Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 7845107, 11 pages
https://doi.org/10.1155/2020/7845107

Research Article

Secure Green-Oriented Multiuser Scheduling for Wireless-Powered Internet of Things

Xiaohui Shang,[1,2] **Hao Yin**,[2] **Aijun Liu**,[1] **Mu Li**,[1,2] **Yida Wang**,[1] **and Yong Wang**[1]

[1]*College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China*
[2]*Institute of Systems Engineering, AMS, Beijing 100039, China*

Correspondence should be addressed to Xiaohui Shang; shangxiaohui1214@126.com

Received 20 June 2019; Revised 7 August 2019; Accepted 30 August 2019; Published 7 January 2020

Guest Editor: Hasan Ali Khattak

In this paper, we consider the secure green-oriented multiuser scheduling for the wireless-powered Internet of Things (IoT) scenario, in which multiple source sensors communicate with a controller assisted by an intermediate sensor with the existence of a passive tapping device. Due to the limited energy, all sensors must acquire energy from external power beacons (PBs). Specifically, for the security improvement, we introduce two multiuser scheduling schemes possessing the optimal PB chosen by the relay, i.e., the best source sensor is scheduled in a random way (BSR), while the best source sensor is decided by the best PB (BSBP). Furthermore, for every scheme, we derive the analytical expressions for the secrecy outage probability (SOP) and investigate the secure energy efficiency (SEE) optimization problem with constricted transmission power in PBs. Simulation results reveal that the BSBP scheme provides better secrecy performance, and elevating the PBs quantity or reducing both the ratio of distance from PBs to source users and the total communication distance to some extent is helpful for improving SEE. In addition, the time-switching factor shows an important effect upon secrecy performance of the considered system.

1. Introduction

As the key architecture of the fifth generation (5G) mobile communication system, the Internet of Things (IoT) has attracted more and more attention [1]. The primary driving thought for the prospective IoT has relation with smart sensors, and wireless sensor networks (WSNs) have been observed as key enablers of IoT applications recently, where multiple sensor nodes are caused by instant or periodic data acquisition in multiple environments [2]. However, among various types of IoT sensors, most of the objects are resource-constrained, battery-powered, and characterized by both of the low energy and poor computation capacity, resulting in the one of the biggest barrier impeding generalization of IoT in the future which is the limitation of energy [3]. Meanwhile, the rapid development of IoT will give rise to the massive deployment of sensor nodes and a vast amount of information exchange, making it unfeasible to flexibly recharge and control the power-constricted devices. Due to the rising power costs, green-oriented methods have inevitably become the dominating design consideration in the IoT system. Fortunately, far-field wireless energy transfer (WET), which enables wireless devices to acquire energy from the broadcast signals for their operation and information exchange, has considered as an appealing method to provide consistent and stable energy to power-constrained users of IoT, particularly when traditional energy harvesting (EH) techniques from reproducible energy sources are inapplicable [4]. Such a new communication type is known as wireless-powered communication (WPC), where the wireless users of IoT are powered through surrounding electromagnetic signals, which is likely to be dedicated wireless transmitters utilized to charge wireless terminals. As such, it can completely eliminate the burden of battery renewal and/or recharging, avoid the interruption caused by the running out of power, and provide networks with theoretically perpetual lifespans [5].

Generally, a basic hurdle of wireless transmission upon the basis of WPC rest with the fast attenuation of radio frequency (RF) signals with distance changing. Moreover,

energy amount acquired at wireless-powered devices is fairly restricted, which limits the coverage severely and has become a bottleneck for the widespread application of WPC. Consequently, the design of energy-efficient transmission is of great significance for transforming the green concept into future wireless-powered IoT. Although the harvested energy from RF signals appears to be inefficient and the WPC-based wireless communication seems to be not widely available at the current stage, practical applications for power-constrained devices of IoT have already been investigated, and more feasible applications will be implemented in the near future [6–8]. Until now, a lot of research efforts have also been devoted to explore the advantages of WPC in most applications of IoT since it could be easily combined with wireless terminals [9–13]. Specifically, typical wireless-powered communication networks (WPCN) were investigated in [9], where introduction of a dynamic time division multiple access (TDMA) protocol was performed for a multiuser WPCN, and the best time allocation for the downlink WPC and the uplink wireless information transmission (WIT) had been analyzed. Until now, the studies on WPCN have been extended to various communication systems. In particular, a joint wireless power transfer (WPT) and relay selection method were proposed for WPCN in [10], where the source and relays utilize the time-switching-based RF-EH method to acquire energy from a power beacon (PB) with multiple antennas. Differently, secrecy performance discussion of EH wireless sensor networks was examined in [11], where the authors proposed an optimization method, in which a wireless-powered friendly jammer was utilized for improving the secrecy performance of the considered model. Furthermore, the authors in [12] analyzed the secrecy performance of the EH sensor system and proposed a best-relay-and-best-jammer protocol for enhancing the secrecy of a system with the source user and multiple sensor relays harvesting energy from diverse PBs. Recently, inspired by abovementioned works, a secure energy-efficient transmission design for wireless-powered IoT possessing various PBs was investigated in [13], where the authors introduce different relay selection schemes possessing the optimal PB under the selection of the single source and solve the optimization problem of secure energy efficiency (SEE). It is worth mentioning that above works mostly focused on the secrecy performance improvement contributed by relay selection, while ignored the practical scenario with multiusers, which can be considered as the typical application of IoT.

1.1. Related Works. Remarkably, in an effort to reduce the complexity and the costs of resource-constricted wireless-powered IoT, the multiuser scheduling has drawn wide attention due to the significant potential performance improvement [14–19]. Particularly, the authors in [14] explore the largest energy efficiency for multiuser WPCN by joint power control and time allocation while taking account of the initial battery energy level of all the users. Furthermore, the authors in [15] applied the notion of proportional fair scheduling to WPCN and overcome the doubly near fair problem by an opportunistic scheme. Meanwhile, in a multiuser system, the authors in [16] consider multiuser scheduling criteria taking into account cochannel interference in a multicell environment and propose an adaptive scheduling scheme. Then, in a WPCN-based multi-input multioutput (MU-MIMO) multiuser system, [17] proposes a zero-forcing-based transmission method by a downlink energy beamformer to optimize the related parameters. Afterwards, the authors in [18] concentrate on an MIMO-WPCN, in which a dedicated multiantenna PB transfers RF energy to some starve users, and then these users send required information to the destination. And, last but not the least, [19] focuses on the cumulative transmission framework of multiuser scheduling in full-duplex wireless-powered IoT system and designs a novel throughput-oriented scheduling strategy, which models the dynamic charging and discharging procedures for all the devices in IoT as a finite-state Markov chain.

On the contrary, the broadcast characteristics of wireless transmission make the WPT and WIT more vulnerable to malicious attacks, turning secure transmission into a burdensome task [20]. Typically, the upper layer cryptographic techniques are explored for securing the privacy information against intercepting in traditional wireless transmissions [21]. However, conventional cryptographic technology is limited in wireless-powered IoT because of the requirements of high hardware complicacy and massive energy [22]. Furthermore, an eavesdropper (Eve) possessing unlimited computing capacity is likely to make such technology compromised [23]. Fortunately, physical layer security (PLS), as a promising approach to make sure the safety of wireless communication, has been a high-effectiveness supplement to current solutions. As far as wireless PLS is concerned, the fundamental thought is to utilize the features of wireless channels for transmitting information in a reliable manner from the source to the intended receiver and to make sure the privacy of the information, to put in different way, not to be intercepted or eavesdropped [24]. Currently, PLS has been broadly deployed for ensuring security of future wireless networks [25, 26] because it can provide the security of new network architectures such as the IoT. In recent years, some literatures have explored secure communications in multiuser-scheduling-aided WPCN [27, 28]. Specifically, [27] investigates the secrecy performance of dual-hop multiuser relay system by exploiting the maximal ratio transmission (MRT) scheme and proposes a threshold-based multiuser scheduling method. On the contrary, the authors in [28] consider a multiantenna wireless network, in which the base station and the users have been given with multiple antennas. However, it is worth noting that few works have considered the SEE in wireless-powered IoT scenario.

1.2. Paper Contributions and Organization. Enlightened by the aforementioned observations, this paper focuses on the secrecy performance analysis of a typical wireless-powered IoT, in which multiple source sensors that perform monitoring or operating tasks in a localized group and an

intermediate node performs as relay are powered by multiple dedicated PBs. Furthermore, we propose two multiuser scheduling schemes and compare their secrecy performance for providing the secure energy-efficient transmissions. The main contributions of our work are listed as follows:

(i) We explore the PLS in the wireless-powered IoT and propose two green-oriented multiuser scheduling schemes, in which the optimal PB is decided by the relay; meanwhile, the best source is scheduled in a random way (BSR) or chosen by the best PB (BSBP), respectively.

(ii) For the two proposed schemes, we obtain the closed-form expressions of the secrecy outage probability (SOP) and solve the SEE optimization problem with constrained transmission power in PB by resorting to the searching method. Compared with the BSR scheme characterized by lower complexity and simpler application, the BSBP scheme can make full use of the power transfer links contributed by diverse PBs and present the better secrecy performance.

(iii) Simulation results demonstrate that increasing the number of PBs is favorable to improve the SEE of the studied scenario. Meanwhile, decreasing both the ratio of distance from PBs to the sources and the total communication distance to some extent is advantageous for SEE. Additionally, the time-switching factor has an important effect upon the secrecy performance of the considered system, which is worth designing and optimizing carefully.

The remaining part of this paper is summarized as follows. Section 2 provides details concerning the system model, the process of WPT, signal analysis, and two proposed multiuser scheduling schemes. Section 3 derives the exact SOP of BSR and BSBP schemes, respectively. Then, in Section 4, the SEE optimization research is given. The simulation results are presented in Section 5. Eventually, conclusions of this paper are drawn in Section 6.

2. System and Channel Model

The system model, the process of WPT, signal analysis, and two multiuser scheduling strategies are presented in this section.

2.1. System Model. Consider a dual-hop multiuser uplink WPCN for the IoT application as illustrated in Figure 1, where multiple source users S_n, $n \in \mathcal{M} = \{1, \ldots, N\}$ communicate with the controller D aided by the decode-and-forward (DF) relay, and are overheard by the passive Eve E. Considering the constricted coverage of sensors, we assume the direct $S_n \longrightarrow D$ link is not available [10]. Meanwhile, owing to the limitation of energy in the IoT system, S_n and R have to gain energy by WPT from a selected P_m, $m \in \mathcal{M} = \{1, \ldots, M\}$ to support data transmission. And, the controller is powered by on-grid power. Apart from that, considering the size and cost limitations, it is assumed that, in each sensor, the destination D and the Eve E are single-antenna and half-duplex devices [12]. It is worth highlighting that the above configurations have numerous practical applications, such as in IoT, where the multiple source sensors upload information via a certain sensor (performs as relay) that is limited to a single antenna due to size limitations and cost.

Furthermore, we consider that each link will be affected by Rayleigh fading. Thus, the power gains of the channel are subject to exponential distribution with parameter λ_{XY}, where $X \in \{P_m, S_n, R\}$ and $Y \in \{S_n, R, E, D\}$. Meanwhile, the additive white Gaussian noise (AWGN) at R and D has zero mean and variance N_0. Compared with the full channel state information (CSI) assumption in [12, 27], where perfect CSI is considered in order to investigate the performance bound, we consider only the statistic CSI can be acquired, which is more practical due to the weak computation ability and small memory of sensors. The specific estimation method for obtaining CSI is shown in [29]. In practice, when the eavesdropper is a member of the network and wants to interpret information that is not passed on to him, the partial CSI of the wiretap link is available.

In order to facilitate mathematical modeling, the channel coefficients of the $P_m \longrightarrow S_n$, $P_m \longrightarrow R$, $S_n \longrightarrow R$, $S_n \longrightarrow E$, $R \longrightarrow E$, and $R \longrightarrow D$ transmission channels are represented by $h_{P_m S_n}$, $h_{P_m R}$, $h_{S_n R}$, $h_{S_n E}$, h_{RE}, and h_{RD}, respectively, which are independent and distributed in an identical manner (i.i.d.) from one block to next. Meanwhile, the distances of the $P_m \longrightarrow S_n$, $P_m \longrightarrow R$, $S_n \longrightarrow R$, $S_n \longrightarrow E$, $R \longrightarrow E$, and $R \longrightarrow D$ transmission links are represented by $d_{P_m S_n}$, $d_{P_m R}$, $d_{S_n R}$, $d_{S_n E}$, d_{RE}, and d_{RD}, respectively. Furthermore, it is assumed that the multiple PBs and multiple source users are close in proximity, i.e., a certain clustering protocol in place. This assumption is generally used in the WPCN [12], which brings about the equivalent mean channel power gains of the channels $P_m \longrightarrow S_n$, $P_m \longrightarrow R$, $S_n \longrightarrow R$, and $S_n \longrightarrow E$, respectively. For convenience, we define $\lambda_{P_m S_n} = \lambda_{PS}$, $\lambda_{P_m R} = \lambda_{PR}$, $\lambda_{S_n R} = \lambda_{SR}$, and $\lambda_{S_n E} = \lambda_{SE}$ for any $m \in \mathcal{M}$ and $n \in \mathcal{N}$.

2.2. Wireless Power Transfer. In the WPT process, the receiver adopts the EH model based on rectangular antenna structure. For the rectangular antenna, the received signal can be converted into a direct current (DC) signal by a rectifier consisting of a passive low-pass filter (LPF) and a Schottky diode [30]. Then, it is considered that the harvested energy by all users at the stage of WPT is entirely used to transmit message in WIT, which is known as the harvest-use (HU) mode as in [31]. This consideration is practical for devices of IoT because they are limited by the size and cost, which leads to the smaller batteries. As for the relaying strategy, the time-switching-based receiver (TSR) protocol is applied in the data transmission, thanks to its high throughput compared with power splitting-based receiver (PSR) protocol [32]. In particular, the duration between two successive data transmission is defined as a transfer time slot T, αT denotes the time of WPT, and $(1 - \alpha)T$ represents the duration of WIT as

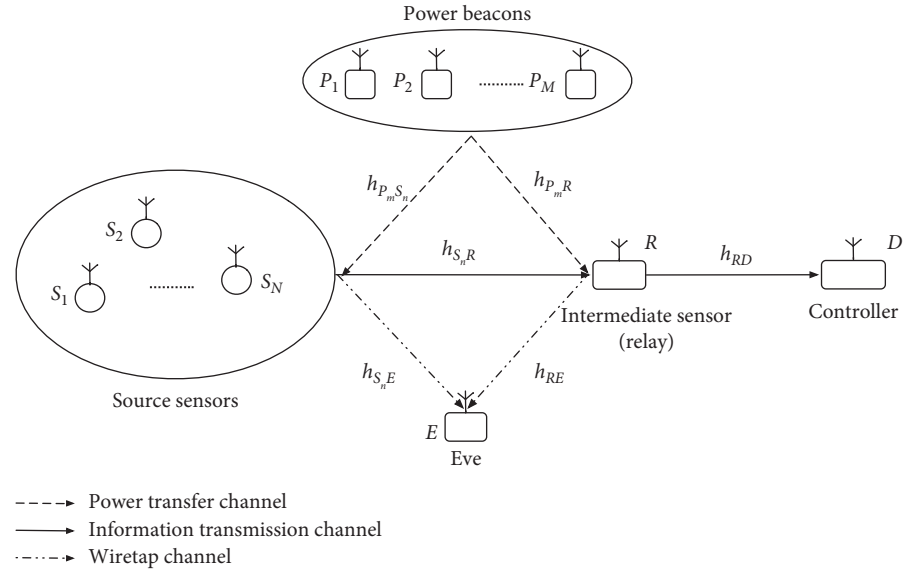

Figure 1: System model.

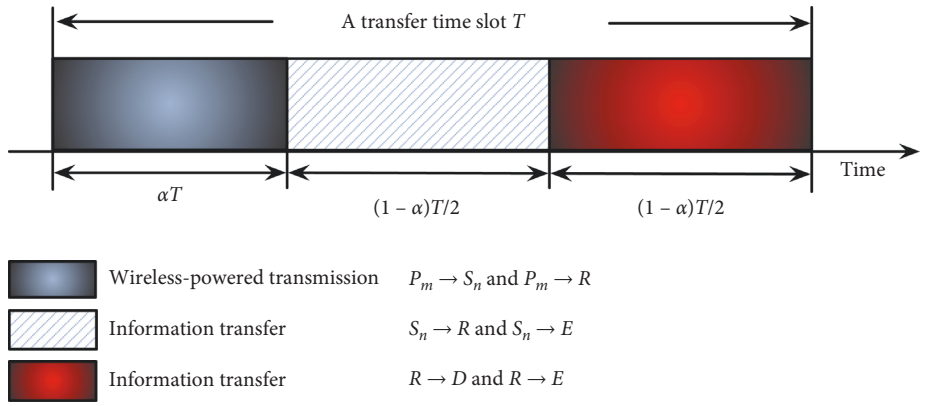

Figure 2: Time-switching relaying strategy. The communication time slot T is applied for WPT and WIT, where αT is applied for harvesting energy from the chosen PB; meanwhile, the rest time $(1-\alpha)T$ is provided to send the data from the source user to the controller D.

illustrated in Figure 2, where $\alpha \in (0,1)$ is the time-switching coefficient. Based on the dual-hop communication, the time window of WIT is divided into two parts, i.e., $(1-\alpha)T/2$ is for $S_n \longrightarrow R$ and the remaining $(1-\alpha)\ T/2$ is provided for $R \longrightarrow D$.

Then, we consider the scenario that a particular PB is activated, while other PBs remain silent in order to reduce the computational complexity and energy consumption, because PB selection is an green-oriented WPT scheme [12]. To be more specific, the PB with the best link for the $P_m \longrightarrow R$ channel is chosen to implement WPT for S_n and R. The index of certain PB can be expressed as

$$m^* = \arg\max_{m \in \mathcal{M}} \left\{ \left| h_{P_mR} \right|^2 \right\}, \tag{1}$$

where $|h_{P_mR}|^2$ is power gain of the link from the selected P_m to R. Furthermore, the harvested energy at S_n and R can be expressed as follows [33]:

$$E_{S_n} = \eta P_B \alpha T \frac{\left| h_{P_{m^*}S_n} \right|^2}{d^{\theta}_{P_{m^*}S_n}} = \eta P_B \alpha T \gamma_{P_{m^*}S_n},$$
$$E_R = \eta P_B \alpha T \frac{\left| h_{P_{m^*}R} \right|^2}{d^{\theta}_{P_{m^*}R}} = \eta P_B \alpha T \gamma_{P_{m^*}R}, \tag{2}$$

where $10\% < \eta < 80\%$ denotes the EH efficiency factor, which is mainly determined by the EH circuitry and frequencies (e.g., 15 MHz–2.5 GHz) [34]; P_B represents the transmit power of the PBs; θ is the path loss exponent; $|h_{P_{m^*}S_n}|^2$ and $|h_{P_{m^*}R}|^2$ are power gains of the channels from the selected P_m to S_n and R, respectively; $\gamma_{P_{m^*}S_n} = |h_{P_{m^*}S_n}|^2 / d^{\theta}_{P_{m^*}S_n}$ and $\gamma_{P_{m^*}R} = |h_{P_{m^*}R}|^2 / d^{\theta}_{P_{m^*}R}$. Note that we neglect the harvested energy from the noise since the source users and the relay sensor are passive, and their received noise powers are much smaller than the received powers contributed by the PBs [35].

Lemma 1. *If X_k, $k \in \mathcal{K} = \{1, \ldots, K\}$, is the random variable subject to the exponential i.i.d, the probability density function (PDF) and the cumulative distribution function (CDF) of $X = \max_{k\in\mathcal{K}}\{X_k\}$ can be expressed by*

$$f_X(x) = K\lambda_X e^{-\lambda_X x}\left(1 - e^{-\lambda_X x}\right)^{K-1}, \tag{3}$$

$$F_X(x) = \left(1 - e^{-\lambda_X x}\right)^K, \tag{4}$$

in which x denotes the independent variable, and $1/\lambda_X$ is the average channel gain.

According to Lemma 1, the PDF of $\gamma_{P_{m^*}R}$ can be derived as

$$f_{\gamma_{P_{m^*}R}}(x) = M\lambda_{PR} e^{-x\lambda_{PR}}\left(1 - e^{-x\lambda_{PR}}\right)^{M-1}, \tag{5}$$

where $1/\lambda_{PR} = E[|h_{P_{m^*}R}|^2]/d^{\theta}_{P_{m^*}R} = E[\gamma_{P_{m^*}R}]$ and $E[\cdot]$ is an expectation operator.

Assuming that the channel fading factors are still unchanged within a transfer time slot, the transmit power of S_n and R are represented as follows [36]:

$$P_{S_n} = \frac{E_{S_n}}{(1-\alpha)T/2} = \frac{2\eta P_B \gamma_{P_{m^*}S_n}\alpha}{1-\alpha}, \tag{6}$$

$$P_R = \frac{E_R}{(1-\alpha)T/2} = \frac{2\eta P_B \gamma_{P_{m^*}R}\alpha}{1-\alpha}. \tag{7}$$

From (6) and (7), it is assumed that the SNRs at R and E in the first hop are denoted as γ_{SR} and γ_{SE}, while the SNRs at D and E in the latter hop are represented as γ_{RD} and γ_{RE}. And the SNRs can be given as

$$\begin{aligned}\gamma_{SR} &= \frac{P_{S_n}\left|h_{S_{n^*}R}\right|^2}{N_0 d^{\theta}_{S_{n^*}R}} \\ &= \frac{2\eta\alpha P_B \gamma_{P_{m^*}S_{n^*}}\left|h_{S_{n^*}R}\right|^2}{N_0(1-\alpha)d^{\theta}_{S_{n^*}R}} \\ &= \gamma_B \xi \gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R},\end{aligned} \tag{8}$$

where n^* is the index of the chosen source sensor (i.e., scheduled user), $\gamma_B = P_B/N_0$, $\xi = 2\eta\alpha/1-\alpha$, and $\chi_{S_{n^*}R} = |h_{S_{n^*}R}|^2/d^{\theta}_{S_{n^*}R}$. Comparably, γ_{SE}, γ_{RD}, and γ_{RE} are given as

$$\begin{aligned}\gamma_{SE} &= \gamma_E \xi \gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}, \\ \gamma_{RD} &= \gamma_B \xi \gamma_{P_{m^*}R}\chi_{RD}, \\ \gamma_{RE} &= \gamma_E \xi \gamma_{P_{m^*}R}\chi_{RE},\end{aligned} \tag{9}$$

where $\gamma_E = P_B/N_E$, N_E denotes the variance of AWGN at E, and $\chi_{S_{n^*}E} = |h_{S_{n^*}E}|^2/d^{\theta}_{S_{n^*}E}$, $\chi_{RD} = |h_{RD}|^2/d^{\theta}_{RD}$, and $\chi_{RE} = |h_{RE}|^2/d^{\theta}_{RE}$.

2.3. Multiuser Scheduling Scheme. Then, when the best PB is determined, we pay attention to the two multiuser scheduling schemes, one is a straightforward scheme with the lower complexity, in which the best source is scheduled randomly from multiple users (BSR), and another is a joint PB and source user selection scheme, in which the best source is chosen by the optimal PB (BSBP).

2.3.1. The BSR Scheme. For reduction of the complexity and costs of considered networks, the source user is scheduled randomly among the candidates in the BSR scheme. It is worth noting that $\gamma_{P_{m^*}S_n}$, χ_{S_nR}, χ_{S_nE}, χ_{RD}, and χ_{RE} are exponentially distributed with parameters $1/\lambda_{PS}$, $1/\lambda_{SR}$, $1/\lambda_{SE}$, $1/\lambda_{RD}$, and $1/\lambda_{RE}$, respectively.

Remark 1. The BSR scheme is applicable for the delay-sensitive and resource-constricted scenarios owing to its lower complexity of computation. However, the BSR scheme fails to have the diversity gain contributed by diverse users, which hinders the secrecy improvement of communication systems.

2.3.2. The BSBP Scheme. Aiming to obtain the diversity gain, the best user is chosen from the perspective of P_{m^*} in this scheme. Specifically, based on the CSI of the $P_{m^*} \longrightarrow S_n$ channels, the index of the scheduled source n^* can be drawn as

$$n^* = \arg\max_{n\in\mathcal{N}}\left(\left|h_{P_{m^*}S_n}\right|^2\right). \tag{10}$$

Therefore, $\chi_{S_{n^*}R}$, $\chi_{S_{n^*}E}$, χ_{RD}, and χ_{RE} are exponentially distributed with parameters $1/\lambda_{SR}$, $1/\lambda_{SE}$, $1/\lambda_{RD}$, and $1/\lambda_{RE}$, respectively, while the PDF of $\gamma_{P_{m^*}S_{n^*}}$ can be drawn according to Lemma 1:

$$f_{\gamma_{P_{m^*}S_{n^*}}}(x) = N\lambda_{PS} e^{-x\lambda_{PS}}\left(1 - e^{-x\lambda_{PS}}\right)^{N-1}, \tag{11}$$

where $1/\lambda_{PS} = E[|h_{P_{m^*}S_{n^*}}|^2]/d^{\theta}_{P_{m^*}S_{n^*}} = E[\gamma_{P_{m^*}S_{n^*}}]$.

Remark 2. According to the (10) and (11), we find that the BSBP scheme is able to obtain the diversity gain contributed by multiple users. Note that this scheme schedules the source user, taking into account the selection of PB adequately. As a result, this scheme can decline the interruption probability of information communication for source sensors in an effective way, which is beneficial to energy-limited IoT applications.

3. Secrecy Outage Probability Analysis

In the system, we consider that S_n and R use the different codebooks to improve secrecy performance. In line with [37], the secrecy capacity of the scenario can be indicated as

$$C_s = \min\left(C_{s1}, C_{s2}\right), \tag{12}$$

where C_{s1} and C_{s2} denote the achievable secrecy capacity of the dual-hop, respectively, which is presented to be

$$C_{s1} = \varepsilon\left[\log_2\left(\frac{1+\gamma_{SR}}{1+\gamma_{SE}}\right)\right]^+,$$
$$C_{s2} = \varepsilon\left[\log_2\left(\frac{1+\gamma_{RD}}{1+\gamma_{RE}}\right)\right]^+, \tag{13}$$

where the reason why the factor $\varepsilon = (1-\alpha)/2$ is that, the communication time of every hop is $(1-\alpha)T/2$ during a transmission slot, $[x]^+ = \max(x, 0)$. Therefore, the secrecy capacity C_s can be updated as

$$C_s = \varepsilon\left[\log_2 \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right)\right]. \tag{14}$$

Regarding evaluation of the secrecy performance, the SOP is used as the figure of merit, which is regarded as an important indicator of PLS generally. From the perspective of information theory, the transmission incurs secrecy outage if C_s is less than a predetermined secrecy rate threshold R_{th}. Specifically, the SOP of every scheme $P_{\text{sop}}^{(\text{sch})}$ can be shown as

$$P_{\text{sop}}^{(\text{sch})} = \Pr\left(C_s^{(\text{sch})} < R_{\text{th}}\right) = \Pr\left(\gamma_{\text{sec}}^{(\text{sch})} < \beta\right), \tag{15}$$

where $\text{sch} \in \{\text{BSR}, \text{BSBP}\}$, $C_s^{(\text{sch})}$ is the secrecy capacity of each scheme, and $\Pr\{\cdot\}$ is the probability.

$$\gamma_{\text{sec}}^{(\text{sch})} = \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right),$$
$$\beta = 2^{R_{\text{th}}/\varepsilon}. \tag{16}$$

3.1. Derivation for the BSR Scheme. According to the BSR scheme, each source user of the system has the same opportunity to participate in the transmission. Therefore, the exact SOP of the BSR scheme should be formulated as

$$P_{\text{sop}}^{(\text{BSR})} = \frac{1}{N}\sum_{n=1}^{N} P_{sop,S_nR} = 1 - \sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1} \times \frac{4\gamma_B(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{m\lambda_{PS}\lambda_{PR}\lambda_{SR}\lambda_{RD}}}{\xi(\gamma_B\lambda_{SE}+\beta\gamma_E\lambda_{SR})(\gamma_B\lambda_{RE}+\beta\gamma_E\lambda_{RD})}$$
$$\times K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right) \times K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right), \tag{17}$$

where P_{sop,S_nR} is the SOP when the source user S_n is decided and $K_1(\cdot)$ represents the modified Bessel function of the second kind [38].

Proof. See Appendix A. □

3.2. Derivation for the BSBP Scheme. Furthermore, according to (16), the closed-form expression of SOP for BSBP scheme is calculated as

$$P_{\text{sop}}^{(\text{BSBP})} = 1 - \sum_{n=1}^{N}\sum_{m=1}^{M}\binom{N}{n}\binom{M}{m}(-1)^{m+n} \times \frac{4\gamma_B(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{mn\lambda_{PS}\lambda_{PR}\lambda_{SR}\lambda_{RD}}}{\xi(\gamma_B\lambda_{SE}+\beta\gamma_E\lambda_{SR})(\gamma_B\lambda_{RE}+\beta\gamma_E\lambda_{RD})}$$
$$\times K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right) \times K_1\left(2\sqrt{\frac{n\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right). \tag{18}$$

Proof. See Appendix B. □

4. Secure Energy Efficiency Maximization

Generally, security improvement comes at the expense of more energy consumption frequently. With regard to energy-limited IoT applications, recklessly pursuing secrecy improvement has a negative effect on the performance of networks. Consequently, it is of great significance to make sure the safe communication in the application of IoT with low energy cost. From the above, the SEE is utilized as the proper metric for evaluation of the secrecy performance [39]. Mathematically, the SEE of above discussed schemes can be given as

$$\eta_s^{(\text{sch})} = \frac{R_{\text{th}}\left(1 - P_{\text{sop}}^{(\text{sch})}\right)}{P_{\text{total}}}, \tag{19}$$

where $\eta_s^{(\text{sch})}$ denotes the SEE of each scheme, $P_{\text{total}} = \kappa P_B + P_c$ represents the total power cost at PBs, κ denotes the power factor, and P_c and P_B stand for the fixed power and transmit power at PBs, respectively. Consider that the

harvested energy by the sensors is fully used for data transmission, while the power consumption of the circuity is ignored.

To find the best transmit power of PBs and the time-switching factor, the SEE maximization problem can be considered as

$$\begin{aligned} \max_{P_B,\alpha} \ & \eta_s^{(\mathrm{sch})} = \frac{R_{\mathrm{th}}\left(1 - P_{\mathrm{sop}}^{(\mathrm{sch})}\right)}{P_{\mathrm{total}}} \\ \text{s.t.} \ & 0 < P_B \le P_{\max} \\ & 0 < \alpha < 1, \end{aligned} \tag{20}$$

where $P_{\max}$ denotes the maximum transmit power of PBs. Obviously, the solving process of the exact expressions for P_B and α is rather tedious. Instead, by using the searching method, the optimal P_B and α can be derived on the basis of simulation and numerical analysis. It ought to be highlighted that equation (20) is of more practical importance to the IoT scenarios.

5. Numerical Results and Discussion

In this section, some numerical outcomes are provided for validation of the abovementioned secrecy analysis and for discussion of the joint effect of corresponding parameters upon the secrecy performance of the two proposed multiuser scheduling schemes. Consistent with [40], the simulation is conducted on a linear topology, in which the multiuser sensors in a localized group as well as multiple PBs, relay R, and controller D are arranged horizontally. Unless otherwise stated, we use the following parameters in accordance with [10] throughout this section. In particular, we set $\gamma_E = 20$ dB, the predetermined secrecy rate $R_{\mathrm{th}} = 0.2$ bits/s/Hz, the energy conversion efficiency $\eta = 0.6$, the distances are set to $d_{RD} = d_{SE} = d_{RE} = 3$ m, $d_{BS} = (1/2)d_{SR}$, and $d_{BR} = d_{SR} - d_{BS}$. Moreover, we set the number of the users $N = 3$, the power coefficient $\kappa = 2.63$, the path loss exponent $\theta = 2$, and $P_c = 112.2$ mW. It is obvious that the theoretical results agree exactly with the simulation results, which validates the correctness of our derivations. It is worth noting that all the numerical results in this section come from the simulation environment of MATLAB, which are all true experimental results. Combining the parameter setting in the article with the program code, all the results can be reproduced.

Figure 3 describes the SOP of the proposed multiuser scheduling schemes versus γ_B for different M with $\alpha = 0.5$, $N = 3$. Overall, it can be seen in this figure that the proposed BSBP scheme can achieve better secrecy performance than the BSR scheme in the whole range of γ_B with different M, which indicates that the BSBP scheme is more effective to improve the secrecy performance of the considered system. Furthermore, the number of PBs contributes to the improvement of SOP. This is attributed to the fact that more PBs are able to provide larger diversity gain for improving SOP.

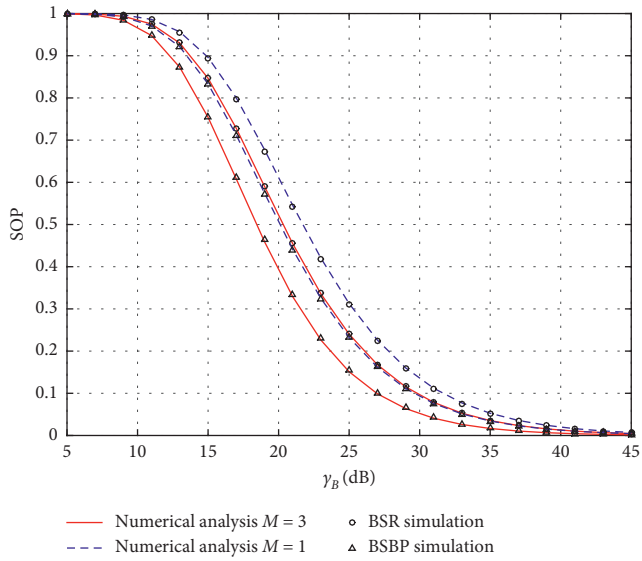

Figure 3: Effect of γ_B and M upon the secrecy outage probability with $\alpha = 0.5$ and $N = 3$.

Figure 4 shows the SEE of the system with BSR/BSBP scheme versus γ_B for different M with $\alpha = 0.5$ and $N = 3$. It is illustrated in this figure that the function of SEE and γ_B is unimodal function. The reason is that increasing γ_B brings about the improvement of SEE in low energy consumption, but it has a negative impact on the SEE in high energy consumption. Furthermore, as expected, the SEE of BSBP scheme outperforms that of the BSR scheme in the whole region, which demonstrates the advantage of BSBP in improving the secrecy performance. In addition, by increasing the number of PBs, the better security can be achieved, which can be understood through the following discussion. Furthermore, Figure 5 depicts the SEE of two multiuser scheduling strategies versus α with $N = 3$ and $\gamma_B = 20$ dB in consideration of various M. Obviously, the function of SEE and α is also unimodal function. This is due to the fact that when α is small, the harvested energy is commonly insufficient for the operation of multiple source sensors and relay sensor, while if α is large excessively, the duration of information communication will be restricted seriously, which will result in high transmission interruption probability. On the contrary, similar to Figure 4, the BSBP scheme always provides the best SEE performance with varying α and M, which validates the advantage of proposed BSBP scheme again.

Figure 6 presents the SEE of the two proposed strategies versus d_{PS} and M with $\alpha = 0.5$ and $\gamma_B = 20$ dB. It can be observed that when the group of PBs is closer to multiple source users and the number of PBs is much more relative, the two proposed strategies achieve the best efficiency. Meanwhile, the BSBP scheme is more effective when M is larger, which can be explained as the abovementioned discussion.

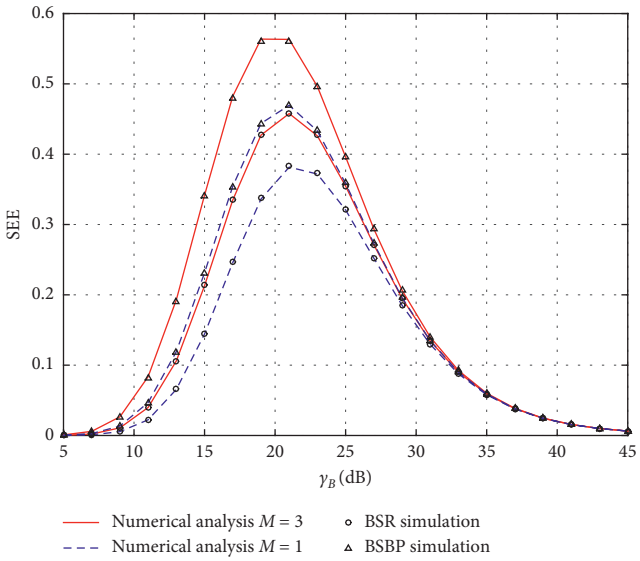

FIGURE 4: Effect of γ_B and M upon the secrecy energy efficiency with $\alpha = 0.5$ and $N = 3$.

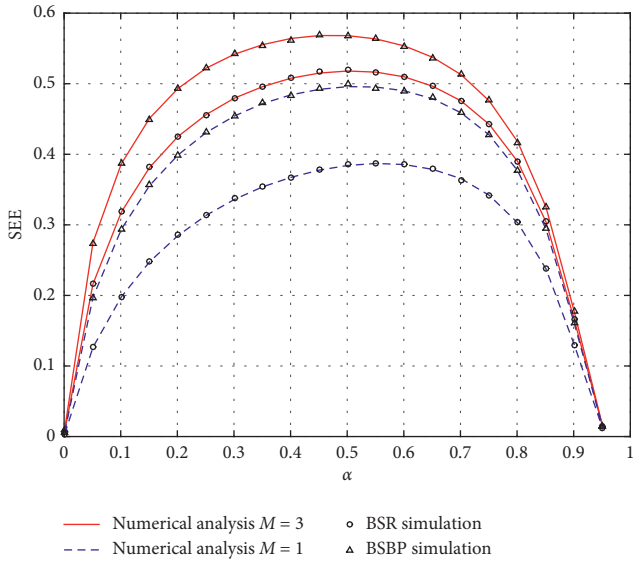

FIGURE 5: Effect of α and M upon the secrecy energy efficiency with $N = 3$ and $\gamma_B = 20$ dB.

Figure 7 plots the impact of d_{SD} and d_{PS} on the optimization of SEE by the searching method with BSR/BSBP scheme for $\gamma_B = 20$ dB. As shown clearly in the figure, the proposed multiuser scheduling schemes are more effective when d_{SD} and d_{PS} are smaller. As a matter of fact, the condition makes it possible for the sensors to acquire plenty of energy more readily, of which effect is equivalent to increasing P_B or expand α.

6. Conclusion

In this paper, the secrecy performance analysis of wireless-powered IoT possessing diverse PBs has been investigated. Specifically, the two green-oriented multiuser scheduling schemes to promote the secrecy performance of the networks are proposed. For each scheme, the analytical closed-form expression of SOP is obtained, while the optimization problem of SEE is solved by resorting to the searching method. To shed light on future applications of wireless-powered IoT, simulation results are presented to demonstrate the accuracy of our analysis, and the secrecy performance of the two proposed schemes is discussed, subject to various important parameters of the system.

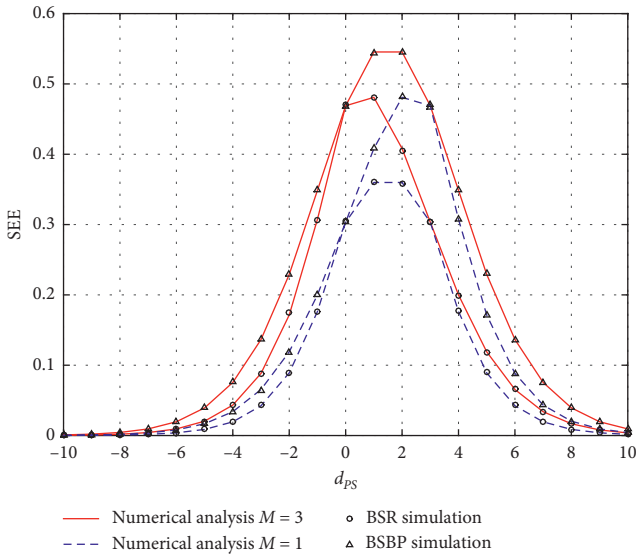

FIGURE 6: Effect of d_{PS} and M upon the secrecy energy efficiency with $\alpha = 0.5$ and $\gamma_B = 20$ dB.

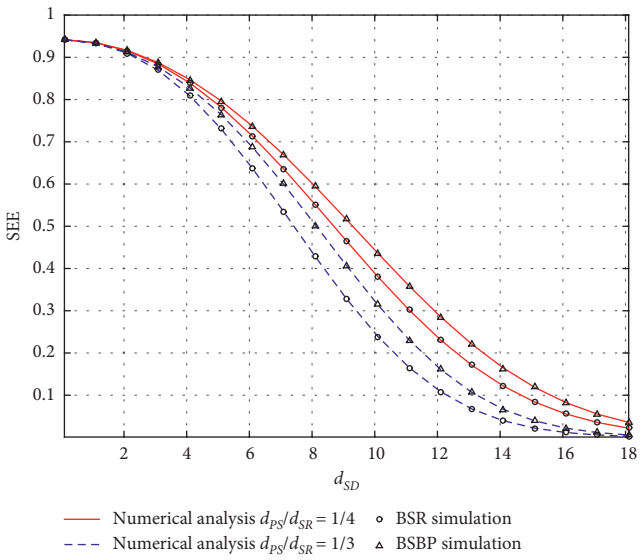

FIGURE 7: Effect of d_{SD} and d_{PS} upon the secrecy energy efficiency with $\gamma_B = 20$ dB.

Appendix

A. Proof of Formula (17)

According to (16), $\gamma_{\text{sec}}^{(\text{BSR})}$ is given by

$$\gamma_{\text{sec}}^{(\text{BSR})} = \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right) = \min\left(\gamma_{\text{sec}\,1}^{(\text{BSR})}, \gamma_{\text{sec}\,2}^{(\text{BSR})}\right). \tag{A.1}$$

Then, in line with (15) and (16), we have

$$P_{\text{sop}}^{(\text{BSR})} = P_{\text{sop},S_nR} = \Pr\left(\gamma_{\text{sec}}^{(\text{BSR})} < \beta\right) = F_{\gamma_{\text{sec}}^{(\text{BSR})}}(\beta), \tag{A.2}$$

where $F_{\gamma_{\text{sec}}^{(\text{BSR})}}(\beta)$ is the CDF of $\gamma_{\text{sec}}^{(\text{BSR})}$, which can be given with the help of (A.1) by

$$\begin{aligned} F_{\gamma_{\text{sec}}^{(\text{BSR})}}(\beta) &= \Pr\left\{\gamma_{\text{sec}}^{(\text{BSR})} < \beta\right\} \\ &= \Pr\left\{\min\left(\gamma_{\text{sec}\,1}^{(\text{BSR})}, \gamma_{\text{sec}\,2}^{(\text{BSR})}\right) < \beta\right\} \\ &= 1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSR})} > \beta\right\}\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSR})} > \beta\right\} \\ &= 1 - \left[1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSR})} < \beta\right\}\right] \times \left[1 - \Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSR})} < \beta\right\}\right]. \end{aligned} \tag{A.3}$$

Furthermore, $\Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSR})} < \beta\right\}$ and $\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSR})} < \beta\right\}$ can be derived aided by the Eq. (3.351.3) in [38], and the expression is listed as follows:

$$\begin{aligned} \Pr\left\{\gamma_{\text{sec}1}^{(\text{BSR})} < \beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}} < \beta\right\} \\ &= \int_0^\infty\int_0^\infty F_{\chi_{S_{n^*}R}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right] \times f_{\gamma_{P_{m^*}S_{n^*}}}(x) f_{\chi_{S_{n^*}E}}(y)\,\mathrm{d}x\,\mathrm{d}y \\ &= 1 - \frac{\gamma_B\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_B + \beta\gamma_E\lambda_{SR}} \times 2\sqrt{\frac{\lambda_{SR}(\beta-1)}{\gamma_B\xi\lambda_{PS}}}K_1 \cdot \left(2\sqrt{\frac{\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right), \end{aligned} \tag{A.4}$$

$$\begin{aligned} \Pr\left\{\gamma_{\text{sec2}}^{(\text{BSR})} < \beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}} < \beta\right\} \\ &= \int_0^\infty\int_0^\infty F_{\chi_{RD}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right] \times f_{\gamma_{P_{m^*}R}}(x) f_{\chi_{RE}}(y)\,\mathrm{d}x\,\mathrm{d}y \\ &= 1 - \sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1}\frac{m\gamma_B\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_B + \beta\gamma_E\lambda_{RD}} \times 2\sqrt{\frac{\lambda_{RD}(\beta-1)}{m\gamma_B\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right). \end{aligned} \tag{A.5}$$

Finally, by substituting (A.4) and (A.5) into (A.3) and performing some mathematical manipulations, (17) can be derived.

B. Proof of Formula (18)

Similar with $\gamma_{\text{sec}}^{(\text{BSR})}$ in (A.1), $\gamma_{\text{sec}}^{(\text{BSBP})}$ can be shown as

$$\gamma_{\text{sec}}^{(\text{BSBP})} = \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right) = \min\left(\gamma_{\text{sec}1}^{(\text{BSBP})}, \gamma_{\text{sec}2}^{(\text{BSBP})}\right). \tag{B.1}$$

Meanwhile, according to (15) and (16), we find

$$P_{\text{sop}}^{(\text{BSBP})} = \Pr\left(\gamma_{\text{sec}}^{(\text{BSBP})} < \beta\right) = F_{\gamma_{\text{sec}}^{(\text{BSBP})}}(\beta), \tag{B.2}$$

where $F_{\gamma_{\text{sec}}^{(\text{BSBP})}}(\beta)$ is the CDF of $\gamma_{\text{sec}}^{(\text{BSBP})}$, and it can be expressed with the help of (A.1) as

$$\begin{aligned} F_{\gamma_{\text{sec}}^{(\text{BSBP})}}(\beta) &= \Pr\left\{\gamma_{\text{sec}}^{(\text{BSBP})} < \beta\right\} \\ &= \Pr\left\{\min\left(\gamma_{\text{sec}\,1}^{(\text{BSBP})}, \gamma_{\text{sec}2}^{(\text{BSBP})}\right) < \beta\right\} \\ &= 1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} > \beta\right\}\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})} > \beta\right\} \\ &= 1 - \left[1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} < \beta\right\}\right] \times \left[1 - \Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})} < \beta\right\}\right]. \end{aligned} \tag{B.3}$$

After that, $\Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} < \beta\right\}$ and $\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})} < \beta\right\}$ can be obtained using the Eq. (3.351.3) in [38] and the expression listed below:

$$\begin{aligned} \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} < \beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}} < \beta\right\} \\ &= \int_0^\infty\int_0^\infty F_{\chi_{S_{n^*}R}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right] \times f_{\gamma_{P_{m^*}S_{n^*}}}(x) f_{\chi_{S_{n^*}E}}(y)\,\mathrm{d}x\,\mathrm{d}y \\ &= 1 - \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n\gamma_B\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_B + \beta\gamma_E\lambda_{SR}} \times 2\sqrt{\frac{\lambda_{SR}(\beta-1)}{n\gamma_B\xi\lambda_{PS}}}K_1\left(2\sqrt{\frac{n\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right), \end{aligned} \tag{B.4}$$

$$\begin{aligned}\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})}<\beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*R}}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*R}}\chi_{RE}}<\beta\right\}\\ &= \int_0^\infty\int_0^\infty F_{\chi_{RD}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right]\\ &\quad\times f_{\gamma_{P_{m^*R}}}(x)f_{\chi_{RE}}(y)\mathrm{d}x\,\mathrm{d}y\\ &= 1-\sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1}\frac{m\gamma_B\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_B+\beta\gamma_E\lambda_{RD}}\\ &\quad\times 2\sqrt{\frac{\lambda_{RD}(\beta-1)}{m\gamma_B\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right).\end{aligned} \tag{B.5}$$

Finally, by substituting (B.4) and (B.5) into (B.3) and performing some mathematical manipulations, (18) can be derived.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant numbers 61501508 and 61671476.

Supplementary Materials

The supplementary materials mainly include three folders. First of all, the folder named "Additional materials," which contains some pictures, is provided to illustrate the authenticity and reproducibility of our experimental results. It is worth noting that the above results are derived from the experimental environment of MATLAB and can be obtained by appropriately adjusting the simulation program that is given later. Then, the folder "Code" gives some simulation programs, on the basis of which we can reproduce our research results. Specific procedures and related instructions can be found in the simulation program. Furthermore, the *M* file in the folder "code", named WPCCN6_SEE_gammaB, is the main program. Based on the main program, by changing the different performance indicators, i.e., SOP or SEE required, Figures 3 and 4 in our manuscript can be derived. Meanwhile, other *M* files in the folder "code" are the callable programs. On the contrary, the files named "WPCCN_fig0.fig" and "WPCCN_fig1.fig" in the folder "code" are the numerical results of the simulation experiment, which had been given in our paper, i.e., Figures 3 and 4. Finally, the folder named "ReadMe" is a document explaining the simulation program, which can also be seen as a simple explanation of the supplementary material. It is worth noting that all the numerical results in our paper come from the simulation environment of MATLAB, which all are true experimental results. The specific experimental parameters are given in Section 5. Combining the parameter setting in the article with the program code, all the results can be reproduced. All program codes in the folder "code" are our original, which are refused to forward to others. If anyone has any questions, please contact us via email. The mailbox address is shangxiaohui1214@126.com. (*Supplementary Materials*)

References

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[2] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1565–1568, 2017.

[3] A. S. M. Z. Kausar, A. W. Reza, M. U. Saleh, and H. Ramiah, "Energizing wireless sensor networks by energy harvesting systems: scopes, challenges and approaches," *Renewable & Sustainable Energy Reviews*, vol. 38, pp. 973–989, 2014.

[4] Z. Hadzi-Velkov, I. Nikoloska, G. K. Karagiannidis, and T. Q. Duong, "Wireless networks with energy harvesting and power transfer: joint power and time allocation," *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 50–54, 2015.

[5] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative strategies for wireless-powered communications: an overview," *IEEE Wireless Communications*, vol. 25, no. 4, pp. 1–8, 2018.

[6] Y.-J. Kim, H. S. Bhamra, J. Joseph, and P. P. Irazoqui, "An ultra-low-power RF energy-harvesting transceiver for multiple-node sensor application," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 11, pp. 1028–1032, 2015.

[7] J. Bito, R. Bahr, J. G. Hester, S. A. Nauroze, A. Georgiadis, and M. M. Tentzeris, "A novel solar and electromagnetic energy harvesting system with a 3-D printed package for energy efficient internet-of-things wireless sensors," *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 5, pp. 1831–1842, 2017.

[8] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: a contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.

[9] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 1, pp. 418–428, 2014.

[10] N.-P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5G wireless communications: a joint relay selection and wireless power transfer approach," *IEEE Access*, vol. 4, pp. 3349–3359, 2016.

[11] V. N. Vo, T. G. Nguyen, C. So-In, and D.-B. Ha, "Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access*, vol. 5, pp. 25196–25206, 2017.

[12] V. N. Vo, T. G. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy," *IEEE Access*, vol. 6, pp. 23406–23419, 2018.

[13] Y. Wang, W. Yang, X. Shang, J. Hu, Y. Huang, and Y. Cai, "Energy-efficient secure transmission for wireless powered

internet of things with multiple power beacons," *IEEE Access*, vol. 6, pp. 75086–75098, 2018.

[14] Q. Wu, M. Tao, D. W. Ng, W. Chen, and R. Schober, "Energy-efficient transmission for wireless powered multiuser communication networks," in *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, pp. 154–159, London, UK, June 2015.

[15] Z. Hadzi-Velkov, I. Nikoloska, H. Chingoska, and N. Zlatanov, "Proportional fair scheduling in wireless networks with RF energy harvesting and processing cost," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2107–2110, 2016.

[16] I. Bang, S. M. Kim, and D. K. Sung, "Adaptive multiuser scheduling for simultaneous wireless information and power transfer in a multicell environment," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7460–7474, 2017.

[17] J. Choi, C. Song, and J. Joung, "Wireless powered information transfer based on zero-forcing for multiuser MIMO systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8561–8570, 2018.

[18] H. Lee, H. Kin, K.-J. Lee, and I. Lee, "Asynchronous designs for multiuser MIMO wireless powered communication networks," *IEEE Systems Journal*, vol. 13, no. 3, pp. 1–11, 2018.

[19] D. Zhai, H. Chen, Z. Lin, Y. Li, and B. Vucetic, "Accumulate then transmit: multiuser scheduling in full-duplex wireless-powered IoT systems," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2753–2767, 2018.

[20] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[21] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1133–1143, 2014.

[22] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[23] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780–787, 2016.

[24] M. Bloch and J. Barros, *Physical-layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, UK, 2011.

[25] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 90–103, 2015.

[26] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, 2015.

[27] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-*m* fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8009–8024, 2016.

[28] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5189–5202, 2016.

[29] G. Wang, Q. Liu, R. He, F. Gao, and C. Tellambura, "Acquisition of channel state information in heterogeneous cloud radio access networks: challenges and research directions," *IEEE Wireless Communications*, vol. 22, no. 3, pp. 100–107, 2015.

[30] T. Paing, J. Shin, R. Zane, and Z. Popovic, "Resistor emulation approach to low-power RF energy harvesting," *IEEE Transactions on Power Electronics*, vol. 23, no. 3, pp. 1494–1501, 2008.

[31] Z. Chen, L. Hadley, Z. Ding, and X. Dai, "Improving secrecy performance of a wirelessly powered network," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4996–5008, 2017.

[32] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, 2013.

[33] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4767, 2013.

[34] N. Shinohara, *Wireless Power Transfer via Radiowaves*, Wiley, Hoboken, NJ, USA, 2014.

[35] X. Kang, Y.-C. Liang, and J. Yang, "Riding on the primary: a new spectrum sharing paradigm for wireless-powered IoT devices," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6335–6347, 2018.

[36] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, 2017.

[37] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[38] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, Cambridge, MA, USA, 7th edition, 2007.

[39] J. Farhat, G. Brante, R. D. Souza, and J. L. Rebelatto, "Energy efficiency of repetition coding and parallel coding relaying under partial secrecy regime," *IEEE Access*, vol. 4, pp. 7275–7288, 2016.

[40] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 401–415, 2016.