Secrecy Performance of Backscatter Communications With Multiple Self-Powered Tags

Zhipeng Liu, Yinghui Ye, *Member, IEEE*, Xiaoli Chu, *Senior Member, IEEE*, and Haijian Sun, *Member, IEEE*

***Abstract*— Backscatter communication (BackCom) networks are vulnerable to eavesdropping, while its secrecy performance has not been sufficiently studied. In this letter, we propose a tag selection strategy to optimize the ergodic secrecy capacity (ESC) and the secrecy outage probability (SOP) simultaneously for a multi-tag self-powered BackCom network in the presence of an eavesdropper. Concretely, an adaptive power reflection coefficient scheme is first designed to maximize the instantaneous secrecy capacity per tag, based on which the one with the highest secrecy capacity is selected to backscatter message. To evaluate the resulting secrecy performance, we first obtain the exact cumulative distribution function of the instantaneous secrecy capacity under independent but non-identically distributed Nakagami-m fading channels, and then derive the ESC and the SOP, respectively. Simulation results validate the theoretical analyses and demonstrate that the proposed strategy is superior to the existing strategies.**

***Index Terms*— Backscatter communications, ergodic secrecy capacity, physical layer security, secrecy outage probability.**

I. INTRODUCTION

A. Background

OWING to its ultralow power and low cost, backscatter communication (BackCom) has been identified as a promising paradigm for supporting green Internet-of-Things (IoT) [1]. However, BackCom signals are susceptible to wiretapped threats from eavesdroppers due to its broadcast nature, thus the secrecy issue of BackComs cannot be ignored. Despite there are some theoretical foundations for establishing secure transmission in other scenarios, e.g., the cooperative relaying [2], the distinct communication framework and the multiplicative channel characteristic of BackCom make it impossible to apply them, and pose extreme challenges for investigating the secrecy performance improvement [3], [4], [5], [6].

In [3], the authors considered a monostatic BackCom network with an eavesdropper, and derived the secrecy outage probability (SOP) by considering the channel correlation between the forwarding and backscattering links. For a non-orthogonal multiple access based ambient BackCom network, Li *et al.* [4] investigated the intercept and outage probabilities of the eavesdropper and the licensed users, respectively. The intercept and outage probabilities were derived for a cognitive BackCom network [5]. In contrast to [3], [4], [5], the authors in [6] jointly considered the energy harvesting (EH) and the power consumption at each tag in a self-powered BackCom network with multiple tags, where a tag selection strategy is proposed to maximize the power of the backscattered signal, subject to the energy-causality constraint, i.e., the harvested energy at a tag must be sufficient for powering its circuit operation.

B. Motivation and Contribution

Maximizing the power of the backscattered signal can improve the SOP of BackCom networks [6], but it might have a sid-effect on the instantaneous secrecy capacity. Concretely, when the channel conditions of backscattering links are poor, the secrecy capacities of tags may be negative and monotonously decreasing as the power of the backscattered signal increases. While not affecting the SOP, this effect might degrade the ergodic secrecy capacity (ESC), which is an important performance metric to characterize the average secrecy capacity of a BackCom network but was ignored in the existing works (see [3], [4], [5], [6] and reference therein).

Inspired by the above, this letter develops and analyzes a tag selection strategy that can maximize the ESC and minimize the SOP simultaneously for a BackCom network with multiple self-powered tags, where the destination node and the eavesdropper are equipped with multiple antennas. The main contributions of this work are listed as follows. We first design an adaptive power reflection coefficient (PRC) scheme that optimizes the PRC of each tag based on the instantaneous channel state information (CSI) to maximize its instantaneous secrecy capacity under the energy-causality constraint. Then, we propose a tag selection strategy that selects the tag with the highest secrecy capacity to backscatter message to the destination. Furthermore, we analytically evaluate the ESC and the SOP of the proposed tag selection strategy under independent but non-identically distributed (i.n.i.d.) Nakagami-m channel fading. Finally, simulation results reveal the effects of multitudinous network parameters on the secrecy performance and manifest the superiority of the proposed strategy.

II. SYSTEM MODEL

As illustrated in Fig. 1, we consider a passive BackCom network, including one dedicated radio frequency (RF) source

---

Manuscript received 22 July 2022; accepted 14 August 2022. Date of publication 23 August 2022; date of current version 12 December 2022. The work of Zhipeng Liu was supported by BUPT Excellent Ph.D. Students Foundation under Grant CX2022106. The work of Yinghui Ye was supported by the National Natural Science Foundation of China under Grant 62201451. The work of Haijian Sun was supported by the U.S. National Science Foundation under Grant CNS-2153428. The associate editor coordinating the review of this letter and approving it for publication was C. Kundu. *(Corresponding author: Yinghui Ye.)*

Zhipeng Liu is with the Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: zhipeng_liu_steve@163.com).

Yinghui Ye is with the Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications, Xi'an 710122, China (e-mail: connectyyh@126.com).

Xiaoli Chu is with the Department of Electronic and Electrical Engineering, The University of Sheffield, Sheffield S10 2TN, U.K. (e-mail: x.chu@sheffield.ac.uk).

Haijian Sun is with the School of Electrical and Computer Engineering, The University of Georgia, Athens, GA 30602 USA (e-mail: hsun@uga.edu).

Digital Object Identifier 10.1109/LCOMM.2022.3201031

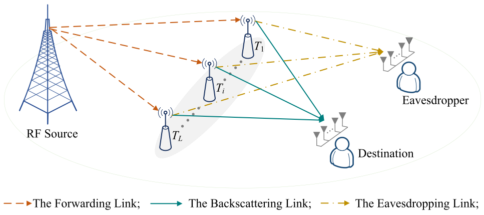

Fig. 1. System model of the studied BackCom network.

S equipped with a single antenna,[1] one destination node D with $N \geq 1$ antenna(s), one eavesdropper node E with $M \geq 1$ antenna(s), and L tags $\{T_i\}_{i=1}^{L}$. The tag encodes information to the signal transmitted by S and backscatters the modulated signal to D, while harvesting energy from S to sustain its operation. To reduce the communication overhead and enhance the secrecy transmission, we consider the opportunistic tag selection, where only one tag is selected for backscattering information to D in each transmission block.

We assume that all channels are quasi-static and follow i.n.i.d. Nakagami-m fading. Let $f_i \sim Naka\left(m_{s,i}, \Omega_{s,i}\right)$ denote the channel coefficient of the $S \rightarrow T_i$ link (i.e., the forwarding link), where $m_{s,i}$ and $\Omega_{s,i}$ represent the fading severity parameter and average power of the Nakagami random variable f_i, respectively, $i \in \{1, \ldots, L\}$. Moreover, the n-th ($n = 1, 2, \ldots, N$) element of the $T_i \rightarrow D$ (i.e., the backscattering link) channel fading vector $\mathbf{g}_i$ is given by $g_{i,n} \sim Naka\left(m_{d,i}, \Omega_{d,i}\right)$, and the m-th ($m = 1, 2, \ldots, M$) element of the $T_i \rightarrow E$ (i.e., the eavesdropping link) channel fading vector $\mathbf{h}_i$ is given by $h_{i,m} \sim Naka\left(m_{e,i}, \Omega_{e,i}\right)$, where $m_{d,i}$ ($m_{e,i}$) and $\Omega_{d,i}$ ($\Omega_{e,i}$) represent the fading severity parameter and average power of the variable $g_{i,n}$ ($h_{i,m}$), respectively.

For T_i, the received signal from S can be written as $y_i = f_i x_s$, where x_s is the signal transmitted by S with $\mathbb{E}\left\{|x_s|^2\right\} = P_s$ being the source transmit power. Then, by virtue of a PRC β_i $(0 \leq \beta_i \leq 1)$ that can separate the received signal into two parts [8], T_i uses $\sqrt{\beta_i} y_i$ for backscattering message and the rest for EH. Due to the nonlinearity of components involved in the EH module, we consider a nonlinear EH model [8], and the total energy harvested at T_i can be calculated as

$$P_i = P_i^{\max}\left(1 - e^{-\varphi_i^{(1)} P_i^r + \varphi_i^{(1)}\varphi_i^{(0)}}\right) \Big/ \left(1 + e^{-\varphi_i^{(1)} P_i^r + \varphi_i^{(1)}\varphi_i^{(2)}}\right), \quad (1)$$

where $P_i^{\max}$ denotes the saturated power at T_i, $P_i^r = (1-\beta_i) P_s |f_i|^2$ is the input power for EH at T_i, $\varphi_i^{(0)}$ represents the EH circuit sensitivity threshold, $\varphi_i^{(1)}$ and $\varphi_i^{(2)}$ are two fixed parameters of the EH module determined by the resistance, capacitance, etc.

Let P_i^c represent the circuit power consumption of T_i. Only if $P_i \geq P_i^c$, then T_i is activated and can backscatter the information to D. In this case, the destination node D performs maximum ratio combining (MRC) across its N antennas on the received signal from T_i and obtains

$$y_{d,i} = \sqrt{\eta_i \beta_i} f_i \mathbf{w}_{d,i}^{\dagger} \mathbf{g}_i x_s c_i + n_{d,i}, \quad (2)$$

where η_i represents the backscattering efficiency, $\mathbf{w}_{d,i}^{\dagger} = \mathbf{g}_i^{\dagger} / \|\mathbf{g}_i\|$ denotes the receive beamforming weight vector at D with conjugation operation $(\cdot)^{\dagger}$ and l_2-norm operation $\|\cdot\|$, c_i represents the desirable signal of T_i with $\mathbb{E}\left\{|c_i|^2\right\} = 1$, and $n_{d,i} \sim CN\left(0, \sigma^2\right)$ is the additive white Gaussian noise (AWGN) at D.

According to (2), the signal-to-noise ratio (SNR) at D from the $T_i \rightarrow D$ link can be written as

$$\gamma_i^d = \eta_i \beta_i P_s |f_i|^2 \left\|\mathbf{w}_{d,i}^{\dagger} \mathbf{g}_i\right\|^2 / \sigma^2. \quad (3)$$

Likewise, the SNR at E from the $T_i \rightarrow E$ link is given as

$$\gamma_i^e = \eta_i \beta_i P_s |f_i|^2 \left\|\mathbf{w}_{e,i}^{\dagger} \mathbf{h}_i\right\|^2 / \sigma^2, \quad (4)$$

where $\mathbf{w}_{e,i}^{\dagger} = \mathbf{h}_i^{\dagger} / \|\mathbf{h}_i\|$ denotes the receive beamforming weight vector at E.

Based on (3) and (4), the instantaneous secrecy capacity of the $S - T_i - D$ link can be calculated as [9]

$$C_i^s = \log_2\left(\frac{\eta_i \beta_i P_s |f_i|^2 \left\|\mathbf{w}_{d,i}^{\dagger} \mathbf{g}_i\right\|^2 + \sigma^2}{\eta_i \beta_i P_s |f_i|^2 \left\|\mathbf{w}_{e,i}^{\dagger} \mathbf{h}_i\right\|^2 + \sigma^2}\right). \quad (5)$$

III. TAG SELECTION STRATEGY AND SECRECY PERFORMANCE ANALYSES

A. Tag Selection Strategy

In this section, we propose a tag selection strategy[2] for optimizing the ESC and the SOP simultaneously, where an adaptive PRC scheme is first designed to maximize the instantaneous secrecy capacity of each tag, and then the one with the highest secrecy capacity is selected to carry out BackCom. Toward this end, Theorem 1 is introduced in what follows.

Theorem 1: The optimal PRC of tag T_i that maximizes its instantaneous secrecy capacity and the corresponding maximum secrecy capacity can be obtained respectively as

$$\beta_i^* = \begin{cases} 0, & |f_i|^2 > \frac{\Phi_i}{P_s} \ \& \ \left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 \leq \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2 \\ & \text{or } |f_i|^2 \leq \frac{\Phi_i}{P_s}, \\ 1 - \frac{\Phi_i}{P_s |f_i|^2}, & |f_i|^2 > \frac{\Phi_i}{P_s} \ \& \ \left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 > \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2, \end{cases} \quad (6)$$

and

$$C_i^{s^*} = \begin{cases} 0, & |f_i|^2 > \frac{\Phi_i}{P_s} \ \left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 \leq \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2 \\ & \text{or } |f_i|^2 \leq \frac{\Phi_i}{P_s}, \\ \log_2\left(1 + \frac{\eta_i \left(P_s |f_i|^2 - \Phi_i\right)\left(\left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 - \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2\right)}{\eta_i \left(P_s |f_i|^2 - \Phi_i\right)\left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2 + \sigma^2}\right), \\ |f_i|^2 > \frac{\Phi_i}{P_s} \ \left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 > \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2, \end{cases} \quad (7)$$

where $\Phi_i = \ln\left(P_i^{\max} e^{\varphi_i^{(1)}\varphi_i^{(0)}} + P_i^c e^{\varphi_i^{(1)}\varphi_i^{(2)}} / \left(P_i^{\max} - P_i^c\right)\right) / \varphi_i^{(1)}$.

Proof: See Appendix A.

Remark 1: Using Theorem 1, the optimal tag can be determined by the following process. First, the subset of tags that meet the energy-causality constraint is identified as $\mathcal{S}_1 = \left\{T_i \,\middle|\, |f_i|^2 > \frac{\Phi_i}{P_s}, 1 \leq i \leq L\right\}$. Then, within $\mathcal{S}_1$,

---

[1] Since the joint design for the transmit beamforming at S and the PRC per tag is extremely challenging, we focus on the dynamic PRC design in the proposed tag selection strategy via assuming S with a single antenna [7].

[2] Our work and existing EH-based relay selection strategies (see [2] and reference therein) are oriented towards the BackCom and cooperative communication respectively. Besides, the proposed strategy considers the dynamic PRC optimization that does not appear in the above relay selection strategies.

a further subset of tags that each sees a stronger backscattering link than an eavesdropping link is identified as $\mathcal{S}_2 = \left\{T_i \left| \left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 > \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2, T_i \in \mathcal{S}_1 \right.\right\}$. Finally, the tag that has the largest secrecy capacity among all the tags in $\mathcal{S}_2$ is selected to backscatter information, viz., $T_{i^*} = \arg\max_{T_i \in \mathcal{S}_2} C_i^{s^*}$. Especially, the instantaneous secrecy capacity of the studied network is obtained as $C_s = \max_{T_i \in S_2} C_i^{s^*}$.

Remark 2: Our proposed tag selection strategy is advantageous to that proposed in [6] and the reasons are as follows. The authors in [6] maximized the power of the backscattered signal per tag while satisfying the energy-causality constraint, and then selected the tag with the largest secrecy capacity to convey message. Nevertheless, according to [6, eq. (6)], the secrecy capacity achieved by the selected tag may be negative in [6] because the tag selection did not consider the backscattering link's channel quality with respect to that of the eavesdropping link. On the contrary, in our proposed tag selection strategy, if the energy-causality constraint is not satisfied or the corresponding backscattering link is worse than the eavesdropping link, the tag T_i remains silent, i.e., $C_i^{s^*} = 0$, as shown in (6) and (7); otherwise, $C_i^{s^*} > 0$ holds, in this case, our strategy maximizes the secrecy capacity of T_i. Accordingly, the selected tag makes the instantaneous secrecy capacity non-negative. Although the above difference between our proposed strategy and the one of [6] has no impact on the SOP, the ESC achieved by our proposed strategy is larger than that of [6], as verified by our simulation results in Section IV.

B. Secrecy Performance

In this work, we consider multiple antennas for D and E, and the Nakagami-m channel fading for reflecting the more degrees-of-freedom of practical propagation environments. This makes our considered model more general than [6] with single antenna and Rayleigh fading. Moreover, in contrast to [6] studying only the SOP, this subsection aims to evaluate the SOP and ESC of the proposed tag selection strategy.

Referring to [10], the ESC can characterize the stochastic C_s averaged over all fading states, given by

$$C_{er} = \mathbb{E}\left[C_s\right] \triangleq \mathbb{E}\left[\max_{1\le i\le L} C_i^{s^*}\right] = \mathbb{E}\left[\log_2\left(1 + \max_{1\le i\le L} \gamma_i^{s^*}\right)\right]. \quad (8)$$

When $|f_i|^2 > \frac{\Phi_i}{P_s}$ and $\left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 > \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2$, $\gamma_i^{s^*} = \frac{\eta_i\left(P_s|f_i|^2 - \Phi_i\right)\left(\left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 - \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2\right)}{\eta_i\left(P_s|f_i|^2 - \Phi_i\right)\left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2 + \sigma^2}$; otherwise, $\gamma_i^{s^*} = 0$.

Letting $\gamma_s = \max_{1\le i\le L} \gamma_i^{s^*}$, we rewrite (8) as

$$C_{er} = \int_0^{\infty} \log_2(1+u) f_{\gamma_s}(u)\, du \overset{(a)}{=} \int_0^{\infty} \frac{1 - F_{\gamma_s}(u)}{\ln(2)(1+u)} du, \quad (9)$$

where step (a) holds by using integration by parts, and $f_{\gamma_s}(u)$ and $F_{\gamma_s}(u)$ are the probability density function (PDF) and the cumulative distribution function (CDF) of the variable γ_s, respectively. Next, we will derive the CDF $F_{\gamma_s}(u)$, and then calculate the integral involved in (9).

On the basis of (8), $F_{\gamma_s}(u)$ can be written as

$$\begin{aligned} F_{\gamma_s}(u) &= \Pr\left\{\max_{1\le i\le L} \gamma_i^{s^*} < u\right\} = \prod_{i=1}^{L} \Pr\left\{\gamma_i^{s^*} < u\right\} \\ &= \prod_{i=1}^{L}\left(\underbrace{\Pr\left\{\beta_i^* = 0\right\}}_{\Xi_1} + \underbrace{\Pr\left\{\beta_i^* > 0, \gamma_i^{s^*} < u\right\}}_{\Xi_2}\right). \end{aligned} \quad (10)$$

The term Ξ_1 of (10) can be calculated using (6) as

$$\Xi_1 = \underbrace{\Pr\left\{|f_i|^2 \le \frac{\Phi_i}{P_s}\right\}}_{\Xi_1^1} + \underbrace{\Pr\left\{|f_i|^2 > \frac{\Phi_i}{P_s}, \left\|w_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 \le \left\|w_{e,i}^{\dagger}\mathbf{h}_i\right\|^2\right\}}_{\Xi_1^2}. \quad (11)$$

We define $X = |f_i|^2$, $Y = \left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2$ and $Z = \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2$, whose PDFs are expressed respectively as $f_X(x) = \frac{x^{m_{s,i}-1}}{\Gamma(m_{s,i})\theta_{s,i}^{m_{s,i}}} e^{-\frac{x}{\theta_{s,i}}}$, $f_Y(y) = \frac{y^{m_{d,i}N-1}}{\Gamma(m_{d,i}N)\theta_{d,i}^{m_{d,i}N}} e^{-\frac{y}{\theta_{d,i}}}$ and $f_Z(z) = \frac{z^{m_{e,i}M-1}}{\Gamma(m_{e,i}M)\theta_{e,i}^{m_{e,i}M}} e^{-\frac{z}{\theta_{e,i}}}$, where $m_{j,i}$ and $\theta_{j,i} = \Omega_{j,i}/m_{j,i}$ denote the shape and scale parameters of a gamma distribution, respectively, and $j \in \{s, d, e\}$.

Hence, Ξ_1^1 in (11) is computed, using [11, eq.(3.381.1)], as

$$\Xi_1^1 = \int_0^{\frac{\Phi_i}{P_s}} f_X(x) dx = \frac{1}{\Gamma(m_{s,i})} \gamma\left(m_{s,i}, \frac{\Phi_i}{P_s\theta_{s,i}}\right). \quad (12)$$

The term Ξ_1^2 of (11) can be written as

$$\begin{aligned} \Xi_1^2 &= \int_{\frac{\Phi_i}{P_s}}^{\infty} \int_0^{\infty} \int_0^{z} f_X(x) f_Z(z) f_Y(y)\, dy dz dx \\ &= \left(1 - \frac{1}{\Gamma(m_{s,i})} \gamma\left(m_{s,i}, \frac{\Phi_i}{P_s\theta_{s,i}}\right)\right) \\ &\quad \times \int_0^{\infty} \frac{z^{m_{e,i}M-1} e^{-\frac{z}{\theta_{e,i}}}}{\Gamma(m_{d,i}N)\Gamma(m_{e,i}M)\theta_{e,i}^{m_{e,i}M}} \gamma\left(m_{d,i}N, \frac{z}{\theta_{d,i}}\right) dz. \end{aligned} \quad (13)$$

Combining [11, eq.(8.352.6)] with [11, eq.(3.381.4)], the closed-form for Ξ_1^2 can be obtained as

$$\begin{aligned} \Xi_1^2 = &\left(1 - \frac{1}{\Gamma(m_{s,i})} \gamma\left(m_{s,i}, \frac{\Phi_i}{P_s\theta_{s,i}}\right)\right)\left(1 - \frac{1}{\Gamma(m_{e,i}M)\theta_{e,i}^{m_{e,i}M}}\right. \\ &\left. \times \sum_{k=0}^{m_{d,i}N-1} \frac{\theta_{d,i}^{m_{d,i}M}}{k!} \left(\frac{\theta_{e,i}}{\theta_{d,i}+\theta_{e,i}}\right)^{k+m_{e,i}M} \Gamma(k+m_{e,i}M)\right). \end{aligned} \quad (14)$$

Substituting (6) into (10), the term Ξ_2 can be written as

$$\Xi_2 = \int_{\frac{\Phi_i}{P_s}}^{\infty} \int_0^{\infty} \int_z^{(1+u)z + \frac{u\sigma^2}{\eta_i(P_s x - \Phi_i)}} f_X(x) f_Z(z) f_Y(y)\, dy dz dx. \quad (15)$$

Utilizing [11, eq.(3.381.1)] and [11, eq.(8.352.6)], Ξ_2 can be rewritten as (16), shown at the bottom of the next page.

Following similar derivations, we can also obtain the closed-form expression for Ξ_2^1 and Ξ_2^2. Adopting binomial expansion for $\left(\frac{1+u}{\theta_{d,i}} z + \frac{u\sigma^2}{\eta_i\theta_{d,i}(P_s x - \Phi_i)}\right)^k$ and [11, eq.(3.381.4)], Ξ_2^3 can be expressed as

$$\begin{aligned} \Xi_2^3 = &\frac{1}{\Gamma(m_{s,i})\Gamma(m_{e,i}M)\theta_{s,i}^{m_{s,i}}\theta_{e,i}^{m_{e,i}M}} \sum_{k=0}^{m_{d,i}N-1} \sum_{j=0}^{k} \frac{\Gamma(i+m_{e,i}M)}{k!} \\ &\times \binom{k}{j} \left(\frac{1+u}{\theta_{d,i}}\right)^j \left(\frac{\theta_{d,i}\theta_{e,i}}{(1+u)\theta_{e,i}+\theta_{d,i}}\right)^{j+m_{e,i}M} \\ &\times \underbrace{\int_{\frac{\Phi_i}{P_s}}^{\infty} x^{m_{s,i}-1} \left(\frac{u\sigma^2}{\eta_i\theta_{d,i}(P_s x - \Phi_i)}\right)^{k-j} e^{-\frac{x}{\theta_{s,i}} - \frac{u\sigma^2}{\eta_i\theta_{d,i}(P_s x - \Phi_i)}} dx}_{\Xi_2^{3,1}}. \end{aligned} \quad (17)$$

After substituting $t = P_s x - \Phi_i$, and then utilizing the binomial expansion for $(t + \Phi_i)^{m_{s,i}-1}$ and [11, eq.(3.471.9)],

$\Xi_2^{3,1}$ can be calculated as

$$\Xi_2^{3,1} = 2\Phi_i^{m_{s,i}-q-1}\left(\frac{u\sigma^2}{\eta_i\theta_{d,i}}\right)^{k-j}\left(\frac{1}{P_s}\right)^{m_{s,i}}\sum_{q=0}^{m_{s,i}-1}\binom{m_{s,i}-1}{j} \times e^{-\frac{\Phi_i}{P_s\theta_{s,i}}}\left(\frac{u\sigma^2 P_s\theta_{s,i}}{\eta_i\theta_{d,i}}\right)^{\frac{j+q-k+1}{2}} K_{j+q-k+1}\left(2\sqrt{\frac{u\sigma^2}{\eta_i P_s\theta_{s,i}\theta_{d,i}}}\right), \tag{18}$$

where $K_v(x)$ denotes the Bessel function of imaginary argument. Based on the aforementioned analyses, the closed-form expression for $F_{\gamma_s}(u)$ can be expressed as (19), shown at the bottom of the page. Then, the CDF of C_s can be obtained directly as $F_{C_s}(\omega) = \Pr\{\gamma_s < 2^\omega - 1\} = F_{\gamma_s}(2^\omega - 1)$ in terms of $C_s = \log_2(1+\gamma_s)$.

Due to the high complexity of $F_{\gamma_s}(u)$, it is hard to directly solve the integral in (9). Hence, we approximate it through adopting the variable substitution $u = \tan\theta$ for (9) and the Gaussian-Chebyshev quadrature successively, and obtain

$$C_{er} = \frac{1}{\ln(2)}\int_0^{\pi/2}\sec^2\theta\frac{1-F_{\gamma_s}(\tan\theta)}{1+\tan\theta}d\theta \simeq \frac{\pi^2}{4\ln(2)\Lambda}\sum_{p=1}^{\Lambda}\sqrt{1-f_p^2}\sec^2(v_p)\frac{1-F_{\gamma_s}(\tan(v_p))}{1+\tan(v_p)}, \tag{20}$$

where $f_p = \cos((2p-1)\pi/2\Lambda)$, $v_p = \pi(f_p+1)/4$, and Λ is the tradeoff parameter between accuracy and complexity [8].

In the studied network, a secrecy outage event occurs if and only if the secrecy capacity falls below a given threshold C_{th}, hence the SOP can be calculated as

$$P_{out} = \Pr\{C_s < C_{th}\} = F_{C_s}(C_{th}) = F_{\gamma_s}\left(2^{C_{th}}-1\right). \tag{21}$$

Besides, one observation from (7) and Remark 1 is that when P_s approaches infinity, C_s is calculated as $\lim_{P_s\to\infty} C_s = \max_{T_i\in S_2}\log_2\left(||\mathbf{w}_{d,i}^\dagger\mathbf{g}_i||^2/||\mathbf{w}_{e,i}^\dagger\mathbf{h}_i||^2\right)$. This makes the SOP a non-zero constant at high P_s in terms of (21), which in turn results in the diversity gain equal to $-\lim_{P_s\to\infty}\log(P_{out})/\log(P_s) = 0$.

IV. SIMULATION RESULTS

In this section, Monte-Carlo simulations are provided to investigate the secrecy performance of the proposed strategy. Especially, the simulation results experience 2×10^6 independent trials, and the channel coefficients are randomly generated as Nakagami fading in each trial. Similar to [6], [8], the simulation parameters are defaulted as follows: $L = 3$, $N = M = 3$, $C_{th} = 0.1$ bps/Hz, $P_i^{\max} = 240\ \mu$W, $\varphi_i^{(0)} = 5\ \mu$W, $\varphi_i^{(1)} = 5000$, $\varphi_i^{(2)} = 0.0002$, $P_i^c = 8.9\ \mu$W, $\eta_i = 0.6$, $\sigma^2 = -120$ dBm/Hz, $\Lambda = 20$, $m_{j,i} = m_j = 2$, and $\Omega_{j,i} = d_{j,i}^{-\alpha_{j,i}}$, $i \in \{1,\ldots,L\}$, $j \in \{s,d,e\}$. In particular, $d_{j,i}$ denotes the distance between j and T_i, and $\alpha_{j,i} = \alpha_j$ represents the path-loss exponent of the $j \to T_i$ link. Moreover, S, D and E are located at $(0,0)$, $(10,4)$ and $(10,-1)$ in meter (m) in a two-dimensional plane, respectively. All tags are uniformly distributed in a circle with a center coordinate $(5,0)$, namely, $(5+r\cos\phi_i, r\sin\phi_i)$, where $r = 2$ denotes the radius of the circle and ϕ_i randomly distributes in $[0,2\pi]$. Any values that are different from their default settings will be explicitly mentioned.

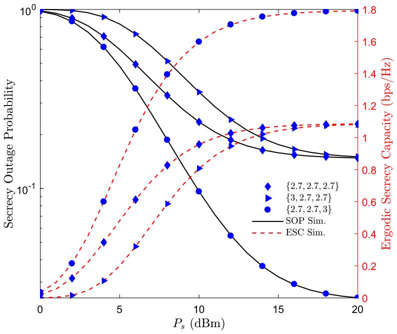

Fig. 2. The ESC and the SOP versus the source transmit power P_s for different values of $\{\alpha_s, \alpha_d, \alpha_e\}$, where $M = 2$.

Fig. 2 jointly depicts the ESC and the SOP against P_s with different $\{\alpha_s, \alpha_d, \alpha_e\}$, aiming at validating the theoretical analyses for the proposed strategy. Clearly, the analytical results obtained from (20) and (21) match well with the simulation results, which verifies the theoretical derivations in Section III-B. Moreover, no matter what P_s and $\{\alpha_s, \alpha_d, \alpha_e\}$ are, the studied network can achieve a non-negative ESC, which agrees well with Remark 2. This is mainly due to the fact that for T_i $(T_i \in \mathcal{S}_1)$, the proposed strategy by virtue of dynamically optimizing PRC makes the corresponding secrecy capacity zero instead of a negative value when $\left\|\mathbf{w}_{d,i}^\dagger\mathbf{g}_i\right\|^2 \le \left\|\mathbf{w}_{e,i}^\dagger\mathbf{h}_i\right\|^2$. Apart from the above, Fig. 2 also shows the effects of multitudinous parameters. Firstly, as shown in this figure, all curves for the ESC (SOP)

$$\Xi_2 = \underbrace{\int_{\frac{\Phi_i}{P_s}}^{\infty}\int_0^{\infty} f_X(x) f_Z(z)\,dzdx}_{\Xi_2^1} - \underbrace{\int_{\frac{\Phi_i}{P_s}}^{\infty}\int_0^{\infty} f_X(x) f_Z(z)\frac{1}{\Gamma(m_{d,i}N)}\gamma\left(m_{d,i}N, \frac{z}{\theta_{d,i}}\right)dzdx}_{\Xi_2^2} - \underbrace{\int_{\frac{\Phi_i}{P_s}}^{\infty}\int_0^{\infty} f_X(x) f_Z(z)\, e^{-\frac{1+u}{\theta_{d,i}}z-\frac{u\sigma^2}{\eta_i\theta_{d,i}(P_s x-\Phi_i)}}\sum_{k=0}^{m_{d,i}N-1}\frac{1}{k!}\left(\frac{1+u}{\theta_{d,i}}z+\frac{u\sigma^2}{\eta_i\theta_{d,i}(P_s x-\Phi_i)}\right)^k dzdx}_{\Xi_2^3}. \tag{16}$$

$$F_{\gamma_s}(u) = \prod_{i=1}^{L}\left(1-\frac{2}{\Gamma(m_{s,i})\theta_{s,i}^{m_s}\Gamma(m_{e,i}M)\theta_{e,i}^{m_{e,i}M}}\sum_{k=0}^{m_{d,i}N-1}\sum_{j=0}^{k}\sum_{q=0}^{m_{s,i}-1}\frac{1}{k!}\binom{k}{j}\left(\frac{1+u}{\theta_{d,i}}\right)^j\left(\frac{\theta_{d,i}\theta_{e,i}}{(1+u)\theta_{e,i}+\theta_{d,i}}\right)^{j+m_{e,i}M}\Gamma(j+m_{e,i}M) \times\left(\frac{u\sigma^2}{\eta_i\theta_{d,i}}\right)^{k-j}\left(\frac{1}{P_s}\right)^{m_{s,i}} e^{-\frac{\Phi_i}{\theta_{s,i}P_s}}\binom{m_{s,i}-1}{q}\Phi_i^{m_{s,i}-q-1}\left(\frac{\theta_{s,i}P_s u\sigma^2}{\eta_i\theta_{d,i}}\right)^{\frac{j+q-k+1}{2}} K_{j+q-k+1}\left(2\sqrt{\frac{u\sigma^2}{\eta_i P_s\theta_{s,i}\theta_{d,i}}}\right)\right). \tag{19}$$

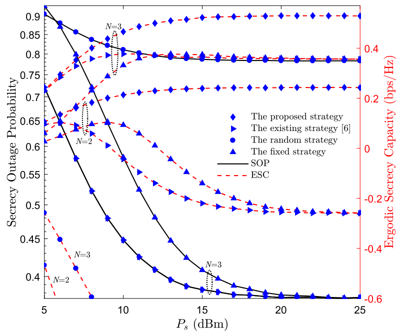

Fig. 3. The secrecy performance under different strategies, where $\{\alpha_s, \alpha_d, \alpha_e\} = \{2.7, 2.7, 2.7\}$.

first increase (decrease) and then converge to a constant. The reason is as follows. One observation from (7) is that $C_i^{s^*}$ corresponding to the nonzero case is a function of channel fading coefficients at high P_s regions, which in turn leads to a convergence behavior. Secondly, for a given α_s, one can see that when α_d is lower than α_e and the corresponding difference is larger, the studied network can achieve higher secrecy performance. Intuitively, under the above conditions, the channel quality of the backscattering link is obviously better than the eavesdropping link, and more tags can attempt communication with D, thereby enhancing the secrecy capacity achieved by the whole network. Thirdly, for a fixed α_d and α_e, the impact of α_s is very severe at lower P_s regions, but it can be negligible with increasing P_s. This is due to the fact that $C_i^{s^*}$ is only determined by both the backscattering and eavesdropping links in terms of (7) when P_s approaches infinity. Finally, the SOP converges to a non-zero constant as P_s increases, which in turn results in a zero diversity gain.

Fig. 3 compares the secrecy performance among the proposed strategy, the existing strategy in [6], the random strategy as well as the fixed strategy. For the random strategy, one of tags in set S_1 is selected randomly to carry out BackCom. Following the fixed strategy, the PRC per tag is set as a constant, based on which the tag with the highest secrecy capacity is selected when satisfying the energy-causality constraint. As illustrated in Fig. 3, although the proposed strategy and the existing one [6] have the same SOP, our work achieves the highest ESC. Particularly, the proposed strategy can guarantee a non-negative ESC no matter what N is, which coincides with the conclusions in Remark 2. For a relatively small N, the instantaneous channel gain of the $T_i \rightarrow D$ link is more likely to be worse than that of the $T_i \rightarrow E$ link, on the basis, the selected tag T_i under three benchmark strategies may generate a negative secrecy capacity according to (5), which in turn deteriorates the ESC. By contrast, the proposed strategy makes the instantaneous secrecy capacity of T_i non-negative at any channel quality, which greatly enhances the ESC.

V. CONCLUSION

In this letter, we have proposed a tag selection strategy to maximize the ESC and minimize the SOP concurrently for a multi-tag enabled BackCom network under an eavesdropper. We have derived the ESC and the SOP under the i.n.i.d. Nakagami-m fading to estimate the secrecy performance of the proposed strategy. Numerical simulations have validated the derived results and revealed the following insights. Firstly, the larger the difference of the channel quality between the backscattering and eavesdropping links, the higher the performance gain of the considered network is. Secondly, the channel quality variation of the forwarding links causes great effects on the ESC and the SOP at low P_s regions, whereas those effects can be ignored at high P_s regions. Finally, the proposed strategy achieves a higher ESC while keeping the same SOP compared with that of the existing strategy.

APPENDIX A

The optimal PRC subjected to the energy-causality constraint can be obtained by solving the following problem,

$$\max_{\beta_i} C_i^s \quad \text{s.t. } P_i \geq P_i^c,\ 0 \leq \beta_i \leq 1. \tag{A.1}$$

After several straightforward mathematical calculations, (A.1) can be transformed as

$$\begin{aligned} &\max_{\beta_i} \log_2\left(1+\frac{\eta_i\beta_i P_s|f_i|^2\left(\left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2-\left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2\right)}{\eta_i\beta_i P_s|f_i|^2\left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2+\sigma^2}\right) \\ &\text{s.t. } 0 \leq \beta_i \leq \max\left(1-\frac{\Phi_i}{P_s|f_i|^2}, 0\right).A.2 \end{aligned} \tag{A.2}$$

If $|f_i|^2 \leq \frac{\Phi_i}{P_s}$ holds, the feasible region of β_i is $\beta_i = 0$, indicating that T_i is unable to derive the circuit operation even using all the received power. In this case, the optimal secrecy capacity $C_i^{s^*}$ is zero. If $|f_i|^2 > \frac{\Phi_i}{P_s}$, the feasible region of β_i is from 0 to $1 - \frac{\Phi_i}{P_s|f_i|^2}$, and the optimal β_i can be determined from the following two cases. *Case I:* if $\left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 \leq \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2$, the objective function of (A.2) is a monotone decreasing function with respect to β_i. Hence, the optimal PRC equals zero, and $C_i^{s^*} = 0$. *Case II:* if $\left\|\mathbf{w}_{d,i}^{\dagger}\mathbf{g}_i\right\|^2 > \left\|\mathbf{w}_{e,i}^{\dagger}\mathbf{h}_i\right\|^2$, the objective function of (A.2) increases as β_i, thus, $\beta_i^* = 1 - \frac{\Phi_i}{P_s|f_i|^2}$. Substituting it into (5), $C_i^{s^*}$ can be obtained. The proof is complete.

REFERENCES

[1] C. Song, Y. Ding, and A. Eid, "Advances in wirelessly powered backscatter communications: From Antenna/RF circuitry design to printed flexible electronics," *Proc. IEEE*, vol. 110, no. 1, pp. 171–192, Jan. 2022.

[2] A.-N. Nguyen, V. Nhan Vo, C. So-In, D.-B. Ha, S. Sanguanpong, and Z. A. Baig, "On secure wireless sensor networks with cooperative energy harvesting relaying," *IEEE Access*, vol. 7, pp. 139212–139225, 2019.

[3] Y. Zhang, F. Gao, L. Fan, X. Lei, and G. K. Karagiannidis, "Secure communications for multi-tag backscatter systems," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1146–1149, Aug. 2019.

[4] X. Li *et al.*, "Hardware impaired ambient backscatter NOMA systems: Reliability and security," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2723–2736, Apr. 2021.

[5] X. Li *et al.*, "Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1066–1076, Sep. 2021.

[6] Y. Liu, Y. Ye, and R. Q. Hu, "Secrecy outage probability in backscatter communication systems with tag selection," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2190–2194, Oct. 2021.

[7] H. Guo, Q. Zhang, S. Xiao, and Y. C. Liang, "Exploiting multiple antennas for cognitive ambient backscatter communication," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 765–775, Feb. 2019.

[8] 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.

[9] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[10] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic secrecy capacity of dual-hop multiple-antenna AF relaying systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1–6.

[11] I. S. Gradshteyb and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.