Reflection Optimization for Covert Ambient Backscatter Systems Under Two Jamming Patterns

Yuanai Xie, *Member, IEEE,* Yaoyao Wen, Xiao Zhang, Pan Lai, Zhixin Liu, *Senior Member, IEEE,* Haoyuan Pan, *Member, IEEE,* and Tse-Tin Chan, *Member, IEEE*

***Abstract*—Ambient backscatter communication (ABC) enables low-cost and energy-efficient connectivity for Internet of Things (IoT) devices by leveraging ambient radio-frequency (RF) signals. However, the passive nature and open wireless medium of ABC systems make them vulnerable to detection by unauthorized receivers (wardens). To mitigate this risk, covert communication, which conceals transmissions by embedding them within noise, offers a promising security enhancement for ABC systems. This paper proposes a jammer-assisted reflection coefficient optimization framework to enhance the covertness and reliability of ABC systems with an endogenous warden and an external jammer. Specifically, we consider two distinct jamming patterns: uniformly distributed and truncated exponentially distributed artificial noise power. We derive closed-form expressions for both the outage probability of the backscatter link and the minimum detection error rate at the warden under these jamming patterns. Based on these expressions, we determine the optimal reflection coefficients that maximize the effective covert rate while satisfying a predefined covertness constraint. Additionally, we introduce the concept of jamming cost to evaluate the efficiency and applicability of different jamming patterns in terms of the required jamming power to achieve a desired level of covertness. Numerical results validate the effectiveness of the proposed optimization framework and reveal that while uniform jamming provides stronger covertness and lower jamming cost, truncated exponential jamming achieves a lower outage probability. These findings provide key insights for designing secure and efficient ABC systems across diverse IoT deployment scenarios.**

***Index Terms*—Ambient backscatter communication, artificial noise, covert communication, covert rate, jamming patterns, reflection coefficient optimization.**

I. Introduction

Ambient backscatter communication (ABC) is a promising technology for sustainable and energy-efficient Internet of Things (IoT) applications [1]. By leveraging ambient radio-frequency (RF) signals from sources such as cellular, TV, and Wi-Fi networks, ABC enables battery-free or energy-harvesting devices to communicate without dedicated transmitters [2]. This approach offers pervasive connectivity, minimal cost, and substantial energy savings, making it well-suited for various low-power IoT applications [3]. For instance, in smart homes, ABC allows devices such as temperature sensors, smart meters, and security systems to function with minimal power by reflecting existing RF signals [4]. In smart cities, ABC supports distributed sensor networks for real-time traffic and environmental monitoring, eliminating frequent battery replacements [5]. In healthcare, ABC facilitates energy-efficient communication for wearable and implantable medical devices, supporting continuous patient monitoring while reducing battery dependency and enabling miniaturization [6]. By leveraging ambient RF signals, ABC enhances the sustainability of IoT systems, making it a key innovation for next-generation wireless technologies.

In an ABC system consisting of an RF source, a battery-free tag, a legacy receiver (acting as an internal warden), and a backscatter receiver, the tag modulates its information onto ambient signals by varying its reflection coefficient, enabling passive communication with the backscatter receiver. While miniaturized tags enhance data interaction, their widespread deployment also introduces security risks, including man-in-the-middle attacks and communication disruptions. For example, in smart cities, compromised transportation data could threaten both personal and corporate assets. In smart healthcare, leaked location data and behavioral patterns from implanted devices could violate privacy. Since the internal warden shares the same frequency band and is often near the tag, it can easily detect backscatter transmissions, increasing the risk of eavesdropping and malicious attacks [7].

Conventional security measures, such as encryption and physical layer security (PLS) [8], are often unsuitable for these resource-constrained and passive devices due to their high computational and energy demands. Additionally, the effectiveness of PLS can be limited in environments with unpredictable or unfavorable channel conditions [9]. To address these challenges, covert communication, which hides backscatter transmissions within noise, has gained attention

This work was supported in part by the National Natural Science Foundation of China under Grants 62273298, 62371302, and 62403500, in part by the Hubei Provincial Natural Science Foundation under Grants 2023AFB202, 2024AFB842, and 2025AFB686, in part by the Fund for Academic Innovation Teams and Research Platform of South-Central Minzu University (Grant Number: XTZ24003), in part by Knowledge Innovation Program of Wuhan-Basic Research (Project No.: 2023010201010151), in part by the Research Start-up Funds of South-Central Minzu University under grants YZZ18006 and YZY23002, in part by the Spring Sunshine Program of Ministry of Education of the People's Republic of China under grant HZKY20220331, and in part by the Research Matching Grant Scheme from the Research Grants Council of Hong Kong. This article was presented in part at the IEEE Global Communications Conference, 2023. *(Corresponding author: Tse-Tin Chan.)*

Y. Xie, Y. Wen, X. Zhang, and P. Lai are with the School of Computer Science, South-Central Minzu University, Wuhan 430074, China (e-mail: 2023002@scuec.edu.cn; 2023120522@mail.scuec.edu.cn; xiao.zhang@my.cityu.edu.hk; plai1@ntu.edu.sg).

Z. Liu is with the School of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China (e-mail: lzxauto@ysu.edu.cn).

H. Pan is with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: hypan@szu.edu.cn).

T.-T. Chan is with the Department of Mathematics and Information Technology, The Education University of Hong Kong, Hong Kong SAR, China (e-mail: tsetinchan@eduhk.hk).

as a promising security solution for ABC systems.

Previous works have explored various techniques for covert communication, such as using artificial noise generated by full-duplex receivers [10], [11] or embedding artificial noise into carrier signals [12]. However, these approaches are often not feasible in ABC systems due to hardware complexity and energy constraints. To address this, this paper employs an external friendly jammer that emits artificial noise to enhance the covertness of backscatter communication. We consider two jamming patterns: the uniform distribution (previously discussed in [13]) and the truncated exponential distribution. These patterns represent different strategies for allocating the jammer's artificial noise power, which directly impacts both the covertness and reliability of the ABC system. In this paper, we formulate and analyze the covert rate maximization problem for the backscatter link under these two jamming patterns. Specifically, we optimize the tag's reflection coefficient for each pattern while ensuring compliance with the covertness constraint. In addition, we examine the effect of different jamming power distributions on system covertness and reliability. Finally, we compare the jamming costs associated with both jamming patterns, defined as the minimum required maximum jamming power needed to achieve a given covertness level. The main contributions of this paper are as follows:

- We consider a practical covert ABC scenario with an endogenous warden and an external friendly jammer. We formulate a reflection coefficient optimization problem for the tag to maximize the effective covert rate of the backscatter link under the covertness constraint and the two different jamming patterns (i.e., uniform and truncated exponential distributions).
- We derive closed-form expressions for the outage probability of the backscatter link and the warden's average minimum detection error rate under both jamming patterns, considering random channel fading and artificial noise randomness.
- We analyze the monotonicity of the effective covert rate and the warden's average minimum detection error rate with respect to the tag's reflection coefficient, leading to optimal reflection coefficient solutions under the two jamming patterns.
- We introduce the concept of jamming cost to evaluate the power efficiency of different jamming patterns, providing insights into the applicability of each pattern across various scenarios.

II. Related Work

A. Ambient Backscatter Communication (ABC)

ABC enables devices to transmit data by reflecting and modulating existing ambient RF signals instead of generating their own. The passive communication mechanism of ABC offers significant advantages, such as low power consumption and cost-effectiveness, but also introduces unique challenges in system design and performance optimization. One of the primary challenges in ABC systems is the non-deterministic and sporadic nature of ambient signals, which can adversely affect the reliability and throughput of the backscatter link [1].

Several studies have attempted to address this challenge from different perspectives. For example, Kishore *et al.* [14] proposed an opportunistic ABC framework for RF-powered cognitive radio networks, optimizing energy efficiency through analytical expressions for throughput and energy consumption. This approach blends opportunistic spectrum sensing, ambient backscattering, and harvest-then-transmit strategies to improve overall system efficiency. To enhance robustness in ABC systems, Zhang *et al.* [15] formulated a chance-constrained optimization problem to maximize the minimum user rate while considering imperfect channel state information (CSI). Their work addresses the uncertainty in channel conditions, which is critical for reliable communication. Ye *et al.* [16] derived outage probabilities for the primary and backscatter links, providing insights into system reliability under various conditions. In addition, Yang *et al.* [17] investigated cooperative ABC systems and designed a cooperative receiver capable of recovering information from both the RF source and the ambient backscatter device. Similarly, Zhao *et al.* [18] investigated cooperative ABC systems and derived ergodic sum capacity expressions for both primary and backscatter transmissions, accounting for sensitivity constraints at the tag.

B. Covert Communication for ABC

Covert communication aims to conceal the presence of transmissions from potential wardens or eavesdroppers by embedding them within noise, thereby enhancing communication security [7]. In the context of ABC systems, covert communication techniques can prevent the warden from detecting the tag's transmissions, addressing critical security concerns in open and shared frequency bands. Several studies have explored covert communication strategies for backscatter systems.

One prominent approach involves utilizing full-duplex receivers to emit artificial noise for covertness. For example, Hu *et al.* [10] were the first to study this aspect and examined its performance under fading channels. Similarly, Liu *et al.* [11] analyzed the feasible region of artificial noise power at the receiver based on the transmission power of the uncontrollable RF source and the reflection coefficient of the tag. They also derived the closed-form covert rate and expected detection error probability at the warden, revealing the existence of their tradeoff. W. Ma *et al.* [19] extended this approach by investigating covert communication in the presence of multiple randomly distributed wardens, analyzing the joint decoding performance of cooperative receivers. They utilized a full-duplex receiver to transmit variable-power interference signals and derived strong covertness constraints. While these studies provide important theoretical contributions, deploying full-duplex receivers to emit artificial noise in ABC systems may not always be feasible due to the high power consumption and complexity associated with full-duplex operation.

Another line of research focuses on the transmitter emitting artificial noise signals to confuse the warden. For instance, Shahzad *et al.* [20] proposed a covert monostatic backscatter system where the transmitter emits artificial noise signals with varying power. Wang *et al.* [12] introduced a covert communication framework for bistatic backscatter systems, employing dedicated carrier signals embedded with artificial noise to support the tag's backscatter communication. However, in resource-constrained ABC systems, requiring time-varying artificial noise from the RF source or embedding it within ambient signals is often impractical.

Recent research has also explored beamforming techniques to achieve covertness in ABC systems. Liu *et al.* [21] proposed a novel scheme in which covertness is attained by utilizing a multi-antenna tag rather than relying on artificial noise or a power-variable RF source.

C. Friendly Jamming in Covert Communication

Using an external friendly jammer to emit artificial noise provides an effective alternative to dedicated transmitters, receivers, or tags. For instance, Liu *et al.* [22] investigated secure communication with a wireless-powered friendly jammer, proposing a two-phase communication protocol where the jammer harvests energy from the source and then uses it to emit artificial noise. To further improve secrecy performance, Li *et al.* [23] proposed friendly jammer selection schemes in multiuser scheduling scenarios and derived their secrecy outage probability expressions. Furthermore, Qi *et al.* [24] considered maximizing cost-efficiency in friendly jamming and interference mitigation under users' transmission rate constraints.

Although friendly jamming has advanced covert communication, its application in ABC systems, particularly the joint effect of the tag's reflection coefficient and the jammer's artificial noise pattern, has been largely overlooked. This work addresses that gap by examining how two representative jamming power distributions, uniform and truncated exponential, enhance covert communication performance in ABC while considering the associated jamming costs. By optimizing the tag's reflection coefficient under these jamming patterns, our approach enables secure communication without requiring complex full-duplex hardware or modifications to the ambient RF source, making it well-suited for practical, resource-constrained IoT applications.

III. Problem Definition

A. System Model

As depicted in Fig. 1, we consider an ambient backscatter system, where an endogenous warden and an external friendly jammer are included. The tag aims to send information passively and covertly to the backscatter receiver by reflecting incident signals from the RF source and exploiting the jammer's artificial noise. Meanwhile, the warden with a radiometer attempts to detect this covert link for potentially malicious purposes. It is worth noting that all nodes in this system are equipped with a single antenna, and each time slot involves n channel uses. The channel gains are assumed to remain constant within each time slot and vary independently across different slots. The channel responses of the links are denoted as g_{sw} (source-warden), g_{st} (source-tag), g_{sr} (source-receiver), g_{jw} (jammer-warden), g_{jr} (jammer-receiver), h_{tw} (tag-warden), and h_{tr} (tag-receiver).

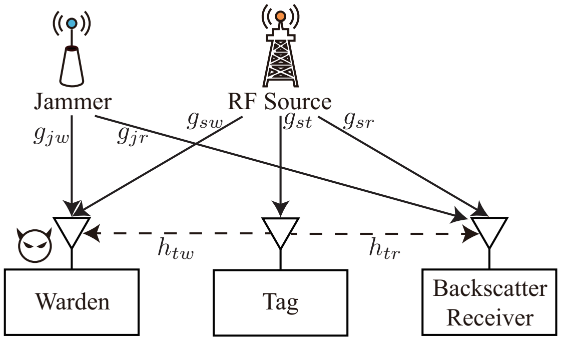


Fig. 1. Covert communication model for ambient backscatter systems.

Given the short range of the tag-receiver link and the unobstructed line-of-sight (LoS) path, h_{tr} is assumed to follow a Rician fading model dominated by a deterministic LoS component with an additional Rayleigh fading component. Following the worst-case scenario in [12], the warden is assumed to be close to the tag, and h_{tw} follows the same fading model. Consequently, the channel responses for both the tag-receiver and tag-warden links can be expressed as

$$h_{ij} = \sqrt{\frac{\kappa}{1+\kappa}} h_{ij}^{\mathrm{LoS}} + \sqrt{\frac{1}{1+\kappa}} h_{ij}^{\mathrm{NLoS}}, \tag{1}$$

where $ij \in \{tr, tw\}$, κ is the Rician factor, h_{ij}^{LoS} and h_{ij}^{NLoS} denote the deterministic LoS component and the Rayleigh fading component, respectively [25]. The Rician factor κ indicates the dominance of the deterministic LoS component over the random multipath component. A large κ corresponds to strong LoS dominance, making the channel conditions more predictable to the warden, thus representing the most challenging scenario for covert communication. In contrast to these links, we assume that the RF source and the jammer are relatively distant from other terminals, resulting in long-distance links with significant multipath effects. Therefore, g_{sw}, g_{st}, g_{sr}, g_{jw}, and g_{jr} are assumed to follow Rayleigh fading, with their average channel gains being $1/\lambda_{kl}$, where $kl \in \{sw, st, sr, jw, jr\}$ [12].

The backscatter signal reflected by the tag is $\mathbf{x}(i) = \sqrt{\alpha P} g_{st} \mathbf{e}(i) \mathbf{s}(i)$, where $i = 1, 2, \ldots, n$ denotes the index of each channel use, α represents the tag's reflection coefficient ($0 < \alpha \leq 1$), and P denotes the RF source's transmit power. The signal emitted by the RF source, $\mathbf{e}(i)$, satisfies $\mathbb{E}[\mathbf{e}(i)\mathbf{e}^*(i)] = 1$, and the signal modulated by the tag, $\mathbf{s}(i)$, satisfies $\mathbb{E}[\mathbf{s}(i)\mathbf{s}^*(i)] = 1$. The reflected jammer signal by the tag is considered negligible due to the weak and random nature of the jamming signal at the tag.

The received signal at the backscatter receiver is given by

$$\mathbf{y}_r(i) = h_{tr}\mathbf{x}(i) + \left(\sqrt{\phi_1 P} g_{sr} \mathbf{e}(i) + \sqrt{\phi_2 J} g_{jr} \mathbf{j}(i)\right) + \mathbf{n}_r(i), \tag{2}$$

where $\mathbf{j}(i)$ and J denote the jammer's artificial noise for the i-th channel use and its transmit power, respectively, satisfying $\mathbb{E}[\mathbf{j}(i)\mathbf{j}^*(i)] = 1$. $\mathbf{n}_r(i)$ represents the additive white Gaussian noise (AWGN) at the backscatter receiver with power σ_r^2. Additionally, ϕ_1 and $\phi_2 \in [0, 1]$ denote the interference cancellation coefficients for the RF source's signal and the jammer's signal, respectively, where $\phi_1 = \phi_2 = 0$ indicates perfect interference cancellation [26], [27]. It is assumed that $\mathbf{x}(i)$ and $\mathbf{e}(i)$ are circularly symmetric complex Gaussian random variables.

B. Problem Formulation

Considering both the channel uncertainty and the randomness of artificial noise from the jammer, we aim to maximize the effective covert rate of the backscatter link while satisfying a covertness constraint. The effective covert rate is defined as $R^c(\alpha) = R(1-\theta(\alpha))$, where R is the predefined transmission rate, and $\theta(\alpha)$ is the outage probability of the backscatter link as a function of the tag's reflection coefficient α. The optimization problem for α can be formulated as

$$\begin{aligned} &\max_{\alpha} \ R^c(\alpha) \\ &\text{s.t.} \begin{cases} 0 < \alpha \leq 1, \\ \mathbb{E}\{\xi^*(\alpha)\} \geq 1 - \epsilon, \end{cases} \end{aligned} \tag{3}$$

where $\mathbb{E}\{\xi^*(\alpha)\}$ represents the average minimum detection error rate at the warden, and $\epsilon \in [0,1]$ is a predefined covertness threshold.

C. Two Types of Jamming Patterns

The jammer emits jamming signals to enhance the covertness of the backscatter link by masking its transmissions. Different jamming patterns, characterized by varying artificial noise power distributions, can impact system covertness and achievable covert rates differently, even when their maximum artificial noise power levels are identical. This paper considers two widely used jamming patterns, uniform distribution [10], [11] and truncated exponential distribution [28], for the jammer's artificial noise power. Later, in Section V, we introduce the concept of jamming cost to quantitatively compare the power efficiency of these patterns.

Pattern I (*Uniform Distribution*): The artificial noise power J follows a uniform distribution over the interval $[0, W]$ with the probability density function (PDF) given by

$$f_J^u(w) = \begin{cases} \frac{1}{W}, & 0 \leq w \leq W, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

where W represents the maximum transmit power of the artificial noise generated by the jammer.

Pattern II (*Truncated Exponential Distribution*): The artificial noise power J follows a truncated exponential distribution over the interval $[0, W]$ with the PDF given by

$$f_J^e(w) = \begin{cases} \frac{\lambda \mathrm{e}^{-\lambda w}}{1-\mathrm{e}^{-\lambda W}}, & 0 \leq w \leq W, \\ 0, & \text{otherwise}, \end{cases} \tag{5}$$

where λ denotes the rate parameter of the truncated exponential distribution.

IV. Optimal Covert Transmission Under Different Jamming Patterns

Considering the channel uncertainty and the randomness of the artificial noise, the problem (3) is challenging to solve directly. To address this challenge, we first derive the outage probability of the backscatter link $\theta(\alpha)$ under both jamming patterns. Subsequently, we analyze the warden's detection mechanism and derive closed-form expressions for the warden's average minimum detection error rates $\mathbb{E}\{\xi^*(\alpha)\}$. Finally, by examining the monotonicity of both the effective covert rates $R^c(\alpha)$ and the warden's average minimum detection error rates $\mathbb{E}\{\xi^*(\alpha)\}$ with respect to the tag's reflection coefficient α, we obtain efficient solutions for the optimal α.

A. Outage Probability at the Backscatter Receiver

The signal-to-interference-plus-noise Ratio (SINR) at the backscatter receiver is given by

$$\mathrm{SINR}_r = \frac{\alpha P |g_{st}|^2 |h_{tr}|^2}{\phi_1 P |g_{sr}|^2 + \phi_2 J |g_{jr}|^2 + \sigma_r^2}. \tag{6}$$

To obtain the outage probability of the backscatter link, it is necessary to consider the randomness in both the channel gains and the jamming's transmit power J.

Lemma 1. *The outage probabilities of the backscatter link under jamming Pattern I and Pattern II are given by*

$$\theta_u(\alpha_u) = 1 - \Phi(c_u) \frac{\ln(\lambda_{jr} + d_u \lambda_{st} W) - \ln(\lambda_{jr})}{d_u W \lambda_{st}}, \tag{7}$$

and

$$\theta_e(\alpha_e) = 1 - \Phi(c_e) \frac{\lambda \mathrm{e}^{\frac{\lambda \lambda_{jr}}{d_e \lambda_{st}}} (\mathrm{Ei}(\frac{-\lambda \lambda_{jr} + d_e W \lambda_{st} \lambda}{d_e \lambda_{st}}) - \mathrm{Ei}(-\frac{\lambda \lambda_{jr}}{d_e \lambda_{st}}))}{d_e \lambda_{st} (1 - \mathrm{e}^{-\lambda W})}, \tag{8}$$

respectively. In this paper, subscript and superscript $x \in \{u, e\}$ is used to denote which jamming pattern is employed, with $x = u$ for Pattern I and $x = e$ for Pattern II. Here, for each $x \in \{u, e\}$, $\Phi(c_x) = \lambda_{sr} \lambda_{jr} \frac{\mathrm{e}^{-b_x \lambda_{st}}}{c_x P \lambda_{st} + \lambda_{sr}}$, $u_x = \frac{2^R - 1}{\alpha_x |h_{tr}|^2 P}$, $c_x = u_x \phi_1 > 0$, $d_x = u_x \phi_2 > 0$, $b_x = u_x \sigma_r^2$. The exponential integral function is given by $\mathrm{Ei}\,(\cdot) = \int_{-\infty}^{x} \frac{\mathrm{e}^t}{t} dt$.

Proof. Based on the definition of transmission outage probability, the outage probability of the backscatter link under jamming *Pattern I* is given by

$$\begin{aligned} \theta_u(\alpha_u) &= \Pr\left\{ \frac{\alpha P |g_{st}|^2 |h_{tr}|^2}{\phi_1 P |g_{sr}|^2 + \phi_2 J |g_{jr}|^2 + \sigma_r^2} \leq 2^R - 1 \right\} \\ &= \int_0^{M_u} \int_0^{\infty} \int_0^{\infty} \int_0^{W} f_u(x, y, z, w)\, dx\, dy\, dz\, dw, \end{aligned} \tag{9}$$

where $f_u(x,y,z,w) = f_{|g_{st}|^2}(x) f_{|g_{sr}|^2}(y) f_{|g_{jr}|^2}(z) f_J^u(w)$, $f_{|g_{st}|^2}(x) = \lambda_{st} \mathrm{e}^{-\lambda_{st} x}$, $f_{|g_{sr}|^2}(y) = \lambda_{sr} \mathrm{e}^{-\lambda_{sr} y}$, $f_{|g_{jr}|^2}(z) = \lambda_{jr} \mathrm{e}^{-\lambda_{jr} z}$, $f_J^u(w)$, and $M_u = c_u P y + d_u w z + b_u$. Note that the random variables $|g_{st}|^2$, $|g_{sr}|^2$, $|g_{jr}|^2$, and J are mutually independent. We calculate the integral in (9) to obtain the closed-form expression of $\theta_u(\alpha_u)$. Similarly, under jamming *Pattern II*, we can derive the closed-form expression for θ_e in (8) by following the same method, but using the truncated exponential distribution for J. □

B. Detection Mechanism at the Warden

To ensure a robust security analysis, we adopt a conservative approach and assume the warden has knowledge of the channel responses g_{sw}, g_{jw}, and h_{tw}. This represents a worst-case scenario for covert communication, as it gives the warden the maximum possible advantage in detecting the tag's transmissions. To create uncertainty at the warden, the jammer randomizes its transmit power, causing fluctuations in the power received by the warden. Consequently, the warden becomes uncertain whether an increase in received power is due to the backscatter link or merely caused by fluctuations in the jammer's artificial noise J.

Since the warden often knows or suspects the time intervals of potential backscatter transmissions, it employs binary hypothesis testing to infer the presence of backscatter communication. By observing the received signals during these time slots, the warden makes a decision based on two hypotheses. Under the null hypothesis $\mathcal{H}_0$, the tag is not transmitting, and under the alternative hypothesis $\mathcal{H}_1$, the tag is transmitting. The received signal at the warden is expressed as $\mathbf{y}_w(i)$ for the i-th channel use, i.e.,

$$\mathbf{y}_w(i) = \begin{cases} \sqrt{P}g_{sw}\mathbf{e}(i) + \sqrt{J}g_{jw}\mathbf{j}(i) + \mathbf{n}_w(i), & \mathcal{H}_0, \\ \sqrt{P}g_{sw}\mathbf{e}(i) + \sqrt{J}g_{jw}\mathbf{j}(i) + h_{tw}\mathbf{x}(i) + \mathbf{n}_w(i), & \mathcal{H}_1, \end{cases} \tag{10}$$

where $\mathbf{n}_w(i)$ is the AWGN at the warden with power σ_w^2.

We assume equal prior probabilities for the hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$. In binary hypothesis testing, the false alarm and miss-detection rates are $P_{FA} = \Pr\{D_1|\mathcal{H}_0\}$ and $P_{MD} = \Pr\{D_0|\mathcal{H}_1\}$, where D_1 and D_0 are the decisions in favor of $\mathcal{H}_1$ or $\mathcal{H}_0$, respectively (i.e., deciding whether the tag is reflecting or not). Under equal priors, the detection error rate is

$$\xi = P_{FA} + P_{MD}. \tag{11}$$

Combining the Neyman-Pearson criterion and the likelihood ratio test [29], the optimal decision rule for the warden to minimize its detection error can be expressed as

$$P_w \underset{D_0}{\overset{D_1}{\gtrless}} \tau, \tag{12}$$

where $P_w = \frac{1}{n}\sum_{i=1}^{n}|\mathbf{y}_w(i)|^2$ is the average received power at the warden over a slot consisting of n channel uses. The detection threshold τ serves as the criterion for deciding the presence or absence of the tag's signal. Based on the strong law of large numbers, we assume an infinite number of channel uses, i.e., $n \to \infty$, giving

$$P_w = \begin{cases} P|g_{sw}|^2 + J|g_{jw}|^2 + \sigma_w^2, & \mathcal{H}_0, \\ P|g_{sw}|^2 + J|g_{jw}|^2 + \alpha P|g_{st}|^2|h_{tw}|^2 + \sigma_w^2, & \mathcal{H}_1. \end{cases} \tag{13}$$

C. Minimum Detection Error Rate at the Warden

If the warden fails to detect the backscatter transmission or has an extremely low probability of detecting it, we can conclude that the tag successfully achieves covert information transmission. To evaluate the system's covertness, it is necessary to assess the warden's detection performance. Therefore, we first derive expressions for the warden's false alarm rate and miss-detection rate.

Lemma 2. *The false alarm and miss-detection rates at the warden for an arbitrary detection threshold under jamming Pattern I and Pattern II are given by*

$$\begin{aligned} P_{FA}^u(\tau_u) &= \begin{cases} 1, & \tau_u < q_1, \\ 1 - \frac{\tau_u - q_1}{W|g_{jw}|^2}, & q_1 \le \tau_u \le q_2, \\ 0, & \tau_u > q_2, \end{cases} \\ P_{MD}^u(\tau_u) &= \begin{cases} 0, & \tau_u < q_3, \\ \frac{\tau_u - q_3}{W|g_{jw}|^2}, & q_3 \le \tau_u \le q_4, \\ 1, & \tau_u > q_4, \end{cases} \end{aligned} \tag{14}$$

and

$$\begin{aligned} P_{FA}^e(\tau_e) &= \begin{cases} 1, & \tau_e < q_{e1}, \\ 1 - \frac{1-\mathrm{e}^{-\frac{\lambda(\tau_e - q_{e1})}{|g_{jw}|^2}}}{1-\mathrm{e}^{-\lambda W}}, & q_{e1} \le \tau_e \le q_{e2}, \\ 0, & \tau_e > q_{e2}, \end{cases} \\ P_{MD}^e(\tau_e) &= \begin{cases} 0, & \tau_e < q_{e3}, \\ \frac{1-\mathrm{e}^{-\frac{\lambda(\tau_e - q_{e3})}{|g_{jw}|^2}}}{1-\mathrm{e}^{-\lambda W}}, & q_{e3} \le \tau_e \le q_{e4}, \\ 1, & \tau_e > q_{e4}, \end{cases} \end{aligned} \tag{15}$$

respectively, where $q_1 = P|g_{sw}|^2 + \sigma_w^2$, $q_2 = P|g_{sw}|^2 + W|g_{jw}|^2 + \sigma_w^2$, $q_3 = P(|g_{sw}|^2 + Q) + \sigma_w^2$, $Q = \alpha_u|g_{st}|^2|h_{tw}|^2$, $q_4 = P(|g_{sw}|^2 + Q) + W|g_{jw}|^2 + \sigma_w^2$, $q_{e1} = P|g_{sw}|^2 + \sigma_w^2$, $q_{e2} = P|g_{sw}|^2 + W|g_{jw}|^2 + \sigma_w^2$, $q_{e3} = P(|g_{sw}|^2 + Q_e) + \sigma_w^2$, $Q_e = \alpha_e|g_{st}|^2|h_{tw}|^2$*, and* $q_{e4} = P(|g_{sw}|^2 + Q_e) + W|g_{jw}|^2 + \sigma_w^2$*. We denote* α_u *and* α_e *as the reflection coefficients under jamming Pattern I and Pattern II, respectively.*

Proof. Through (10), the false alarm rate under jamming *Pattern I* is derived as

$$\begin{aligned} P_{FA}^u(\tau_u) &= \Pr\{P|g_{sw}|^2 + J|g_{jw}|^2 + \sigma_w^2 > \tau_u\} \\ &= \begin{cases} 1, & \tau_u < q_1, \\ \Pr\{J > \frac{\tau_u - \sigma_w^2 - P|g_{sw}|^2}{|g_{jw}|^2}\}, & q_1 \le \tau_u \le q_2, \\ 0, & \tau_u > q_2. \end{cases} \end{aligned} \tag{16}$$

Similarly, the miss-detection rate is determined as

$$\begin{aligned} P_{MD}^u(\tau_u) &= \Pr\{P(|g_{sw}|^2 + Q) + J|g_{jw}|^2 + \sigma_w^2 < \tau_u\} \\ &= \begin{cases} 0, & \tau_u < q_3, \\ \Pr\{J < \frac{\tau_u - q_3}{|g_{jw}|^2}\}, & q_3 \le \tau_u \le q_4, \\ 1, & \tau_u > q_4. \end{cases} \end{aligned} \tag{17}$$

Here, the uniform PDF $f_J^u(w)$ for J is deployed under jamming *Pattern I*. For jamming *Pattern II*, similar derivations are performed using the truncated exponential distribution of J. □

Based on **Lemma 2**, we derive the optimal detection thresholds for the warden under jamming *Pattern I* and *Pattern II*.

Theorem 1. *The warden's optimal detection thresholds under jamming Pattern I and Pattern II are given by*

$$\tau_u^* = \begin{cases} [q_2, q_3], & q_2 < q_3, \\ [q_3, q_2], & q_2 \ge q_3, \end{cases} \tag{18}$$

and

$$\tau_e^* = \begin{cases} [q_{e2}, q_{e3}], & q_{e2} < q_{e3}, \\ [q_{e3}, q_{e2}], & q_{e2} \geq q_{e3}, \end{cases} \tag{19}$$

respectively. The corresponding minimum detection error rates can be expressed as

$$\xi_u^* = \begin{cases} 0, & q_2 < q_3, \\ 1 - \frac{\alpha_u P |g_{st}|^2 |h_{tw}|^2}{W |g_{jw}|^2}, & q_2 \geq q_3, \end{cases} \tag{20}$$

and

$$\xi_e^* = \begin{cases} 0, & q_{e2} < q_{e3}, \\ 1 + \frac{\mathrm{e}^{-\frac{\alpha_e \lambda P |g_{st}|^2 |h_{tw}|^2}{|g_{jw}|^2}} - 1}{1 - \mathrm{e}^{-\lambda W}}, & q_{e2} \geq q_{e3}, \end{cases} \tag{21}$$

respectively.

Proof. Under jamming *Pattern I*, we have $q_1 < q_3$ and $q_4 \geq \max(q_2, q_3)$.

When $q_2 < q_3$, the detection error rate at the warden can be reformulated as

$$\xi_u = \begin{cases} 1, & \tau_u < q_1, \\ 1 - \frac{\tau_u - q_1}{W |g_{jw}|^2}, & q_1 \leq \tau_u < q_2, \\ 0, & q_2 \leq \tau_u \leq q_3, \\ \frac{\tau_u - q_3}{W |g_{jw}|^2}, & q_3 < \tau_u \leq q_4, \\ 1, & \tau_u > q_4. \end{cases} \tag{22}$$

In this case, the warden can set $\tau_u \in [q_2, q_3]$ to achieve $\xi_u = 0$. Correspondingly, the inequality $\alpha_u P |g_{st}|^2 |h_{tw}|^2 > W |g_{jw}|^2$ holds, meaning this covert communication behavior can be detected with a probability of one.

When $q_2 \geq q_3$, the detection error rate at the warden becomes

$$\xi_u = \begin{cases} 1, & \tau_u < q_1, \\ 1 - \frac{\tau_u - q_1}{W |g_{jw}|^2}, & q_1 \leq \tau_u < q_3, \\ 1 - \frac{\alpha_u P |g_{st}|^2 |h_{tw}|^2}{W |g_{jw}|^2}, & q_3 \leq \tau_u \leq q_2, \\ \frac{\tau_u - q_3}{W |g_{jw}|^2}, & q_2 < \tau_u \leq q_4, \\ 1, & \tau_u > q_4. \end{cases} \tag{23}$$

When $q_3 \leq \tau_u \leq q_2$, ξ_u remains constant and is given by $\xi_u = 1 - \alpha_u P |g_{st}|^2 |h_{tw}|^2 / (W |g_{jw}|^2)$. When $q_1 \leq \tau_u < q_3$, ξ_u is strictly decreasing monotonically with respect to τ_u and can be expressed as $\xi_u = 1 - (\tau_u - q_1)/(W |g_{jw}|^2)$. Similarly, when $q_2 < \tau_u \leq q_4$, ξ_u is increasing monotonically with τ_u and is given by $\xi_u = (\tau_u - q_3)/(W |g_{jw}|^2)$.

Based on these observations, the minimum detection error rate ξ_u^* is achieved when the optimal detection threshold τ_u^* lies within the interval $[q_3, q_2]$. In this case, it is given by $\xi_u^* = 1 - (\alpha_u P |g_{st}|^2 |h_{tw}|^2)/(W |g_{jw}|^2)$.

Under jamming *Pattern II*, we have $q_{e1} < q_{e3}$ and $q_{e4} \geq \max(q_{e2}, q_{e3})$. When $q_{e2} < q_{e3}$, the detection error rate at the warden is

$$\xi_e = \begin{cases} 1, & \tau_e < q_{e1}, \\ 1 - \frac{1 - \mathrm{e}^{-\frac{\lambda(\tau_e - q_{e1})}{|g_{jw}|^2}}}{1 - \mathrm{e}^{-\lambda W}}, & q_{e1} \leq \tau_e < q_{e2}, \\ 0, & q_{e2} \leq \tau_e \leq q_{e3}, \\ \frac{1 - \mathrm{e}^{-\frac{\lambda(\tau_e - q_{e3})}{|g_{jw}|^2}}}{1 - \mathrm{e}^{-\lambda W}}, & q_{e3} < \tau_e \leq q_{e4}, \\ 1, & \tau_e > q_{e4}. \end{cases} \tag{24}$$

In this case, the warden can set $\tau_e \in [q_{e2}, q_{e3}]$ to achieve $\xi_e = 0$. The inequality $\alpha_e P |g_{st}|^2 |h_{tw}|^2 > W |g_{jw}|^2$ serves as a criterion for detecting this covert communication behavior with a probability of one.

When $q_{e2} \geq q_{e3}$, the detection error rate at the warden becomes

$$\xi_e = \begin{cases} 1, & \tau_e < q_{e1}, \\ 1 + \frac{\mathrm{e}^{-\frac{\lambda(\tau_e - q_{e1})}{|g_{jw}|^2}} - 1}{1 - \mathrm{e}^{-\lambda W}}, & q_{e1} \leq \tau_e < q_{e3}, \\ 1 + \frac{\mathrm{e}^{-\frac{\alpha_e \lambda P |g_{st}|^2 |h_{tw}|^2}{|g_{jw}|^2}} - 1}{1 - \mathrm{e}^{-\lambda W}}, & q_{e3} \leq \tau_e \leq q_{e2}, \\ \frac{1 - \mathrm{e}^{-\frac{\lambda(\tau_e - q_{e3})}{|g_{jw}|^2}}}{1 - \mathrm{e}^{-\lambda W}}, & q_{e2} < \tau_e \leq q_{e4}, \\ 1, & \tau_e > q_{e4}. \end{cases} \tag{25}$$

When $\tau_e \in [q_{e3}, q_{e2}]$, ξ_u remains constant and is given by $\xi_e = 1 + \big(\mathrm{e}^{-\frac{\alpha_e \lambda P |g_{st}|^2 |h_{tw}|^2}{|g_{jw}|^2}} - 1\big) / \big(1 - \mathrm{e}^{-\lambda W}\big)$. When $\tau_e \in [q_{e1}, q_{e3}]$, ξ_e is strictly decreasing monotonically with τ_e and is expressed as $\xi_e = 1 + \big(\mathrm{e}^{-\frac{\lambda(\tau_e - q_{e1})}{|g_{jw}|^2}} - 1\big) / \big(1 - \mathrm{e}^{-\lambda W}\big)$. Also, when $\tau_e \in [q_{e2}, q_{e4}]$, ξ_e is increasing monotonically with τ_e and is given by $\xi_e = \big(1 - \mathrm{e}^{-\frac{\lambda(\tau_e - q_{e3})}{|g_{jw}|^2}}\big) / (1 - \mathrm{e}^{-\lambda W})$.

Thus, the minimum detection error rate ξ_e^* is achieved when the optimal detection threshold τ_e^* lies within $[q_{e3}, q_{e2}]$, and it is given by $\xi_e^* = 1 + \big(\mathrm{e}^{-\frac{\alpha_e \lambda P |g_{st}|^2 |h_{tw}|^2}{|g_{jw}|^2}} - 1\big) / \big(1 - \mathrm{e}^{-\lambda W}\big)$. □

Remark 1. *The noise variance at the warden, denoted as σ_w^2, does not impact the minimum detection error rates (i.e., ξ_u^* and ξ_e^*) under the two jamming patterns, even though it is considered in the optimal threshold of the radiometer. Under jamming Pattern I, the minimum detection error rate ξ_u^* primarily depends on the reflection coefficient of the tag α_u and the ratio of the RF source's transmit power P to the maximum artificial noise power W. As $\alpha_u \to 0$ or $P/W \to 0$, ξ_u^* approaches 1. Similarly, under jamming Pattern II, the minimum detection error rate ξ_e^* exhibits a similar dependence on the reflection coefficient of the tag α_e and the ratio P/W. As $\alpha_e \to 0$ or $P/W \to 0$, ξ_e^* approaches 1, reflecting the warden's inability to detect the tag's transmission under such conditions.*

D. Average Minimum Detection Error Rate

Equations (20) and (21) present the minimum detection error rates for the two jamming patterns. However, each equation splits into two distinct cases due to inherent channel uncertainties, making it challenging to precisely derive a single closed-form expression for the warden's minimum detection error rate. Therefore, under each jamming pattern, we take the average value of ξ^* across both cases as the covert metric to evaluate the performance of the backscatter link. Consequently, the average minimum detection error rate of the warden, $\mathbb{E}\{\xi^*(\alpha)\}$, is described as a covertness constraint in (3). The next step is to calculate the average minimum detection error rates of the warden under the two jamming patterns, i.e., $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ and $\mathbb{E}\{\xi_e^*(\alpha_e)\}$.

Theorem 2. *Under jamming Pattern I, the average minimum detection error rate at the warden, based on the optimal detection threshold τ_u^*, is given by*

$$\mathbb{E}\{\xi_u^*(\beta_u)\} = 1 - \beta_u^2 + \beta_u \ln \beta_u, \tag{26}$$

where $\beta_u \triangleq (\alpha_u P|h_{tw}|^2\lambda_{jw})/(\alpha_u P|h_{tw}|^2\lambda_{jw} + \lambda_{st}W) \in (0,1)$.

Proof. From (20), the mean value of ξ_u^* is determined as

$$\mathbb{E}\{\xi_u^*\} = \Pr\{q_2 < q_3\} \times 0 + \Pr\{q_2 \geq q_3\} \times \mathbb{E}\{\xi_u^*|q_2 \geq q_3\}. \tag{27}$$

We have

$$\begin{aligned}\Pr\{q_2 \geq q_3\} &= \Pr\left\{|g_{st}|^2 \leq \tfrac{W|g_{jw}|^2}{\alpha_u P|h_{tw}|^2}\right\} \\ &= \int_0^\infty \int_0^{\frac{Wv}{\alpha_u P|h_{tw}|^2}} f_{|g_{st}|^2}(x) f_{|g_{jw}|^2}(v)\,dx\,dv \\ &= \tfrac{\lambda_{st}W}{\alpha_u P|h_{tw}|^2\lambda_{jw} + \lambda_{st}W},\end{aligned} \tag{28}$$

and

$$\begin{aligned}&\mathbb{E}\{\xi_u^*|q_2 \geq q_3\} \\ &= \mathbb{E}\left\{1 - \frac{\alpha_u P|g_{st}|^2|h_{tw}|^2}{W|g_{jw}|^2}|q_2 \geq q_3\right\} \\ &= 1 + \frac{\alpha_u P|h_{tw}|^2\lambda_{jw}}{\lambda_{st}W}\left\{\frac{\lambda_{st}W}{\alpha_u P|h_{tw}|^2\lambda_{jw} + \lambda_{st}W}\right. \\ &\quad \left. - \ln(1 + \frac{\lambda_{st}W}{\alpha_u P|h_{tw}|^2\lambda_{jw}})\right\}.\end{aligned} \tag{29}$$

Substituting (28) and (29) into (27) completes the proof. □

Theorem 3. *Under jamming Pattern II, the average minimum detection error rate at the warden, based the optimal detection threshold τ_e^*, is derived as*

$$\begin{aligned}\mathbb{E}\{\xi_e^*(\beta_e)\} &= -\tfrac{\beta_e \mathrm{e}^{-\lambda W}}{(\beta_e+1)(1-\mathrm{e}^{-\lambda W})} + \tfrac{\lambda W}{(1-\mathrm{e}^{-\lambda W})(\beta_e+1)} \mathrm{e}^{\frac{\lambda W}{\beta_e}} \\ &\quad \times \left(\Gamma\left(-1, \tfrac{\lambda W}{\beta_e}\right) - \Gamma\left(-1, \tfrac{\lambda W}{\beta_e} + \lambda W\right)\right),\end{aligned} \tag{30}$$

where $\beta_e = W\lambda_{st}/\left(\alpha_e P|h_{tw}|^2\lambda_{jw}\right) \in (0,1)$ *and* $\Gamma(a,x) = \int_x^\infty t^{a-1}\mathrm{e}^{-t}dt, x > 0, a \in \mathbb{R}$, *denotes the upper incomplete gamma function [30].*

Proof. From (21), the mean value of ξ_e^* is given by

$$\begin{aligned}\mathbb{E}\{\xi_e^*\} = &\Pr\{q_{e2} < q_{e3}\} \times 0 \\ &+ \Pr\{q_{e2} \geq q_{e3}\} \times \mathbb{E}\{\xi_e^*|q_{e2} \geq q_{e3}\}.\end{aligned} \tag{31}$$

We have

$$\begin{aligned}&\Pr\{q_{e2} \geq q_{e3}\} \\ &= \Pr\left\{|g_{st}|^2 \leq \frac{W|g_{jw}|^2}{\alpha_e P|h_{tw}|^2}\right\} \\ &= \int_0^\infty \int_0^{\frac{Wv}{\alpha_e P|h_{tw}|^2}} f_{|g_{st}|^2}(x) f_{|g_{jw}|^2}(v)\,dx\,dv \\ &= \frac{\lambda_{st}W}{\alpha_e P|h_{tw}|^2\lambda_{jw} + \lambda_{st}W} \\ &= \frac{\beta_e}{\beta_e + 1},\end{aligned} \tag{32}$$

and

$$\begin{aligned}&\mathbb{E}\{\xi_e^*|q_{e2} \geq q_{e3}\} \\ &= \mathbb{E}\left\{1 + \frac{\mathrm{e}^{-\frac{\alpha_e\lambda P|g_{st}|^2|h_{tw}|^2}{|g_{jw}|^2}} - 1}{1 - \mathrm{e}^{-\lambda W}}|q_{e2} \geq q_{e3}\right\} \\ &= 1 - \frac{1}{1 - \mathrm{e}^{-\lambda W}} + \frac{1}{1 - \mathrm{e}^{-\lambda W}} \int_0^\infty f_{|g_{jw}|^2}(v) \times \\ &\quad \int_0^{Wv/(\alpha_e P|h_{tw}|^2)} \mathrm{e}^{-\frac{\alpha_e\lambda P|h_{tw}|^2 x}{v}} f_{|g_{st}|^2}(x)\,dx\,dv \\ &= 1 - \frac{1}{1 - \mathrm{e}^{-\lambda W}} + \frac{\lambda W}{(1 - \mathrm{e}^{-\lambda W})\beta_e} \mathrm{e}^{\frac{\lambda W}{\beta_e}} \\ &\quad \times \left(\Gamma\left(-1, \frac{\lambda W}{\beta_e}\right) - \Gamma\left(-1, \frac{\lambda W}{\beta_e} + \lambda W\right)\right).\end{aligned} \tag{33}$$

Substituting (32) and (33) into (31) completes the proof. □

After deriving the closed-form expression for ξ^* under the two jamming patterns, the deterministic covertness constraints are reformulated based on the constraint in (3). Moreover, the corresponding objectives are transformed using (7) and (8). Consequently, we formulate two deterministic reflection optimization problems for the two jamming patterns.

E. Optimal Reflection Coefficients and Covert Rates

Since the optimal reflection coefficients α_u^* and α_e^* cannot be determined directly, we perform monotonicity analyses under the two jamming patterns to derive efficient solutions. Under jamming *Pattern I*, the monotonicity of the warden's average minimum detection error rate $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ and the effective covert rate $R_u^c(\alpha_u)$ with respect to the reflection coefficient α_u is analyzed in Appendix A. Likewise, under jamming *Pattern II*, the monotonicity of the warden's average minimum detection error rate $\mathbb{E}\{\xi_e^*(\alpha_e)\}$ and the effective covert rate $R_e^c(\alpha_e)$ with respect to the reflection coefficient α_e is analyzed in Appendix B. Using the results of **Theorem 4**, the optimal reflection coefficients α_u^* and α_e^*, which maximize their respective covert rates under the given covertness threshold ϵ, can be determined efficiently.

Theorem 4. *Given the RF source's transmit power P and the jammer's power distribution, the optimal reflection coefficients for jamming Pattern I and Pattern II, which achieve the maximum covert rate under the given covertness threshold ϵ, are expressed as*

$$\alpha_u^* = \min\left\{\frac{W\beta_u^\epsilon\lambda_{st}}{(1-\beta_u^\epsilon)P|h_{tw}|^2\lambda_{jw}}, 1\right\}, \tag{34}$$

and

$$\alpha_e^* = \min\left\{\frac{W\lambda_{st}}{\beta_e^\epsilon P|h_{tw}|^2\lambda_{jw}}, 1\right\}, \tag{35}$$

respectively. The corresponding maximum covert rates are determined as

$$R_u^c = R\Phi(c_u^*)\frac{\ln(\lambda_{jr} + c_u^*\lambda_{st}W\phi_2/\phi_1) - \ln(\lambda_{jr})}{c_u^*W\lambda_{st}\phi_2/\phi_1}, \tag{36}$$

and

$$\begin{aligned}R_e^c = &-R\Phi(c_e^*)\tfrac{\lambda \mathrm{e}^{\frac{\lambda\lambda_{jr}}{\lambda_{st}c_e^*\phi_2/\phi_1}}}{c_e^*\lambda_{st}(1-\mathrm{e}^{-\lambda W})\phi_2/\phi_1} \\ &\times(\mathrm{Ei}(-\tfrac{\lambda\lambda_{jr}}{\lambda_{st}c_e^*\phi_2/\phi_1}) - \mathrm{Ei}(-\tfrac{\lambda(\lambda_{jr}+\lambda_{st}c_e^*W\phi_2/\phi_1)}{\lambda_{st}c_e^*\phi_2/\phi_1}))\end{aligned}, \tag{37}$$

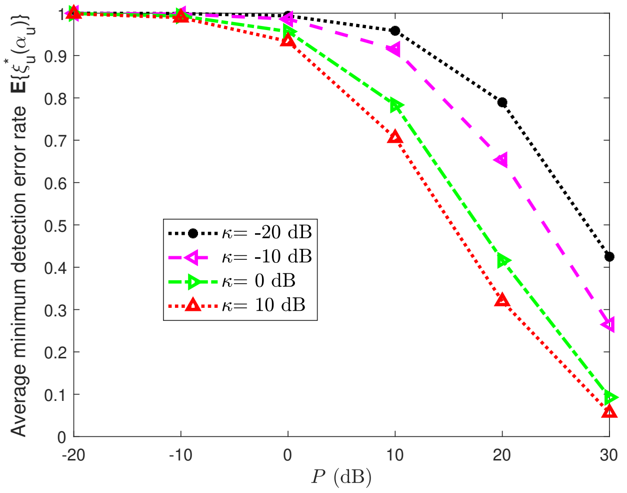


Fig. 2. Average minimum detection error rate $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ for jamming *Pattern I* vs. RF source's transmit power P with $W = -10$ dB and $\alpha_u = 0.5$.

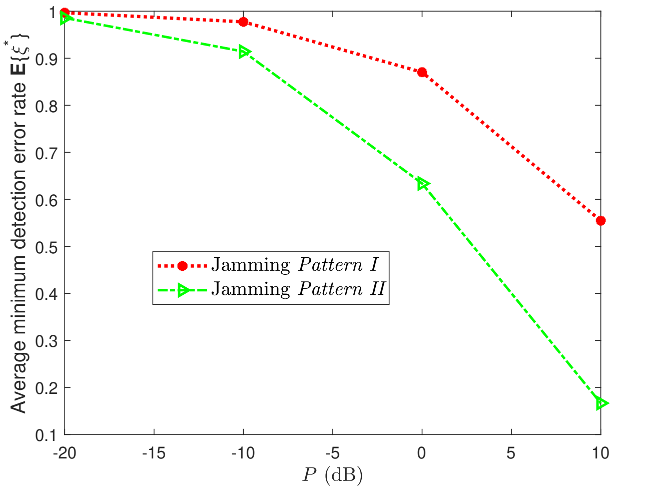


Fig. 3. Comparison of the average minimum detection error rates $\mathbb{E}\{\xi^*(\alpha)\}$ for the two jamming patterns with $W = -10$ dB, $\kappa = 10$ dB, and $\alpha = 0.5$.

respectively, where the function $\Phi(c_x) = \lambda_{sr}\lambda_{jr}\frac{\mathrm{e}^{-b_x\lambda_{st}}}{c_x P\lambda_{st}+\lambda_{sr}}$, $c_u^* = \max\left\{\frac{\phi_1(2^R-1)(1-\beta_u^\epsilon)|h_{tw}|^2\lambda_{jw}}{\beta_u^\epsilon W|h_{tr}|^2\lambda_{st}}, \frac{\phi_1(2^R-1)}{|h_{tr}|^2P}\right\}$, $c_e^* = \max\left\{\frac{\phi_1(2^R-1)|h_{tw}|^2\beta_e^\epsilon\lambda_{jw}}{W|h_{tr}|^2\lambda_{st}}, \frac{\phi_1(2^R-1)}{|h_{tr}|^2P}\right\}$, β_u^ϵ *is the solution of* $\mathbb{E}\{\xi_u^*(\beta_u)\} = 1-\epsilon$ *for* β_u*, and* β_e^ϵ *is the solution of* $\mathbb{E}\{\xi_e^*(\beta_e)\} = 1-\epsilon$ *for* β_e*.*

Proof. The proof is provided in Appendices A and B. □

Remark 2. *To address computational complexity, we derive closed-form expressions involving multiple random variables. These expressions, along with rigorous monotonicity analyses, are expressed as parameterized forms, introducing no additional runtime complexity. The determination of the optimal reflection coefficients necessitates solving for* β_u^ϵ *and* β_e^ϵ*, which incurs a small computational overhead. To efficiently obtain these values, we employ the bisection method. Let* N_u *and* N_e *denote the number of iterations under jamming Pattern I and Pattern II, respectively. The computational complexities for these two patterns are* $O(\log N_u)$ *and* $O(\log N_e)$*, respectively.*

V. Numerical Results and Analysis

This simulation set considers the large-scale channel fading model described in [12]. The LoS channel coefficient is given by $|h_{ij}^{\text{LoS}}|^2 = K^2 G_{ij} d_{ij}^{-\nu}$, and the average channel gain between nodes a and b is expressed as $1/\lambda_{ab} = K^2 G_{ab} d_{ab}^{-\varphi}$, where $ab \in \{ij, kl\}$, the constant $K = \lambda/4\pi$, which relies on the carrier wavelength λ. The NLoS channel coefficient $|h_{ij}^{\text{NLoS}}|^2$ follows an exponential distribution with parameter λ_{ij}. ν and φ represent the path loss exponents for LoS and non-LoS links, respectively. d_{ab} and G_{ab} denote the distance and the antenna gain between the transmitting node a and the receiving node b. For simplicity, we set $\phi_1 = \phi_2 = 0.01$. Additionally, the carrier frequency is 915 MHz, $\nu = 2$, $\varphi = 4$, $d_{st} = d_{sr} = d_{sw} = 100$ m, $d_{jr} = d_{jw} = 80$ m, $d_{tw} = 5$ m, and $d_{tr} = 1$ m.

Under jamming *Pattern I*, we set the maximum artificial noise power of the jammer $W = -10$ dB and the reflection coefficient $\alpha_u = 0.5$. It can be observed from Fig. 2 that the warden's average minimum detection error rates, denoted as $\mathbb{E}\{\xi_u^*(\alpha_u)\}$, decrease monotonically with increasing power of the RF source, P, for various Rician factors κ. However, since the RF source's transmit power is typically fixed in practical scenarios, optimizing the tag's reflection coefficient based on (34) becomes essential for effective covert communication. Furthermore, it is noteworthy that $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ decreases as the Rician factor κ increases. This phenomenon can be attributed to the deterministic LoS component, which becomes more prominent at higher κ values, resulting in higher information leakage power compared to the attenuated power of the random Rayleigh fading component. This observation further supports that multipath communication environments provide an advantage for covert communication.

For a clearer comparison of the warden's average minimum detection error rates $\mathbb{E}\{\xi^*(\alpha)\}$ under the two jamming patterns, Fig. 3 illustrates the trends of $\mathbb{E}\{\xi^*(\alpha)\}$ as a function of P. Compared with jamming *Pattern I*, the warden's average minimum detection error rate (i.e., $\mathbb{E}\{\xi_e^*(\alpha_e)\}$) under jamming *Pattern II* is lower, regardless of the ambient power of the RF source. This result illustrates that jamming *Pattern I* deployed by the jammer achieves better covertness than jamming *Pattern II* under varying power levels of the RF source. The reason lies in the statistical differences between these two jamming power distributions. The uniformly distributed jamming power ensures that every value within the range is equally likely, creating a higher level of unpredictability for the warden. In contrast, the truncated exponential distribution skews towards lower power values, leading to less effective masking of the tag's signal and a reduced level of covertness as P increases. Therefore, jamming *Pattern II* makes the tag's transmissions more likely to be detected by the warden.

To verify the relationship between the transmission outage probability of the backscatter link θ and the reflection coefficient α, Figs. 4 and 5 depict the performance trends of θ under various factors. Specifically, Fig. 4 examines the

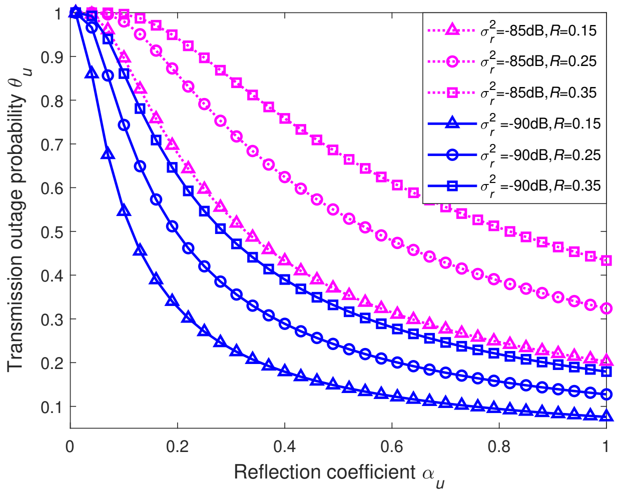


Fig. 4. Outage probability of the backscatter link θ_u for jamming *Pattern I* vs. reflection coefficient α_u with $W = 10$ dB and $P = 30$ dB.

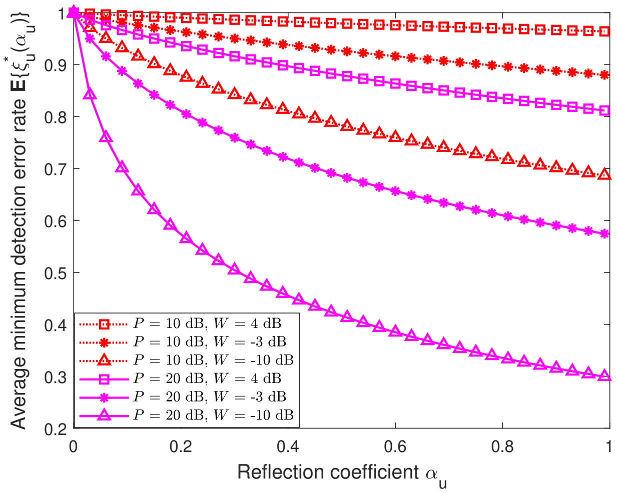


Fig. 6. Average minimum detection error rate $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ for jamming *Pattern I* vs. reflection coefficient α_u.

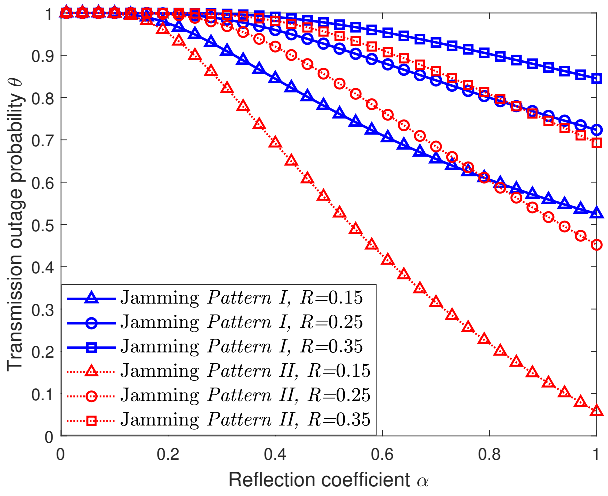


Fig. 5. Comparison of the outage probability of the backscatter link θ for the two jamming patterns with $W = 10$ dB and $P = 20$ dB.

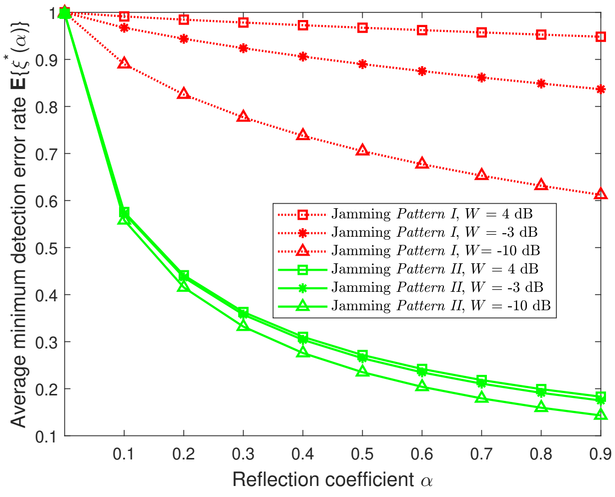


Fig. 7. Comparison of the average minimum detection error rates $\mathbb{E}\{\xi^*(\alpha)\}$ for the two jamming patterns with $P = 10$ dB.

impact of varying values of predefined transmission rate R and backscatter receiver noise power σ_r^2 under jamming *Pattern I*, while Fig. 5 compares the effects of different jamming patterns with varying R. Notably, Figs. 4 and 5 show that the backscatter link's outage probability θ decreases monotonically as α increases. However, θ is larger when higher values of σ_r^2 or R are used, or when jamming *Pattern I* is employed, with a maximum difference of over 8 times compared to jamming *Pattern II*. This comparison illustrates that jamming *Pattern II* provides better reliability for the backscatter link compared to jamming *Pattern I*, while still maintaining the covertness constraint.

Figs. 6 and 7 verify the monotonic decrease of the average minimum detection error rate of the warden $\mathbb{E}\{\xi^*(\alpha)\}$ with respect to the reflection coefficient α. This trend is analyzed across various values of the RF source power P and the maximum artificial noise power W, as well as different jamming patterns. In Fig. 6, an increase in W results in a higher $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ under jamming *Pattern I*, while an increase in P results in a lower $\mathbb{E}\{\xi_u^*(\alpha_u)\}$. Fig. 7 shows that the average minimum detection error rates of the warden under jamming *Pattern II* exhibit a more pronounced downward trend and are consistently lower than those under *Pattern I* across the range of α. Hence, *Pattern I* provides a higher level of covertness, with a maximum difference more than 5 times that of jamming *Pattern II*.

These observations confirm that jamming *Pattern I* achieves stronger covertness, while jamming *Pattern II* is less covert but may offer better reliability. This trade-off highlights the suitability of jamming *Pattern I* for scenarios prioritizing covertness, whereas jamming *Pattern II* may be preferable in applications requiring higher communication reliability.

While Figs. 4–7 verify the monotonic relationships between the outage probability θ and the reflection coefficient α, as

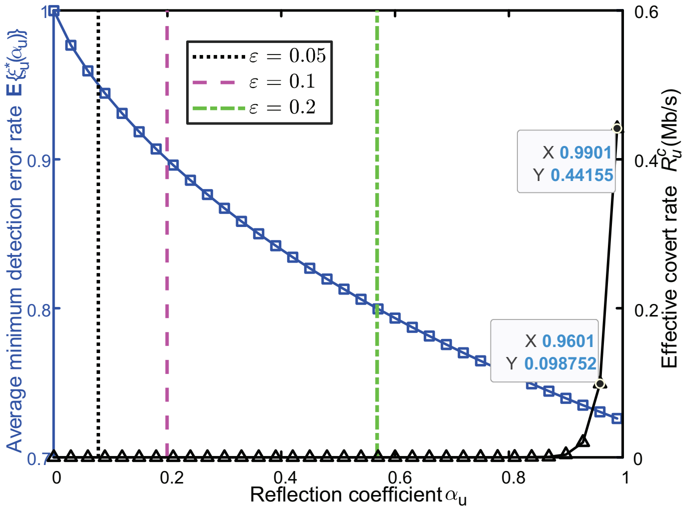


Fig. 8. Average minimum detection error rate $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ (colored in blue) and effective covert rate R_u^c (colored in black) vs. reflection coefficient α_u under different covertness thresholds ϵ for jamming *Pattern I*.

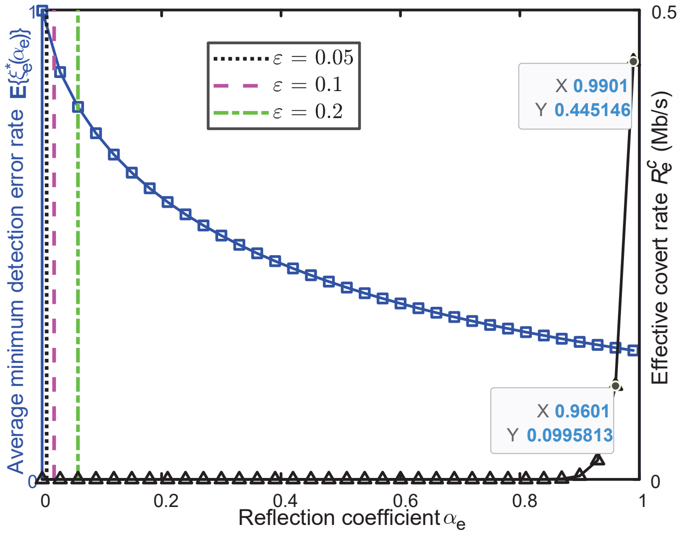


Fig. 9. Average minimum detection error rate $\mathbb{E}\{\xi_e^*(\alpha_e)\}$ (colored in blue) and effective covert rate R_e^c (colored in black) vs. reflection coefficient α_e under different covertness thresholds ϵ for jamming *Pattern II*.

well as between the warden's average minimum detection error rate $\mathbb{E}\{\xi^*(\alpha)\}$ and α, these relationships alone do not provide a direct method for determining the optimal value of α. Therefore, Figs. 8 and 9 illustrate the trends of two achievable effective covert rates (R_u^c and R_e^c under jamming *Pattern I* and *Pattern II*, respectively) versus α for different covertness thresholds ϵ.

In Figs. 8 and 9, R^c (the black curve) exhibits a monotonically increasing trend with α, while $\mathbb{E}\{\xi^*(\alpha)\}$ (the blue curve) decreases monotonically. These trends lead to clear and definitive solutions for the two jamming patterns, represented as α_u^* in (34) (for jamming *Pattern I*) and α_e^* in (35) (for jamming *Pattern II*). The maximum achievable effective covert rates, R_u^c and R_e^c, are determined by the intersection points of the vertical dashed lines (representing different covertness thresholds) with the growth curve of the effective covert rates. Additionally, these figures show that a lower covertness threshold ϵ corresponds to both a lower optimal covert rate R_u^{c*} (R_e^{c*}) and a smaller optimal reflection coefficient α_u^* (α_e^*). This highlights the inherent trade-off between achieving higher covert rates and maintaining stronger covertness. Overall, these results demonstrate that solving for the optimal reflection coefficient provides an effective balance between the covertness and the effective covert rate of the backscatter link.

To effectively evaluate the efficiency of different jamming patterns, we introduce a novel metric termed "jamming cost", defined as the minimum required maximum jamming power W to achieve a given covertness level. This metric directly measures power efficiency and clarifies which jamming pattern is more viable for different IoT scenarios. To provide a baseline for comparison, we also analyze a direct-link system [10], where the transmitter sends data directly to the receiver without using a backscattering tag. We compare the performance of both systems under these two jamming patterns.

Let "ABC-U" and "ABC-E" denote ABC systems under jamming *Pattern I* and *Pattern II*, respectively, and let "DL-U" and "DL-E" denote direct-link systems under jamming *Pattern I* and *Pattern II*, respectively. Both systems are configured in an identical network topology, with the primary distinction that the direct-link system does not incorporate backscatter link. Since the existing direct-link system does not involve the reflection coefficient α, using the maximum jamming power as the cost disproportionately inflates the jamming cost for the direct link compared to the backscatter link. To ensure a fair comparison, we set the transmitter's power in the direct link as αP (α denotes the same power allocation coefficient as the reflection coefficient), and then consider the maximum jamming power as the jamming cost for achieving covertly secure transmission.

Table I summarizes the comparisons of jamming costs under the covertness threshold ϵ of 0.05, 0.1, 0.15, and 0.2. The cases where the tag's reflection coefficient $\alpha \in [0, 0.3]$ are considered because the warden's average minimum detection error rates under the two jamming patterns remain high, as shown in Fig. 7. As the covertness threshold ϵ decreases and the values of α or αP increase, the jamming costs of all schemes exhibit an upward trend. The jamming cost of ABC-E is 2–11 times higher than that of ABC-U, with this ratio decreasing as α increases. Both schemes operate normally under all the parameter settings. However, DL schemes incur significantly higher jamming costs than ABC schemes. In addition, DL-E fails under most parameter settings and only functions when ϵ is large and αP is small, whereas DL-U remains operational but at excessive costs. When ϵ decreases from 0.2 to 0.05, ABC schemes experience moderate cost growth, DL-U shows rapid growth, and DL-E quickly fails. In conclusion, ABC-U is the most suitable choice for scenarios requiring low jamming costs, while DL schemes have limited practical value due to either narrow operating range or excessive costs.

Fig. 10 depicts a comparison of jamming costs among ABC-U, ABC-E, and DL-U under various average minimum detection error rates of the warden. Compared to the direct-

TABLE I
COMPARISON OF JAMMING COSTS UNDER VARIOUS COVERTNESS THRESHOLDS ϵ

W ϵ Case		0.2	0.15	0.1	0.05
ABC-U	α=0.001	0.001	0.002	0.003	0.008
	α=0.005	0.005	0.009	0.015	0.039
	α=0.01	0.011	0.017	0.031	0.078
	α=0.03	0.032	0.051	0.092	0.233
ABC-E	α=0.001	0.011	0.013	0.017	0.026
	α=0.005	0.027	0.033	0.045	0.079
	α=0.01	0.042	0.052	0.072	0.141
	α=0.03	0.088	0.115	0.181	0.952
DL-U [10]	αP=0.01	0.123	0.194	0.352	0.893
	αP=0.05	0.616	0.972	1.757	4.464
	αP=0.1	1.232	1.944	3.515	8.928
	αP=0.3	3.697	5.833	10.646	26.784
DL-E	αP=0.01	0.287	0.536	Failure	Failure
	αP=0.05	Failure	Failure	Failure	Failure
	αP=0.1	Failure	Failure	Failure	Failure
	αP=0.3	Failure	Failure	Failure	Failure

Note: "Failure" indicates the scheme could not meet covertness constraints.

link system, the ABC system under both jamming patterns requires significantly less jamming power (i.e., lower jamming cost) to achieve equivalent covertness, underscoring the effectiveness of integrating ABC with covert communication. Additionally, *Pattern I* requires less jamming power than *Pattern II* for a given target of average minimum detection error rate $\mathbb{E}\{\xi^*(\alpha)\}$, highlighting its cost-effectiveness for highly security-sensitive applications.

In summary, the results in this section indicate that jamming *Pattern I* provides a higher level of covertness with lower jamming cost than jamming *Pattern II*, making it better suited for low-cost applications requiring high security. In contrast, jamming *Pattern II* demonstrates greater resilience to interruptions and achieves a lower outage probability, making it more reliable in scenarios where communication stability is prioritized alongside covertness. These findings underscore the necessity of employing diverse jamming patterns to efficiently meet personalized service goals across varying scenarios, and further demonstrate the effectiveness of the proposed ABC system under the two jamming patterns.

VI. CONCLUSION

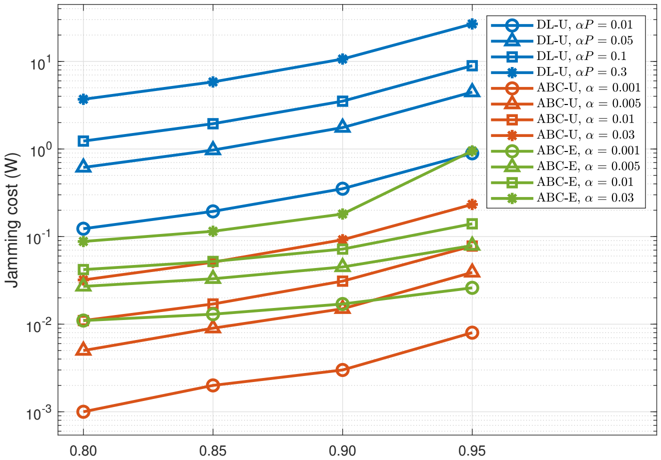


Fig. 10. Comparison of jamming costs under various average minimum detection error rates $\mathbb{E}\{\xi^*(\alpha)\}$ with $P = 10$ dB.

This paper investigated the reflection optimization problem for covert transmission in an ambient backscatter communication (ABC) system with an external friendly jammer. To enhance the covert performance of the backscatter link, we examined two jamming power distributions, uniform and truncated exponential, and analyzed their impact on system performance. We derived closed-form expressions for both the outage probability of the backscatter link and the warden's minimum detection error rate under these jamming patterns. By leveraging monotonicity analyses, we identified the tag's optimal reflection coefficient that maximize the effective covert rate under a given covertness constraint. Numerical simulations reveal that uniform jamming achieves higher covertness than truncated exponential jamming (by up to over 5 times). Conversely, truncated exponential jamming offers stronger interference resistance and experiences a lower outage probability (by up to over 8 times), making it more robust for applications prioritizing reliable communication. From a "jamming cost" perspective, i.e., the minimum required maximum jamming power to achieve a given covertness level, uniform jamming is more economical in low-cost settings (by up to 11 times). These results not only highlight the effectiveness of the proposed reflection optimization framework, but also serve as a practical guide for selecting jamming patterns under varying requirements in emerging IoT environments. As future work, we will extend our analysis to more complex real-world system models and hardware constraints. We also plan to prototype multi-tag, multi-jammer setups and investigate learning-based covert detection at the warden for enhanced adaptability.

APPENDIX A
PROOF OF THEOREM 4 FOR JAMMING PATTERN I

The first and second derivatives of $\mathbb{E}\{\xi_u^*(\beta_u)\}$ are given by $\mathbb{E}'\{\xi_u^*(\beta_u)\} = -2\beta_u + \ln\beta_u + 1$, and $\mathbb{E}''\{\xi_u^*(\beta_u)\} = -2 + \frac{1}{\beta_u}$, respectively. The maximum of $\mathbb{E}'\{\xi_u^*(\beta_u)\}$ is $\mathbb{E}'\{\xi_u^*(1/2)\} = -\ln 2 < 0$, indicating that $\mathbb{E}\{\xi_u^*(\beta_u)\}$ decreases monotonically with β_u. Consequently, $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ also decreases monotonically with α_u due to the positive correlation between α_u and β_u. This implies that the optimized covert rate R_u^c increases monotonically with α_u.

By analyzing the expression of R_u^c in (36), it is clear that R_u^c can be expressed as $R_u^c = R\Phi(c_u)f(d_u)$ where $d_u = c_u\phi_2/\phi_1$ and

$$\begin{aligned}\Phi(c_u) &= \frac{\lambda_{sr}\lambda_{jr}\mathrm{e}^{-c_u\sigma_r^2\lambda_{st}/\phi_1}}{c_u P\lambda_{st}+\lambda_{sr}} > 0,\\ f(d_u) &= \frac{\ln(\lambda_{jr}+d_u\lambda_{st}W)-\ln(\lambda_{jr})}{d_u W\lambda_{st}} > 0.\end{aligned} \tag{38}$$

The first derivatives of $\Phi(c_u)$ and $f(d_u)$ with respect to c_u and d_u are given by

$$\Phi'(c_u) = -\frac{\lambda_{st}^2\lambda_{jr}(\sigma_r^2(\lambda_{sr}+c_u\lambda_{st}P)/\phi_1+P)\mathrm{e}^{-\frac{c_u\lambda_{st}\sigma_r^2}{\phi_1}}}{(\lambda_{sr}+c_u\lambda_{st}P)^2} < 0 \tag{39}$$

and

$$f'(d_u) = \frac{\frac{d_uW\lambda_{st}}{d_uW\lambda_{st}+\lambda_{jr}} - \ln(d_uW\lambda_{st}+\lambda_{jr}) + \ln(\lambda_{jr})}{d_u^2W\lambda_{st}} = \frac{m(d_u)}{d_u^2}, \tag{40}$$

respectively. To further determine the monotonicity of $f(d_u)$ with respect to d_u, we define a function $m(d_u) \triangleq d_uW\lambda_{st}/(d_uW\lambda_{st}+\lambda_{jr}) - (\ln(d_uW\lambda_{st}+\lambda_{jr}) - \ln(\lambda_{jr}))/(W\lambda_{st})$. Accordingly, the first derivative of $m(d_u)$ is given as

$$m'(d_u) = -\frac{d_uW\lambda_{st}}{(d_uW\lambda_{st}+\lambda_{jr})^2} \leq 0. \tag{41}$$

Since $m'(d_u) < 0$, $m(d_u)$ decreases monotonically with d_u, implying $m(d_u) < m(0) = 0$, $f'(d_u) < 0$, and $\Phi'(c_u) < 0$. Hence, both $f(d_u)$ and $\Phi(c_u)$ are decreasing monotonically with respect to d_u and c_u, respectively. Combining this with (38), R_u^c decreases monotonically with c_u but increases with α_u due to the negative correlation among α_u, d_u, and c_u. Since $\mathbb{E}\{\xi_u^*(\alpha_u)\}$ decreases monotonically with α_u, we set the optimal reflection coefficient α_u^* as (34).

Appendix B
Proof of Theorem 4 for Jamming Pattern II

Let $G(y) = y\mathrm{e}^y\left(\Gamma\left(-1,y\right)-\Gamma\left(-1,y+\lambda W\right)\right)$. When $y = \frac{\lambda W}{\beta_e}$, we get $G(\frac{\lambda W}{\beta_e}) = \frac{\lambda W}{\beta_e}\mathrm{e}^{\frac{\lambda W}{\beta_e}}\left(\Gamma\left(-1,\frac{\lambda W}{\beta_e}\right)-\Gamma\left(-1,\frac{\lambda W}{\beta_e}+\lambda W\right)\right)$. The first derivative of $G(y)$ is $G'(y) = \frac{e^{-\lambda W}y^2-(\lambda W+y)^2}{(\lambda W+y)^2y} + e^y(y+1)(\Gamma(-1,y)-\Gamma(-1,\lambda W+y))$. In practical ABC systems, the product of λ and W is positive, i.e., $\lambda W > 0$. For $y > 0$, as illustrated in Fig. 11, $\Gamma(-1,y)-\Gamma(-1,\lambda W+y) > 0$. Since $\frac{e^{-\lambda W}y^2-(\lambda W+y)^2}{(\lambda W+y)^2y} < 0$, $G'(y) < 0$, which means $G(\frac{\lambda W}{\beta_e})$ increases monotonically with β_e.

Observing that $1-\frac{1}{1-\mathrm{e}^{-\lambda W}}$ is a constant, we deduce from (33) that $\mathbb{E}\{\xi_e^*(\beta_e)|q_{e2} \geq q_{e3}\}(> 0)$ increases monotonically with β_e. Furthermore, since $\Pr\{q_{e2} \geq q_{e3}\} = \frac{\beta_e}{\beta_e+1} > 0$ and $\frac{\beta_e}{\beta_e+1}$ also increases monotonically with β_e, it follows directly that $\mathbb{E}\{\xi_e^*(\beta_e)\}$ increases monotonically with β_e. Finally, due to the negative correlation between α_e and β_e, it is concluded that $\mathbb{E}\{\xi_e^*\}$ decreases monotonically with α_e.

The next step is to prove that the optimized covert rate, R_e^c, increases monotonically with α_e. From (37), we have $R_e^c = -R\Phi(c_e)f_e(d_e)$, where $d_e = c_e\phi_2/\phi_1$ and

$$\begin{aligned}\Phi(c_e) &= \frac{\lambda_{sr}\lambda_{jr}\mathrm{e}^{-c_e\sigma_r^2\lambda_{st}/\phi_1}}{c_eP\lambda_{st}+\lambda_{sr}} > 0,\\ f_e(d_e) &= \frac{\lambda\mathrm{e}^{\frac{\lambda\lambda_{jr}}{\lambda_{st}d_e}}\left(\mathrm{Ei}\left(-\frac{\lambda\lambda_{jr}}{\lambda_{st}d_e}\right)-\mathrm{Ei}\left(-\frac{\lambda(\lambda_{jr}+\lambda_{st}d_eW)}{\lambda_{st}d_e}\right)\right)}{d_e\lambda_{st}(1-\mathrm{e}^{-\lambda W})} < 0.\end{aligned} \tag{42}$$

To clarify the monotonicities of $\Phi(c_e)$ and $f_e(d_e)$ with respect to c_e and d_u, their first derivatives are separately given as

$$\Phi'(c_e) = -\frac{\lambda_{st}^2\lambda_{jr}(\sigma_r^2(c_eP\lambda_{st}+\lambda_{sr})/\phi_1+P)\mathrm{e}^{-c_e\sigma_r^2\lambda_{st}/\phi}}{(c_eP\lambda_{st}+\lambda_{sr})^2} < 0, \tag{43}$$

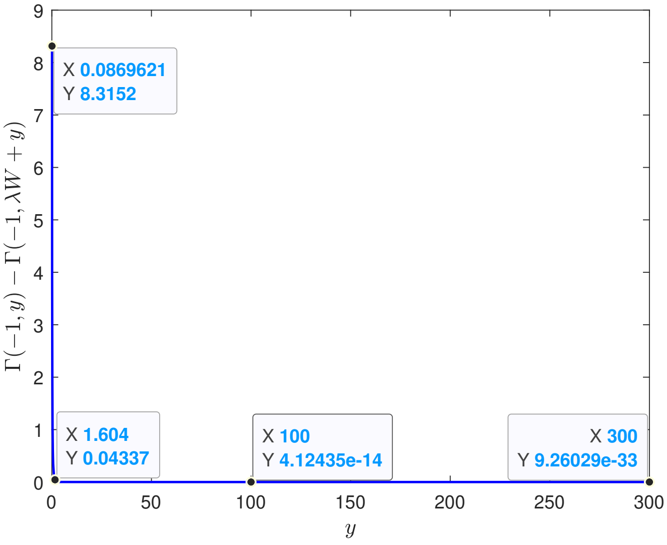


Fig. 11. Plot of $\Gamma(-1,y)-\Gamma(-1,\lambda W+y)$ as a function of y, for the case $\lambda W = 2$.

and

$$f_e'(d_e) = \frac{h(d_e)}{\lambda_{st}^2\left(1-\mathrm{e}^{-\lambda W}\right)d_e^3}, \tag{44}$$

respectively, where

$$\begin{aligned}h(d_e) \;&= \lambda\mathrm{e}^{\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}}(\lambda_{st}d_e+\lambda_{jr}\lambda)\Bigg(\mathrm{Ei}\left(-\frac{\lambda(\lambda_{jr}+\lambda_{st}Wd_e)}{\lambda_{st}d_e}\right)\\ &-\mathrm{Ei}\left(-\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}\right)+\lambda_{st}d_e\left(\frac{\lambda_{jr}\mathrm{e}^{-\lambda\left(\frac{\lambda_{jr}}{\lambda_{st}d_e}+W\right)}}{\lambda_{st}Wd_e+\lambda_{jr}}-\mathrm{e}^{-\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}}\right)\Bigg).\end{aligned} \tag{45}$$

To further determine its monotonicity, let

$$\begin{aligned}H(d_e) \;&= (\lambda_{st}d_e+\lambda_{jr}\lambda)\Bigg(\mathrm{Ei}\left(-\frac{(\lambda_{jr}+\lambda_{st}Wd_e)\lambda}{\lambda_{st}d_e}\right)\\ &-\mathrm{Ei}\left(-\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}\right)\Bigg)+\lambda_{st}d_e\left(\frac{\lambda_{jr}\mathrm{e}^{-\lambda\left(\frac{\lambda_{jr}}{\lambda_{st}d_e}+W\right)}}{\lambda_{st}Wd_e+\lambda_{jr}}-\mathrm{e}^{-\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}}\right)\end{aligned} \tag{46}$$

then

$$\begin{aligned}H'(d_e) \;&= -\frac{\lambda_{st}\mathrm{e}^{-\left(\frac{\lambda\lambda_{jr}}{\lambda_{st}d_e}+\lambda W\right)}}{(\lambda_{st}Wd_e+\lambda_{jr})^2}\Bigg((\lambda_{st}Wd_e+\lambda_{jr})^2\mathrm{e}^{\left(\frac{\lambda\lambda_{jr}}{\lambda_{st}d_e}+\lambda W\right)}\\ &\left(\mathrm{Ei}\left(-\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}\right)-\mathrm{Ei}\left(-\frac{(\lambda_{jr}+\lambda_{st}Wd_e)\lambda}{\lambda_{st}d_e}\right)\right)+\lambda_{st}\lambda_{jr}Wd_e\Bigg).\end{aligned} \tag{47}$$

Let $A = \frac{\lambda_{st}\mathrm{e}^{-\lambda\left(\frac{\lambda_{jr}}{\lambda_{st}d_e}+W\right)}}{(\lambda_{st}Wd_e+\lambda_{jr})^2} > 0$, $B = \mathrm{e}^{\lambda\left(\frac{\lambda_{jr}}{\lambda_{st}d_e}+W\right)} > 1$, $-C = \left(\mathrm{Ei}\left(-\frac{\lambda_{jr}\lambda}{\lambda_{st}d_e}\right)-\mathrm{Ei}\left(-\frac{(\lambda_{jr}+\lambda_{st}Wd_e)\lambda}{\lambda_{st}d_e}\right)\right) < 0$, then $H'(d_e) = -A\left(-BC(\lambda_{st}Wd_e+\lambda_{jr})^2+\lambda_{st}\lambda_{jr}Wd_e\right)$, and $H'(d_e) = ABC({\lambda_{jr}}^2+{d_e}^2{\lambda_{st}}^2W^2)-\lambda_{jr}\lambda_{st}Wd_e(1-2BC)A > 0$.

Since $H'(d_e) > 0$, it follows that $H(d_e)$ increases monotonically with d_e and satisfies $H(0) = 0$. Note that $h(d_e) > 0$ since $d_e > 0$, it indicates that $f_e'(d_e) > 0$, and $\Phi'(c_e) < 0$. These show that $f_e(d_e)$ monotonically increasing functions with d_e and $\Phi(c_e)$ monotonically decreasing functions with c_e. Combining this with (42), R_e^c decreases monotonically with c_e and d_e but increases with α_e due to its negative correlation with c_e and d_e. Considering that $\mathbb{E}\{\xi_e^*\}$ decreases monotonically with α_e, we can set the optimal reflection coefficient α_e^* as (35).

References

[1] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, “Ambient backscatter communications: A contemporary survey,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2889–2922, 4th Quart., 2018.

[2] F. Rezaei, D. Galappaththige, C. Tellambura, and S. Herath, “Coding techniques for backscatter communications–A contemporary survey,” *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1020–1058, 2nd Quart., 2023.

[3] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, “Ambient backscatter assisted wireless powered communications,” *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 170–177, Apr. 2018.

[4] W. Liu, Y. C. Liang, Y. Li, and B. Vucetic, “Backscatter multiplicative multiple-access systems: Fundamental limits and practical design,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5713–5728, Sep. 2018.

[5] Z. Chi, X. Liu, W. Wang, Y. Yao, and T. Zhu, “Leveraging ambient LTE traffic for ubiquitous passive communication,” in *Proc. ACM SIGCOMM*, Aug. 2020, pp. 172–185.

[6] F. Jameel, R. Duan, Z. Chang, A. Liljemark, T. Ristaniemi, and R. Jantti, “Applications of backscatter communications for healthcare networks,” *IEEE Netw.*, vol. 33, no. 6, pp. 50–57, Dec. 2019.

[7] X. Chen et al., “Covert communications: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2nd Quart., 2023.

[8] Y. Xu et al., “Robust secure beamforming design for multi-RIS-aided MISO systems with hardware impairments and channel uncertainties,” *IEEE Trans. Commun.*, vol. 73, no. 3, pp. 1517–1530, Mar. 2025.

[9] Y.-A. Xie et al., “Securing federated learning: A covert communication-based approach,” *IEEE Netw.*, vol. 37, no. 1, pp. 118–124, Jan. 2023.

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

[11] J. Liu, J. Yu, X. Chen, R. Zhang, S. Wang, and J. An, “Covert communication in ambient backscatter systems with uncontrollable RF source,” *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1971–1983, Mar. 2022.

[12] Y. Wang, S. Yan, W. Yang, Y. Huang, and C. Liu, “Energy-efficient covert communications for bistatic backscatter systems,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2906–2911, Mar. 2021.

[13] Y. Xie, T.-T. Chan, X. Zhang, P. Lai, and H. Pan, “Reflection-optimized covert communication for jammer-aided ambient backscatter systems,” in *Proc. IEEE GLOBECOM*, Dec. 2023, pp. 4277–4282.

[14] R. Kishore, S. Gurugopinath, P. C. Sofotasios, S. Muhaidat, and N. Al-Dhahir, “Opportunistic ambient backscatter communication in RF-powered cognitive radio networks,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 413–426, Jun. 2019.

[15] Y. Zhang, B. Li, F. Gao, and Z. Han, “A robust design for ultra-reliable ambient backscatter communication systems,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8989–8999, Oct. 2019.

[16] Y. Ye, L. Shi, X. Chu, and G. Lu, “On the outage performance of ambient backscatter communications,” *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7265–7278, Aug. 2020.

[17] G. Yang, Q. Zhang, and Y.-C. Liang, “Cooperative ambient backscatter communications for green Internet-of-Things,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1116–1130, Apr. 2018.

[18] W. Zhao, J. Zhu, X. She, G. Wang, and C. Tellambura, “Ergodic capacity analysis for cooperative ambient communication system under sensitivity constraint,” *IEEE Commun. Lett.*, vol. 27, no. 10, pp. 2822–2826, Oct. 2023.

[19] W. Ma, Y. Zhang, X. Zou, L. Yan, and T. Jiang, “Covert ambient backscatter communication against randomly distributed wardens,” *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 8238–8252, Jun. 2024.

[20] K. Shahzad and X. Zhou, “Covert communication in backscatter radio,” in *Proc. IEEE ICC*, May 2019, pp. 1–6.

[21] J. Liu, J. Yu, D. Niyato, R. Zhang, X. Gao, and J. An, “Covert ambient backscatter communications with multi-antenna tag,” *IEEE Trans. Wireless Commun.*, vol. 22, no. 9, pp. 6199–6212, Sep. 2023.

[22] W. Liu, X. Zhou, S. Durrani, and P. Popovski, “Secure communication with a wireless-powered friendly jammer,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[23] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y.-D. Yao, “Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks,” *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3482–3495, May 2019.

[24] N. Qi, Z. Su, W.-J. Wang, R. Yao, and T. A. Tsiftsis, “Cost-efficient wireless friendly jamming and interference mitigation: No pains, no gains,” *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 2252–2265, Feb. 2024.

[25] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

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

[27] B. Lyu, C. You, Z. Yang, and G. Gui, “The optimal control policy for RF-powered backscatter communication networks,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2804–2808, Mar. 2018.

[28] Z. Zhang, A. Chaaban, and L. Lampe, “Physical layer security in LiFi systems,” *Philosophical Transactions of the Royal Society A*, 2019.

[29] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*. New York, NY, USA: Springer, 2022.

[30] A. R. DiDonato, “An approximation for $\int_x^\infty e^{-t^2/2}\, t^p \, dt$, $x > 0$, p real,” *Mathematics of Computation*, vol. 32, no. 141, pp. 271—275, Jan. 1978.

Yuanai Xie (Member, IEEE) received the Ph.D. degree in control science and engineering from Yanshan University, Qinhuangdao, China, in 2022.

He is currently a lecturer in the College of Computer Science, South-Central Minzu University, Wuhan, China. Prior to this, he was a visiting Ph.D. Student with Nanyang Technological University, from 2021 to 2022. He was a Postdoctoral Research Fellow with the Department of Mathematics and Information Technology, The Education University of Hong Kong (EdUHK), from 2023 to 2024. His research interests include wireless resource optimization and physical layer security.

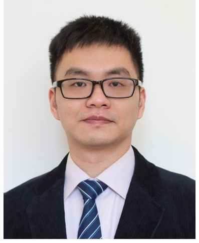
Yaoyao Wen received the bachelor’s degree from South-Central Minzu University, China, in 2023. She is currently pursuing the master’s degree in the School of Computer Science at the same university. Her research interests include resource allocation in covert communications, Internet of Things, and LLM-enabled reasoning.

Xiao Zhang (Member, IEEE) received the B.Eng. and M.Eng. degrees from the South-Central Minzu University, Wuhan, China, in 2009 and 2011 respectively, and the Ph.D. degree from Department of Computer Science in City University of Hong Kong, Hong Kong, 2016. He was a visiting scholar with Utah State University, Utah, USA and University of Lethbridge, Alberta, Canada. During 2016-2019, he was a Postdoc Research Fellow at Singapore University of Technology and Design. Currently, he is associate professor with the College of Computer Science, South-Central Minzu University, China. His research interests include wireless and UAV networking, algorithms design and analysis, and combinatorial optimization.

Pan Lai received the Ph.D. degree from the School of Computer Engineering, Nanyang Technological University, Singapore, in 2016.

He is currently an Associate Professor in the College of Computer Science, South-Central Minzu University, Wuhan, China. From 2016 to 2019, he was a Postdoctoral Research Fellow with the Singapore University of Technology and Design, Singapore. His research interests include resource allocation and scheduling algorithm design in computer and network systems, network economics, and machine learning. He has published many papers in TON, TNSE, INFOCOM, IPDPS, MASCOTS, GLOBECOM, etc.

Zhixin Liu (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in control theory and engineering from Yanshan University, Qinhuangdao, China, in 2000, 2003, and 2006, respectively. He is currently a Professor with the Department of Automation, School of Electrical Engineering, Yanshan University. He visited the University of Alberta, Edmonton, AB, Canada, from 2009 to 2010. He is the author or coauthor of more than 100 papers in technical journals and conference proceedings. His research interests include performance optimization and energy-efficient protocol design in wireless sensor networks, resource allocation in cognitive radio networks, and vehicular networks.



Haoyuan Pan (Member, IEEE) received the B.E. and Ph.D. degrees in Information Engineering from The Chinese University of Hong Kong (CUHK), Hong Kong, in 2014 and 2018, respectively.

He was a Post-Doctoral Fellow with the Department of Information Engineering, CUHK, from 2018 to 2020. He is currently an assistant professor with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. His research interests include wireless communications and networks, Internet of Things (IoT), semantic communications, and age of information (AoI). He received the Best Paper Award at IEEE Wireless Communications and Networking Conference (WCNC) 2024.

Tse-Tin Chan (Member, IEEE) received his B.Eng. (First Class Hons.) and Ph.D. degrees in Information Engineering from The Chinese University of Hong Kong (CUHK), Hong Kong SAR, China, in 2014 and 2020, respectively.

He is currently an Assistant Professor with the Department of Mathematics and Information Technology, The Education University of Hong Kong (EdUHK), Hong Kong SAR, China. Prior to this, he was an Assistant Professor with the Department of Computer Science, The Hang Seng University of Hong Kong (HSUHK), Hong Kong SAR, China, from 2020 to 2022. His research interests include wireless communications and networking, Internet of Things (IoT), age of information (AoI), and AI in wireless communications.