Integrated Full-Duplex Detection and Jamming for Adversarial Communication Throughput Minimization

Yangfan Xu, Bao Gui
School of Computer and Information Engineering, Chuzhou University, Chuzhou, 239000 China.

This paper investigates the integrated full-duplex detection and jamming for minimizing the adversarial communication throughput in wireless systems. In a hostile military scenario consisting of an adversary transmitter (Alice), an adversary receiver (Bob), and a friendly full-duplex warden (Willie), where warden aims to simultaneously detect the presence of adversary transmissions via energy detection and interfere with their communication by transmitting artificial noise (AN). To address the inherent trade-off between detection performance degradation caused by self-interference and jamming capability, we propose a power control strategy to minimize the adversary's throughput subject to detection capability and maximum power constraints. Specifically, we derive an upper bound on the detection error probability to quantify detection performance and establish a detection requirement constraint. Subsequently, an optimization problem is formulated to minimize the communication throughput. By analyzing the monotonicity of the objective and constraint functions, the optimal AN transmit power is determined. Numerical results demonstrate the trade-off between jamming capability and detection reliability, revealing that the achievable minimum throughput is critically constrained by the detection requirement and the maximum AN power. This work provides significant insights into the development of secure communication and counter-measure strategies.

***Index Terms*—Full-duplex, signal detection, jamming, throughput minimization, power control.**

I. Introduction

With the rapid advancement of wireless communication technology, signal sensing serves as a critical component of communication systems, performing essential tasks such as spectrum resource management, interference identification, and security defense [1], [2]. The core objective of a detector is to accurately determine the presence of target signals within complex electromagnetic environments, which directly impacts the reliability of communication systems and the level of information security defense [3], [4]. Within traditional detection frameworks, energy detection has emerged as the optimal method for detecting the presence of unknown signals due to its independence from signal prior information, low computational complexity, and theoretical optimality [5], [6]. This approach is particularly suitable for the military adversarial scenario, where the warden lacks any a prior information and requires low-complexity detection method. Therefore, this approach is widely applied in scenarios such as cognitive radio, Internet of Things (IoT) device monitoring, and wireless environment surveillance [7], [8]. For instance, in cognitive radio networks, secondary users employ energy detection to sense primary user signals and avoid interference, with its performance directly determining spectrum sharing effectiveness [9]. In IoT scenarios involving massive device access, low-power devices rely on the efficiency of energy detection to minimize computational costs [10].

However, with the development of communication technology, detectors face unprecedented technical challenges. One challenge comes from the widespread adoption of low-power communication technologies, which leads to high detection error probability due to low signal-to-noise ratios in detection channels [11]. For example, in industrial IoT, sensors employ power control techniques to extend device battery life, reducing signal power to levels near or even below the noise.

Additionally, the emergence of covert communication technologies poses a fundamental challenge to detection theory [12]. Covert communication ensures that the probability for a detector to detect communication between two legitimate users is negligible, thereby hiding the transmission itself [13]. The work in [14] jointly optimizes the flying location and transmit power for an unmanned aerial vehicle (UAV) conducting covert operations in military surveillance scenario. The work in [15] investigates covert communication in multi-relay IoT systems with multiple energy harvesting jammers with a harvesting-then-jamming protocol and proposes the relay and jammer selection strategy. The work in [16] proposes an energy-efficient covert offloading scheme for blockchain-enabled IoT, enabling sensors to upload tasks undetected by attackers while ensuring the effectiveness of paid computation offloading. The work in [17] employs covert communication to transmit privacy-sensitive data over device-to-device communication links, thereby reducing the probability of detection. Consequently, covert communication, as an emerging information security technology, has been extensively studied in scenarios like military anti-interception communications and privacy-sensitive data transmission [18], [19]. Therefore, from the detector's perspective, analyzing and enhancing detection performance holds significant importance.

Existing covert communication studies focus on improving the covertness of legitimate communications by reducing adversary detection probability, while few address the reverse demand of friendly real-time detection and jamming for adversarial communications. We adopt a full-duplex warden to realize simultaneous detection and jamming and balance the inherent self-interference trade-off.

This paper considers a practical application in military scenarios involving the detection and jamming of enemy

Manuscript received December 25, 2025; revised March 29, 2026. Corresponding author: Bao Gui (email: guibao1@163.com).

communications, where friendly units detect whether the adversary is communicating and transmit artificial noise to jam communications. Specifically, a full-duplex detector detects communication activity and transmits artificial noise to jam communications, minimizing the adversary's communication throughput. Considering that both communication detection and jamming play critical roles in military operations, a single unit must simultaneously perform both tasks. For the full-duplex detector, transmitting artificial noise creates self-interference, thereby reducing the detection probability of enemy communications. This implies a trade-off between detection and jamming capabilities, necessitating a balance between detection and jamming. Consequently, researching methods for a full-duplex detector to detect and jam legitimate communications holds significant importance. To balance jamming capability and detection reliability, we propose a power control scheme that maximizes jamming performance by optimizing the artificial noise power while maintaining the required detection reliability by imposing strict constraints on the detection capability, thereby addressing the trade-off.

In this paper, based on the above scenario, we analyze the detector's capability to detect communications and establish detection requirement constraints to ensure a certain level of detection capability. Furthermore, we optimize the transmit power of the detector's artificial noise to minimize the adversary's communication throughput. By constraining the detection capability and power control of the full-duplex detector, we can interfere with communications as much as possible while maintaining detection capability.

The rest of this paper is organized as follows: Section II details the system model. Section III presents the optimization problem and solves it. Section IV shows numerical results. Finally, section V concludes this paper.

II. System Model

As shown in Fig. 1, we consider a wireless communication scenario consisting of an adversarial signal transmitter Alice, an adversarial receiver Bob, and a friendly detector Willie. In this system model, Alice communicates with Bob while Willie simultaneously detects Alice's transmission signals and generates artificial noise to jam the communication. Alice and Bob each have one antenna, while Willie has two antennas for transmission and reception. This wireless communication system includes three channel links—the communication link from Alice to Bob, the detection link from Alice to Willie, and the jamming link from Willie to Bob. All three channel links are modeled as additive white Gaussian noise (AWGN) channels. The communication system uses a finite number of channels, with the communication block length set to N for all three channel links.

A. Detection Performance

To obtain the detection error probability of detector Willie for analyzing detection performance, we first present the received

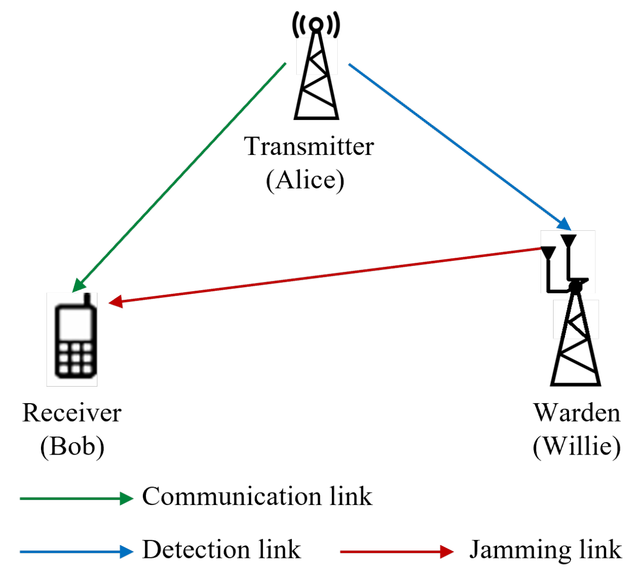

Fig. 1. Illustration of wireless communication scenario

signal at the i-th channel used by detector Willie as

$$y_w[i] = \begin{cases} \sqrt{\rho P_w} x_w[i] + n_w[i], & H_0 \\ \sqrt{P_a} x_a[i] + \sqrt{\rho P_w} x_w[i] + n_w[i], & H_1 \end{cases} \quad (1)$$

where H_0 denotes that Alice does not transmit a signal, H_1 denotes that Alice transmits a signal, ρ is Willie's self-interference coefficient, P_w is the transmission power of Willie's artificial noise, $x_w[i] \sim \mathcal{CN}(0,1)$ is Willie's transmission signal, $n_w[i] \sim \mathcal{CN}(0,\sigma_w^2)$ is the complex Gaussian noise at Willie's location, σ_w^2 is the noise power at Willie's location, P_a is the fixed transmit power of Alice's communication signal, and $x_a[i] \sim \mathcal{CN}(0,1)$ is Alice's transmission signal.

Assuming hypotheses H_0 and H_1 have equal prior probabilities, Willie makes a binary decision, denoted as D_0 and D_1, to determine whether Alice is engaged in transmission behavior. This is a standard and reasonable assumption for adversarial wireless communication detection scenarios where the warden has no a priori statistical information about the adversary's transmission activity. Therefore, Willie's detection error probability ξ is defined as

$$\xi = P_{\text{FA}} + P_{\text{MD}} = \Pr\{D_1 | H_0\} + \Pr\{D_0 | H_1\}, \quad (2)$$

where $\Pr\{D_1 | H_0\}$ is Willie's false alarm probability, and $\Pr\{D_0 | H_1\}$ is Willie's miss detection probability.

Willie's optimal energy detection is a likelihood ratio detection, whose detection strategy is given by

$$\frac{\mathbb{P}_1 \triangleq \prod_{i=1}^{N} f(y_w[i] \mid H_1)}{\mathbb{P}_0 \triangleq \prod_{i=1}^{N} f(y_w[i] \mid H_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} 1, \quad (3)$$

where $\mathbb{P}_0$ and $\mathbb{P}_1$ denote the likelihood functions of the received signal under the H_0 and H_1 hypotheses, respectively, and $f(y_w[i] \mid H_0)$ and $f(y_w[i] \mid H_1)$ denote the probability density functions of the received signal under the H_0 and H_1

hypotheses, respectively. Based on equation (1), $f(y_w[i] \mid H_0)$ and $f(y_w[i] \mid H_1)$ can be expressed as

$$f(y_w[i] \mid H_0) = \mathcal{CN}(0, \rho P_w + \sigma_w^2), \tag{4}$$

$$f(y_w[i] \mid H_1) = \mathcal{CN}(0, P_a + \rho P_w + \sigma_w^2). \tag{5}$$

According to the likelihood ratio test conducted by Willie, its detection error probability can be further expressed as

$$\xi = 1 - \mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1), \tag{6}$$

where $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$ denotes the total deviation distance between $\mathbb{P}_0$ and $\mathbb{P}_1$. Based on the relationship between total deviation distance and Hellinger distance, the following inequality holds:

$$\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \geq H^2(\mathbb{P}_0, \mathbb{P}_1), \tag{7}$$

where $H^2(\mathbb{P}_0, \mathbb{P}_1)$ is the square of the Hellinger distance between $\mathbb{P}_0$ and $\mathbb{P}_1$. Based on the definition of the Hellinger distance and Equations (3), (4), and (5), $H^2(\mathbb{P}_0, \mathbb{P}_1)$ can be derived as

$$\begin{aligned}
&H^2(\mathbb{P}_0, \mathbb{P}_1) \\
&= 1 - \int_{\mathcal{X}} \sqrt{\prod_{i=1}^{N} f(y_w[i] \mid H_0) \prod_{i=1}^{N} f(y_w[i] \mid H_1) dx} \\
&= 1 - \int_{\mathcal{X}} \sqrt{\left[\frac{1}{\pi^2(\rho P_w + \sigma_w^2)(P_a + \rho P_w + \sigma_w^2)}\right]^N} \\
&\times \sqrt{\exp\left(\prod_{i=1}^{N} |x|^2 \left(-\frac{1}{\rho P_w + \sigma_w^2} - \frac{1}{P_a + \rho P_w + \sigma_w^2}\right)\right)} dx \\
&= 1 - \left[\int_{\mathcal{X}} \frac{\exp\left(-\frac{|x|^2}{2}\left(\frac{1}{\rho P_w + \sigma_w^2} + \frac{1}{P_a + \rho P_w + \sigma_w^2}\right)\right)}{\pi\sqrt{(\rho P_w + \sigma_w^2)(P_a + \rho P_w + \sigma_w^2)}} dx\right]^N \\
&= 1 - \left[\frac{1}{\pi\sqrt{(\rho P_w + \sigma_w^2)(P_a + \rho P_w + \sigma_w^2)}}\right. \\
&\quad \left. \times \frac{2\pi(\rho P_w + \sigma_w^2)(P_a + \rho P_w + \sigma_w^2)}{P_a + 2\rho P_w + 2\sigma_w^2}\right]^N \\
&= 1 - \left[\frac{2\sqrt{(\rho P_w + \sigma_w^2)(P_a + \rho P_w + \sigma_w^2)}}{P_a + 2\rho P_w + 2\sigma_w^2}\right]^N,
\end{aligned} \tag{8}$$

where $\mathcal{X}$ is the support set of $f(y_w[i] \mid H_0)$ and $f(y_w[i] \mid H_1)$. Substituting (7) into (6) , we obtain an upper bound for the detection error probability, which is given by

$$\xi = 1 - \mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \leq 1 - H^2(\mathbb{P}_0, \mathbb{P}_1). \tag{9}$$

We define $T = 1 - H^2(\mathbb{P}_0, \mathbb{P}_1)$ to represent Willie's detection metric, where a smaller T indicates a lower detection error probability and stronger detection capability. Setting T to be less than a small fixed threshold value ε means Willie's detection error probability will not exceed this threshold, representing the detection requirement. Thus, the detection requirement constraint is obtained by

$$\begin{aligned}
T &= 1 - H^2(\mathbb{P}_0, \mathbb{P}_1) \\
&= \left[\frac{2\sqrt{(\rho P_w + \sigma_w^2)(P_a + \rho P_w \sigma_w^2 + \sigma_w^2)}}{P_a + 2\rho P_w + 2\sigma_w^2}\right]^N \leq \varepsilon.
\end{aligned} \tag{10}$$

B. Communication Throughput

To determine the communication throughput from Alice to Bob as a measure of communication performance, we first define the signal-to interference-plus-noise ratio (SINR) at Bob as

$$\gamma_b = \frac{P_a}{\rho P_w + \sigma_b^2}, \tag{11}$$

where σ_b^2 is the noise power of the complex Gaussian noise at Bob. For finite block-length communications, the decoding error probability cannot be neglected. When the transmission rate R and block length N of the communication from Alice to Bob are fixed, the decoding error probability δ can be approximated by

$$\delta \approx Q\left(\frac{\sqrt{N}(1+\gamma_b)\left(\ln(1+\gamma_b) - R\ln 2\right)}{\sqrt{\gamma_b(\gamma_b+2)}}\right), \tag{12}$$

where $Q(\cdot)$ is the Q-function, also known as the right-tail function of the standard normal distribution, defined as $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) dt$. Therefore, the communication throughput η is given by

$$\begin{aligned}
\eta &= NR(1-\delta) \\
&= NR\left[1 - Q\left(\frac{\sqrt{N}(1+\gamma_b)\left(\ln(1+\gamma_b) - R\ln 2\right)}{\sqrt{\gamma_b(\gamma_b+2)}}\right)\right].
\end{aligned} \tag{13}$$

Communication throughput represents the number of bits that wireless communication can effectively transmit. To achieve throughput minimization under Willie jamming, throughput is adopted as the performance metric for communication.

III. Communication Throughput Minimization

Our objective is to minimize communication throughput while ensuring Willie's detection capability.

A. Optimization Problem Formulation

Minimizing throughput under Willie's jamming is formulated as an optimization problem constrained by detection requirement and artificial noise transmit power, which is described as

$$\begin{aligned}
\min_{P_w} \quad & \eta \\
\text{s.t.} \quad & P_w \leq P_{\max}, & \text{(14a)} \\
& T \leq \varepsilon, & \text{(14b)}
\end{aligned}$$

where $P_w \leq P_{\max}$ is the maximum transmit power constraint for artificial noise, $P_{\max}$ is the maximum transmit power of artificial noise. $T \leq \varepsilon$ is the detection requirement constraint, and ε is the detection requirement reflecting the level of detection capability.

B. Solution of the Optimization Problem

To solve the optimization equation, it is necessary to analyze the monotonicity of the objective and constraint functions. First, we analyze the monotonicity of communication throughput with respect to the transmit power of Willie's artificial noise P_w. Expressing the integer term within the brackets of the Q function in (13) as ζ, the first derivative of communication throughput η with respect to the SINR at Bob is given by

$$\frac{\partial \eta}{\partial \gamma_b} = NR \frac{1}{\sqrt{2\pi}} e^{-\frac{\zeta^2}{2}} \frac{\partial \zeta}{\partial \gamma_b}, \tag{15}$$

where $\frac{\partial \zeta}{\partial \gamma_b}$ is the first derivative of ζ with respect to γ_b, which given by

$$\frac{\partial \zeta}{\partial \gamma_b} = \frac{\sqrt{N}\left[\gamma_b^2 + 2\gamma_b + R\ln 2 - \ln(1+\gamma_b)\right]}{\left[\gamma_b(2+\gamma_b)\right]^{3/2}}. \tag{16}$$

Note that $\frac{\partial\left(\gamma_b^2+2\gamma_b-\ln(1+\gamma_b)\right)}{\partial \gamma_b} = \frac{2\gamma_b^2+4\gamma_b+1}{1+\gamma_b} > 0$ and $\gamma_b^2 + 2\gamma_b - \ln(1+\gamma_b)|_{\gamma_b=0} = 0$, we have $\frac{\partial \zeta}{\partial \gamma_b} > 0$. Substituting into Equation (15) yields $\frac{\partial \eta}{\partial \gamma_b} > 0$, indicating that the communication throughput η monotonically increases with the SINR at Bob. Furthermore, according to (11), the SINR at Bob is a monotonically decreasing function of the transmit power of Willie's artificial noise. Therefore, the communication throughput η monotonically decreases as the transmit power of Willie's artificial noise P_w increases.

Next, we analyze the monotonicity of the detection metric T with respect to the transmit power of Willie's artificial noise P_w. According to (10), the monotonicity of the detection metric T with respect to the transmit power of Willie's artificial noise P_w is identical to $T^{2/N}$ with respect to P_w. The derivative of $T^{2/N}$ with respect to the transmit power of Willie's artificial noise P_w is given by

$$\frac{\partial T^{2/N}}{\partial P_w} = \frac{4{P_a}^2}{\left(P_a + 2\rho P_w + 2\sigma_w^2\right)^3} > 0. \tag{17}$$

Therefore, the detection metric T increases monotonically as the transmit power of Willie's artificial noise P_w increases.

Based on the fact that, as the transmit power of Willie's artificial noise P_w increases, communication throughput η monotonically decreases, while detection metric T monotonically increases. Therefore, the optimal transmit power of Willie's artificial noise, denoted as P_w^*, should be the minimum value between the upper bound of transmit power determined by the maximum transmit power constraint and the detection requirement constraint. P_w^* can be expressed as

$$P_w^* = \min\left\{P_{\max}, P_w^{\varepsilon}\right\}, \tag{18}$$

where P_w^{ε} is the root of the equation $T = 1 - H^2(\mathbb{P}_0, \mathbb{P}_1) = \varepsilon$. Solving the equation yields the analytical solution, which is given by

$$P_w^{\varepsilon} = \frac{1}{\rho}\left(-\frac{P_a}{2} + \frac{P_a}{2\sqrt{1-\varepsilon^{2/N}}} - \sigma_w^2\right). \tag{19}$$

Substituting the optimal transmit power of Willie's artificial noise P_w^{ε} into (11) yields the optimal SINR at Bob γ_b^*. Substituting γ_b^* into (13) then yields the minimum communication throughput η^*, thereby solving the optimization problem. The optimal SINR at Bob γ_b^* and the minimum communication throughput η^* are specifically expressed by

$$\gamma_b^* = \frac{P_a}{\rho \min\left\{P_{\max}, P_w^{\varepsilon}\right\} + \sigma_b^2}, \tag{20}$$

$$\eta^* = NR\left[1 - Q\left(\frac{\sqrt{N}(1+\gamma_b^*)\left(\ln(1+\gamma_b^*) - R\ln 2\right)}{\sqrt{\gamma_b^*(\gamma_b^*+2)}}\right)\right]. \tag{21}$$

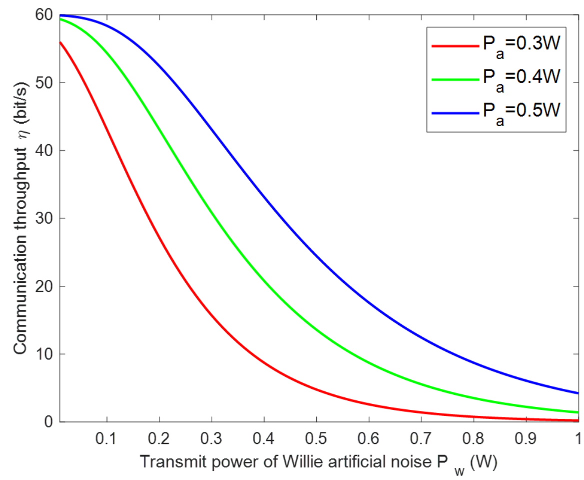

Fig. 2. The communication throughput η versus the transmit power of Willie's artificial noise P_w under different transmit power of Alice's communication signal P_a.

IV. Numerical Results

In this section, numerical results are provided to demonstrate Willie's jamming and detection performance. Unless otherwise specified, system parameters are set as: $\rho = 0.05$, $\sigma_b^2 = \sigma_w^2 = 0.2$W, $N = 20$, $P_{\max} = 1$W, $\varepsilon = 0.1$, and $R = 3$ bits/s.

In Fig.2, we illustrate how communication throughput η varies with the transmission power of Willie's artificial noise P_w at different Alice transmission power P_a. From Fig. 2, we observe that as the transmit power of Willie's artificial noise P_w increases, communication throughput η decreases accordingly. This is because a higher P_w indicates Willie's stronger jamming ability for communications, thereby reducing communication throughput. Moreover, it can be observed that as transmit power of Alice's communication signal P_a increases, the communication throughput η also increases. This is because the greater P_a means Alice can send more signals, thereby increasing the communication throughput.

In Fig. 3, we show the change in detection metric T with the transmit power of Willie's artificial noise P_w at different Alice's transmit powers. From Fig. 3, we observe that as the transmit power of Willie's artificial noise P_w increases, the detection metric T also increases. Note that the larger T correspond to the weaker detection capability, and thus as P_w increases, the corresponding detection capability weakens. This is because

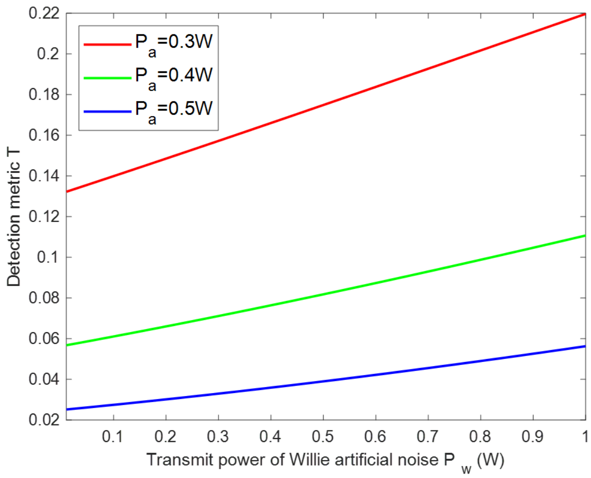

Fig. 3. The detection metric T versus the transmit power of Willie's artificial noise P_w under different transmit power of Alice's communication signal P_a.

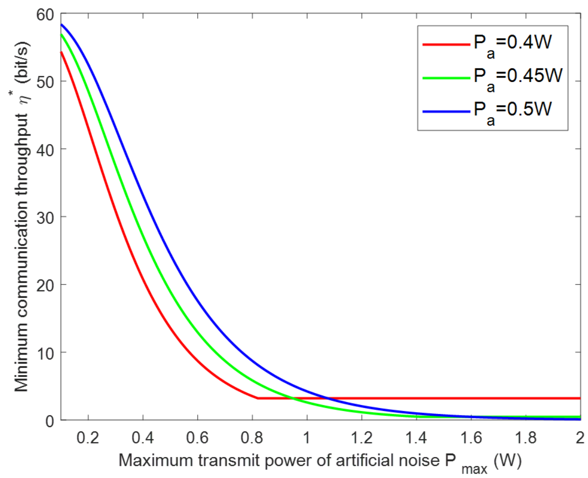

Fig. 5. The minimum communication throughput η^* versus the maximum transmit power of artificial noise $P_{\max}$ under different transmit power of Alice's communication signal P_a.

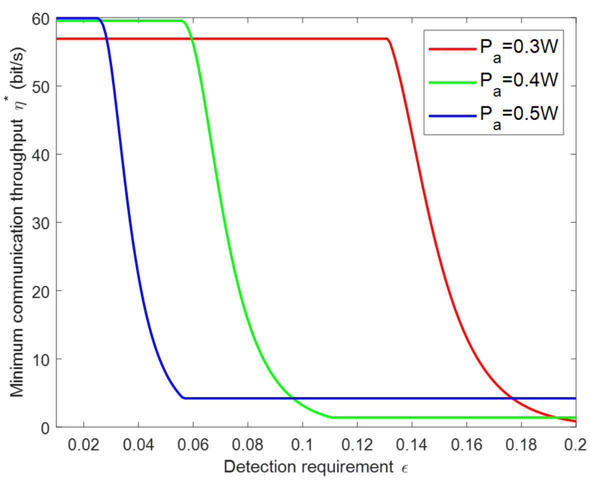

Fig. 4. The minimum communication throughput η^* versus the detection requirement ε under different transmit power of Alice's communication signal P_a.

a larger P_w indicates stronger self-interference from Willie, increasing its own detection error probability and consequently reducing detection capability. Additionally, we observe that as Alice's transmit power P_a increases, the detection metric T decreases. This is because the greater P_a means Alice transmits more signals, making the communication easier to detect. By combining Fig. 2 and 3 for analysis, it can be observed that for full-duplex detector Willie, there exists a trade-off between jamming capability and detection capability.

In Fig 4, we illustrate the variation of minimum communication throughput η^* with the detection requirement ε under different transmit power of Alice's communication signal P_a. It can be observed that as ε increases, the minimum communication throughput η^* initially remains constant, then decreases, and finally stabilizes at a fixed value. The reason behind this is as following. As ε increases, detection capability requirements gradually relax. When ε is relatively small, the detection constraint $T \leq \varepsilon$ is overly stringent, making the optimization problem infeasible, i.e., no feasible artificial noise transmit power exists to satisfy this constraint, meaning there is no valid power allocation for Willie to meet the strict detection requirement. With ε increases, the relaxation of detection requirement allows Willie to transmit artificial noise at the minimum feasible power to interfere with communication. In this case, the optimal transmit power for Willie's artificial noise P_w^* is P_w^ε in (18), where P_w^ε increases with increasing ε. Meanwhile, communication throughput is a monotonically decreasing function of the transmit power of Willie's artificial noise, leading to a decrease in the minimum communication throughput η^*. When ε further increases, the optimal transmit power of Willie's artificial noise P_w^* is a constant value $P_{\max}$ in (18). Consequently, the minimum communication throughput η^* remains unchanged. Additionally, it can be observed that as Alice's transmit power P_a increases, the corresponding ε for the same minimum communication throughput η^* decreases. This occurs because a larger P_a makes communication easier to detect, meaning that relatively stricter detection capability requirement can be satisfied at relatively larger P_a.

In Fig. 5, we show the minimum communication throughput η^* versus the maximum transmit power of artificial noise $P_{\max}$ for different Alice's transmit power P_a. It can be observed that as $P_{\max}$ increases, the minimum communication throughput η^* first decreases and then remains constant. This is because when $P_{\max}$ is relatively small, the optimal transmit power of Willie 's artificial noise P_w^* is $P_{\max}$, so the minimum communication throughput η^* decreases as η^* increases. When $P_{\max}$ increases to exceed P_w^ε, the optimal transmit power of Willie's artificial noise remains fixed at P_w^ε, causing the minimum communication throughput η^* to stabilize. Additionally, it is evident that as Alice's transmit power P_a increases, the corresponding $P_{\max}$ required to achieve the same minimum communication throughput η^* also increases. This is because a higher P_a allows Willie to generate artificial noise at greater power to interfere with communication, which implies that as P_a increases, the strength of the jamming must also be enhanced. Moreover, a notable performance crossover can be noted, i.e., the smaller P_a (e.g., 0.4 W) has the lowest η^* at small $P_{\max}$ but the highest η^* at large $P_{\max}$. This is because the performance crossover is driven by the regime shift of the optimization problem from power-constrained to detection-constrained as $P_{\max}$ increases, which flips the optimal transmit power of Willie 's artificial noise determining η^* from $P_{\max}$ to P_w^{ε}.

V. Conclusion

In this paper, we have investigated the integrated detection and jamming full-duplex warden in wireless communication systems. This full-duplex warden employed energy detection to identify covert communications and transmitted artificial noise to jam communications, addressing the challenge of communication detection and countermeasures in high-level data security and data privacy scenarios. Specifically, it achieved communication throughput minimization by optimizing the transmit power of artificial noise under detection requirement constraint and maximum artificial noise transmit power constraint. By proposing throughput minimization and analyzing the monotonicity of the objective and constraint functions, the optimal artificial noise transmit power was determined to minimize communication throughput. Through numerical results, we showed the jamming and detection performance of warden. This paper provides an effective proactive detection and countermeasure approach for scenarios with stringent requirements for data security and protection, such as preventing potential IoT information leaks and safeguarding privacy in industrial internet environments.

An important direction for future research is to extend the proposed framework to practical wireless fading channel scenarios (e.g., Rayleigh or Rician fading), where the channel gain randomness will be incorporated to further improve the practicality and applicability of the full-duplex detection and jamming scheme.

References

[1] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[2] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, First quarter 2009.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[4] 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, Oct. 2019.

[5] H. Urkowitz, “Energy detection of unknown deterministic signals,” *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[6] S. P. Herath, N. Rajatheva, and C. Tellambura, “Energy detection of unknown signals in fading and diversity reception,” *IEEE Transactions on Communications*, vol. 59, no. 9, pp. 2443–2453, Sep. 2011.

[7] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, “Spectrum sensing for cognitive radio : State-of-the-art and recent advances,” *IEEE Signal Processing Magazine*, vol. 29, no. 3, pp. 101–116, May 2012.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourth quarter 2015.

[9] Y.-C. Liang, Y. Zeng, E. C. Peh, and A. T. Hoang, “Sensing-throughput tradeoff for cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[10] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, “Massive non-orthogonal multiple access for cellular IoT: Potentials and limitations,” *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, Sep. 2017.

[11] U. Raza, P. Kulkarni, and M. Sooriyabandara, “Low power wide area networks: An overview,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 855–873, Second quarter 2017.

[12] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, “Covert communications: A comprehensive survey,” *IEEE Communications Surveys Tutorials*, vol. 25, no. 2, pp. 1173–1198, Second quarter 2023.

[13] 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, Sep. 2013.

[14] S. Yan, S. V. Hanly, and I. B. Collings, “Optimal transmit power and flying location for UAV covert wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 11, pp. 3321–3333, Nov. 2021.

[15] H. Lv, B. Yang, X. Sun, C. Gao, B. Gui, and T. Taleb, “Energy-harvesting jammer-aided covert communications in wireless multirelay IoT systems,” *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 17 443–17 455, Jun. 2025.

[16] Y. Jiang, Y. Wang, H. Wu, Y. Liu, and L. Hu, “Energy-efficient covert offloading in blockchain-enabled IoT: Joint artificial noise and computation resource allocation,” *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 6889–6901, Mar. 2025.

[17] Y. Jiang, L. Wang, H. Zhao, and H.-H. Chen, “Covert communications in D2D underlaying cellular networks with power domain NOMA,” *IEEE Systems Journal*, vol. 14, no. 3, pp. 3717–3728, Sep. 2020.

[18] Y. Jiang, L. Wang, H.-H. Chen, and X. Shen, “Physical layer covert communication in B5G wireless networks—its research, applications, and challenges,” *Proceedings of the IEEE*, vol. 112, no. 1, pp. 47–82, Jan. 2024.

[19] Y. Zhang, L. Yang, X. Li, K. Guo, and H. Liu, “Covert communications for STAR-RIS-assisted industrial networks with a full duplex receiver and RSMA,” *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 22 483–22 493, Jun. 2024.