Reflection-Optimized Covert Communication for Jammer-Aided Ambient Backscatter Systems

Yuanai Xie*, Tse-Tin Chan†, Xiao Zhang*, Pan Lai*, Haoyuan Pan‡
* College of Computer Science, South-Central Minzu University, Wuhan 430074, China
† Department of Mathematics and Information Technology, The Education University of Hong Kong, Hong Kong SAR, China
‡ College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China
E-mails: xieyuan_ai@163.com, tsetinchan@eduhk.hk, xiao.zhang@my.cityu.edu.hk, plai1@ntu.edu.sg, hypan@szu.edu.cn

***Abstract*—The integration of Ambient Backscatter Communication (ABC) with covert communication is expected to support emerging Internet of Things (IoT) applications (e.g., Radio Frequency (RF)-powered networks) due to the need for low-cost connectivity and confidential transmission. In general, the purpose of covert communication is to hide the existence of the RF-powered wireless link to ensure the information security of the ABC link. However, the ABC link may have a high rate requirement, thus inevitably increasing the risk of information leakage. Hence, this paper considers jammer-aided endogenous covert communication, where an RF tag sends information covertly to an ABC receiver and exploits the jammer's Artificial Noise (AN) under the supervision of a warden-like legacy receiver. To obtain the maximum data rate of the backscatter link without being detected, we derive the minimum detection error rate of the warden and the outage probability of the backscatter link under random channel fading and the jammer's AN, respectively. Then, we optimize the tag's reflection coefficient to maximize its effective covert rate under the covert constraint based on the warden's mean detection error rate. Since the optimal reflection coefficient cannot be solved directly, monotonicity analyses of the objective and the constraint with respect to the reflection coefficient are adopted to achieve an efficient solution. Numerical results demonstrate the effectiveness of the optimized reflection coefficient for the jammer-aided system.**

***Index Terms*—Ambient backscatter, covert communication, effective covert rate, reflection coefficient.**

I. Introduction

To enable the sustainable Internet of Things (IoT) scenarios, e.g., Radio Frequency (RF)-powered networks [1-3], backscatter communication is deemed as a promising technique due to its ubiquitous connectivity, low cost, and considerable energy savings [4, 5]. Existing backscatter communication models can be classified into three categories: 1) monostatic, 2) bistatic, and 3) ambient [6]. Unlike the first two models requiring dedicated RF emitters, Ambient Backscatter Communication (ABC) has the advantages of minimal cost and manual maintenance due to the use of ambient signals (e.g., TV, cellular, and Wi-Fi signals). Moreover, ABC can achieve more ubiquitous communication, sensing, and computing for advanced and battery-free IoT applications [2, 7, 8], such as cell phones [2], motion sensing devices [7], and backscatter-tag assisted vehicular positioning systems [8].

The typical ABC system contains an RF Source (RFS), a tag, a Legacy Receiver (LR), and an ABC Receiver (AR). The system is always like an underlay cognitive radio network where the links of RFS-LR and Tag-AR are equivalent to the primary and secondary links, respectively. Due to the open and shared frequency bands, the backscatter link is more vulnerable to eavesdropping or malicious attacks from the LR, especially when the link's data rate is high. Hence, it is vital to consider and address this endogenous information security issue for ABC systems. Traditional security countermeasures are mainly encryption techniques and Physical Layer Security (PLS) [9]. Nevertheless, encryption techniques require high computation costs while PLS falls short of the higher security rating [9]. Hence, covert communication, which hides the existence of wireless transmission from the detection of wardens, is widely used to provide cost-effective and higher-level security. However, existing studies [10-13] consider an external warden excluded from the discussed system, and thus fails to involve the information security issue from covert communication-based endogenous ABC system. In this context, the tag's reflection coefficient optimization and extra covert techniques can be adopted to maximize its transmission rate without being detected by the inside warden (i.e., LR).

So far, there are few works about covert communication in backscatter system [10, 11]. In [10], the authors proposed a covert monostatic backscatter system, where the transmitter emits Artificial Noise (AN) signals with variable power to confuse the warden and avoid the detection, without considering the effects of channel fading and tag's reflection coefficient. Under these factors, the authors in [11] presented a new covert communication framework for bistatic backscatter systems, where the dedicated carrier signals with AN are used to support the tag's backscatter communication and degrade the warden's detection performance. However, the

This work was supported in part by the National Natural Science Foundation of China under Grant 61902437, in part by the Hubei Provincial Natural Science Foundation under Grants 2020CFB629 and 2023AFB202, in part by the Fundamental Research Funds for the Central Universities under Grant CZQ23016, in part by the Chunhui Program of Ministry of Education under Grant HZKY20220331, in part by the Research Start-up Funds of South-Central Minzu University under Grants YZZ18006 and YZY23001, and in part by the Faculty Development Scheme under Grant UGC/FDS14/E02/21 and the Research Matching Grant Scheme from the Research Grants Council of Hong Kong. *(Corresponding author: Xiao Zhang.)*

979-8-3503-1090-0/23/$31.00 © 2023 IEEE

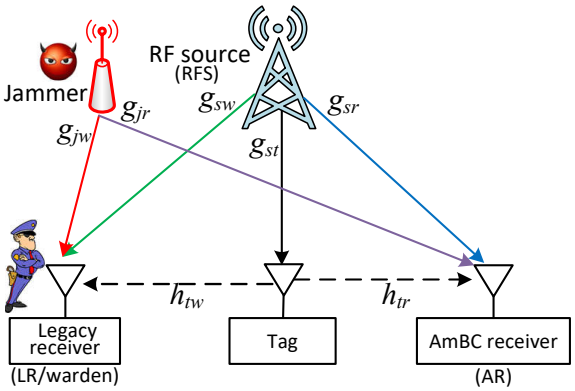

Fig. 1: Covert communication model for ambient backscatter systems.

time-variant AN from the transmitter or carrier emitter is costly and intractable, and it is impossible to design AN in ambient signals. Hence, it is more reasonable to consider a jammer with AN in the ABC system. In [12], the possibilities and conditions of covert communication in wireless fading channels are explored using the AN generated by a full-duplex receiver. Similar work can be found in [13] due to the highly controllable AN of full-duplex receiver. However, it is impractical to use the full-duplex enabled AR in the ABC system. Nevertheless, the optimized reflection coefficient of the tag can remedy the limitation of having no full-duplex receiver and balance the random jamming. Besides, channel fading can also be considered to determine the ABC system's reliability.

In this paper, we present a novel covert communication-based design for ABC systems, which is achieved by optimizing the tag's reflection coefficient to maximize the effective covert rate of the ABC link under a covert constraint. The key contributions of this paper are summarized as follows:

- We consider the tag's reflection coefficient optimization to maximize its data rate without being detected by the endogenous LR in the same system. To the best of our knowledge, this is the first exploration of the potential and practical case.
- We consider an extra covert design for the ABC system, where a cooperative jammer with an integrable uniformly distributed AN helps the ABC link to avoid being detected and ensure a secure information transmission.
- In light of the randomness in channel fading and jammer's AN, we derive the warden's detection error rate and the backscatter link's outage probability to evaluate the system's covertness and reliability. The reflection coefficient of the tag is optimized to maximize its effective covert rate under a covert constraint. Since the optimal reflection coefficient cannot be solved directly, we use monotonicity analyses for the formulated problem to achieve an efficient solution.

II. System Model and Detection Mechanism

A. System Model

As shown in Fig. 1, an ambient backscatter system with a jammer is considered. The Tag needs to send information covertly and passively to the AR by exploiting the jammer's AN and reflecting incident signals from RFS, while the warden-like LR with a radiometer tries to detect this covert link for its malicious purpose. Note that all the nodes are equipped with a single antenna, the AR can be replaced by an IoT device, and each time slot involves n channel use. Besides, the channel gain is assumed as a constant within one time slot but varies independently over different slots. The channel responses of RFS-LR, RFS-Tag, RFS-AR, Jammer-LR, Jammer-AR, Tag-LR, and Tag-AR links are denoted by g_{sw}, g_{st}, g_{sr}, g_{jw}, g_{jr}, h_{tw}, and h_{tr}, respectively. Considering that the Tag-AR link operates over a short distance and the LoS path of the channel is not blocked, h_{tr} is assumed to obey Rician fading dominated by a deterministic LoS component and a Rayleigh fading component. Given the worst-case perspective in [11], the LR is considered to be close to the Tag, and h_{tw} obeys the same fading model. Hence, the channel responses of Tag-AR and Tag-LR links can be formulated as

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

where $ij \in \{tr, tw\}$, k is the Rician factor, h_{ij}^{LoS} and h_{ij}^{NLoS} are the deterministic LoS component and the Rayleigh fading component, respectively [14]. Contrary to these links, we consider that the RFS and the Jammer are relatively far from other terminals, and these long-distance links have obvious multipath effects. Hence, g_{sw}, g_{st}, g_{sr}, g_{jw} and g_{jr} are assumed to obey Rayleigh fading, and their average channel gains are $1/\lambda_{kl}$, where $kl \in \{sw, st, sr, jw, jr\}$ [11].

The backscatter signal reflected by Tag is $\mathbf{x}(i) = \sqrt{\alpha P} g_{st} \mathbf{e}(i) \mathbf{s}(i)$, where $i = 1, 2, \ldots, n$ is the index of each channel use, α is Tag's reflection coefficient and P is RFS's transmit power. The reflected jammer signal from Tag is ignored due to the weak and random jamming signal strength at Tag. The i-th element of vector $\mathbf{e}$, i.e., $\mathbf{e}(i)$, is the signal emitted at RFS for the i-th channel use, while $\mathbf{s}(i)$ is the signal modulated at Tag. Note that $\mathbb{E}[\mathbf{e}(i)\mathbf{e}^*(i)] = 1$ and $\mathbb{E}[\mathbf{s}(i)\mathbf{s}^*(i)] = 1$. The received signal at AR is given by

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

where $\mathbf{j}(i)$ and J denote Jammer's AN for the i-th channel use and transmit power, respectively, satisfying $\mathbb{E}[\mathbf{j}(i)\mathbf{j}^*(i)] = 1$. $\mathbf{n}_r(i)$ is the additive white Gaussian noise (AWGN) at AR with power σ_r^2, $\phi \in [0, 1]$ is the interference cancellation coefficient, and $\phi = 0$ means the perfect interference cancellation [13, 15]. $\mathbf{x}(i)$, $\mathbf{e}(i)$ and $\mathbf{j}(i)$ are assumed as circularly symmetric complex Gaussian random variables [11].

B. Detection Mechanism at Warden (LR)

In this system, RFS, Jammer, Tag, and AR work cooperatively to hide the communication behavior between Tag and

AR from LR. Tag thus knows the distribution of Jammer's power in advance and can adjust its reflection coefficient α accordingly. The power P of RFS is fixed and publicly known by other terminals, while the AN power J varies from slot to slot and obeys an integrable uniform distribution in the interval $[0, \overline{J}]$ with Probability Density Function (PDF) given as

$$f_J(w) = \begin{cases} \frac{1}{\overline{J}}, & 0 \le w \le \overline{J}, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

From a conservative perspective, LR is considered to have the knowledge about g_{sw}, g_{jw} and h_{tw} in the involved slot, the randomness in Jammer's transmit power is introduced to create uncertainty in LR's received power. Then, LR is unsure whether an increase in the received power is caused by the backscatter communication link or the power fluctuation of Jammer's AN signal. Besides, given that LR can capture the synchronized information about backscatter communication, LR uses a binary hypothesis detection by observing the vector $\mathbf{y}_w(i)$ within a time slot [16], where Tag absorbs incident signals in the null hypothesis $\mathcal{H}_0$ while it reflects incident signals in the alternative hypothesis $\mathcal{H}_1$.

Under these hypotheses, the composite received signal at LR of the vector $\mathbf{y}_w$ for the i-th channel use is given by

$$\mathbf{y}_w(i) = \begin{cases} \sqrt{P} g_{sw}\mathbf{e}(i) + \sqrt{J} g_{jw}\mathbf{j}(i) + \mathbf{n}_w(i), & \mathcal{H}_0, \\ \sqrt{P} g_{sw}\mathbf{e}(i) + \sqrt{J} g_{jw}\mathbf{j}(i) + \mathbf{x}(i) h_{tw} + \mathbf{n}_w(i), & \mathcal{H}_1, \end{cases} \tag{4}$$

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

We consider the equal prior probability of $\mathcal{H}_0$ and $\mathcal{H}_1$ here. The detection error rate ξ, i.e., the sum of the false alarm and miss-detection rates, can be defined as,

$$\xi = P_{FA} + P_{MD}, \tag{5}$$

where $P_{FA} = \Pr\{D_1|\mathcal{H}_0\}$ and $P_{MD} = \Pr\{D_0|\mathcal{H}_1\}$ denote the false alarm and miss-detection rates, respectively. Due to the binary hypothesis detection, D_1 and D_0 represent the binary decisions that infer whether Tag reflects or not, respectively.

Combined with the Neyman-Pearson criterion and the Likelihood Ratio test [17], the optimal decision rule for LR to minimize his detection error is given by

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

where $P_w = \frac{1}{n}\sum_{i=1}^{n} |\mathbf{y}_w(i)|^2$ is the average power received at LR in a slot, and τ is the detection threshold (i.e., the tolerable interference energy limit) of LR. Based on the strong law of large numbers, an infinite number of channels, i.e., $n \to \infty$, is considered, thus

$$P_w = \begin{cases} P|g_{sw}|^2 + J|g_{jw}|^2 + \sigma_w^2, & \mathcal{H}_0, \\ P|g_{sw}|^2 + J|g_{jw}|^2 + \alpha P|g_{st}|^2|h_{tw}|^2 + \sigma_w^2, & \mathcal{H}_1. \end{cases} \tag{7}$$

III. Performance Optimization for ABC Link

In this section, both LR's minimal detection error rate and the backscatter communication outage probability are first derived to evaluate the ABC link's covertness and reliability, respectively. Accordingly, the data rate maximization problem is constructed and solved under the covert constraint derived from LR's mean detection error rate.

A. Minimal Detection Error Rate at Warden (LR)

Lemma 1. *The false alarm and miss-detection rates at LR for arbitrary detection threshold τ are determined by*

$$\begin{aligned} P_{FA}(\tau) &= \begin{cases} 1, & \tau < q_1, \\ 1 - \frac{\tau - q_1}{\overline{J}|g_{jw}|^2}, & q_1 \le \tau \le q_2, \\ 0, & \tau > q_2, \end{cases} \\ P_{MD}(\tau) &= \begin{cases} 0, & \tau < q_3, \\ \frac{\tau - q_3}{\overline{J}|g_{jw}|^2}, & q_3 \le \tau \le q_4, \\ 1, & \tau > q_4. \end{cases} \end{aligned} \tag{8}$$

where $q_1 = P|g_{sw}|^2 + \sigma_w^2$, $q_2 = P|g_{sw}|^2 + \overline{J}|g_{jw}|^2 + \sigma_w^2$, $q_3 = P(|g_{sw}|^2 + Q) + \sigma_w^2$, $Q = \alpha|g_{st}|^2|h_{tw}|^2$, $q_4 = P(|g_{sw}|^2 + Q) + \overline{J}|g_{jw}|^2 + \sigma_w^2$.

Proof. As per (7), the false alarm rate is determined by

$$\begin{aligned} P_{FA}(\tau) &= \Pr\{P|g_{sw}|^2 + J|g_{jw}|^2 + \sigma_w^2 > \tau\} \\ &= \begin{cases} 1, & \tau < q_1, \\ \Pr\{J > \frac{\tau - \sigma_w^2 - P|g_{sw}|^2}{|g_{jw}|^2}\}, & q_1 \le \tau \le q_2, \\ 0, & \tau > q_2. \end{cases} \end{aligned} \tag{9}$$

Similarly, the miss-detection rate is determined by

$$\begin{aligned} P_{MD}(\tau) &= \Pr\{P(|g_{sw}|^2 + Q) + J|g_{jw}|^2 + \sigma_w^2 < \tau\} \\ &= \begin{cases} 0, & \tau < q_3, \\ \Pr\{J < \frac{\tau - q_3}{|g_{jw}|^2}\}, & q_3 \le \tau \le q_4, \\ 1, & \tau > q_4, \end{cases} \end{aligned} \tag{10}$$

where the uniform PDF (i.e., $f_J(w)$) of J is used. □

From **Lemma 1**, we further derive the optimal value of the detection threshold τ.

Theorem 1. *LR's optimal detection threshold is given by*

$$\tau^* = \begin{cases} [q_2, q_3], q_2 < q_3, \\ [q_3, q_2], q_2 \ge q_3, \end{cases} \tag{11}$$

and the related minimal detection error rate is formulated as

$$\xi^* = \begin{cases} 0, & q_2 < q_3, \\ 1 - \frac{\alpha P|g_{st}|^2|h_{tw}|^2}{\overline{J}|g_{jw}|^2}, & q_2 \ge q_3. \end{cases} \tag{12}$$

Proof. Note that $q_1 < q_3$ and $q_4 \ge \max(q_2, q_3)$.

When $q_2 < q_3$, the detection error rate at warden (LR) is

$$\xi = \begin{cases} 1, & \tau < q_1, \\ 1 - \frac{\tau - q_1}{\overline{J}|g_{jw}|^2}, & q_1 \le \tau < q_2, \\ 0, & q_2 \le \tau \le q_3, \\ \frac{\tau - q_3}{\overline{J}|g_{jw}|^2}, & q_3 \le \tau \le q_4, \\ 1, & \tau > q_4. \end{cases} \tag{13}$$

Hence, it is easy for warden/LR to set $\tau \in [q_2, q_3]$ so that $\xi = 0$. In this case, $\alpha P|g_{st}|^2|h_{tw}|^2 > \overline{J}|g_{jw}|^2$, which detects the covert communication with probability one.

When $q_2 \ge q_3$, the detection error rate at warden/LR is

$$\xi = \begin{cases} 1, & \tau < q_1, \\ 1 - \frac{\tau - q_1}{\overline{J}|g_{jw}|^2}, & q_1 \le \tau < q_3, \\ 1 - \frac{\alpha P|g_{st}|^2|h_{tw}|^2}{\overline{J}|g_{jw}|^2}, & q_3 \le \tau \le q_2, \\ \frac{\tau - q_3}{\overline{J}|g_{jw}|^2}, & q_2 \le \tau \le q_4, \\ 1, & \tau > q_4. \end{cases} \tag{14}$$

Hence, $\xi = 1-\alpha P|g_{st}|^2|h_{tw}|^2/(\overline{J}|g_{jw}|^2)$ is a constant when $q_3 \le \tau \le q_2$. However, $\xi = 1-(\tau - q_1)/(\overline{J}|g_{jw}|^2)$ is strictly monotonically decreasing with τ at the condition of $q_1 \le \tau < q_3$. Also, $\xi = (\tau - q_3)/(\overline{J}|g_{jw}|^2)$ is monotonically increasing with τ when $q_2 \le \tau \le q_4$. Based on these, the minimal detection error rate ξ^* can be achieved when the optimal detection threshold $\tau^* = [q_3, q_2]$, where $\xi^* = 1-(\alpha P|g_{st}|^2|h_{tw}|^2)/(\overline{J}|g_{jw}|^2)$. □

Remark 1. *The noise variance at LR, i.e., σ_w^2 does not affect the minimal detection error rate, ξ^*, even if it is included in the optimal threshold of the radiometer. The minimal detection error rate, ξ^* is mainly determined by Tag's reflection coefficient α and the ratio of the RFS's power P to the maximal AN power $\overline{J}$, since as $\alpha \to 0$ or $P/\overline{J} \to 0$, $\xi^* \to 1$.*

B. Mean Detection Error Rate

Due to channel uncertainty, (12) shows two cases for minimal detection error rate of LR. Hence, we consider the mean value of ξ^* over both cases as the covert metric of the backscatter link. Accordingly, the covertness constraint can be formulated as $\mathbb{E}\{\xi^*\} \ge 1-\varepsilon$, where $\mathbb{E}\{\xi^*\}$ is mean detection error rate of LR and $\varepsilon \in [0,1]$ represents a predetermined covert threshold.

Theorem 2. *Under the optimal detection threshold τ^*, the mean detection error rate at LR is determined by*

$$\mathbb{E}\{\xi^*(\beta)\} = 1 - \beta^2 + \beta \ln \beta, \tag{15}$$

where $\beta \triangleq (\alpha P|h_{tw}|^2\lambda_{jw})/(\alpha P|h_{tw}|^2\lambda_{jw} + \lambda_{st}\overline{J}) \in (0,1)$.

Proof. Through (12), the mean ξ^* is determined by

$$\mathbb{E}\{\xi^*\} = \Pr\{q_2 < q_3\} \times 0 + \Pr\{q_2 \ge q_3\} \times \mathbb{E}\{\xi^* | q_2 \ge q_3\}. \tag{16}$$

Accordingly, we have

$$\begin{aligned} \Pr\{q_2 \ge q_3\} &= \Pr\left\{|g_{st}|^2 \le \tfrac{\overline{J}|g_{jw}|^2}{\alpha P|h_{tw}|^2}\right\} \\ &= \int_0^{+\infty}\int_0^{\frac{\overline{J}|g_{jw}|^2}{\alpha P|h_{tw}|^2}} f_{|g_{st}|^2}(x) f_{|g_{jw}|^2}(y) dxdy \\ &= \frac{\lambda_{st}\overline{J}}{\alpha P|h_{tw}|^2\lambda_{jw} + \lambda_{st}\overline{J}}, \end{aligned} \tag{17}$$

$$\begin{aligned} \mathbb{E}\{\xi^*|q_2 \ge q_3\} &= \mathbb{E}\left\{1 - \tfrac{\alpha P|g_{st}|^2|h_{tw}|^2}{\overline{J}|g_{jw}|^2} | q_2 \ge q_3\right\} \\ &= 1 + \frac{\alpha P|h_{tw}|^2\lambda_{jw}}{\lambda_{st}\overline{J}}\left\{\frac{\lambda_{st}\overline{J}}{\alpha P|h_{tw}|^2\lambda_{jw} + \lambda_{st}\overline{J}}\right. \\ &\quad \left. - \ln\left(1 + \tfrac{\lambda_{st}\overline{J}}{\alpha P|h_{tw}|^2\lambda_{jw}}\right)\right\}, \end{aligned} \tag{18}$$

and taking them into (16) completes the proof. □

C. Outage Probability at AR

Through (2), the signal-to-interference-plus-noise ratio (SINR) at AR is given by

$$\mathrm{SINR}_{ar} = \frac{\alpha P|g_{st}|^2|h_{tr}|^2}{\phi P|g_{sr}|^2 + \phi J|g_{jr}|^2 + \sigma_r^2}. \tag{19}$$

We consider that the transmission rate of the backscatter link is predetermined and denoted as R. In light of the randomness in $|g_{st}|^2$, $|g_{sr}|^2$, $|g_{jr}|^2$ and J, the link is easily interrupted with a certain outage probability when $C < R$, where C is the channel capacity of the backscatter link.

Lemma 2. *The outage probability of the ABC link is given by*

$$\theta = 1 - \lambda_{sr}\lambda_{jr}\mathrm{e}^{-b\lambda_{st}} \frac{\ln(c\overline{J}\lambda_{st} + \lambda_{jr}) - \ln(\lambda_{jr})}{c\overline{J}\lambda_{st}(cP\lambda_{st} + \lambda_{sr})}, \tag{20}$$

where $c = \mu\phi > 0$, $b = \mu\sigma_r^2 > 0$, and $\mu = \frac{2^R-1}{\alpha|h_{tr}|^2 P} > 0$.

Proof. The outage probability is given by

$$\begin{aligned} \theta &= \Pr\left\{\tfrac{\alpha P|g_{st}|^2|h_{tr}|^2}{\phi P|g_{sr}|^2 + \phi J|g_{jr}|^2 + \sigma_r^2} \le 2^R - 1\right\} \\ &= \int_0^{\overline{J}}\int_0^{+\infty}\int_0^{+\infty}\int_0^{M} f(x,y,z,w) dxdydzdw, \end{aligned} \tag{21}$$

where $f(x,y,z,w) = f_{|g_{st}|^2}(x) f_{|g_{sr}|^2}(y) f_{|g_{jr}|^2}(z) f_J(w)$ since these random variables $|g_{st}|^2$, $|g_{sr}|^2$, $|g_{jr}|^2$, and J are mutually independent. $f_{|g_{st}|^2}(x) = \lambda_{st}\mathrm{e}^{-\lambda_{st}x}$, $f_{|g_{sr}|^2}(y) = \lambda_{sr}\mathrm{e}^{-\lambda_{sr}y}$, $f_{|g_{jr}|^2}(z) = \lambda_{jr}\mathrm{e}^{-\lambda_{jr}z}$, and $M = cPy + cwz + b$. The closed-form expression of θ can be obtained by calculating the integral in (21). □

D. Optimal Reflection Coefficient α^* and Covert Rate

To maximize the effective covert rate of this system, which is subject to a certain covert constraint, we have

$$\begin{aligned} \max_{\alpha} \ & R_c \\ s.t. \ & \begin{cases} 0 < \alpha \le 1, \\ \mathbb{E}\{\xi^*\} \ge 1 - \varepsilon, \end{cases} \end{aligned} \tag{22}$$

where $R_c = R(1-\theta)$.

However, the optimal reflection coefficient α^* cannot be obtained directly for the problem in (22). Hence, the monotonicity of LR's mean detection error rates $\mathbb{E}\{\xi^*\}$ and the effective covert rate R_c with respect to the reflection coefficient α is analyzed in Appendix A. According to **Theorems 3**, the optimal coefficient α^* to achieve the maximal covert rate under a given covertness threshold ε can be solved efficiently.

Theorem 3. *With known RFS's power P and Jammer's power distribution, the optimal coefficient α^* to achieve the maximal covert rate under a given covertness threshold ε is given by*

$$\alpha^* = \min\left\{\frac{\lambda_{st}\overline{J}\beta_\varepsilon}{(1-\beta_\varepsilon)P|h_{tw}|^2\lambda_{jw}}, 1\right\} \tag{23}$$

and the maximal covert rate is determined by

$$R_c = R\lambda_{sr}\lambda_{jr}\mathrm{e}^{-\mu^*\sigma_r^2\lambda_{st}} \frac{\ln(\mu^*\phi\overline{J}\lambda_{st} + \lambda_{jr}) - \ln(\lambda_{jr})}{\mu^*\phi\overline{J}\lambda_{st}(\mu^*\phi P\lambda_{st} + \lambda_{sr})}, \tag{24}$$

where $\mu^* = \max\left\{\frac{(2^R-1)(1-\beta_\varepsilon)|h_{tw}|^2\lambda_{jw}}{\beta_\varepsilon|h_{tr}|^2\overline{J}\lambda_{st}}, \frac{2^R-1}{|h_{tr}|^2 P}\right\}$, and β_ε is the solution of $\mathbb{E}\{\xi^*(\beta)\} = 1-\varepsilon$ for β, and $\mathbb{E}\{\xi^*(\beta)\}$ is formulated as (15)*.*

Proof. Please refer to the Appendix A. □

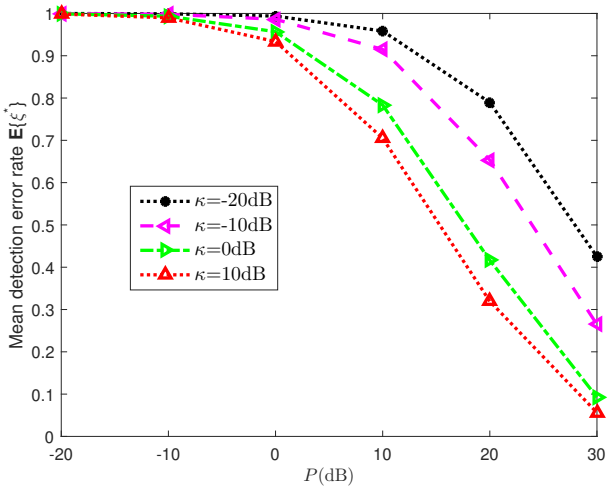

Fig. 2: Mean detection error rate $\mathbb{E}\{\xi^*\}$ vs. P, where $\overline{J} = -10dB$ and $\alpha = 0.5$.

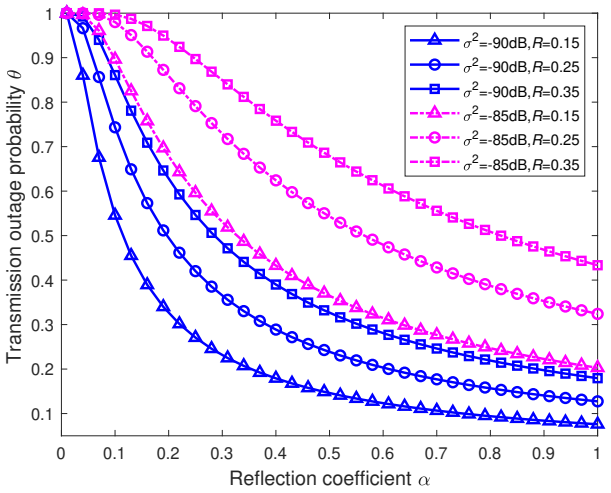

Fig. 3: Outage probability θ vs. α, where $\overline{J} = 0dB$ and $P = 30dB$.

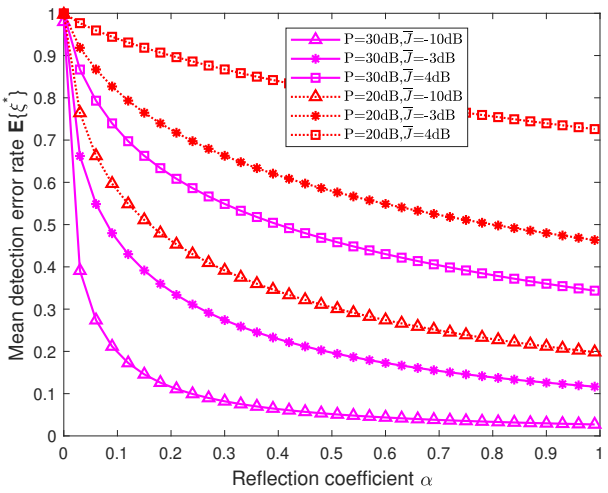

Fig. 4: Mean detection error rate $\mathbb{E}\{\xi^*\}$ vs. α.

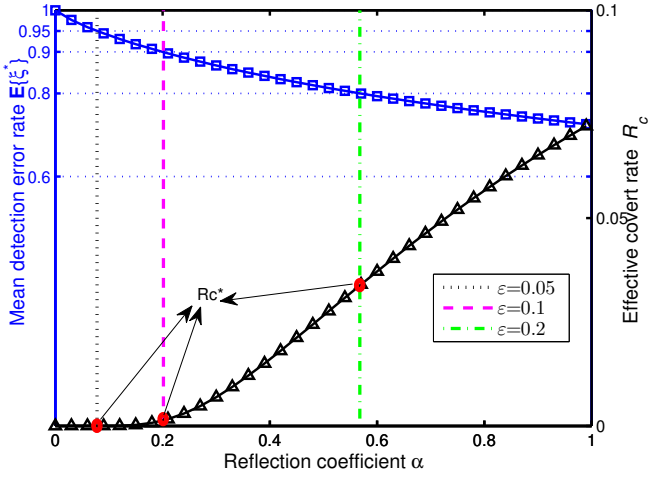

Fig. 5: $\mathbb{E}\{\xi^*\}$ and R_c vs. α under various thresholds ε.

IV. Numerical Results and Analysis

The large-scale channel fading model in [11] is considered. We have $|h_{ij}^{\mathrm{LoS}}|^2 = K^2 G_{ij} d_{ij}^{-\nu}$ and $1/\lambda_{ab} = K^2 G_{ab} d_{ab}^{-\varphi}$, where $ab \in \{ij, kl\}$, $|h_{ij}^{\mathrm{NLoS}}|^2 \sim \mathrm{Exp}(\lambda_{ij})$, and $K = \lambda/4\pi$ is a constant depending on the carrier wavelength λ, ν and φ denote the path loss exponents of LoS and non-LoS links, respectively. G_{ab} and d_{ab} are the antenna gain and the distance between the transmitting node a and the receiving node b, respectively. Besides, we set the cancellation coefficient as $\phi = 0.01$, the carrier frequency as 915 MHz, $\nu = 2$ and $\varphi = 4$, $d_{st} = d_{sr} = d_{sw} = 100$ m, $d_{jr} = d_{jw} = 80$ m, $d_{tw} = 5$ m, and $d_{tr} = 1$ m.

When the maximal AN power $\overline{J} = -10dB$ and the reflection coefficient $\alpha = 0.5$, Fig. 2 reveals LR's mean detection error rates (i.e., $\mathbb{E}\{\xi^*\}$) are monotonically decreasing with the powers of RFS (i.e., P) under different Rician factor κ. However, the power of RFS is pre-fixed. According to (23), it is necessary to optimize tag's reflection coefficient to guarantee an efficient covertness of the ABC link. Besides, we also observe that $\mathbb{E}\{\xi^*\}$ decreases with an increase in κ. This is because the deterministic LoS component is increasing with the Rician factor κ, which leads to a higher information leakage power level compared to the reduced power level of the random Rayleigh fading component. This fact also illustrates that the multipath communication environment is more suitable for covert communication.

Fig. 3 shows the relationship between the transmission outage probability θ and α under different values of R and σ_r^2. In fact, the result further demonstrates that the outage probability θ is a monotonically decreasing function of α. The reason is that the increase in α yields a better quality of the backscatter link, which can be more robust to combat the fluctuant interference. Also, Fig. 3 illustrates that θ increases with the preset rate R and AR's noise power σ_r^2.

Fig. 4 depicts $\mathbb{E}\{\xi^*\}$ is monotonically decreasing with α under different values of P and $\overline{J}$. Besides, it is observed that the increase in $\overline{J}$ leads to a higher mean detection error rate at LR, while the increase in P causes a lower detection error rate. The reason is that the random jamming power generating the AN hinders LR's detection process, but the increase in RFS's

fixed power raises the probability of the backscatter link being exposed. The result also shows that the covert transmission can hardly be detected (i.e., $\mathbb{E}\{\xi^*\} \to 1$) when $\alpha \to 0$. Specially, Fig. 4 shows $\mathbb{E}\{\xi^*\} \to 1$ when the maximal AN power $\overline{J}$ is large enough.

Although Figs. 3 and 4 demonstrate the monotonic relationships between θ and α, and between $\mathbb{E}\{\xi^*\}$ and α, respectively, these relationships are split and fail to determine the optimality of α. Hence, Fig. 5 shows the achievable effective covert rate R_c versus α under various thresholds ε. In this figure, we observe that R_c is monotonically increasing with α while $\mathbb{E}\{\xi^*\}$ has the opposite trend. This fact eventually leads to an obvious solution (i.e., α^* in (23)), and the maximal effective covert rate R_c^* can be determined by the intersection points circled in the figure. Besides, Fig. 5 indicates the lower threshold ε brings a lower optimal covert rate R_c^* and a smaller optimal reflection coefficient α^*. If ε is specified to be big enough (e.g., $\varepsilon = 0.4$), $\alpha^* = 1$ due to its boundary restriction, the corresponding R_c^* reaches the upper bound of R_c. In summary, these results validate **Theorems 2** and **3**.

V. Conclusion

This paper studied the potential use of covert communications for ABC systems with the help of the AN generated by a jammer. To evaluate the ABC link's covertness and reliability, the warden's minimal detection error rate and the link's outage probability were derived, respectively. Then, we formulated a covert constraint of the ABC link based on the warden's mean detection error rate. Under the covert constraint, the tag's reflection coefficient was optimized to maximize its effective covert rate. The numerical results validated the achievability of this ABC system. Also, our analysis demonstrated that the ABC link requires a trade-off between its covert rate and the covertness of its information transmission.

Appendix A
Proof of Theorem 3

The first and second derivatives of $\mathbb{E}\{\xi^*(\beta)\}$ are $\mathbb{E}\{\xi^*(\beta)\}' = -2\beta + \ln\beta + 1$, $\mathbb{E}\{\xi^*(\beta)\}'' = -2 + \frac{1}{\beta}$, respectively. Hence, the maximal value of $\mathbb{E}\{\xi^*(\beta)\}'$ is $\mathbb{E}\{\xi^*(1/2)\}' = -\ln 2 < 0$, which demonstrates that $\mathbb{E}\{\xi^*(\beta)\}$ monotonically decreases with β. Hence, $\mathbb{E}\{\xi^*\}$ monotonically decreases with α due to the positive correlation between α and β. Then, we can prove that the optimized covert rate, R_c, monotonically increases with α. From (20), we have $R_c = R\lambda_{sr}\lambda_{jr}g(c)f(c)$, where

$$\begin{aligned} g(c) &= \tfrac{\mathrm{e}^{-c\sigma^2\lambda_{st}/\phi}}{cP\lambda_{st}+\lambda_{sr}} > 0, \\ f(c) &= \tfrac{\ln(c\overline{J}\lambda_{st}+\lambda_{jr})-\ln(\lambda_{jr})}{c\overline{J}\lambda_{st}} > 0. \end{aligned} \tag{25}$$

To obtain the monotonicities of $g(c)$ and $f(c)$ with respect to c, their first derivatives are separately given as

$$\begin{aligned} g'(c) &= -\tfrac{\lambda_{st}(\sigma^2(cP\lambda_{st}+\lambda_{sr})/\phi+P)\mathrm{e}^{-c\sigma^2\lambda_{st}/\phi}}{(cP\lambda_{st}+\lambda_{sr})^2} < 0, \\ f'(c) &= \tfrac{\frac{c\overline{J}\lambda_{st}}{c\overline{J}\lambda_{st}+\lambda_{jr}}-\ln(c\overline{J}\lambda_{st}+\lambda_{jr})+\ln(\lambda_{jr})}{c^2\overline{J}\lambda_{st}} = \tfrac{m(c)}{c^2}. \end{aligned} \tag{26}$$

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

$$m'(c) = -\frac{c\overline{J}\lambda_{st}}{(c\overline{J}\lambda_{st}+\lambda_{jr})^2} \le 0. \tag{27}$$

Note that $m'(c) < 0$ since $c > 0$, it indicates that $m(c)$ monotonically decreases with c. We have $m(c) < m(0) = 0$, $f'(c) < 0$, and $g'(c) < 0$. These show that both $f(c)$ and $g(c)$ are monotonically decreasing functions with c. Combining with (25), R_c monotonically decreases with c but increases with α due to the negative correlation between α and c. Given the fact that $\mathbb{E}\{\xi^*\}$ monotonically decreases with α, the optimal reflection coefficient α^* can be set as (23).

References

[1] S. Gollakota, M. S. Reynolds, J. R. Smith, and D. J. Wetherall, "The emergence of RF-powered computing," *Computer*, vol. 47, no. 1, pp. 32–39, Jan. 2014.

[2] G. Maselli, M. Pietrogiacomi, M. Piva, and J. A. Stankovic, "Battery-free smart objects based on RFID backscattering," *IEEE Internet Things Mag.*, vol. 2, no. 3, pp. 32–36, Sep. 2019.

[3] C. Shao, H. Roh, and W. Lee, "Next-generation RF-powered networks for Internet of Things: Architecture and research perspectives," *J. Netw. Comput. Appl.*, vol. 123, pp. 23–31, Dec. 2018.

[4] X. Guo *et al.*, "Efficient ambient LoRa backscatter with on-off keying modulation," *IEEE/ACM Trans. Netw.*, vol. 30, no. 2, pp. 641–654, Apr. 2022.

[5] 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.

[6] 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.

[7] X. Li, H. Tang, G. Hu, B. Zhao, and J. Liang, "ViPSN-pluck: A transient-motion-powered motion detector," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3372–3382, Mar. 2022.

[8] K. Han, S.-W. Ko, S. Lee, W.-S. Ko, and K. Huang, "Joint frequency-and-phase modulation for backscatter-tag assisted vehicular positioning," in *Proc. IEEE SPAWC*, Jul. 2019, pp. 1–5.

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

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] J. Hu, Y. Wu, R. Chen, F. Shu, and J. Wang, "Optimal detection of UAV's transmission with beam sweeping in covert wireless networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1080–1085, Jan. 2020.

[17] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*, 4th ed. New York: Springer, 2022.