SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2024, Vol. 67, Iss. 8, 182301:1–182301:17
https://doi.org/10.1007/s11432-023-4025-2

Legitimate monitor by proactive guarding for counter covert communications

Manlin WANG[1], Bin XIA[1*] & Jiangzhou WANG[2]

[1]*School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[2]*School of Engineering, University of Kent, Canterbury* CT2 7NT*, UK*

Received 8 December 2023/Revised 21 March 2024/Accepted 7 May 2024/Published online 23 July 2024

Abstract Covert communication has been widely investigated to avoid the transmission behavior being overheard by the warder. However, covert communication may be illegitimately utilized by unauthorized parties to evade the supervision of authorized agencies, which leads to great challenges to information security. To meet the need for authorized parties to monitor and prevent illegitimate transmission between unauthorized nodes, a novel paradigm, called legitimate monitor, is proposed for counter covert communications. In the preceding covert communication system, the covert transmission rate is the focus. Differently, the core concern of the legitimate monitor system is the outage probability of the transmission between unauthorized nodes, which should be maximized to interrupt the potential but undetectable transmission. To achieve these goals effectively, a proactive guarding approach is proposed, where the authorized warder detects the transmission behavior and emits jamming signals to interfere with the potential transmission, simultaneously. In particular, the jamming power at the warder is optimized under cases where the instantaneous/statistical channel state information is available. Besides, the corresponding outage probability is derived to evaluate the system performance, which can also be simplified to scenarios with a passive warder. Numerical results demonstrate that proactive guarding outperforms the passive one, especially when the warder is not proximal to the unauthorized transmitter. In addition, the proposed jamming power allocation scheme also outperforms other benchmark schemes.

Keywords legitimate monitor, counter covert communication, full-duplex technology, outage probability, power allocation optimization

1 Introduction

1.1 Background and motivation

In various communication scenarios, confidential and private information is transmitted over open wireless channels, which makes transmission security a critical and challenging issue. To guarantee transmission, cryptography-based approach and physical layer security (PLS) technology have been developing for decades [1–3]. By utilizing encryption and PLS technology, the transmission content is protected to prevent it from being deciphered by unauthorized users. In some application scenarios with higher-level security requirements, mere transmission behavior exposure leads to devastating consequences. Thus, covert communication has been proposed and received widespread attention from academia and industry, preventing transmission from being detected by unauthorized users [4, 5].

In recent years, covert communication has been thoroughly investigated from the perspective of information theory and practical application scenarios. For example, the fundamental limitation of covert communication was first revealed by [6] in additive white Gaussian noise (AWGN) channels, which states that $\mathcal{O}(\sqrt{n})$ bits can be transmitted covertly and reliably in n channel uses. After the milestone result provided in [6], plenty of studies have been further conducted to extend the above result into multiple access channels [7], broadcast channels [8], and backscatter channels [9]. After the pioneering fundamental studies in [6–9], several techniques have been embedded into covert communication systems to improve the transmission rate, such as the cooperative jamming [10], the multiple antenna technology [11], and

* Corresponding author (email: bxia@sjtu.edu.cn)

© Science China Press 2024

the intelligent reflecting surface (IRS) [12]. In all these studies [6–12], the transceivers default to the authorized users, and from this perspective, the communication rate is maximized while ensuring its covertness from unauthorized warders.

However, wireless communication links can also be illegitimately used by unauthorized parties for harmful purposes, which poses a great threat to national security. In fact, point-to-point wireless communication can be achieved without passing through any authorized base stations, making information surveillance difficult. Further, covert communication can be realized between these nodes to evade legitimate monitoring, such as in mobile ad hoc network scenarios [13] and device-to-device network scenarios [14]. Besides, unauthorized unmanned aerial vehicles serve as relay nodes that can flexibly extend the covert communication distance between the above nodes [15]. Therefore, covert communication is a double-edged sword. It can not only protect the transmission security of legitimate users, but also hide illegal transmissions with harmful purposes.

Motivated by these facts, there is a growing need for authorized parties to monitor and prevent illegitimate transmission between unauthorized nodes. To cope with the hidden danger of potential covert communication, a novel paradigm (called legitimate monitor) is proposed, which shifts from the conventional covert communication against the unauthorized warder to the new information surveillance by the authorized warder. In particular, it is necessary to stand on the opposite side of the covert communication research, arguing that the warder is authorized and the transceiver conducting the covert communication is unauthorized.

1.2 Related work

In the scope of legitimate monitor, the warder detects the potential transmission and makes its judgments as accurate as possible, which is the same as the setting in conventional covert communication literature. However, it is worth noting that the ultimate purpose of the considered legitimate monitor system is different from the covert communication system [6–15], and the legitimate eavesdropping system [16–24]. The essential differences among them are succinctly stated as follows.

For conventional covert communication [6], the ultimate goal is to improve the transmission rate (or the throughput) while satisfying the transmission covertness constraint, that is, to guarantee the detection error probability at the warder is higher than a predetermined threshold (such as $1-10^{-2}$). On the contrary, for legitimate monitor, the ultimate goal is to intercept the undetectable transmission between unauthorized nodes. When the detection error probability at the warder already exceeds the predetermined threshold, we call the illegitimate transmission undetectable. The outage probability of the undetectable transmission is expected to be maximized in the legitimate monitor system.

For wireless information surveillance, a related field called legitimate eavesdropping has attracted considerable research interest in recent years. In a legitimate eavesdropping system, the authorized eavesdropper focuses on efficiently decoding the confidential information transmitted by the unauthorized transmitter [16, 17]. In [18], a spoofing relay technique is adopted to construct or destruct the source signals for decoding more efficiently. Moreover, an IRS is also embedded to enhance the eavesdropping performance in [19, 20]. Besides, a worse case is considered by [21] where the suspicious users apply jamming to defend against eavesdropping. Further, the above system model is extended to two suspicious links networks [22], multi-relay systems [23], and wireless energy harvesting scenarios [24].

Notably, the aforementioned system is different from the considered legitimate monitor system for counter covert communications intrinsically in this paper. In the former systems [16–24], the authorized eavesdropper focuses on efficiently decoding the confidential information transmitted by the unauthorized transmitter where the exposure of transmission behavior is permitted and uninterested. However, in legitimate monitor systems here, the covert communication between unauthorized nodes fails when the warder can accurately detect the transmission behavior. Furthermore, when the transmission between unauthorized nodes already satisfies the covertness requirement, the outage probability of the undetectable transmission is the core concern of this system, where the warder tries to interrupt the potential transmission exceeding the detection error probability threshold.

Overall, a comprehensive comparison between this work (legitimate monitor) and the existing studies about covert communication and legitimate eavesdropping is summarized in Table 1 [6–25].

Table 1 Main differences between this work and other studies

	Covert communication	Legitimate eavesdropping	This work (legitimate monitor)
Scenarios and purpose	Legitimate: transceivers Illegitimate: warder Hide transmission behavior	Legitimate: eavesdropper Illegitimate: transceivers Eavesdrop (decoding) signals	Legitimate: warder Illegitimate: transceivers Detect and interrupt potential transmission
System model	Receiver: decode Warder: detect	Receiver: decode Eavesdropper: decode	Receiver: decode Warder: detect
Crucial metric	Throughput	Eavesdropping rate	Outage probability
Adopted strategies	Uncertainty utilization: AWGN [6–9, 13, 25], multi-antenna [11], IRS [12], jamming [10, 15], channel interference [14]	Channel differentiation: jamming [16, 17, 21–24], spoofing relay [18], IRS [19, 20]	Uncertainty avoidance and jamming: proactive guarding, other methods (further work)

1.3 Main contribution

In practice, such a legitimate monitor is particularly challenging since the warder cannot be located in close proximity to the unauthorized transmitter, which greatly reduces the accuracy of detection. For example, a safety zone can be achieved by the unauthorized transmitter to avoid the warder in a limited range around it [26, 27]. In these scenarios, even if the detection error probability exceeds the predetermined threshold, the potential transmission can still happen, which brings great security threats to the legitimate monitor system. To address this issue, in this paper, we propose a proactive guarding approach in which the warder operates in a full-duplex mode. On the one hand, the warder detects illegitimate transmission based on the received signals. On the other hand, it sends jamming signals to interfere with the potential transmission. The main contributions of this paper are summarized as follows.

• To cope with the growing need for authorized parties to monitor and prevent illegitimate transmission, a novel legitimate monitor paradigm is considered for counter covert communications. Different from the conventional covert communication system and the legitimate eavesdropping system, the ultimate goal in the considered legitimate monitor system is to intercept the undetectable transmission between unauthorized nodes. Therefore, a proactive guarding approach is proposed to improve the system performance, where the authorized warder detects the transmission behavior and interferes with the potential transmission, simultaneously.

• To maximize the outage probability of the illegitimate transmission, the global optimal jamming power allocation scheme at the warder in each transmission round is proposed based on the instantaneous channel state information (I-CSI). Specially, the detection error probability at the warder in one transmission round and its approximation are provided. Besides, when the illegitimate transmission satisfies the covertness requirement (i.e., detection error probability exceeds the predetermined threshold), the outage probability of the undetectable transmission is derived in terms of the jamming power. In addition, to maximize the outage probability, the optimization problem is formulated and solved where the jamming power in each round is optimized globally. Finally, to evaluate the performance of the legitimate monitor system under I-CSI, the expression of outage probability under optimized jamming power is derived, which can be extended to the passive guarding scenario.

• Considering the authorized warder and the unauthorized transceivers are non-cooperative in general, the I-CSI is challenging to obtain. In the case of only statistical channel state information (S-CSI), the optimal jamming power allocation scheme at the warder is also proposed to maximize the outage probability of the illegitimate transmission. In particular, the optimal jamming power is closely related to the ability of self-interference cancellation (SIC) at the warder, where the jamming signal is not always beneficial to the legitimate monitor system. Besides, the corresponding outage probability is also derived to evaluate the system performance, and the above results under S-CSI can also be extended to the passive guarding scenarios.

• Numerical simulations verify the accuracy of the analytical results and the efficiency of the proposed jamming power allocation schemes. Besides, the impacts of the main system parameters (the residual factor of SIC, the jamming power constraint, and the location of the warder) on the system performance are illustrated. It shows that the proactive guarding approach outperforms the passive guarding approach, especially when the warder is proximate to the unauthorized receiver but far from the unauthorized transmitter.

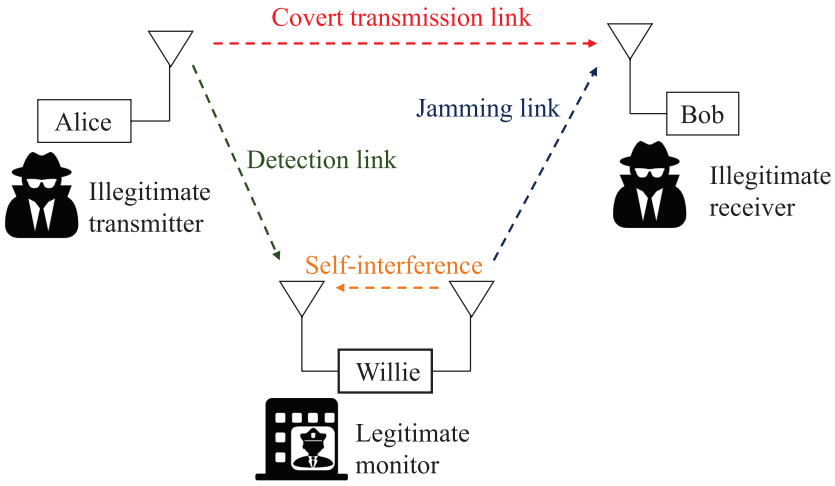

Figure 1 (Color online) System model of legitimate monitor paradigm with proactive guarding approach.

1.4 Organization and notations

The remainder of this paper is organized as follows. In Section 2, the considered legitimate monitor system is presented. The optimal jamming power allocation schemes are provided under I-CSI and S-CSI in Sections 3 and 4, respectively. In Section 5, the system performance is evaluated based on the numerical results. Finally, the paper is concluded in Section 6.

Notation. $\mathbb{E}[\cdot]$ and $|\cdot|$ denote the expectation operator and the absolute value operator, respectively. $\mathcal{CN}(0,\sigma^2)$ denotes the complex Gaussian distribution with zero mean and variance σ^2. $\mathcal{U}[a,b]$ denotes the uniform distribution on the interval $[a,b]$. $\Pr(\cdot)$ denotes the probability of an event. $\Gamma(n)=(n-1)!$ denotes the Gamma function, and $\gamma(n,x)=\int_0^x \mathrm{e}^{-t}t^{n-1}\mathrm{d}t$ denotes the lower incomplete Gamma function. $\mathrm{Ei}(x)=\int_x^\infty \frac{\mathrm{e}^{-t}}{t}\mathrm{d}t$ denotes the exponential integral function.

2 System model

2.1 Signal and channel models

As shown in Figure 1, we consider a legitimate monitor system where the unauthorized transmitter (Alice) tries to communicate with the unauthorized receiver (Bob) covertly. The authorized warder (Willie) detects the transmission behavior and interferes with the transmission between the unauthorized nodes (Alice and Bob). The unauthorized transmitter and receiver are equipped with a single antenna, and the authorized warder is equipped with two antennas in a full-duplex mode, one for detecting (receiving) and the other for jamming (transmitting)[1)].

The wireless channels from Alice to Bob ($h_{ab}(v)$), Alice to Willie ($h_{aw}(v)$), and Willie to Bob ($h_{wb}(v)$) are subject to the quasi-static Rayleigh fading, where v denotes the joint fading state in one transmission round (including n channel uses) [25]. The channel coefficients remain constant during one transmission round, and are independently and identically distributed (i.i.d.) among different rounds. Specifically, $h_{ab}(v)\sim\mathcal{CN}(0,\lambda_{ab})$, $h_{aw}(v)\sim\mathcal{CN}(0,\lambda_{aw})$, and $h_{wb}(v)\sim\mathcal{CN}(0,\lambda_{wb})$, where λ_{ij} for $ij\in\{ab,aw,wb\}$ denotes the large scale path loss. In Section 3, the case is considered where I-CSIs of all links (i.e., $h_{ab}(v)$, $h_{aw}(v)$, and $h_{wb}(v)$) are assumed to be obtained at Alice and Willie. The global I-CSI assumption has been commonly made in the information-theoretic literature as a special but fundamental scenario to investigate the system performance bound, such as studies with covert communications [28, 29] and legitimate eavesdropping [17]. Besides, in Section 4, the case is considered where only S-CSIs (i.e., λ_{ab},

1) To reveal the essence of the paradigm for counter covert communications, the basic single antenna scenario is considered here. Although the multi-antenna technology can be applied to Alice (or Willie), which potentially degrades (or enhances) the system performance, the beamforming vector at each node is required to be designed finely, which is beyond the scope of this paper and left for further work.

λ_{aw}, and λ_{wb}) are available at Alice and Willie [30][2)].

In one transmission round, Alice transmits n covert signals $x_a[i], i \in \{1,\ldots,n\}$ to Bob, while Willie sends n jamming signals $x_w[i], i \in \{1,\ldots,n\}$ to Bob. Besides, Willie collects n received signals to detect whether or not Alice has transmitted. The average transmit power at Alice in one round under fading state v is defined as $P_a(v)$, i.e., $\mathbb{E}[|x_a[i]|^2] = P_a(v)$. Furthermore, Gaussian signaling is adopted at Alice, i.e., $x_a[i] \sim \mathcal{CN}(0, P_a(v))$, which is optimal for the covert transmission [31]. Similarly, the average jamming power at Willie in one round under fading state v is defined as $P_w(v)$ and $x_w[i] \sim \mathcal{CN}(0, P_w(v))$. Here, the Gaussian signaling is adopted for the jamming signal to interfere with the potential transmission [32][3)]. The AWGN at Bob and Willie are defined as $n_b[i] \sim \mathcal{CN}(0, \sigma_b^2)$ and $n_w[i] \sim \mathcal{CN}(0, \sigma_w^2)$, where σ_b^2 and σ_w^2 are the noise variances at Bob and Willie, respectively.

2.2 Binary hypothesis testing

In order to detect the presence of covert communications, Willie must distinguish between two hypotheses in each transmission round as follows:

$$y_w[i] = \begin{cases} I[i] + n_w[i],\ i \in \{1,\ldots,n\}, & \mathcal{H}_0 \\ h_{aw}(v)x_a[i] + I[i] + n_w[i],\ i \in \{1,\ldots,n\}, & \mathcal{H}_1 \end{cases} \tag{1}$$

where $\mathcal{H}_0$ denotes the null hypothesis that Alice has not transmitted, $\mathcal{H}_1$ denotes the alternative hypothesis that Alice has transmitted. $y_w[i]$ is the received signal at Willie, and $I[i]$ is residual self-interference (RSI) after SIC. Specific methods for SIC can be referred to [33], including the antenna SIC technique, analog SIC technique, digital SIC technique, and their combinations. According to the modeling and characterization in the practical experiments, $I[i]$ can be modeled as complex Gaussian random variables with zero mean and variance $\varphi P_w(v)$ [34], where the RSI factor $\varphi \in [0,1]$ denotes the ratio of the RSI power to the jamming power after SIC, which embodies the capability of SIC. The smaller φ is, the stronger the capability of SIC is.

Following along the same lines as the proof of Lemma 3 in [35], it can be proven that the optimal detector for the warder is the radiometer. The proof is conducted by employing the Fisher-Neyman factorization theorem and likelihood ratio ordering concepts, omitted here for brevity. Thus, the radiometer, which possesses theoretical optimality on the one hand and low implementation complexity of practical applications on the other, is employed at the warder as follows:

$$T = \frac{1}{n}\sum_{i=1}^{n} |y_w[i]|^2 \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \tau(v), \tag{2}$$

where T is the average power of the received signal in each transmission round at Willie, $\tau(v)$ denotes the detection threshold under fading state v, $\mathcal{D}_0$ and $\mathcal{D}_1$ denote the binary decisions that infer whether Alice transmits or not, respectively.

Since one of the core tasks for the warder is to detect the illegitimate transmission behavior, the detection performance is crucial to be evaluated, which is qualified by the detection error probability [6]. In general, the prior probabilities of hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are assumed to be equal [12,25,36]. As such, the detection error probability $\xi(\tau(v))$ at Willie is defined as the sum of the false alarm probability and the missed detection probability, similar to [6,9–11]:

$$\xi(\tau) = \Pr(\mathcal{D}_1 \mid \mathcal{H}_0) + \Pr(\mathcal{D}_0 \mid \mathcal{H}_1) = \Pr(T > \tau(v) \mid \mathcal{H}_0) + \Pr(T < \tau(v) \mid \mathcal{H}_1), \tag{3}$$

where $\Pr(\mathcal{D}_1 \mid \mathcal{H}_0)$ denotes the false alarm probability, and $\Pr(\mathcal{D}_0 \mid \mathcal{H}_1)$ denotes the missed detection probability. Besides, the detection threshold $\tau(v)$ can be adjusted by Willie to minimize the detection error probability, where the optimal threshold is defined as $\tau^*(v)$ and the minimum detection error probability is defined as $\xi(\tau^*(v))$, correspondingly.

In the considered system, Alice tries to communicate with Bob covertly. In other words, Alice needs to ensure that the detection error probability at the warder exceeds the predetermined threshold, i.e.,

2) The large-scale path loss can be estimated relatively easily with some prior information, such as the relative locations and the fading exponent. In addition, some advanced detecting instruments (e.g., "Ghostbuster" [30]) can also be adopted to obtain S-CSI.

3) Here, the optimal signaling is worth revealing from the information-theoretic perspective. For example, the benefits of improper Gaussian signaling have been verified in interference-limited networks compared with the proper one [32].

$\xi(\tau^*(v)) \geqslant 1-\varepsilon$, where $\varepsilon \in [0,1]$ specifies the covertness tolerance [11,12,25]. Otherwise, covert transmission between unauthorized nodes fails. In fact, Alice can adjust the transmit power to meet the covertness requirement above. However, the covertness requirement limits the maximum transmit power at Alice, which also limits the signal-to-noise ratio (SNR) at Bob. Besides, the jamming signals emitted by Willie may further affect the SNR at Bob, which may also cause an outage of the undetectable transmission. Thus, even if the transmission from Alice to Bob is covert and cannot be accurately detected by Willie, there is a certain probability that this illegitimate and undetectable transmission will be interrupted.

In the following sections, the outage probability of the undetectable transmission is adopted as the core performance metric. And the impacts of the system parameters (including the jamming power and covertness tolerance) on the outage probability are elaborated.

3 Performance analysis and optimization under I-CSI

In this section, the system performance under I-CSI is investigated. Specially, the detection error probability at the warder with I-CSI is derived. In addition, the outage probability of the illegitimate transmission is derived in terms of the jamming power in each transmission round. Finally, the jamming power is optimized to maximize the outage probability, and the corresponding outage probability with optimized jamming power is derived to evaluate the system performance.

3.1 Detection performance at Willie

With a given detection threshold $\tau(v)$, the detection error probability in one transmission round under fading state v is expressed as

$$\begin{aligned}\xi\left(\tau(v)\right) &= \Pr\left(T > \tau(v)|H_0\right) + \Pr\left(T < \tau(v)|H_1\right) \\ &\overset{\text{(a)}}{=} 1 - \frac{1}{\Gamma\left(n\right)}\left(\gamma\left(n, \frac{n\tau(v)}{\varphi P_w(v)+\sigma_w^2}\right) - \gamma\left(n, \frac{n\tau(v)}{\varphi P_w(v)+\sigma_w^2+P_a(v)|h_{aw}(v)|^2}\right)\right),\end{aligned} \tag{4}$$

where the step (a) holds since T in (3) follows chi-squared distribution with $2n$ degrees of freedom.

Since Willie knows the I-CSI $h_{aw}(v)$ in each round, Willie can adjust the threshold $\tau(v)$ to minimize the detection error probability for each round, where the optimal threshold $\tau^*(v)$ is given by

$$\tau^*(v) = \frac{(\varphi P_w(v)+\sigma_w^2)(\varphi P_w(v)+\sigma_w^2+P_a(v)|h_{aw}(v)|^2)}{P_a(v)|h_{aw}(v)|^2}\ln\left(\frac{\varphi P_w(v)+\sigma_w^2+P_a(v)|h_{aw}(v)|^2}{\varphi P_w(v)+\sigma_w^2}\right). \tag{5}$$

By substituting (5) into (4), the minimum detection error probability $\xi(\tau^*(v))$ can be obtained. Due to the complicated form of (4), it is intractable to further reveal the system performance and guide the jamming power allocation. To address this issue, a tractable approximation of the minimum detection error probability in high covertness scenarios with a moderate number of channel use (i.e., $\xi\left(\tau^*\left(v\right)\right) \geqslant 0.9, n \geqslant 50$) is provided. In most covert transmission scenarios, the covertness tolerance ε is set less than 0.1, such as in [11, 14, 15, 26, 27]. Thus, the above interest detection error probability interval ($\xi\left(\tau^*\left(v\right)\right) \geqslant 0.9$) is suitable for most covert transmission scenarios. Besides, the above interest interval for the number of channel use ($n \geqslant 50$) is also suitable for most communication scenarios, including the short packet communication applications [25]. According to [25, Appendix C], by applying the midpoint rule for Riemann sums and the asymptotic property of the Gamma function, the approximation of the detection error probability in high covertness scenarios with moderate number of channel use can be derived as

$$\xi\left(\tau^*\left(v\right)\right) \approx 1 - \sqrt{\frac{n}{2\pi}}\frac{P_a(v)|h_{aw}(v)|^2}{\varphi P_w(v)+\sigma_w^2}, \tag{6}$$

where the detail derivation for (6) is omitted here for brevity. It can be seen from (6) that the detection error probability decreases with $P_a(v)$ and n, while increasing with $P_w(v)$ and φ. Moreover, the tightness of (6) is validated by Section 5 in this paper with extensive Monte Carlo simulation results. Thus, the above approximation of the detection error probability is adopted in the following analysis.

3.2 Problem formulation

When Alice transmits, the SNR at Bob under fading state v can be expressed as

$$\gamma(v)=\frac{P_a(v)|h_{ab}(v)|^2}{P_w(v)|h_{wb}(v)|^2+\sigma_b^2}. \tag{7}$$

To guarantee the transmission covertness (i.e., detection error probability at Willie exceeding $1-\varepsilon$), the transmit power at Alice is limited as follows based on the approximation (6):

$$P_a(v)\leqslant\sqrt{\frac{2\pi}{n}}\frac{\varepsilon(\varphi P_w(v)+\sigma_w^2)}{|h_{aw}(v)|^2}. \tag{8}$$

Thus, the SNR under the covertness requirement can be re-expressed as

$$\gamma^c(v)\approx\sqrt{\frac{2\pi}{n}}\frac{\varepsilon\left(\varphi P_w(v)+\sigma_w^2\right)|h_{ab}(v)|^2}{|h_{aw}(v)|^2(P_w(v)|h_{wb}|^2+\sigma_b^2)}, \tag{9}$$

which is affected by the jamming power $P_w(v)$, the covertness tolerance ε, and I-CSIs.

In addition, to cope with the hidden danger of potential covert communication, illegitimate transmission between unauthorized nodes must be prevented. Thus, the outage probability of the undetectable transmission is the core concern, which can be expressed as

$$P_{\text{out}}^I(\{P_w(v)\})=\Pr\left(\gamma^c(v)<2^R-1\right)=\mathbb{E}_v\left[X(v)\right], \tag{10}$$

where R is the transmission rate between Alice and Bob measured by bits per channel use (bpcu). And $X(v)$ is the indicator function to denote the event of transmission outage between Alice and Bob under fading state v, where $X(v)=1$ for the case $\gamma^c(v)<2^R-1$ and $X(v)=0$ otherwise.

From the perspective of legitimate monitor for counter covert communications, Willie can adjust the jamming power $P_w(v)$ in each round to maximize the outage probability of the undetectable transmission. Thus, the corresponding optimization problem can be formulated as

$$\begin{aligned}(\text{P1}):\max_{\{P_w(v)\}}\quad & P_{\text{out}}^I(\{P_w(v)\}) && (11)\\ \text{s.t. }\ & \mathbb{E}_v\left[P_w(v)\right]\leqslant P_{\max}, && (11a)\\ & P_w(v)\geqslant 0,\forall v, && (11b)\end{aligned}$$

where $P_{\max}$ in (11a) denotes the long-term average jamming power constraint for Willie [17]. Although the objective function in (11) is non-concave over the optimization variable, the global optimal solution can be obtained by the following methods.

3.3 Optimal solution and performance analysis

Under average jamming power constraint, the strong duality holds between the problem (P1) and its Lagrange dual problem. This fact can be verified by using the Lyapunov theorem in functional analysis as elaborated in [37], and it can also be verified by using the time-sharing condition defined in [38].

Thus, by applying the Lagrange duality method, the optimal jamming power in each round for (P1) is provided as follows.

Theorem 1. The optimal jamming power in each round for (P1) is given by

$$P_w^*(v)=\begin{cases}\frac{\beta(v)}{\alpha(v)}, & 0<\frac{\alpha(v)}{\beta(v)}<\lambda^*,\alpha(v)<0,\\ 0, & \text{otherwise},\end{cases} \tag{12}$$

where $\alpha(v)=\sqrt{\frac{2\pi}{n}}\varepsilon\varphi|h_{ab}(v)|^2-\left(2^R-1\right)|h_{aw}(v)|^2|h_{wb}(v)|^2$, $\beta(v)=\left(2^R-1\right)\sigma_b^2|h_{aw}(v)|^2-\sqrt{\frac{2\pi}{n}}\varepsilon\sigma_w^2|h_{ab}(v)|^2$, and λ^* denotes the optimal dual variable associated with the constraint (11a) as $\mathbb{E}_v\left[P_w^*(v)\right]=P_{\max}$.

Proof. See Appendix A.

It can be seen from (12) and Appendix A that the optimal jamming power allocation scheme is affected by $\alpha(v)$ and $\beta(v)$. For a fading state v with $\beta(v)>0$, the undetectable transmission fails even if Willie

does not jam. It implies that when the ratio of channel gains $\frac{|h_{aw}(v)|^2}{|h_{ab}(v)|^2} > \frac{\sqrt{\frac{2\pi}{n}}\varepsilon\sigma_w^2}{(2^R-1)\sigma_b^2}$ holds, the illegitimate transmission with rate R and covertness tolerance ε is impossible.

Besides, for a fading state v with $\alpha(v) > 0, \beta(v) < 0$, the illegitimate transmission holds no matter how much jamming power Willie adopts. It implies that when the ratio of channel gains $\frac{|h_{aw}(v)|^2}{|h_{ab}(v)|^2} < \min\{\sqrt{\frac{2\pi}{n}}\frac{\varepsilon\varphi}{(2^R-1)|h_{wb}(v)|^2}, \sqrt{\frac{2\pi}{n}}\frac{\varepsilon\sigma_w^2}{(2^R-1)\sigma_b^2}\}$ holds, the illegitimate transmission with rate R and covertness tolerance ε can be successful. In fact, the above condition holds a high probability when the SIC capacity is not sufficient, or the variance of AWGN at Willie is large.

In addition, for a fading state v with $\alpha(v) < 0, \beta(v) < 0$, $\frac{\beta(v)}{\alpha(v)}$ denotes the required jamming power for Willie to interrupt the undetectable transmission successfully. Among these fading states, Willie selects to jam those with $\frac{\alpha(v)}{\beta(v)} < \lambda^*$, so as to maximize the outage probability while satisfying the average jamming power constraint.

Based on Theorem 1 and the analysis attached to it, the outage probability with optimized jamming power can be derived as

$$\begin{aligned}
&P_{\text{out}}^I\left(\{P_w^*(v)\}\right) = \Pr\left(\beta(v) > 0\right) + \Pr\left(\alpha(v) < 0, 0 < \frac{\alpha(v)}{\beta(v)} \leqslant \lambda^*\right) \\
&\overset{\text{(a)}}{=} \int_0^{\infty}\int_0^{\infty}\int_0^{\frac{\sigma_b^2}{\kappa\varepsilon\sigma_w^2}y} \frac{\mathrm{e}^{-\frac{x}{\lambda_{ab}}-\frac{y}{\lambda_{aw}}-\frac{z}{\lambda_{wb}}}}{\lambda_{ab}\lambda_{aw}\lambda_{wb}}\mathrm{d}x\mathrm{d}y\mathrm{d}z + \int_{\frac{\sigma_b^2\varphi}{\sigma_w^2}}^{\infty}\int_0^{\infty}\int_{\frac{\sigma_b^2}{\kappa\varepsilon\sigma_w^2}y}^{\frac{(\lambda^*\sigma_b^2 y+yz)}{\kappa\varepsilon(\varphi+\lambda^*\sigma_w^2)}} \frac{\mathrm{e}^{-\frac{x}{\lambda_{ab}}-\frac{y}{\lambda_{aw}}-\frac{z}{\lambda_{wb}}}}{\lambda_{ab}\lambda_{aw}\lambda_{wb}}\mathrm{d}x\mathrm{d}y\mathrm{d}z \qquad (13)\\
&= \frac{\sigma_b^2\lambda_{aw}+\kappa\varepsilon\sigma_w^2\lambda_{ab}\mathrm{e}^{-\frac{\sigma_b^2\varphi}{\sigma_w^2\lambda_{wb}}}}{\sigma_b^2\lambda_{aw}+\kappa\varepsilon\sigma_w^2\lambda_{ab}} + \frac{\kappa\varepsilon\lambda_{ab}(\varphi+\lambda^*\sigma_w^2)}{\lambda_{wb}\lambda_{aw}}\mathrm{e}^{\frac{\lambda^*\sigma_b^2\lambda_{aw}+\kappa\varepsilon\lambda_{ab}(\varphi+\lambda^*\sigma_w^2)}{\lambda_{aw}\lambda_{wb}}}\mathrm{Ei}\left(-\frac{(\sigma_b^2\lambda_{aw}+\kappa\varepsilon\sigma_w^2\lambda_{ab})(\lambda^*\sigma_w^2+\varphi)}{\sigma_w^2\lambda_{aw}\lambda_{wb}}\right),
\end{aligned}$$

where $\kappa = \sqrt{\frac{2\pi}{n}}\frac{1}{2^R-1}$, and the step (a) holds since the channels $h_{ab}(v)$, $h_{aw}(v)$, and $h_{wb}(v)$ are independent and subject to the Rayleigh fading. It can be seen from (13) that the outage probability increases with the dual variable λ^*, where λ^* increases with $P_{\max}$. Thus, the average jamming power constraint (11a) limits the system performance under I-CSI scenarios. In addition, the outage probability under I-CSI is affected by various parameters, such as the noise variance (σ_b^2, σ_w^2), the large scale path loss (λ_{aw}, λ_{ab}, λ_{wb}), the covertness tolerance ε, and the transmission rate R. Although it is difficult to derive the relationship between the outage probability and these parameters directly due to the complicated expression (13), it can be revealed by simulation results, as shown in Section 5.

When $P_{\max} = 0$, the system degrades to the scenario with a passive warder, where Willie only detects the transmission but does not emit jamming signals. The detection error probability can be obtained by substituting $P_w(v) = 0$ into (4), and the SNR at Bob under covertness requirement can also be obtained by (9). Further, the outage probability can be derived by substituting $P_{\max} = 0$ into (13) as

$$P_{\text{out}}^I\left(\{P_w(v) = 0\}\right) = \frac{\sigma_b^2\lambda_{aw}}{\sigma_b^2\lambda_{aw} + \kappa\varepsilon\sigma_w^2\lambda_{ab}}. \qquad (14)$$

In addition, when the jamming power constraint is loose enough, i.e., $P_{\max} \to \infty$, the outage probability can be derived as

$$\lim_{P_{\max}\to\infty} P_{\text{out}}^I(\{P_w^*(v)\}) = \frac{\sigma_b^2\lambda_{aw}+\kappa\varepsilon\sigma_w^2\lambda_{ab}\mathrm{e}^{-\frac{\sigma_b^2\varphi}{\sigma_w^2\lambda_{wb}}}}{\sigma_b^2\lambda_{aw}+\kappa\varepsilon\sigma_w^2\lambda_{ab}} + \frac{\kappa\varepsilon\varphi\lambda_{ab}\mathrm{e}^{\frac{\kappa\varepsilon\varphi\lambda_{ab}}{\lambda_{aw}\lambda_{wb}}}}{\lambda_{wb}\lambda_{aw}}\mathrm{Ei}\left(-\frac{\kappa\varphi\lambda_{ab}\varepsilon\sigma_w^2+\varphi\lambda_{aw}\sigma_b^2}{\sigma_w^2\lambda_{aw}\left(2^R-1\right)\lambda_{wb}}\right), \qquad (15)$$

which is affected by the RSI factor φ. Specially, when the SIC capacity is sufficient enough and the jamming power constraint is loose enough (i.e., $\varphi \to 0$, $P_{\max} \to \infty$), the outage probability approaches 1.

4 Performance analysis and optimization under S-CSI

In this section, the system performance under S-CSI is investigated. Specially, the average detection error probability at the warder with S-CSI is derived. In addition, the outage probability of the illegitimate

transmission is derived in terms of the jamming power. Finally, the jamming power is optimized to maximize the outage probability, and the corresponding outage probability with optimized jamming power is derived to evaluate the system performance.

4.1 Detection performance at Willie

Since the I-CSI is unavailable in this case, the transmit power $P_a(v)$ at Alice and the jamming power $P_w(v)$ at Willie cannot be designed based on I-CSI as shown in Section 3. Thus, the transmit power and the jamming power are assumed to be fixed among different rounds [25, 39], where $P_a(v) = P_a, \forall v$ and $P_w(v) = P_w, \forall v$ in this section for notation simplification.

In addition, in this scenario, the average detection error probability at Willie is adopted as a metric to evaluate the detection performance [12, 25]. To minimize the average detection error probability, the optimal detection threshold in this case is given by

$$\tau^* = \arg\min_{\tau} \mathbb{E}_{|h_{aw}(v)|^2} \left[\xi\left(\tau\right)\right], \tag{16}$$

which remains the same among different transmission rounds.

With given threshold τ, the average detection error probability is given by [36]

$$\bar{\xi}(\tau) = \mathbb{E}_{|h_{aw}(v)|^2} \left[\xi\left(\tau\right)\right] \overset{(a)}{=} 1 - \frac{1}{\Gamma\left(n\right)} \int_0^{\infty} \left(\gamma\left(n, \frac{n\tau}{\varphi P_w + \sigma_w^2}\right) - \gamma\left(n, \frac{n\tau}{\varphi P_w + \sigma_w^2 + x}\right)\right) \frac{\mathrm{e}^{-\frac{y}{P_a \lambda_{aw}}}}{P_a \lambda_{aw}} \mathrm{d}y, \tag{17}$$

where the step (a) holds since the channel $h_{aw}(v)$ is subject to the quasi-static Rayleigh fading.

By applying Gaussian-Chebyshev Quadrature technology [12, 25], the average detection error probability at Willie with an optimal threshold can be derived as

$$\bar{\xi}\left(\tau^*\right) = 1 - \frac{1}{\Gamma(n)} \gamma\left(n, \frac{n\tau^*}{\varphi P_w + \sigma_w^2}\right) - \frac{\pi}{B P_a \lambda_{aw}} \sum_{i=1}^{B} \gamma\left(n, \frac{n\tau^*}{\varphi P_w + \sigma_w^2 + \tan\theta_i}\right) \frac{\sqrt{\theta_i\left(\frac{\pi}{2} - \theta_i\right)} \mathrm{e}^{-\frac{\tan\theta_i}{P_a \lambda_{aw}}}}{\cos^2 \theta_i}, \tag{18}$$

where B is the parameter of Gaussian-Chebyshev Quadrature, $\theta_i = \frac{\pi}{4}\left(1 + \cos\frac{(2i-1)\pi}{2B}\right)$, and corresponding detection threshold τ^* which minimizes (18) can be calculated as follows, as proven in [25, Appendix D]:

$$\tau^* = -\frac{\varphi P_w + \sigma_w^2}{n} \ln\left(\frac{\pi}{B P_a \lambda_{aw}} \sum_{i=1}^{B} \frac{\mathrm{e}^{-\frac{n\tau^*}{\varphi P_w + \sigma_w^2 + \tan\theta_i}} \sqrt{\theta_i\left(\frac{\pi}{2} - \theta_i\right)} \mathrm{e}^{-\frac{\tan\theta_i}{P_a \lambda_{aw}}}}{\left(1 + \tan\theta_i / (\varphi P_w + \sigma_w^2)\right)^n \cos^2\theta_i}\right). \tag{19}$$

Due to the complicated form of (18), it is intractable for further analysis and optimization. Thus, a tractable approximation of average detection probability under high covertness with a moderate number of channel use n scenarios (i.e., $\bar{\xi}\left(\tau^*\right) \geqslant 0.9, n \geqslant 50$) can be given as

$$\bar{\xi}\left(\tau^*\right) \approx 1 - \sqrt{\frac{n}{2\pi}} \frac{P_a \lambda_{aw}}{\varphi P_w + \sigma_w^2}, \tag{20}$$

which is elaborated in [36, Appendix B] and [25, Appendix A] using the Taylor series expansion technology and the asymptotic property of the Gamma function, and the detail deviation is omitted here for brevity. Similar to (6) under I-CSI, the detection error probability decreases with P_a and n while increasing with P_w and φ. Differently, the result (20) under S-CSI is affected by λ_{aw} not h_{aw} in (6) under I-CSI. Moreover, the tightness of (20) is also verified by extensive Monte Carlo simulation results in Section 5.

4.2 Problem formulation

To guarantee the transmission covertness in this scenario, i.e., the average detection error probability at Willie exceeds the predetermined threshold ($\bar{\xi}(\tau) \geqslant 1 - \varepsilon$), the transmit power at Alice is limited as

$$P_a \leqslant \sqrt{\frac{2\pi}{n}} \frac{\varepsilon(\varphi P_w + \sigma_w^2)}{\lambda_{aw}}. \tag{21}$$

By substituting the maximum transmit power (21) into (7), the SNR at Bob under the covertness requirement can be obtained. Further, the outage probability of the undetectable transmission in this case can be derived as

$$\begin{aligned} P_{\text{out}}^{S}(P_w) = \mathbb{E}_v\left[X(v)\right] &\overset{\text{(a)}}{=} \int_0^{\infty} \int_0^{\frac{\lambda_{aw}(P_w z+\sigma_b^2)}{\kappa\varepsilon(\varphi P_w+\sigma_w^2)}} \frac{\mathrm{e}^{-\frac{x}{\lambda_{ab}}-\frac{z}{\lambda_{wb}}}}{\lambda_{ab}\lambda_{wb}}\mathrm{d}x\mathrm{d}z \\ &= 1-\frac{\kappa\varepsilon(\varphi P_w+\sigma_w^2)\lambda_{ab}}{\lambda_{aw}\lambda_{wb}P_w+\kappa\varepsilon(\varphi P_w+\sigma_w^2)\lambda_{ab}}\mathrm{e}^{-\frac{\lambda_{aw}\sigma_b^2}{\kappa\varepsilon(\varphi P_w+\sigma_w^2)\lambda_{ab}}}, \end{aligned} \tag{22}$$

where the step (a) holds since the channels $h_{ab}(v)$ and $h_{wb}(v)$ are subject to the Rayleigh fading.

From the perspective of legitimate monitor for counter covert communications, Willie can adjust the jamming power P_w to maximize the outage probability between Alice and Bob, which is formulated as

$$(\text{P2}): \max_{P_w} \quad P_{\text{out}}^{S}(P_w) \tag{23}$$

$$\text{s.t. } 0 \leqslant P_w \leqslant P_{\max}, \tag{23a}$$

where Eq. (23a) denotes the jamming power constraint at Willie, in which the long-term average power constraint (11a) degenerates into (23a) since the jamming power remains the same among different transmission rounds.

4.3 Optimal solution and performance analysis

Since the outage probability in this case can be expressed explicitly in terms of P_w as shown in (22), the optimal solution for (P2) can be obtained by analyzing the monotonicity of $P_{\text{out}}^{S}(P_w)$ with respect to P_w.

Theorem 2. The optimal jamming power for (P2) is given by

$$P_w^* = \begin{cases} 0, & r_1 \leqslant \frac{\varphi}{\lambda_{wb}}, \\ P_o, & r_2 \leqslant \frac{\varphi}{\lambda_{wb}} < r_1, \\ P_{\max}, & \frac{\varphi}{\lambda_{wb}} < r_2, \end{cases} \tag{24}$$

where $P_o = \min\{P_{\max}, P_r\}$, $P_r = \frac{\kappa\varepsilon\lambda_{ab}\sigma_w^2(\varphi\sigma_b^2-\sigma_w^2\lambda_{wb})}{\varphi(\kappa\varepsilon\sigma_w^2\lambda_{ab}\lambda_{wb}-\kappa\varphi\varepsilon\sigma_b^2\lambda_{ab}-\sigma_b^2\lambda_{aw}\lambda_{wb})}$, $r_1 = \frac{\sigma_w^2}{\sigma_b^2}$, and $r_2 = r_1 - \frac{\lambda_{aw}}{\kappa\varepsilon\lambda_{ab}}$.

Proof. See Appendix B.

It can be seen from (24) and Appendix B that when the ratio of the RSI factor φ to the fading coefficient λ_{wb} exceeds the ratio of noise variances r_1, the extra jamming signal is harmful to the legitimate monitor system. Thus, in this case, the passive guarding approach is optimal, which is better than the proactive guarding approach. That is because the loss of detection accuracy by jamming signals outweighs the gain from the reliability reduction of the undetectable transmission.

Besides, when the ratio $\frac{\varphi}{\lambda_{wb}}$ decreases and falls into the interval $[r_2, r_1)$, the outage probability increases with P_w when $P_w \leqslant P_r$. It implies that in this case the jamming signal is beneficial to the legitimate monitor system, but the optimal jamming power is not necessarily the maximum one.

In addition, when the ratio $\frac{\varphi}{\lambda_{wb}}$ is lower than r_2, the outage probability always decreases with P_w. This implies that when the SIC capability is sufficient, the jamming signal is always beneficial to the legitimate monitor system, and the optimal jamming power is accurately the maximum.

Overall, these results reveal that the jamming signals are not necessarily beneficial to the legitimate monitor system under S-CSI. Specially, the SIC capacity is a critical factor that significantly affects the performance of the proactive guarding approach. When the SIC capacity is insufficient, the jamming signal is detrimental, while it is beneficial when the SIC capacity is sufficient.

Besides, the outage probability with optimized jamming power can be obtained by substituting (24) into (22) as follows:

$$P_{\text{out}}^{S}\left(P_w^*\right) = \begin{cases} 1-\mathrm{e}^{-\frac{\lambda_{aw}\sigma_b^2}{\kappa\varepsilon\sigma_w^2\lambda_{ab}}}, & r_1 \leqslant \frac{\varphi}{\lambda_{wb}}, \\ 1-\frac{\kappa\varepsilon(\varphi P_o+\sigma_w^2)\lambda_{ab}}{\lambda_{aw}\lambda_{wb}P_o+\kappa\varepsilon(\varphi P_o+\sigma_w^2)\lambda_{ab}}\mathrm{e}^{-\frac{\lambda_{aw}\sigma_b^2}{\kappa\varepsilon(\varphi P_o+\sigma_w^2)\lambda_{ab}}}, & r_2 \leqslant \frac{\varphi}{\lambda_{wb}} < r_1, \\ 1-\frac{\kappa\varepsilon\left(\varphi P_{\max}+\sigma_w^2\right)\lambda_{ab}}{\lambda_{aw}\lambda_{wb}P_{\max}+\kappa\varepsilon(\varphi P_{\max}+\sigma_w^2)\lambda_{ab}}\mathrm{e}^{-\frac{\lambda_{aw}\sigma_b^2}{\kappa\varepsilon\left(\varphi P_{\max}+\sigma_w^2\right)\lambda_{ab}}}, & \frac{\varphi}{\lambda_{wb}} < r_2, \end{cases} \tag{25}$$

where the expression in (25) for the case $r_1 \leqslant \frac{\varphi}{\lambda_{wb}}$ is also suitable for the sceanrio with a passive warder.

Different from the results (13) under I-CSI, it can be seen from (25) that the range of $\frac{\varphi}{\lambda_{wb}}$ affects the expression of outage probability. In this case, the maximum jamming power constraint (23a) does not always limit the system performance, which differs from the results under I-CSI scenarios, as elaborated in Section 3. Specially, under the case $r_1 \leqslant \frac{\varphi}{\lambda_{wb}}$ or the case $r_2 \leqslant \frac{\varphi}{\lambda_{wb}} < r_1$ with $P_{\max} \geqslant P_o$, the system performance is independent with $P_{\max}$. Under the case $r_2 \leqslant \frac{\varphi}{\lambda_{wb}} < r_1$ with $P_{\max} < P_o$ or the case $\frac{\varphi}{\lambda_{wb}} < r_2$, the system performance is limited by $P_{\max}$. In addition, the outage probability increases with the decrease of ε. This is because when the transmission covertness requirement restricts the transmit power at Alice.

Further, when the jamming power constraint is loose enough, i.e., $P_{\max} \to \infty$, the outage probability under the case $r_1 \leqslant \frac{\varphi}{\lambda_{wb}}$ is the same as that in (25). And the outage probability under the case $r_2 \leqslant \frac{\varphi}{\lambda_{wb}} < r_1$ can be obtained by (25) by replacing P_o with P_r. In addition, the outage probability under the case $\frac{\varphi}{\lambda_{wb}} < r_2$ can be derived as

$$\lim_{P_{\max}\to\infty} P_{\text{out}}^{S}\left(P_w^*\right) = \frac{\lambda_{aw}\lambda_{wb}}{\lambda_{aw}\lambda_{wb} + \kappa\varepsilon\varphi\lambda_{ab}}, \tag{26}$$

which is affected by the RSI factor φ but not by the AWGN variances σ_w^2 and σ_b^2. Especially, when the SIC capacity is sufficient and the jamming power constraint is loose (i.e., $\varphi \to 0$ and $P_{\max} \to \infty$), the outage probability approaches 1.

5 Numerical simulation

In this section, representative numerical results are provided to evaluate the system performance. The parameter settings are as follows, unless specified otherwise: Alice, Bob, and Willie are located at (0, 0), (140 m, 0), and (100 m, 20 m) in a two-dimensional plane, respectively. The path loss is modeled as $\lambda_{ij} = -69.8 - 20\log_{10}(d_{ij})\,\text{dB}, ij \in \{ab, aw, wb\}$, where d_{ij} denotes the distance between nodes i and j. We set the AWGN variances as $\sigma_b^2 = \sigma_w^2 = -80$ (dBm), the number of channel use as $n = 500$, and the Gaussian-Chebyshev Quadrature parameter as $B = 10^5$. The adopted benchmark schemes are defined as follows.

- Full-duplex with fixed jamming power (FD-F) scheme: The full-duplex warder with fixed jamming power (e.g., $P_w(v) = P_{\max}$) [25].
- Full-duplex with random jamming power (FD-R) scheme: The full-duplex warder with random jamming power (e.g., $P_w(v) \sim \mathcal{U}[0, 2P_{\max}]$) [40].
- Half-duplex with fixed jamming power (HD-F) scheme: Each transmission round is divided into two equal-length phases, Phase I and Phase II. In a random phase (Phase I or II), the warder detects the transmission without emitting jamming signals. Besides, in the other phase, the warder emits jamming signals with the maximum power since no RSI exits in this half-duplex mode [19].
- Passive guarding (PG) scheme: The warder only detects the transmission (e.g., $P_w(v) = 0$) [11].

In Figure 2, the impacts of the transmit power and the jamming power on the detection error probability are investigated. The value of $|h_{aw}|^2$ and λ_{aw} adopted here is selected as typical representatives when d_{aw} falls in the range $[100, 300]$ (m) [41]. The curves with "Sim.", "Exa." and "App." denote the results obtained by Monte Carlo simulations, the analytical expression (4)/(18), and the approximations (6)/(20), respectively. Each result on the curves with "Sim." is obtained by performing 10^8 Monte Carlo simulations. It can be seen that the curves with Monte Carlo simulations, the analytical expressions and the approximations coincide under various parameters in high covertness scenarios (i.e., $\xi(\tau^*(v))/\bar{\xi}(\tau^*) \geqslant 0.9$), which demonstrates the accuracy of the analytical expressions and the tightness of the approximations. Besides, the detection error probability increases with the jamming power while decreasing with the transmit power. In addition, the detection error probability decreases with the increases of the channel gain (and the path loss coefficient) while it increases with the increases of the RSI factor. These results reveal the impact of the channel gain and RSI factor on the detection performance, which further implies that the optimal design of the system is closely related to these factors.

In Figure 3, the impacts of the transmission rate and the jamming power constraint on the outage probability are investigated under I-CSI scenarios. In Figure 3(a), the outage probability increases with the transmission rate and decreases with the covertness tolerance. It implies that a fundamental

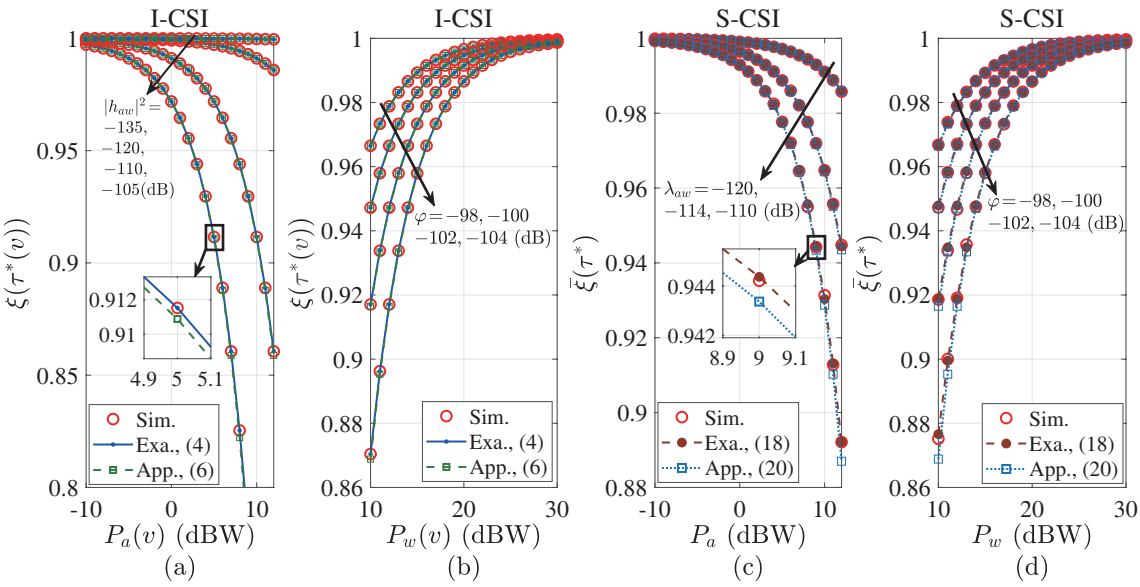

Figure 2 (Color online) Decoding error probability versus the transmit and jamming power under I-CSI and S-CSI. (a) $\varphi = -100$ (dB), $P_w(v) = 20$ (dBW); (b) $|h_{aw}|^2 = -112$ (dB), $P_a(v) = 0$ (dBW); (c) $\varphi = -100$ (dB), $P_w = 20$ (dBW); (d) $\lambda_{aw} = -112$ (dB), $P_a = 0$ (dBW).

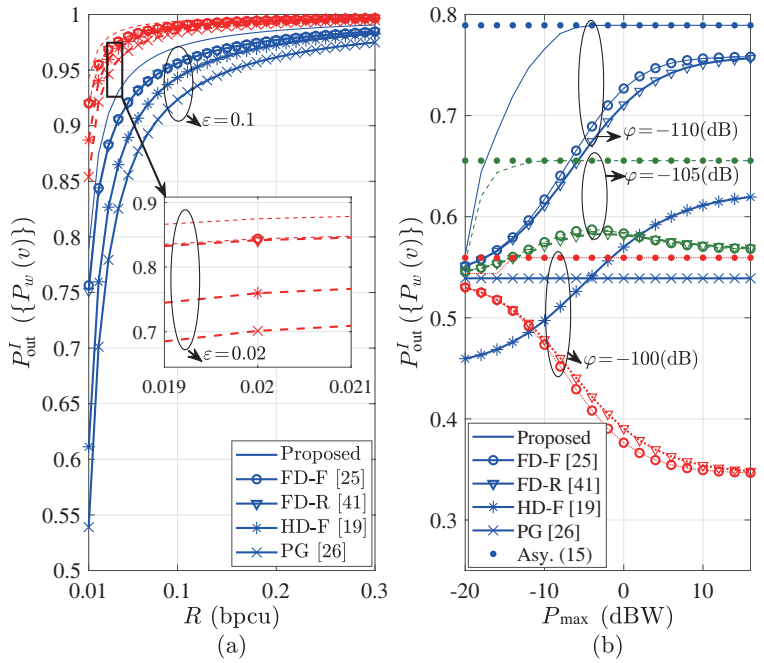

Figure 3 (Color online) Outage probability under I-CSI versus the transmission rate and the average jamming power constraint. (a) $\varphi = -110$ (dB), $P_{\max} = 10$ (dBW); (b) $\varepsilon = 0.1$, $R = 0.01$ (bpcu).

tradeoff exists among the transmission reliability (evaluated by $P_{\text{out}}^I(\{P_w(v)\})$), transmission covertness (evaluated by ε), and transmission efficiency (evaluated by R). Besides, the proposed scheme outperforms other benchmark schemes, including the FD-F scheme, FD-R scheme, HD-F scheme, and PG scheme. In Figure 3(b), the outage probability with the proposed scheme first increases with $P_{\max}$ and then is saturated, which coincides with (15). However, the outage probabilities with FD-F scheme and FD-R scheme decrease with $P_{\max}$ when $P_{\max}$ is large enough and $\varphi \geqslant -105$ (dB), since the damage caused by the jamming signal exceeds its gain in these cases. In addition, the proposed scheme also outperforms the HD-F scheme when $\varphi \leqslant -105$ (dB), which holds broadly in practical full-duplex systems, for example, $\varphi = -122.5$ (dB) has been validated by [42] recently. These results reveal the impact of parameters $(R, \varepsilon, \varphi, P_{\max})$ on the system performance, and verify the superiority of the proposed scheme under I-CSI

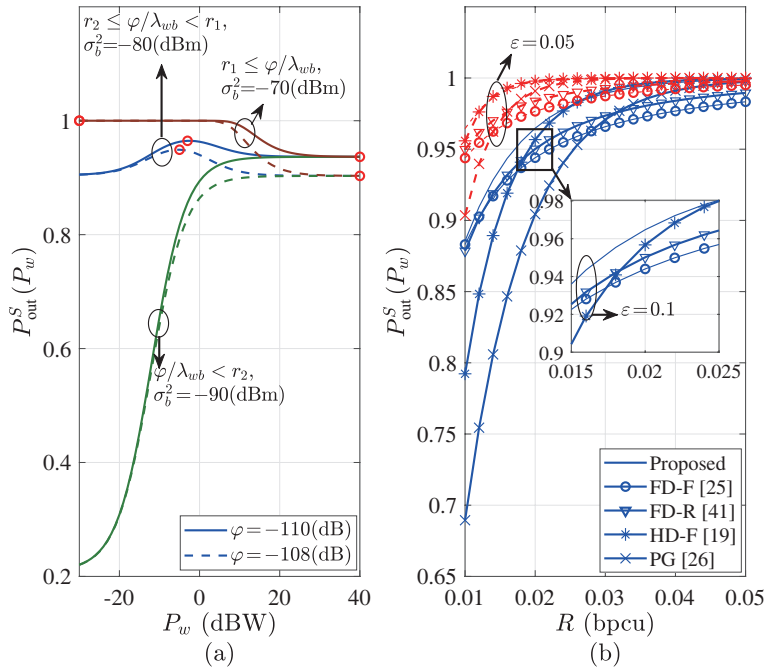

Figure 4 (Color online) Outage probability under S-CSI versus the jamming power and the transmission rate. (a) $\sigma_w^2 = -80$ (dBm), $\varepsilon = 0.1$, and $R = 0.02$ (bpcu); (b) $\sigma_w^2 = \sigma_b^2 = -80$ (dBm), $P_{\max} = 10$ (dBW), and $\varphi = -110$ (dB).

compared with other benchmarks.

In Figure 4, the impacts of the jamming power and transmission rate on the outage probability are investigated under S-CSI scenarios. It can be seen from Figure 4(a) that when $\varphi/\lambda_{wb} < r_2$, the outage probability increases with P_w. When $r_2 \leqslant \varphi/\lambda_{wb} < r_1$, the outage probability first increases and then decreases with P_w. When $r_1 \leqslant \varphi/\lambda_{wb}$, the outage probability decreases with P_w. Besides, when $P_w \to \infty$, the outage probability approaches (26), which is affected by φ but not σ_b^2. When $P_w \to 0$, the performance is affected by σ_b^2 but not φ. In addition, it can be seen from Figure 4(b) that the fundamental tradeoff among the transmission reliability (evaluated by $P_{\text{out}}^S(P_w)$), transmission covertness (evaluated by ε), and transmission efficiency (evaluated by R) also exists under the S-CSI scenarios. Besides, the proposed scheme always outperforms the FD-F scheme, FD-R scheme, and PG scheme regardless of the value of R. Moreover, when R is small, the proposed scheme significantly outperforms the HD-F scheme. As R increases, the gap between the results of the proposed scheme and the HD-F scheme gradually decreases until it almost disappears. These results verify the superiority of the proposed scheme compared with other benchmarks under S-CSI.

In Figure 5, the impact of the location of Willie on the outage probability is investigated under I-CSI scenarios. The values on the contour lines represent the outage probability. It can be seen from Figure 5(a) that the outage probability increases as Willie gets closer to Alice/Bob under the proactive guarding approach. For example, the outage probability of illegitimate transmission exceeds 0.9 when $d_{aw} < 30$ (m) or $d_{wb} < 10$ (m). However, the outage probability under the passive guarding approach is less than 0.4 when Willie is proximal to Bob. These results demonstrate the superiority of the proposed scheme compared with the passive guarding approach, especially when Willie cannot be deployed close to Alice.

In Figure 6, the impact of the location of Willie on the outage probability is investigated under S-CSI scenarios. The values on the contour lines represent the outage probability. Similar to the results shown in Figure 5, it can be seen that the outage probability increases as Willie gets close to Alice or Bob under proactive guarding. And the proactive guarding approach outperforms the passive one especially when Willie is not proximal to Alice. Therefore, these results in Figures 5 and 6 guide the deployment of Willie in a practical system. When adopting the proposed scheme, whether Willie is located close to Alice or Bob, the purpose of counter covert communications can be effectively achieved.

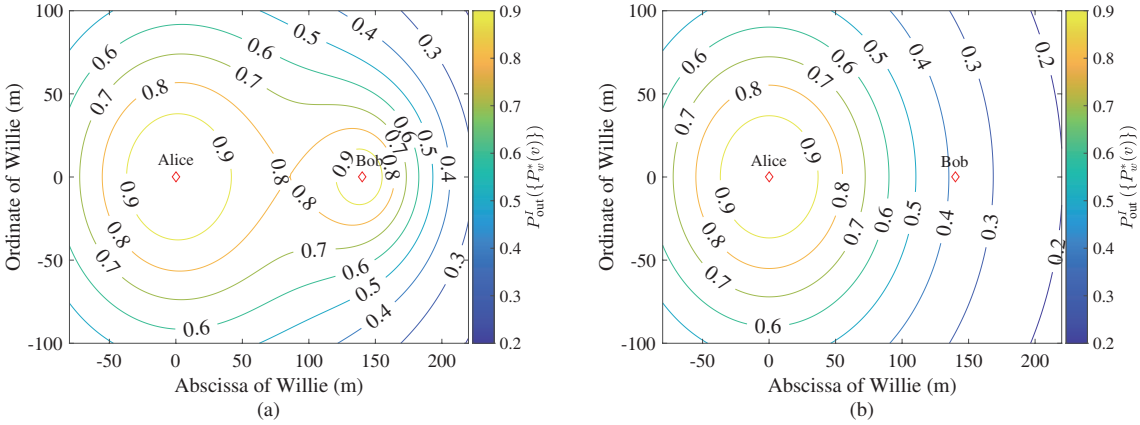

Figure 5 (Color online) Outage probability under I-CSI versus the location of Willie. $R = 0.01$ (bpcu), $P_{\max} = 20$ (dBW), $\varphi = -110$ (dB), and $\varepsilon = 0.1$. (a) Proactive guarding; (b) passive guarding.

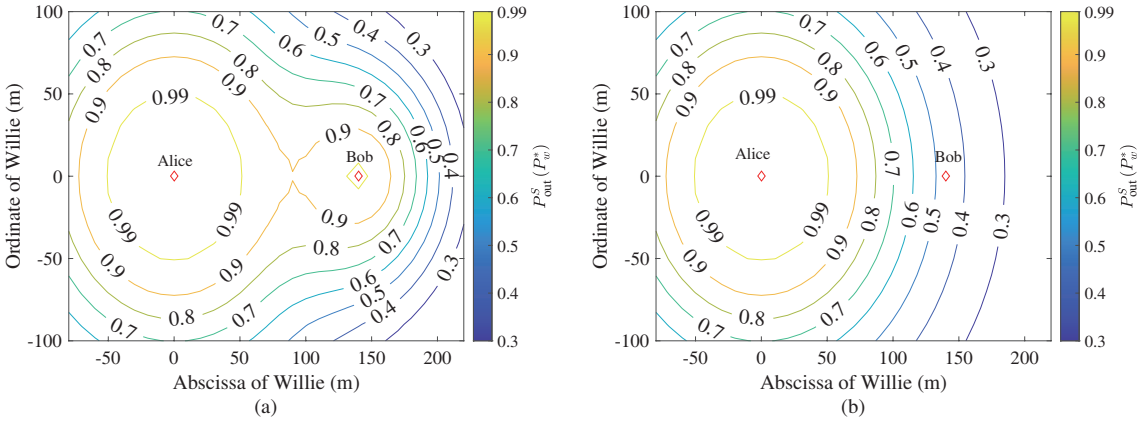

Figure 6 (Color online) Outage probability under S-CSI versus the location of Willie. $R = 0.01$ (bpcu), $P_{\max} = 20$ (dBW), $\varphi = -110$ (dB), and $\varepsilon = 0.1$. (a) Proactive guarding; (b) passive guarding.

6 Conclusion

In this paper, we have proposed a novel paradigm for counter covert communications, called legitimate monitor, where the outage probability of the undetectable transmission between unauthorized nodes is the core concern. To intercept the illegitimate transmission effectively, a proactive guarding approach has been provided since the unauthorized transmitter may deploy a certain range of safety zones to prevent monitoring. Considering the availability of the channel state information in practical applications, the jamming power at the proactive warder has been optimized and the system performance has been revealed in the I-CSI scenario and S-CSI scenario, respectively. Numerical results demonstrate the accuracy of the derived results and the superiority of the proposed scheme compared with other benchmark schemes, including the existing FD-F scheme, FD-R scheme, and PG scheme. Besides, the full-duplex warder also outperforms the half-duplex one when the RSI is relatively small, which holds broadly in practical full-duplex systems. Moreover, by adopting the proposed scheme, the purpose of counter covert communications can be effectively achieved whether the warder is located close to the unauthorized transmitter or the receiver.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant No. 62271309) and Shanghai Municipal Science and Technology Major Project (Grant No. 2021SHZDZX0102).

References

1 Illi E, Qaraqe M, Althunibat S, et al. Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing IoT networks. IEEE Commun Surv Tutorials, 2024, 26: 347–388

2 Teng Y, Li J Y, Huang M X, et al. Low-complexity and high-performance receive beamforming for secure directional modulation networks against an eavesdropping-enabled full-duplex attacker. Sci China Inf Sci, 2022, 65: 119302

3 Wang D W, He T M, Zhou F H, et al. Outage-driven link selection for secure buffer-aided networks. Sci China Inf Sci, 2022, 65: 182303

4 Chen X, An J, Xiong Z, et al. Covert communications: a comprehensive survey. IEEE Commun Surv Tutorials, 2023, 25: 1173–1198

5 Lu K, Liu H, Zeng L, et al. Applications and prospects of artificial intelligence in covert satellite communication: a review. Sci China Inf Sci, 2023, 66: 121301

6 Bash B A, Goeckel D, Towsley D. Limits of reliable communication with low probability of detection on AWGN channels. IEEE J Sel Areas Commun, 2013, 31: 1921–1930

7 Arumugam K S K, Bloch M R. Covert communication over a K-user multiple-access channel. IEEE Trans Inform Theor, 2019, 65: 7020–7044

8 Tan V Y F, Lee S H. Time-division is optimal for covert communication over some broadcast channels. IEEE Trans Inform Forensic Secur, 2019, 14: 1377–1389

9 Chen W, Ding H, Wang S, et al. On the limits of covert backscatter communication over undecodable ambient signals. IEEE Trans Inform Forensic Secur, 2023, 18: 4198–4213

10 Zheng T X, Yang Z, Wang C, et al. Wireless covert communications aided by distributed cooperative jamming over slow fading channels. IEEE Trans Wireless Commun, 2021, 20: 7026–7039

11 Wang M, Xia B, Xu Z, et al. Performance analysis and optimization for coordinated direct and relay covert transmission with multiantenna warder. IEEE Internet Things J, 2023, 10: 13414–13427

12 Wang M, Xia B, Yao Y, et al. Fundamental limit among covertness, reliability, latency and throughput for IRS-enabled short-packet communications. IEEE Trans Wireless Commun, 2024, 23: 3886–3900

13 Im H S, Lee S H. Mobility-assisted covert communication over wireless ad hoc networks. IEEE Trans Inform Forensic Secur, 2021, 16: 1768–1781

14 Li J, Wu D, Yue C, et al. Energy-efficient transmit probability-power control for covert D2D communications with age of information constraints. IEEE Trans Veh Technol, 2022, 71: 9690–9704

15 Rao H, Xiao S, Yan S, et al. Optimal geometric solutions to UAV-enabled covert communications in line-of-sight scenarios. IEEE Trans Wireless Commun, 2022, 21: 10633–10647

16 Xu D, Zhu H. Proactive eavesdropping via jamming over short packet suspicious communications with finite blocklength. IEEE Trans Commun, 2022, 70: 7505–7519

17 Xu J, Duan L, Zhang R. Proactive eavesdropping via cognitive jamming in fading channels. IEEE Trans Wireless Commun, 2017, 16: 2790–2806

18 Zeng Y, Zhang R. Wireless information surveillance via proactive eavesdropping with spoofing relay. IEEE J Sel Top Signal Process, 2016, 10: 1449–1461

19 Hu G, Si J, Cai Y, et al. Intelligent reflecting surface-assisted proactive eavesdropping over suspicious broadcasting communication with statistical CSI. IEEE Trans Veh Technol, 2022, 71: 4483–4488

20 Hu G, Li Z, Si J, et al. Analysis and optimization of STAR-RIS-assisted proactive eavesdropping with statistical CSI. IEEE Trans Veh Technol, 2023, 72: 6850–6855

21 Xu D. Proactive eavesdropping of jamming-assisted suspicious communications in fading channels: a Stackelberg game approach. IEEE Trans Commun, 2024, 72: 2913–2928

22 Zhang H, Duan L, Zhang R. Jamming-assisted proactive eavesdropping over two suspicious communication links. IEEE Trans Wireless Commun, 2020, 19: 4817–4830

23 Hu Y D, Gao R F, Li Y, et al. On proactive eavesdropping using anti-relay-selection jamming in multi-relay communication systems. Sci China Inf Sci, 2019, 62: 042304

24 Xu D, Zhu H B. Proactive eavesdropping of wireless powered suspicious interference networks. Sci China Inf Sci, 2021, 64: 229305

25 Wang M, Yao Y, Xia B, et al. Covert and reliable short-packet communications over fading channels against a proactive warder: analysis and optimization. IEEE Trans Wireless Commun, 2024, 23: 3932–3945

26 Rao H, Wu M, Wang J, et al. D2D covert communications with safety area. IEEE Syst J, 2021, 15: 2331–2341

27 Ma R, Yang W, Tao L, et al. Covert communications with randomly distributed wardens in the finite blocklength regime. IEEE Trans Veh Technol, 2022, 71: 533–544

28 Ma S, Zhang Y, Li H, et al. Robust beamforming design for covert communications. IEEE Trans Inform Forensic Secur, 2021, 16: 3026–3038

29 Wang C, Li Z, Zhang H, et al. Achieving covertness and security in broadcast channels with finite blocklength. IEEE Trans Wireless Commun, 2022, 21: 7624–7640

30 Chaman A, Wang J, Sun J, et al. Ghostbuster: detecting the presence of hidden eavesdroppers. In: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, New York, 2018. 337–351

31 Yan S, Cong Y, Hanly S V, et al. Gaussian signalling for covert communications. IEEE Trans Wireless Commun, 2019, 18: 3542–3553

32 Xu D, Zhu H. Unsuspicious user enabled proactive eavesdropping in interference networks using improper gaussian signaling.

IEEE Trans Commun, 2023, 71: 2891–2905
33 Kim D, Lee H, Hong D. A survey of in-band full-duplex transmission: from the perspective of PHY and MAC layers. IEEE Commun Surv Tut, 2015, 17: 2017–2046
34 Alexandris K, Balatsoukas-Stimming A, Burg A. Measurement-based characterization of residual self-interference on a full-duplex MIMO testbed. In: Proceedings of IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2014. 329–332
35 Sobers T V, Bash B A, Guha S, et al. Covert communication in the presence of an uninformed jammer. IEEE Trans Wireless Commun, 2017, 16: 6193–6206
36 Shahzad K, Zhou X. Covert wireless communications under quasi-static fading with channel uncertainty. IEEE Trans Inform Forensic Secur, 2021, 16: 1104–1116
37 Luo Z-Q, Zhang S Z. Dynamic spectrum management: complexity and duality. IEEE J Sel Top Signal Process, 2008, 2: 57–73
38 Yu W, Lui R. Dual methods for nonconvex spectrum optimization of multicarrier systems. IEEE Trans Commun, 2006, 54: 1310–1322
39 Che B, Shi H, Yang W, et al. Covert wireless communication against jamming-assisted proactive detection. IEEE Wireless Commun Lett, 2023, 12: 1304–1308
40 Lu X, Huang Y, Yan S, et al. Energy-efficient covert wireless communication through probabilistic jamming. IEEE Wireless Commun Lett, 2023, 12: 932–936
41 Zhou X, Yan S, Wu Q, et al. Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint. IEEE Trans Wireless Commun, 2022, 21: 532–547
42 Yu B, Qian C, Lin P, et al. Full duplex communication with practical self-interference cancellation implementation. In: Proceedings of IEEE International Conference on Communications (ICC), Seoul, 2022. 1100–1105

Appendix A Proof of Theorem 1

Since the zero duality gap holds for (P1) revealed by [37,38], the Lagrange duality method can be applied to solve the problem (P1) optimally. Let $\lambda \geqslant 0$ denote the dual variable associated with the average jamming power constraint in (11a). Then the partial Lagrangian of problem (P1) is expressed as

$$\mathcal{L}\left(\{P_w(v)\},\lambda\right)=\mathbb{E}_v\left[X(v)\right]-\lambda\left(\mathbb{E}_v\left[P_w\left(v\right)\right]-P_{\max}\right). \tag{A1}$$

Accordingly, the dual problem of (P1) is given by

$$\text{(D1)}:\max_{\lambda\geqslant 0} f\left(\lambda\right), \tag{A2}$$

where $f\left(\lambda\right)$ in (D1) denotes the dual function as

$$f\left(\lambda\right)=\max_{\{P_w(v)\geqslant 0\}}\mathcal{L}\left(\{P_w(v)\},\lambda\right). \tag{A3}$$

Since strong duality holds between (P1) and its dual problem (D1), we solve (P1) by equivalently solving (D1). In particular, we first solve problem (A3) to obtain $f\left(\lambda\right)$ under any given λ and then solve problem (D1) to find the optimal λ, defined as λ^*.

First, consider problem (A3) under any given $\lambda \geqslant 0$. By discarding the constant term $\lambda P_{\max}$, problem (A3) can be decomposed into a sequence of subproblems as follows, each for one fading state v:

$$\max_{P_w(v)\geqslant 0} X(v)-\lambda P_w\left(v\right). \tag{A4}$$

For notation simplification, let $\alpha(v)=\sqrt{\frac{2\pi}{n}}\varepsilon\varphi|h_{ab}(v)|^2-(2^R-1)|h_{aw}(v)|^2|h_{wb}(v)|^2$ and $\beta(v)=(2^R-1)\sigma_b^2|h_{aw}(v)|^2-\sqrt{\frac{2\pi}{n}}\varepsilon\sigma_w^2|h_{ab}(v)|^2$. Then, the subproblem (A4) can be divided and solved in the following six cases.

Case 1. When $\alpha(v)>0,\beta(v)>0$, and $0\leqslant P_w(v)<\frac{\beta(v)}{\alpha(v)}$, it implies that $X(v)=1$, for which the optimal solution can be expressed as $P_w^{(\lambda)}(v)=0$ and the corresponding objective function value for (A4) can be calculated as $X(v)-\lambda P_w^{(\lambda)}\left(v\right)=1$.

Case 2. When $\alpha(v)>0,\beta(v)>0$, and $P_w(v)\geqslant\frac{\beta(v)}{\alpha(v)}$, it implies that $X(v)=0$, for which the optimal solution can be expressed as $P_w^{(\lambda)}(v)=\frac{\beta(v)}{\alpha(v)}$ and the corresponding objective function value for (A4) can be calculated as $X(v)-\lambda P_w^{(\lambda)}\left(v\right)=-\frac{\lambda\beta(v)}{\alpha(v)}<1$.

Comparing the objective function value under Cases 1 and 2, it can be concluded that when $\alpha(v)>0,\beta(v)>0$, the optimal solution can be expressed as $P_w^{(\lambda)}(v)=0$.

Case 3. When $\alpha(v)>0,\beta(v)<0$, it implies that $X(v)=0$, for which the optimal solution can be expressed as $P_w^{(\lambda)}(v)=0$ and the corresponding function objective value for (A4) can be calculated as $X(v)-\lambda P_w^{(\lambda)}\left(v\right)=0$.

Case 4. When $\alpha(v)<0,\beta(v)>0$, it implies that $X(v)=1$, for which the optimal solution can be expressed as $P_w^{(\lambda)}(v)=0$ and the corresponding function objective value for (A4) can be calculated as $X(v)-\lambda P_w^{(\lambda)}\left(v\right)=1$.

Case 5. When $\alpha(v)<0,\beta(v)<0$, and $P_w(v)\geqslant\frac{\beta(v)}{\alpha(v)}$, it implies that $X(v)=1$, for which the optimal solution can be expressed as $P_w^{(\lambda)}(v)=\frac{B}{A}$ and the corresponding objective function value for (A4) can be calculated as $X(v)-\lambda P_w^{(\lambda)}\left(v\right)=1-\frac{\lambda\beta(v)}{\alpha(v)}$.

Case 6. When $\alpha(v)<0,\beta(v)<0$, and $0\leqslant P_w\leqslant\frac{\beta(v)}{\alpha(v)}$, it implies that $X(v)=0$, for which the optimal solution can be expressed as $P_w^{(\lambda)}(v)=0$ and the corresponding objective function value for (A4) can be calculated as $X(v)-\lambda P_w^{(\lambda)}\left(v\right)=0$.

Comparing the objective function value under Cases 5 and 6, it can be concluded that when $\frac{\alpha(v)}{\beta(v)} > \lambda$, the optimal solution can be expressed as $P_w^{(\lambda)}(v) = \frac{\beta(v)}{\alpha(v)}$, otherwise the optimal solution can be expressed as $P_w^{(\lambda)}(v) = 0$.

By summarizing the above six cases, the optimal solution to the problem (A3) is given as

$$P_w^{(\lambda)}(v) = \begin{cases} \frac{\beta(v)}{\alpha(v)}, & 0 < \frac{\alpha(v)}{\beta(v)} < \lambda, \alpha(v) < 0, \\ 0, & \text{otherwise}, \end{cases} \tag{A5}$$

and the dual function $f(\lambda)$ in (A3) can be obtained with (A5).

Next, the dual problem (D1) can be solved by bisection method since the subgradient of $f(\lambda)$ is indeed $s(\lambda) = P_{\max} - \mathbb{E}_v[P_w^{(\lambda)}(v)]$ under any given $\lambda \geqslant 0$. In fact, $\mathbb{E}_v[P_w^{(\lambda)}(v)] \to \infty$ when $\lambda \to 0$, and $\mathbb{E}_v[P_w^{(\lambda)}(v)] \to 0$ when $\lambda \to \infty$. Thus, λ^* is set such that $s(\lambda^*) = 0$ numerically, and the solution for (P1) can be obtained by substituting the optimal dual variable λ^* into (A5).

Overall, Theorem 1 is proven completely.

Appendix B Proof of Theorem 2

The first-order derivative of $P_{\text{out}}^S(P_w)$ with respect to P_w can be derived as

$$\frac{\mathrm{d}P_{\text{out}}^S(P_w)}{\mathrm{d}P_w} = \frac{P_w\varphi\lambda_{aw}\left(\kappa\varepsilon\sigma_w^2\lambda_{ab}\lambda_{wb} - \kappa\varphi\varepsilon\sigma_b^2\lambda_{ab} - \sigma_b^2\lambda_{aw}\lambda_{wb}\right) + \sigma_w^2\lambda_{aw}\left(\kappa\varepsilon\sigma_w^2\lambda_{ab}\lambda_{wb} - \kappa\varphi\varepsilon\sigma_b^2\lambda_{ab}\right)}{\left(\varphi P_w + \sigma_w^2\right)\left(P_w\left(\kappa\varphi\varepsilon\lambda_{ab} + \lambda_{aw}\lambda_{wb}\right) + \kappa\varepsilon\sigma_w^2\lambda_{ab}\right)^2} \mathrm{e}^{-\frac{\lambda_{aw}\sigma_b^2}{\kappa\varepsilon(P_w\varphi\lambda_{ab} + \varepsilon\sigma_w^2\lambda_{ab})}}. \tag{B1}$$

From (B1), the following three results can be obtained.

When $\sigma_w^2\lambda_{wb} - \varphi\sigma_b^2 \leqslant 0$, the first-order derivative $\frac{\mathrm{d}P_{\text{out}}^S(P_w)}{\mathrm{d}P_w} \leqslant 0$ holds for $P_w \in [0, \infty)$. Thus, when $\frac{\sigma_w^2}{\sigma_b^2} \leqslant \frac{\varphi}{\lambda_{wb}}$, the outage probability decreases with the jamming power, resulting in the optimal jamming power $P_w^* = 0$.

When $\kappa\varepsilon\sigma_w^2\lambda_{ab}\lambda_{wb} - \kappa\varphi\varepsilon\sigma_b^2\lambda_{ab} - \sigma_b^2\lambda_{aw}\lambda_{wb} > 0$, the first-order derivative $\frac{\mathrm{d}P_{\text{out}}^S(P_w)}{\mathrm{d}P_w} > 0$ holds for $P_w \in [0, \infty)$. Thus, when $\frac{\varphi}{\lambda_{wb}} < \frac{\sigma_w^2}{\sigma_b^2} - \frac{\lambda_{aw}}{\kappa\varepsilon\lambda_{ab}}$, the outage probability increases with the jamming power, resulting in the optimal jamming power $P_w^* = P_{\max}$.

When $\sigma_w^2\lambda_{wb} - \varphi\sigma_b^2 > 0$ and $\kappa\varepsilon\sigma_w^2\lambda_{ab}\lambda_{wb} - \kappa\varphi\varepsilon\sigma_b^2\lambda_{ab} - \sigma_b^2\lambda_{aw}\lambda_{wb} \leqslant 0$, the first-order derivative $\frac{\mathrm{d}P_{\text{out}}^S(P_w)}{\mathrm{d}P_w} > 0$ holds for $P_w \in [0, P_r)$ with $P_r = \frac{\kappa\varepsilon\lambda_{ab}\sigma_w^2(\varphi\sigma_b^2 - \sigma_w^2\lambda_{wb})}{\varphi(\kappa\varepsilon\sigma_w^2\lambda_{ab}\lambda_{wb} - \kappa\varphi\varepsilon\sigma_b^2\lambda_{ab} - \sigma_b^2\lambda_{aw}\lambda_{wb})}$. Besides, the first-order derivative $\frac{\mathrm{d}P_{\text{out}}^S(P_w)}{\mathrm{d}P_w} \geqslant 0$ holds for $P_w \in [P_r, \infty)$. Thus, the outage probability increases with the jamming power P_w on the interval $[0, P_r]$, resulting in the optimal jamming power $P_w^* = \min\{P_{\max}, P_r\}$.

Overall, Theorem 2 is proven completely.