \tag{33}$$

the probability of overt decoding the outage probability is obtained by

$$\begin{aligned}
P_{\text{out},C} &= \Pr(I(\mathbf{v};\mathbf{y}_c) < R_v) \\
&= \Pr\left(|h_{ac}|^2 < \frac{(2^{R_v}-1)(\sigma_n^2 + \phi |h_{cc}|^2 P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))P_a} \right) \\
&= 1 - \int_0^{\infty} \exp\left(- \frac{(2^{R_v}-1)(\sigma_n^2 + x\phi P_c)}{(\alpha - (1-\alpha)(2^{R_v}-1))^{+}\sigma_{ac}^2 P_a} \right) p_{|h_{cc}|^2}(x)dx \\
&= 1 - \frac{\exp\left(- \frac{(2^{R_v}-1)\sigma_n^2}{(\alpha-(1-\alpha)(2^{R_v}-1))^{+}P_a\sigma_{ac}^2} \right)}{1 + \frac{(2^{R_v}-1)\phi P_c \sigma_{cc}^2}{(\alpha-(1-\alpha)(2^{R_v}-1))^{+}P_a\sigma_{ac}^2}}.
\end{aligned} \tag{34}$$

The throughput (bits/Hz/s) of the overt message is given by

$$\eta_v = R_v \times (1 - P_{\text{out},C}). \tag{35}$$

To maximize the throughput of the overt message, the overt transmission rate R_v should be chosen properly by numerical search. When $\alpha = 1$ (no transmission of covert message), the overt throughput, denoted as $\eta_{v,nc}$, can be obtained from (34) and (35),

$$\eta_{v,nc} = \max_{R_v} R_v \times \frac{\exp(-(2^{R_v}-1)\sigma_n^2/(P_a\sigma_{ac}^2))}{1 + (2^{R_v}-1)\phi P_c \sigma_{cc}^2/(P_a\sigma_{ac}^2)}. \tag{36}$$

Therefore, we obtain from (35) and (36) that the overt throughput loss (bits/Hz/s) is given by

$$\eta_{v,\text{loss}} = \eta_{v,nc} - \eta_v, \tag{37}$$

which can be found by numerical search.

6. Numerical Results

The numerical results of the average detection error probability, ξ, the covert throughput, η_u, and the overt throughput loss, $\eta_{v,\text{loss}}$, under different values of the transmit SNR P_a/σ_n^2, the AN transmit SNR P_c/σ_n^2 and the cancellation coefficient ϕ are shown. For simplicity, we set $\sigma_{ij}^2 = 1$ for all i, j and, for any figure with a different value of σ_{ij}^2, it will be mentioned. Note that, throughout the simulation, the transmission rate R_v used to maximize the overt throughput η_v in (36) was firstly calculated and then used to compute the average detection error probability and the covert throughput.

6.1. Average Detection Error Probability At Warden Willie

Figure 3 illustrates the average detection error probability ξ versus P_a/σ_n^2 for different values of the AN transmit SNR, P_c/σ_n^2. It can be observed that the average detection error probability ξ decreases and converges to 0 as Alice's transmit power increases. The average detection error probability significantly increases as the AN transmit SNR, P_c/σ_n^2, increases, even if Willie perfectly knows the AN power, and converges to 1 for a high AN transmit SNR, as also shown in Figure 4 of ξ versus P_c/σ_n^2 for different values of ϕ. This indicates that the AN helps to improve the covertness because the warden fails to decode the covert message $\mathbf{u}$ when the AN power increases. It can also be observed that the warden's uncertainty (imperfect knowledge) in the received AN power can significantly increases the detection error (for example, a comparison between the line at $P_c/\sigma_n^2 = 0$ dB and that with perfect knowledge of the received AN power) and, thus, the mutual impact of decoding and AN uncertainty on the warden's detection error is critical.

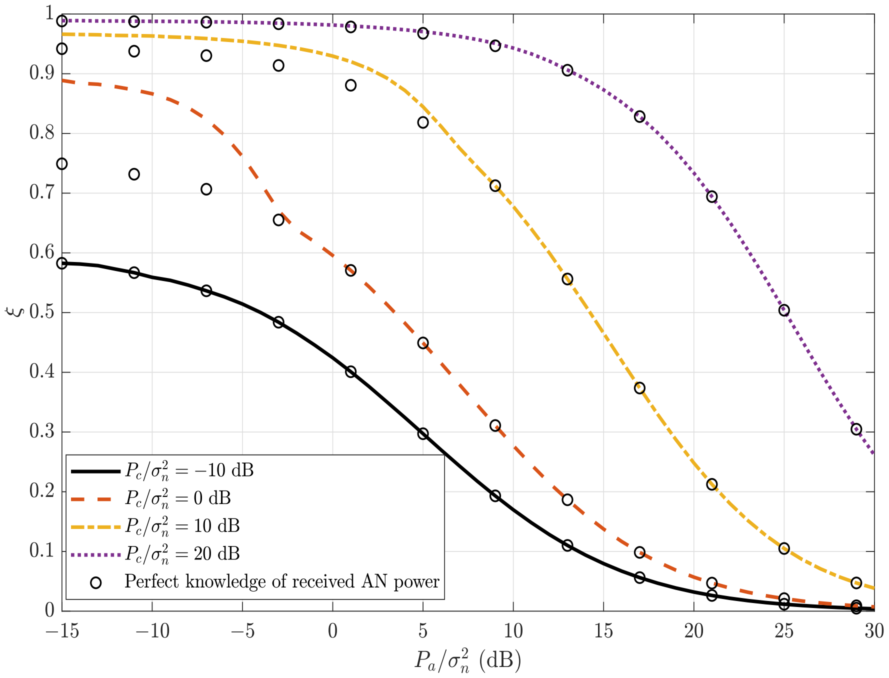

Figure 3. The average detection error probability, ξ, versus Alice's transmit power, P_a/σ_n^2, for different values of P_c/σ_n^2; $\alpha = 0.8$ and $\phi = 0.01$.

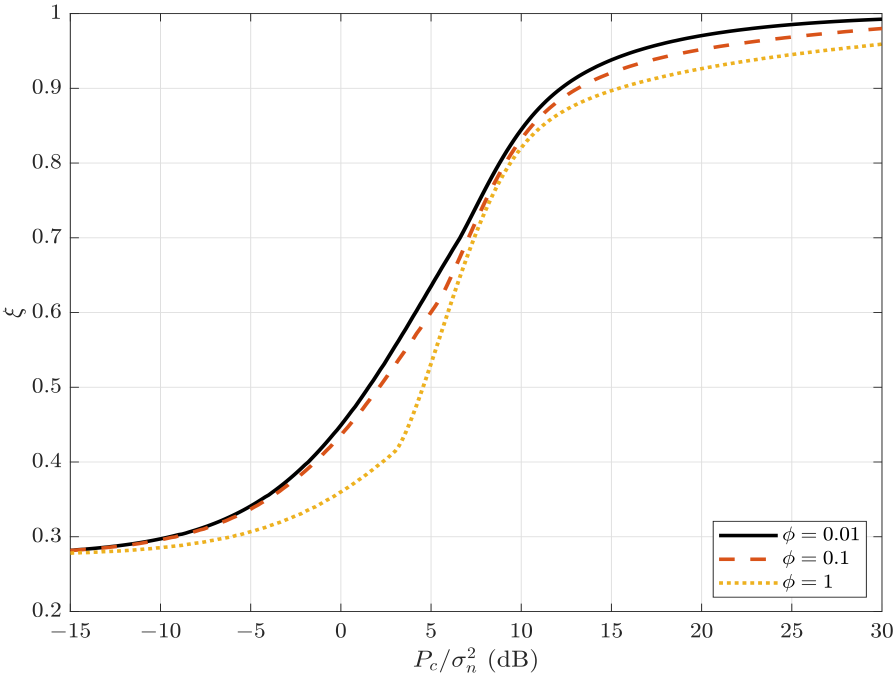

Figure 4. The average detection error probability, ξ, versus Carol's AN-transmit SNR, P_c/σ_n^2, for different values of ϕ; $\alpha = 0.8$ and $P_a/\sigma_n^2 = 5$ dB.

Figure 4 illustrates the average detection error probability versus Carol's AN transmit SNR, P_c/σ_n^2, for different values of ϕ. It can be observed that the average detection error probability increases as the cancellation coefficient, ϕ, decreases. This means that the improved performance of Carol's self-interference cancellation can also help to improve the covertness.

Figure 5 illustrates the average detection error probability, ξ, versus σ_{cw}^2 for different values of P_c/σ_n^2. It can be observed that the average detection error probability increases as σ_{cw}^2 increases (the warden is located close to the overt user) and that the increase is more significant for larger P_c/σ_n^2. This indicates the efficiency of the AN generated by the overt user to improve the covertness and also emphasizes that the improvement in the secure connection for the overt user results in an improvement in covertness for the covert user.

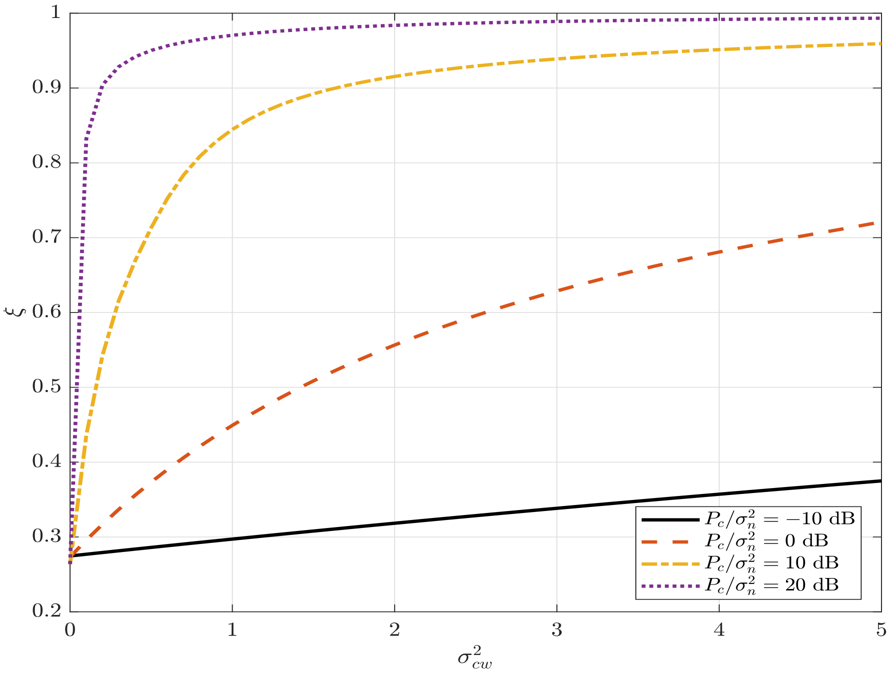

Figure 5. The average detection error probability, ξ, versus σ_{cw}^2 for different values of P_c/σ_n^2; $\alpha = 0.8$, $\phi = 0.01$ and $P_a/\sigma_n^2 = 5$ dB.

6.2. Covert Throughput and Overt Throughput Loss

Figure 6 presents the covert throughput versus R_u (bits/Hz/s) for different values of ϵ. It can be observed that there exists a unique transmission rate of the covert message to maximize the covert throughput; for example, regarding the covertness requirement of 0.1 ($\epsilon = 0.1$), the covert throughput is maximized at $R_u \simeq 0.42$. It can also be observed that the maximum covert throughput decreases significantly for a stricter covert requirement (ϵ decreases). For example, the maximum covert throughput of 0.028 (bits/Hz/s) for $\epsilon = 0.05$ is increased to 0.053 (bits/Hz/s) for $\epsilon = 0.1$.

Figure 7 presents the maximum covert throughput $\eta_{u,\max}$ versus σ_{cw}^2 for different values of ϕ. It can be observed that $\eta_{u,\max}$ increases significantly as σ_{cw}^2 increases and, thus, the AN will be more effective when Willie is located closer to Carol. It can also be observed that the covert throughput increases as ϕ decreases and the increase provided by the better performance of the self-interference cancellation is nearly constant. This indicates the positive impact of the overt receiver's performance of self-interference cancellation on the covert performance.

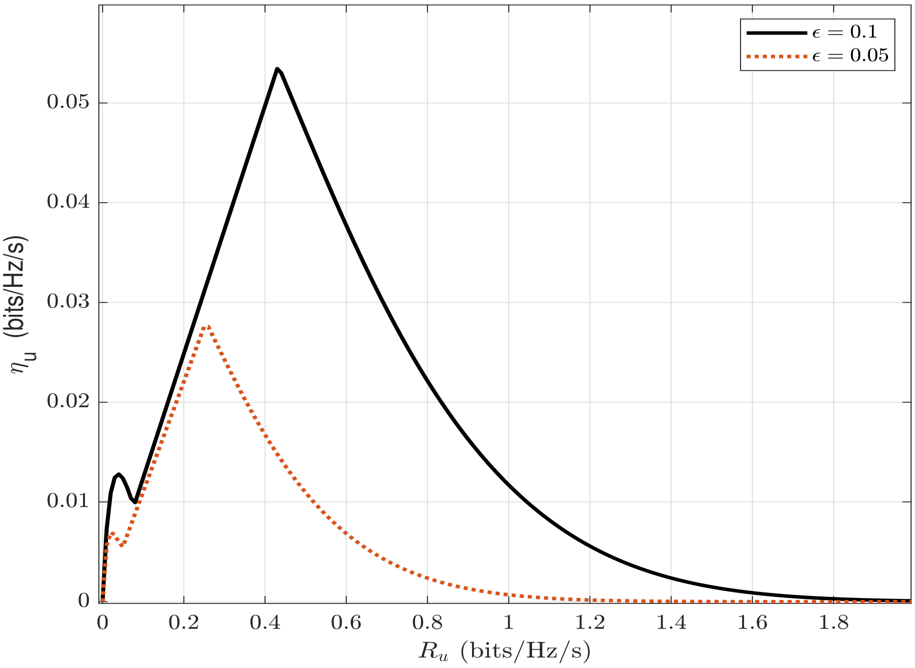

Figure 6. The covert throughput, η_u (bits/Hz/s), versus R_u, for different values of ϵ; $\alpha = 0.8$, $\phi = 0.01$ and $P_c/\sigma_n^2 = 5$ dB.

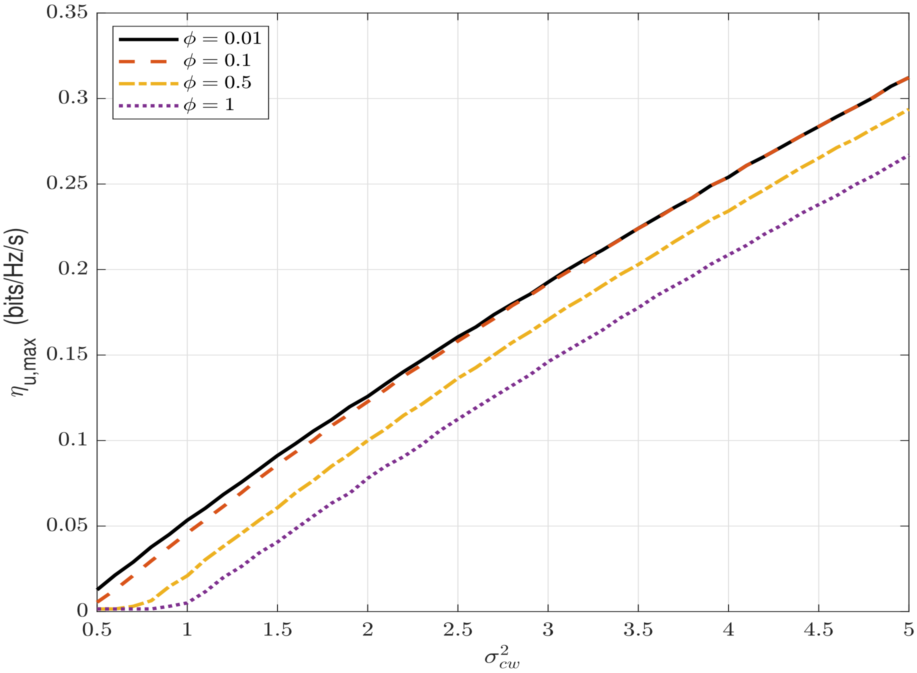

Figure 7. The maximum covert throughput, $\eta_{u,\max}$ (bits/Hz/s), versus σ_{cw}^2, for different values of ϕ; $\epsilon = 0.1$, $\alpha = 0.8$ and $P_c/\sigma_n^2 = 5$ dB.

Figure 8 presents the maximum covert throughput $\eta_{u,\max}$ versus σ_{cb}^2 for different values of ϕ. It can be observed that $\eta_{u,\max}$ decreases significantly as σ_{cb}^2 increases and, thus, the AN makes more interference when Bob is located closer to Carol. It can also be observed that the maximum covert throughput increases as ϕ decreases and the increase is more significant for smaller σ_{cb}^2. This indicates the mutual positive impact of the overt receiver's performance of self-interference cancellation and the location between Bob and Carol on the covert performance.

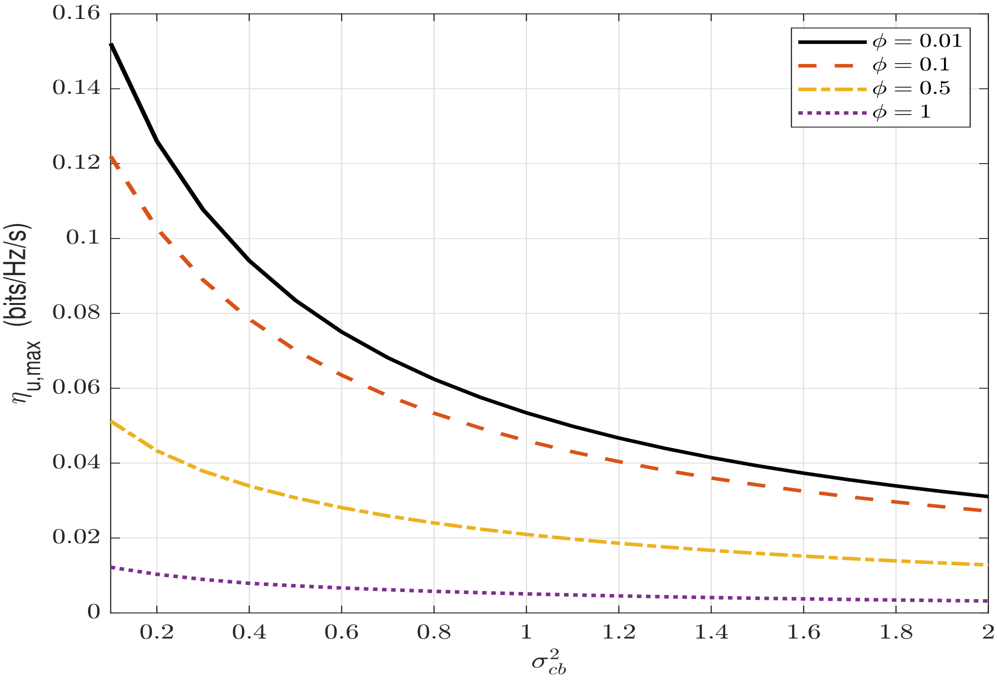

Figure 8. The maximum covert throughput, $\eta_{u,\max}$ (bits/Hz/s), versus σ_{cb}^2, for different values of ϕ; $\epsilon = 0.1$, $\alpha = 0.8$ and $P_c/\sigma_n^2 = 5$ dB.

Figures 9 and 10 show the maximum covert throughput $\eta_{u,\max}$ with the overt throughput, η_v, and the overt throughput loss $\eta_{v,loss}$ versus the AN transmit SNR P_c/σ_n^2, respectively, for different values of ϵ. It can be observed in Figure 9 that the covert throughput as well as the overt throughput increases as the transmit AN power, P_c/σ_n^2, increases. The increase in the covert and overt throughput is due to the increase in the maximum allowed transmission power P_a^*. However, in Figure 10, the overt throughput loss also increases significantly as the AN transmit SNR, P_c/σ_n^2, increases. This means that, in order to achieve a significant increase in the covert throughput by increasing AN's transmit power, it requires a trade of high overt throughput loss. For example, regarding $P_c/\sigma_n^2 = 30$ (dB) and $\epsilon = 0.1$, in order to obtain 0.12 (bits/Hz/s) of covert throughput, it requires an overt throughput loss of 0.22 (bits/Hz/s), which is higher than the covert throughput. It can be observed in both Figures 9 and 10 that the increase in covert throughput and overt throughput loss is less significant for stricter covert requirements (smaller ϵ).

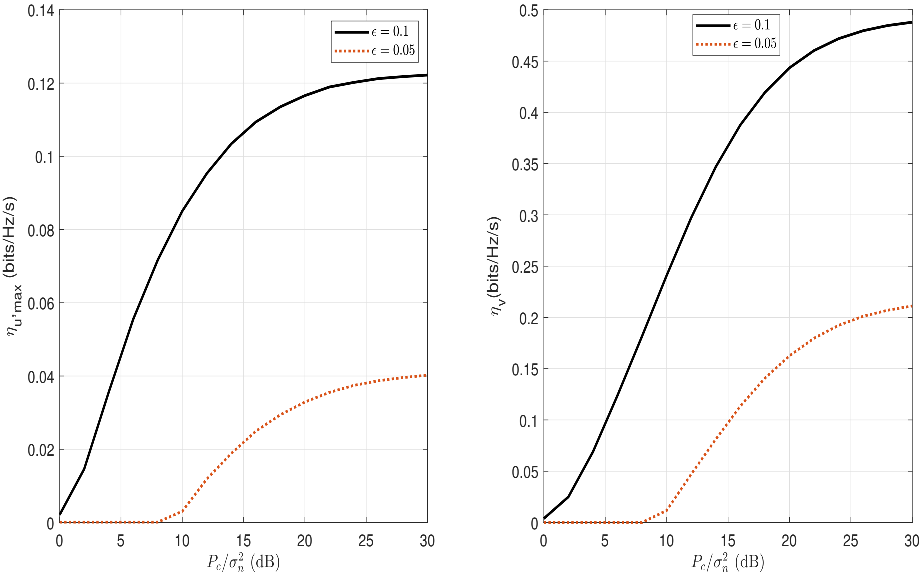

Figure 9. The maximum covert throughput, $\eta_{u,\max}$ (bits/Hz/s), and the overt throughput, η_v, versus the AN transmit SNR, P_c/σ_n^2, for different values of ϵ; $\phi = 0.1$ and $\alpha = 0.8$.

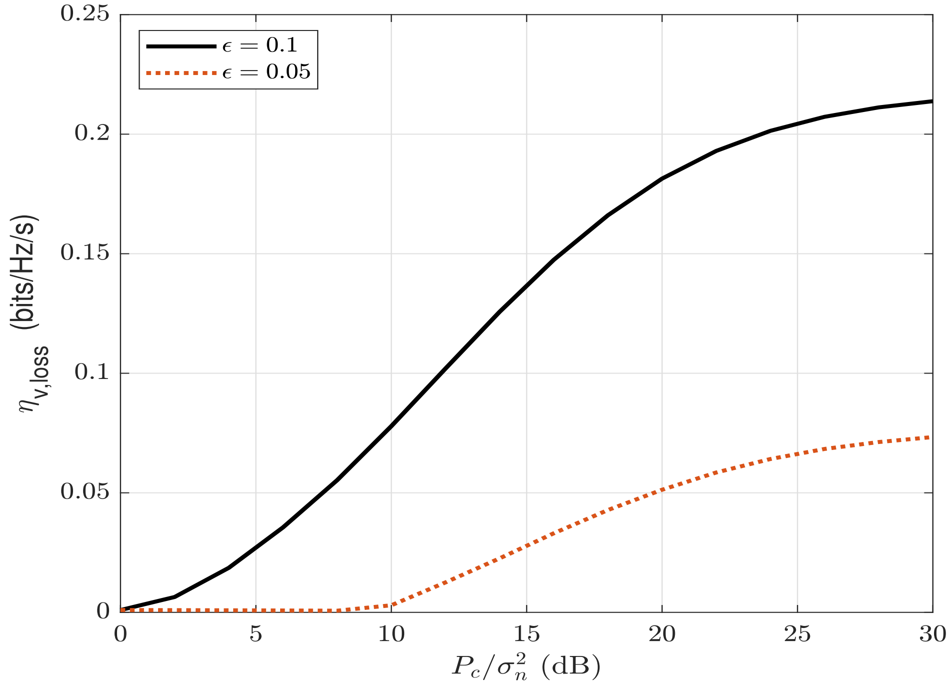

Figure 10. The overt throughput loss, $\eta_{v,\text{loss}}$ (bits/Hz/s), versus the AN transmit SNR, P_c/σ_n^2, for different values of ϵ; $\phi = 0.1$ and $\alpha = 0.8$.

In summary, the highlighted results are summarized in Table 2.

Table 2. Summary of key results.

	Pros	Cons
Average detection error probability	- increases when the AN power P_C increases - increases when the self-interference cancellation is improved (the cancel coefficient ϕ decreases) - increases when the warden is located close to the overt user (σ^2_{cw} increases)	
Covert throughput	- increases when the AN power P_C increases - increases when the self-interference cancellation is improved (the cancel coefficient ϕ decreases) - increases when the warden is located close to the overt user (σ^2_{cw} increases)	- decreases when the covert user is located close to the overt user (σ^2_{cb} increases)
Overt throughput loss		- high loss to increase the covert throughput - increases when ϵ increases

7. Conclusions and Discussion

This paper exploited the secure connection transmissions with a FD receiver to hide the covert information. The warden's uncertainties in decoding the overt message and AN-received power were used to guarantee the covertness. The average detection error probability, the covert throughput and the overt throughput loss were calculated. The results showed that AN generated by the overt user can help to improve the covertness and increase the maximum allowed transmit power, and, hence, the covert throughput. The covertness was further improved for the larger transmit power of AN; however, it requires the trade of high overt throughput loss. The result also showed that the improved performance of self-interference cancellation and secure connection at the overt receiver can help to improve the covertness, indicating the positive impact of the improved existing transmissions on the covert performance. In practice, FD communication is still understudied due to its hardware limitations and the requirement of modifying or creating/updating to a new protocol [31]. Consequently, our proposed scheme also has the potential to be implemented and tested on a hardware platform for civil or military applications, and the implementation can be more or less costly, depending on the techniques chosen and the scale of application.

Author Contributions: Conceptualization, L.L.N., T.-T.N., R.G. and H.Q.T.; data curation, L.L.N., T.-T.N., A.F. and H.Q.T.; formal analysis, L.L.N., A.F., R.G. and H.Q.T.; funding acquisition, A.F. and R.G.; investigation, L.L.N., R.G. and H.Q.T.; methodology, L.L.N., T.-T.N., R.G. and H.Q.T.; project administration, R.G.; resources, L.L.N.; software, L.L.N.; supervision, H.Q.T.; validation, T.-T.N., A.F., R.G. and H.Q.T.; visualization, L.L.N. and H.Q.T.; writing—original draft, L.L.N.; writing—review and editing, A.F., R.G. and H.Q.T. All authors have read and agreed to the published version of the manuscript.

Funding: This study was carried out in close international collaboration between the School of Electrical Engineering, International University, Vietnam National University of Ho Chi Minh city and Lab-STICC, University of Brest, France. This research is supported by the Brest Institute of Computer Science and Mathematics (IBNM) CyberIoT Chair of Excellence of the University of Brest.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

In this Appendix, we prove (6). Since v_i, $1 \le i \le n$, is identical and has a complex normal distribution with a PDF of

$$f(v_i|H_0) = \exp(-|v_i|^2)/\pi. \tag{A1}$$

Then, we obtain from (5) that

$$E_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_0)] = E_{\mathbf{v}}\left[\frac{\exp\left(-\frac{||\mathbf{y}_w - h_{aw}\sqrt{P_a}\mathbf{v}||^2}{\sigma_n^2 + |h_{cw}|^2 P_c}\right)}{(\pi(\sigma_n^2 + |h_{cw}|^2 P_c))^n}\right] \tag{A2}$$

$$= \frac{\prod_{i=1}^n \int_{v_i} \exp\left(-\frac{|y_{w,i} - h_{aw}\sqrt{P_a}v_i|^2}{\sigma_n^2 + |h_{cw}|^2 P_c}\right)\exp(-|v_i|^2)dv_i}{(\pi^2(\sigma_n^2 + |h_{cw}|^2 P_c))^n}. \tag{A3}$$

Let $h_{aw} = |h_{aw}|e^{j\rho}$ and $\tilde{v}_i = v_i e^{j\rho}$. Then, the PDF of $\tilde{v}_i$ is identical to (A1) and, hence, we obtain

$$E_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_0)] = \frac{\prod_{i=1}^n \int_{v_i} \exp\left(-\frac{|y_{w,i} - |h_{aw}|\sqrt{P_a}\tilde{v}_i|^2}{\sigma_n^2 + |h_{cw}|^2 P_c}\right)\exp(-|\tilde{v}_i|^2)dv_i}{(\pi^2(\sigma_n^2 + |h_{cw}|^2 P_c))^n}. \tag{A4}$$

For real values of t and z, one can show that

$$\int_{-\infty}^{\infty} \exp(-(t - |h_{aw}|^2\sqrt{P_a}z)^2/a)\exp(-z)dz = \sqrt{\frac{\pi a P_a}{a + |h_{aw}|^2 P_a}}\exp(-t/(a + |h_{aw}|^2 P_a)). \tag{A5}$$

Then, it can be obtained from (A4) that

$$E_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_0)] = \frac{\prod_{i=1}^n \exp\left(-\frac{|y_{w,i}|^2}{\sigma_n^2 + |h_{cw}|^2 P_c + |h_{aw}|^2 P_a}\right)}{(\pi(\sigma_n^2 + |h_{cw}|^2 P_c + |h_{aw}|^2 P_a))^n} \tag{A6}$$

$$= \frac{\exp\left(-\frac{||\mathbf{y}_w||^2}{\sigma_n^2 + |h_{cw}|^2 P_c + |h_{aw}|^2 P_a}\right)}{(\pi(\sigma_n^2 + |h_{cw}|^2 P_c + |h_{aw}|^2 P_a))^n}. \tag{A7}$$

Similarly,

$$E_{\mathbf{v}}[\Pr(\mathbf{y}_w|\mathbf{v}, H_1)] = \frac{\prod_{i=1}^n \int_{v_i} \exp\left(-\frac{|y_{w,i} - h_{aw}\sqrt{\alpha P_a}v_i|^2}{\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a}\right)\exp(-|v_i|^2)dv_i}{(\pi^2(\sigma_n^2 + |h_{cw}|^2 P_c + (1-\alpha)|h_{aw}|^2 P_a))^n} \tag{A8}$$

$$= \frac{\exp\left(-\frac{||\mathbf{y}_w||^2}{\sigma_n^2 + |h_{cw}|^2 P_c + |h_{aw}|^2 P_a}\right)}{(\pi(\sigma_n^2 + |h_{cw}|^2 P_c + |h_{aw}|^2 P_a))^n}, \tag{A9}$$

where (A9) is also derived following (A5).

Appendix B

In this Appendix, we find the optimal detection threshold used to minimize $(P'_f(h_{aw}) + P'_m(h_{aw}))$ and its resulting minimum. Let $x = 1/\lambda'$. Since $r_1 \geq r_0$, $s_0 \geq s_1$, $\delta_0 \geq \delta_1$, it follows from (14) and (15) that

$$\begin{aligned} & P'_f(h_{aw}) + P'_m(h_{aw}) \\ = & \begin{cases} 1 - \exp(-\delta_0), & x \geq \frac{s_0+\delta_0}{r_0}, \\ 1 - \exp(-(r_0 x - s_0)), & \frac{s_1+\delta_1}{r_1} \leq x < \frac{s_0+\delta_0}{r_0}, \\ 1 - \exp(-(r_0 x - s_0)) + \exp(-(r_1 x - s_1)) - \exp(-\delta_1), & x < \frac{s_1+\delta_1}{r_1}. \end{cases} \end{aligned} \tag{A10}$$

It follows from the second function of (A10) that $(P'_f(h_{aw}) + P'_m(h_{aw}))$ is an increasing function of x for $(s_1 + \delta_1)/r_1 \leq x < (s_0 + \delta_0)/r_0$ and, hence, $(P'_f(h_{aw}) + P'_m(h_{aw}))$ is minimized at $x = (s_1 + \delta_1)/r_1$ and maximized at $x = (s_0 + \delta_0)/r_0$. Then, the minimum of $(P'_f(h_{aw}) + P'_m(h_{aw}))$ can be found by finding the optimum detection threshold and minimum of

$$P'_f(h_{aw}) + P'_m(h_{aw}) = 1 - \exp(s_0 - r_0 x) + \exp(s_1 - r_1 x) - \exp(-\delta_1), \tag{A11}$$

for $x < (s_1 + \delta_1)/r_1$. Taking the first derivative and setting (A11) to zero yields

$$x = \min\{(\ln(r_1/r_0) - (s_0 - s_1))/(r_1 - r_0), (s_1 + \delta_1)/r_1\} \tag{A12}$$

and, then, the resulting minimum of $(P'_f(h_{aw}) + P'_m(h_{aw}))$.

References

1. Talbot, J.; Welsh, D. *Complexity and Cryptograhpy: An Introduction*; Cambrige University Press: Cambrige, UK, 2006.
2. Phan, V.D.; Nguyen, T.N.; Le, A.V.; Voznak, M. A Study of Physical Layer Security in SWIPT-Based Decode-and-Forward Relay Networks with Dynamic Power Splitting. *Sensors* **2021**, *21*, 5692. [CrossRef] [PubMed]
3. Youn, J.; Son, W.; Jung, B.C. Physical-layer security improvement with reconfigurable intelligent surfaces for 6G wireless communication systems. *Sensors* **2021**, *21*, 1439. [CrossRef] [PubMed]
4. Silva, A.; Gomes, M.; Vilela, J.P.; Harrison, W.K. SDR Proof-of-Concept of Full-Duplex Jamming for Enhanced Physical Layer Security. *Sensors* **2021**, *21*, 856. [CrossRef] [PubMed]
5. Bash, B.A.; Goeckel, D.; Towsley, D. Limits of reliable communication with low probability of detection on AWGN channels. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1921–1930. [CrossRef]
6. Che, P.H.; Bakshi, M.; Jaggi, S. Reliable deniable communication: Hiding messages in noise. In Proceedings of the IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013; pp. 2945–2949.
7. Bloch, M.R. Covert communication over noisy channels: A resolvability perspective. *IEEE Trans. Inf. Theory* **2016**, *62*, 2334–2354. [CrossRef]
8. Wang, L.; Wornell, G.W.; Zheng, L. Fundamental limits of communication with low probability of detection. *IEEE Trans. Inf. Theory* **2016**, *62*, 3493–3503. [CrossRef]
9. Tahmasbi, M.; Bloch, M.R. First-and second-order asymptotics in covert communication. *IEEE Trans. Inf. Theory* **2018**, *65*, 2190–2212. [CrossRef]
10. Yan, S.; Cong, Y.; Hanly, S.V.; Zhou, X. Gaussian signalling for covert communications. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 3542–3553. [CrossRef]
11. Tandra, R.; Sahai, A. SNR walls for signal detection. *IEEE J. Sel. Top. Signal Process.* **2008**, *2*, 4–17. [CrossRef]
12. Lee, S.; Baxley, R.J.; Weitnauer, M.A.; Walkenhorst, B. Achieving Undetectable Communication. *IEEE J. Sel. Top. Signal Process.* **2015**, *9*, 1195–1205. [CrossRef]
13. He, B.; Yan, S.; Zhou, X.; Lau, V.K.N. On Covert Communication With Noise Uncertainty. *IEEE Commun. Lett.* **2017**, *21*, 941–944. [CrossRef]
14. Bash, B.A.; Goeckel, D.; Towsley, D. Covert communication gains from adversary's ignorance of transmission time. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 8394–8405. [CrossRef]
15. Ta, H.Q.; Kim, S.W. Covert communication under channel uncertainty and noise uncertainty. In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
16. Yan, S.; He, B.; Zhou, X.; Cong, Y.; Swindlehurst, A.L. Delay-intolerant covert communications with either fixed or random transmit power. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 129–140. [CrossRef]
17. Goeckel, D.; Bash, B.; Guha, S.; Towsley, D. Covert Communications When the Warden Does Not Know the Background Noise Power. *IEEE Commun. Lett.* **2016**, *20*, 236–239. [CrossRef]
18. Shmuel, O.; Cohen, A.; Gurewitz, O. Multi-Antenna Jamming in Covert Communication. *IEEE Trans. Commun.* **2021**, *69*, 4644–4658. [CrossRef]

19. 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]
20. 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]
21. 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.
22. Hu, J.; Yan, S.; Zhou, X.; Shu, F.; Li, J.; Wang, J. Covert communication achieved by a greedy relay in wireless networks. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 4766–4779. [CrossRef]
23. Tao, L.; Yang, W.; Yan, S.; Wu, D.; Guan, X.; Chen, D. Covert communication in downlink NOMA systems with random transmit power. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 2000–2004. [CrossRef]
24. Kim, S.W.; Ta, H.Q. Covert Communications over Multiple Overt Channels. *IEEE Trans. Commun.* **2021**, *70*, 1112–1124. [CrossRef]
25. Zhou, X.; McKay, M.R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [CrossRef]
26. Arumugam, K.S.K.; Bloch, M.R. Embedding covert information in broadcast communications. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2787–2801. [CrossRef]
27. Axell, E.; Leus, G.; Larsson, E.G.; Poor, H.V. Spectrum sensing for cognitive radio: State-of-the-art and recent advances. *IEEE Signal Process. Mag.* **2012**, *29*, 101–116. [CrossRef]
28. Polyanskiy, Y.; Poor, H.V.; Verdú, S. Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theory* **2010**, *56*, 2307–2359.
29. Shi, L.; Li, Z.; Bi, X.; Liao, L.; Xu, J. Full-duplex multi-hop wireless networks optimization with successive interference cancellation. *Sensors* **2018**, *18*, 4301. [CrossRef] [PubMed]
30. Everett, E.; Sahai, A.; Sabharwal, A. Passive self-interference suppression for full-duplex infrastructure nodes. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 680–694. [CrossRef]
31. Kolodziej, K.E. *In-Band Full-Duplex Wireless Systems Handbook*; Artech House: Norwood, MA, USA, 2021.