IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 25, 2018, accepted November 13, 2018, date of publication November 28, 2018,
date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2883143

Energy-Efficient Secure Transmission for Wireless Powered Internet of Things With Multiple Power Beacons

YIDA WANG[1], WEIWEI YANG[1], (Member, IEEE), XIAOHUI SHANG[1], JIANWEI HU[1], (Student Member, IEEE), YUZHEN HUANG[1,2], (Member, IEEE), AND YUEMING CAI[1], (Senior Member, IEEE)

[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Weiwei Yang (wwyang1981@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61771487, Grant 61471393, and Grant 61501507, and in part by the Jiangsu Provincial Natural Science Foundation of China under Grant BK20150719.

ABSTRACT In this paper, we investigate the energy-efficient secure uplink transmission for the wireless powered Internet of Things (IoT), where one energy-constrained source and multiple energy-constrained relays harvest energy from multiple power beacons (PBs) in the presence of a passive eavesdropper. To perform energy-efficient secure communications, we consider three relay selection schemes with the best PB selected by the source, i.e., the best relay is selected randomly, the best relay is selected by the source, and the best relay is selected by the best PB (BRBP), respectively. For each scheme, the exact closed-form expressions of power outage probability (POP), secrecy outage probability (SOP), and secure energy efficiency (SEE) are derived over the Rayleigh fading channel. Furthermore, we formulate the SEE maximization problem under the transmit power constraint to optimize the transmit power in PBs and the time-switching factor. Considering the resource limitation for IoT devices, we adopt a low-complexity Dinkelbach algorithm combined with Brent's method to solve this multi-parameter fractional optimization problem. Simulation results demonstrate that the BRBP scheme achieves the best SOP performance and either increasing the number of PBs or decreasing the threshold of POP can significantly improve the SEE of the considered system.

INDEX TERMS Wireless powered communication networks, Internet of Things (IoT), physical layer security, relay selection, secrecy outage probability, secure energy efficiency.

I. INTRODUCTION

Internet of Things (IoT) presents extensive potential in future applications, including remote healthcare system, industrial control, traffic control and etc. [1], [2]. Nevertheless, IoT devices are resource-constrained and characterized by low capabilities in terms of both energy and computation capacity [3]. Energy efficiency is perhaps the most important aspect of IoT, in particular because most IoT devices expect to be operational for a very long period [4]. With responding to this, wireless powered communication networks (WPCNs) provide a promising approach to sustain IoT in a long run, where the battery of wireless communication devices can be remotely replenished by wireless power transmitters [5], [6].

However, a bottleneck for the wide proliferation of WPCNs is the very limited amount of harvested energy, which significantly degrades the performance of WPCNs [7]. Intuitively, multi antennas techniques can be implemented to alleviate this influence [8]. Unfortunately, this solution may be infeasible in many IoT applications due to the size and cost limitations. Contrarily, cooperative relaying [9]–[12] and deploying external power beacons (PBs) [13], [14] are two effective approaches to solve this problem. On the one hand, there are two celebrated relaying protocols based on the different receiver architectures, i.e., time-switching relaying (TSR) protocol and power-splitting relaying (PSR) protocol [9]. Then, [10] optimizes the transmission rate of TSR and PSR protocols in a single-relay cooperative network. Afterwards, the authors in [11] investigate the two-way relay network with energy harvesting (EH) nodes to maximize the throughput. Furthermore, a multi-pair two-way

relay network consisting of two groups of EH nodes and a massive multiple-input multiple-output (MIMO) relay is studied in [12]. On the other hand, the WPCN consisting of one dedicated multi-antenna PB and multiple single antenna source-destination pairs is analyzed in [13] to maximize the weighted sum-throughput. Furthermore, [14] investigates the dual-hop relaying system, where both the source and relay are powered by a dedicated PB.

A. RELATED WORK

In order to avoid the complex synchronization issue for resource-limited IoT devices, the relay selection mechanism is a proper cooperative relaying technique to achieve the same diversity gain as the non-orthogonal relaying and orthogonal relaying approaches [15], [16]. Therefore, the EH-relay selection has gained considerate attention due to the great potential performance improvement [17]–[22]. In [17], the authors propose two distributed relays selection schemes in a multiple EH-relays network, i.e., maximum harvested energy (MHE) and maximum signal-to-noise ratio (MSNR). Afterwards, [18] investigates two relay selection schemes in the cooperative network with spatially random EH-relays, i.e., the random relay selection (RRS) and the relay selection based on the closest distance (RCS). Furthermore, Krikidis [19] utilizes the battery information of EH-relays in relay selection schemes. He proposes the random relay selection with battery information (RRSB) and relay selection based on the closest distance with battery information (RCSB) schemes. Meanwhile, the authors in [20] propose a new relay selection scheme based on TSR protocol that mitigates the risk of ill relay selection due to the mismatch between the source-relay and relay-destination channel conditions. Then, in a stochastic networks with multiple source-destination communication pairs and multiple in-between relays, [21] finds the area spectrum efficiency can be significantly enhanced compared with the non-cooperative system. And [22] focuses on the relay interference channels, where multiple source-destination pairs communicate through their dedicated EH-relays, and develop a distributed power splitting framework using game theory.

Although the relay-selection-aided WPCN has significant advantages, the broadcast nature of wireless communications makes the data transmission more vulnerable to security attacks [23]. The upper layer cryptographic techniques are typically deployed to secure the confidential messages against wiretapping in conventional wireless communications [24]. Nevertheless, traditional cryptographic techniques are restricted for many IoT devices in WPCNs due to requirements of high hardware complexity and large amount of energy [25]. Moreover, an eavesdropper (EAV) with unlimited computing power may still decipher these techniques using brute-force attack [26]. Fortunately, physical layer security (PLS), which exploits the characteristics of wireless channels to improve the security of wireless transmission, has been proposed as a good supplement of current cryptographic mechanism [27]–[30]. Recently, several works have investigated secure communications in relay-selection-aided WPCNs [31]–[33]. Inspired by the idea of wireless powered friendly jammer in [34] and [35], the authors in [31] select a pair out of intermediate energy-constrained nodes as a relay and a jammer in a TSR-based WPCN. Then the system performance is evaluated in terms of secrecy outage probability (SOP) in the presence of multiple passive Eves. As the extend of [31] and [32] studies a TSR-based wireless sensor network, where a sensor source and multiple sensor relays harvest energy from multiple dedicated PBs. Then the authors propose a best-relay-and-best-jammer scheme to select a pair of sensor relays as a relay and a jammer to improve the SOP of the considered system. In addition, [33] investigates a TSR-based WPCN, where a source and multiple relays harvest energy from a multi-antenna PB. Then, the authors analyzed the SOP of two relay selection schemes based on the partial and full knowledge of channel state information with two antenna selection schemes for harvesting energy at source and relays.

B. CONTRIBUTIONS

However, above works only focus on the security improvement via relay selection schemes in WPCNs, while neglect the energy efficiency problem. On one hand, greedily pursuing secrecy performance may bring about larger energy consumption, which is very disadvantageous for energy-constrained IoT devices. On the other hand, when the harvested energy in the energy-constrained source or the energy-constrained relay is insufficient, the system can not support the data transmission, i.e., the power outage occurs [36]. Therefore, it is necessary to ensure the data transmission for wireless powered IoT works in a secure and energy-efficient way.

In this paper, we investigate the uplink transmission for wireless powered IoT, where one source and multiple relays are powered by multiple dedicated PBs. Then, we consider three PB and relay selection schemes in order to provide the energy-efficient secure communications. The contributions of this paper can be summarized as follows:

- We consider three PB and relay selection schemes, where the best PB is selected by the source while the best relay is selected randomly (BRR), selected by the source (BRS), and selected by the best PB (BRBP), respectively. Compared with the BRR scheme and the BRS scheme, the BRBP scheme is able to fully utilize the power transfer channels contributed by multiple PBs.
- We derive the closed-form expressions of the probability of power outage (POP), SOP, and SEE for three PB and relays selection schemes. Simulation results demonstrate that BRBP scheme presents the best performance due to its lower outage probability of data transmission. In addition, increasing the number of PBs and decreasing the threshold of the POP can significantly improve the SEE of the considered system.
- We formulate the SEE maximization problem with the transmit power constraint at PBs. Resorting to

the Dinkelbach algorithm with Brent's method, the transmit power in PBs and the time-switching factor can be optimized to maximize SEE. Compared with the time-consuming exhaustive search approaches in [32] and [37], this low complex optimizing algorithm is more efficient for the resource-constrained wireless powered IoT.

The remainder of the paper is organized as follows: Section II presents the system model. Section III gives the performance analysis of POP, SOP, and SEE, respectively. Section IV provides the formulation of SEE maximization problem and illustrates the optimization algorithm. Section V presents simulation results. Finally, conclusions are given in Section VI.

II. SYSTEM MODEL

We investigate the uplink transmission in a WPCN for the IoT application, where a source sensor S intends to transmit a packet to a base station B with the help of multiple intermediate relay sensors R_n, $n \in \mathcal{N} = \{1, \cdots, N\}$, in the presence of a passive EAV E, as illustrated in Fig. 1. In consideration of the limited coverage of sensors, the direct $S \to B$ transmission is assumed unavailable [31], [33].

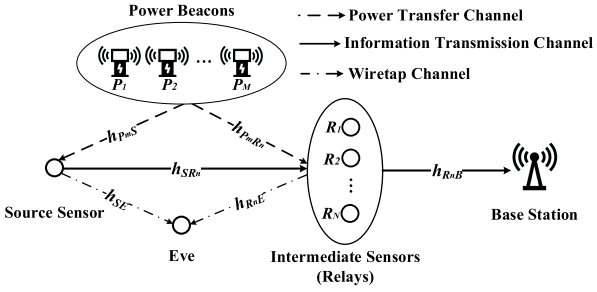


FIGURE 1. System model.

Meanwhile, due to the limitation of energy, S and R_n must acquire energy by wireless powered transfer (WPT) from multiple PBs P_m, $m \in \mathcal{M} = \{1, \cdots, M\}$, to support wireless information transmission (WIT). In addition, taking into account the size and cost limitations, we assume all S, R_n, P_m, B and E are each equipped with a single antenna [32].

Here, we assume that all the channels are subject to Rayleigh fading, i.e., the channel power gains are exponential distributed with parameter λ_{XY}, where $X \in \{P_m, S, R_n\}$ and $Y \in \{S, R_n, E, B\}$. The additive white Gaussian noise (AWGN) at R_n and B has zero mean and variance N_0. The AWGN at E has zero mean and variance N_E. It is worth mentioning that the statistical CSI of the wiretap channel can be obtained when Eve is also the member of the communication system and tries to intercept the signals not intended to her [5], [6].

For mathematical modeling purposes, the channel coefficients of the $P_m \to S$, $P_m \to R_n$, $S \to R_n$, $S \to E$, $R_n \to E$, and $R_n \to B$ communication links are denoted by h_{P_mS}, $h_{P_mR_n}$, h_{SR_n}, h_{SE}, h_{R_nB}, and h_{R_nE}, respectively. Meanwhile, we assume that both of the PBs and intermediate sensors are clustered relatively close together, i.e., location-based clustering. Thus, the distance of $P_m \to S$, $P_m \to R_n$, $S \to R_n$, $S \to E$, $R_n \to E$, and $R_n \to B$ can be denoted as d_{PS}, d_{PR}, d_{SR}, d_{SE}, d_{RB}, and d_{RE}, respectively. Moreover, it results in the equivalent average channel power gains of the links $P_m \to S$, $P_m \to R_n$, $S \to R_n$, $R_n \to E$, and $R_n \to B$, i.e., $\lambda_{P_mS} = \lambda_{PS}$, $\lambda_{P_mR_n} = \lambda_{PR}$, $\lambda_{SR_n} = \lambda_{SR}$, $\lambda_{R_nE} = \lambda_{RE}$, and $\lambda_{R_nB} = \lambda_{RB}$ for any $m \in \mathcal{M}$ and $n \in \mathcal{N}$. It is important to note that this assumption is commonly used in the context of the WPCNs (e.g., [32], [38] and references therein).

A. COMMUNICATION TECHNIQUE

In the process of WPT, the rectenna-based EH module is applied in the receiver. In the rectenna, the received RF band signal can be converted to a direct current (DC) signal by a rectifier, which consists of a Schottky diode and a passive low-pass filter (LPF) [39]. Afterwards, we assume that the energy harvested by sensors during the WPT is fully consumed to send signal in the process of WIT, which is termed as the harvest-use (HU) mode [6]. Therefore, at the beginning of every transmission block, there is no residual harvested energy in S and R_n. This assumption is reasonable for sensors because they are equipped only with small batteries for energy storage due to the size and cost limitations. Moreover, we adopt PB selection as in [32], [40], and [41], in which only one PB is selected as active while other PBs keep silent. It is because PB selection is an energy-efficient WPT solution and can effectively reduce the computational complexity.

As for the relaying protocol, we adopt the TSR protocol that employs time-domain multiplexing to accomplish WPT and WIT within the same transmission block. Compared with PSR protocol that splits the harvest power into two parts, TSR protocol can be immediately implemented with off-the-shelf hardware by adjusting the time-switching factor denoted as α [20]. Specifically, in a transmission block time denoted as T (i.e., one HU period), αT is the time for WPT and $(1-\alpha)T$ is the time for WIT, where $\alpha \in (0, 1)$. The time window for WIT is separated into two phrases due to the two-hop transmission, i.e., $(1-\alpha)T/2$ is used for $S \to R_n$, and the rest time $(1-\alpha)T/2$ is used for $R_n \to B$ as illustrated in Fig. 2.

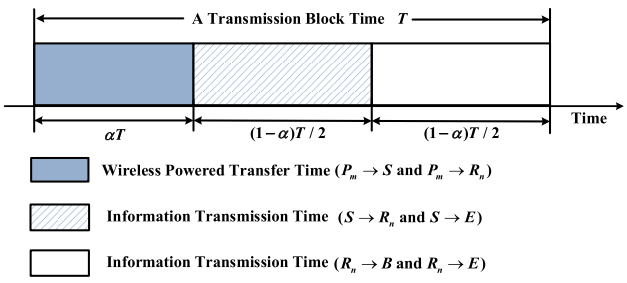


FIGURE 2. Time-switching relaying protocol. The considered transmission block time T is used for both WPT and WIT, in which the time αT is used to harvest energy from multiple PBs, while the remaining time $(1-\alpha)T$ is used to transmit the packet from the source sensor to the base station.

It is noted that we assume the harvested energy in all relays can only be used in the current transmission block and can not be accumulated. It is caused by the small batteries equipped in all relays, which are limited with the cost and size. Indeed, this HU mode is a common assumption in the research of WPCN as in [31], [32], and [42], which can avoid the complex transition analysis of the battery status. It is also interesting to consider the scenario that the relays can accumulate energy by harvest-store-use (HSU) mode or harvest-use-store (HUS) mode in [43]. But it is out the scope of this paper and will be investigated in our future work.

Therefore, the energy harvested at S and R_n can be interpreted as follows:

$$E_S = \eta P_B \alpha T \left|h_{P_m S}\right|^2, \tag{1}$$

$$E_{R_n} = \eta P_B \alpha T \left|h_{P_m R_n}\right|^2, \tag{2}$$

where $0 < \eta < 1$ is the EH efficiency coefficient, P_B is the transmit power of PBs, $\left|h_{P_m S}\right|^2$ and $\left|h_{P_m R_n}\right|^2$ are channel power gains of the links from P_m to S and from P_m to R_n, respectively.

Under the assumption that the channel fading coefficients remain constant during a transmission block time [31], the transmit power of S and R_n are given by

$$P_S = \frac{2E_S}{(1-\alpha)T} = \frac{2\eta P_B \left|h_{P_m S}\right|^2 \alpha}{(1-\alpha)}, \tag{3}$$

$$P_{R_n} = \frac{2E_{R_n}}{(1-\alpha)T} = \frac{2\eta P_B \left|h_{P_m R_n}\right|^2 \alpha}{(1-\alpha)}. \tag{4}$$

It needs to be emphasized that the received power for sensors must exceed the minimum threshold power θ_{th} to sustain the data transmission [44], [45].

From (3) and (4), the SNRs at R and E in the first hop and the SNRs at B and E in the second hop e.g., γ_{SR}, γ_{SE}, γ_{RB}, and γ_{RE} can be expressed as

$$\begin{aligned}\gamma_{SR} &= \frac{P_S \left|h_{SR_n}\right|^2}{N_0} = \frac{2\eta\alpha P_B \left|h_{P_m S}\right|^2 \left|h_{SR_n}\right|^2}{N_0(1-\alpha)} \\ &= \gamma_P \xi \left|h_{P_m S}\right|^2 \left|h_{SR_n}\right|^2,\end{aligned} \tag{5}$$

where $\gamma_P = \frac{P_B}{N_0}$ and $\xi = \frac{2\eta\alpha}{1-\alpha}$. Similarly, γ_{SE}, γ_{RD} and γ_{RE} are shown as

$$\gamma_{SE} = \gamma_E \xi \left|h_{P_m S}\right|^2 \left|h_{S_n E}\right|^2, \tag{6}$$

$$\gamma_{RB} = \gamma_P \xi \left|h_{P_m R_n}\right|^2 \left|h_{R_n B}\right|^2, \tag{7}$$

$$\gamma_{RE} = \gamma_E \xi \left|h_{P_m R_n}\right|^2 \left|h_{R_n E}\right|^2, \tag{8}$$

where $\gamma_E = \frac{P_B}{N_E}$.

B. POWER BEACON AND RELAY SELECTION

In this part, we provide three PB and relay selection schemes. In the first two schemes, the PB selection and relay selection are independent, where the best relay is selected randomly (BRR) and the best relays is selected by source (BRS), respectively. Contrarily, another scheme is a joint relay and PB selection scheme, where the best relay is selected by the best PB (BRBP).

Here, we consider that a particular PB is selected to activate for the reduction of computational complexity and energy cost [32]. In all schemes, the best PB is selected according to the links from $P_m \to S$. Thus, the index of the selected PB can be given by

$$m^* = \arg \max_{m \in \mathcal{M}} \{\left|h_{P_m S}\right|^2\}, \tag{9}$$

Lemma 1: From [32], if X_k, $k \in \mathcal{K} = \{1 \cdots K\}$, is the random variable that follows the independent and identical exponential distribution, the cumulative distribution function (CDF) and the probability density function (PDF) of $X = \max_{k \in \mathcal{K}} \{X_k\}$ can be calculated as follows:

$$F_X(x) = (1 - e^{-\lambda_X x})^K, \tag{10}$$

$$f_X(x) = K\lambda_X e^{-\lambda_X x}(1 - e^{-\lambda_X x})^{K-1}, \tag{11}$$

where x is the independent variable of PDF.

With the help of Lemma 1, we can obtain the PDFs of $\left|h_{P_{m^*} S}\right|^2$ as follows:

$$f_{\left|h_{P_{m^*} S}\right|^2}(x) = M\lambda_{PS} e^{-x\lambda_{PS}}(1 - e^{-x\lambda_{PS}})^{M-1}, \tag{12}$$

where $\lambda_{PS} = \lambda_{P_m S} = E(\left|h_{P_m S}\right|^2)$, $E(\cdot)$ is is an expectation operator. It is noted that $\left|h_{P_{m^*} R_n}\right|^2$, $\left|h_{SR_n}\right|^2$, $|h_{SE}|^2$, $\left|h_{R_n E}\right|^2$ and $\left|h_{R_n B}\right|^2$ are exponential distributed with parameters $\lambda_{PR} = \lambda_{P_m R} = E(\left|h_{P_m R}\right|^2)$, $\lambda_{SR} = \lambda_{SR_n} = E(\left|h_{SR_n}\right|^2)$, $\lambda_{SE} = E(|h_{SE}|^2)$, $\lambda_{RE} = \lambda_{R_n E} = E(\left|h_{R_n E}\right|^2)$ and $\lambda_{RB} = \lambda_{R_n B} = E(\left|h_{R_n B}\right|^2)$, respectively. It is noted that the distributed parameters are inversely proportional to the correspond path loss, i.e., $\lambda_{ij} \propto 1/d_{ij}^{\nu}$, ν is the path loss factor. Without loss of generality, in this paper, we assume $\lambda_{ij} = 1/d_{ij}^{\nu}$.

1) THE BRR SCHEME

As a benchmark, the relay is selected randomly from multiple intermediate sensors in the BRR scheme.

Although the BRR scheme is a benchmark invoked for comparison purposes, this scheme is applicable for the delay-sensitive scenarios thanks to its low computational complexity. In exchange, the BRR scheme does not possess the diversity gain contributed by multiple relays.

2) THE BRS SCHEME

In order to acquire the diversity gain, it is nature to select the best relay by the source based on the CSI of the $S \to R_n$ links, which is termed as the BRS scheme. Specifically, the index of the selected relay n^* is given by

$$n^* = \arg \max_{n \in \mathcal{N}} (\left|h_{SR_n}\right|^2). \tag{13}$$

The $\left|h_{P_{m^*} R_{n^*}}\right|^2$, $\left|h_{R_{n^*} E}\right|^2$ and $\left|h_{R_{n^*} B}\right|^2$ are exponential distributed with parameters λ_{PR}, λ_{RE} and λ_{RB}, respectively. And

the PDF of $\left|h_{SR_{n^*}}\right|^2$ can be derived from Lemma 1 as follows:

$$f_{\left|h_{SR_{n^*}}\right|^2}(x) = N\lambda_{SR}e^{-x\lambda_{SR}}(1-e^{-x\lambda_{SR}})^{N-1}. \quad (14)$$

Compared with the BRR scheme, the BRS scheme can acquire the diversity gain contributed by multiple relays. It is worth noting that the relay selection in the BRS scheme only relies on the quality of the $S \rightarrow R_n$ links, which is independent of the PB selection. However, the BRS scheme neglects the potential insufficient charging for the relay selected from multiple energy-constrained intermediate sensors.

3) THE BRBP SCHEME

To take the full advantage of the WPT with multiple PBs, the best relay is selected from the perspective of P_{m^*} in the BRBP scheme. To be more specific, the index of the selected relay n^* is based on the CSI of the $P_{m^*} \rightarrow R_n$ links, which can be expressed as

$$n^* = \arg \max_{n\in\mathcal{N}}(\left|h_{P^*_m R_n}\right|^2). \quad (15)$$

The $\left|h_{SR_{n^*}}\right|^2$, $\left|h_{R_{n^*}E}\right|^2$ and $\left|h_{R_{n^*}B}\right|^2$ are exponential distributed with parameter λ_{SR}, λ_{RE} and λ_{RB}. And the PDF of $\left|h_{P_{m^*}R_{n^*}}\right|^2$ can be derived from Lemma 1 as follows:

$$f_{\left|h_{P_{m^*}R_{n^*}}\right|^2}(x) = N\lambda_{PR}e^{-x\lambda_{PR}}(1-e^{-x\lambda_{PR}})^{N-1}. \quad (16)$$

Similarly, the BRBP scheme can acquire the diversity gain contributed by multiple relays. Moreover, the relay selection in the BRBP scheme is closely related to the PB selection. Consequently, the BRBP scheme can effectively decrease the outage probability of data transmission, which is more appropriate for energy-constrained IoT scenarios, compared with the other two schemes.

III. PERFORMANCE ANALYSIS

In this section, the probabilities of power outage, secrecy outage, and overall secrecy outage for three schemes are derived in turn. In order to capture both security and energy efficiency issues, the considered system is further evaluated by the metric of SEE.

A. POWER OUTAGE PROBABILITY

The received power at sensors must be greater than the minimum power threshold θ_{th} to sustain the data transmission. As in [44]–[46], θ_{th} indicates the minimum threshold power to activate the energy harvesting circuitry at S and R_{n^*}. If the received power is less than the power threshold, the energy harvesting circuitry stays inactive leading to the power outage.

Therefore, the POP $P^{(sch)}_{pout}$ can be given by

$$\begin{aligned} P^{(sch)}_{pout} &= \Pr\{\min(P_s, P_{R_{n^*}}) < \theta_{th}\} \\ &= \Pr\{\min(\left|h_{P_{m^*}S}\right|^2, \left|h_{P_{m^*}R_{n^*}}\right|^2) < \varphi_{th}\} \\ &= 1-\Pr\{\left|h_{P_{m^*}S}\right|^2 > \varphi_{th}\} \times \Pr\{\left|h_{P_{m^*}R_{n^*}}\right|^2 > \varphi_{th}\} \\ &= 1-\int_{\varphi_{th}}^{\infty} f_{|h_{P_{m^*}S}|^2}(x)dx \times \int_{\varphi_{th}}^{\infty} f_{|h_{P_{m^*}R_{n^*}}|^2}(y)dy, \end{aligned} \quad (17)$$

where $sch \in \{BRR, BRS, BRBP\}$, $\varphi_{th} = \frac{(1-\alpha)\theta_{th}}{2\eta\alpha P_B} = \frac{\gamma_{th}}{\xi\gamma_P}$, and $\gamma_{th} = \frac{\theta_{th}}{N_0}$.

By substituting (12) and (16) into (17) and combining the relative PDFs, the POPs of three schemes can be expressed as follows:

$$P^{(BRR)}_{pout} = P^{(BRS)}_{pout} = 1-[1-(1-e^{-\lambda_{PS}\varphi_{th}})^M]e^{-\lambda_{PR}\varphi_{th}}, \quad (18)$$

$$\begin{aligned} P^{(BRBP)}_{pout} &= 1-[1-(1-e^{-\lambda_{PS}\varphi_{th}})^M][1-(1-e^{-\lambda_{PR}\varphi_{th}})^N] \\ &= (1-e^{-\lambda_{PS}\varphi_{th}})^M + (1-e^{-\lambda_{PR}\varphi_{th}})^N \\ &\quad -(1-e^{-\lambda_{PS}\varphi_{th}})^M(1-e^{-\lambda_{PR}\varphi_{th}})^N. \end{aligned} \quad (19)$$

Remark 1: From (18) and (19), it is observed that the BRR scheme and the BRS scheme have the same POP. It is caused by the fact that the relay selection is independent of the PB selection in these two schemes. Contrarily, the BRBP scheme selects the best relay based on the selection of PB, which is able to more fully utilize the power transfer channels contributed by multiple PBs. Consequently, the BRBP scheme has lower POP because the selected relay can harvest enough energy more easily.

B. SECRECY OUTAGE PROBABILITY

In order to enhance security performance, S and R_n use the different code books in the considered system. According to [47], the achievable secrecy rate of the considered two-hop system can be expressed as follows:

$$R_s = \min(R_{s1}, R_{s2}), \quad (20)$$

where R_{s1} and R_{s2} are the achievable secrecy rate of the first hop and the second hop, which can be indicated as

$$R_{s1} = \varepsilon\left[\log_2(\frac{1+\gamma_{SR}}{1+\gamma_{SE}})\right]^+, \quad (21)$$

$$R_{s2} = \varepsilon\left[\log_2(\frac{1+\gamma_{RD}}{1+\gamma_{RE}})\right]^+. \quad (22)$$

Here the coefficient $\varepsilon = (1-\alpha)/2$ illustrates the fact that, the transmission duration of each hop is $(1-\alpha)T/2$ during a transmission block time, $[x]^+ = \max(x, 0)$. Thus, the achievable secrecy rate R_s can be rewritten as

$$R_s = \varepsilon\log_2\left[\min\left(\frac{1+\gamma_P\xi\left|h_{P_{m^*}S}\right|^2\left|h_{SR_{n^*}}\right|^2}{1+\gamma_E\xi\left|h_{P_{m^*}S}\right|^2|h_{SE}|^2}, \frac{1+\gamma_P\xi\left|h_{P_{m^*}R_{n^*}}\right|^2\left|h_{R_{n^*}B}\right|^2}{1+\gamma_E\xi\left|h_{P_{m^*}R_{n^*}}\right|^2\left|h_{R_{n^*}E}\right|^2}\right)\right] \quad (23)$$

As an important measure of the secrecy performance, the SOP is defined as the probability that the achievable secrecy rate R_s falls below a predetermined secrecy rate threshold R_{th}.

$$P_{sout}^{(sch)} = \Pr(R_s^{(sch)} < R_{th}) = \Pr(\gamma_{\text{sec}}^{(sch)} < \beta), \tag{24}$$

$$\gamma_{\text{sec}}^{(sch)} = \min\left(\frac{1+\gamma_P\xi\left|h_{P_{m^*}S}\right|^2|h_{SR_{n^*}}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}S}\right|^2|h_{SE}|^2}, \frac{1+\gamma_P\xi\left|h_{P_{m^*}R_{n^*}}\right|^2|h_{R_{n^*}B}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}R_{n^*}}\right|^2|h_{R_{n^*}E}|^2}\right), \tag{25}$$

To be more specific, the SOP of each scheme $P_{sout}^{(sch)}$ can be expressed as (24) and (25), as shown at the top of this page, and $\beta = 2^{R_{th}/\varepsilon}$.

1) SOP OF THE BRR SCHEME

As aforementioned, the BBR scheme gives the equal chance to each source-relay pair. Therefore, the SOP of this scheme can be expressed as the mean SOP of N source-relay pairs, which can be given by

$$\begin{aligned} P_{sout}^{(BRR)} &= \frac{1}{N}\sum_{n=1}^{N} P_{out,SR_n} = 1 - \sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1} \\ &\times \frac{4(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{m\lambda_{PS}\lambda_{PR}m\lambda_{SR}\lambda_{RB}}}{\xi(\gamma_P\lambda_{SE}+\beta\gamma_E\lambda_{SR})(\gamma_P\lambda_{RE}+\beta\gamma_E\lambda_{RB})} \\ &\times K_1\left(2\sqrt{\frac{\lambda_{PR}\lambda_{RB}(\beta-1)}{\gamma_B\xi}}\right) \\ &\times K_1\left(2\sqrt{\frac{mk\lambda_{PS}\lambda_{SR}(\beta-1)}{\gamma_B\xi}}\right), \end{aligned} \tag{26}$$

where P_{sout,SR_n} denotes the SOP when the relay R_n is selected, and $K_1(\cdot)$ is the modified Bessel function of the second kind as described in [48].

Proof: The proof is given in Appendix A. ■

2) SOP OF THE BRS SCHEME

With the help of (25), the SOP of the considered system of the BRS scheme can be expressed as follows:

$$\begin{aligned} P_{sout}^{(BRS)} &= 1 - \sum_{n=1}^{N}\sum_{m=1}^{M}\binom{N}{n}\binom{M}{m}(-1)^{m+n} \\ &\times \frac{4(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{mn\lambda_{PS}\lambda_{PR}\lambda_{SR}\lambda_{RB}}}{\xi(\gamma_P\lambda_{SE}+n\beta\gamma_E\lambda_{SR})(\gamma_P\lambda_{RE}+\beta\gamma_E\lambda_{RB})} \\ &\times K_1\left(2\sqrt{\frac{\lambda_{PR}\lambda_{RB}(\beta-1)}{\gamma_P\xi}}\right) \\ &\times K_1\left(2\sqrt{\frac{m\lambda_{PS}\lambda_{SR}(\beta-1)}{\gamma_P\xi}}\right). \end{aligned} \tag{27}$$

Proof: The proof is given in Appendix B. ■

3) SOP OF THE BRBP SCHEME

By using the similar procedure, the closed-form expression of SOP for BRBP scheme can be given by

$$\begin{aligned} P_{sout}^{(BRBP)} &= 1 - \sum_{n=1}^{N}\sum_{m=1}^{M}\binom{N}{n}\binom{M}{m}(-1)^{m+n} \\ &\times \frac{4(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{mn\lambda_{PS}\lambda_{PR}\lambda_{SR}\lambda_{RB}}}{\xi(\gamma_P\lambda_{SE}+\beta\gamma_E\lambda_{SR})(\gamma_P\lambda_{RE}+\beta\gamma_E\lambda_{RB})} \\ &\times K_1\left(2\sqrt{\frac{n\lambda_{PR}\lambda_{RB}(\beta-1)}{\gamma_P\xi}}\right) \\ &\times K_1\left(2\sqrt{\frac{m\lambda_{PS}\lambda_{SR}(\beta-1)}{\gamma_P\xi}}\right). \end{aligned} \tag{28}$$

Proof: The proof is given in Appendix C. ■

C. OVERALL SECRECY OUTAGE PROBABILITY

For the WPCN with an energy-constrained source and multiple energy-constrained relays, the uplink data transmission is infeasible when the harvested energy in the source and the selected relay is not sufficient. Meanwhile, in the presence of a passive Eve, it is necessary to ensure the secrecy of the data transmission when the harvested energy is sufficient. Therefore, from [46], the overall SOP in WPCN $P_{out}^{(sch)}$ is expressed as

$$P_{out}^{(sch)} = P_{pout}^{(sch)} + (1 - P_{pout}^{(sch)})P_{sout}^{(sch)}, \tag{29}$$

where $P_{pout}^{(sch)}$ can be acquired from (18) and (19).

Remark 2: From (18)-(19) and (26)-(29), we observe that the overall SOPs of three schemes are lower when there is more PBs. In particular, the BRR scheme is the special case of the BRS scheme or BRBP scheme when $N = 1$. Thus, the SOP and POP of BRR scheme are independent of the number of relays. Meanwhile, it validates the fact that the BRR scheme does not possess the diversity gain contributed by multiple relays. In contrast, the overall SOPs of BRS and BRBP schemes decline with the increase of the number of relays. Furthermore, the structure of (29) illustrates that the POP has a great impact on the overall SOP. Thus, the BRBP scheme can acquire better performance of the overall SOP thanks to its lower POP.

D. SECURE ENERGY EFFICIENCY

Generally, the security improvement is often at the cost of the larger energy consumption. For energy-constrained IoT scenarios, blindly pursuing secrecy performance is destructive for the overall performance. Therefore, it is necessary to ensure the secure transmission in IoT scenarios works with lower energy consumption. With responding to this, the SEE is adopted here as the appropriate metric to evaluate the overall performance for the considered system. The SEE is defined as the ratio between the amount of successfully secure transmitted bits and the total power used to perform

such transmission [50]. Mathematically, the SEE in the considered system can be expressed as follows:

$$\eta_s^{(sch)} = \frac{R_{th}(1 - P_{out}^{(sch)})}{P_{total}}, \tag{30}$$

where $P_{total} = \kappa P_B + P_c$ is the total power consumption at PBs, κ is the power coefficient, P_B and P_c account for transmit power and the static power at PBs. The harvested energy at sensors is assumed to be totally transformed to radiation power with circuitry power consumption ignored [49].

Remark 3: From (26)-(28), the security performance can be improved by increasing the transmit power in PBs. However, the denominator of SEE in (30) is an increasing function of the transmit power. Thus, overload transmit power has a negative effect on the SEE. On the other hand, increasing time-switching factor can effectively decrease POP, but also increase SOP. Therefore, how to maximize the SEE by optimizing the transmit power in PBs and the time-switching factor is of more practical operational significance for the considered system.

IV. SECURE ENERGY EFFICIENCY MAXIMIZATION

In this section, the formulation of the SEE maximization problem is firstly presented. Then, the specific SEE maximization algorithm is given.

A. PROBLEM FORMULATION

To determine the optimal transmit power in PBs and the time-switching factor, we formulate the SEE optimization problem as follows:

$$\begin{aligned} P1: \quad & \max_{P_B,\alpha} \ \eta_s^{(sch)} = \frac{R_{th}(1-P_{out}^{(sch)})}{P_{total}} \\ & s.t. \ 0 < P_B \le P_{\max}, \\ & \quad 0 < \alpha < 1, \end{aligned} \tag{31}$$

where $P_{\max}$ represents the maximum transmit power in PBs.

It can be observed from (26)-(28) that P_B is coupled with α and the Problem P1 is non-convex. Therefore, a rigorous analysis of optimal exact expressions for P_B and α is intractable and we pursue a suboptimal design by adopting the alternating optimization. The basic idea of alternating optimization is to solve Problem P1 by fixing either P_B or α and then alternates until convergence.

Firstly, we focus on the optimal P_B design for a fixed α as

$$P2: \quad \max_{P_B \in S} \ \frac{f_1(P_B)}{f_2(P_B)}, \tag{32}$$

where $S = \{P_B \ | \ 0 < P_B \le P_{\max}\}$, $f_1(P_B) = R_{th}[1 - P_{out}^{(sch)}(P_B)]$ and $f_2(P_B) = \kappa P_B + P_c$.

Theorem 1: Problem P2 is a concave-convex fractional problem (CCFP).

Proof: Due to the affine form, S is a convex set and $f_2(P_B)$ is a convex function with respect to (w.r.t) P_B. Then the concavity of $f_1(P_B)$ is proved by the negative semidefiniteness of Hessian metric, which can be verified numerically and is omitted here. Above conditions is exact the definition of CCFP in [51]. ■

With the help the Theorem 1, Problem P2 can be solved by the Dinkelbach algorithm, which is an iterative and distributed approach to solve the CCFP. Therefore, the remaining task is to solve to optimal α by fixing P_B. By fixing P_B, Problem P1 reduces to

$$\begin{aligned} P3: \quad & \max_{\alpha} \ \eta_s^{(sch)} = \frac{R_{th}(1-P_{out}^{(sch)})}{P_{total}} \\ & 0 < \alpha < 1, \end{aligned} \tag{33}$$

Define $F(\alpha) = \eta_s^{(sch)}(\alpha)$. The first-order derivative $\frac{\partial F(\alpha)}{\partial \alpha}$ is positive when $\alpha \to 0$ and negative when $\alpha \to 1$. Therefore, there exists a unique solution satisfying $\frac{\partial F(\alpha)}{\partial \alpha} = 0$. Considering the complex structure of $\eta_s^{(sch)}$ w.r.t α, it is proper to adopt the low complex Brent's method to solve P3, which is an improved one-dimension search method by narrowing the linear feasible region without derivative.

B. OPTIMIZATION ALGORITHM

In this part, we illustrate the specific algorithms for optimizing transmit power in PBs and the optimizing time-switching factor, respectively. At last, we give the overall alternating optimization algorithm.

1) OPTIMIZATION TRANSMIT POWER

According to above analysis, we adopt the Dinkelbach algorithm to solve Problem P2. The basic idea of Dinkelbach algorithm is solving a sequence of easier problems, which converges to the global solution of the CCFP with the help of an auxiliary parameter λ. To be more specific, Dinkelbach algorithm is built on the relation between the (32) and the function with the subtractive form as follows:

$$F(\lambda) = \max_{P_B \in S} \{f_1(P_B) - \lambda f_2(P_B)\}, \tag{34}$$

where $f_1(P_B)$ is maximized while $f_2(P_B)$ is minimized, with the parameter λ determining the weight associated with the denominator. Consider $P_B^* \in S$ and $\lambda^* = \frac{f_1(P_B^*)}{f_2(P_B^*)}$. Then P_B^* is a solution of (32) if and only if

$$P_B^* = \arg \max_{P_B \in S} \{f_1(P_B) - \lambda^* f_2(P_B)\}. \tag{35}$$

This implies

$$\begin{aligned} f_1(P_B) - \lambda^* f_2(P_B) &\le f_1(P_B^*) - \lambda^* f_2(P_B^*) \\ &= F(\lambda^*) = 0, \ \forall P_B \in S, \end{aligned} \tag{36}$$

which in turn can be rewritten as the condition as follows:

$$\lambda^* = \frac{f_1(P_B^*)}{f_2(P_B^*)} \ge \frac{f_1(P_B)}{f_2(P_B)}, \ \forall P_B \in S. \tag{37}$$

Therefore, the updating rule for λ can be expressed as

$$\lambda_{i+1} = \frac{f_1(P_{B_i}^*)}{f_2(P_{B_i}^*)} = \lambda_i - \frac{f_1(P_{B_i}^*) - \lambda_i f_2(P_{B_i}^*)}{-f_2(P_{B_i}^*)} = \lambda_i - \frac{F(\lambda_i)}{F'(\lambda_i)}. \tag{38}$$

It is worth noting that Dinkelbach algorithm follows Newton's method as far as updating λ is concerned, which exhibits a super-linear convergence rate [52].

2) OPTIMIZATION TIME-SWITCHING FACTOR

In order to solve Problem P3 in low complexity, we adopt Brent's method, which employs narrowing the linear feasible region to avoid the derivative. Indeed, Brent's method is an improved method combining two classical one-dimension search methods, that is the golden section search and the inverse parabolic interpolation. Specifically, Brent's method gives the priority to the inverse parabolic interpolation, and resorts to the golden section search when the inverse parabolic interpolation is invalid [53].

Then, we give a brief description of Brent's method in the optimization α when fixing P_B. Firstly, we choose an initial triple $\upsilon_0 = (\alpha_1, \alpha_3, \alpha_2)$, where $\alpha_1 < \alpha_3 < \alpha_2$ within initial interval $\alpha \in (0, 1)$. Then, we fit υ_0 by a parabola, of which maximum point α_4 can be acquired by the equation as follows:

$$\alpha_4 = \alpha_2 - \frac{1}{2}\frac{(\alpha_2-\alpha_1)^2[f(\alpha_2)-f(\alpha_3)] - (\alpha_2-\alpha_3)^2[f(\alpha_2)-f(\alpha_1)]}{(\alpha_2-\alpha_1)[f(\alpha_2)-f(\alpha_3)] - (\alpha_2-\alpha_3)[f(\alpha_2)-f(\alpha_1)]} \tag{39}$$

If the fitting is invalid or α_4 is located outside of the interval between α_1 and α_2, α_4 will be obtained by gold section search. Afterwards, compare the $\eta_s^{(sch)}(\alpha_4)$ and $\eta_s^{(sch)}(\alpha_3)$. If $\eta_s^{(sch)}(\alpha_4)$ is larger, the triplet will be updated as $\upsilon_1 = (\alpha_3, \alpha_4, \alpha_2)$, otherwise, $\upsilon_1 = (\alpha_1, \alpha_3, \alpha_4)$. Finally, at each iteration, the interval of the triple becomes smaller, until the interval is smaller than the predefined tolerance.

3) ALGORITHM DESCRIPTION

As shown in Algorithm 1, the overall optimization algorithm consists of one outer-loop and two inner-loops. The outer-loop is to control the iteration of SEE and stop when the difference of adjacent iteration is lower than the tolerance δ_0. And the first inner-loop uses the Dinkelbach algorithm to tackle the optimizing P_B w.r.t fixed α. Then the other inner-loop uses Brent's method to solve the optimizing α when fixing P_B. The first inner-loop stops when the tolerance δ_1 is achieved, while the other inner-loop ends when it achieves the stop criterion with tolerance δ_2.

Algorithm 1 Secure Energy Efficiency Maximization Algorithm

Input: M, N, R_{th}, θ_{th}, λ_{PS}, λ_{PR}, λ_{SR}, λ_{RB}, λ_{SE}, λ_{RE}, κ, P_c and tolerances δ_0, δ_1, δ_2.
Output: P_B^*, α^*, and $\eta_s^{*(sch)}$

Initialize: $k = 1$, $\eta_{s,0}^{(sch)} = 0$ and $\eta_{s,1}^{(sch)} = 1$
while $\eta_{s,k}^{(sch)} - \eta_{s,k-1}^{(sch)} \geq \delta_0$ **do**
  Initialize: $i = 0$, $\lambda_0 = 0$
  while: $|F(\lambda_i)| \geq \delta_1$ **do**
    Use $\lambda = \lambda_i$ in (36) to obtain P_{B_i};
    $\lambda_{i+1} = \frac{f_1(P_{B_i})}{f_2(P_{B_i})}$;
    $i++$;
  end
  $P_{B_k}^* = P_{B_i}$;
  Initialize: $i = 1$, $\upsilon_0 = (\alpha_1, \alpha_3, \alpha_2)$
  while: $|F(\lambda_i)| \geq \delta_2$ **do**
    if inverse parabolic interpolation is feasible;
    Update α_4 by inverse parabolic interpolation;
    else
    Update α_4 by golden section search;
    if $\eta_s^{(sch)}(\alpha_4) > \eta_s^{(sch)}(\alpha_3)$
    $\alpha_1 = \alpha_3$;
    $\alpha_3 = \alpha_4$;
    else
    $\alpha_2 = \alpha_4$;
    Update the triplet υ_i by the new $(\alpha_1, \alpha_3, \alpha_2)$
    $i++$;
  end
  $\alpha_k^* = \alpha_4$;
  $k++$;
  Update $\eta_{s,k}^{(sch)}$ by $P_{B_k}^*$ and α_k^*;
end
return $P_B^* = P_{B_k}^*$, $\alpha^* = \alpha_k^*$, and $\eta_s^{*(sch)} = \eta_{s,k}^{(sch)}$;

V. SIMULATION RESULTS

In this section, we provide some simulation results based on Monte Carlo to validate the aforementioned analysis. As in [33], we exploit the following parameters as $\gamma_E = 20$ dB, $R_{th} = 0.2$ bits/s/Hz, $\eta = 0.6$, $\lambda_{SR} = \lambda_{RD} = \lambda_{SE} = \lambda_{RE} = 10$, $\lambda_{BS} = \lambda_{BR} = 1$. Meanwhile, we set $N = 5$, $\kappa = 2.63$, and $P_c = 100$ mW as [37]. In each figure, the theoretical curves and simulation points match precisely with each other in all regions, which verifies the accuracy of our analysis.

Fig. 3 plots the impact of γ_P on the POP and overall SOP with $\alpha = 0.5$, $M = 3$, and $\gamma_{th} = 10$ dB. We observe that the POP of the BRR scheme and that of the BRS scheme are identical, which is much weaker than that of the BRBP scheme. This is due to the fact that the BRBP scheme makes full use of the power transfer channels and possess the diversity gain contributed not only by relays, but also by PBs. We further observe that the BRBP scheme still exhibits the best

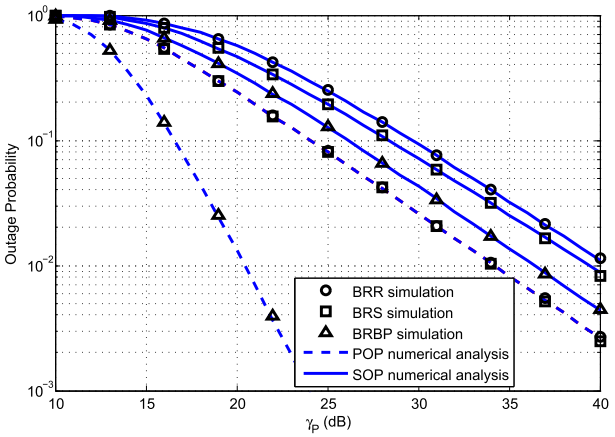


FIGURE 3. Impact of γ_P on the power outage probability and overall secrecy outage probability with $\alpha = 0.5$, $M = 3$, and $\gamma_{th} = 10$ dB.

performance of overall SOP considering POP. This indicates that the potential insufficiency of the acquired energy for sensors may seriously deteriorate the overall SOP, which also reflects the importance of energy efficiency for IoT scenarios.

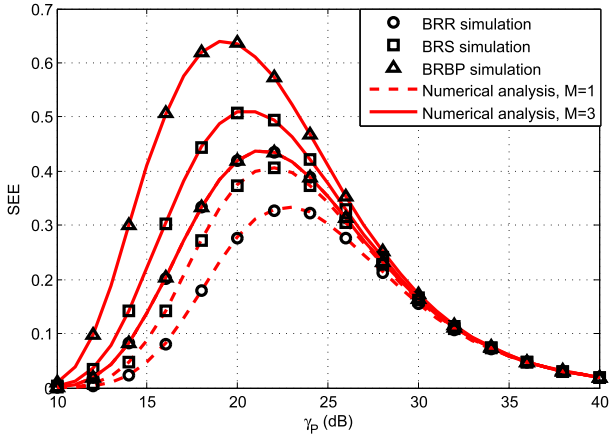


FIGURE 4. Impact of γ_P and M on the secrecy energy efficiency with $\alpha = 0.5$ and $\gamma_{th} = 10$ dB.

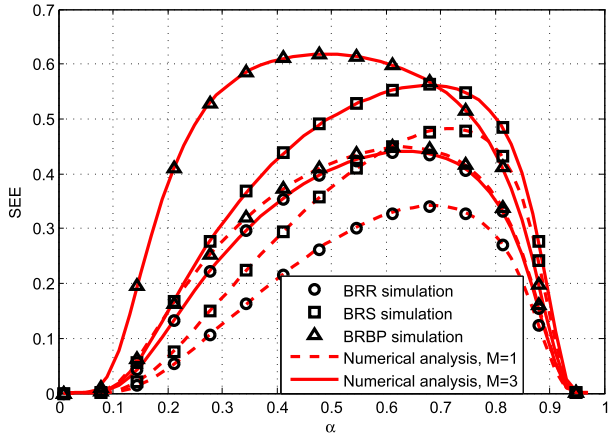


FIGURE 5. Impact of α and M on the secrecy energy efficiency with $\gamma_P = 20$ dB and $\gamma_{th} = 10$ dB.

Figs. 4 and 5 plot the SEE versus γ_P with $\alpha = 0.5$ when $\gamma_{th} = 10$ dB and the SEE versus α with $\gamma_P = 20$ dB when $\gamma_{th} = 10$ dB, respectively. Firstly, we observe that both of the function of SEE w.r.t γ_P and the function of SEE w.r.t α are unimodal function. The former result is because the SEE improves with the increasing of γ_P in low energy consumption, while the denominator of SEE deteriorates quickly in high energy consumption. The latter result is because the harvested energy for sensors is often insufficient when α is small, while if α is too large, the data transmission duration will be very short leading to high transmission interruption probability. Moreover, we observe that the SEE performance is better when there is more PBs. This can be explained that more PBs can provide lager diversity gain to decline POP. In addition, the BRBP scheme shows the best SEE performance in most conditions, which can be explained similarly as the analysis in last paragraph.

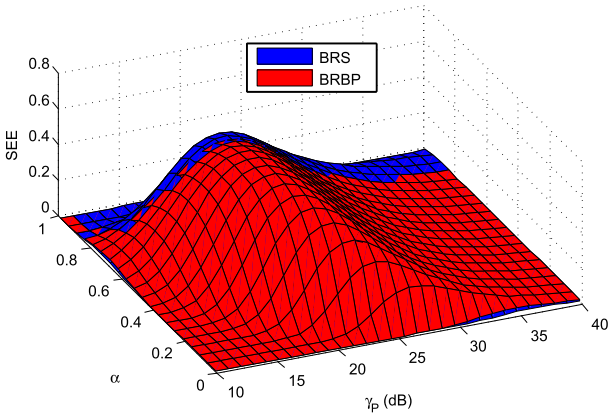


FIGURE 6. Overall impact of γ_P and α on the secrecy energy efficiency with $M = 3$ and $\gamma_{th} = 10$ dB.

Fig. 6 is the 3-dimension figure of the BRS and BRBP schemes to illustrate the impacts of γ_P and α on SEE performance with $M = 3$ and $\gamma_{th} = 10$ dB. It is worth noting that the SEE performance of the BRBP scheme is better than that of the BRS scheme in most occasions. However, when the α is very large, the SEE of the BRS scheme is higher. It is due to the fact that if the proportion of EH time in a transmission block time is very large, the harvested energy for sensors is generally ample. As such, the security replaces the energy efficiency as the dominant factor of the overall performance and thus the BRS scheme focused on the security is more advantageous.

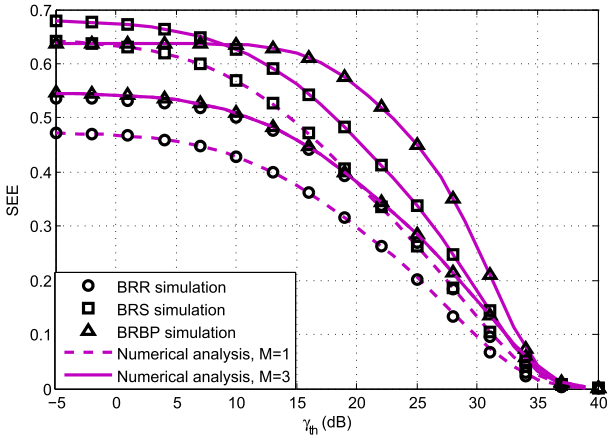


FIGURE 7. Impact of γ_{th} and M on the optimization of secrecy energy efficiency.

Fig. 7 describes the impact of γ_{th} and M on the SEE optimized by the Dinkelbach approach combined with Brent's method. We observe that the BRBP scheme is more advantageous when γ_{th} and M is larger. By contrast, when the γ_{th} is lower, the POP decreases, which is constructive for the BRS scheme. Indeed, this condition enables the sensors harvest sufficient energy more easily, of which effect is similar with the operation of increasing P_B or increasing α.

VI. CONCLUSION

In this paper, we consider three PB and relay selection schemes in a wireless powered IoT with multiple PBs. For three schemes, the closed-form expressions of POP, SOP, and SEE are derived. Then the SEE maximization problem with the transmit power constraint at PBs is formulated and solved by the Dinkelbach algorithm combining Brent's method to optimize the transmit power at PBs and the time-switching factor. Simulation results indicate that it is favorable to put more PBs in the considered system, which is contribute to the improvement of SOP and SEE. Meanwhile, the BPBR scheme shows the best SEE performance among three schemes in most scenarios. But when the time-switching factor is very large or the power outage threshold is lower, the BRS scheme is more advantageous because the source sensor and relays can harvest ample energy more easily. It is worth noting that the influence of the charging distance is not analyzed in this paper, which can be also optimized for the mobile PB in our future works.

APPENDIX A

From (23), γ_{sec,SR_n} can be expressed as

$$\begin{aligned}&\gamma_{sec,SR_n}\\&=\min\left(\frac{1+\gamma_P\xi\left|h_{P_{m^*}S}\right|^2|h_{SR_n}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}S}\right|^2|h_{SE}|^2},\frac{1+\gamma_P\xi\left|h_{P_{m^*}R_n}\right|^2|h_{R_nB}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}R_n}\right|^2|h_{R_nE}|^2}\right)\\&=\min\left(\gamma_{sec1,SR_n},\gamma_{sec2,SR_n}\right)\end{aligned}\tag{40}$$

Then, from (20), we have

$$P_{sout,SR_n}=\Pr(\gamma_{sec,SR_n}<\beta)=F_{\gamma_{sec,SR_n}}(\beta)\tag{41}$$

where $F_{\gamma_{sec,SR_n}}(\beta)$ is the CDF of γ_{sec,SR_n}, which can be given by

$$\begin{aligned}&F_{\gamma_{sec,SR_n}}(\beta)\\&=\Pr\{\gamma_{sec,SR_n}<\beta\}\\&=\Pr\{\min\left(\gamma_{sec1,SR_n},\gamma_{sec2,SR_n}\right)<\beta\}\\&=1-\Pr\{\gamma_{sec1,SR_n}>\beta\}\Pr\{\gamma_{sec2,SR_n}>\beta\}\\&=1-[1-\Pr\{\gamma_{sec1,SR_n}<\beta\}]\times[1-\Pr\{\gamma_{sec2,SR_n}<\beta\}].\end{aligned}\tag{42}$$

Afterwards, $\Pr\{\gamma_{sec1,SR_n}<\beta\}$ and $\Pr\{\gamma_{sec2,SR_n}<\beta\}$ can be derived with the help of Eq. (3.351.3) in [48] and the binomial expansion as follows:

$$\begin{aligned}&\Pr\{\gamma_{sec1,SR_n}<\beta\}\\&=\Pr\left\{\frac{1+\gamma_P\xi\left|h_{P_{m^*}S}\right|^2|h_{SR_n}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}S}\right|^2|h_{SE}|^2}<\beta\right\}\\&=\int_0^\infty\int_0^\infty F_{|h_{SR_n}|^2}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_P\xi x}\right]\\&\quad\times f_{\left|h_{P_{m^*}S}\right|^2}(x)f_{|h_{SE}|^2}(y)dxdy\\&=1-\sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1}\frac{m\gamma_P\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_P+\beta\gamma_E\lambda_{SR}}\\&\quad\times2\sqrt{\frac{\lambda_{SR}(\beta-1)}{m\gamma_P\xi\lambda_{PS}}}K_1\left(2\sqrt{\frac{m\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_P\xi}}\right),\end{aligned}\tag{43}$$

$$\begin{aligned}&\Pr\{\gamma_{sec2,SR_n}<\beta\}\\&=\Pr\left\{\frac{1+\gamma_P\xi\left|h_{P_{m^*}R_n}\right|^2|h_{R_nB}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}R_n}\right|^2|h_{R_nE}|^2}<\beta\right\}\\&=\int_0^\infty\int_0^\infty F_{|h_{R_nB}|^2}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_P\xi x}\right]\\&\quad\times f_{\left|h_{P_{m^*}R_n}\right|^2}(x)f_{|h_{R_nE}|^2}(y)dxdy\\&=1-\frac{\gamma_P\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_P+\beta\gamma_E\lambda_{RB}}\\&\quad\times2\sqrt{\frac{\lambda_{RB}(\beta-1)}{\gamma_P\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{\lambda_{PR}\lambda_{RB}(\beta-1)}{\gamma_P\xi}}\right).\end{aligned}\tag{44}$$

By substituting the (43) and (44) into (42), after some mathematical manipulation, we have (26).

APPENDIX B

From (23), $\gamma_{sec}^{(BRS)}$ can be expressed as

$$\begin{aligned}&\gamma_{sec}^{(BRS)}\\&=\min\left(\frac{1+\gamma_P\xi|h_{P_{m^*}S}|^2|h_{SR_{n^*}}|^2}{1+\gamma_E\xi|h_{P_{m^*}S}|^2|h_{SE}|^2},\frac{1+\gamma_P\xi|h_{P_{m^*}R_{n^*}}|^2|h_{R_{n^*}B}|^2}{1+\gamma_E\xi|h_{P_{m^*}R_{n^*}}|^2|h_{R_{n^*}E}|^2}\right)\\&=\min\left(\gamma_{\text{sec }1}^{(BRS)},\gamma_{\text{sec }2}^{(BRS)}\right).\end{aligned}\tag{45}$$

Then, from (20), we have

$$P_{sout}^{(BRS)}=\Pr(\gamma_{sec}^{(BRS)}<\beta)=F_{\gamma_{sec}^{(BRS)}}(\beta),\tag{46}$$

where $F_{\gamma_{sec}^{(BRS)}}(\beta)$ is the CDF of $\gamma_{sec}^{(BRS)}$, which can be given by

$$\begin{aligned}F_{\gamma_{sec}^{(BRS)}}(\beta)&=\Pr\{\gamma_{sec}^{(BRS)}<\beta\}\\&=\Pr\{\min\left(\gamma_{sec1}^{(BRS)},\gamma_{sec2}^{(BRS)}\right)<\beta\}\\&=1-\Pr\{\gamma_{sec1}^{(BRS)}>\beta\}\Pr\{\gamma_{sec2}^{(BRS)}>\beta\}\\&=1-[1-\Pr\{\gamma_{sec1}^{(BRS)}<\beta\}]\times[1-\Pr\{\gamma_{sec2}^{(BRS)}<\beta\}].\end{aligned}\tag{47}$$

Afterwards, $\Pr\{\gamma_{sec1}^{(BRS)}<\beta\}$ and $\Pr\{\gamma_{sec2}^{(BRS)}<\beta\}$ can be derived with the help of Eq. (3.351.3) in [48] and the binomial expansion as follows:

$$\begin{aligned}&\Pr\{\gamma_{sec1}^{(BRS)}<\beta\}\\&=\Pr\left\{\frac{1+\gamma_P\xi\left|h_{P_{m^*}S}\right|^2|h_{SR_{n^*}}|^2}{1+\gamma_E\xi\left|h_{P_{m^*}S}\right|^2|h_{SE}|^2}<\beta\right\}\\&=\int_0^\infty\int_0^\infty F_{|h_{SR_{n^*}}|^2}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_P\xi x}\right]\\&\quad\times f_{\left|h_{P_{m^*}S}\right|^2}(x)f_{|h_{SE}|^2}(y)dxdy\end{aligned}$$

$$= 1 - \sum_{n=1}^{N}\sum_{m=1}^{M}\binom{N}{n}\binom{M}{m}(-1)^{m+n}\frac{m\gamma_P\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_P + n\beta\gamma_E\lambda_{SR}} \times 2\sqrt{\frac{n\lambda_{SR}(\beta-1)}{m\gamma_P\xi\lambda_{PS}}}K_1\left(2\sqrt{\frac{mn\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_P\xi}}\right), \quad (48)$$

$$\Pr\{\gamma_{sec2}^{(BRS)} < \beta\} = \Pr\left\{\frac{1+\gamma_P\xi\left|h_{P_{m^*}R_{n^*}}\right|^2\left|h_{R_{n^*}B}\right|^2}{1+\gamma_E\xi\left|h_{P_{m^*}R_{n^*}}\right|^2\left|h_{R_{n^*}E}\right|^2} < \beta\right\}$$
$$= \int_0^\infty\int_0^\infty F_{\left|h_{R_{n^*}B}\right|^2}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_P\xi x}\right] \times f_{\left|h_{P_{m^*}R_{n^*}}\right|^2}(x)f_{\left|h_{R_{n^*}E}\right|^2}(y)dxdy$$
$$= 1 - \frac{\gamma_P\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_P + \beta\gamma_E\lambda_{RB}} \times 2\sqrt{\frac{\lambda_{RB}(\beta-1)}{\gamma_P\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{\lambda_{PR}\lambda_{RB}(\beta-1)}{\gamma_P\xi}}\right). \quad (49)$$

By substituting the (48) and (49) into (47), after some mathematical manipulation, we have (27).

APPENDIX C

Similarly, $\Pr\{\gamma_{sec1}^{(BRBP)} < \beta\}$ and $\Pr\{\gamma_{sec2}^{(BRBP)} < \beta\}$ can be derived with the help of Eq. (3.351.3) in [48] and the binomial expansion as follows:

$$\Pr\{\gamma_{sec1}^{(BRBP)} < \beta\} = \Pr\left\{\frac{1+\gamma_P\xi\left|h_{P_{m^*}S}\right|^2\left|h_{SR_{n^*}}\right|^2}{1+\gamma_E\xi\left|h_{P_{m^*}S}\right|^2|h_{SE}|^2} < \beta\right\}$$
$$= \int_0^\infty\int_0^\infty F_{|h_{SR_{n^*}}|^2}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_P\xi x}\right] \times f_{\left|h_{P_{m^*}S}\right|^2}(x)f_{|h_{SE}|^2}(y)dxdy$$
$$= 1 - \sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1}\frac{m\gamma_P\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_P + \beta\gamma_E\lambda_{SR}} \times 2\sqrt{\frac{\lambda_{SR}(\beta-1)}{m\gamma_P\xi\lambda_{PS}}}K_1\left(2\sqrt{\frac{m\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_P\xi}}\right), \quad (50)$$

$$\Pr\{\gamma_{sec2}^{(BRBP)} < \beta\} = \Pr\left\{\frac{1+\gamma_P\xi\left|h_{P_{m^*}R_{n^*}}\right|^2\left|h_{R_{n^*}B}\right|^2}{1+\gamma_E\xi\left|h_{P_{m^*}R_{n^*}}\right|^2\left|h_{R_{n^*}E}\right|^2} < \beta\right\}$$
$$= \int_0^\infty\int_0^\infty F_{\left|h_{R_{n^*}B}\right|^2}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_P\xi x}\right] \times f_{\left|h_{P_{m^*}R_{n^*}}\right|^2}(x)f_{\left|h_{R_{n^*}E}\right|^2}(y)dxdy$$
$$= 1 - \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n\gamma_P\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_P + \beta\gamma_E\lambda_{RB}} \times 2\sqrt{\frac{\lambda_{RB}(\beta-1)}{n\gamma_P\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{n\lambda_{PR}\lambda_{RB}(\beta-1)}{\gamma_P\xi}}\right). \quad (51)$$

From (50) and (51), after some mathematical manipulation, we have (28).

REFERENCES

[1] M. Gholami and R. W. Brennan, "A comparison of alternative distributed dynamic cluster formation techniques for industrial wireless sensor networks," *Sensors*, vol. 16, no. 1, p. 65, Jan. 2016.
[2] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1565–1568, Jul. 2017.
[3] 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.
[4] 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," *Renew. Sustain. Energy Rev.*, vol. 38, pp. 973–989, Oct. 2014.
[5] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3858–3871, Sep. 2016.
[6] Z. Chen, L. Hadley, Z. Ding, and X. Dai, "Improving secrecy performance of a wirelessly powered network," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4996–5008, Nov. 2017.
[7] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative strategies for wireless-powered communications: An overview," *IEEE Wireless Commun.*, vol. 25, no. 4, pp. 112–119, Aug. 2018, doi: 10.1109/MWC.2017.1700245.
[8] G. Yang, C. K. Ho, R. Zhang, and Y. L. Guan, "Throughput optimization for massive MIMO systems powered by wireless energy transfer," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 8, pp. 1640–1650, Aug. 2015.
[9] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.
[10] M. Ju, K.-M. Kang, K.-S. Hwang, and C. Jeong, "Maximum transmission rate of PSR/TSR protocols in wireless energy harvesting DF-based relay networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2701–2717, Dec. 2015.
[11] K. Tutuncuoglu, B. Varan, and A. Yener, "Throughput maximization for two-way relay channels with energy harvesting nodes: The impact of relaying strategies," *IEEE Trans. Commun.*, vol. 63, no. 6, pp. 2081–2093, Jun. 2015.
[12] X. Wang, J. Liu, and C. Zhai, "Wireless power transfer-based multi-pair two-way relaying with massive antennas," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7672–7684, Nov. 2017.
[13] Y. Ma, H. Chen, Z. Lin, Y. Li, and B. Vucetic, "Distributed and optimal resource allocation for power beacon-assisted wireless-powered communications," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3569–3583, Oct. 2015.
[14] C. Zhong, G. Zheng, Z. Zhang, and G. K. Karagiannidis, "Optimum wirelessly powered relaying," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1728–1732, Oct. 2015.
[15] Y. Zou and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*. Berlin, Germany: Springer, 2016.
[16] W. Cao, Y. Zou, and Z. Yang, "Joint source-relay selection for improving wireless physical-layer security," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–5.
[17] J. Yan, C. Zhang, and Z. Gao, "Distributed relay selection protocols for simultaneous wireless information and power transfer," in *Proc. IEEE 25th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Washington, DC, USA, Sep. 2014, pp. 474–479.
[18] Z. Ding, I. Krikidis, B. Sharif, and H. V. Poor, "Wireless information and power transfer in cooperative networks with spatially random relays," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4440–4453, Aug. 2014.
[19] I. Krikidis, "Relay selection in wireless powered cooperative networks with energy storage," *IEEE J. Sel. Area Commun.*, vol. 33, no. 12, pp. 2596–2610, Dec. 2015.
[20] K.-H. Liu and T.-L. Kung, "Performance improvement for RF energy-harvesting relays via relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8482–8494, Sep. 2017.
[21] C. Zhai and J. Liu, "Cooperative wireless energy harvesting and information transfer in stochastic networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, pp. 1–22, Mar. 2015.

[22] H. Chen, Y. Li, Y. Jiang, Y. Ma, and B. Vucetic, "Distributed power splitting for SWIPT in relay interference channels using game theory," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 410–420, Jan. 2015.

[23] 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 Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856–3867, Jun. 2016.

[24] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1133–1143, May 2014.

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

[26] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 780–787, Apr. 2016.

[27] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[28] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

[30] 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 Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[31] 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 Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[32] 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, Apr. 2018.

[33] 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.

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

[35] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.

[36] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[37] D. Chen, W. Yang, J. Hu, Y. Cai, and X. Tang, "Energy-efficient secure transmission design for the Internet of Things with an untrusted relay," *IEEE Access*, vol. 6, pp. 11862–11870, Feb. 2018.

[38] H. Chen, Y. Li, J. L. Rebelatto, B. F. Uchôa-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, Apr. 2015.

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

[40] T.-V. Truong, N.-V. Vo, D.-B. Ha, and D.-D. Tran, "Secrecy performance analysis of energy harvesting wireless networks with multiple power transfer stations and destinations in the presence of multiple eavesdroppers," in *Proc. 3rd Nat. Found. Sci. Technol. Develop. Conf. Inf. Comput. Sci. (NICS)*, Danang, Vietnam, Sep. 2016, pp. 107–112.

[41] 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, Oct. 2017.

[42] J. Yan, C. Zhang, and Z. Gao, "Distributed relay selection protocols for simultaneous wireless information and power transfer," in *Proc. IEEE 25th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Washington, DC, USA, Sep. 2014, pp. 474–479.

[43] F. Yuan, Q. T. Zhang, S. Jin, and H. Zhu, "Optimal harvest-use-store strategy for energy harvesting wireless systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 698–710, Feb. 2015.

[44] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[45] J. Guo, S. Durrani, X. Zhou, and H. Yanikomeroglu, "Outage probability of ad hoc networks with wireless information and power transfer," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 409–412, Aug. 2015.

[46] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[47] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[48] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

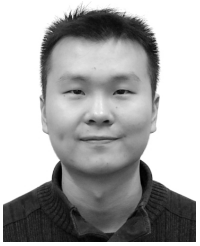
[49] M. Xia and S. Aissa, "On the efficiency of far-field wireless power transfer," *IEEE Trans. Signal Process.*, vol. 63, no. 11, pp. 2835–2847, Jun. 2015.

[50] 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, Oct. 2016.

[51] A. Zappone and E. Jorswieck, "Energy efficiency in wireless networks via fractional programming theory," *Found. Trends Commun. Inf. Theory*, vol. 11, nos. 3–4, pp. 185–396, 2015.

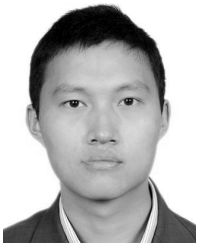
[52] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, no. 7, pp. 492–498, Mar. 1967.

[53] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes: The Art Of Scientific Computing*, 3rd ed. New York, NY, USA: Cambridge Univ. Press, 2007.

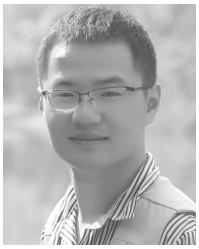


YIDA WANG received the B.S. degree in automation from Xiamen University, Xiamen, China, in 2015, and the M.S. degree in information and communication engineering from the College of Communication Engineering, Army Engineering University of PLA, Nanjing, China, in 2018, where he is currently pursuing the Ph.D. degree in information and communications engineering. His current research interests include cooperative communications, wireless sensor networks, the Internet of Things, physical-layer security, and energy harvesting.

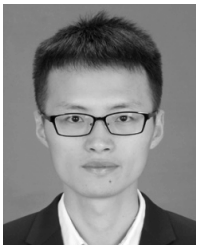
WEIWEI YANG (S'08–M'12) received the B.S., M.S., and Ph.D. degrees from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively. His research interests include orthogonal frequency-domain multiplexing systems, signal processing in communications, cooperative communications, wireless sensor networks, and network security.



XIAOHUI SHANG received the B.S. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2009, and the M.S. degree in information and communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2012. He is currently pursuing the Ph.D. degree in information and communications engineering with the Army Engineering University of PLA, Nanjing. His current research interests include cooperative communications, wireless sensor networks, MIMO, physical-layer security, and energy beamforming.



JIANWEI HU (S'14) received the B.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2012, where he is currently pursuing the Ph.D. degree in communications and information system. His research interests include MIMO systems, cooperative communications, and network security.



YUZHEN HUANG (S'12–M'16) received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, in 2008 and 2013, respectively. He is currently an Assistant Professor with the College of Communications Engineering, Army Engineering University of PLA. He has published nearly 70 research papers in international journals. His research interests include channel coding, MIMO systems, cooperative communications, physical layer security, and cognitive radio systems. He received the Best Paper Award at WCSP 2013. He received an IEEE Communications Letters Exemplary Reviewer Certificate in 2014. He served as an Associate Editor for the *KSII Transactions on Internet and Information Systems*.

YUEMING CAI (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982, and the M.S. degree in micro-electronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include MIMO systems, OFDM systems, signal processing in communications, cooperative communications, and wireless sensor networks.