Physical Layer Security for Wireless-Powered Ambient Backscatter Cooperative Communication Networks

Xingwang Li, *Senior Member, IEEE,* Junjie Jiang, Hao Wang, Gaojie Chen, *Senior Member, IEEE,* Jianhe Du, *Member, IEEE,* Chunqiang Hu, *Member, IEEE,* and Shahid Mumtaz, *Senior Member, IEEE*

Abstract

Low power consumption and high spectrum efficiency as the great challenges for multi-device access to Internet-of-Things (IoT) have put forward stringent requirements on the future intelligent network. Ambient backscatter communication (ABcom) is regarded as a promising technology to cope with the two challenges, where backscatter device (BD) can reflect ambient radio frequency (RF) signals without additional bandwidth. However, minimalist structural design of BD makes ABcom security vulnerable in wireless propagation environments. By virtue of this fact, this paper considers the physical layer security (PLS) of a wireless-powered ambient backscatter cooperative communication network threatened by an eavesdropper, where a BD with nonlinear energy harvesting model cooperates with decode-and-forward (DF) relay for secure communication. The PLS performance is investigated by deriving the secrecy outage probability (SOP) and secure energy efficiency (SEE). Specifically, the closed-form and

Xingwang Li, JunjieJiang and Hao Wang are with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454000, China (e-mail: lixingwangbupt@gmail.com; jiangjunjiehpu@163.com; wanghao@hpu.edu.cn)

Gaojie Chen is with the 5GIC & 6GIC, Institute for Communication Systems (ICS), University of Surrey, Guildford, GU2 7XH, United Kingdom (e-mail: gaojie.chen@surrey.ac.uk).

Jianhe Du is with the State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing 100024, China (e-mail: dujianhe1@gmail.com)

Chunqiang Hu is with the School of Big Data & Software Engineering, Chongqing University, Chongqing 400030, China (e-mail:chu@cqu.edu.cn.)

Shahid Mumtaz is with the Institute of Telecommunications, 3810078 Aveiro, Portugal, and also with the ARIES Research Center, Universidad Antonio de Nebrija, E-28040 Madrid, Spain (e-mail: smumtaz@av.it.pt).

asymptotic expressions of SOP are derived as well as the secrecy diversity order for the first time. As an energy-constrained device, balancing power consumption and security is major concern for BD, thus the SEE of the proposed network is studied. The results from numerical analysis show that the performance improvement of SOP and SEE is impacted by system parameters, including transmission power, secrecy rate threshold, reflection efficiency and distance between the source and BD, which provide guidance on balancing security and energy efficiency in ambient backscatter cooperative relay networks.

Index Terms

Ambient backscatter, cooperative communication, nonlinear energy harvesting, secrecy outage probability, secure energy efficiency.

I. Introduction

The booming multi-device access has brought great challenges to power consumption and spectrum efficiency of Internet-of-Things (IoT). Whereas traditional cooperative relay networks can improve the coverage and reliability of wireless networks, the inherent drawbacks that low spectrum efficiency for half duplex relays and serious self-interference for full duplex relays are contrary to the demands of IoT [1]–[3]. To address these problems, some promising technologies have been proposed to combine with relay communication for high spectrum efficiency and low operating cost, such as ambient backscatter communication (ABcom) [4], energy harvesting (EH) [5].

In ABcom systems, backscatter device (BD) has simple structure without high-cost and power-hungry components (e.g., oscillators, amplifiers, and filters), which cater to IoT devices for low cost and low power consumption. Furthermore, the high spectrum efficiency is embodied in ABcom since it does not require additional bandwidth [6]. The BD can harvest energy from ambient radio frequency (RF) signals, that is used to activate the circuit and reflect signals, thus it enjoys low power consumption. These advantages have aroused the research interests on ABcom systems. For instance, in [7], the outage performance of ABcom systems over Gaussian channels was studied by deriving the expressions of outage probability (OP). The authors in [8] proposed a multiple decode-and-forward (DF) relays cooperative ABcom network, where only one relay that can maximize the quality of service (QoS) was selected. Furthermore, ABcom systems combined with other promising technologies were investigated in much of the existing literature. Li $et\ al.$ in [9] derived the expressions for the effective capacity of ABcom non-orthogonal multiple access (NOMA) systems. In [10], the asymptotic behaviors of OP and intercept probability (IP)

in two-way ABcom networks were studied. A quantitative comparison between ABcom and harvest-then-transmit was performed in [11], illustrating the significant benefits of ABcom in low power consumption.

Due to BDs rely on ambient RF signals to drive circuit and complete communication, ABcom needs to coexist with the existing communication system [12]. Recently, the combination of relay-based cooperative transmission and ABcom has attracted attention. In [13], the opportunistic ambient backscatter assisted DF relay scheme was proposed, where BD embedded in the relay was triggered by power difference between first-hop and second-hop. Based on this model, the outage performance of the two-way communication was analyzed in [12], revealing that the outage performance is better when BD is close to the destination. The authors in [14] studied the sum-throughput and energy efficiency of cognitive DF relay networks, where ABcom was employed as secondary communication. Whereas the advantage of the high spectrum efficiency for BD cannot be effectively utilized in [14], since the link between the source and BD was not considered. In [15], the capacity was maximized by adjusting the power splitting (PS) factor and the time allocation in ABcom, where tag did not reflect signals to the destination only to the relay.

The wireless-powered networks are proposed to solve the problem of limited battery life and frequent replacement of sensors in IoT networks [16], [17]. In wireless-powered ABcom systems, BDs as battery-free devices rely on EH technology to activate circuits for backscatter communication. Given that the low operating costs of ABcom benefits from EH, the performance of ABcom networks with considering EH has been widely studied in various scenarios [18]–[22]. Among them, in [18], BDs were adopted a nonlinear EH strategy that could achieve adaptive reflection coefficient to enhance reliability of backscatter link. The authors in [19] studied the diversity gain of EH tag selection networks by deriving the high signal-to-noise ratio (SNR) approximation of secrecy outage probability (SOP), indicating that the diversity order is zero owing to eavesdropper limits the improvement of SOP in the high SNR regions. Different from only PS scheme in previous works, the time switching (TS) scheme was also employed at BD in [20], where the optimal TS ratio is determined by the circuit power consumption and received power of BD. In [21], the optimal energy efficiency can be achieved by optimizing the time allocation for sleep and active states, where BD harvests energy in both states and reflects signals only in the active state. In [22], ambient RF signals with high power were detected as EH and backscatter communication resources for BD with the aid of the spectrum sensing and

energy detection techniques.

However, simple structure restricts the use of complex encoding and modulation modes for BDs, resulting in some inherent defects. The main one is that encryption modes with high energy consumption and complexity can not be applied to BD. Therefore, the security of ABcom is vulnerable to various threats, such as eavesdropping and attacking. To address this problem, the physical layer security (PLS) was proposed as an effective approach to ensure the information transmission security at the physical layer, which is defined the capacity difference between the legitimate channels and the eavesdropping channels [23], [24]. The research works on PLS performance of ABcom systems are as follows [25]–[28]. The authors of [25] considered a practical ABcom scenario where both the reader and eavesdropper are in motion, and the secrecy performance was studied with imperfect channel estimation. Considering that the addition noise source is unsuitable for moving vehicles, the authors in [26] proposed vehicles and pedestrians networks with ABcom where artificial noise was produced at ambient RF source to enhance the PLS performance. In [27], the ergodic rates and OPs for backscatter-NOMA systems and symbiotic radio systems were analyzed to understand how the NOMA and the symbiotic radio affect each other. The authors of [28] studied the outage performance of commensal, parasitic and competitive schemes in a cooperative ABcom system, and found that the performance for ABcom is the same when the SNR threshold approaches to zero.

On the other hand, the energy efficiency has been major concern for communication devices, especially energy-constrained devices. Improving energy efficiency is conducive to reduce the operating costs of communication systems and expedite the deployment of IoT [29], [30]. However, the energy efficiency optimization is subject to numerous constraints in various scenes. Security constraint is a critical one that is caused by the presence of eavesdroppers in wireless communications. The secure energy efficiency (SEE) was proposed to measure both security and energy efficiency, which is defined as the amount of information transmitted secretly per unit energy [31]. The SEE performance has been investigated for networks with various technologies, including relay [32], unmanned aerial vehicle (UAV) [33] and BD [34]. Wang $et\ al.$ studied the effects of target secrecy rate and distance between the source and the destination on SEE of amplify-and-forward multi-relay networks [32]. In [33], the SEE maximization problem in wireless sensor networks with UAVs was jointly formulated by transmit powers, UAV trajectory and sensor node scheduling. The authors of [34] investigated the SEE of two-way communication networks that adopted the backscatter jamming strategy to reduce the risk of eavesdropping. The

secrecy performance of full duplex jamming relay network was studied in [35], and indicated that the secrecy performance of the full duplex jamming strategy is better than that of half duplex and full duplex strategies. Based upon above analysis, our work regards BD not only as collaborator to transmit signals but also as jammer for degrading eavesdropping.

A. Motivation and Contributions

In the above-mentioned literature on cooperative relay networks with BD, in [12], [13], the BD was not active in the second time slot, because there was no communication link between the relay and BD. Similarly, in [14], [15], the destination did not receive signals from BD in the first time slot. The foregoing networks cannot fully exploit the advantage of high spectral efficiency of ABcom. In addition, the secrecy performance and SEE have not been studied in cooperative relay communication networks with ABcom considered the links between BD and each node. To fill this gap, we propose a cooperative ABcom with a DF relay, where the links between BD and other nodes all exist. The SOP and SEE are investigated in the presence of eavesdropper. The key contributions of the article can be summarized as:

1) We present an innovative cooperative ABcom with a DF relay, and study security performance and SEE in the presence of an eavesdropper. Wherein the BD acts not only as collaborator for reflecting signals but also as jammer for disturbing eavesdropper. It harvests the energy from signals transmitted by both source and relay to drive the circuit and backscatter signals. The signal transmission from the source to the destination can be done in one time slot in virtue of BD, improving reception efficiency at the destination.
2) We derive the closed-form expression of SOP to investigate the secrecy performance when the selection combining (SC) mechanism is employed at the destination and eavesdropper. For further insights on the secrecy performance, we derive the asymptotic expression of SOP in the high SNR regions as well as the secrecy diversity order. The effects of transmission power, reflection efficiency and distance between the source and BD on secrecy performance are studied.
3) To balance the security and energy efficiency, we study the SEE of the system and investigate the effects of transmission power and secrecy rate threshold on the SEE. We find that the SEE performance can be optimal by adjusting the secrecy rate threshold for various transmission power.

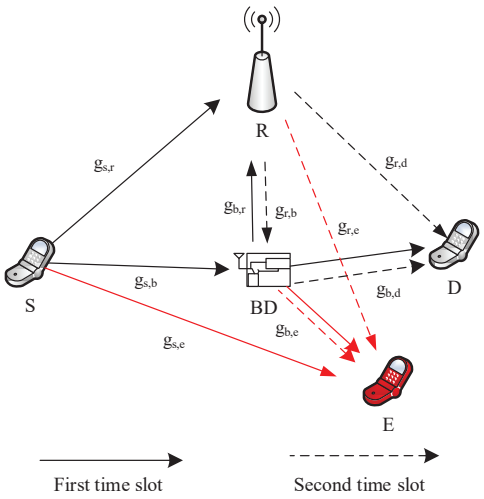

Fig. 1. Ambient backscatter cooperative DF relay communication system model.

B. Organization and Notations

The rest of the article is composed as follows. In Section II, the cooperative ABcom model is constructed as well as a detailed discussion on received signals and energy consumption model. In Section III, the closed-form/asymptotic expressions of SOP and the elaboration on SEE are derived. Numerical results in section IV are provided to validate the correctness of the theoretical analysis, followed by conclusions in Section V.

The $E(\cdot)$ is the expectation operation and $\mathcal{CN}(u,\sigma^2)$ is deemed as the complex Gaussian random variable with mean u and variance σ^2. The $\Pr(\cdot)$ is deemed as the probability and $K_v(\cdot)$ is the vth order modified Bessel function of the second kind. Besides, $\mathrm{Ei}(\cdot)$ denotes the exponential integral function. The cumulative distribution function (CDF) and the probability dense function (PDF) of a random variable v are expressed as $F_v(\cdot)$ and $f_v(\cdot)$.

II. SYSTEM MODEL

As shown in Fig. 1, we propose a cooperative ABcom network, which includes source (S), relay (R), BD, destination (D) and an eavesdropper (E). We define $g_{i,j}$, $(i,j \in \{s,r,b,d,e\})$ as the channel responses from i to j. Due to deep shadowing, there is no direct link between the source and the destination. It is assumed that each node is equipped with a single antenna. All channels are modeled as the independent Rayleigh fading channels. We have $g_{i,j} \sim \mathcal{CN}(0,\lambda_{ij})$.

A. Received Signals and Signal-to-Noise Ratio

In the first time slot, the source transmits signals to the half-duplex DF relay and BD, where BD harvests energy from transmitted signals to activate the circuit and reflect signals. In the second time slot, the relay forwards the signals to the destination, while BD harvests energy from forwarding signals and reflects signals. The eavesdropper intercepts the signals sent by the source and relay while the interception be obstructed by backscattered signals during the whole signal transmission.

In the first time slot, the relay receives signals from the source and BD with its own message c_t, where $E\left(|c_t|^2\right) = 1$. The received signals at the relay can be expressed as

$$y_R = \sqrt{P_s} g_{s,r} x_s + \sqrt{\mu \beta_1 P_s} g_{s,b} g_{b,r} x_s c_t + n_r, \tag{1}$$

where P_s is transmission power of the source. $n_r \sim \mathcal{CN}(0, \sigma_r^2)$ is the complex Gaussian noise with zero mean and σ_r^2 variance. β_1 is the reflection coefficient in the first time slot. μ represents the reflection efficiency and denotes the signal being effectively reflected by BD [19]. x_s denotes the transmitted signals from the source. The received signal-to-interference-plus-noise ratio (SINR) at the relay can be obtained as

$$\gamma_R = \frac{P_s |g_{s,r}|^2}{\mu \beta_1 P_s |g_{s,b}|^2 |g_{b,r}|^2 + \sigma_r^2}. \tag{2}$$

In the first time slot, the destination only receives backscattered signals, thus the received signals at the destination can be expressed as

$$y_D^{(1)} = \sqrt{\mu \beta_1 P_s} g_{s,b} g_{b,d} x_s c_t + n_d, \tag{3}$$

where $n_d \sim \mathcal{CN}(0, \sigma_d^2)$ is the complex Gaussian noise at the destination with zero mean and σ_d^2 variance. Thus, the received SNR can be written as

$$\gamma_D^{(1)} = \frac{\mu \beta_1 P_s |g_{s,b}|^2 |g_{b,d}|^2}{\sigma_d^2}. \tag{4}$$

In the first time slot, the eavesdropper intercepts signals from the source and BD, thus the received signals at the eavesdropper can be expressed as

$$y_E^{(1)} = \sqrt{P_s} g_{s,e} x_s + \sqrt{\mu \beta_1 P_s} g_{s,b} g_{b,e} x_s c_t + n_e, \tag{5}$$

where $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ is the complex Gaussian noise at the eavesdropper with σ_e^2 variance. For convenience of analysis, we assume $\sigma_r^2 = \sigma_d^2 = \sigma_e^2 = \sigma^2$. The received SINR at the eavesdropper in the first time slot can be written as

$$\gamma_E^{(1)} = \frac{P_s |g_{s,e}|^2}{\mu \beta_1 P_s |g_{s,b}|^2 |g_{b,e}|^2 + \sigma_e^2}. \tag{6}$$

In the second time slot, the relay forwards the signals to the destination, while BD reflects signals from the relay. The received signals at the destination in the second time slot can be expressed as

$$y_D^{(2)} = \sqrt{P_r} g_{r,d} x_s + \sqrt{\mu \beta_2 P_r} g_{r,b} g_{b,d} x_s c_t + n_d, \tag{7}$$

where P_r is transmission power of the relay and β_2 is the reflection coefficient in the second time slot. The received SINR at the destination in the second time slot can be given as

$$\gamma_D^{(2)} = \min \left(\gamma_R, \frac{P_r |g_{r,d}|^2}{\mu \beta_2 P_r |g_{r,b}|^2 |g_{b,d}|^2 + \sigma_d^2} \right). \tag{8}$$

In the second time slot, the eavesdropper intercepts signals from the relay and BD, thus the received signals can be expressed as

$$y_E^{(2)} = \sqrt{P_r} g_{r,e} x_s + \sqrt{\mu \beta_2 P_r} g_{r,b} g_{b,e} x_s c_t + n_e. \tag{9}$$

The SINR at the eavesdropper in the second time slot can be written as

$$\gamma_E^{(2)} = \frac{P_r |g_{r,e}|^2}{\mu \beta_2 P_r |g_{r,b}|^2 |g_{b,e}|^2 + \sigma_e^2}. \tag{10}$$

B. Energy Consumption Model

The energy consumption of nodes can be divided into two parts: the transmitted power and the energy consumed by its circuit modules. The source only transmits the signal in the first time slot and keeps silent in the next time slot, thus the energy consumed at the source is composed as

$$E_s = \frac{T}{2} \left(P_s + P_c^s \right), \tag{11}$$

where P_c^s represents circuit power consumption of the source, and T denotes the entire transmission slot. The relay receives and decodes the signals in the first time slot and forwards decoded signals to the destination in the second time slot. Thus, the energy consumed at the relay including circuit consumption and transmission power in the second time slot, which can be given as

$$E_r = T \left(\frac{1}{2} P_r + P_c^r \right), \tag{12}$$

where P_c^r denotes the circuit power consumption at the relay. Similarly, the circuit of destination is activated to receive signals in two time slots, thus the energy consumed at the destination can be given by

$$E_d = T P_c^d, \tag{13}$$

where P_c^d denotes the circuit power consumption at the destination. The harvested energy at BD in the first time slot can be slit two parts: $\sqrt{\beta_1}x_s$ is used to reflect signals, and $\sqrt{1-\beta_1}x_s$ is used to drive circuit. The reflection coefficient is determined by a practical nonlinear EH model at BD, which is explained as follows. The harvested power P_h at BD in the first time slot can be given as [36]

$$P_h = \frac{P_{\max}\left(1 - e^{-v_1 P_i + v_1 v_0}\right)}{1 + e^{-v_1 P_i + v_1 v_2}}, \tag{14}$$

where P_i denotes the input power to activate circuit at BD, and $P_i = (1-\beta_1) P_s |g_{s,b}|^2$. P_{max} is the saturated threshold for input power and v_0 is the sensitivity threshold. v_1 and v_2 are parameters determined by the hardware composition of the circuit. When the harvested power P_h is higher than its own circuit consumption P_c, i.e., $P_h > P_c$, BD can be activated and work. Thus, reflection coefficient in the first time slot can be determined as

$$\beta_1 = \max\left(1 - \frac{\Phi}{P_s |g_{s,b}|^2}, 0\right), \tag{15}$$

where $\Phi = \frac{\ln \frac{P_{\max} e^{v_1 v_2} + P_c e^{v_1 v_0}}{P_{\max} - P_c}}{v_1}$. Similarly, the reflection coefficient in the second time slot can be given as

$$\beta_2 = \max\left(1 - \frac{\Phi}{P_r |g_{r,b}|^2}, 0\right). \tag{16}$$

Note that the energy consumption at BD is included in the source and relay energy consumption, because BD does not generate additional energy and its energy is harvested from the source and relay. The total energy consumption of cooperative ABcom system can be expressed as

$$E_{total} = E_s + E_r + E_d = T\left(\frac{P_s + P_r + P_c^s}{2} + P_c^d + P_c^r\right). \tag{17}$$

III. PERFORMANCE ANALYSIS

In this section, the secrecy performance of the considered system is studied by deriving the expressions of SOP. The asymptotic expression of SOP in the high SNR regions is derived as well as the secrecy diversity order. Furthermore, the SEE is investigated to analyze the relationship between energy efficiency and secrecy performance.

A. Secrecy Outage Performance Analysis

The SC mechanism is employed at the destination and eavesdropper in this system.[1] Thus, channel capacities can be expressed as

$$C_{\phi} = \frac{1}{2}\log\left(1+\max\left(\gamma_{\phi}^{(1)},\gamma_{\phi}^{(2)}\right)\right), \tag{18}$$

where $\phi \in \{D, E\}$. Then, the secrecy capacity can be expressed as

$$C_S = \max\left(C_D - C_E, 0\right). \tag{19}$$

The SOP is defined as the probability that secrecy capacity is below the secrecy rate threshold, thus SOP in the proposed system can be expressed as

$$P_{out} = \Pr\left(C_S < R_s\right), \tag{20}$$

where R_s is the secrecy rate threshold. Due to $\gamma_D^{(1)}$, $\gamma_D^{(2)}$ and $\gamma_E^{(1)}$ contain $|g_{s,b}|^2$, their CDFs are not independent. Similarly, the CDFs of $\gamma_D^{(2)}$ and $\gamma_E^{(2)}$ are not independent. Thus, the SOP for the channel correlation scheme is given in the following theorem.

Theorem 1: The SOP for the channel correlation scheme can be expressed as

$$\begin{aligned} P_{out} = &\int_{\frac{\Phi}{P_s}}^{\infty}\int_{\frac{\Phi}{P_r}}^{\infty}\int_{0}^{\infty} F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(\left(\tau x+\tau-1\right)|t,u\right) \\ &\times f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\left(x\,|t,u\right)\mathrm{d}x f_{\left|g_{s,b}\right|^2}\left(t\right)\mathrm{d}t f_{\left|g_{r,b}\right|^2}\left(u\right)\mathrm{d}u, \end{aligned} \tag{21}$$

where $f_{\left|g_{s,b}\right|^2}\left(t\right) = \frac{e^{-\frac{t}{\lambda_{sb}}}}{\lambda_{sb}}$, $f_{\left|g_{r,b}\right|^2}\left(u\right) = \frac{e^{-\frac{u}{\lambda_{rb}}}}{\lambda_{rb}}$. $F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(x\,|t,u\right)$ can be given as

$$F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(x\,|t,u\right) = \left(1-e^{-\frac{x\sigma^2}{\mu P_s\left(t-\frac{\Phi}{P_s}\right)\lambda_{bd}}}\right)\left(1-\frac{e^{-\frac{x\sigma^2}{P_s\lambda_{sr}}-\frac{x\sigma^2}{P_s\lambda_{rd}}}}{W_t\left(r\right)W_u\left(d\right)}\right), \tag{22}$$

where $W_t\left(i\right) = \mu\left(t-\frac{\Phi}{P_s}\right)x\frac{\lambda_{bi}}{\lambda_{si}}+1$ and $W_u\left(i\right) = \mu\left(u-\frac{\Phi}{P_r}\right)x\frac{\lambda_{bi}}{\lambda_{ri}}+1$, $i \in \{b, r, e\}$. $f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\left(x\,|t,u\right)$ can be given as

$$\begin{aligned} f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\left(x\,|t,u\right) =& e^{-\frac{x\sigma^2}{P_r\lambda_{re}}}\left(\frac{\frac{\sigma^2}{\lambda_{se}P_s}+\frac{\mu\left(t-\frac{\Phi}{P_s}\right)\lambda_{be}}{\lambda_{se}W_t^{\,2}\left(e\right)}}{W_t\left(e\right)}\right)\left(1-\frac{e^{-\frac{x\sigma^2}{P_r\lambda_{re}}}}{W_u\left(e\right)}\right) \\ &+ e^{-\frac{x\sigma^2}{P_s\lambda_{se}}}\left(1-\frac{e^{-\frac{x\sigma^2}{P_s\lambda_{se}}}}{W_t\left(e\right)}\right)\left(\frac{\frac{\sigma^2}{\lambda_{re}P_r}+\frac{\mu\left(u-\frac{\Phi}{P_r}\right)\lambda_{be}}{\lambda_{re}W_u^{\,2}\left(e\right)}}{W_u\left(e\right)}\right). \end{aligned} \tag{23}$$

[1]The maximum ratio combining (MRC) mechanism is also applicable in this study. For calculation convenience, SC mechanism is adopted in this study.

Proof 1: See Appendix A.

Unfortunately, the exact expression of SOP is difficult to derive caused by complex multiple of integrals. To circumvent this problem, we assume that $\gamma_D^{(1)}$, $\gamma_D^{(2)}$, $\gamma_E^{(1)}$, $\gamma_E^{(2)}$ are independent, which will provide a tight approximation results.[2] By doing that, the closed-form expression of SOP is provided in the following theorem.

Theorem 2: The closed-form expression of SOP can be expressed as

$$\begin{aligned} P_{out} =& \frac{\pi M}{2N} e^{-\frac{\Phi}{P_s\lambda_{sb}}-\Delta_0} \sum_{i=0}^{N} \left(1-\Delta_3 K_1\left(\Delta_3\right)\right)\left(G\left(j\right)+G\left(\bar{j}\right)\right) \\ & \times \left(1-\left(1-e^{-\frac{\Phi}{P_s\lambda_{sb}}} H\left(1\right)\right)\left(1-e^{-\frac{\Phi}{P_r\lambda_{rb}}} H\left(2\right)\right)\right)\sqrt{1-\delta_i^2}, \end{aligned} \tag{24}$$

where $\tau = 2^{2R_s}$, $\psi = \frac{M(\delta_i+1)}{2}$, $\delta_i = \cos\left(\frac{2i-1}{2N}\pi\right)$, $\xi = \left(\tau\left(\psi+1\right)-1\right)$, $\Delta_0 = \frac{\Phi}{P_s\lambda_{sb}} + \frac{\Phi}{P_r\lambda_{rb}}$, $\Delta_1 = \frac{\lambda_{sr}}{\mu\xi\lambda_{sb}\lambda_{br}}$, $\Delta_{1,1} = \frac{\xi\sigma^2}{P_s\lambda_{sr}}$, $\Delta_2 = \frac{\lambda_{rd}}{\mu\xi\lambda_{rb}\lambda_{bd}}$, $\Delta_{2,1} = \frac{\xi\sigma^2}{P_r\lambda_{rd}}$, $\Delta_3 = 2\sqrt{\frac{\xi\sigma^2}{\mu P_s\lambda_{sb}\lambda_{bd}}}$, $\Delta_4 = \frac{\lambda_{re}}{\psi\mu\lambda_{rb}\lambda_{be}}$, $\Delta_{4,1} = \frac{\psi\sigma^2}{P_r\lambda_{re}}$, $\Delta_{4,2} = -\frac{\lambda_{re}}{\psi^2\mu\lambda_{rb}\lambda_{be}}$, $\Delta_{4,3} = \Delta_{4,2} - \frac{\sigma^2}{P_r\lambda_{re}}$, $\Delta_5 = \frac{\lambda_{se}}{\psi\mu\lambda_{sb}\lambda_{be}}$, $\Delta_{5,1} = \frac{\psi\sigma^2}{P_s\lambda_{se}}$, $\Delta_{5,2} = -\frac{\lambda_{se}}{\psi^2\mu\lambda_{sb}\lambda_{be}}$, $\Delta_{5,3} = \Delta_{5,2} - \frac{\sigma^2}{P_s\lambda_{se}}$, N is a trade-off parameter between accuracy and complexity, M is a large number and $\mathrm{Ei}\left(x\right) = \int_{-\infty}^{x} \frac{e^t}{t}\mathrm{d}t$ is the exponential integral function. $K_1\left(\cdot\right)$ is the first order modified Bessel function of the second kind. The function $H\left(k\right) = 1 + \Delta_k e^{\Delta_k - \Delta_{k,1}}\mathrm{Ei}\left(-\Delta_k\right)$, $k \in \{1,2,4,5\}$. The function $G(j)$ can be written as

$$G\left(j\right) = \Delta_{j,2} e^{\Delta_j - \Delta_{j,1}}\mathrm{Ei}\left(-\Delta_j\right) H\left(\bar{j}\right) + \Delta_{j,3}\Delta_j e^{\Delta_j - \Delta_{j,1}}\mathrm{Ei}\left(-\Delta_j\right) H\left(\bar{j}\right) + \Delta_{j,2} e^{-\Delta_{j,1}} H\left(\bar{j}\right), \tag{25}$$

where $j \in \{4,5\}$. If $j = 4$, $\bar{j} = 5$, and vice versa.

Proof 2: See Appendix B.

Corollary 1: In the high SNR regions, the SOP asymptotic expression can be given by

$$\begin{aligned} P_{out,\infty} =& \left(1-\frac{\Phi}{P_s\lambda_{sb}}-\Delta_0\right)\frac{\pi M}{2N}\sum_{i=0}^{N}\left(-\frac{\Delta_3^2}{2}\ln\left(\frac{\Delta_3}{2}\right)\right)\left(G_\infty\left(j\right)+G_\infty\left(\bar{j}\right)\right) \\ & \times\left(1-\left(1-\left(1-\frac{\Phi}{P_s\lambda_{sb}}\right)H_\infty\left(1\right)\right)\left(1-\left(1-\frac{\Phi}{P_r\lambda_{rb}}\right)H_\infty\left(2\right)\right)\right)\sqrt{1-\delta_i^2}, \end{aligned} \tag{26}$$

where the functions $H_\infty\left(k\right)$ and $G_\infty\left(j\right)$ can be expressed as

$$H_\infty\left(k\right) = 1 + \left(1-\Delta_{k,1}\right)\Delta_k e^{\Delta_k}\mathrm{Ei}\left(-\Delta_k\right). \tag{27}$$

$$G_\infty\left(j\right) = \left(1-\Delta_{j,1}\right)\Delta_{j,2} e^{\Delta_j}\mathrm{Ei}\left(-\Delta_j\right)\left(1+\Delta_j+\frac{e^{-\Delta_j}}{\mathrm{Ei}\left(-\Delta_j\right)}\right)H_\infty\left(\bar{j}\right). \tag{28}$$

[2]The correlation caused by common terms is weak, and the numerical results demonstrate the accuracy of the approximate results.

Proof 3: We define that $\gamma = P/\sigma^2$ denotes the transmission SNR, where the transmission power P includes P_s and P_r. When $\gamma \to \infty$, $\Delta_3 \to 0$ and $\Delta_{k,1} \to 0$. According to the asymptotic principle, (23) can be obtained by utilizing $xK_1(x) \approx 1 + \frac{x^2}{2}\ln\left(\frac{x}{2}\right)$ [37] and $e^{-x} \approx 1 - x$, when $x \to 0$.

For further insights on the secrecy performance in the high SNR regions, the secrecy diversity order is also studied, which is given as

$$d = -\lim_{\gamma\to\infty} \frac{\log P_{out,\infty}}{\log \gamma}. \tag{29}$$

Corollary 2: The secrecy diversity order can be calculated as

$$d = 1. \tag{30}$$

Remark 1: From corollaries 1,2 and Theorems 1,2, we can find that: 1) Increasing transmission power can improve the received SNR at the destination, while the SINR at the eavesdropper gets close to constant, thereby boosting secrecy capacity and strengthening security; 2) When reflection efficiency increases, the received SNR at the destination and the interference at the eavesdropper can be heightened due to the enhancement of the backscattered signal, thus secrecy performance becomes enhanced; 3) The system can enjoy secrecy diversity gain owing to secrecy diversity order is 1.

B. Secure Energy Efficiency Analysis

The SEE can be expressed as the ratio of total secrecy information bit to system power consumption.

Theorem 3: The SEE in the proposed system can be expressed as

$$\eta = \frac{R_s\left(1 - P_{out}\right)}{E_{total}}. \tag{31}$$

Remark 2: From Theorem 3, it can be found that: 1) Increasing the transmission power can ameliorate the SEE, but when the transmission power is excessively high the SEE is low, thus an optimal transmission power to maximize SEE exists; 2) When raising R_s, the secrecy performance degrades owing to P_{out} rises, thus there exists a trade-off between secrecy rate and SEE performance with respect to R_s.

TABLE I

SIMULATION PARAMETERS.

Saturated threshold for input power	$P_{max} = 240$ μW
Circuit power consumption of BD	$P_c = 8.9$ μW
Circuit power consumption of source, destination and relay	$P_c^s = P_c^d = P_c^r = 10$ mW
Sensitivity threshold	$v_0 = 5$ μW
Noise power	$\sigma^2 = -30$ dBm
Channel parameters	$\lambda_{i,j} = d_{i,j}^{-\alpha}$
Distances between nodes	$\{d_{s,r}, d_{s,b}, d_{s,e}, d_{r,b}, d_{b,r}, d_{b,e}, d_{b,d}, d_{r,d}, d_{r,e}\} = \{5, 1.5, 3.5, 4, 4, 2, 6.5, 6, 6\}$ m
Path loss exponent	$\alpha = 3$
Fixed parameters	$v_1 = 5000$ and $v_2 = 0.0002$

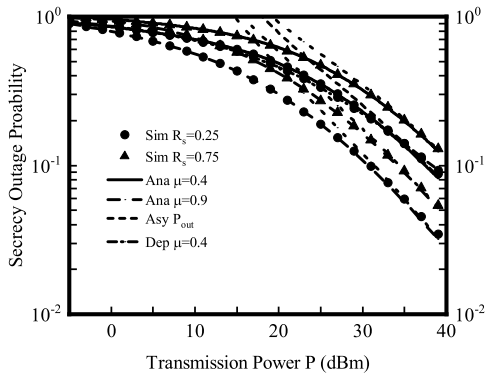

Fig. 2. SOP versus P for different μ and R_s values.

IV. NUMERICAL RESULTS

In this section, the numerical simulation results, that consider 10^5 Monte Carlo trials, are provided to verify the correctness of the previous analysis. The parameters are set as in Table I. In the following figures, Sim. denotes Monte-Carlo simulation results, Ana. denotes the analytical results, and Asy. denotes asymptotic results, Dep. denotes the analytical results of (21).

The simulation results of SOP versus transmission power for different reflection efficiencies and secrecy rate thresholds are plotted in Fig. 2. It can be found that the approximate results are close to exact results, which proves the accuracy of the approximate results. The SOP decreases with the increase of transmission power, improving the security of the system. It can be seen that the SOP is close to 1 when transmission power is low. This is because the secrecy performance is

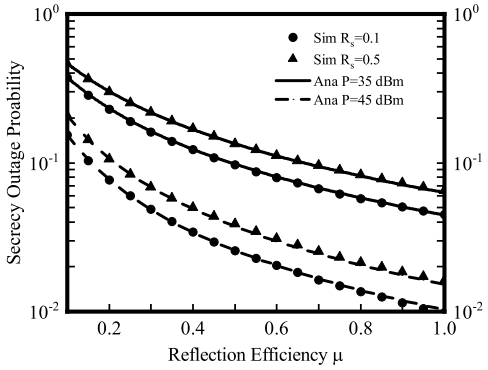

Fig. 3. SOP versus μ for different P values.

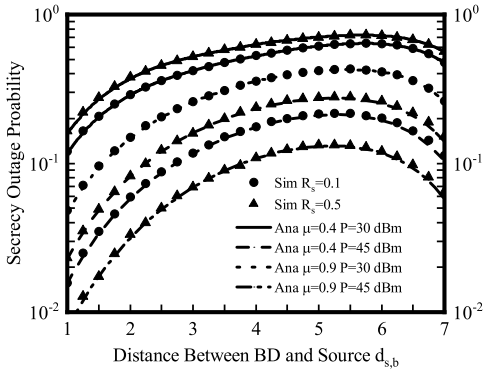

Fig. 4. SOP versus $d_{s,b}$ for different μ values.

poor at the destination caused by low reception SNR. In the high SNR regions, the asymptotic results are consistent with the numerical results and the analytical results. In addition, it can be found that the system security becomes strengthened with raising reflection efficiency and lowing secrecy rate threshold.

The SOP versus reflection efficiency for different transmission powers are plotted in Fig. 3. The system secrecy performance can be enhanced with increasing reflection efficiency, which is consistent with the above analysis. This is because raising reflection efficiency can amplify the strength of the backscattered signals, facilitating backscatter communication. Meanwhile, the risk of decoding is lessened by intensifying interference with the eavesdropper.

Fig. 4 illustrates the SOP versus distance between the source and BD for different reflection efficiencies. Here, we assume that the distance from the source to the destination is 8 m, and BD is located in the line between the source and the destination. When $d_{s,b}$ is small, BD can

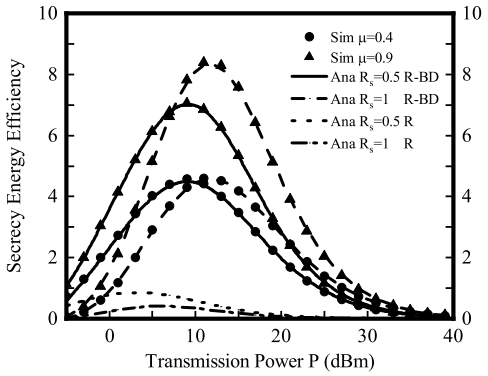

Fig. 5. SEE versus P for different μ and R_s values.

harvest more energy to reflect signals, heightening interference with the eavesdropper. Thus, the minimization SOP can be achieved. The curve rises because the energy harvested at BD is lessened with the distance between the source and BD becomes far, resulting in impaired backscatter communication. When distance between BD and the destination is less than the distance between BD and the eavesdropper, i.e., $d_{b,d} < d_{b,e}$, the capacity difference between legitimate reflection channel and eavesdropping reflection channel expands with the augmenting $d_{s,b}$, which is beneficial to ameliorate secrecy performance. Thus, the curve of SOP drops on the right side of Fig. 4. Similarly, when $d_{s,b}$ is about 5.5 m, the secrecy performance is the worst.

The SEE versus transmission power for different reflection efficiencies and secrecy rate thresholds are plotted in Fig. 5. When transmission power increases, the system security is heightened whereas SEE increases first, and then decreases, which means that there is critical point to maximize the SEE. This is because in the high SNR regions, the secrecy performance gain is less than 10^{-1} with the increasing transmission power, thus impairing SEE performance. Compared with only-relay communication systems, the proposed cooperative relay scheme with BD can significantly upgrade the system SEE. To maximize SEE, R_s is set to 1 is better than 0.5 when $\mu = 0.9$, but it needs more transmission power to achieve. Meanwhile, it can be seen that the greater SEE can be attained by reducing R_s when transmission power is lower. On the contrary, when transmission power is high, higher R_s enables better SEE performance. Thus, it can be inferred that the optimal SEE performance is achieved by adjusting both the secrecy rate threshold and transmission power. In addition, the SEE curve with high reflection efficiency is consistently higher than that with low reflection efficiency, which benefited from the improved energy utilization of BD. It is also shown that when SEE is maximum, the value of transmission

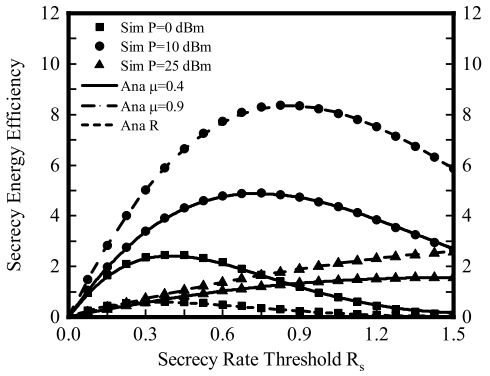

Fig. 6. SEE versus R_s for different P values.

power is about 10 dBm.

Fig. 6 reveals the variations of SEE versus secrecy rate threshold for different transmission powers. We can find that the maximum value of SEE appears when the transmitting power is about 10 dBm. Thus, we first analyze the impact of R_s on SEE when $P = 10$ dBm. It can be observed that SEE increases first and then decreases with increasing R_s. This is because when R_s is low, raising R_s can boost transmission rate on condition that the system security can be ensured, thus enhancing SEE. However, when R_s is high, the secrecy performance is damaged resulting in worse information leakage, thus SEE performance is degraded. In addition, when the transmission power is greater than 10 dBm, the secrecy performance becomes enhanced, thus the SEE curves can keep rising. In low R_s regions, it can be found that the values of SEE at low transmission power are not always lower than that of SEE when transmission power is high. Therefore, the value of R_s should be adjusted according to the transmission power for optimal SEE performance. On the other hand, it can be seen that the proposed cooperative communication network has obvious advantages in SEE compared with only-relay networks.

V. Conclusion

In this paper, a novel cooperative ABcom network with a DF relay was proposed, in which a wireless-powered BD acted not only as collaborator for assisting information transmission in the first time slot and as jammer for eavesdropper in both time slots. The secrecy performance and energy efficiency were studied by analyzing SEE and the derived closed-form/asymptotic expressions of SOP. Through analyzing, it is found that the system parameter settings have different effects on SOP and SEE. To be specific, elevating transmission power enhances se-

curity, whereas SEE first increases and then decreases. The SOP and SEE performance can be significantly strengthened by raising reflection efficiency. The effect of the secrecy rate threshold on the SEE is different under various transmission power conditions, thus the optimal threshold that maximize SEE should be adjusted according to the transmitting power. Furthermore, the system SOP and SEE performance can be enhanced by shortening the distance between the source and BD. These findings provided guidance to set system parameters for balancing the security and energy efficiency in cooperative ABcom communication networks.

APPENDIX A
PROOF OF THEOREM 1

The secrecy capacity C_S can be given as

$$C_S = \max\left(\frac{1}{2}\log\left(\frac{1+\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}{1+\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\right),0\right). \tag{A.1}$$

Due to the CDFs of the SNR and SINRs are not independent as well as the CDFs of $\gamma_D^{(2)}$ and $\gamma_E^{(2)}$. Thus, substituting (18) and (19) into (20), the SOP can be given as

$$P_{out} = \int_{\frac{\Phi}{P_s}}^{\infty}\int_{\frac{\Phi}{P_r}}^{\infty}\int_0^{\infty} F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(\left(\tau x+\tau-1\right)|t,u\right) f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\left(x|t,u\right)\mathrm{d}x f_{\left|g_{s,b}\right|^2}(t)\,\mathrm{d}t f_{\left|g_{r,b}\right|^2}(u)\,\mathrm{d}u, \tag{A.2}$$

where $\tau = 2^{2R_s}$, $f_{\left|g_{s,b}\right|^2}(t) = \frac{e^{-\frac{t}{\lambda_{sb}}}}{\lambda_{sb}}$ and $f_{\left|g_{r,b}\right|^2}(u) = \frac{e^{-\frac{u}{\lambda_{rb}}}}{\lambda_{rb}}$. $F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(x|t,u\right)$ can be expressed as

$$\begin{aligned} F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(x|t,u\right) &= \Pr\left(\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right) < x|t,u\right) \\ &= F_{\gamma_D^{(1)}}\left(x|t\right)\times F_{\gamma_D^{(2)}}\left(x|t,u\right), \end{aligned} \tag{A.3}$$

where

$$\begin{aligned} F_{\gamma_D^{(1)}}\left(x|t\right) &= \Pr\left(\gamma_D^{(1)} < x|t\right) \\ &= \Pr\left(\mu\beta_1 P_s t|g_{b,d}|^2 < x\sigma^2|t\right) \\ &= 1-e^{-\frac{x\sigma^2}{\mu P_s\left(t-\frac{\Phi}{P_s}\right)\lambda_{bd}}}. \end{aligned} \tag{A.4}$$

where β_1 is replaced by (15). The CDF of received SINR at the destination in the second time slot can be given as

$$\begin{aligned} F_{\gamma_D^{(2)}}\left(x\left|t,u\right.\right) &= \Pr\left(\min\left(\gamma_R,\gamma_D\right)<x\left|t,u\right.\right) \\ &= 1-\left[1-F_{\gamma_R}\left(x\left|t\right.\right)\right]\left[1-F_{\gamma_D}\left(x\left|u\right.\right)\right], \end{aligned} \tag{A.5}$$

where $\gamma_D=\frac{P_r\left|g_{r,d}\right|^2}{\mu\beta_2 P_r\left|g_{r,b}\right|^2\left|g_{b,d}\right|^2+\sigma^2}$, and β_2 is replaced by (16). $F_{\gamma_R}\left(x\right|t)$ can be written as

$$\begin{aligned} F_{\gamma_R}\left(x\right|t) &= \Pr\left(\frac{P_s|g_{s,r}|^2}{\mu\beta_1 P_s t|g_{b,r}|^2+\sigma^2}<x\middle|t\right) \\ &= \Pr\left(|g_{s,r}|^2<\mu|g_{b,r}|^2\left(t-\frac{\Phi}{P_s}\right)x+\frac{x\sigma^2}{P_s}\middle|t\right) \\ &= 1-\frac{\lambda_{sr}e^{-\frac{x\sigma^2}{P_s\lambda_{sr}}}}{\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{br}+\lambda_{sr}}. \end{aligned} \tag{A.6}$$

Similarly, $F_{\gamma_D}\left(x\right|u)$ can be written as

$$F_{\gamma_D}\left(x\right|u)=\Pr\left(\frac{P_r|g_{r,d}|^2}{\mu\beta_2 P_r u|g_{b,d}|^2+\sigma^2}<x\middle|u\right)=1-\frac{\lambda_{rd}e^{-\frac{x\sigma^2}{P_r\lambda_{rd}}}}{\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{bd}+\lambda_{rd}}. \tag{A.7}$$

Substituting (A.6) and (A.7) into (A.5), $F_{\gamma_D^{(2)}}\left(x\left|t,u\right.\right)$ can be obtained as

$$F_{\gamma_D^{(2)}}\left(x\left|t,u\right.\right)=1-\frac{\lambda_{sr}e^{-\frac{x\sigma^2}{P_s\lambda_{sr}}}}{\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{br}+\lambda_{sr}}\frac{\lambda_{rd}e^{-\frac{x\sigma^2}{P_s\lambda_{rd}}}}{\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{bd}+\lambda_{rd}}. \tag{A.8}$$

Thus, $F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(x\right)$ can be given by

$$F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}\left(x\left|t,u\right.\right)=\left(1-e^{-\frac{x\sigma^2}{\mu P_s\left(t-\frac{\Phi}{P_s}\right)\lambda_{bd}}}\right)\left(1-\frac{\lambda_{sr}e^{-\frac{x\sigma^2}{P_s\lambda_{sr}}}}{\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{br}+\lambda_{sr}}\frac{\lambda_{rd}e^{-\frac{x\sigma^2}{P_s\lambda_{rd}}}}{\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{bd}+\lambda_{rd}}\right). \tag{A.9}$$

Similarly, $F_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\left(x\right)$ can be written as

$$\begin{aligned} F_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}\left(x\left|t,u\right.\right) &= F_{\gamma_E^{(1)}}\left(x\right|t)\times F_{\gamma_E^{(2)}}\left(x\right|u) \\ &= \left(1-\frac{\lambda_{se}e^{-\frac{x\sigma^2}{P_s\lambda_{se}}}}{\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{be}+\lambda_{se}}\right)\left(1-\frac{\lambda_{re}e^{-\frac{x\sigma^2}{P_r\lambda_{re}}}}{\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{be}+\lambda_{re}}\right). \end{aligned} \tag{A.10}$$

$f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)$ can be derived as

$$f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x\,|t,u) = \left(\frac{\frac{\sigma^2}{P_s}e^{-\frac{x\sigma^2}{P_s\lambda_{se}}}}{\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{be}+\lambda_{se}} + \frac{\lambda_{se}\mu\left(t-\frac{\Phi}{P_s}\right)\lambda_{be}e^{-\frac{x\sigma^2}{P_s\lambda_{se}}}}{\left(\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{be}+\lambda_{se}\right)^2}\right) \times \left(1-\frac{\lambda_{re}e^{-\frac{x\sigma^2}{P_r\lambda_{re}}}}{\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{be}+\lambda_{re}}\right) + \left(1-\frac{\lambda_{se}e^{-\frac{x\sigma^2}{P_s\lambda_{se}}}}{\mu\left(t-\frac{\Phi}{P_s}\right)x\lambda_{be}+\lambda_{se}}\right) \times \left(\frac{\frac{\sigma^2}{P_r}e^{-\frac{x\sigma^2}{P_r\lambda_{re}}}}{\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{be}+\lambda_{re}} + \frac{\lambda_{re}\mu\left(u-\frac{\Phi}{P_r}\right)\lambda_{be}e^{-\frac{x\sigma^2}{P_r\lambda_{re}}}}{\left(\mu\left(u-\frac{\Phi}{P_r}\right)x\lambda_{be}+\lambda_{re}\right)^2}\right). \quad \text{(A.11)}$$

APPENDIX B
PROOF OF THEOREM 2

The SOP for channel uncorrelation scheme can be expressed as

$$P_{out} = \int_0^\infty F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}(\tau x+\tau-1)\, f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)\,\mathrm{d}x, \quad \text{(B.1)}$$

where $F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}(x)$ can be expressed as

$$\begin{aligned} F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}(x) &= \Pr\left(\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)<x\right) \\ &= F_{\gamma_D^{(1)}}(x)\times F_{\gamma_D^{(2)}}(x). \end{aligned} \quad \text{(B.2)}$$

$F_{\gamma_D^{(1)}}(x)$ can be written as

$$\begin{aligned} F_{\gamma_D^{(1)}}(x) &= \Pr\left(|g_{b,d}|^2 < \frac{x}{\mu P_s\left(|g_{s,b}|^2-\frac{\Phi}{P_s}\right)}\right) \\ &= \int_{\frac{\Phi}{P_s}}^\infty \int_0^{\frac{x}{\mu P_s\left(y-\frac{\Phi}{P_s}\right)}} f_{|g_{b,d}|^2}(z)\, f_{|g_{s,b}|^2}(y)\,\mathrm{d}z\mathrm{d}y, \\ &= e^{-\frac{\Phi}{P_s\lambda_{sb}}} - \frac{e^{-\frac{\Phi}{P_s\lambda_{sb}}}}{\lambda_{sb}}\int_0^\infty e^{-\frac{x}{\mu P_s y\lambda_{bd}}-\frac{y}{\lambda_{sb}}}\mathrm{d}y, \end{aligned} \quad \text{(B.3)}$$

where $f_{|g_{s,b}|^2}(y) = \frac{e^{-\frac{y}{\lambda_{sb}}}}{\lambda_{sb}}$, $f_{|g_{b,d}|^2}(z) = \frac{e^{-\frac{z}{\lambda_{bd}}}}{\lambda_{bd}}$ and the integral can be resolved by [38, eq.(3.324.1)]. The $F_{\gamma_D^{(1)}}(x)$ can be expressed as

$$F_{\gamma_D^{(1)}}(x) = e^{-\frac{\Phi}{P_s\lambda_{sb}}}\left(1-2\sqrt{Q_1}K_1\left(2\sqrt{Q_1}\right)\right). \quad \text{(B.4)}$$

$$
\begin{aligned}
F_{\gamma_R}(x) &= \Pr\left(\frac{P_s|g_{s,r}|^2}{\mu\beta_1 P_s|g_{s,b}|^2|g_{b,r}|^2+\sigma^2} < x\right) = \Pr\left(|g_{s,r}|^2 < \mu|g_{b,r}|^2\left(|g_{s,b}|^2 - \frac{\Phi}{P_s}\right)x + \frac{x\sigma^2}{P_s}\right) \\
&= \int_{\frac{\Phi}{P_s}}^{\infty}\int_0^{\infty}\left(1 - e^{-z\mu\left(y-\frac{\Phi}{P_s}\right)\frac{x}{\lambda_{sr}} - \frac{x\sigma^2}{P_s\lambda_{sr}}}\right) f_{|g_{b,r}|^2}(z)\, f_{|g_{s,b}|}(y)\,\mathrm{d}z\mathrm{d}y \\
&= \int_{\frac{\Phi}{P_s}}^{\infty}\frac{e^{-\frac{y}{\lambda_{sb}}}}{\lambda_{sb}}\mathrm{d}y \; - \int_0^{\infty}\int_{\frac{\Phi}{P_s}}^{\infty} e^{-z\mu\left(y-\frac{\Phi}{P_s}\right)\frac{x}{\lambda_{sr}} - \frac{x\sigma^2}{P_s\lambda_{sr}}}\; \frac{e^{-\frac{y}{\lambda_{sb}}}}{\lambda_{sb}}\mathrm{d}y\, f_{|g_{b,r}|^2}(z)\,\mathrm{d}z \\
&= e^{-\frac{\Phi}{P_s\lambda_{sb}}} - \frac{\lambda_{sr}e^{-\frac{x\sigma^2}{P_s\lambda_{sr}} - \frac{\Phi}{P_s\lambda_{sb}}}}{\lambda_{br}} \underbrace{\int_0^{\infty}\frac{e^{-\frac{z}{\lambda_{br}}}}{zx\mu\lambda_{sb}+\lambda_{sr}}\mathrm{d}z}_{I_1} \\
&= e^{-\frac{\Phi}{P_s\lambda_{sb}}} + \frac{\lambda_{sr}e^{\frac{\lambda_{sr}}{x\mu\lambda_{sb}\lambda_{br}} - \frac{x\sigma^2}{P_s\lambda_{sr}} - \frac{\Phi}{P_s\lambda_{sb}}}}{x\mu\lambda_{br}\lambda_{sb}}\mathrm{Ei}\left(-\frac{\lambda_{sr}}{x\mu\lambda_{sb}\lambda_{br}}\right).
\end{aligned} \tag{B.6}
$$

---

where $Q_1 = \frac{x}{\mu P_s\lambda_{sb}\lambda_{bd}}$. The CDF of received SINR at the destination in the second time slot can be given as

$$
\begin{aligned}
F_{\gamma_D^{(2)}}(x) &= \Pr\left(\min\left(\gamma_R, \gamma_D\right) < x\right) \\
&= 1 - \left[1 - F_{\gamma_R}(x)\right]\left[1 - F_{\gamma_D}(x)\right],
\end{aligned} \tag{B.5}
$$

where $\gamma_D = \frac{P_r\left|g_{r,d}\right|^2}{\mu\beta_2 P_r\left|g_{r,b}\right|^2\left|g_{b,d}\right|^2+\sigma^2}$, and β_2 is replaced by (16). $F_{\gamma_R}(x)$ can be written as (B.6), where the integral I_1 can be resolved by [38, eq.(3.352.4)].

Similarly, $F_{\gamma_D}(x)$ can be written as

$$
F_{\gamma_D}(x) = e^{-\frac{\Phi}{P_r\lambda_{rb}}} + \frac{\lambda_{rd}e^{\frac{\lambda_{rd}}{x\mu\lambda_{rb}\lambda_{bd}} - \frac{x}{P_r\lambda_{rd}} - \frac{\Phi}{P_r\lambda_{rb}}}}{x\mu\lambda_{rb}\lambda_{bd}}\mathrm{Ei}\left(-\frac{\lambda_{rd}}{x\mu\lambda_{rb}\lambda_{bd}}\right). \tag{B.7}
$$

Substituting (B.6) and (B.7) into (B.5), $F_{\gamma_D^{(2)}}(x)$ can be obtained as

$$
F_{\gamma_D^{(2)}}(x) = 1 - \left(1 - e^{-\frac{\Phi}{P_s\lambda_{sb}}}\left(1 + Q_2 e^{Q_2 - \frac{x}{P_s\lambda_{sr}}}\mathrm{Ei}\left(-Q_2\right)\right)\right)\left(1 - e^{-\frac{\Phi}{P_r\lambda_{rb}}}\left(1 + Q_3 e^{Q_3 - \frac{x}{P_r\lambda_{rd}}}\mathrm{Ei}\left(-Q_3\right)\right)\right), \tag{B.8}
$$

where $Q_2 = \frac{\lambda_{sr}}{x\mu\lambda_{sb}\lambda_{br}}$ and $Q_3 = \frac{\lambda_{rd}}{x\mu\lambda_{rb}\lambda_{bd}}$. Thus, $F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}(x)$ can be given by

$$
\begin{aligned}
F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}(x) &= e^{-\frac{\Phi}{P_s\lambda_{sb}}}\left(1 - 2\sqrt{Q_1}K_1\left(2\sqrt{Q_1}\right)\right) \\
&\times \left(1 - \left(1 - e^{-\frac{\Phi}{P_s\lambda_{sb}}}\left(1 + Q_2 e^{Q_2 - \frac{x}{P_s\lambda_{sr}}}\mathrm{Ei}\left(-Q_2\right)\right)\right)\left(1 - e^{-\frac{\Phi}{P_r\lambda_{rb}}}\left(1 + Q_3 e^{Q_3 - \frac{x}{P_r\lambda_{rd}}}\mathrm{Ei}\left(-Q_3\right)\right)\right)\right).
\end{aligned} \tag{B.9}
$$

$$f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)=e^{-\frac{\Phi}{P_r\lambda_{rb}}-\frac{\Phi}{P_s\lambda_{sb}}}\left[\begin{array}{l}\frac{-Q_4e^{-\frac{x\sigma^2}{P_r\lambda_{re}}+Q_4}\mathrm{Ei}(-Q_4)}{x}\left(1+Q_4+\frac{x\sigma^2}{P_r\lambda_{re}}+\frac{e^{-Q_4}}{\mathrm{Ei}(-Q4)}\right)\\ \times\left(1+Q_5e^{Q_5-\frac{x\sigma^2}{P_s\lambda_{se}}}\mathrm{Ei}\left(-Q_5\right)\right)-\frac{Q_5e^{-\frac{x\sigma^2}{P_s\lambda_{se}}+Q_5}\mathrm{Ei}(-Q_5)}{x}\\ \times\left(1+Q_4e^{Q_4-\frac{x\sigma^2}{P_r\lambda_{re}}}\mathrm{Ei}\left(-Q_4\right)\right)\left(1+Q_5+\frac{x\sigma^2}{P_s\lambda_{se}}+\frac{e^{-Q_5}}{\mathrm{Ei}(-Q_5)}\right)\end{array}\right] \tag{B.11}$$

Similarly, $F_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)$ can be written as

$$F_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)=e^{-\frac{\Phi}{P_r\lambda_{rb}}-\frac{\Phi}{P_s\lambda_{sb}}}\left(1+Q_4e^{Q_4-\frac{x\sigma^2}{P_r\lambda_{re}}}\mathrm{Ei}\left(-Q_4\right)\right)\left(1+Q_5e^{Q_5-\frac{x\sigma^2}{P_s\lambda_{se}}}\mathrm{Ei}\left(-Q_5\right)\right), \tag{B.10}$$

where $Q_4=\frac{\lambda_{re}}{x\mu\lambda_{rb}\lambda_{be}}$ and $Q_5=\frac{\lambda_{se}}{x\mu\lambda_{sb}\lambda_{be}}$. $f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)$ can be derived as (B.11).

From substituting (B.9) and (B.11) into (B.1), we can know that the expression of SOP is difficult to calculate by direct integration. Thus, the solution appeals to Gaussian Chebyshev approximation [27]. We make the function $\omega(x)=F_{\max\left(\gamma_D^{(1)},\gamma_D^{(2)}\right)}(\tau x+x-1)f_{\max\left(\gamma_E^{(1)},\gamma_E^{(2)}\right)}(x)$. It can be derived that $\omega'(x)<0$ and $\lim_{x\to\infty}\omega(x)=0$. Thus, when M is a large number, we have $\int_M^{\infty}\omega(x)\,\mathrm{d}x\ \to\ 0$. Equation (B.1) is expressed as $P_{out}=\int_0^M\omega(x)\,\mathrm{d}x$. By using Gaussian Chebyshev approximation, (24) can be obtained.

REFERENCES

[1] Z. Abdullah, G. Chen, S. Lambotharan, and J. A. Chambers, "Optimization of intelligent reflecting surface assisted full-duplex relay networks," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 363–367, Feb. 2021.

[2] G. Chen, J. P. Coon, A. Mondal, B. Allen, and J. A. Chambers, "Performance analysis for multihop full-duplex IoT networks subject to poisson distributed interferers," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3467–3479, Apr. 2019.

[3] G. Li, H. Liu, G. Huang, X. Li, B. Raj, and F. Kara, "Effective capacity analysis of reconfigurable intelligent surfaces aided NOMA network," *EURASIP Journal on Wireless Communications and Networking*, vol. 198, pp. 1–16, Dec. 2021.

[4] X. Li, M. Zhao, M. Zeng, S. Mumtaz, V. G. Menon, Z. Ding, and O. A. Dobre, "Hardware impaired ambient backscatter NOMA systems: Reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, Apr. 2021.

[5] L. Shi, Y. Ye, R. Q. Hu, and H. Zhang, "System outage performance for three-step two-way energy harvesting DF relaying," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3600–3612, Apr. 2019.

[6] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. K. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green internet-of-things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, Sep. 2021.

[7] W. Zhao, G. Wang, S. Atapattu, C. Tellambura, and H. Guan, "Outage analysis of ambient backscatter communication systems," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1736–1739, Aug. 2018.

[8] D. Li, "Backscatter communication powered by selective relaying," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 14 037–14 042, Nov. 2020.

[9] X. Li, H. Liu, G. Li, Y. Liu, M. Zeng, and Z. Ding, "Effective capacity analysis of AmBC-NOMA communication systems," *IEEE Transactions on Vehicular Technology*, pp. 1–6, Jun. 2022.

[10] H. Wang, J. Jiang, G. Huang, W. Wang, D. Deng, B. M. ElHalawany, and X. Li, "Physical layer security of two-way ambient backscatter communication systems," *Wireless Communications and Mobile Computing*, vol. 2022, Mar. 2022.

[11] R. Du, T. Ohlson Timoudas, and C. Fischione, "Comparing backscatter communication and energy harvesting in massive IoT networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 429–443, Jan. 2022.

[12] Y. Liu, Y. Ye, G. Yan, and Y. Zhao, "Outage performance analysis for an opportunistic source selection based two-way cooperative ambient backscatter communication system," *IEEE Communications Letters*, vol. 25, no. 2, pp. 437–441, Feb. 2021.

[13] D. Li, "Two birds with one stone: Exploiting decode-and-forward relaying for opportunistic ambient backscattering," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1405–1416, Mar. 2020.

[14] S. T. Shah, K. W. Choi, T.-J. Lee, and M. Y. Chung, "Outage probability and throughput analysis of SWIPT enabled cognitive relay network with ambient backscatter," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3198–3208, Aug. 2018.

[15] D. Li, "Backscatter communication via harvest-then-transmit relaying," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6843–6847, Jun. 2020.

[16] R. M. Ferdous, A. W. Reza, and M. F. Siddiqui, "Renewable energy harvesting for wireless sensors using passive RFID tag technology: A review," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1114–1128, May 2016.

[17] Y. Xu and G. Gui, "Optimal resource allocation for wireless powered multi-carrier backscatter communication networks," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1191–1195, Aug. 2020.

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

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

[20] L. Shi, R. Q. Hu, Y. Ye, and H. Zhang, "Modeling and performance analysis for ambient backscattering underlaying cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6563–6577, Jun. 2020.

[21] Y. Ye, L. Shi, R. Qingyang Hu, and G. Lu, "Energy-efficient resource allocation for wirelessly powered backscatter communications," *IEEE Communications Letters*, vol. 23, no. 8, pp. 1418–1422, Aug. 2019.

[22] X. Liu, Y. Gao, and F. Hu, "Optimal time scheduling scheme for wireless powered ambient backscatter communications in IoT networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2264–2272, Apr. 2019.

[23] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 1861–1874, May 2016.

[24] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[25] T. S. Muratkar, A. Bhurane, P. K. Sharma, and A. Kothari, "Physical layer security analysis in ambient backscatter communication with node mobility and imperfect channel estimation," *IEEE Communications Letters*, vol. 26, no. 1, pp. 27–30, Jan. 2022.

[26] M. Li, X. Yang, F. Khan, M. A. Jan, W. Chen, and Z. Han, "Improving physical layer security in vehicles and pedestrians networks with ambient backscatter communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9380–9390, Jul. 2022.

[27] Q. Zhang, L. Zhang, Y.-C. Liang, and P.-Y. Kam, "Backscatter-NOMA: A symbiotic system of cellular and internet-of-things networks," *IEEE Access*, vol. 7, pp. 20 000–20 013, 2019.

[28] H. Ding, D. B. da Costa, and J. Ge, "Outage analysis for cooperative ambient backscatter systems," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 601–605, May 2020.

[29] Y. Xu, Z. Qin, G. Gui, H. Gacanin, H. Sari, and F. Adachi, "Energy efficiency maximization in NOMA enabled backscatter communications with QoS guarantee," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 353–357, Feb. 2021.

[30] D. Wang, B. Bai, W. Chen, and Z. Han, "Energy efficient secure communication over decode-and-forward relay channels," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 892–905, Mar. 2015.

[31] M. El-Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1909–1920, Sep. 2013.

[32] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[33] M. Li, X. Tao, N. Li, H. Wu, and J. Xu, "Secrecy energy efficiency maximization in UAV-enabled wireless sensor networks without eavesdropper's CSI," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3346–3358, Mar. 2022.

[34] S. Xu, X. Song, S. Li, J. Cao, J. Zhu, and Z. Xie, "Cooperative encryption over backscatter: Secure green communication for two-way energy harvesting relay networks," *ICT Express*, 2022.

[35] G. Chen, P. Xiao, J. R. Kelly, B. Li, and R. Tafazolli, "Full-duplex wireless-powered relay in two way cooperative networks," *IEEE Access*, vol. 5, pp. 1548–1558, 2017.

[36] S. Wang, M. Xia, K. Huang, and Y.-C. Wu, "Wirelessly powered two-way communication with nonlinear energy harvesting model: Rate regions under fixed and mobile relay," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8190–8204, Dec. 2017.

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

[38] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic Press, 2007.