Jamming Signal Cancellation by Channel Inversion Power Control for Preserving Covert Communications

Ngo Thanh Hai and Dang Le Khoa

Department of Telecommunications and Networks, University of Science, VNU-HCM, Ho Chi Minh, Viet Nam

https://doi.org/10.26636/jtit.2023.169323

Abstract — Uninformed jammers are used to facilitate covert communications between a transmitter and an intended receiver under the surveillance of a warden. In reality, the signals the uniformed jammer emits to make the warden's decision uncertain have inadvertently interfered with the detection of the intended receiver. In this paper, we apply truncated channel inversion power control (TCIPC) to both the transmitter and the uninformed jammer. The TCIPC scheme used on the uninformed jammer may help the intended receiver remove jamming signals using the successive interference cancellation (SIC) technique. Under the assumption that the warden knows the channel coefficient between two intended transceivers and achieves the optimal detection power threshold, we form the optimization problem to maximize the effective transmission rate (ETR) under covertness and decoding constraints. With the aim of enhancing covertness-related performance, we achieve the optimal power control parameters and determine system parameter-related constraints required for the existence of these solutions. According to the simulations, the use of the TCIPC scheme on the uninformed jammer significantly improves covertness-related performance in comparison to that of random power control (RPC) and constant power control (CPC) schemes. In addition, simulation results show that, for the TCIPC scheme: 1) the maximum ETR tends to converge as the transmitter's or the uninformed jammer's maximum transmit power increases, and 2) there exists an optimal value of the transmitter's predetermined transmission rate to achieve the optimal performance.

Keywords — channel inversion power control, covert wireless communication, effective transmission rate, uninformed jammer.

1. Introduction

The development of next generation wireless networks (5G and beyond), combined with the increasing use of the Internet of Things (IoT), has resulted in a large amount of private and secure information being transmitted over wireless networks. However, due to nature of the wireless medium in which the broadcasts take place, it is easy to overhear the transmission. Traditional security techniques have utilized encryption to guarantee the confidentiality of information exchanged over the wireless channel. Unfortunately, in recent years, encryption techniques may be compromised by powerful adversaries (e.g. a quantum computer) [1]. In addition, decryption is sometimes unnecessary in certain applications. For instance, in military communications, the detection of a transmission may reveal the actual activity and its location within a given region. Therefore, physical layer security has emerged as a promising research direction for ensuring the privacy of users and requiring simple computations to be performed on the devices. Covert wireless communication is a peculiar type of a physical layer security solution, as it offers good security and privacy levels, not only protecting the content of communications but also hiding the existence of wireless transmissions [2].

The first studies focusing on covert wireless communications were performed by Bash *et al.* [3]. The authors built square root law over additive white Gaussian noise (AWGN) channels stating that $o\left(\sqrt{n}\right)$ bits may be sent from the transmitter to the receiver over n channel uses, while lower-bounding the detection error of a warden to no less than a specified value ε. This pioneering work opened up two research directions:

- exploring the fundamental limits of covert communications in [3] to identify the amount of information that may be conveyed covertly via a legitimate channel,
- developing advanced techniques to improve covertness-related performance.

As far as the former of the aforementioned research directions is concerned, subsequent work has expanded the results concerning the covert information theory for binary symmetrical channels (BSC) [4], discrete memory-less channels (DMC) [5], and the AWGN channel [6]. The researchers aim to investigate and extend the square root law to various wireless channel models. However, research described in [7] has pointed out that according to the square root law, the achievable covert rate would approach zero as $n \to \infty$, which is completely undesired. Therefore, the latter research direction has emerged in an attempt to solve this problem.

This type of research aims to attain a positive covert rate. The addition of artificial noise (AN) is one of the transmission strategies seeking to effectively improve covertness-related performance. The authors in [8] investigated the covert throughput in device-to-device communications. Here, a base station was equipped with an antenna array to transmit artificial noise. The artificial noise source was also set up on a legitimate receiver [9] adopted channel inversion power control (CIPC) to achieve covert communications. He *et al.*

extended covertness-related research by deploying dedicated jammers in a Poisson field of interferers [10]. As a result, the authors showed that as long as the interference-limited region is taken into account, the density and transmit power of the interferers do not affect the covert throughput. Covert communications can also be achieved with multi-hop routing transmission strategies. In [11], the authors considered multi-hop covert communications in the presence of multiple collaborating wardens and came up with efficient algorithms to identify optimal paths. In particular, covert communications and secure transmissions were jointly addressed in untrusted relaying networks with multiple wardens [12]. Unmanned aerial vehicles (UAVs) were also explored in the context of multi-hop transmissions, acting in the capacity of covert assistants [13] or wardens [14].

As far as transmission strategies with artificial noise are concerned, apart from additional noise modules installed on the source or destination side [8], [9], the adoption of dedicated noise nodes – “jammers” – in the environment has resulted in effective covertness. Adjustment of the jammer’s system parameters and fading properties affecting its communication with other nodes has resulted in uncertain decisions being taken by wardens with regard to the presence of legitimate nodes. The first type of jammer applied to covert communication is the uninformed jammer [15]. In this case, the jammer sends jamming signals simultaneously with covert signals and without cooperation with the source. The authors in [15] analyzed system performance focusing on the AWGN channel and the block fading channel. They showed, in particular, that a positive rate of covert communication exists on the hidden channel.

Capturing salient aspects of a continuous-time covert communication system as time T and bandwidth W, the authors in [16] investigated covertness on the continuous-time channel. In this channel in particular, research has shown that $\mathcal{O}(WT)$ information bits can be transmitted covertly and reliably with the assistance of an uninformed jammer. Power adaptations aiming to enhance covertness-related performance were studied in [17]. The authors sought the optimal power adaptation that minimizes the average outage probability subject to the covertness constraint. This optimal problem was analyzed under two scenarios: the AWGN model and the Rayleigh fading model for the uninformed jammer-to-warden channel.

Even though uninformed jammers result in a decrease in the warden’s detection accuracy, the lack of coordination between the transmitter and jammers considerably affects the performance of the desired covert communication. Cooperative jammers are designed to balance the detection error of the wardens with the covertness-related performance of the system. The authors in [18] used a relay as a cooperative jammer for achieving covertness. An assumption has been made that a pre-shared secret enables the permissible nodes to know which slot will be used for the transmission of covert information. Hence, for slots without covert information to send, the relay acts as a cooperative jammer with random noise power. Conversely, the relay amplifies and forwards information in covert transmission slots. Multiple friendly helper nodes have been considered for covert communication [7]. Here, the instantaneous channel gains to the legitimate receiver are known to those helpers. If those gains fall below a pre-established selection threshold, the respective helpers will be chosen to transmit jamming signals.

A more general study was implemented in [19] in order to compare three node schemes: uninformed, informed, and coordinated jammers. In the context of coordination, a jammer can coordinate with the transmitter via a secret key. In particular, the authors found out the fundamental interplay between the covert communication rate, local randomness, and the secret key rate. It is expected that the cooperating nodes will not only decrease the warden’s ability to detect, but also will rarely interfere with the legitimate signal.

As proposed in [20], the cognitive jammer is a jamming strategy aimed at improving covertness-related performance. Normally, the cognitive jammer includes a sensing module for making decisions. If it determines that no covert communication is taking place, it will send jamming signals and will remain silent otherwise. In [20], the cognitive jammer divides the time of an n-symbols block fading into two parts: 1) the time of the first m symbols for sensing channels, and 2) the time of the remaining $n - m$ symbols for jamming the signal transmission. In fact, the cognitive jammer identifies the transmitter’s transmitting state as quickly as possible, so m is taken as insignificant relative to n. However, because the warden detects the transmission using all n symbols, the cognitive jammer is ineffective in detecting channel usage in comparison to the warden’s ability to detect it. In particular, if the warden is aware of the cognitive parameter m, in the worst-case scenario, it can make the detection decision at the time of transmitting the first m symbols, when there are no jamming signals. Consequently, the cognitive jamming scheme will be a potential research direction in the future.

With the cooperative jammer, we need to negotiate the time slot for sending out jamming signals between the jammer and the transmitter. On the other hand, if we adopt the cognitive jammer for covert communication, it will be necessary to divide the time slot for sensing the transmitting state effectively. Without negotiation and continuity of jamming signals, they are robust properties of the uninformed jammer, but the intended receiver must suffer interference from the jammer due to the random transmit power.

In this paper, we apply truncated channel inversion power control (TCIPC) [9] to the uninformed jammer to aid in removing interference at the intended receiver. With TCIPC, the power received from the uninformed jammer is a fixed value, so the successive interference cancellation (SIC) technique can be relied upon to achieve desired signals. Furthermore, the signals received at the warden still depend on random values. The contributions of this paper are as follows:

– We consider a system model consisting of a transmitter, an intended receiver, a warden, and an uninformed jammer. The TCIPC scheme is adopted at the transmitter and the uninformed jammer. Based on the TCIPC scheme, the intended receiver uses SIC to cancel jamming signals. Moreover, we consider the worst-case scenario when the warden knows the channel coefficient between two legitimate transceivers.

- We analyze the detection error probability (DEP) for the warden, the connection outage probability for the intended receiver, and the effective transmission rate (ETR) for the system. This analysis lets us determine the optimal power control parameters of the transmitter and the jammer in order to maximize ETR under covertness and decoding constraints.
- In terms of covertness-related performance, the TCIPC scheme is compared with previous transmission schemes of the uninformed jammer, such as random power control (RPC) and constant power control (CPC) solutions. In addition, we also assess the effect that the system's parameters exert on covertness-related performance.

The rest of this paper is organized as follows. Section 2 describes the system model, the communication scenario and the detection strategy with a radiometer of the warden. In Section 3, we analyze the covertness-related performance and formulate the optimization problem under covertness and decoding constraints. Work focusing on RPC and CPC schemes is described in Section 4. Numerical results are presented in Section 5 to verify the analytical results and to provide useful insights into the impact of the system's parameters. Finally, conclusions are drawn in Section 6.

Notation: The modulus of a complex number is denoted by $|.|$, and the sign $(.)^*$ means its conjugation. Scalar variables are expressed as italic symbols. Vectors are denoted as lower-case boldface symbols. The expectation of a random variable is denoted $\mathrm{E}[.]$.

2. System Model

2.1. Communication Scenario

We consider a covert communication model depicted in Fig. 1, where the transmitter (Alice) intends to transmit covert information to the receiver (Bob) in the presence of the warden (Willie). The uninformed jammer (Jammer) sends jamming signals to support covert communication from Alice to Bob by confusing Willie's detection. We assume that Alice-to-Bob, Jammer-to-Bob, and Jammer-to-Willie wireless channels are block quasi-static Rayleigh fading, with the channel coefficients of $h_{u,v} \sim \mathcal{CN}(0, \lambda_{u,v})$, $\lambda_{u,v} = d_{u,v}^{-\theta}$, where the subscript (u, v) can be (a, b), (j, b), and (j, w), responding to the above links. The distance from node u to node v is denoted as $d_{u,v}$ and θ is the path loss exponent. Due to block quasi-static Rayleigh fading, $h_{u,v}$ is constant in one block fading but varies from one block to another. All nodes are equipped with a single antenna.

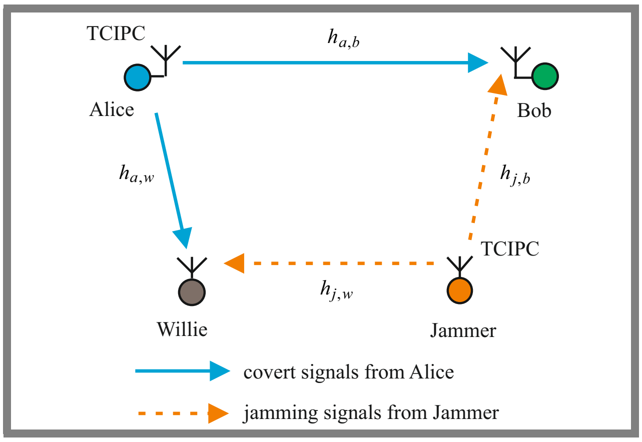

Fig. 1. Covert communication network model with the TCIPC scheme for Alice and Jammer.

Ordinarily, Willie finds it hard to estimate the channel coefficient between Alice and Bob due to their different locations. It is widely believed that a half-wavelength guard zone is sufficient to decorrelate the warden channel. However, a comprehensive study performed in [21], [22] has shown that for many correlation channel models, the warden can obtain largely correlated observations, even for large spatial separations, when Willie is still within the line-of-sight beam of the Alice-to-Bob link. Thus, Willie is able to obtain some leakage about $h_{a,b}$. Because we feel skeptical about this risk, we make a conservative assumption that Willie knows $h_{a,b}$. Furthermore, from a security standpoint, we place Alice in a pessimistic position and Willie in an optimistic position. Therefore, it is quite proper to assume that the Alice-to-Willie channel is an AWGN channel. We can mathematically express the Alice-to-Willie link as $h_{a,w} = \sqrt{\lambda_{a,w}}$, and $\lambda_{a,w} = d_{a,w}^{-\theta}$, where $h_{a,w}$ and $d_{a,w}$ are the channel coefficient and the distance of this link, respectively [17].

Bob broadcasts, periodically, pilot signals to enable channel estimation at Alice and Jammer ($h_{a,b}$ and $h_{j,b}$, respectively). Normally, channel estimation is necessary for Bob to detect signals, so Alice needs to send a pilot. However, her pilot transmission might increase the ability of Willie's detection. Therefore, we apply the TCIPC scheme to the Alice transmitter to hide the communication. Based on the TCIPC principle, Alice only transmits covert signals with power P_a when the channel power gain from Alice to Bob is greater than a certain value. The transmit power P_a varies as $|h_{a,b}|^2$ to keep the received power at Bob constant, and it is expressed as:

$$P_a = \begin{cases} \dfrac{\mathrm{Q}_a}{|h_{a,b}|^2}, & |h_{a,b}|^2 \geqslant \dfrac{\mathrm{Q}_a}{P_a^{max}} \\ 0 \quad , & |h_{a,b}|^2 < \dfrac{\mathrm{Q}_a}{P_a^{max}} \end{cases}, \tag{1}$$

where P_a^{max} is the maximum transmit power of Alice. We also use the TCIPC scheme at Jammer to help Bob cancel jamming signals. Then, the transmit power P_j of Jammer is given by:

$$P_j = \begin{cases} \dfrac{\mathrm{Q}_j}{|h_{j,b}|^2}, & |h_{j,b}|^2 \geqslant \dfrac{\mathrm{Q}_j}{P_j^{max}} \\ 0 \quad , & |h_{j,b}|^2 < \dfrac{\mathrm{Q}_j}{P_j^{max}} \end{cases}, \tag{2}$$

where P_j^{max} is the maximum transmit power of Jammer.

It is shown that P_j is a random value and changes with $h_{j,b}$ which leads to uncertainty in Willie's decision. Moreover, Willie does not know $h_{j,w}$, which is also a factor contributing to this uncertainty. Alice only transmits covert signals when the necessary condition T_a is met (i.e., $|h_{a,b}|^2 \geqslant \frac{\mathrm{Q}_a}{P_a^{max}}$). Thus, the probability of T_a is given by:

$$\begin{aligned} P_{T_a} &= \Pr\left(|h_{a,b}|^2 \geqslant \frac{\mathrm{Q}_a}{P_a^{max}}\right) \\ &= \mathrm{e}^{-\frac{\mathrm{Q}_a}{\lambda_{a,b} P_a^{max}}} . \end{aligned} \tag{3}$$

Similarly, the probability of the transmission condition T_j (i.e., $|h_{j,b}|^2 \geqslant \frac{\mathrm{Q}_j}{P_j^{max}}$) of Jammer is expressed as:

$$\begin{aligned} P_{T_j} &= \Pr\left(|h_{j,b}|^2 \geqslant \frac{\mathrm{Q}_j}{P_j^{max}}\right) \\ &= \mathrm{e}^{-\frac{\mathrm{Q}_j}{\lambda_{j,b} P_j^{max}}} . \end{aligned} \tag{4}$$

2.2. Detection Strategy with a Radiometer at Willie

When the condition T_j fails, Jammer does not transmit jamming signals and sends a negative acknowledgment (NAK) to inform his transmission state [23]. In this case, Alice remains silent due to the lack of a shield from Jammer. When Jammer sends out jamming signals, Alice will receive an acknowledgment (ACK) from Jammer and will transmit covert signals when the condition T_a is true with a probability of $\frac{1}{2}$. Willie's received signal in the i-th channel use within a specific time slot is given by:

$$\mathbf{y}_w(i) = \begin{cases} \sqrt{P_j} h_{j,w} \mathbf{x}_j(i) + \mathbf{n}_w(i), & H_0 \\ \sqrt{P_a} h_{a,w} \mathbf{x}_a(i) + \sqrt{P_j} h_{j,w} \mathbf{x}_j(i) + \mathbf{n}_w(i), & H_1, \end{cases} \tag{5}$$

where $i = 1, \ldots, n$ is the index of channel use. Vectors $\mathbf{x}_j = \frac{h_{j,b}^*}{|h_{j,b}|}\mathbf{x}_j'$, and $\mathbf{x}_a = \frac{h_{a,b}^*}{|h_{a,b}|}\mathbf{x}_a'$ are the signals transmitted by Jammer and Alice with $\mathrm{E}\left[|\mathbf{x}_j'(i)|^2\right] = \mathrm{E}\left[|\mathbf{x}_a'(i)|^2\right] = 1$, respectively [9]. Vector $\mathbf{n}_w$ is the AWGN at Willie with the variance of each element as σ_w^2. The null hypothesis H_0 states that Alice does not transmit signals and the alternative hypothesis H_1 means that Alice is transmitting signals. Similarly to [17], [24], [25], the decision rule with a radiometer in the detector at Willie is:

$$P_w \underset{D_0}{\overset{D_1}{\gtrless}} \tau \,, \tag{6}$$

where $P_w = \frac{1}{n}\sum\limits_{i=1}^{n} |\mathbf{y}_w(i)|^2$ is the average received power in a time slot, and τ is the detection power threshold at Willie, while D_0 and D_1 are Willie's decisions that determine H_0 and H_1, respectively. The detection performance of Willie is measured by the detection error probability (DEP) such as:

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

where $\alpha = \Pr\left(D_1 | H_0, T_j\right)$ is the false alarm probability and $\beta = \Pr\left(D_0 | H_1, T_j\right)$ is the miss detection probability.

3. Analysis and Optimization of Covertness-related Performance

3.1. Detection Performance at Willie

We use the outage approach to analyze detection performance at Willie. This approach aims at suppressing the dependence on the number of transmitted symbols n by letting $n \to \infty$ [17], [24], [25], P_w is given by:

$$P_w = \begin{cases} P_j |h_{j,w}|^2 + \sigma_w^2 & , \quad H_0 \\ P_a \lambda_{a,w} + P_j |h_{j,w}|^2 + \sigma_w^2, & H_1 \end{cases} . \tag{8}$$

Then, in Lemma 1, we have the following characterizations for the false alarm and miss detection probabilities at Willie.

Lemma 1. The false alarm and miss detection probabilities at Willie are expressed respectively as:

$$\alpha = \begin{cases} 1 & , \quad \tau \leqslant \sigma_w^2 \\ \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau - \sigma_w^2)\lambda_{j,b} + \lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau - \sigma_w^2}{\lambda_{j,w} P_j^{max}}} & , \quad \tau > \sigma_w^2 \end{cases} , \tag{9}$$

$$\beta = \begin{cases} 0 & , \quad \tau \leqslant \Omega \\ 1 - \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau - \Omega)\lambda_{j,b} + \lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau - \Omega}{\lambda_{j,w} P_j^{max}}} & , \quad \tau > \Omega \end{cases} , \tag{10}$$

where $\Omega = \frac{\mathrm{Q}_a}{|h_{a,b}|^2}\lambda_{a,w} + \sigma_w^2$.

Proof: See Appendix A.

Following Eqs. (9) and (10), we get the DEP of Willie as:

$$\begin{aligned} \xi &= \alpha + \beta \\ &= \begin{cases} 1 & , \quad \tau \leqslant \sigma_w^2 \\ \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau - \sigma_w^2)\lambda_{j,b} + \lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau - \sigma_w^2}{\lambda_{j,w} P_j^{max}}} & , \quad \sigma_w^2 \leqslant \tau \leqslant \Omega \\ 1 - \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau - \Omega)\lambda_{j,b} + \lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau - \Omega}{\lambda_{j,w} P_j^{max}}} & \\ \quad + \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau - \sigma_w^2)\lambda_{j,b} + \lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau - \sigma_w^2}{\lambda_{j,w} P_j^{max}}} & , \quad \Omega \leqslant \tau \end{cases} . \end{aligned} \tag{11}$$

We note that the false alarm and miss detection probabilities are expressed with an arbitrary detection power threshold τ. In fact, Willie will modify the system parameters to minimize DEP and make covert communications more difficult. In this section, Willie makes adjustments to threshold τ for a decision. We derive the optimal detection power threshold and the minimum DEP for Willie in Theorem 1.

Theorem 1. Willie's optimal detection power threshold is given by:

$$\tau^* = \frac{\mathrm{Q}_a}{|h_{a,b}|^2}\lambda_{a,w} + \sigma_w^2, \tag{12}$$

and the corresponding minimum DEP is expressed as:

$$\xi^* = \frac{\lambda_{j,w}\mathrm{Q}_j |h_{a,b}|^2}{\lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a + \lambda_{j,w}\mathrm{Q}_j |h_{a,b}|^2} \mathrm{e}^{-\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w} P_j^{max} |h_{a,b}|^2}} . \tag{13}$$

Proof: See Appendix B.

We want to determine the optimal power control parameters Q_a and Q_j in order to maximize the effective transmission rate of the system under covertness and decoding constraints (as discussed in the following section). Assuming that the covertness constraint is stated as having Wille's minimum detection error probability that is greater than a given threshold, then the optimal values of Q_a and Q_j will be expressed as functions of $h_{a,b}$. However, Jammer is unaware of $h_{a,b}$, and Bob needs a fixed received power of Q_a to decode Alice's signals. Therefore, we denote the expected value of ξ^* with all possible values of $h_{a,b}$ as a performance parameter whose characterization is expressed in Lemma 2.

Lemma 2. A lower bound of the expected value of the minimum DEP is given by:

$$\overline{\xi}^* > \overline{\xi}_l^*, \tag{14}$$

where

$$\overline{\xi}_l^* = \frac{1}{\lambda_{a,b}} \int_0^\infty \frac{\lambda_{j,w}\mathrm{Q}_j x}{\lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a + \lambda_{j,w}\mathrm{Q}_j x} \mathrm{e}^{-\left(\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max}x} + \frac{1}{\lambda_{a,b}}x\right)} \mathrm{d}x\,.$$

Proof: See Appendix C.

3.2. Connection Outage Probability at Bob

When Alice and Jammer transmit covert signals and jamming signals to Bob, respectively, the signal received in the i-th channel use within a time slot is:

$$\begin{aligned}\mathbf{y}_b(i) &= \sqrt{P_a}h_{a,b}\mathbf{x}_a(i) + \sqrt{P_j}h_{j,b}\mathbf{x}_j(i) + \mathbf{n}_b(i) \\ &= \sqrt{\mathrm{Q}_a}\mathbf{x}'_a(i) + \sqrt{\mathrm{Q}_j}\mathbf{x}'_j(i) + \mathbf{n}_b(i),\end{aligned} \tag{15}$$

where vector $\mathbf{n}_b$ is the AWGN at Bob with the variance of each element expressed as σ_b^2. We use the successive interference cancellation (SIC) technique [25], [26] – widely used in the non-orthogonal multiple access (NOMA) systems – to decode Jammer's and Alice's signals at Bob. According to SIC, Bob first decodes Jammer's signals, and then cancels them from the received signals and decodes Alice's signals. Thus, the received signal-to-interference and noise ratio (SINR) corresponding to the process of detecting Jammer's signals at Bob is:

$$\gamma_j = \frac{\mathrm{Q}_j}{\mathrm{Q}_a + \sigma_b^2}\,. \tag{16}$$

The condition for SIC carried out successfully at Bob is expressed as [25]:

$$\gamma_j \geqslant 2^{R_j} - 1\,, \tag{17}$$

where R_j is the predetermined transmission rate of Jammer. After Jammer's signals are eliminated, the signal-to-noise ratio (SNR) of Alice's signals is:

$$\gamma_a = \frac{\mathrm{Q}_a}{\sigma_b^2}\,. \tag{18}$$

We assume that the predetermined transmission rate of Alice is R_a, the condition for the successful detection of Alice's signals is expressed as:

$$\gamma_a \geqslant 2^{R_a} - 1\,. \tag{19}$$

It is noted that since the TCIPC scheme is applied to both Alice and Jammer, γ_j and γ_a do not depend on random variables. In the formulation of the optimization problem, we can set Q_j and Q_a such that the decoding constraints in Eqs. (17) and (19) are satisfied, and Bob can decode the signals successfully.

Remark 1. Willie treats Jammer's signals as jamming signals because channel coefficients $h_{j,w}$ and $h_{j,b}$ are unavailable at Willie. On the other hand, Jammer can work as an associate of Bob to aid covert communications. For example, Bob places Jammer in a communication zone to send out jamming signals and collect sensitive information from Willie, such as location, detection techniques, and so on. However, in order for Bob to achieve information from Jammer, Bob's received power needs to match a fixed value for Jammer's signals. A common way is for Jammer to adopt a constant transmit power as well as send pilots for Bob's channel estimation. Nevertheless, in the worst case, when Willie can get $h_{j,w}$ from Jammer's pilots, covert communications will be discontinued due to the lack of random sources in Willie's received power. The TCIPC scheme is a simple technique to guarantee a constant received power at Bob by utilizing pilots transmitted from Bob instead of Jammer. Furthermore, thanks to the TCIPC scheme, both $h_{j,b}$ and $h_{j,w}$ are factors confusing Willie's decision. When the received power matches a defined value, SIC is applied to Bob to decode Jammer's and Alice's signals.

3.3. Optimal Power Control Parameters for Jammer and Alice

In this section, we optimize covertness-related performance to meet both Bob's reliability and the system's covertness requirements. We define the effective transmission rate R_e which quantifies the amount of information that can be reliably transmitted from Alice to Bob when the decoding constraints are satisfied, as follows:

$$\begin{aligned}R_e &= \frac{1}{2}R_a P_{T_a} P_{T_j} \\ &= \frac{1}{2}R_a \mathrm{e}^{-\left(\frac{\mathrm{Q}_a}{\lambda_{a,b}P_a^{max}} + \frac{\mathrm{Q}_j}{\lambda_{j,b}P_j^{max}}\right)},\end{aligned} \tag{20}$$

where factor $\frac{1}{2}$ is the transmission probability of Alice when condition T_a is true. We set $1-\varepsilon$ as the covertness threshold. Then, the problem of optimizing the power control parameters Q_j and Q_a, maximizing R_e under the covertness constraint C_1 and the constraints for successful decoding C_2, C_3 is:

$$\begin{aligned}&\underset{\mathrm{Q}_j,\mathrm{Q}_a}{\text{Argmax}} \quad R_e, \\ &\text{subject to:} \\ &\qquad C_1:\ \overline{\xi}_l^* \geqslant 1-\varepsilon\,, \\ &\qquad C_2:\ \gamma_j \geqslant 2^{R_j}-1\,, \\ &\qquad C_3:\ \gamma_a \geqslant 2^{R_a}-1\,.\end{aligned} \tag{21}$$

The covertness constraint C_1 is still ensured when we allow $\overline{\xi}_l^*$ to be greater than $1-\varepsilon$. For ease of representation, we put $F(Q_j, Q_a) = \overline{\xi}_l^* - (1-\varepsilon)$, then the solutions to the optimization problem are expressed in the following theorem.

Theorem 2. For the optimization problem in Eq. (21), the constraint C regarding system parameters for the existence of optimal solutions is:

$$2\sqrt{\frac{\lambda_{a,w}\left(2^{R_a}-1\right)\sigma_b^2}{\lambda_{j,w}\lambda_{a,b}P_j^{max}}}K_1\left(2\sqrt{\frac{\lambda_{a,w}\left(2^{R_a}-1\right)\sigma_b^2}{\lambda_{j,w}\lambda_{a,b}P_j^{max}}}\right)\geqslant 1-\varepsilon, \tag{22}$$

where $K_1(.)$ is the modified Bessel function of the second kind [27]. Let $\mathrm{Q}_j^\dagger$ be the solution of $F\left[\mathrm{Q}_j,\left(2^{R_a}-1\right)\sigma_b^2\right]=0$, when the condition of system parameters satisfies Eq. (22), the optimal choices of Q_j and Q_a for the optimization problem are expressed as:

$$\begin{aligned}\mathrm{Q}_j^* &= \max\left[\left(2^{R_j}-1\right)2^{R_a}\sigma_b^2,\mathrm{Q}_j^\dagger\right],\\ \mathrm{Q}_a^* &= \left(2^{R_a}-1\right)\sigma_b^2.\end{aligned} \tag{23}$$

Proof: See Appendix D.

4. Work on RPC and CPC

Here, we analyze the system's performance for two Jammer-related schemes: random power control (RPC) and constant power control (CPC). This serves as a foundation for comparing them with the TCIPC scheme.

4.1. Random Power Control Scheme

For the RPC scheme, the transmit power of Jammer changes randomly and obeys a continuous uniform distribution over the interval $[0, P_j^{max}]$ [9], [17], with the probability distribution function given by:

$$f_{P_j}(x)=\begin{cases}\frac{1}{P_j^{max}}, & 0\leqslant x\leqslant P_j^{max}\\ 0\quad, & \text{otherwise.}\end{cases} \tag{24}$$

Following the decision rule given in Eq. (6) and using the same argument as in Lemma 1, we obtain the false alarm probability as:

$$\begin{aligned}\alpha &= \Pr\left(P_w\geqslant\tau|\,H_0\right)\\ &= \Pr\left(P_j\left|h_{j,w}\right|^2+\sigma_w^2\geqslant\tau\right)\\ &= \begin{cases}1 &, \quad \tau\leqslant\sigma_w^2\\ \int_0^{P_j^{max}}\int_{\frac{\tau-\sigma_w^2}{x}}^{\infty} f_{P_j}(x)f_{\left|h_{j,w}\right|^2}(y)\mathrm{d}y\mathrm{d}x, & \tau>\sigma_w^2\end{cases}\\ &= \begin{cases}1 &, \quad \tau\leqslant\sigma_w^2\\ \int_0^{P_j^{max}}\int_{\frac{\tau-\sigma_w^2}{x}}^{\infty}\frac{1}{P_j^{max}\lambda_{j,w}}\mathrm{e}^{-\frac{1}{\lambda_{j,w}}y}\mathrm{d}y\mathrm{d}x, & \tau>\sigma_w^2\end{cases}\\ &= \begin{cases}1 &, \quad \tau\leqslant\sigma_w^2\\ \frac{1}{P_j^{max}}\int_{\frac{1}{P_j^{max}}}^{\infty}\frac{1}{t^2}\mathrm{e}^{-\frac{\tau-\sigma_w^2}{\lambda_{j,w}}t}\mathrm{d}t, & \tau>\sigma_w^2\end{cases}\\ &\overset{(c)}{=} \begin{cases}1 &, \quad \tau\leqslant\sigma_w^2\\ \frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}\mathrm{Ei}\left(-\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}\right)+\mathrm{e}^{-\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}}, & \tau>\sigma_w^2.\end{cases}\end{aligned} \tag{25}$$

In Eq. (25), we obtain step (c) by using Eq. (3.351 4) in [27], and $\mathrm{Ei}(x)=-\int_{-x}^{\infty}\frac{\mathrm{e}^{-t}}{t}\mathrm{d}t$ is the exponential integral function.

Similarly, the miss detection probability is:

$$\begin{aligned}\beta &= \Pr\left(P_w<\tau|\,H_1\right)\\ &= \Pr\left(P_j\left|h_{j,w}\right|^2+\Omega<\tau\right)\\ &= \begin{cases}0 &, \quad \tau\leqslant\Omega\\ 1-\frac{\tau-\Omega}{\lambda_{j,w}P_j^{max}}\mathrm{Ei}\left(-\frac{\tau-\Omega}{\lambda_{j,w}P_j^{max}}\right)-\mathrm{e}^{-\frac{\tau-\Omega}{\lambda_{j,w}P_j^{max}}}, & \tau>\Omega,\end{cases}\end{aligned} \tag{26}$$

where Ω is defined in Lemma 1. Then, the detection error probability (DEP) of the RPC scheme is:

$$\begin{aligned}\xi &= \alpha+\beta\\ &= \begin{cases}1 &, \quad \tau\leqslant\sigma_w^2\\ \frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}\mathrm{Ei}\left(-\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}\right)+\mathrm{e}^{-\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}} &, \quad \sigma_w^2\leqslant\tau\leqslant\Omega\\ 1-\frac{\tau-\Omega}{\lambda_{j,w}P_j^{max}}\mathrm{Ei}\left(-\frac{\tau-\Omega}{\lambda_{j,w}P_j^{max}}\right)-\mathrm{e}^{-\frac{\tau-\Omega}{\lambda_{j,w}P_j^{max}}} & \\ \quad+\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}\mathrm{Ei}\left(-\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}\right)+\mathrm{e}^{-\frac{\tau-\sigma_w^2}{\lambda_{j,w}P_j^{max}}} &, \quad \tau\geqslant\Omega.\end{cases}\end{aligned} \tag{27}$$

We define the $f(x)$ function as $f(x)=x\mathrm{Ei}(-x)+\mathrm{e}^{-x}$, then the first derivative of $f(x)$ is given by $f'(x)=\mathrm{Ei}(-x)$. Taking advantage of this result, for $\sigma_w^2\leqslant\tau\leqslant\Omega$, we can prove that the first derivative of ξ is observed to be less than 0 and ξ is a monotonically decreasing function of τ. In addition, due to $\Omega>\sigma_w^2$, the first derivative of ξ is positive when $\tau\geqslant\Omega$. In this case, ξ is a monotonically increasing function of τ. Thus, Willie will set the optimal detection power threshold as $\tau^*=\Omega$ and the corresponding minimum DEP is given by:

$$\begin{aligned}\xi^* =\ & \frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max}\left|h_{a,b}\right|^2}\mathrm{Ei}\left(-\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max}\left|h_{a,b}\right|^2}\right)\\ &+\mathrm{e}^{-\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max}\left|h_{a,b}\right|^2}}.\end{aligned} \tag{28}$$

Under the optimal power detection threshold setting from Eq. (28), the expected minimum DEP is defined as:

$$\begin{aligned}\overline{\xi}^* &= \mathrm{E}\left[\xi^*\left(\left|h_{a,b}\right|^2\right)\right]\\ &= \frac{1}{P_{T_a}}\int_{\frac{\mathrm{Q}_a}{P_a^{max}}}^{\infty}\xi^*(x)f_{\left|h_{a,b}\right|^2}(x)\mathrm{d}x\,.\end{aligned} \tag{29}$$

Alice uses the TCIPC scheme to transmit covert signals to Bob. Bob is unaware of channel state information of $h_{j,b}$, and the transmit power of Jammer is random, so he treats the Jammer's signals as interference. The SINR of decoding Alice's signals at Bob is represented as:

$$\gamma_a=\frac{\mathrm{Q}_a}{P_j\left|h_{j,b}\right|^2+\sigma_b^2}\,. \tag{30}$$

For the predetermined transmission rate of Alice as R_a, the connection outage performance at Bob is:

$$\begin{aligned}\delta &= \Pr\left(\gamma_a < 2^{R_a} - 1\right)\\ &= \Pr\left(P_j \left|h_{j,b}\right|^2 > \frac{\mathrm{Q}_a}{2^{R_a} - 1} - \sigma_b^2\right)\\ &\overset{(c)}{=} \begin{cases} 1 & , \quad \mathrm{Q}_a < \mathrm{Q}_l \\ \frac{\mathrm{Q}_a - \mathrm{Q}_l}{\left(2^{R_a}-1\right)\lambda_{j,b} P_j^{max}} \mathrm{Ei}\left[-\frac{\mathrm{Q}_a - \mathrm{Q}_l}{\left(2^{R_a}-1\right)\lambda_{j,b} P_j^{max}}\right] & \\ + \mathrm{e}^{-\frac{\mathrm{Q}_a - \mathrm{Q}_l}{\left(2^{R_a}-1\right)\lambda_{j,b} P_j^{max}}} & , \quad \mathrm{Q}_a \geqslant \mathrm{Q}_l , \end{cases}\end{aligned} \tag{31}$$

where $\mathrm{Q}_l = \left(2^{R_a} - 1\right)\sigma_b^2$, and the result in step (c) of Eq. (31) is based on the false alarm probability analysis in Eq. (25).

From Eqs. (29) and (31), we formulate the optimization problem for the RPC scheme with the effective transmission rate (ETR) R_e as the objective function and with the covertness constraint given by:

$$\begin{aligned} &\underset{\mathrm{Q}_a}{\text{Argmax}} \quad R_e = \tfrac{1}{2} R_a P_{T_a} (1 - \delta) \ , \\ &\text{subject to:} \quad \overline{\xi}^* \geqslant 1 - \varepsilon \ . \end{aligned} \tag{32}$$

The optimization problem Eq. (32) can be solved by numerical search in the set of Q_a which satisfies $\overline{\xi}^* \geqslant 1 - \varepsilon$.

4.2. Constant Power Control Scheme

In this subsection, we consider the constant power control (CPC) scheme in terms of optimizing ETR and satisfying the covertness constraint in order to provide a comparative evaluation of Jammer's different transmission schemes. As far as the CPC scheme is concerned, Jammer transmits jamming signals with the constant transmit power of P_j^{max}. Willie does not know the channel coefficient $h_{j,w}$, which makes his decision uncertain. Thus, by the same argument as in Lemma 1, we get the false alarm and miss detection probabilities, respectively, as:

$$\begin{aligned} \alpha &= \begin{cases} 1 & , \quad \tau \leqslant \sigma_w^2 \\ \mathrm{e}^{-\frac{\tau - \sigma_w^2}{\lambda_{j,w} P_j^{max}}} & , \quad \tau > \sigma_w^2 \ , \end{cases} \\ \beta &= \begin{cases} 0 & , \quad \tau \leqslant \Omega \\ 1 - \mathrm{e}^{-\frac{\tau - \Omega}{\lambda_{j,w} P_j^{max}}} & , \quad \tau > \Omega \ . \end{cases} \end{aligned} \tag{33}$$

From Eq. (33), we get the DEP of Willie as $\xi = \alpha + \beta$. Moreover, we can prove that Willie chooses $\tau^* = \Omega$ as an optimal detection power threshold for decision and the corresponding minimum DEP is:

$$\xi^* = \mathrm{e}^{-\frac{\mathrm{Q}_a \lambda_{a,w}}{\lambda_{j,w} P_j^{max} \left|h_{a,b}\right|^2}} \ . \tag{34}$$

According to Eq. (29), we also derive the expected minimum DEP $\overline{\xi}^*$ for the CPC scheme. Since the channel state information of $h_{j,b}$ is unavailable at Bob, the SINR corresponding to the process of detecting Alice's signals is written by:

$$\gamma_a = \frac{\mathrm{Q}_a}{P_j^{max} \left|h_{j,b}\right|^2 + \sigma_b^2} \ . \tag{35}$$

Hence, the connection outage performance at Bob is expressed as:

$$\begin{aligned}\delta &= \Pr\left(\gamma_a < 2^{R_a} - 1\right)\\ &= \Pr\left[\left|h_{j,b}\right|^2 > \frac{1}{P_j^{max}}\left(\frac{\mathrm{Q}_a}{2^{R_a} - 1} - \sigma_b^2\right)\right]\\ &= \begin{cases} 1 & , \quad \mathrm{Q}_a < \mathrm{Q}_l \\ \mathrm{e}^{-\frac{\mathrm{Q}_a - \mathrm{Q}_l}{\left(2^{R_a}-1\right)\lambda_{j,b} P_j^{max}}} & , \quad \mathrm{Q}_a \geqslant \mathrm{Q}_l \ . \end{cases}\end{aligned} \tag{36}$$

Similar to the RPC scheme in Eq. (32), we formulate the optimization problem for the CPC scheme at Alice, which can be solved by numerical search in the set of Q_a satisfying $\overline{\xi}^* \geqslant 1 - \varepsilon$.

5. Numerical Results

In this section, we conduct numerical simulations to verify the detection performance of Willie and the covertness-related performance of the system. Without loss of generality, the system parameters are set to $d_{a,b} = 25$ m, $d_{a,w} = 35$ m, $d_{j,w} = 15$ m, $d_{j,b} = 20$ m, $\alpha = 2$, $\sigma_w^2 = \sigma_b^2 = 0$ dBm and $\varepsilon = 0.2$.

Figure 2 shows false alarm probability α, miss detection probability β, and detection error probability ξ versus Willie's detection power threshold τ for Jammer's three transmission schemes: TCIPC, RPC, and CPC. We set $P_a^{max} = 40$ dBm, $\mathrm{Q}_a = 25$ dBm, $P_j^{max} = 50$ dBm, $\mathrm{Q}_j = 30$ dBm, and $\left|h_{a,b}\right|^2 = \lambda_{a,b}$. We obtain Monte Carlo simulation results by generating a sufficiently large number of random values of $\left|h_{j,b}\right|^2$, $\left|h_{j,w}\right|^2$, and P_j. For the first observation of three schemes, the false alarm probability α decreases to 0 with the increase in τ. The miss detection probability β, in turn, first stays at 0, and as τ increases, β increases and eventually stays at 1. Moreover, we learn that the curves of the detection error probability ξ are the sum of α and β and have minimum values at $\tau^* = \Omega$ for all three of Jammer's transmission

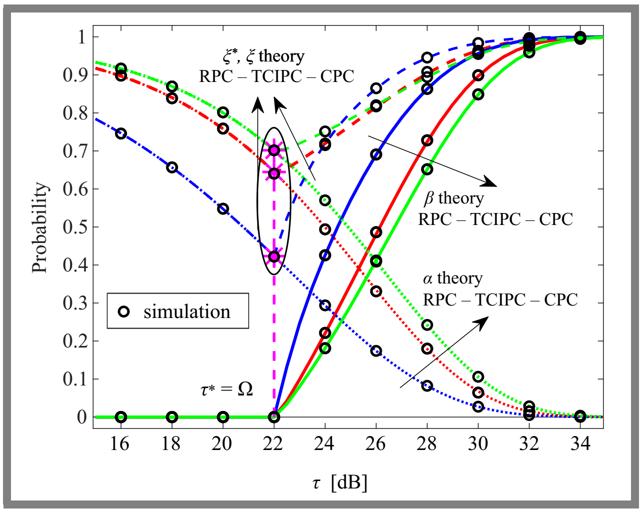

Fig. 2. False alarm probability α, miss detection probability β, and detection error probability ξ versus threshold τ for Willie's detection process with Jammer's three transmission schemes.

schemes. These results are consistent with the analytical results in Theorem 1, Subsections 4.1 and 4.2. As illustrated in Fig. 2, we also observe that the simulated points agree quite well with the theoretical ones. Especially, Jammer's transmission scheme with RPC offers the worst covertness-related performance of the three schemes, while the CPC scheme achieves superior performance compared to the two remaining schemes.

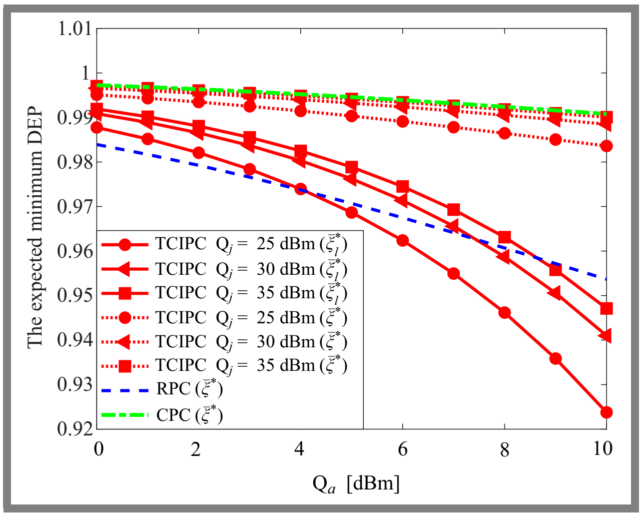

Fig. 3. Expected minimum DEP $\overline{\xi}^*$ and its lower bound $\overline{\xi}_l^*$ versus Q_a under varying values of Q_j.

In Fig. 3, the expected minimum DEP $\overline{\xi}^*$ is plotted versus Q_a for Jammer's three transmission schemes, and the lower bound of $\overline{\xi}^*$ is presented for the TCIPC scheme with varying values of the power control parameter Q_j. We set $P_a^{max} = 40$ dBm, $P_j^{max} = 50$ dBm, and $|h_{a,b}|^2 = \lambda_{a,b}$. For the TCIPC scheme, the numerical simulation results of the lower bound $\overline{\xi}_l^*$ are consistent with the exact results of $\overline{\xi}^*$ as in Lemma 2, so the covertness constraint is still guaranteed when we do not let the lower bound be lower than the covertness threshold. As one may observe from Fig. 3, $\overline{\xi}_l^*$ and $\overline{\xi}^*$ decrease gradually as Q_a increases for all three schemes. This is because the larger the value of Q_a, the easier the Willie's detection. The CPC scheme achieves superior performance in comparison to TCIPC and RPC schemes in terms of the expected minimum DEP. Let us now consider the TCIPC scheme, where the power control parameter of Jammer Q_j also has an effect on Willie's expected minimum DEP, i.e. $\overline{\xi}_l^*$ and $\overline{\xi}^*$ go up along with the increase in Q_j. This result indicates that it will become more challenging for Willie to detect Alice's signals as Jammer's noise source is amplified. In addition, in the high regime of Q_j as $\mathrm{Q}_j = 35$ dBm, the exact results of $\overline{\xi}^*$ of the TCIPC scheme converge to that of the CPC scheme. Mathematically, this result may be deduced from Eq. (13) and Eq. (34) when Q_j approaches infinity. To sum up, Fig. 3 shows that the appropriate values of the power control parameters Q_a and Q_j are very effective in confusing the detection at Willie.

In Fig. 4, we show the relationship between the effective transmission rate (ETR) R_e and the power control parameter Q_a for three transmission schemes. In the case of the TCIPC scheme, we also consider the impact of Q_j on the ETR. Here, we assume that $P_a^{max} = 40$ dBm, $P_j^{max} = 50$ dBm, $R_j = 2$ bits per channel use (bpcu), and $R_a = 3$ bpcu. As one may see from Fig. 4, the values of R_e equal 0 when an outage occurs in the system. For the TCIPC scheme, when the decoding constraints C_2 and C_3 are satisfied, the effective transmission rate R_e decreases gradually, as Q_a increases. This result is consistent with the proof of Theorem 2 in Appendix D.

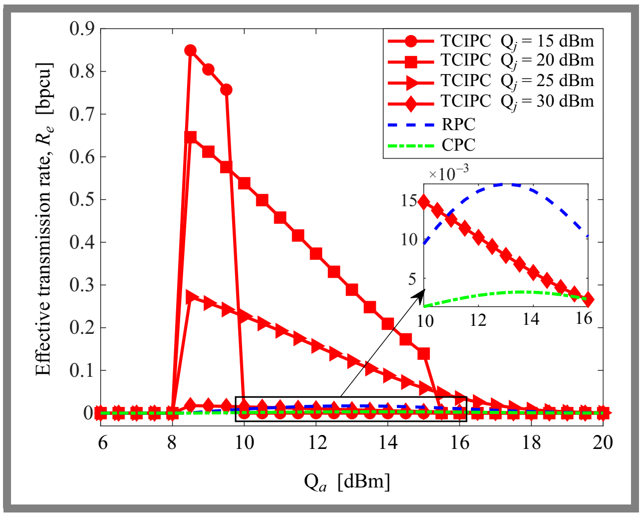

Fig. 4. Effective transmission rate R_e [bpcu] versus Q_a under different values of Q_j.

Regarding the RPC and CPC schemes, also in Fig. 4 we can observe that R_e initially increases and then decreases as Q_a increases, which indicates that there exists an optimal value of Q_a to maximize the ETR for the two schemes. In the TCIPC scheme, the power control parameter Q_j has a significant effect on the ETR of the system, i.e. the smaller the power control parameter Q_j is, the better the effective transmission rate R_e, and outperforming that of the RPC and CPC schemes. However, the outage region of the system is expanded with the decrease in Q_j since Bob's ability to successfully decode Jammer's and Alice's signal diminishes. According to Figs. 3 and 4, it is worth noting that selecting the appropriate values for Q_a and Q_j is necessary to achieve a balance between the effective transmission rate and the covertness constraint, which has been modeled in the optimization problem of the three transmission schemes.

Figures 5 and 6 depict the variation curves of the maximum effective transmission rate (ETR) R_e^* versus the maximum transmit power of Jammer and Alice, respectively, for Jammer's three transmission schemes. Here, we set $R_a = 3$ bpcu, and $R_j = 2$ bpcu. For the RPC and CPC schemes, the maximum ETR first increases and then decreases gradually, which reveals that there are optimal values for P_j^{max} and P_a^{max} to optimize the maximum effective transmission rate. This is due to the fact that when P_j^{max} increases, the covertness constraint approaches the satisfaction point and there is a positive ETR for the system; however, a large P_j^{max} may have a negative effect on increasing the interference at Bob (due to a predefined value of P_a^{max}). Regarding P_a^{max} for the RPC and CPC schemes, P_a^{max} has a dual impact on the system's performance, as increasing P_a^{max} not only decreases Willie's detection error probability, but also increases Alice's transmission probability (i.e. P_{T_a}). This observation suggests that, in addition to optimizing the parameter Q_a, we also have to select optimal values for parameters P_j^{max} and P_a^{max} in order to achieve optimal performance of the RPC and CPC schemes.

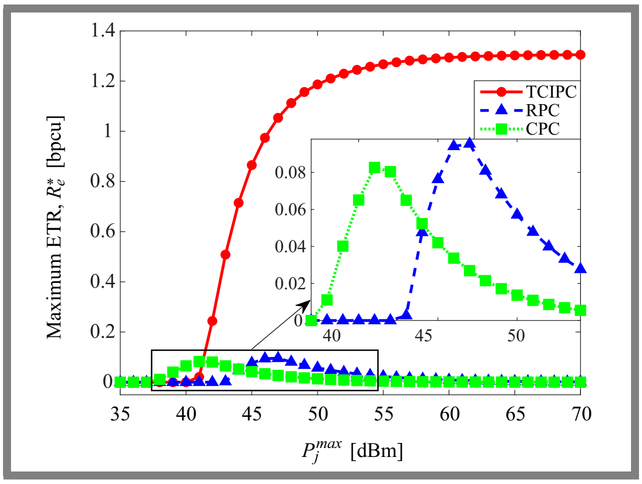

Fig. 5. Maximum effective transmission rate R_e^* versus P_j^{max} for Jammer's three transmission schemes.

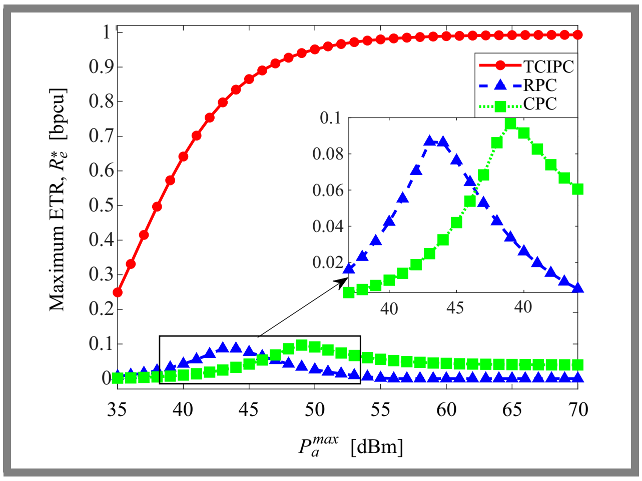

Fig. 6. Maximum effective transmission rate R_e^* versus P_a^{max} for Jammer's three transmission schemes.

For the TCIPC scheme, R_e^* increases gradually as P_j^{max} and P_a^{max} increase, and then converges to a constant value. Typically, an increase in P_j^{max} not only causes Willie's decision to be uncertain, but also has a negative impact on Bob's decoding. However, in the TCIPC scheme, the SIC technique is adopted to help Bob cancel interference and successfully decode the desired signals. As P_j^{max} approaches infinity, the Jammer's transmission probability increases (i.e. P_{T_j}), allowing the maximum ETR to converge to an upper limit. In the optimization problem of the TCIPC scheme, Q_j^*, Q_a^*, and the lower bound of $\overline{\xi}^*$ are independent of P_a^{max}, so an increase in P_a^{max} causes Alice's transmission to become more frequent and the maximum ETR to reach a constant value. Thus, with the TCIPC scheme, increasing P_j^{max} or P_a^{max} blindly can not continuously improve the maximum ETR. Specifically, in terms of the maximum effective transmission rate, the TCIPC scheme outperforms both the RPC and CPC schemes.

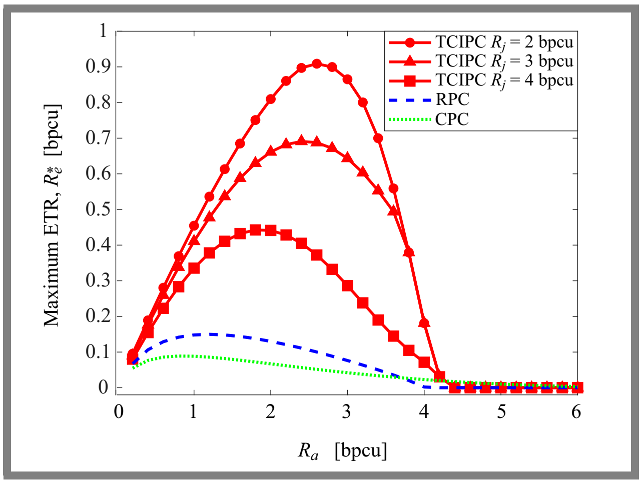

Fig. 7. Maximum effective transmission rate R_e^* versus predetermined transmission rate of Alice R_a under different values of R_j.

In Fig. 7, we show the maximum effective transmission rate (ETR) of R_e^* versus Alice's predetermined transmission rate R_a. Using the TCIPC scheme, we also depict the maximum ETR for various values of Jammer's predetermined transmission rate R_j. Here, we assume that $P_j^{max} = 45$ dBm, and $P_a^{max} = 45$ dBm. We can observe from this figure that R_e^* initially reaches a peak and then decreases gradually as R_a increases, which indicates that there exists an optimal value of R_a to maximize R_e^* for each of Jammer's three transmission schemes. Regarding the RPC and CPC schemes, to compensate the increase in R_a, we need to more power from Q_a for Alice's transmission. According to Figs. 3 and 4, the increase in Q_a first raises the ETR of the system while still ensuring observance of the covertness constraint, but a large Q_a may have an adverse effect on reducing the minimum DEP at Willie. According to constraints C_2 and C_3, the TCIPC scheme requires more power from Q_j and Q_a to meet Bob's decoding when R_a increases. A rise in Q_a can decrease Alice's transmission probability (i.e. P_{T_a}). Additionally, Willie's ability to detect transmission improves as Q_j rises. Thus, R_a has a dual effect on the performance of the system for each of Jammer's three transmission schemes. In addition to optimizing Q_j and Q_a, we also have to determine the optimal value of R_a to maximize the performance of the system. As also shown Fig. 7, the maximum ETR improves significantly when R_j exhibits a declining trend. Furthermore, the TCIPC scheme has a greater maximum ETR in comparison to the RPC and CPC schemes.

6. Conclusions

In this paper, we investigated the truncated channel inversion power control (TCIPC) scheme adopted by Alice and Jammer to facilitate covert communications from Alice to Bob, and Jammer's interference removal relying on the successive interference cancellation (SIC) technique at Bob. The problem of maximizing the effective transmission rate under the constraints of covertness and Bob's decoding was formulated. From the optimization problem, we achieved the optimal solutions for the power control parameters of Alice and Jammer, as well as the constraint regarding system parameters for the existence of these solutions. A comparison of the TCIPC scheme with Jammer's previous transmission schemes, such as random power control (RPC) scheme and constant power control (CPC) scheme, was also carried out.

Since the TCIPC scheme fixes the received power at Bob and uses the SIC technique for interference cancellation, its covertness-related performance is superior to those of the two other schemes. Our investigation showed that, for the TCIPC scheme, there exists an optimal value of Alice's predetermined transmission rate to maximize the maximum effective transmission rate. Furthermore, the maximum effective transmission rate increases monotonically as the maximum transmit power of Alice or Jammer increases and then converges to a constant value. Finally, with the TCIPC scheme for Alice and Jammer, we are able to conclude that the system is capable of achieving covert communications.

Acknowledgements

This research is funded by University of Science, VNU-HCM under grant number T2021-27.

Appendix A: Proof of Lemma 1

From Eqs. (7) and Eq. (8), the false alarm probability is written as:

$$\begin{aligned}
\alpha &= \Pr\left(P_w \geqslant \tau \middle| H_0, T_j \right) \\
&= \Pr\left(\frac{\mathrm{Q}_j \left|h_{j,w}\right|^2}{\left|h_{j,b}\right|^2} + \sigma_w^2 \geqslant \tau \middle| \left|h_{j,b}\right|^2 \geqslant \frac{\mathrm{Q}_j}{P_j^{max}} \right) \\
&= \frac{1}{P_{T_j}} \Pr\left[\mathrm{Q}_j \left|h_{j,w}\right|^2 \geqslant \left(\tau - \sigma_w^2\right) \left|h_{j,b}\right|^2, \left|h_{j,b}\right|^2 \geqslant \frac{\mathrm{Q}_j}{P_j^{max}} \right] \\
&= \begin{cases} 1 & , \tau \leqslant \sigma_w^2 \\ \frac{1}{P_{T_j}} \int_{\frac{\mathrm{Q}_j}{P_j^{max}}}^{\infty} \int_{\frac{\left(\tau-\sigma_w^2\right)y}{\mathrm{Q}_j}}^{\infty} f_{\left|h_{j,w}\right|^2}(x) f_{\left|h_{j,b}\right|^2}(y) \mathrm{d}x\mathrm{d}y, & \tau > \sigma_w^2 \end{cases} \\
&= \begin{cases} 1 & , \tau \leqslant \sigma_w^2 \\ \mathrm{e}^{\frac{\mathrm{Q}_j}{\lambda_{j,b} P_j^{max}}} \int_{\frac{\mathrm{Q}_j}{P_j^{max}}}^{\infty} \int_{\frac{\left(\tau-\sigma_w^2\right)y}{\mathrm{Q}_j}}^{\infty} \frac{\mathrm{e}^{-\left(\frac{x}{\lambda_{j,w}} + \frac{y}{\lambda_{j,b}}\right)}}{\lambda_{j,w}\lambda_{j,b}} \mathrm{d}x\mathrm{d}y, & \tau > \sigma_w^2 \end{cases} \\
&= \begin{cases} 1 & , \tau \leqslant \sigma_w^2 \\ \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau-\sigma_w^2)\lambda_{j,b}+\lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau-\sigma_w^2}{\lambda_{j,w} P_j^{max}}} & , \tau > \sigma_w^2. \end{cases}
\end{aligned} \tag{37}$$

Similarly, from Eqs. (7) and (8), the miss detection probability is analyzed as:

$$\begin{aligned}
\beta &= \Pr\left(P_w < \tau \middle| H_1, T_j \right) \\
&= \Pr\left(\frac{\mathrm{Q}_a \lambda_{a,w}}{\left|h_{a,b}\right|^2} + \frac{\mathrm{Q}_j \left|h_{j,w}\right|^2}{\left|h_{j,b}\right|^2} + \sigma_w^2 < \tau \middle| \left|h_{j,b}\right|^2 \geqslant \frac{\mathrm{Q}_j}{P_j^{max}} \right) \\
&= \frac{1}{P_{T_j}} \Pr\left[\mathrm{Q}_j \left|h_{j,w}\right|^2 < \left(\tau - \Omega\right) \left|h_{j,b}\right|^2, \left|h_{j,b}\right|^2 \geqslant \frac{\mathrm{Q}_j}{P_j^{max}} \right] \\
&= \begin{cases} 0 & , \tau \leqslant \Omega \\ \frac{1}{P_{T_j}} \int_{\frac{\mathrm{Q}_j}{P_j^{max}}}^{\infty} \int_0^{\frac{(\tau-\Omega)y}{\mathrm{Q}_j}} f_{\left|h_{j,w}\right|^2}(x) f_{\left|h_{j,b}\right|^2}(y) \mathrm{d}x\mathrm{d}y, & \tau > \Omega \end{cases} \\
&= \begin{cases} 0 & , \tau \leqslant \Omega \\ \mathrm{e}^{\frac{\mathrm{Q}_j}{\lambda_{j,b} P_j^{max}}} \int_{\frac{\mathrm{Q}_j}{P_j^{max}}}^{\infty} \int_0^{\frac{(\tau-\Omega)y}{\mathrm{Q}_j}} \frac{\mathrm{e}^{-\left(\frac{x}{\lambda_{j,w}} + \frac{y}{\lambda_{j,b}}\right)}}{\lambda_{j,w}\lambda_{j,b}} \mathrm{d}x\mathrm{d}y, & \tau > \Omega \end{cases} \\
&= \begin{cases} 0 & , \tau \leqslant \Omega \\ 1 - \frac{\lambda_{j,w}\mathrm{Q}_j}{(\tau-\Omega)\lambda_{j,b}+\lambda_{j,w}\mathrm{Q}_j} \mathrm{e}^{-\frac{\tau-\Omega}{\lambda_{j,w} P_j^{max}}} & , \tau > \Omega. \end{cases}
\end{aligned} \tag{38}$$

The proof is completed.

Appendix B: Proof of Theorem 1

Following Eq. (11), it is shown that $\xi = 1$ is the worst case for $\tau \leqslant \sigma_w^2$. When $\sigma_w^2 \leqslant \tau \leqslant \Omega$, we observe that ξ is a continuous decreasing function of τ, so Willie chooses $\tau = \Omega$ as the optimal threshold in this case. For $\Omega \leqslant \tau$, carrying out the first derivative of ξ, we have:

$$\begin{aligned}
&\frac{\partial \xi}{\partial \tau} \\
&= \frac{\lambda_{j,w}\lambda_{j,b}\mathrm{Q}_j P_j^{max} + \mathrm{Q}_j \left[\left(\tau-\Omega\right)\lambda_{j,b}+\lambda_{j,w}\mathrm{Q}_j\right]}{P_j^{max}\left[\left(\tau-\Omega\right)\lambda_{j,b}+\lambda_{j,w}\mathrm{Q}_j\right]^2} \mathrm{e}^{-\frac{\tau-\Omega}{\lambda_{j,w} P_j^{max}}} \\
&- \frac{\lambda_{j,w}\lambda_{j,b}\mathrm{Q}_j P_j^{max} + \mathrm{Q}_j \left[\left(\tau-\sigma_w^2\right)\lambda_{j,b}+\lambda_{j,w}\mathrm{Q}_j\right]}{P_j^{max}\left[\left(\tau-\sigma_w^2\right)\lambda_{j,b}+\lambda_{j,w}\mathrm{Q}_j\right]^2} \mathrm{e}^{-\frac{\tau-\sigma_w^2}{\lambda_{j,w} P_j^{max}}}.
\end{aligned} \tag{39}$$

Since $\Omega > \sigma_w^2$, we deduce that $\frac{\partial \xi}{\partial \tau} > 0$. Hence, ξ is a continuous increasing function of τ. Thus, Willie sets $\tau = \Omega$ as the optimal threshold for $\Omega \leqslant \tau$ case. Therefore, Willie's detection power threshold is $\tau^* = \Omega = \frac{\mathrm{Q}_a}{\left|h_{a,b}\right|^2}\lambda_{a,b} + \sigma_w^2$. Substituting τ^* into Eq. (11), we achieve the minimum DEP. The proof is completed.

Appendix C: Proof of Lemma 2

From Eq. (13), let ξ^* be a function of $\left|h_{a,b}\right|^2$, $\xi^*\left(\left|h_{a,b}\right|^2\right)$, then the expected minimum DEP at Willie is given by:

$$\begin{aligned}\overline{\xi}^{*} &= \int_{\frac{\mathrm{Q}_a}{P_a^{max}}}^{\infty} \xi^{*}(x) f_{|h_{a,b}|^2}\left(x \,\middle|\, |h_{a,b}|^2 \geqslant \frac{\mathrm{Q}_a}{P_a^{max}}\right) \mathrm{d}x \\ &= \frac{1}{P_{T_a}} \int_{\frac{\mathrm{Q}_a}{P_a^{max}}}^{\infty} \xi^{*}(x) f_{|h_{a,b}|^2}(x)\, \mathrm{d}x \\ &= \mathrm{e}^{\frac{\mathrm{Q}_a}{\lambda_{a,b} P_a^{max}}} \int_{\frac{\mathrm{Q}_a}{P_a^{max}}}^{\infty} \xi^{*}(x) \frac{1}{\lambda_{a,b}} \mathrm{e}^{-\frac{1}{\lambda_{a,b}} x} \mathrm{d}x \,. \end{aligned} \tag{40}$$

Putting $G(y) = \mathrm{e}^{\frac{1}{\lambda_{a,b}} y} \int_y^{\infty} \xi^{*}(x) \frac{1}{\lambda_{a,b}} \mathrm{e}^{-\frac{1}{\lambda_{a,b}} x} \mathrm{d}x$, the first derivation of $G(y)$ is expressed as:

$$G'(y) = \mathrm{e}^{\frac{1}{\lambda_{a,b}} y} \int_y^{\infty} \frac{\mathrm{d}\xi^{*}(x)}{\mathrm{d}x} \frac{1}{\lambda_{a,b}} \mathrm{e}^{-\frac{1}{\lambda_{a,b}} x} \mathrm{d}x \,. \tag{41}$$

We have the first derivative of $\xi^{*}(x)$ as:

$$\begin{aligned}\frac{\mathrm{d}\xi^{*}(x)}{\mathrm{d}x} = &\left[\frac{\mathrm{Q}_j \left(\lambda_{a,w}\lambda_{j,w}\mathrm{Q}_j\mathrm{Q}_a + \lambda_{a,w}\lambda_{j,w}\lambda_{j,b}P_j^{max}\mathrm{Q}_a\right)}{P_j^{max}\left(\lambda_{j,w}\mathrm{Q}_j x + \lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a\right)^2}\right. \\ &\left. + \frac{\lambda_{j,b}\lambda_{a,w}^2\mathrm{Q}_j\mathrm{Q}_a^2}{P_j^{max}\left(\lambda_{j,w}\mathrm{Q}_j x + \lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a\right)^2 x}\right] \mathrm{e}^{-\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max} x}} . \end{aligned} \tag{42}$$

Since $\frac{\mathrm{d}\xi^{*}(x)}{\mathrm{d}x} > 0$, we can deduce that $G(y)$ is an increasing function of y and $G\left(\frac{\mathrm{Q}_a}{P_a^{max}}\right) > G(0)$. This means that $\overline{\xi}^{*} > \overline{\xi}_l^{*}$, and $\overline{\xi}_l^{*} = G(0)$ is given in Lemma 2. Thus, the proof is completed.

Appendix D: Proof of Theorem 2

Using the Leibniz integral rule to $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right) = \overline{\xi}_l^{*} - (1-\varepsilon)$, we have the partial derivatives as:

$$\begin{aligned} F'_{\mathrm{Q}_j} = &\int_0^{\infty} \frac{\lambda_{a,w}\lambda_{j,w}\lambda_{j,b}\mathrm{Q}_a x}{\lambda_{a,b}\left(\lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a + \lambda_{j,w}\mathrm{Q}_j x\right)^2} \\ &\times \mathrm{e}^{-\left(\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max} x} + \frac{1}{\lambda_{a,b}} x\right)} \mathrm{d}x \,, \end{aligned} \tag{43}$$

$$\begin{aligned} F'_{\mathrm{Q}_a} = &-\int_0^{\infty} \frac{\lambda_{a,w}\mathrm{Q}_j\left[\left(\lambda_{j,b}P_j^{max} + \mathrm{Q}_j\right)\lambda_{j,w}x + \lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a\right]}{\lambda_{a,b}P_j^{max}\left(\lambda_{a,w}\lambda_{j,b}\mathrm{Q}_a + \lambda_{j,w}\mathrm{Q}_j x\right)^2} \\ &\times \mathrm{e}^{-\left(\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max} x} + \frac{1}{\lambda_{a,b}} x\right)} \mathrm{d}x \,. \end{aligned} \tag{44}$$

It is shown that when Q_j approaches 0 and Q_a is arbitrary, $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$ tends to $-(1-\varepsilon)$. Conversely, when Q_a approaches 0 and Q_j is arbitrary, $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$ tends to ε, so there exist the solutions to $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right) = 0$. Moreover, it is noted that $F'_{\mathrm{Q}_j} > 0$ and $F'_{\mathrm{Q}_a} < 0$, then from $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right) = 0$ we can express Q_a as a function of Q_j which is called the implicit function $\mathrm{Q}_a = g\left(\mathrm{Q}_j\right)$ and $g\left(\mathrm{Q}_j\right)$ is unique. Using the principle of implicit differentiation to $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right) = 0$, we obtain the first derivative of $g\left(\mathrm{Q}_j\right)$ as:

$$\frac{\mathrm{d}g\left(\mathrm{Q}_j\right)}{\mathrm{d}\mathrm{Q}_j} = -\frac{F'_{\mathrm{Q}_j}}{F'_{\mathrm{Q}_a}} > 0. \tag{45}$$

Thus, $\mathrm{Q}_a = g\left(\mathrm{Q}_j\right)$ is the increasing function of Q_j. Moreover, at one point $\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$ with $\mathrm{Q}_a \to 0$, constraint C_1 is satisfied. Hence, the set of all points $\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$ for constraint C_1 is expressed as:

$$D_1 = \begin{cases} 0 < \mathrm{Q}_j \\ 0 < \mathrm{Q}_a \leqslant g\left(\mathrm{Q}_j\right) . \end{cases} \tag{46}$$

D_1 is outlined in Fig. 8a (shown shaded).

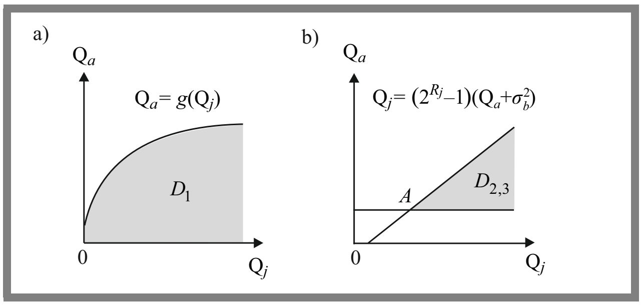
a)
Q_a
$\mathrm{Q}_a = g(\mathrm{Q}_j)$
D_1
0
Q_j
b)
Q_a
$\mathrm{Q}_j = (2^{R_j} - 1)(\mathrm{Q}_a + \sigma_b^2)$
A
$D_{2,3}$
0
Q_j

Fig. 8. Outline of the value domains $\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$: a) for D_1, b) for $D_{2,3}$, where $A = \left[\left(2^{R_j} - 1\right) 2^{R_a} \sigma_b^2, \left(2^{R_a} - 1\right) \sigma_b^2\right]$.

We observe that when Q_j tends to infinity, $F\left(\mathrm{Q}_j, \mathrm{Q}_a\right) = 0$ is written as:

$$\frac{1}{\lambda_{a,b}} \int_0^{\infty} \mathrm{e}^{-\left(\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}P_j^{max} x} + \frac{1}{\lambda_{a,b}} x\right)} \mathrm{d}x - (1-\varepsilon) = 0. \tag{47}$$

By applying $\int_0^{\infty} \mathrm{e}^{-\left(\frac{\beta}{4x} + \gamma x\right)} \mathrm{d}x = \sqrt{\frac{\beta}{\gamma}} K_1\left(\sqrt{\beta\gamma}\right)$ [27] to Eq. (47), we get:

$$2\sqrt{\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}\lambda_{a,b}P_j^{max}}} K_1\left(2\sqrt{\frac{\lambda_{a,w}\mathrm{Q}_a}{\lambda_{j,w}\lambda_{a,b}P_j^{max}}}\right) - (1-\varepsilon) = 0 \,, \tag{48}$$

where $K_1(.)$ is the modified Bessel function of the second kind. The left-hand side in Eq. (48) is a decreasing function of Q_a, so when Q_j tends to infinity, Q_a approaches a constant Q_a^{asy} where Q_a^{asy} is a solution of Eq. (48).

According to constraints C_2 and C_3, the set of all points $\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$ satisfying these two constraints is:

$$D_{2,3} = \begin{cases} \left(2^{R_j} - 1\right)\left(\mathrm{Q}_a + \sigma_b^2\right) \leqslant \mathrm{Q}_j \\ \left(2^{R_a} - 1\right)\sigma_b^2 \leqslant \mathrm{Q}_a \,, \end{cases} \tag{49}$$

and $D_{2,3}$ is outlined as the shaded section in Fig. 8b. Based on sets D_1 and $D_{2,3}$, in order to obtain solutions for the optimization problem in Eq. (21), we need:

$$\mathrm{Q}_a^{asy} \geqslant \left(2^{R_a} - 1\right)\sigma_b^2 \,, \tag{50}$$

due to the decreasing property of the left-hand side in Eq. (48), from Eq. (49), we get the constraint C of the system parameters as Eq. (22) in Theorem 2.

It is noted that when $\left(\mathrm{Q}_j, \mathrm{Q}_a\right)$ approaches $(0, 0)$, R_e increases to R_a. We consider that the point A is given in Fig. 8b, $\mathrm{Q}_j^{\dagger}$ is the solution of $F\left[\mathrm{Q}_j, \left(2^{R_a}-1\right)\sigma_b^2\right] = 0$, and constraint C is guaranteed, then the optimal values of Q_j and Q_a are argued as follows:

– If $A \in D_1$, then $\mathrm{Q}_j^{\dagger} \leqslant \left(2^{R_j}-1\right)2^{R_a}\sigma_b^2$ and A is the optimal point, it means that:

$$\begin{aligned} \mathrm{Q}_j^* &= \left(2^{R_j}-1\right)2^{R_a}\sigma_b^2 \,, \\ \mathrm{Q}_a^* &= \left(2^{R_a}-1\right)\sigma_b^2 \,. \end{aligned} \tag{51}$$

– If $A \notin D_1$, then $\mathrm{Q}_j^{\dagger} \geqslant \left(2^{R_j}-1\right)2^{R_a}\sigma_b^2$ the solutions of the optimization problem are:

$$\begin{aligned} \mathrm{Q}_j^* &= \mathrm{Q}_j^{\dagger} \,, \\ \mathrm{Q}_a^* &= \left(2^{R_a}-1\right)\sigma_b^2 \,. \end{aligned} \tag{52}$$

In summary, the optimal choice of Q_j and Q_a is achieved in Eq. (23). The proof is completed.

References

[1] S. Rich and B. Gellman, "NSA seeks to build quantum computer that could crack most types of encryption", *The Washington Post*, no. 2, 2014 [Online]. Available: http://wapo.st/19DycJT

[2] S. Yan, X. Zhou, J. Hu, and S.V. Hanly, "Low probability of detection communication: Opportunities and challenges", *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, 2019 (https://doi.org/10.1109/MWC.001.1900057).

[3] B.A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels", *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013 (https://doi.org/10.1109/JSAC.2013.130923).

[4] P.H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise", in *2013 IEEE International Symposium on Information Theory*, 2013, pp. 2945–2949 (https://doi.org/10.1109/ISIT.2013.6620765).

[5] M.R. Bloch, "Covert communication over noisy channels: A resolvability perspective", *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, 2016 (https://doi.org/10.1109/TIT.2016.2530089).

[6] A. Abdelaziz and C.E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel", in *2017 IEEE Conference on Communications and Network Security* (*CNS*), 2017, pp. 1–9 (https://doi.org/10.1109/CNS.2017.8228657).

[7] T.X. Zheng *et al.*, "Wireless covert communications aided by distributed cooperative jamming over slow fading channels", *IEEE Transactions on Wireless Communications*, vol. 20, no. 11, pp. 7026–7039, 2021 (https://doi.org/10.1109/TWC.2021.3080382).

[8] Y. Jiang, L. Wang, and H.H. Chen, "Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission", *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2980–2992, 2020 (https://doi.org/10.1109/TVT.2020.2966538).

[9] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert wireless communications with channel inversion power control in Rayleigh fading", *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12135–12149, 2019 (https://doi.org/10.1109/TVT.2019.2949304).

[10] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a Poisson field of interferers", *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6005–6017, 2018 (https://doi.org/10.1109/TWC.2018.2854540).

[11] A. Sheikholeslami *et al.*, "Multi-hop routing in covert wireless networks", *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3656–3669, 2018 (htpps://doi.org/10.1109/TWC.2018.2812881).

[12] M. Forouzesh, P. Azmi, A. Kuhestani, and P.L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens", *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020 (https://doi.org/10.1109/TCOMM.2020.2978206).

[13] R. Zhang *et al.*, "UAV relay assisted cooperative jamming for covert communications over Rician fading", *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7936–7941, 2022 (htpps://doi.org/10.1109/TVT.2022.3164051).

[14] H.M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks", *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 389–401, 2020 (htpps://doi.org/10.1109/TCOMM.2019.2950940).

[15] T.V. Sobers, B.A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer", *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017 (htpps://doi.org/10.1109/TWC.2017.2720736).

[16] K. Li, T.V. Sobers, D. Towsley, and D. Goeckel, "Covert communication in continuous-time systems in the presence of a jammer", *IEEE Transactions on Wireless Communications*, vol. 21, no. 7, pp. 4883–4897, 2022 (htpps://doi.org/10.1109/TWC.2021.3134179).

[17] K. Li, P.A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer", *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3463–3473, 2020 (htpps://doi.org/10.1109/TWC.2020.2973975).

[18] K. Shahzad, "Relaying via cooperative jamming in covert wireless communications", in *2018 12th International Conference on Signal Processing and Communication Systems* (*ICSPCS*), 2018, pp. 1–6 (htpps://doi.org/10.1109/ICSPCS.2018.8631772).

[19] H. ZivariFard, M.R. Bloch, and A. Nosratinia, "Covert communication in the presence of an uninformed, informed, and coordinated jammer", in *2022 IEEE International Symposium on Information Theory* (*ISIT*), 2022, pp. 306–311 (htpps://doi.org/10.1109/ISIT50566.2022.9834682).

[20] W. Xiong, Y. Yao, X. Fu, and S. Li, "Covert communication with cognitive jammer", *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1753–1757, 2020 (htpps://doi.org/10.1109/LWC.2020.3003472).

[21] X. He, H. Dai, W. Shen, P. Ning, and R. Dutta, "Toward proper guard zones for link signature", *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2104–2117, 2016 (htpps://doi.org/10.1109/TWC.2015.2498621).

[22] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions", in *2016 IEEE Globecom Workshops* (*GC Wkshps*), 2016, pp. 1–6 (htpps://doi.org/10.1109/GLOCOMW.2016.7849064).

[23] Z. Xiang *et al.*, "'Secure transmission in HARQ-assisted non-orthogonal multiple access networks", *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2171–2182, 2020 (htpps://doi.org/10.1109/TIFS.2019.2955792).

[24] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Robust power allocation in covert communication: Imperfect CDI", *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5789–5802, 2021 (htpps://doi.org/10.1109/TVT.2021.3076709).

[25] L. Tao *et al.*, "Covert communication in downlink NOMA systems with random transmit power", *IEEE Wireless Communications Letters*, vol. 9, no. 11, pp. 2000–2004, 2020 (htpps://doi.org/10.1109/LWC.2020.3011191).

[26] K. Higuchi and A. Benjebbour, "Non-orthogonal multiple access (NOMA) with successive interference cancellation for future radio access", *IEICE Transactions on Communications*, vol. E98.B, no. 3, pp. 403–414, 2015 (htpps://doi.org/doi.org/10.1587/transcom.E98.B.403).

[27] D. Zwillinger and A. Jeffrey, *Table of Integrals, Series, and Products*, 7th ed. Elsevier, 1200 p., 2007 (ISBN 9780123736376).

Ngo Thanh Hai, M.Sc.
Faculty of Electronics and Telecommunications
https://orcid.org/0000-0002-6865-4305
E-mail: ngohai@hcmus.edu.vn
Department of Telecommunications and Networks, University of Science, VNU-HCM, Ho Chi Minh, Viet Nam

Dang Le Khoa, Ph.D.
Head of the Telecommunications and Networks Department
https://orcid.org/0000-0003-0024-3419
E-mail: dlkhoa@hcmus.edu.vn
Department of Telecommunications and Networks, University of Science, VNU-HCM, Ho Chi Minh, Viet Nam