Covert Wireless Communications With Channel Inversion Power Control in Rayleigh Fading

Jinsong Hu, *Member, IEEE*, Shihao Yan, *Member, IEEE*, Xiangyun Zhou, *Senior Member, IEEE*, Feng Shu, *Member, IEEE*, and Jun Li, *Senior Member, IEEE*

***Abstract*—In this work, we adopt channel inversion power control (CIPC) to achieve covert communications aided by a full-duplex receiver. Specifically, the transmitter varies the power and phase of transmitted signals as per the channel to the receiver, such that the receiver can decode these signals without knowing the channel state information. This eliminates the required feedback from the transmitter to the receiver, which aids hiding the transmitter from a warden. The truncated CIPC and conventional CIPC schemes are proposed and examined, where for truncated CIPC covert transmission ceases when the channel quality from the transmitter to the receiver is low, while for conventional CIPC covert transmission always occurs regardless of this channel quality. We examine their performance in terms of the achieved effective covert throughput (ECT), which quantifies the amount of information that the transmitter can reliably convey to the receiver, subject to the constraint that the warden's detection error probability is no less than some specific value. Our examination shows that the truncated CIPC scheme can outperform the conventional CIPC scheme due to this constraint.**

***Index Terms*—Physical layer security, covert communications, full duplex, artificial noise.**

I. Introduction

With the ever-increasing use of the Internet of Things (IoT), various types of small devices are becoming part of the wireless connected world, whose overall goal is to improve the quality of our daily life. In a wide range of application scenarios, the security of IoT is a critical issue. For example, in health-care systems, some wireless sensors collect patients' health information such as heart rate and blood pressure. This type of information is private and highly confidential and hence a secure transmission is of a high demand. However, due to broadcast nature of the wireless medium, the transmission in IoT can be easily detected or eavesdropped on by unauthorized users [1], [2].

Traditional security techniques offer protection against eavesdropping through encryption [3], [4], guaranteeing the integrity of messages over the air. However, it has been shown in the recent years that even the most robust encryption techniques can be defeated by a powerful adversary (e.g., a quantum computer) [5]. Meanwhile, physical layer security, on the other hand, exploits the dynamic characteristics of the wireless medium to preserve the confidentiality of the transmitted information in wireless networks [6]–[10]. For example, the authors in [10] proposed a new scheme to enhance the secure communications of both primary and secondary users in the underlay multiple-input multiple-output cognitive-radio network with the aid of a bi-directional zero-forcing beamformer. On the contrary, apart from protecting the content of communication by using physical layer security techniques, covert communications (also termed low probability of detection communications) are emerging as new and cutting-edge wireless communication security techniques, which aim to enable a wireless transmission between two users while guaranteeing a negligible probability of detecting this transmission at a warden [11]–[16]. It is worth noting that covert communication is about hiding the existence/action of communication. It assumes that the attacker wants to know whether transmission has happened or not. Its scope does not include whether the message transmitted is decoded by the attacker (or eavesdropper), i.e., decoding of the message is not relevant to covert communication problem. In some practical situations, attackers only want to know whether the action of communication has happened, because knowing the action of communication may be sufficient for the attacker to make its decision on what to do next. For example, when detecting there is a suspicious communication in the battlefield, the attacker can send out a troop to investigate the situation. In this situation, it is not practical for the attacker to simply assume that communication is always happening, because this then requires the attacker to send out a troop to investigate all the time. This is why and where the study of covert communication becomes important.

In the literature, the fundamental limit of covert communications over additive white Gaussian noise (AWGN) channels has been studied in [11]. It is proved that $\mathcal{O}(\sqrt{n})$ bits of information

Manuscript received December 19, 2018; revised May 2, 2019 and July 31, 2019; accepted October 20, 2019. Date of publication October 24, 2019; date of current version December 17, 2019. This work was supported in part by National Key R&D Program under Grant 2018YFB1004800 and in part by National Natural Science Foundation of China under Grants 61771244, 61727802, 61872184, and 61901121. The review of this article was coordinated by Dr. S. Majhi. *(Corresponding author: Shihao Yan.)*

J. Hu is with the College of Physics and Information, Fuzhou University, Fuzhou 350116, China, and also with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: jinsong.hu@fzu.edu.cn).

S. Yan is with the School of Engineering, Macquarie University, Sydney, NSW 2109, Australia (e-mail: shihao.yan@mq.edu.au).

X. Zhou is with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

F. Shu is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China, and also with the School of Information and Communication Engineering, Hainan University, Hainan 570228, China (e-mail: shufeng0101@163.com).

J. Li is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: jun.li@njust.edu.cn).

Digital Object Identifier 10.1109/TVT.2019.2949304

can be transmitted to a legitimate receiver reliably and covertly in n channel uses as $n \to \infty$. Following [11], covert communications have been studied in a few scenarios. For example, covert communications can be achieved when the warden has uncertainty about the receiver noise power [17]. In [18], the authors adopted a friendly jammer, which generates artificial noise to create uncertainty at the warden Willie, in order to help achieve covert communications. The authors of [19] considered covert communications with a Poisson field of interferers, in which it was proved that the density and the transmit power of the interferers do not affect the covert communication performance when the network stays in the interference-limited regime. The covert communication with interference uncertainty from non-cooperative transmitters is studied in [20]. The effect of finite blocklength (i.e., short delay constraints) over AWGN channels on covert communications was examined in [21], which proves that the effective throughput of covert communications is maximized when all available channel uses are utilized. A covert communication system under block fading channels was examined in [22], [23], where transceivers have uncertainty on the related channel state information (CSI). Covert communications in the context of relay networks was examined in [24], [25], which shows that a relay can transmit confidential information to the corresponding destination covertly on top of forwarding the source's message. In [26], the optimality of Gaussian signalling was examined in the context of covert communications with two different constraints, where Gaussian signalling was proved to be optimal for one covert communication constraint, but not optimal the other one.

The aforementioned works in the literature mainly focused on how to hide the wireless transmission action (not the transmitter itself), since some information that can indicate the existence of the transmitter was assumed a priori known. For example, in [17], [21], [22], [24], [27] it is assumed that the instantaneous wireless channels from the transmitter to the warden are known by the warden, which means that the warden knows the existence of the transmitter and is to detect whether a wireless transmission occurs. We note that the ultimate goal of covert communications is to achieve a shadow wireless network [12], in which the transmitter itself should be hidden from the warden. If the existence of the transmitter in covert communication system is known to the warden with the prior knowledge, the transmitter may suffer a fatal attack from warden directly and not to mention the further transmission. In other words, the unauthorized node cannot know the existence of transmitter when transmitter keep passive and never transmits signals before, which is assumed in our work. For example, the hiding of UAV's existence in some sensitive areas is a critical task for covert communications. In general, the main challenges in the detection of UAV with aid of traditional measures like visual detection are the high mobility, the small size of the target, and some low visibility scenarios (e.g, in the night). Since the covert transmission along with radio wave propagation, the detection for transmission is a quite direct way to implement at a warden. In [28]–[30], the authors utilized an artificial-noise-aided full-duplex receiver to achieve covert communications in wireless fading channels with the important difference that the CSI is assumed to be perfectly known to the warden in [28], [29]. We note that in [30] it was assumed that Willie only knows the channel distribution information, while, however, it was assumed that Bob knows the CSI perfectly. In addition, in [30] it has not been clarified how to prevent Willie from knowing the CSI while enabling Bob to know the CSI perfectly. In this work, we adopt the channel inversion power control (CIPC) at the transmitter (Alice) to achieve covert communications, in which the transmitter varies the power and phase of its transmitted signals as per the channel from itself to the receiver (Bob) in order to keep the signal power at the receiver equal to a certain constant value. As such, in the CIPC schemes adopted in this work, neither Bob nor Willie knows the corresponding CSI perfectly, since initially Alice does not transmit any (pilot) signal at all. Therefore, this work can aid hiding the transmitter Alice, while [28], [29] can only hide the transmission action of a known transmitter (due to the assumed known CSI). Relative to [30], this work newly propose the CIPC schemes with detailed performance analysis, which clarifies how to avoid Willie from knowing the CSI (thus knowing the existence of Alice) while guaranteeing reliable communication to Bob (without requiring Bob to know the CSI).

Hiding the wireless transmission aims to enable a communication from transmitter to receiver while guaranteeing a negligible detection probability of this communication at a warden. While hiding the transmitter means the transmitter means not letting anyone know there exists such a communication node. This work aim at an initial step towards to hiding the transmitter by removing the requirement on such CSI, because this information can indicate the existence of the transmitter. In a standard (non-covert) communication system, CIPC can significantly decreases the outage probability [31]. It is well known that the truncated CIPC scheme is more general, which includes the conventional CIPC scheme as a special case with the maximum value of the transmit power approaches the infinity and can achieve the minimum value of the outage probability. However, when considering covert communications, conventional CIPC scheme might make it easy for the signal to be observed at Willie and hence its utility is less clear, which motivates us to consider the these two CIPC scheme and compare their performance in this work. Moreover, the IoT device (e.g., Alice) is usually equipped with a single antenna each and could not cooperate in the typical application scenario of IoT [32]. As such, the receiver Bob as more powerful base station can use an additional antenna to transmit artificial noise (AN) for further degrading the detection performance of Willie.

Our main specific contributions are summarized as below.

- We adopt the CIPC at the transmitter to achieve covert communications, in which the transmitter varies its transmitted signal power as per the channel from itself to the receiver, such that the received power of the covert information signal is a fixed value Q. With channel reciprocity, this strategy does not require the transmitter to transmit pilot signals for channel estimation or to feed back the estimated channel to the receiver before covert communications, which can potentially aid hiding the transmitter. In this work, two

specific CIPC schemes are studied and the performance of these two covert transmission schemes is thoroughly examined.

- We first consider the truncated CIPC scheme, where the covert transmission ceases when the quality of the channel from the transmitter to the receiver is lower than a specific value determined by the maximum transmit power. For this scheme, we analyze the detection performance at the warden, based on which we determine the effective covert throughput (ECT) that quantifies the amount of information that can be conveyed from the transmitter to the receiver subject to the warden's detection error probability being no less than some specific value. Specifically, the detection error probability at the warden is derived in a closed-form expression, which leads to that the optimal detection threshold is analytically achieved. This analysis enables us to determine the optimal value of Q that maximizes the ECT for the truncated CIPC scheme.
- We also consider the conventional CIPC scheme as a benchmark to examine the performance limit of CIPC in an asymptotic scenario, where there is no maximum power constraint at the transmitter and the covert transmission always occurs regardless of the channel quality. Solid examination on this scheme has been conducted, since mathematically the conventional CIPC scheme cannot be regarded as a special case of the truncated CIPC scheme. For the conventional CIPC scheme, our analysis shows that the value of Q can be varied to counteract the impact of the transmit power of AN on the warden's detection performance and thus the achieved ECT approaches an analytical derived upper bound as the maximum transmit power of AN tends to infinity.

The rest of this paper is organized as follows. Section II details our system model and adopted assumptions. In Section III, we examine the performance the truncated CIPC scheme in the context of covert communications. Section IV presents our analysis on the conventional CIPC scheme. Section V provides numerical results to confirm our analysis and provide useful insights with regard to the comparison between these two schemes. Finally, conclusions are drawn in Section VI.

Notation: Scalar variables are denoted by italic symbols. Vectors are denoted by lower-case boldface symbols. Given a complex vector, $(\cdot)^\dagger$ denotes the conjugate transpose. Given a complex number, $|\cdot|$ denotes its modulus and $(\cdot)^*$ denotes the conjugation.

II. System Model

A. Considered Communication Scenario

As shown in Fig. 1, we consider a wireless communication scenario, where Alice (i.e., the transmitter) wants to transmit information covertly to Bob, while trying to hide herself from Willie (i.e., the warden). Meanwhile, Willie is to detect Alice's transmission by observing the wireless environment. We assume the wireless channels within our system model are subject to independent quasi-static Rayleigh fading with equal block length, which means that all the channel coefficients are independent

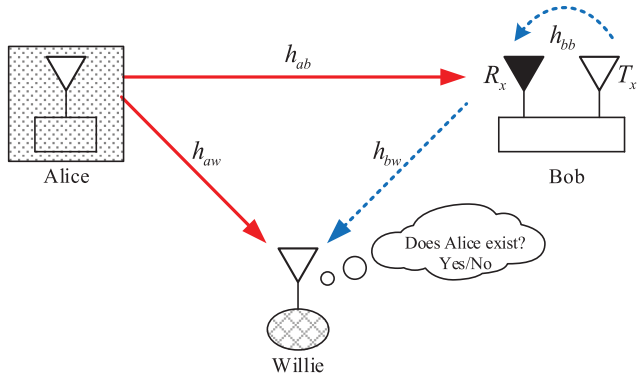


Fig. 1. Covert communications network model.

and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with zero-mean and unit-variance. Time is slotted and the quasi-static Rayleigh fading channel coefficient remains fixed for a slot. Alice and Willie are assumed to have a single antenna, while besides the single receiving antenna, Bob uses an additional antenna for transmission of AN in order to deliberately confuse Willie. The channel from Bob to Alice, Bob to Willie, Bob to Bob, Alice to Bob, or Alice to Willie, is denoted by h_j and the mean value of $|h_j|^2$ is denoted by λ_j, where the subscript j can be ba, bw, bb, ab, aw, respectively. For j is ba, bb, ab. these values can be known as a prior. For the channels from Alice to Willie or Bob to Willie, we can obtain the values of λ_{aw} and λ_{bw} when consider the worst-case scenario or get these value from the history observation data (e.g., Willie can possibly know the suspicious area of Alice). For example, the location of Alice can be assumed at an annular region centered on the location of Willie, which is similar to the annulus threat model mentioned in [33]. Then, we can obtain the approximate value of λ_{aw} in a statistical way.

In order to achieve the ultimate goal of hiding the presence of Alice, in the considered scenario as a base station Bob broadcasts pilots periodically in order to enable Alice's estimation of the channel from Bob to Alice (i.e., h_{ba}). Meanwhile, Willie can estimate the channel from Bob to Willie (i.e., h_{bw}), since the pilots transmitted by Bob are publicly known. Considering channel reciprocity, we assume the channel from Alice to Bob is the same as h_{ba}. Since Alice does not transmit any pilots, it is assumed that both Bob and Willie do not know their corresponding channels, h_{ab} and h_{aw}. In order to assist Bob with decoding with no instantaneous channel information, in this work we consider the CIPC at Alice, in which Alice varies its transmit power as per h_{ab} such that $P_a|h_{ab}|^2$ is a fixed value, i.e.,

$$P_a|h_{ab}|^2 = Q, \tag{1}$$

where P_a is the transmit power of Alice.

It should be noted that the proposed CIPC scheme is to achieve covert communications in wireless fading channels without the need for Alice to transmit training signals for Bob to perform channel estimation. This can ensure the existence of Alice is hidden from being detected. Meanwhile, using the constant transmit power scheme commonly requires Alice to transmit training signals for Bob to estimate the channel, which easily

reveals Alice' s existence. Therefore, it is not appropriate to include constant transmit power scheme for comparison.

Considering some specific quality of service (QoS) requirements, we consider that the transmission throughput from Alice to Bob is fixed and predetermined, which is denoted by R. As such, transmission from Alice to Bob incurs outage when $C_{ab} < R$, where C_{ab} is the channel capacity from Alice to Bob. Then, the transmission outage probability is given by

$$\delta = \mathcal{P}[C_{ab} < R]. \tag{2}$$

As such, in this work we adopt the effective covert throughput as the main performance metric for the communication from Alice to Bob.

Next, we detail the transmission from Alice to the full-duplex Bob and derive the associated transmission outage probability. As a practical technique, the full-duplex radio has been widely explored in wireless communications (e.g., [34], [35]). For example, using a full-duplex receiver to generate AN for security enhancement has been widely examined the context of physical layer security (e.g., [28], [36], [37]). Similarly to [28], we consider a full-duplex receiver Bob who simultaneously receives covert information signal from Alice and transmits AN with a random power to confuse the warden Willie on detecting the covert transmission. Generating AN by the full-duplex Bob enables varying the presence and amount of uncertainty at Willie on demand, which leads to that the covert communication between Alice and Bob is fully under the control of Alice and Bob. When Alice transmits the covert information, the signal received at the full-duplex Bob is given by

$$\mathbf{y}_b[i] = \sqrt{P_a} h_{ab} \mathbf{x}_a[i] + \sqrt{\phi P_b} h_{bb} \mathbf{v}_b[i] + \mathbf{n}_b[i], \tag{3}$$

where $\mathbf{x}_a$ is the signal transmitted by Alice, and $\mathbf{n}_b[i]$ is the AWGN at Bob with σ_b^2 as its variance, i.e., $\mathbf{n}_b[i] \sim \mathcal{CN}(0, \sigma_b^2)$, $\mathbf{v}_b$ is the AN signal transmitted by Bob satisfying $\mathbb{E}[\mathbf{v}_b[i]\mathbf{v}_b^\dagger[i]] = 1$, h_{bb} denotes the self-interference channel at Bob (i.e., the channel between Bob's transmitting antenna and Bob's receiving antenna), and P_b is Bob's transmit power of the AN signal. In this work, we adopt a generalized self-interference cancellation model, in which the self-interference can be fully cancelled (i.e., $\phi = 0$) or cannot be fully cancelled (i.e., $0 < \phi \leq 1$), where ϕ in (3) denotes the self-interference cancellation coefficient [38]. In practice, the self-interference may not be fully cancelled due to the fact that self-interference channel may not be perfectly estimated in some specific scenarios [39]. We note that $0 \leq \phi \leq 1$ corresponds to different self-interference cancellation levels [40]. In order to remove the impact of the phase in the complex channel coefficient, Alice has to pre-process the transmitted signal $\mathbf{x}_a$ as

$$\mathbf{x}_a = \frac{h_{ab}^*}{|h_{ab}|} \mathbf{x}_r, \tag{4}$$

where $\mathbf{x}_r$ is the raw information signal satisfying $\mathbb{E}[\mathbf{x}_a[i]\mathbf{x}_a^\dagger[i]] = 1$, $i = 1, 2, \ldots, n$ is the index of each channel use.

In order to create uncertainty at Willie, in this work we assume that P_b changes randomly from slot to slot [18], [41] and follows a continuous uniform distribution over the interval $[0, P_b^{\max}]$ with probability distribution function given by

$$f_{P_b}(x) = \begin{cases} \frac{1}{P_b^{\max}} & \text{if } 0 \leq x \leq P_b^{\max}, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Since Willie possesses the knowledge of h_{bw} in the slot under consideration, for a constant transmit power at Bob, it is straightforward for him to detect the covert transmission when the additional power (on top of his receiver noise power) is received. The purpose of introducing randomness in Bob's transmit power is to create uncertainty in Willie's received power, such that Willie is unsure whether an increase in his received power is due to Alice's transmission or simply due to a variation in Bob's transmit power of the AN signal. We note that we consider the uniform distribution as an initial example and other distributions will be explored in our future works.

B. Detection Performance at Willie

In the considered communication scenario, Willie is to infer the presence of Alice by detecting the wireless transmission from Alice to Bob. As such, Willie has a binary detection problem, in which Alice does not transmit information to Bob in the null hypothesis $\mathcal{H}_0$ but it does in the alternative hypothesis $\mathcal{H}_1$. The ultimate goal for Willie is to detect whether his observation comes from $\mathcal{H}_0$ or $\mathcal{H}_1$ by applying some specific decision rule. The detection performance of Willie is normally measured by the detection error probability, which is defined as

$$\mathcal{P}_e \triangleq \pi_0 \alpha + \pi_1 \beta, \tag{6}$$

where $\mathcal{P}(\mathcal{H}_1) = \pi_0$ is the probability that Alice transmits a covert message, $\mathcal{P}(\mathcal{H}_0) = \pi_1$ is the probability that Alice does not transmit a covert message, $\alpha = \mathcal{P}(\mathcal{D}_1|\mathcal{H}_0)$ is the false alarm probability and $\beta = \mathcal{P}(\mathcal{D}_0|\mathcal{H}_1)$ is the miss detection probability, while $\mathcal{D}_1$ and $\mathcal{D}_0$ are the binary decisions that infer whether Alice transmits information to Bob or not, respectively.

From a conservative point of view, in this work we consider the worst-case scenario for Alice and Bob, where Willie has the ability to develop the detection strategy and the optimal detection threshold on it. As per [13], [18], $\mathcal{P}_e \geq \min\{\pi_0, \pi_1\}(\alpha + \beta)$. As such, Alice can achieve covert communication, for any $\epsilon > 0$, $\min\{\pi_0, \pi_1\}\xi \geq \min\{\pi_0, \pi_1\} - \epsilon$ for n sufficiently large, where ξ is the total error probability, which is given by

$$\xi = \alpha + \beta, \tag{7}$$

and $\epsilon \in [0, 1]$ is a predetermined value to specify the covert communication constraint.

Next, we derive the false alarm and miss detection probabilities at Willie, based on which we derive the optimal detection threshold that minimizes the total error probability. We focus on one communication slot, where Willie has to decide whether Alice transmitted to Bob, or not. Thus Willie faces a binary hypothesis testing problem. The composite received signal model at Willie is given by

$$\mathbf{y}_w[i] = \begin{cases} \sqrt{P_b} h_{bw} \mathbf{v}_b[i] + \mathbf{n}_w[i], & \mathcal{H}_0, \\ \sqrt{P_a} h_{aw} \mathbf{x}_a[i] + \sqrt{P_b} h_{bw} \mathbf{v}_b[i] + \mathbf{n}_w[i], & \mathcal{H}_1. \end{cases} \tag{8}$$

In this work we assume that Willie employs a radiometer as his detection test [17]. Considering the infinite blocklength, i.e., $n \to \infty$, we have

$$T \triangleq \lim_{n\to\infty} \frac{1}{n} T(n) = \begin{cases} P_b|h_{bw}|^2 + \sigma_w^2, & \mathcal{H}_0, \\ P_a|h_{aw}|^2 + P_b|h_{bw}|^2 + \sigma_w^2, & \mathcal{H}_1. \end{cases} \tag{9}$$

Then, the decision rule embedded in the detector at Willie is given by

$$T \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \tau, \tag{10}$$

where τ is the detection threshold for T, which will be optimally determined in order to minimize the total error probability.

III. Truncated Channel Inversion Power Control Scheme

In this section, we examine the possibility and performance of covert communications by utilizing AN generated by the full-duplex Bob (i.e., the receiver), since this AN can lead to a certain amount of uncertainty at Willie. Generating AN by the full-duplex Bob enables varying the presence and amount of uncertainty at Willie on demand, which leads to that the covert communication between Alice and Bob is fully under the control of Alice and Bob.

Considering a practical scenario, the truncated CIPC scheme is considered at Alice in this section, where Alice can only transmit covert information when the quality of the channel from Alice to Bob (i.e., $|h_{ab}|^2$) is greater than some specific value [42]. As such, Alice's transmit power is given by

$$P_a = \begin{cases} \frac{Q}{|h_{ab}|^2}, & |h_{ab}|^2 \geq \frac{Q}{P_a^{\max}}, \\ 0, & |h_{ab}|^2 < \frac{Q}{P_a^{\max}}, \end{cases} \tag{11}$$

where $P_a^{\max}$ is the maximum power constraint at Alice. As per (11), we note that Alice can transmit the covert message when $|h_{ab}|^2 \geq Q/P_a^{\max}$ is met. We denote this necessary condition as C. As such, Alice can transmit $\mathbf{x}_a$ to Bob whenever condition C is met. Considering quasi-static Rayleigh fading, the cumulative distribution function of $|h_{ab}|^2$ is given by $F_{|h_{ab}|^2}(x) = 1 - e^{-x/\lambda_{ab}}$ and thus the probability that C is guaranteed is given by

$$\mathcal{P}_C = \exp\left\{-\frac{Q}{P_a^{\max}\lambda_{ab}}\right\}. \tag{12}$$

Hence, the ECT from Alice to Bob is given by

$$R_c = R(1-\delta)\mathcal{P}_C. \tag{13}$$

A. Detection Performance at Willie

As discussed before, Alice can transmit covert message when condition C is guaranteed. In the truncated CIPC scheme, we assume that Alice will transmit a covert message with probability 1/2 when C is true. As per (12), the probabilities $\mathcal{P}(\mathcal{H}_1)$ and $\mathcal{P}(\mathcal{H}_0)$ are, respectively, given by

$$\begin{aligned} \mathcal{P}(\mathcal{H}_1) = \pi_1 &= \frac{1}{2}\mathcal{P}_C \\ &= \frac{1}{2}\exp\left\{-\frac{Q}{P_a^{\max}\lambda_{ab}}\right\}, \end{aligned} \tag{14}$$

and

$$\begin{aligned} \mathcal{P}(\mathcal{H}_0) = \pi_0 \\ = 1 - \frac{1}{2}\exp\left\{-\frac{Q}{P_a^{\max}\lambda_{ab}}\right\}. \end{aligned} \tag{15}$$

Following the decision rule given in (10), we derive the false alarm and miss detection probabilities at Willie in the following theorem.

Theorem 1: The false alarm and miss detection probabilities at Willie are derived in (16) and (17), shown at the bottom of this page, respectively

$$\alpha = \begin{cases} 1, & \tau < \sigma_w^2, \\ 1 - \dfrac{\tau - \sigma_w^2}{P_b^{\max}|h_{bw}|^2}, & \sigma_w^2 \leq \tau \leq \nu, \\ 0, & \tau > \nu, \end{cases} \tag{16}$$

where

$$\nu \triangleq P_b^{\max}|h_{bw}|^2 + \sigma_w^2, \tag{18}$$

and the exponential integral function $\mathrm{Ei}(\cdot)$ is given by

$$\mathrm{Ei}(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t}\mathrm{d}t. \tag{19}$$

Proof: This proof is provided in Appendix A. ■

We note that the false alarm and miss detection probabilities derived in Theorem 1 are for an arbitrary detection threshold τ. In practice, Willie will determine the optimal detection threshold that minimizes the detection error probability given in (6). Considering that the probabilities $\mathcal{P}(\mathcal{H}_1)$ and $\mathcal{P}(\mathcal{H}_0)$ are not functions of the detection threshold at Willie, the optimal detection threshold is also the one that minimizes the total error probability (i.e., $\alpha + \beta$) given by (7), which is derived in the following theorem.

Proposition 1: For the decision rule given in (10), Willie's optimal threshold that minimizes the total error probability is derived as

$$\tau^* = \nu, \tag{20}$$

$$\beta = \begin{cases} 0, & \tau < \sigma_w^2 \\ \frac{\tau-\sigma_w^2}{P_b^{\max}|h_{bw}|^2} - \frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}}\right)}{P_b^{\max}\lambda_{ab}|h_{bw}|^2}\left[\mathrm{Ei}\left(-\frac{(\tau-\sigma_w^2)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right) - \mathrm{Ei}\left(-\frac{Q}{P_a^{\max}\lambda_{ab}}\right)\right], & \sigma_w^2 \leq \tau \leq \nu \\ 1 - \frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}}\right)}{P_b^{\max}|h_{bw}|^2\lambda_{ab}}\left[\mathrm{Ei}\left(-\frac{(\tau-\sigma_w^2)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right) - \mathrm{Ei}\left(-\frac{(\tau-\nu)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right)\right], & \tau > \nu \end{cases} \tag{17}$$

and the corresponding minimum total error probability is given by

$$\xi^* = 1 - \frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}}\right)}{P_b^{\max}\lambda_{ab}|h_{bw}|^2} \times \left[\mathrm{Ei}\left(-\frac{P_b^{\max}|h_{bw}|^2\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right) - \mathrm{Ei}\left(-\frac{Q}{P_a^{\max}\lambda_{ab}}\right)\right]. \quad (21)$$

where $\nu = P_b^{\max}|h_{bw}|^2 + \sigma_w^2$ as defined in (18).

Proof: This proof is provided in Appendix B. ■

Following Theorem 1 and Proposition 1, we note that although the noise power at Willie i.e., σ_w^2 appears in the expressions of the false alarm probability, miss detection probability, and the optimal detection threshold, it does not affect the minimum total error probability, ξ^*, at Willie. This is due to the fact that Willie knows σ_w^2 and thus he can adjust the optimal detection threshold accordingly to counteract the impact of σ_w^2. We also note that for $\tau^* = \nu$ the false alarm probability is zero, which means that Willie adjusts the detection threshold to force the false alarm probability being zero in order to minimize the total error probability. This is achievable, since as assumed Willie knows the value range of Bob's transmit power of the AN signal (i.e., the maximum value of P_b, which is $P_b^{\max}$).

B. Transmission From Alice to Bob

In this subsection, we detail the transmission from Alice to the full-duplex Bob and derive the associated transmission outage probability.

Following (3), the signal to interference plus noise ratio (SINR) at Bob used to decode $\mathbf{x}_a$ is given by

$$\gamma_b = \frac{P_a|h_{ab}|^2}{\phi P_b|h_{bb}|^2+\sigma_b^2} = \frac{Q}{\phi P_b|h_{bb}|^2+\sigma_b^2}, \quad (22)$$

since Alice varies its transmit power as per h_{ab} such that $P_a|h_{ab}|^2 = Q$. Due to the randomness in $|h_{bb}|^2$ and P_b, we note that the residual error after self-interference cancellation is complex Gaussian and its variance is proportional to $P_b|h_{bb}|^2$. Then, the transmission from Alice to Bob will incur outage when $C_{ab} < R$, where $C_{ab} = \log_2(1+\gamma_b)$ is the channel capacity from Alice to Bob and R is the fixed transmission throughput from Alice to Bob. We note that γ_b cannot be larger than Q/σ_b^2, which is achieved when $\phi = 0$ (i.e., when the self-interference can be fully cancelled). As such, in order to guarantee the transmission outage probability being less than one, we to have to ensure $R < \log_2(1+Q/\sigma_b^2)$, which is assumed to be true in this section. We next derive the transmission outage probability from Alice to Bob in the following proposition.

Proposition 2: The transmission outage probability from Alice to the full-duplex Bob is derived as

$$\delta = e^{-\eta} + \eta\mathrm{Ei}(-\eta), \quad (23)$$

where

$$\eta = \frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\,\lambda_{bb}\phi P_b^{\max}}. \quad (24)$$

Proof: This proof is provided in Appendix C ■

Following Proposition 2, we determine some properties of the transmission outage probability in the following corollary.

Corollary 1: The transmission outage probability δ is a monotonically decreasing function of η, which leads to the fact that δ monotonically decreases with Q but increases with $P_b^{\max}$.

Proof: In order to determine the monotonicity of δ with respect to η, we derive its first derivative as

$$\frac{\partial\delta}{\partial\eta} = -2e^{-\eta} + \mathrm{Ei}(-\eta). \quad (25)$$

We note that $\eta \geq 0$ as per its definition given in (24) and thus we have $\partial\delta/\partial\eta \leq 0$ due to $-2e^{-\eta} < 0$ and $\mathrm{Ei}(-\eta) < 0$, which indicates that δ monotonically decreases with η. Again, as per the definition of η in (24), we can see that η is a monotonically increasing function of Q but a monotonically decreasing function of $P_b^{\max}$, which completes the proof of Corollary 1. ■

C. Optimization of Effective Covert Throughput

In this subsection, we examine the maximum ECT achieved in the considered scenario with the full-duplex Bob subject to a certain covert communication constraint. In this scenario, Willie knows h_{bw}, which is the reason that the detection performance (e.g., false alarm probability, miss detection probability, optimal detection threshold, and the minimum total error probability) at Willie depends on h_{bw}. However, Alice does not know h_{bw} and thus cannot guarantee the covert communication constraint $\min\{\pi_0,\pi_1\}\xi^*(|h_{aw}|^2,Q) \geq \min\{\pi_0,\pi_1\} - \epsilon$. As such, in the following proposition we present the expected value of $\xi^*(|h_{aw}|^2,Q)$ over all realizations of $|h_{bw}|^2$, which is denoted by $\overline{\xi^*}(Q)$, and then we use $\min\{\pi_0,\pi_1\}\overline{\xi^*}(Q) \geq \min\{\pi_0,\pi_1\} - \epsilon$ as the covert communication constraint in this section.

The optimization problem at Alice of maximizing the ECT subject to a certain covert communication constraint is given by

$$Q^* = \underset{Q}{\mathrm{argmax}}\, R_c \quad \text{s.t.} \quad \min\{\pi_0,\pi_1\}\overline{\xi^*}(Q) \geq \min\{\pi_0,\pi_1\} - \epsilon, \quad (26)$$

where $\min\{\pi_0,\pi_1\} = 1/2\exp\{-Q/(P_a^{\max}\lambda_{ab})\}$, $\overline{\xi^*}(Q)$ is the expected value of the minimum total error probability $\xi^*(|h_{bw}|^2,Q)$ over all realizations of $|h_{bw}|^2$, which is given by

$$\begin{aligned}\overline{\xi^*}(Q) &= \int_0^\infty \xi^*(|h_{bw}|^2,Q)\frac{e^{-\frac{|h_{bw}|^2}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}|h_{bw}|^2 \\ &= 1 - \int_0^\infty \frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}} - \frac{|h_{bw}|^2}{\lambda_{bw}}\right)}{P_b^{\max}\lambda_{ab}\lambda_{bw}|h_{bw}|^2} \\ &\quad\times\left[\mathrm{Ei}\left(-\frac{P_b^{\max}|h_{bw}|^2\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right) - \mathrm{Ei}\left(-\frac{Q}{P_a^{\max}\lambda_{ab}}\right)\right]\mathrm{d}|h_{bw}|^2, \end{aligned} \quad (27)$$

and the objective function $R_c = R(1-\delta)\mathcal{P}_C$ in (26) is the ECT from Alice to Bob, which is defined in (13) and is not a monotonic function of Q. This is because that the outage δ is a monotonically decreasing function of Q as per Corollary 1 and $\mathcal{P}_C$ is a monotonically decreasing function of Q as per (12). The optimization problem (26) can be solved by numerical search in the set of Q which satisfies $1/2\exp(-Q/(P_a^{\max}\lambda_{ab}))[1-\overline{\xi^*}(Q)] \leq \epsilon$.

IV. Conventional Channel Inversion Power Control Scheme

In this section, we consider the conventional CIPC scheme in the context of covert communications. The conventional CIPC scheme is a special case of truncated CIPC scheme with $P_a^{\max} \to \infty$. However, we note the fact that the minimum total error probability at Willie for the conventional CIPC scheme cannot be directly obtained from that of the truncated CIPC scheme by setting $P_a^{\max} \to \infty$, $\xi^* \to 1-(Q\lambda_{aw})/(P_b^{\max}\lambda_{ab}|h_{bw}|^2)[(-\infty)-(-\infty)]$, due to the involved Ei functions. This fact motivates us to consider the conventional CIPC scheme and directly analyze its performance in this section, based on which we are able to provide the comparison result between the truncated and conventional CIPC schemes.

A. Detection Performance at Willie

In the conventional CIPC scheme, we assume that Alice will transmit a covert message with probability $1/2$, since Alice can always transmit covert information and the uninformative priors $\pi_0 = \pi_1 = 1/2$ means a random guess of Alice's covert transmission at Willie. As such, the probability $\mathcal{P}(\mathcal{H}_1)$ and $\mathcal{P}(\mathcal{H}_0)$ are, respectively, given by

$$\mathcal{P}(\mathcal{H}_1) = \pi_1 = \frac{1}{2}, \tag{28}$$

and

$$\mathcal{P}(\mathcal{H}_0) = \pi_0 = \frac{1}{2}. \tag{29}$$

Following the decision rule given in (10), we derive the false alarm and miss detection probabilities at Willie in the conventional CIPC scheme with the full-duplex Bob in the following theorem.

Theorem 2: For Willie, the expression of false alarm probability is same as (16) and the miss detection probability is derived in (30), shown at the bottom of this page, where we recall that ν is defined in (18).

Proof: This proof is provided in Appendix D. ■

We note that the false alarm and miss detection probabilities derived in Theorem 2 are for an arbitrary detection threshold τ. In practice, Willie will determine the optimal detection threshold that minimizes the total error probability, which is derived in the following theorem.

Proposition 3: For the decision rule given in (10), Willie's optimal threshold that minimizes the total error probability is derived as

$$\tau^* = \nu, \tag{31}$$

and the corresponding minimum total error probability is given by

$$\xi^* = 1 - \frac{Q\lambda_{aw}}{P_b^{\max}\lambda_{ab}|h_{bw}|^2}\ln\left(1+\frac{P_b^{\max}\lambda_{ab}|h_{bw}|^2}{Q\lambda_{aw}}\right). \tag{32}$$

where $\nu = P_b^{\max}|h_{bw}|^2 + \sigma_w^2$ as defined in (18).

Proof: As per (7), (16), and (30), the total error probability at Willie is given by (33), shown at the bottom of this page. The rest part of the proof is omitted here, which is similar to that of Proposition 1. ■

B. Optimization of Effective Covert Throughput

In this subsection, we examine the maximum ECT achieved in the conventional CIPC scheme. The procedures for solving the optimization problem are similar to that in Section III.C.

Proposition 4: The expected value of the minimum total error probability ξ^* over all realizations of h_{bw} is derived as

$$\begin{aligned}\overline{\xi^*}(Q) = 1 - \frac{1}{4\varphi(Q)}\Bigg\{ &- \frac{8}{\varphi(Q)}{}_3F_3\left([1,1,1],[2,2,2],\frac{1}{\varphi(Q)}\right) \\ &+ 4\varsigma\mathrm{Ei}\left(-\frac{1}{\varphi(Q)}\right) + 4\ln(\varphi(Q))\Bigg(-\mathrm{Ei}\left(-\frac{1}{\varphi(Q)}\right) \\ &- \frac{\ln(\varphi(Q))}{2} + \varsigma\Bigg) + \pi^2 - 2\varsigma^2\Bigg\},\end{aligned} \tag{34}$$

where $\varphi(Q) \triangleq P_b^{\max}\lambda_{ab}\lambda_{bw}/(Q\lambda_{aw})$, ${}_3F_3([\cdot,\cdot,\cdot],[\cdot,\cdot,\cdot],\cdot)$ is Gauss hypergeometric functions and ς is the Euler constant.

$$\beta = \begin{cases} 0, & \tau < \sigma_w^2 \\ \frac{1}{P_b^{\max}|h_{bw}|^2}\left(\tau - \sigma_w^2 - \frac{Q\lambda_{aw}}{\lambda_{ab}}\ln\left(1+\frac{(\tau-\sigma_w^2)\lambda_{ab}}{Q\lambda_{aw}}\right)\right), & \sigma_w^2 \leq \tau \leq \nu \\ 1 - \frac{Q\lambda_{aw}}{P_b^{\max}|h_{bw}|^2\lambda_{ab}}\ln\left(1+\frac{P_b^{\max}|h_{bw}|^2}{\tau+Q\lambda_{aw}/\lambda_{ab}-\nu}\right), & \tau > \nu \end{cases} \tag{30}$$

$$\xi = \begin{cases} 1, & \tau < \sigma_w^2 \\ 1 - \frac{Q\lambda_{aw}}{P_b^{\max}|h_{bw}|^2\lambda_{ab}}\ln\left(1+\frac{(\tau-\sigma_w^2)\lambda_{ab}}{Q\lambda_{aw}}\right), & \sigma_w^2 \leq \tau \leq \nu \\ 1 - \frac{Q\lambda_{aw}}{P_b^{\max}|h_{bw}|^2\lambda_{ab}}\ln\left(1+\frac{P_b^{\max}|h_{bw}|^2}{\tau+Q\lambda_{aw}/\lambda_{ab}-\nu}\right), & \tau > \nu \end{cases} \tag{33}$$

Proof: Following (32), the expected value of $\xi^*(|h_{bw}|^2, Q)$ with respect with $|h_{bw}|^2$ is given by

$$\begin{aligned}\overline{\xi^*}(Q) &= \int_0^\infty \xi^*(|h_{bw}|^2, Q)\frac{e^{-\frac{|h_{bw}|^2}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}|h_{bw}|^2 \\ &\overset{a}{=} \int_0^\infty \left\{1 - \frac{Q\lambda_{aw}}{P_b^{\max}\lambda_{ab}x}\ln\left(1+\frac{P_b^{\max}\lambda_{ab}x}{Q\lambda_{aw}}\right)\right\} \\ &\quad\times \frac{e^{-\frac{x}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}x \\ &= \int_0^\infty \frac{e^{-\frac{x}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}x - \int_0^\infty \frac{Q\lambda_{aw}}{P_b^{\max}\lambda_{ab}x} \\ &\quad\times \ln\left(1+\frac{P_b^{\max}\lambda_{ab}x}{Q\lambda_{aw}}\right)\frac{e^{-\frac{x}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}x \\ &= 1 - \frac{Q\lambda_{aw}}{P_b^{\max}\lambda_{ab}\lambda_{bw}}\int_0^\infty \frac{e^{-\frac{x}{\lambda_{bw}}}}{x} \\ &\quad\times \ln\left(1+\frac{P_b^{\max}\lambda_{ab}x}{Q\lambda_{aw}}\right)\mathrm{d}x, \end{aligned} \tag{35}$$

where $\overset{a}{=}$ is obtained by using $|h_{bw}|^2 = x$, and solving the integral in (35) leads to the desired result in (34). ■

The optimization problem at Alice of maximizing the ECT subject to a certain covert communication constraint is given by

$$\begin{aligned} Q^* &= \underset{Q}{\operatorname{argmax}}\, R_c \\ &\text{s.t.} \quad \min\{\pi_0, \pi_1\}\overline{\xi^*}(Q) \geq \min\{\pi_0, \pi_1\} - \epsilon. \end{aligned} \tag{36}$$

where $\pi_0 = \pi_1 = 1/2$ as defined in (29) and (28), respectively. We note that the transmission outage probability of the conventional CIPC scheme is the same as that given in (23) of the truncated CIPC scheme and we have $\mathcal{P}_C = 1$ in the conventional CIPC scheme.

We next determine the solution to the optimization problem given in (36) and derive the maximum ECT in the following theorem.

Theorem 3: For given $P_b^{\max}$ and ϵ, the solution to (36), i.e., the optimal value of Q that maximizes the ECT R_c subject to $\overline{\xi^*}(Q) \geq 1 - 2\epsilon$, is derived as

$$Q^* = Q_\epsilon, \tag{37}$$

and the achieved maximum ECT is given by

$$R_c^* = R(1 - e^{-\eta^*} - \eta^*\mathrm{Ei}(-\eta^*)), \tag{38}$$

where Q_ϵ is the solution to $\overline{\xi^*}(Q) = 1 - 2\epsilon$ of Q and η^* is given by

$$\eta^* = \frac{Q^* - (2^R - 1)\sigma_b^2}{(2^R - 1)\,\lambda_{bb}\phi P_b^{\max}}. \tag{39}$$

Proof: This proof is provided in Appendix E. ■

Corollary 2: As Bob's maximum transmit power of the AN signal approaches infinity (i.e., $P_b^{\max} \to \infty$), the achievable maximum ECR approaches a fixed value, which is given by

$$\begin{aligned}\lim_{P_b^{\max}\to\infty} R_c^* = R\Bigg(1 - \exp\left(-\frac{1}{(2^R-1)\lambda_{ab}\phi\theta_\epsilon}\right) \\ + \frac{\mathrm{Ei}\left(-\frac{1}{(2^R-1)\lambda_{ab}\phi\theta_\epsilon}\right)}{(2^R-1)\lambda_{ab}\phi\theta_\epsilon}\Bigg).\end{aligned} \tag{40}$$

Proof: As per (32) and (53), we note that the solution of θ_ϵ to $\overline{\xi^*}(\theta) = 1 - 2\epsilon$ does not affect by the value of $P_b^{\max}$. As such, we still have t_ϵ as the solution to $\overline{\xi^*}(\theta) = 1 - 2\epsilon$ as $P_b^{\max} \to \infty$. Then, substituting $Q^* = P_b^{\max}/\theta_\epsilon$ into (39) we have

$$\lim_{P_b^{\max}\to\infty} \eta^* = \frac{1}{(2^R - 1)\,\lambda_{bb}\phi\theta_\epsilon}. \tag{41}$$

Then, substituting (41) into (38) we achieve the desired result in (40) after some algebraic manipulations. ■

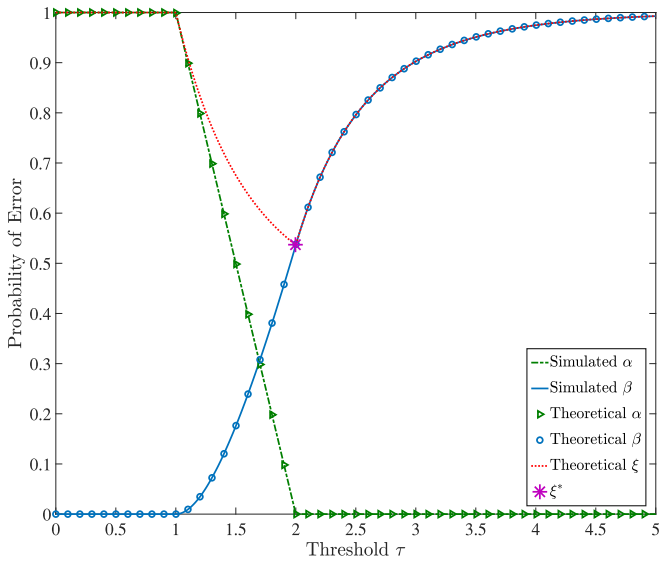


Fig. 2. Willie's false alarm probability α, miss detection probability β, and total error probability ξ versus threshold τ for covert communications in the truncated CIPC scheme, where $Q = 1$, $P_b^{\max} = 0$ dBm, $P_a^{\max} = 0$ dBm, $|h_{bw}|^2 = 1$, and $\sigma_w^2 = 0$ dBm.

V. Numerical Results

In this section, we first present numerical results to verify our analysis on the covert communications in the considered two schemes (i.e., conventional CIPC and truncated CIPC). Then, we provide a thorough performance examination of the covert communications in each scheme. Based on our examination, we draw many useful insights and guidelines on how to design and implement covert communications in practical scenarios. Without other statements, we set $R = 1$, $\lambda_{ab} = \lambda_{aw} = \lambda_{bb} = \lambda_{bw} = 1$.

Fig. 2 illustrates the false alarm probability α, miss detection probability β, and total error probability ξ versus Willie's detection threshold τ in the truncated CIPC scheme. The simulated curves of α and β are obtained based on $\alpha = \mathcal{P}[P_b|h_{bw}|^2 + \sigma_w^2 > \tau]$ and $\beta = \mathcal{P}[(Q|h_{aw}|^2)/$

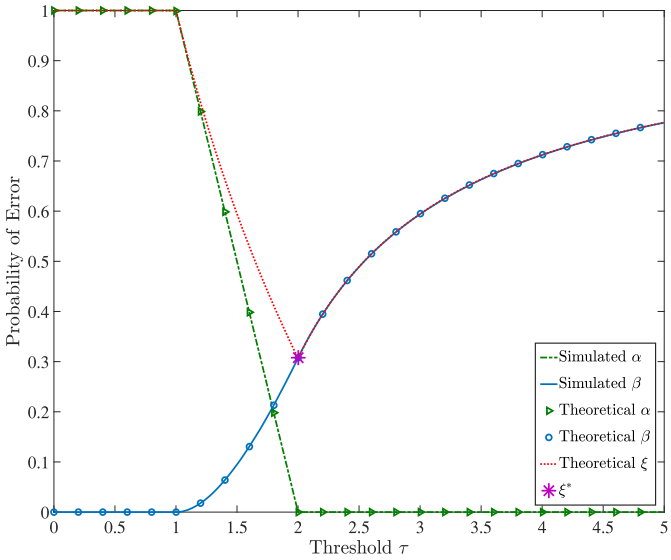


Fig. 3. Willie's false alarm probability α, miss detection probability β, and total error probability ξ versus threshold τ for covert communications in the conventional CIPC scheme, where $Q = 1$, $P_b^{\max} = 0$ dBm, $|h_{bw}|^2 = 1$, and $\sigma_w^2 = 0$ dBm.

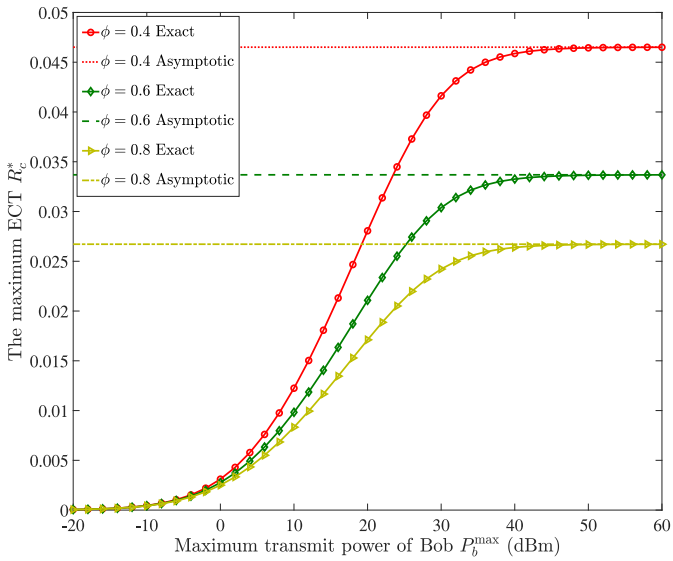


Fig. 4. Maximum ECT R_c^* versus Bob's maximum transmit power $P_b^{\max}$ under different value of ϕ in the conventional CIPC scheme, where $\epsilon = 0.01$, $R = 1$, and $\sigma_b^2 = 0$ dBm.

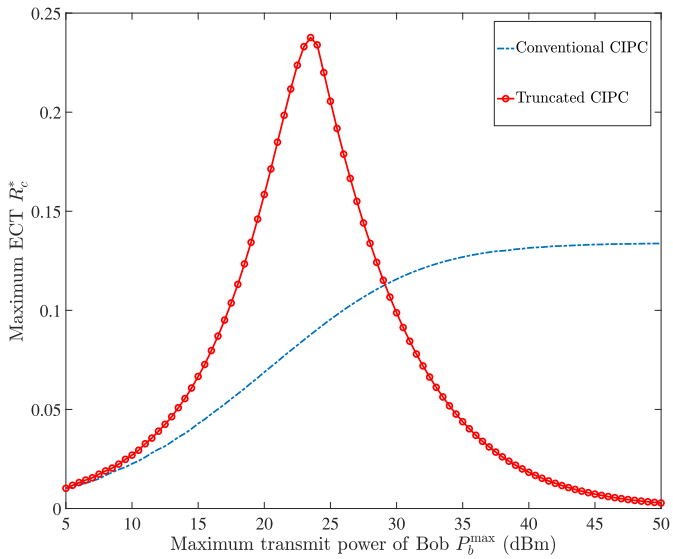


Fig. 5. Maximum ECT R_c^* versus Bob's maximum transmit power $P_b^{\max}$ optimized over Q and R, where $\phi = 0.1$, $\epsilon = 0.01$, $P_a^{\max} = 10$ dBm, $R = 1$, and $\sigma_b^2 = 0$ dBm.

$|h_{ab}|^2 + P_b|h_{bw}|^2 + \sigma_w^2 < \tau|C]$, respectively. The corresponding Monte-Carlo simulation results are achieved by generating sufficiently large number of the random values of P_b, $|h_{aw}|^2$, and $|h_{ab}|^2$. As expected, we first observe that the simulated curves precisely match the theoretical ones, which confirms the correctness of our Theorem 1. We also observe that there is indeed an optimal value of τ that minimizes ξ and this value satisfies $\tau^* = \nu$, which verifies the correctness of our Proposition 1.

In Fig. 3, we plot the false alarm probability α, miss detection probability β, and total error probability ξ versus Willie's detection threshold τ in the conventional CIPC scheme. The simulated curves of α and β are obtained based on $\alpha = \mathcal{P}[P_b|h_{bw}|^2 + \sigma_w^2 > \tau]$ and $\beta = \mathcal{P}[(Q|h_{aw}|^2)/|h_{ab}|^2 + P_b|h_{bw}|^2 + \sigma_w^2 < \tau]$, respectively. The corresponding Monte-Carlo simulation results are achieved by generating sufficiently large number of the random values of P_b, $|h_{aw}|^2$, and $|h_{ab}|^2$. As expected, in this figure we first observe that the simulated curves precisely match the theoretical ones, which confirms the correctness of our Theorem 2. We also observe that the total error probability ξ dramatically varies with the detection threshold τ, which demonstrates the necessity of optimizing τ by Willie and the importance of our Proposition 3, which derives the optimal detection threshold minimizes ξ in a closed-form expression. Finally, we observe that the optimal value of τ is equal to ν, which simultaneously forces the false alarm probability α at Willie being zero and minimizes the miss detection probability β.

In Fig. 4, we plot the maximum ECT R_c^* versus Bob's maximum transmit power of the AN signal $P_b^{\max}$ with different values of the self-interference cancellation parameter ϕ. In this figure, we first observe that R_c^* monotonically increases as $P_b^{\max}$ increases, which demonstrates that the covert communications from Alice becomes easier when Bob has more power to transmit AN to aid. However, we also note that as $P_b^{\max} \to \infty$ the maximum ECT R_c^* approaches the upper bound given in our Corollary 2. Intuitively, this can be explained by the fact that the transmitted AN not only creates interference at Willie but also leads to self-interference at Bob. In this figure, we also observe that the upper bound on the achieved R_c^* decreases significantly as ϕ increases, since a larger ϕ indicates a larger self-interference at Bob.

In Fig. 5, we plot the maximum ECT R_c^*, which is achieved by the optimal Q, versus Bob's maximum transmit power of the AN signal $P_b^{\max}$. In this figure, we first observe that R_c^* achieved by the truncated CIPC scheme first increases and then decreases as $P_b^{\max}$ increases, which indicates that there is an optimal value of $P_b^{\max}$ that maximizes R_c^*. This due to the

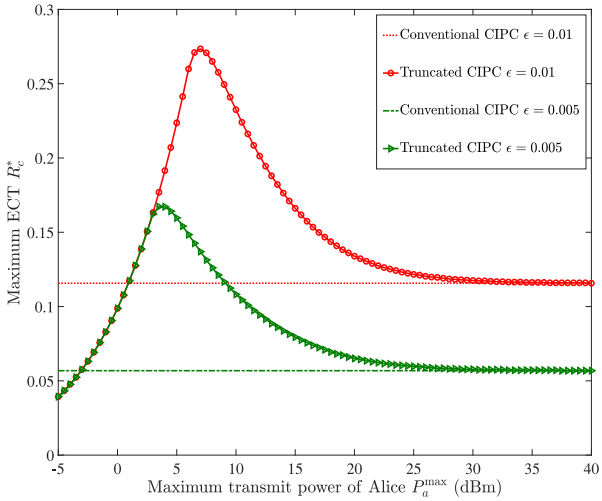


Fig. 6. Maximum ECT R_c^* versus Alice's maximum transmit power $P_a^{\max}$ optimized over Q and R under different value of ϵ, where $P_b^{\max} = 20$ dBm, $\sigma_b^2 = -10$ dBm, $R = 1$, and $\phi = 0.1$.

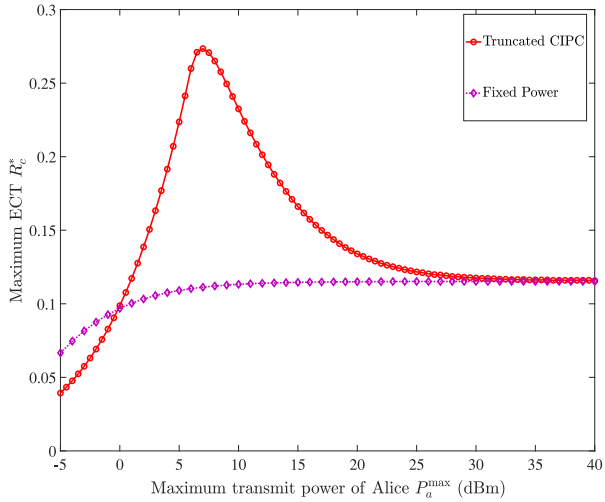


Fig. 7. Maximum ECT R_c^* versus Alice's maximum transmit power $P_a^{\max}$ for covert communications in the truncated CIPC and fixed power transmission schemes, where $P_b^{\max} = 20$ dBm, $\sigma_b^2 = -10$ dBm, $R = 1$, and $\phi = 0.1$.

fact a small $P_b^{\max}$ cannot cause enough uncertainty at Willie to hide Alice's covert transmission, while a large $P_b^{\max}$ may have greater impact on increasing the interference at Bob than increasing uncertainty at Willie (since $P_a^{\max}$ is predefined in the truncated CIPC scheme). Meanwhile, we also observe that the R_c^* achieved by the conventional CIPC scheme continuously increases as $P_b^{\max}$ increases, which is due to the fact that in the conventional CIPC scheme we can vary Q to counteract the impact of $P_b^{\max}$ on the detection performance at Willie (can be seen from Corollary 2) and the outage probability converges to a specific constant value as $P_b^{\max}$ increases (can be seen from (41)). Furthermore, in this figure we observe that the maximum value of R_c^* for the truncated CIPC scheme is higher than that for the conventional CIPC scheme, which demonstrates that the truncated CIPC scheme can outperform the conventional CIPC scheme. Intuitively, this is due to the fact that increasing $P_a^{\max}$ can decrease the detection error probability at Willie (i.e., it becomes easier for Willie to detection Alice's covert transmission), although increasing $P_a^{\max}$ always increases the ECT from Alice to Bob.

In Fig. 6, we plot the maximum ECT R_c^*, achieved by the conventional and truncated CIPC schemes with the optimal Q, versus the maximum transmit power at Alice $P_a^{\max}$ with different levels of covert communication constraints (i.e., different values of ϵ). In this figure, we first observe that R_c^* achieved by the truncated CIPC scheme first increases and then decreases as $P_a^{\max}$ increases, which indicates that there is an optimal value of $P_a^{\max}$ that maximizes R_c^*. This can be explained by the fact that increasing $P_a^{\max}$ simultaneously decreases the detection error probability at Willie and the probability that Alice can transmit covert information to Bob (i.e., $\mathcal{P}_C$), which means that $P_a^{\max}$ has a two-side impact on the considered covert communications. This observation indicates, on top of optimizing the fixed value Q, we also have to optimally design the parameter $P_a^{\max}$ in order to achieve the optimal performance of CIPC in the context of covert communications. This is different from optimizing the performance of CIPC in point-to-point communications, where the performance of CIPC monotonically increases with $P_a^{\max}$ and thus solely optimizing Q is sufficient. We also observe that, as $P_a^{\max}$ increases, the R_c^* of the truncated CIPC scheme approaches that of the conventional CIPC scheme, which confirms the correctness of our examinations. As expected, we also observe that R_c^* increases as ϵ increases, which demonstrates that it is the covert communication constraint that mainly limits R_c^*.

In Fig. 7, we plot the maximum ECT R_c^* versus Alice's maximum transmit power $P_a^{\max}$ for the truncated CIPC scheme and fixed power transmission scheme in [28]. For the fixed power transmission scheme, the fixed value of transmit power at Alice is optimized to achieve the maximum covert rate R_c^* with the power constraint $P_a \leq P_a^{\max}$. In this figure, we observe that for the fixed power transmission schemes R_c^* monotonically increases as $P_a^{\max}$ increases and approaches a fixed value when $P_a^{\max}$ is sufficiently large. It is also noted that the fixed power transmission scheme outperforms the truncated CIPC transmission scheme when $P_a^{\max}$ is in the low regime, which means that truncated CIPC transmission scheme sacrifices part of covert throughput compared with the fixed power transmission scheme. However, when $P_a^{\max}$ is larger than some specific values (e.g., when $P_a^{\max} \geq 0$ dBm), the performance of truncated CIPC transmission scheme is better than that of the fixed power transmission scheme. This is mainly due to the fact that the transmit power constraints are not limits of the covert transmission performance when $P_a^{\max}$ is relatively large.

VI. Conclusion

This work examined covert communications with a full-duplex receiver over Rayleigh fading channels, in which the transmitter Alice adopts the CIPC to transmit information to the receiver Bob covertly while trying to hide herself from the warden Willie. We analyzed Willie's detection performance limits for the considered truncated and conventional CIPC schemes, based on which the achievable ECTs of these two schemes were determined. Our examination shows that there exists an

optimal value of the maximum transmit power at Bob that maximizes the ECT in the truncated CIPC scheme, while the ECT monotonically increases and approaches an upper bound as this maximum transmit power at Bob increases in the conventional CIPC scheme. Our analysis and examinations provided practical guidelines on conducting covert communications and potentially hiding a transmitter in Rayleigh fading scenarios. Future work will focus on scenarios where number of antennas is larger than 1. The warden Willie is normally passive and never transmits signals, which means that it is hard for the transmitter to obtain the CSI of the channel from the transmitter to Willie. Without this CSI, the transmitter cannot utilize the zero-forcing algorithm with the aid of multiple antennas to avoid the detection at Willie. Therefore, more research will be focused on the case where warden is equipped with multiple antennas and provide more precise results relating to it.

APPENDIX A
PROOF OF THEOREM 1

Following (9) and (10), and noting that $\mathcal{H}_0$ can happen regardless of whether the condition C is guaranteed, the false alarm probability is given by

$$\begin{aligned}\alpha &= \mathcal{P}\left[P_b|h_{bw}|^2+\sigma_w^2>\tau|C\right]+\mathcal{P}\left[P_b|h_{bw}|^2+\sigma_w^2>\tau|C'\right]\\ &= \mathcal{P}\left[P_b|h_{bw}|^2+\sigma_w^2>\tau\right]\\ &= \begin{cases}1, & \tau<\sigma_w^2,\\ \int_{\frac{\tau-\sigma_w^2}{|h_{bw}|^2}}^{P_b^{\max}} f_{P_b}(x)\mathrm{d}x, & \sigma_w^2\le\tau\le\nu,\\ 0, & \tau>\nu,\end{cases}\\ &= \begin{cases}1, & \tau<\sigma_w^2,\\ \int_{\frac{\tau-\sigma_w^2}{|h_{bw}|^2}}^{P_b^{\max}} \frac{1}{P_b^{\max}}\mathrm{d}x, & \sigma_w^2\le\tau\le\nu,\\ 0, & \tau>\nu.\end{cases}\end{aligned} \tag{42}$$

Then, solving the integral in (42) leads to the desired result in (16).

As per (9) and (10), the miss detection probability is given by (43), shown on the next page, where $\mathcal{P}_C^{-1}$ is the reciprocal of $\mathcal{P}_C$ and equal to $\exp\{Q/(\lambda_{ab}P_a^{\max})\}$. Then, we achieve the desired result in (17) after some algebraic manipulations.

APPENDIX B
PROOF OF PROPOSITION 1

As per (7), (16), and (17), the total error probability at Willie is given by (44), shown on the next page.

We first note that $\xi=1$ is the worst case scenario for Willie and thus Willie does not set $\tau<\sigma_w^2$. As per (21), for $\sigma_w^2\le\tau\le\nu$ the total error probability ξ is a monotonically decreasing function of τ. Thus, Willie will set ν as the threshold to minimize ξ in this case. For $\tau>\nu$, we have

$$\frac{\partial\xi}{\partial\tau}=\frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}}\right)}{P_b^{\max}|h_{bw}|^2\lambda_{ab}}\left[g(-\kappa_1)-g(-\kappa_2)\right], \tag{45}$$

where

$$\begin{aligned}g(x)&\triangleq\frac{e^x}{x},\\ \kappa_1&\triangleq\frac{(\tau-\sigma_w^2)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}},\\ \kappa_2&\triangleq\frac{(\tau-\nu)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}.\end{aligned} \tag{46}$$

In order to check the sign of $g(-\kappa_1)-g(-\kappa_2)$ in (45), we derive the first derivative of $g(x)$ with respect to x as

$$\frac{\partial g(x)}{\partial x}=\frac{e^x(x-1)}{x^2}. \tag{47}$$

As per (47) we can see that $\partial g(x)/\partial x<0$ for $x<0$. Noting that $\kappa_1>\kappa_2$, we have $g(-\kappa_1)-g(-\kappa_2)>0$. Noting that $\kappa_1>\kappa_2$, the value of the term $g(-\kappa_1)-g(-\kappa_2)$ is larger than 0, which leads to the value of $\partial\xi/\partial\tau>0$. As such, ξ is a monotonically increasing function of τ based on (44), which indicates that Willie will try to set ν as the threshold again to minimize ξ under this case. We also note that for the two cases, i.e., $\sigma_w^2\le\tau\le\nu$ and $\tau>\nu$, setting $\tau=\nu$ can achieve the same total error probability. As such, we can conclude that the optimal detection threshold is τ.

APPENDIX C
PROOF OF PROPOSITION 2

Based on the definition of the transmission outage probability given in (2), we have

$$\begin{aligned}\delta&=\mathcal{P}\left[\log_2(1+\gamma_b)\le R\right]\\ &=\mathcal{P}\left[\frac{Q}{\phi P_b|h_{bb}|^2+\sigma_b^2}\le 2^R-1\right]\\ &=\int_0^{P_b^{\max}}\int_{\frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\phi y}}^{+\infty} f_{|h_{bb}|^2}(x)f_{P_b}(y)\mathrm{d}x\mathrm{d}y\\ &=\int_0^{P_b^{\max}}\int_{\frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\phi y}}^{+\infty}\frac{\exp\left(-\frac{x}{\lambda_{bb}}\right)}{\lambda_{bb}P_b^{\max}}\mathrm{d}x\mathrm{d}y\\ &=\frac{1}{P_b^{\max}}\int_0^{P_b^{\max}}\exp\left\{-\frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\lambda_{bb}\phi y}\right\}\mathrm{d}y\\ &=\exp\left(-\frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\lambda_{ab}\phi P_b^{\max}}\right)+\frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\lambda_{ab}\phi P_b^{\max}}\\ &\quad\times\mathrm{Ei}\left(-\frac{Q-(2^R-1)\sigma_b^2}{(2^R-1)\lambda_{ab}\phi P_b^{\max}}\right).\end{aligned} \tag{48}$$

Following (48), we achieve the desired result in (23) after some algebraic manipulations.

$$
\begin{aligned}
\beta &= \mathcal{P}\left[P_a|h_{aw}|^2 + P_b|h_{bw}|^2 + \sigma_w^2 < \tau | C\right] \\
&= \mathcal{P}\left[\frac{Q|h_{aw}|^2}{|h_{ab}|^2} + P_b|h_{bw}|^2 + \sigma_w^2 < \tau | C\right] \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \mathcal{P}_C^{-1}\mathcal{P}\left[P_b < \frac{\tau-\sigma_w^2-Q|h_{aw}|^2/|h_{ab}|^2}{|h_{bw}|^2}\right], & \sigma_w^2 \le \tau \le \nu, \\ \mathcal{P}_C^{-1}\mathcal{P}\left[\frac{|h_{aw}|^2}{|h_{ab}|^2} < \frac{\tau-\sigma_w^2-P_b|h_{bw}|^2}{Q}\right], & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \mathcal{P}_C^{-1}\int_{\frac{Q}{P_a^{\max}}}^{\infty}\int_0^{\frac{(\tau-\sigma_w^2)z}{Q}}\int_0^{\frac{\tau-\sigma_w^2-Qy/z}{|h_{bw}|^2}} f_{P_b}(x)f_{|h_{aw}|^2}(y)f_{|h_{ab}|^2}(z)\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \mathcal{P}_C^{-1}\int_0^{P_b^{\max}}\int_{\frac{Q}{P_a^{\max}}}^{\infty}\int_0^{\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)y}{Q}} f_{|h_{aw}|^2}(x)f_{|h_{ab}|^2}(y)f_{P_b}(z)\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \mathcal{P}_C^{-1}\int_{\frac{Q}{P_a^{\max}}}^{\infty}\int_0^{\frac{(\tau-\sigma_w^2)z}{Q}}\int_0^{\frac{\tau-\sigma_w^2-Qy/z}{|h_{bw}|^2}} \frac{\exp\left\{-\left(\frac{y}{\lambda_{aw}}+\frac{z}{\lambda_{ab}}\right)\right\}}{\lambda_{aw}\lambda_{ab}P_b^{\max}}\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \mathcal{P}_C^{-1}\int_0^{P_b^{\max}}\int_{\frac{Q}{P_a^{\max}}}^{\infty}\int_0^{\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)y}{Q}} \frac{\exp\left\{-\left(\frac{x}{\lambda_{aw}}+\frac{y}{\lambda_{ab}}\right)\right\}}{\lambda_{aw}\lambda_{ab}P_b^{\max}}\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \mathcal{P}_C^{-1}\int_{\frac{Q}{P_a^{\max}}}^{\infty}\int_0^{\frac{(\tau-\sigma_w^2)z}{Q}} \frac{(\tau-\sigma_w^2-Qy/z)\exp\left\{-\left(\frac{y}{\lambda_{aw}}+\frac{z}{\lambda_{ab}}\right)\right\}}{\lambda_{aw}\lambda_{ab}P_b^{\max}|h_{bw}|^2}\mathrm{d}y\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \mathcal{P}_C^{-1}\int_0^{P_b^{\max}}\int_{\frac{Q}{P_a^{\max}}}^{\infty} \frac{\left(1-\exp\left(-\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)y}{Q\lambda_{aw}}\right)\right)\exp\left(-\frac{y}{\lambda_{ab}}\right)}{\lambda_{ab}P_b^{\max}}\mathrm{d}y\mathrm{d}z, & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \mathcal{P}_C^{-1}\int_{\frac{Q}{P_a^{\max}}}^{\infty} \frac{\left((\tau-\sigma_w^2)z+Q\lambda_{aw}\left(\exp\left(-\frac{(\tau-\sigma_w^2)z}{Q\lambda_{aw}}\right)-1\right)\right)\exp\left(-\frac{z}{\lambda_{ab}}\right)}{\lambda_{ab}P_b^{\max}|h_{bw}|^2 z}\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \mathcal{P}_C^{-1}\int_0^{P_b^{\max}} \frac{1}{P_b^{\max}}\left\{\exp\left(-\frac{Q}{P_a^{\max}\lambda_{ab}}\right) - \frac{Q\lambda_{aw}\exp\left(-\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right)}{\lambda_{ab}(\tau-\sigma_w^2-z|h_{bw}|^2)+Q\lambda_{aw}}\right\}\mathrm{d}z, & \tau > \nu. \end{cases} \end{aligned} \tag{43}
$$

$$
\xi = \begin{cases} 1, & \tau < \sigma_w^2, \\ 1 - \frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}}\right)}{P_b^{\max}\lambda_{ab}|h_{bw}|^2}\left[\mathrm{Ei}\left(-\frac{(\tau-\sigma_w^2)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right) - \mathrm{Ei}\left(-\frac{Q}{P_a^{\max}\lambda_{ab}}\right)\right], & \sigma_w^2 \le \tau \le \nu, \\ 1 - \frac{Q\lambda_{aw}\exp\left(\frac{Q}{P_a^{\max}\lambda_{ab}}\right)}{P_b^{\max}\lambda_{ab}|h_{bw}|^2}\left[\mathrm{Ei}\left(-\frac{(\tau-\sigma_w^2)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right) - \mathrm{Ei}\left(-\frac{(\tau-\nu)\lambda_{ab}+Q\lambda_{aw}}{P_a^{\max}\lambda_{aw}\lambda_{ab}}\right)\right], & \tau > \nu. \end{cases} \tag{44}
$$

$$
\begin{aligned}
\beta &= \mathcal{P}\left[P_a|h_{aw}|^2 + P_b|h_{bw}|^2 + \sigma_w^2 < \tau\right] \\
&= \mathcal{P}\left[\frac{Q|h_{aw}|^2}{|h_{ab}|^2} + P_b|h_{bw}|^2 + \sigma_w^2 < \tau\right] \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \mathcal{P}\left[P_b < \frac{\tau-\sigma_w^2 - Q|h_{aw}|^2/|h_{ab}|^2}{|h_{bw}|^2}\right], & \sigma_w^2 \le \tau \le \nu, \\ \mathcal{P}\left[\frac{|h_{aw}|^2}{|h_{ab}|^2} < \frac{\tau-\sigma_w^2 - P_b|h_{bw}|^2}{Q}\right], & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \int_0^{+\infty}\int_0^{\frac{(\tau-\sigma_w^2)z}{Q}}\int_0^{\frac{\tau-\sigma_w^2-Qy/z}{|h_{bw}|^2}} f_{P_b}(x) f_{|h_{aw}|^2}(y) f_{|h_{ab}|^2}(z)\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \int_0^{P_b^{\max}}\int_0^{+\infty}\int_0^{\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)y}{Q}} f_{|h_{aw}|^2}(x) f_{|h_{ab}|^2}(y) f_{P_b}(z)\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \int_0^{+\infty}\int_0^{\frac{(\tau-\sigma_w^2)z}{Q}}\int_0^{\frac{\tau-\sigma_w^2-Qy/z}{|h_{bw}|^2}} \frac{\exp\left\{-\left(\frac{y}{\lambda_{aw}}+\frac{z}{\lambda_{ab}}\right)\right\}}{\lambda_{aw}\lambda_{ab}P_b^{\max}}\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \int_0^{P_b^{\max}}\int_0^{+\infty}\int_0^{\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)y}{Q}} \frac{\exp\left\{-\left(\frac{x}{\lambda_{aw}}+\frac{y}{\lambda_{ab}}\right)\right\}}{\lambda_{aw}\lambda_{ab}P_b^{\max}}\mathrm{d}x\mathrm{d}y\mathrm{d}z, & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \int_0^{+\infty}\int_0^{\frac{(\tau-\sigma_w^2)z}{Q}} \frac{(\tau-\sigma_w^2-Qy/z)\exp\left\{-\left(\frac{y}{\lambda_{aw}}+\frac{z}{\lambda_{ab}}\right)\right\}}{\lambda_{aw}\lambda_{ab}P_b^{\max}|h_{bw}|^2}\mathrm{d}y\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \int_0^{P_b^{\max}}\int_0^{+\infty} \frac{\left(1-\exp\left(-\frac{(\tau-\sigma_w^2-z|h_{bw}|^2)y}{Q\lambda_{aw}}\right)\right)\exp\left(-\frac{y}{\lambda_{ab}}\right)}{\lambda_{ab}P_b^{\max}}\mathrm{d}y\mathrm{d}z, & \tau > \nu, \end{cases} \\
&= \begin{cases} 0, & \tau < \sigma_w^2, \\ \int_0^{+\infty} \frac{\left((\tau-\sigma_w^2)z + Q\lambda_{aw}\left(\exp\left(-\frac{(\tau-\sigma_w^2)z}{Q\lambda_{aw}}\right)-1\right)\right)\exp\left(-\frac{z}{\lambda_{ab}}\right)}{\lambda_{ab}P_b^{\max}|h_{bw}|^2 z}\mathrm{d}z, & \sigma_w^2 \le \tau \le \nu, \\ \int_0^{P_b^{\max}} \frac{(\tau-\sigma_w^2-z|h_{bw}|^2)\lambda_{ab}}{(\tau-\sigma_w^2-z|h_{bw}|^2)\lambda_{ab}+Q\lambda_{aw}}\mathrm{d}z, & \tau > \nu. \end{cases}
\end{aligned} \tag{49}
$$

APPENDIX D
PROOF OF THEOREM 2

As per (9) and (10), the miss detection probability is given by (49), shown on the top of this page. Then, we achieve the desired result in (30) after some algebraic manipulations.

APPENDIX E
PROOF OF THEOREM 3

As per Corollary 1, the transmission outage probability δ is a monotonically decreasing function of Q, which leads to the fact that the ECT R_c monotonically increases with Q. Following this fact, we next prove another fact that the expected minimum total error probability $\overline{\xi^*}(Q)$ is a monotonically increasing function of Q. These two facts indicate that the optimal value of Q (i.e., the solution to (36)) is the one that ensures $\overline{\xi^*}(Q) = 1 - 2\epsilon$. To this end, we next prove that $\overline{\xi^*}(Q)$ is a monotonically decreasing function of Q. Following (35) and using the Leibniz integral rule, we derive the first derivative of $\overline{\xi^*}(Q)$ with respect to Q as

$$
\begin{aligned}
\frac{\partial\overline{\xi^*}(Q)}{\partial Q} &= \frac{\partial}{\partial Q}\left(\underbrace{\int_0^{\infty}\xi^*(|h_{bw}|^2, Q)\frac{e^{-\frac{|h_{bw}|^2}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}|h_{bw}|^2}_{\overline{\xi^*}(Q)}\right) \\
&= \int_0^{\infty}\frac{\partial\xi^*(|h_{bw}|^2, Q)}{\partial Q}\frac{e^{-\frac{|h_{bw}|^2}{\lambda_{bw}}}}{\lambda_{bw}}\mathrm{d}|h_{bw}|^2.
\end{aligned} \tag{50}
$$

Considering $e^{-\frac{x}{\lambda_{bw}}}/\lambda_{bw} > 0$ in (50), we could conclude that $\partial\overline{\xi^*}(Q)/\partial Q < 0$ if we could prove $\xi^*(|h_{bw}|^2, Q)$ is a decreasing function of Q. Following (32), we have

$$
\frac{\partial\xi^*(\theta)}{\partial\theta} = \frac{u(\theta)}{\theta^2(1+\theta)}, \tag{51}
$$

where

$$u(\theta) \triangleq \left(1+\frac{\theta\lambda_{ab}|h_{bw}|^2}{\lambda_{aw}}\right)\ln\left(1+\frac{\theta\lambda_{ab}|h_{bw}|^2}{\lambda_{aw}}\right) - \frac{\theta\lambda_{ab}|h_{bw}|^2}{\lambda_{aw}}, \tag{52}$$

$$\theta \triangleq \frac{P_b^{\max}}{Q}. \tag{53}$$

We note that the sign of $\partial\xi^*(\theta)/\partial\theta$ depends on the value of $u(\theta)$. In order to determine the value range of $u(\theta)$, we first derive the first derivative of $u(\theta)$ with respect to θ as

$$\frac{\partial u(\theta)}{\partial\theta} = \frac{\lambda_{ab}|h_{bw}|^2}{\lambda_{aw}}\ln\left(1+\frac{\theta\lambda_{ab}|h_{bw}|^2}{\lambda_{aw}}\right) > 0. \tag{54}$$

Noting $\lim_{\theta\to 0} u(\theta) = 0$ and following (54), we can conclude that $u(\theta) \geq 0$ for $\theta > 0$, which indicates that $\partial\xi^*(\theta)/\partial\theta \geq 0$. Noting that θ is a monotonically decreasing function of Q, we can conclude that $\xi^*(|h_{bw}|^2, Q)$ is a decreasing function of Q. This completes the proof of this theorem.

REFERENCES

[1] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[2] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[4] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction*. Cambridge, MA, USA: Cambridge Univ. Press, 2006.

[5] S. Rich and B. Gellman, "NSA seeks to build quantum computer that could crack most types of encryption," *Washington Post*, 2014, [Online]. Available: http://wapo.st/19DycJT

[6] N. Zhao, F. R. Yu, M. Li, and V. C. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[7] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[8] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[9] F. Shu, X. Wu, J. Hu, J. Li, R. Chen, and J. Wang, "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 890–904, Apr. 2018.

[10] N. Nandan, S. Majhi, and H.-C. Wu, "Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5327–5337, Aug. 2018.

[11] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[12] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

[13] B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversary's ignorance of transmission time," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8394–8405, Dec. 2016.

[14] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

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

[16] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[17] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. T. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[18] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

[19] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a Poisson field of interferers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6005–6017, Sep 2018.

[20] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communication with interference uncertainty," in *Proc. IEEE Int. Conf. Commun.*, May 2018, pp. 1–6.

[21] S. Yan, B. He, Y. Cong, and X. Zhou, "Covert communication with finite blocklength in AWGN channels," in *Proc. IEEE Int. Conf. Commun*, May 2017, pp. 1–6.

[22] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *Proc. IEEE VTC Spring*, Jun. 2017, pp. 1–5.

[23] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 129–140, Jan. 2018.

[24] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," in *Proc. IEEE GLOBECOM*, Dec. 2017, pp. 1–6.

[25] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jul. 2018.

[26] S. Yan, Y. Cong, S. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3542–3553, May 2019.

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

[28] J. Hu, K. Shahzad, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert communications with a full-duplex receiver over wireless fading channels," in *Proc. IEEE Int. Conf. Commun.*, May 2018, pp. 1–6.

[29] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[30] T. Xu, L. Xu, X. Liu, and Z. Lu, "Covert communication with a full-duplex receiver based on channel distribution information," in *Proc. Int. Symp. Antennas Propag. EM Theory*, Dec. 2018, pp. 1–4.

[31] N. J. Steven Weber and J. G. Andrews, "The effect of fading, channel inversion, and threshold scheduling on ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4127–4149, Nov. 2007.

[32] H.-M. Wang, B.-Q. Zhao, and T.-X. Zheng, "Adaptive full-duplex jamming receiver for secure D2D links in random networks," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254–1267, Feb. 2019.

[33] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.

[34] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[35] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[36] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

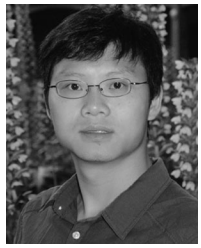
[37] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret pilot-aided channel training and power allocation in full-duplex wiretap channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2788–2800, Nov. 2018.

[38] E. Ahmed and A. M. Eltawil, "All-digital self-interference cancellation technique for full-duplex systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3519–3532, Jul. 2015.

[39] D. Kim, H. Ju, S. Park, and D. Hong, "Effects of channel estimation error on full-duplex two-way networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4666–4672, Nov. 2013.
[40] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 680–694, Feb. 2014.
[41] T. V. Sobers, B. A. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert communication with the help of an uninformed jammer achieves positive rate," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Nov. 2015, pp. 625–629.
[42] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4454–4469, Aug. 2014.

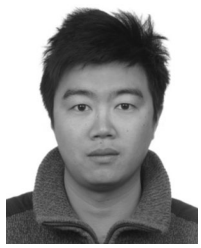
Jinsong Hu (S'17–M'19) received the B.S. and Ph.D. degrees from the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China, in 2013 and 2018, respectively. From 2017 to 2018, he was a Visiting Ph.D. Student with the Research School of Engineering, Australian National University, Canberra, ACT, Australia. He is currently a Lecturer with the College of Physics and Information Engineering, Fuzhou University, Fuzhou, China. His current research interests include array signal processing, covert communications, and physical layer security. He was a TPC Member for the IEEE International Conference on Communications in 2019.

Shihao Yan (S'11–M'15) received the B.S. degree in communication engineering and the M.S. degree in communication and information systems from Shandong University, Jinan, China, in 2009 and 2012, respectively, and the Ph.D. degree in electrical engineering from The University of New South Wales, Sydney, NSW, Australia, in 2015. From 2015 to 2017, he was a Postdoctoral Research Fellow in the Research School of Engineering, The Australian National University, Canberra, Australia. He is currently a University Research Fellow with the School of Engineering, Macquarie University, Sydney, NSW, Australia. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, covert communications, and location spoofing detection.



Xiangyun Zhou (SM'17) received the Ph.D. degree from Australian National University (ANU), Canberra, ACT, Australia, in 2010. He is an Associate Professor with ANU. His research interests are in the fields of communication theory and wireless networks. He was an Editor for the IEEE Transactions on Wireless Communications, IEEE WIRELESS COMMUNICATIONS LETTERS and the IEEE COMMUNICATIONS LETTERS. He served as a Guest Editor for the IEEE COMMUNICATIONS MAGAZINE feature topic on wireless physical layer security in 2015. He also served as symposium/track and workshop co-chairs for major IEEE conferences. He was the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is the recipient of the Best Paper Award at ICC'11 and IEEE ComSocAsia-Pacific Outstanding Paper Award in 2016. He was named the Best Young Researcher in the Asia-Pacific Region in 2017 by IEEE ComSoc Asia-Pacific Board.

Feng Shu (M'16) received the B.S., M.S., and Ph.D. degrees from the Fuyang Teaching College, Fuyang, China, in 1994, XiDian University, Xi'an, China, in 1997, and Southeast University, Nanjing, China, in 2002, respectively. From September 2009 to 2010, he is a Visiting Post-doctor with the University of Texas at Dallas. In October 2005, he joined the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China, where he is currently a Professor and a Supervisor of Ph.D. and graduate students. He is also with the School of Information and Communication Engineering, Hainan University, Hainan, and the College of Computer and information, Fujian Agriculture and Forestry University, Fuzhou, China. He has been awarded with Mingjian Scholar Chair Professor and Fujian Hundred-talents Program in Fujian Province, China. He has authored more 200 journal papers on signal processing and communications, with more than 110 SCI-indexed papers and more than 90 IEEE journal papers. He holds ten Chinese patents.



Jun Li (M'09–SM'16) received the Ph.D. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2009. From January 2009 to June 2009, he was with the Department of Research and Innovation, Alcatel Lucent Shanghai Bell, as a Research Scientist. Since 2015, he has been with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. His research interests include network information theory, channel coding theory, wireless network coding, and cooperative communications.