IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 28, 2021, accepted March 16, 2021, date of publication March 19, 2021, date of current version April 6, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3067472

Secure Multiuser Scheduling for Hybrid Relay-Assisted Wireless Powered Cooperative Communication Networks With Full-Duplex Destination-Based Jamming

XIAOHUI SHANG[1,2], HAO YIN[2], YIDA WANG[1], MU LI[3], AND YONG WANG[1]
[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Institute of Systems Engineering, Academy of Military Science, Beijing 100039, China
[3]61618 Troops of PLA, Beijing 100094, China

Corresponding author: Xiaohui Shang (shangxiaohui1214@126.com)

ABSTRACT In this paper, we investigate secure communication in a hybrid relay (HR)-assisted wireless powered cooperative communication network (WPCCN), where an eavesdropper tries to intercept the data transmitted by a source user and the HR simultaneously. The HR has the ability to wireless powered the energy-constrained multiple users in the downlink and to relay the received confidential information in the uplink. In particular, the full-duplex destination-based jamming (FD-DBJ) strategy is exploited to improve the secrecy performance. Moreover, in order to conduct effective secure communications, we design two multiuser scheduling schemes, i.e., random user selection (RUS), and best user selection (BUS) based on the main channel quality. In order to evaluate the secrecy performance, we analytically derive the energy outage probability (EOP), the secrecy outage probability (SOP), and the hybrid outage probability (HOP), respectively. As such, we formulate the secrecy throughput (ST) maximization problem to optimize the predetermined transmission rate. Our analysis and numerical results reveal that: 1) The BUS scheme has better security performance. 2) Both of the energy conversion efficiency and the number of users have a positive effect on secrecy performance. 3) The FD-DBJ scheme is an effective method to achieve secure communications. 4) The time-switching factor and predetermined transmission rate have a crucial influence on the secrecy performance, which should be considered carefully in system design.

INDEX TERMS Wireless powered cooperative communication networks, hybrid relay, full-duplex destination-based jamming, physical layer security, secrecy outage probability.

I. INTRODUCTION

A. BACKGROUND

With the continuous development of wireless communication technology, the world is witnessing a new network architecture characterized by fast transmission speed, large network capacity and low delay, which is named the fifth generation (5G) mobile communication system [1], [2]. As a typical application of 5G, the Internet of Things (IoT), which connects massive machines and devices in the future communication network, has changed people's life, learning and working methods subtly [3]. However, the widespread application of the IoT unavoidably brings a lot of transmission devices, which are usually low-cost and energy-limited. Meanwhile, the rapid growth of multimedia services and high-speed data, coupled with the demand to improve the quality of service, make the energy consumption gradually increased. At present, the shortage of standby time and energy deficiency have become the main bottleneck, which is fundamentally restricting the large-scale popularization of IoT applications [4]. Fortunately, the emergence of advanced wireless powered communication (WPC), which takes advantage of radio-frequency energy harvesting (RF-EH) technology, provides a viable method to extend the longevity of energy-limited wireless network and to sustain IoT in a long run [5]–[7]. In general, any wireless

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

communication network composed of devices that harvest energy for information exchange needs can be called a wireless powered communication network (WPCN). Specifically, the battery of wireless terminals in WPCN can be remotely replenished by the ambient wireless transmitter or the power beacon (PB) with the help of EH technology, which is helpful to avoid the burden caused by frequent wired charging and battery replacement for communication devices [8]–[10]. As a result, WPC technology has attracted wide attention and has been generally explored in a variety of wireless communication system, such as cognitive radio networks [10], wireless sensor networks (WSNs) [11], IoT [12], [13] and so on.

The main obstacle to the wide application of WPC is the short transmission distance due to the dual path loss and fading, resulting in limited harvested energy at terminals. Intuitively, multi-antenna technology can be used to improve the efficiency of EH [14]. Unfortunately, this solution is not suitable to the devices of IoT, which is restricted to the cost and size owing to the user requirement for lightweight and miniaturization. Recently, the cooperative communication technology, which aims to achieve spatial diversity gain and to improve system performance without increasing complexity and quantity of the device, has been regarded as a promising approach to tackle above problem [15]–[17]. With the deepening of the research on the cooperative communication technology, its positive role in energy consumption and security has been paid more and more attention [18], [19]. In particular, a cooperative communication network with one or more wireless powered nodes is termed wireless powered cooperative communication network (WPCCN) [20], which can effectively expand the coverage and improve the throughout and energy efficiency of WPCN as well as alleviate the influence of node energy constraints on performance of wireless communication system [21]–[23]. Specifically, the WPCN with energy/information relaying, which is regarded as a special case of cooperative networks, can also be considered as a WPCCN.

However, in addition to the above advantages, WPCCN faces more serious threats than traditional wireless networks in terms of security and privacy due to the complexity of network structure and the diversity of nodes, which makes it vulnerable to information interception and eavesdropping [24]. For example, the EH nodes can change their roles and become potential eavesdroppers who want to eavesdrop on information between the source and the controller, which raises a tough security challenge. In general, traditional cryptographic methods are used to ensure the confidentiality of data transmission. However, the higher computational complexity will lead to quite a few unfavorable factors, including network delay, excessive overhead and so on, which are sensitive to future networks. To mitigate this issue, physical layer security (PLS), which contributes to its low latency, low complexity and ability to be combined with other security approaches easily for enhancement of secrecy performance, has been supposed as a promising complement to the current methods of information security [25]–[27].

B. RELATED WORKS

Recently, there are numerous works on the PLS of WPCCN [12], [28]–[30]. Specifically, the authors in [28] proposed two schemes of joint relay and jammer selection to achieve the secure transmission in a WPCCN system with many wireless-powered intermediate nodes. A joint PB and relay selection secure strategy was designed for 5G wireless communications in [29], where a sensor user and multiple intermediate nodes acquire energy from a multi-antenna PB for information transmission. Furthermore, as the extend of [29], the authors in [12] proposed a secure transmission approach, in which the different relay selection schemes are compared and secure energy efficiency (SEE) maximization of the proposed strategies is solved. Differently, secrecy analysis of WPCCN with multiple multi-antenna relays under nonlinear EH and imperfect CSI was explored in [30]. Nevertheless, it should be noted that most of works paid attention to the enhancement of secrecy performance by means of multiple relays or multi-antenna technique, but neglected the important scenario with multiple users, which is considered as the main topology of future networks [31]–[34]. In fact, the multiuser scheduling is considered as an effective means of enhancing the PLS of wireless networks without consuming additional resources.

Meanwhile, the hybrid relay (HR) has been introduced in WPCCN to improve the transmission throughput, which plays a dual-role of PB and relay. Specifically, the HR charges the source user first and then forwards the information transmitted from the source user, i.e., adopting charge-then-forward (CTF) mode [35]–[41]. At present, the research on WPCCN is generally based on EH relay. The so-called EH relay means that the relay in the network has no stable energy supply, so it needs to use WPC technology to harvest energy from the RF signals broadcast by PB or other sources to forward the received information. Thus, the EH relay is an auxiliary information node, which is responsible for forwarding the confidential data. In contrast, another network model with HR is a special topological structure, in which the relay is powered by on-grid power. In the downlink, it can act as a PB to provide energy signals for the EH users, and in the uplink, it can be used as an information fusion node to receive the information of the source and assist in forwarding. The special structure makes HR show dual roles. In fact, compared with the base stations (BS), small HRs are cheaper and can be deployed on a large scale easily. Aided by the HRs, the number of wireless users accessing the network through BS can be greatly reduced. Meanwhile, the devices far from the BS can also achieve better uplink communication quality and downlink wireless powering service through the latest HR. In particular, the concept of HR is first described in [35], and both the working principle and the transmission performance of HR-assisted WPCCN are analyzed. Then, a full-duplex HR model is investigated in [36], where the channel capacity in harvest-use (HU) mode without the battery and in harvest-store-use (HSU) mode with infinite battery capacity is deduced, respectively.

Furthermore, the authors in [37] and in [38] considered a HR model with multiple wireless powered users and multiple access points, in which they maximized the total transmission rate by adjusting the transmission power and time-switching factor of the HR. The authors in [39] explored the energy efficiency maximization for decode-and-forward (DF) and amplify-and-forward (AF) relay-assisted WPCCN through the joint optimization of the duration and the power allocation. The coverage probability of hierarchical wireless powered networks with the HR was discussed in [40]. In addition, the authors in [41] investigated the throughput of wireless-powered relaying systems with the buffer-aided HR.

C. OUR APPROACH AND CONTRIBUTION

Although the introduction of HR into the WPCCN can improve the transmission throughput, the potential malicious HR also poses a severe threat to the security of the WPCCN. It is noted that a malicious HR can intercept the signals transmitted from both of the source user and the legitimate HR, which deteriorates the secrecy performance. In addition, the information leakage from a data-fusion HR may cause greater losses. However, the secrecy of the HR-assisted WPCCN is overlooked in aforementioned works.

Therefore, in this paper, we focus on the PLS of a HR-assisted WPCCN, where a HR charges multiple source users in the downlink and forwards the confidential information transmitted from a selected source user in the presence of a malicious HR as an eavesdropper. In order to achieve the secure transmission, we adopt the user selection scheme based on the channel quality from the source user to the HR and introduce the destination-based jamming (DBJ) generated from a full-duplex (FD) destination node, i.e., the FD-DBJ scheme. Specifically, the main contributions of this work are listed as follows:

- We investigate the PLS in the HR-assisted WPCCN with FD-DBJ and introduce two secure multiuser scheduling schemes: 1) random user scheduling (RUS), i.e., the source user is selected randomly; 2) best user scheduling (BUS), i.e., an optimal source user is selected to transmit information based on the channel quality between the user and the HR. Furthermore, as for the considered system, we derive the exact closed-form expressions of energy outage probability (EOP), secrecy outage probability (SOP), and hybrid outage probability (HOP), respectively.
- Based on the performance analysis to the considered system, we further formulate the secrecy throughput (ST) optimization problem. Then, we propose a low-complexity ST maximization algorithm based on the Brent method to optimize the predetermined transmission rate, which achieves a balance between the communication throughput and secrecy.
- Simulation results show that the BUS scheme can make full use of the multiuser diversity gain and achieve better secrecy performance. Meanwhile, we can adjust some parameters, such as increasing the number of source users, improving the EH efficiency and enhancing the transmit power of the DBJ, to improve the secrecy performance of the considered multiuser WPCCN. In addition, we confirm that the FD-DBJ scheme is an effective method to achieve the secure communication. In addition, both of the time switching factor and the predetermined transmission rate have a significant effect on the ST, which should be considered carefully aiming to secure and efficient communication.

D. ORGANIZATION

The rest of this paper is summarized as follows. We describe the system model and two secure multiuser scheduling strategies in Section 2. Section 3 analyzes the secrecy performance both the RUS and BUS schemes in terms of the exact expressions for EOP, SOP and HOP, and explores the ST optimization problem. Then, Section 4 discusses the simulation results. Finally, Section 5 states conclusions.

Notation: Scalar variables are denoted by italic symbols. Vectors are denoted by boldface symbols. Given a complex number, $|\cdot|$ denotes its modulus. Given an event, $\Pr(\cdot)$ denotes its probability of occurrence. $\mathbb{E}(\cdot)$ denotes the expectation operation.

II. SYSTEM MODEL AND SIGNAL ANALYSIS

A. SYSTEM MODEL

Consider a multiuser WPCCN with HR and FD-DBJ as illustrated in Fig. 1, which is composed of N source users (S_n), $n = \{1, \ldots, N\}$, a HR (R), a destination (D), a passive eavesdropper (E), where the "passive" means that the channel state information (CSI) from S_n, R and D to E are unavailable for the user scheduling. It is noted that the broadcast nature of radio propagation leads to any receivers within the coverage area of a radio transmitter being capable of overhearing the wireless transmission. This makes the wireless communication systems extremely vulnerable to the eavesdropping attack. In contrast of the active attack, the passive eavesdropping attack is hard to be discovered by the legitimate communication parties. In particular, in the HR-aided WPCCN, a malicious HR is easy to intercept considerable information transmitted from both of a source user and a legitimate HR, and in order to keep the network running for a long time, they must harvest energy by WPC technique from the HR to support data interaction [11], [12].

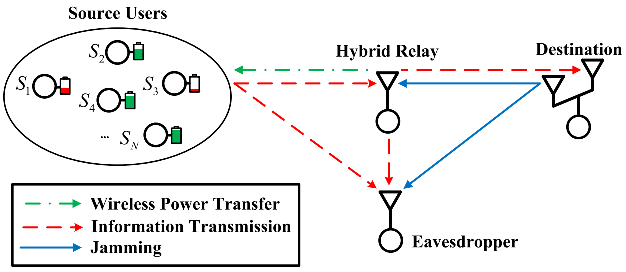


FIGURE 1. System model.

The HR and the destination are powered by on-grid power. Specifically, in the downlink, the HR powers multiple users based on the WPC technique, while it utilizes the decode-and-forward (DF) relay scheme to help the selected user to forward information in the uplink, which makes the HR as a data fusion center for multiple source nodes to improve the system performance. In fact, the HR charges other EH nodes as PB and the HR forwards information as the data fusion node can be considered as two independent processes, which can be realized by operating EH and the information transmission in different frequency bands [42]. In addition, the worse scenario is assumed, that is E can simultaneously intercept the information from S_n and R. Then, due to the cost and size limitations, it is considered that S_n, R and E are single antenna and HD devices. It is worth noting that above structure has important applications in many energy-limited systems, such as the data uploading network with devices for collecting information in dense environment and WSNs. In order to provide secure data transmission, the destination is equipped with two antennas and works in the FD mode, which can be transmitted the jamming signal to confuse the eavesdropper, and received the confidential information from the legitimate nodes simultaneously, i,e, the FD-DBJ scheme is exploited at the destination[1] [43], [44].

Furthermore, the channel coefficients between nodes X and Y are denoted as h_{XY}, in which $X \in \{S_n, R, D\}$, $Y \in \{R, D, E\}$. In the considered system, all channels are assumed to be independent quasi-static Rayleigh fading as [11], [12], [45], which is a special case of Rician fading and can be treated as a fundamental work for more general Rician fading scenario. Therefore, the power gains of link $|h_{XY}|^2$ are distributed exponentially with means $1/\lambda_{XY}$, i.e., $1/\lambda_{XY}$ can fully characterize the signal attenuation caused by fading and path loss [46]. In addition, the direct $S_n \rightarrow D$ link is not available due to the obstacles or severe attenuation [12], [29], so the source users must upload the confidential information by means of HR. Moreover, the N source users are considered to form a cluster. In fact, the assumption is generally adopted in the WPCCN with multiusers or multi-relays [11], [12], [45], which produces the identical mean power gains of the links $S_n \rightarrow R$, $S_n \rightarrow E$, $R \rightarrow S_n$. For simplicity, we define $\lambda_{S_nR} = \lambda_{SR}$, $\lambda_{S_nE} = \lambda_{SE}$, $\lambda_{RS_n} = \lambda_{RS}$.

The entire transmission includes three phases. In the first phase, the HR transmits energy signal to power the multiple users before the information transmission. Then, the remaining time of the information transfer is further divided into two parts, one is that the selected user uploads the confidential data to HR, another is that the HR decodes and forwards it to the destination D, where the HR is served as the trusted relay and the new codewords are adopted to re-encode the information before forwarding for improving the secrecy performance [12], [28]. It is noted that the FD destination always sends the jamming in the whole information transmission process for degrading the channel quality of the eavesdropper. Thus, the division of time slot is shown as Fig. 2, in which T denotes a transfer time slot, αT is the time used for the HR to power all the alternative users, where $\alpha \in (0, 1)$ denotes time-switching factor, $(1-\alpha)T/2$ represents the time used to transmit the information and jamming in the first hop, and the remaining time is used for the information and jamming transfer of the second hop. For convenience, we set $T = 1$.

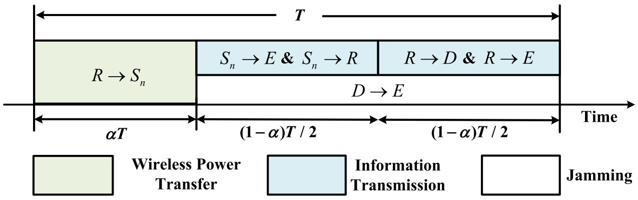


FIGURE 2. Time-switching based scheme.

B. ENERGY HARVESTING AND SIGNAL ANALYSIS

According to the [29], [30], the harvested energy at each S_n in the charging phase is given by

$$E_{S_n} = \eta P_R \alpha T \left|h_{RS_n}\right|^2, \tag{1}$$

where η denotes the energy conversion efficiency factor, which depends on the EH circuits and the rectification process; P_R is the transmit power of the HR when it operates as PB; $\left|h_{RS_n}\right|^2$ is power gains of the links from the HR to S_n. It is worth noting that the nodes in WPCCN are passive users, compared with the energy harvested from HR, the received power from the external noise is very small, which makes the harvested energy from noise can be ignored [28], [30]. Furthermore, it is considered that all the harvested energy at each S_n is used for transmitting data in the next block of information transfer, i.e., the harvest-use (HU) mode is adopted [11]. As such, the transmit power of S_n is given by

$$P_{S_n} = \frac{2E_{S_n}}{(1-\alpha)T} = \frac{2\eta\alpha}{1-\alpha} P_R \left|h_{RS_n}\right|^2. \tag{2}$$

It is noted that, in practice, the energy harvester works in a non-linear mode with a saturation threshold [47], [48]. We note that the harvested energy within a time slot in the considered system is usually much smaller than the saturation threshold in the energy harvester, e.g., the capacitance. Thus, we assume that the non-linear effect of the energy harvester is negligible in our considered system, which is worth studying in future works.

Then, we assume that the optimal user is denoted by S_{n^*}. The received signals at HR and E in the first hop of information transmission are given by

$$y_R = \sqrt{P_{S_{n^*}}} h_{S_{n^*}R} x + n_R, \tag{3}$$

$$y_{E_1} = \sqrt{P_{S_{n^*}}} h_{S_{n^*}E} x + \sqrt{P_D} h_{DE_1} z + n_{E_1}, \tag{4}$$

[1] For a more intuitive analysis, we consider the simple scenario with only two separate antennas at the destination, which can be regarded as the basis of a more complex situation. Therefore, for the improvement of the secrecy performance with low complexity, more efficient antenna selection strategy and beamforming technology are beyond the scope of this paper.

respectively, where x is the confidential information transmitted by S_{n^*}, z denotes the jamming signal transmitted by D. And $P_{S_{n^*}}$ denotes the transmit power of the selected user, P_D denotes the transmit power of the destination. h_{DE_1} denotes the power gain of the channel from the destination to E in the first hop. $n_R \sim CN(0, N_0)$ and $n_{E_1} \sim CN(0, N_0)$ are AWGN at R and E, respectively. It should be noted that in line with [11], [24], [28], the jamming caused by the destination to the HR is neglected in (3). In fact, the HR and the destination are cooperative with each other, which makes the HR can eliminate the interference signal [49]. Thus, the signal-noise-ratio (SNR) at R in the first hop is given by

$$\gamma_R = \frac{P_{S_{n^*}} \left|h_{S_{n^*}R}\right|^2}{N_0}, \tag{5}$$

and the signal-to-interference-plus-noise ratio (SINR) at the eavesdropper E is given by

$$\gamma_{E_1} = \frac{P_{S_{n^*}} \left|h_{S_{n^*}E}\right|^2}{P_D \left|h_{DE_1}\right|^2 + N_0}, \tag{6}$$

where $\left|h_{S_{n^*}R}\right|^2$, $\left|h_{S_{n^*}E}\right|^2$ and $\left|h_{DE_1}\right|^2$ denote the power gains of the channel from S_{n^*} to R, S_{n^*} to E and D to E, respectively. For simplicity, we define $\bar{\gamma}_D = \frac{P_D}{N_0}$.

Then, as [18], the secrecy capacity of the first hop is given by

$$C_{s1} = \frac{1-\alpha}{2}\left(\log_2(1+\gamma_R) - \log_2\left(1+\gamma_{E_1}\right)\right)^+, \tag{7}$$

where $(x)^+ = \max(x, 0)$.

Furthermore, in the next phase of information transmission, the received signals at D and E are given by

$$y_D = \sqrt{P_R} h_{RD} x + n_D, \tag{8}$$
$$y_{E_2} = \sqrt{P_R} h_{RE} x + \sqrt{P_D} h_{DE_2} z + n_{E_2}, \tag{9}$$

respectively, where h_{DE_2} is the power gain of the channel from the destination to E in the second hop, $n_D \sim CN(0, N_0)$ and $n_{E_2} \sim CN(0, N_0)$ are AWGN at D and E, respectively. It should be noted that the self-interference (SI) between the receive antenna and the transmit antenna at the destination is negligible in (8).[2]

Similarly, the SNR at D and SINR at E are given by

$$\gamma_D = \frac{P_R |h_{RD}|^2}{N_0}, \tag{10}$$

$$\gamma_{E_2} = \frac{P_R |h_{RE}|^2}{P_D \left|h_{DE_2}\right|^2 + N_0}, \tag{11}$$

respectively, where $|h_{RD}|^2$, $|h_{RE}|^2$ and $\left|h_{DE_2}\right|^2$ denote the power gains of the links from the R to D, R to E and D to E, respectively. And P_R is the transmit power of HR when it forwards the confidential information. Similarly, for simplicity, we define $\bar{\gamma}_R = \frac{P_R}{N_0}$. It is worth noting that we consider the power of HR in time slot of charging and of forwarding information is set as the same. So we do not focus on the power optimization of HR in different time slots.

Thus, the secrecy capacity of the second hop is given by

$$C_{s2} = \frac{1-\alpha}{2}\left(\log_2(1+\gamma_D) - \log_2\left(1+\gamma_{E_2}\right)\right)^+, \tag{12}$$

C. SECURE MULTIUSER SCHEDULING SCHEME

In this part, we propose two different multiuser scheduling strategies: one is the random user scheduling (RUS), where the alternative user is selected randomly from the cluster of users for reducing computational complexity; another is the best user scheduling (BUS), where the best user can be determined based on the channel quality of $S_n \rightarrow R$ for the improvement of the secrecy performance.

1) THE RUS SCHEME

In line with the RUS scheme, we select the node S_{n^*} among the candidates randomly. Thus, the probability density function (pdf) of $\left|h_{S_{n^*}R}\right|^2$ is subjected to the exponential distribution with parameters $1/\lambda_{SR}$, which is given by

$$f_{\left|h_{S_{n^*}R}\right|^2}(x) = \lambda_{SR} \exp(-\lambda_{SR} x), \tag{13}$$

where $1/\lambda_{SR} = \mathbb{E}\left(\left|h_{S_{n^*}R}\right|^2\right)$.

Furthermore, it is obvious that $\left|h_{RS_{n^*}}\right|^2$, $\left|h_{S_{n^*}E}\right|^2$, $\left|h_{DE_1}\right|^2$, $|h_{RD}|^2$, $|h_{RE}|^2$ and $\left|h_{DE_2}\right|^2$ are subjected to the exponential distribution with parameters $1/\lambda_{RS}$, $1/\lambda_{SE}$, $1/\lambda_{RD}$, $1/\lambda_{RE}$ and $1/\lambda_{DE}$, respectively.

Remark 1: It is noted that depending on the low computational complexity, the RUS scheme is especially suitable for the resource-limited and latency-sensitive scenarios. However, because the user who transmits information is scheduled randomly in RUS scheme, the diversity gain brought by multiple users cannot be acquired, which constricts the secrecy performance of the networks.

2) THE BUS SCHEME

For obtaining the diversity gain, the best user is scheduled based on the main channel quality between S_n and HR. In particular, based on the CSI of the $S_{n^*} \rightarrow R$ links, the selected user S_{n^*} is given by

$$n^* = \arg\max_n \left(\left|h_{S_nR}\right|^2\right), \tag{14}$$

Lemma 1: If X_m, $m \in \{1, 2, \cdots, M\}$, denotes the random variable subjecting to the independent and identical exponential distribution, the pdf and the cumulative distribution function (cdf) of $X = \max(X_m)$ is given by

$$f_X(x) = M\lambda_X \exp(-\lambda_X x)(1 - \exp(-\lambda_X x))^{M-1}, \tag{15}$$
$$F_X(x) = (1 - \exp(-\lambda_X x))^M, \tag{16}$$

[2] It is assumed that the separate-antenna deployment is adopted at the FD destination, i.e., each antenna is used for transmission or reception, respectively [43], [44]. With the help of the latest self-interference cancellation (SIC) technique, such as analog-circuit-domain, propagation-domain, and digital domain methods, SI can be effectively controlled in a negligible range [50], [51].

where x represents the independent random variable, $1/\lambda_X$ denotes the average channel gain.

As a result, based on Lemma 1, we have the pdf of $\left|h_{S_{n^*}R}\right|^2$ in BUS as

$$f_{\left|h_{S_{n^*}R}\right|^2}(x) = N\lambda_{SR}\exp\left(-\lambda_{SR}x\right)\left(1-\exp\left(-\lambda_{SR}x\right)\right)^{N-1}, \tag{17}$$

It is noted that we choose the best user based on the main link, which is independent of the wiretapping link, so the selected user is equivalent to a random one for Eve. Thus, it can be derived that $\left|h_{RS_{n^*}}\right|^2$, $\left|h_{S_{n^*}E}\right|^2$, $\left|h_{DE_1}\right|^2$, $|h_{RD}|^2$, $|h_{RE}|^2$ and $\left|h_{DE_2}\right|^2$ are subjected to the exponential distribution with parameters $1/\lambda_{RS}$, $1/\lambda_{SE}$, $1/\lambda_{RD}$, $1/\lambda_{RE}$ and $1/\lambda_{DE}$, respectively.

Remark 2: It is noted that for ensuring the effectiveness of the BUS strategy, in the uplink information transmission of the system, each alternative user first reports his CSI to the HR, then the HR collects all CSIs to analyze the channel quality of each user comprehensively and selects the best user to transmit confidential information. As per (14) and (17), it can be inferred that the multiuser diversity gain can be acquired for the BUS scheme, which is advantageous for the improvement of system performance. When the selected optimal source transmits confidential information, the networks will achieve a better diversity gain, leading to lower outage probability of the data, which is applicable for future energy-constrained networks.

III. SECRECY PERFORMANCE ANALYSIS

A. HYBRID OUTAGE PROBABILITY

In fact, for the energy-limited future networks, aiming to keep the stable operation of the system, the internal EH nodes need a minimum energy (activation threshold) to activate the EH circuits and to maintain the continuous energy conversion. Otherwise, if the harvested energy of EH nodes is lower than the minimum threshold, the users will always stay in a silent state, resulting in the confidential information cannot be transmitted, i.e., the energy outage occurs [12]. Therefore, in the considered multiuser WPCCN, HOP is adopted as the proper metric commonly, which is closely related to the minimum energy threshold and secure transmission [12], [52]. The HOP, i.e., the outage probability that combining the EOP [53], [54] and SOP, can be given by

$$P_{\text{HOP}}^{(\text{sch})} = P_{\text{EOP}} + \left(1 - P_{\text{EOP}}\right)P_{\text{SOP}}^{(\text{sch})}, \tag{18}$$

where sch $\in$ {RUS, BUS}, $P_{\text{HOP}}^{(\text{sch})}$ denotes the HOP of each scheme. P_{EOP} denotes the EOP of the considered WPCCN, which is identical to each scheme due to the fact that it actually doesn't make any difference in the processes of energy consumption and EH for the wireless powered nodes. Above analysis will be proved in the following section based on the numerical results.

Specifically, when the energy harvested at each user is lower than the inherent activation threshold of the EH circuit, the network only performs energy transfer between the HR and the source users without confidential information transmission, leading to the energy outage [52]–[54]. Note that for ease of analysis, we assume that all the source devices have the same EH module and power conversion circuit, i.e., all the users have the identical activation threshold. As such, EOP is given by

$$\begin{aligned} P_{\text{EOP}} &= \prod_{n=1}^{N} \Pr\left\{P_{S_n} < \Gamma_A\right\} \\ &= \left(\Pr\left(\frac{2\eta\alpha}{1-\alpha}P_R\left|h_{RS_n}\right|^2 < \Gamma_A\right)\right)^N \\ &= \left(F_{\left|h_{RS_n}\right|^2}\left(T_1\right)\right)^N = \left(1 - \exp\left(-T_1\lambda_{RS}\right)\right)^N, \end{aligned} \tag{19}$$

where Γ_A denotes the activation threshold, and $T_1 = \frac{(1-\alpha)\Gamma_A}{2\eta\alpha P_R}$.

Obviously, it can be observed that when the EOP is small, the system will perform the information transmission. At this time, the SOP mainly depends on the relationship between the secrecy capacity of the system and the predetermined transmission rate, which means that the EOP has little impact on the HOP of the network, and the HOP will be restricted by the SOP. On the contrary, when the EOP is large, the harvested energy at the source user is not enough to support the data transmission, and the system will mainly perform the energy transmission, which leads to that the EOP of the system plays a major role in the overall system performance. Therefore, EOP can capture the energy efficiency of the considered WPCCN to a certain extent.

Remark 3: The data transmission will be interrupted if there is no active node in the networks. Thus, when the transmit power of HR is low, the harvested energy at wireless powered users is limited, resulting in the larger EOP, which is equivalent to increase the HOP of the HR-assisted WPCCN. It can be inferred that for maintaining the operation of the network in a long run, it is a very effective way to increase the transmit power of HR, which is helpful to arouse the enthusiasm of EH nodes for information transmission. In addition, it can be observed from (19) that the number of the source users has positive role on the EOP, the latter numerical results will confirm this conclusion.

On the other hand, $P_{\text{SOP}}^{(\text{sch})}$ in (18) denotes the SOP of each scheme, which is generally considered as a vital metric of PLS [28]–[30], [52]. In fact, when secrecy capacity of the system is lower than a predetermined transmission rate threshold R_{th}, the networks incurs secrecy outage. Therefore, $P_{\text{SOP}}^{(\text{sch})}$ is given as

$$P_{\text{SOP}}^{(\text{sch})} = \Pr\left\{C_s^{(\text{sch})} < R_{th}\right\}, \tag{20}$$

where $C_s^{(\text{sch})}$ denotes the secrecy capacity of different schemes. For the DF relay protocol, the selected source node and HR can adopt the different codebooks for improving secrecy performance [55], [56]. In fact, when the selected source user and the HR use different codebooks to transmit the confidential information, the eavesdropper cannot combine the received signal during the two hops, i.e., the maximum ratio combination (MRC) is not available for the eavesdropper. Thus, securing each hop individually is sufficient to prevent the end-to-end transmission from being eavesdropped. To secure the wireless communications, the PLS (i.e., physical-layer security) techniques exploit the physical-layer characteristics of wireless channels [57], which can be supposed as an effective complement to the traditional cryptographic techniques based on the "computationally secure" [58]. Based on the Wyner's wiretap model [59], the PLS techniques can achieve the "information-theoretically secure" if the wiretap channel from a source to an eavesdropper is a degraded version of the main channel from the source to its intended destination. As such, the secrecy of the wireless transmission aided by the PLS techniques is normally measured by the difference between the capacities of the main channel and that of the wiretap channel [60], [61], i.e., secrecy capacity. In the considered system, the secrecy capacity is given by

$$C_s^{((\mathrm{sch}))} = \min\left(C_{s1}^{(\mathrm{sch})}, C_{s2}^{(\mathrm{sch})}\right), \tag{21}$$

in which $C_{s1}^{(\mathrm{sch})}$ and $C_{s2}^{(\mathrm{sch})}$ is the secrecy capacity of first hop and second hop, respectively. It is worth noting that for PLS, the secrecy capacity is the main index used for the performance evaluation of the system, where the "secrecy" is the "secrecy" in the field of PLS actually. Meanwhile, the "secrecy" in the paper can be understood as follows, i.e., the legitimate channel will be heard by the eavesdropped but stays confidential due to the jamming and the multiuser diversity gain.

Then, with the help of (21), $P_{\mathrm{SOP}}^{(\mathrm{sch})}$ in (20) is given by

$$\begin{aligned} P_{\mathrm{SOP}}^{(\mathrm{sch})} &= \Pr\left\{\min\left(C_{s1}^{((\mathrm{sch}))}, C_{s2}^{(\mathrm{sch})}\right) < R_{th}\right\} \\ &= 1 - \Pr\left\{\min\left(C_{s1}^{(\mathrm{sch})}, C_{s2}^{(\mathrm{sch})}\right) > R_{th}\right\} \\ &= 1 - \Pr\left\{C_{s1}^{(\mathrm{sch})} > R_{th}\right\} \Pr\left\{C_{s2}^{(\mathrm{sch})} > R_{th}\right\} \\ &= 1 - \left(1 - P_{\mathrm{SOP1}}^{(\mathrm{sch})}\right)\left(1 - P_{\mathrm{SOP2}}^{(\mathrm{sch})}\right), \end{aligned} \tag{22}$$

where $P_{\mathrm{SOP1}}^{(\mathrm{sch})} = \Pr\left\{C_{s1}^{(\mathrm{sch})} < R_{th}\right\}$ denotes the SOP of the first hop. As per (2), (5), (6) and (7), $P_{\mathrm{SOP1}}^{(\mathrm{sch})}$ is given by

$$\begin{aligned} &P_{\mathrm{SOP1}}^{(\mathrm{sch})} \\ &= \Pr\left\{C_{s1}^{(\mathrm{sch})} < R_{th}\right\} \\ &= \Pr\left\{\frac{1-\alpha}{2}\left[\log_2\left(1+\gamma_R\right) - \log_2\left(1+\gamma_{E_1}\right)\right]^+ < R_{th}\right\} \\ &= \Pr\left\{\left|h_{RS_{n^*}}\right|^2\left|h_{S_{n^*}R}\right|^2 < \frac{\beta\left|h_{RS_{n^*}}\right|^2\left|h_{S_{n^*}E}\right|^2}{\bar{\gamma}_D\left|h_{DE_1}\right|^2+1} + \frac{\xi}{\bar{\gamma}_R}\right\}, \end{aligned} \tag{23}$$

where $\beta = 2^{\frac{2R_{th}}{1-\alpha}}$ and $\xi = \frac{(\beta-1)(1-\alpha)}{2\eta\alpha}$.

Meanwhile, $P_{\mathrm{SOP2}}^{(\mathrm{sch})} = \Pr\left\{C_{s2}^{(\mathrm{sch})} < R_{th}\right\}$ in (22) denotes the SOP of the second hop. With the help of (2) and (10)-(12), $P_{\mathrm{SOP2}}^{(\mathrm{sch})}$ is given by

$$\begin{aligned} &P_{\mathrm{SOP2}}^{(\mathrm{sch})} \\ &= \Pr\left\{C_{s2}^{(\mathrm{sch})} < R_{th}\right\} \\ &= \Pr\left\{\frac{1-\alpha}{2}\left[\log_2\left(1+\gamma_D\right) - \log_2\left(1+\gamma_{E_2}\right)\right]^+ < R_{th}\right\} \\ &= \Pr\left\{\left|h_{RD}\right|^2 < \frac{\beta\left|h_{RE}\right|^2}{\bar{\gamma}_D\left|h_{DE_2}\right|^2+1} + \frac{\beta-1}{\bar{\gamma}_R}\right\}. \end{aligned} \tag{24}$$

1) SOP DERIVATION FOR THE RUS SCHEME

Based on the RUS scheme, the optimal source user is selected randomly in order to cut down the costs and complexity of considered networks, which means that each user can be scheduled for information transmission with the same probability. Thus, the exact SOP of the RUS scheme is given by

$$\begin{aligned} P_{\mathrm{SOP}}^{(\mathrm{RUS})} &= 1 - 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}\xi}{\bar{\gamma}_R}} K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi}{\bar{\gamma}_R}}\right) \\ &\quad\times \exp\left(-\frac{\lambda_{RD}\left(\beta-1\right)}{\bar{\gamma}_R}\right) \\ &\quad\times \left(1 - \frac{\lambda_{SR}\lambda_{DE}}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\Psi\left\{\alpha,\gamma;z_1\right\}\right) \\ &\quad\times \left(1 - \frac{\lambda_{RD}\lambda_{DE}}{\tilde{\lambda}_{RE}\bar{\gamma}_D}\Psi\left\{\alpha,\gamma;z_2\right\}\right), \end{aligned} \tag{25}$$

where $\tilde{\lambda}_{SE} = \frac{\lambda_{SE}}{\beta}$ and $\tilde{\lambda}_{RE} = \frac{\lambda_{RE}}{\beta}$, $K_1\left(\cdot\right)$ is the modified Bessel function of the second kind and $\Psi\left\{\alpha,\gamma;z\right\}$ denotes the confluent hypergeometric function of the second kind [62], in which $\alpha = 1$ and $\gamma = 1$, $z_1 = \frac{\lambda_{DE}\left(\tilde{\lambda}_{SE}+\lambda_{SR}\right)}{\tilde{\lambda}_{SE}\bar{\gamma}_D}$ and $z_2 = \frac{\lambda_{DE}\left(\tilde{\lambda}_{RE}+\lambda_{RD}\right)}{\tilde{\lambda}_{RE}\bar{\gamma}_D}$, respectively.

Proof: Appendix A shows the proof. ■

2) SOP DERIVATION FOR THE BUS SCHEME

On the other hand, for the achievement of the diversity gain, the optimal user is scheduled based on the main channel quality between S_n and HR in the BUS scheme. As for the BUS scheme, the corresponding SOP is given by

$$\begin{aligned} P_{\mathrm{SOP}}^{(\mathrm{BUS})} &= 1 - \sum_{l=1}^{N}\binom{N}{l}\left(-1\right)^{l+1} 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}\xi l}{\bar{\gamma}_R}} \\ &\quad\times K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi l}{\bar{\gamma}_R}}\right)\exp\left(-\frac{\lambda_{RD}\left(\beta-1\right)}{\bar{\gamma}_R}\right) \\ &\quad\times \left(1 - \frac{\lambda_{SR}\lambda_{DE} l}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\Psi\left\{\alpha,\gamma;z_3\right\}\right) \\ &\quad\times \left(1 - \frac{\lambda_{RD}\lambda_{DE}}{\tilde{\lambda}_{RE}\bar{\gamma}_D}\Psi\left\{\alpha,\gamma;z_2\right\}\right), \end{aligned} \tag{26}$$

where $z_3 = \frac{\lambda_{DE}\left(\tilde{\lambda}_{SE}+\lambda_{SR} l\right)}{\tilde{\lambda}_{SE}\bar{\gamma}_D}$.

Proof: See Appendix B. ■

Finally, as per (18), with the help of (19), (25) and (26), the HOP of the HR-assisted WPCCN with FD-DBJ for each scheme can be derived.

Remark 4: It can be observed that the HOP of each scheme is related to N, Γ_A, $\bar{\gamma}_R$, and $\bar{\gamma}_D$. Therefore, we consider the overall performance as a function of the network parameters, including the number of users, the transmit power both of HR and FD-destination, the time-switching factor, the predetermined transmission rate and so on, which will afford some references for the engineering design.

B. SECRECY THROUGHPUT

Generally, when the secure transmission can be provided, the effectiveness of the data transmission is also an important evaluation metric to gain more insights. For the secrecy performance analysis, the ST, which can be defined as the average transmission rate of confidentiality achieving secure and reliable communication between the source users and the desired destination, is often used to measure the secure effectiveness of the considered networks [46]. Mathematically, the ST of above discussed schemes is given by

$$T_s^{(\mathrm{sch})}\left(R_{th}\right) = \left(1 - P_{\mathrm{HOP}}^{(\mathrm{sch})}\left(R_{th}\right)\right) R_{th}, \tag{27}$$

where $T_s^{(\mathrm{sch})}\left(R_{th}\right)$ denotes the ST of each secure scheme, $\left(1 - P_{\mathrm{HOP}}^{(\mathrm{sch})}\left(R_{th}\right)\right)$ represents the probability of the confidential information can be transmitted reliably and safely.

Remark 5: It is noted that from (27), we find that the smaller R_{th} has negative impact on the ST, i.e., if the R_{th} is set too small, the ST will be small. On the other hand, the larger R_{th} will lead to the $P_{\mathrm{SOP}}^{(\mathrm{sch})}$ close to 1, which brings out the larger $P_{\mathrm{HOP}}^{(\mathrm{sch})}$ as well as the smaller ST. Thus, there exists a optimal predetermined transmission rate denoted as R_{th}^{opt} to obtain the optimal ST denoted as T_s^{opt}. Specifically, the predetermined transmission rate optimization problem is given by

$$(\mathbf{P1}): \max_{R_{th}} \; T_s^{(\mathrm{sch})}, \tag{28}$$

It is worth noting that the expression in (28) has important guiding significance for engineering application, so it can play more practical role in the future energy-limited communication scenarios.

C. THE OPTIMIZATION OF PREDETERMINED TRANSMISSION RATE

In fact, the explicit expression for R_{th}^{opt} is hard to acquire. In order to solve the optimization problem (28) in low complexity, we adopt the Brent method, which is a globally optimization method for the optimization problem with a unimodal objective function [63]. Indeed, the Brent method is a root-finding algorithm method without the derivative, which combines the methods of the golden section and the inverse parabolic interpolation. Specifically, the Brent method gives the priority to the inverse parabolic interpolation, and resorts to the golden section search when the inverse parabolic interpolation is invalid [64]. It is noted that the objective function of the secrecy maximization problem is a unimodal function, which will be shown in the numerical results. Thus, the Brent method can globally solve the secrecy throughput maximization problem.

Algorithm 1 Secrecy Throughput Maximization Algorithm

```
Input: $\gamma_R, \gamma_E, \gamma_D, \eta, N, \Gamma_{th}, \alpha$, and tolerances $\delta_0, \delta_1, \delta_2$.
Output: $R_{th}^{\mathrm{opt}}$, and $T_s^{\mathrm{opt}}$
Initialize: $k = 1$, $T_{s,0}^{(\mathrm{sch})} = 0$ and $T_{s,1}^{(\mathrm{sch})} = 1$
while $T_{s,\,k}^{(\mathrm{sch})} - T_{s,\,k-1}^{(\mathrm{sch})} \geq \delta_0$ do
    Initialize: $i = 0$, $\lambda_0 = 0$
    Initialize: $i = 1$, $\upsilon_0 = (R_{th,1}, R_{th,3}, R_{th,2})$
    while: $|F(\lambda_i)| \geq \delta_2$ do
        if inverse parabolic interpolation is feasible;
            Update $R_{th,4}$ by inverse parabolic interpolation;
        else
            Update $R_{th,4}$ by golden section search;
        if $T_s^{(\mathrm{sch})}\left(R_{th,4}\right) > T_s^{(\mathrm{sch})}\left(R_{th,3}\right)$
            $R_{th,1} = R_{th,3}$;
            $R_{th,3} = R_{th,4}$;
        else
            $R_{th,2} = R_{th,4}$;
        Update the triplet $\upsilon_i$ by the new $(R_{th,1}, R_{th,3}, R_{th,2})$
        $i++$;
    end
    $R_{th,\,k}^{\mathrm{opt}} = R_{th,4}$;
    $k++$;
    Update $T_{s,\,k}^{(sch)}$ by $R_{th,\,k}^{\mathrm{opt}}$;
end
return$R_{th}^{\mathrm{opt}} = R_{th,\,k}^{\mathrm{opt}}$, and $T_s^{\mathrm{opt}} = T_{s,\,k}^{(\mathrm{sch})}$;
```

Then, we give a brief description of Brent method in the optimization R_{th} when fixing α as shown in Algorithm 1. Firstly, we choose an initial triple $\upsilon_0 = (R_{th,1}, R_{th,3}, R_{th,2})$, where $R_{th,1} < R_{th,3} < R_{th,2}$ within initial interval $R_{th} \in (0, 2.5)$. Then, we fit υ_0 by a parabola, where the maximum point $R_{th,4}$ is given by

$$\begin{aligned} R_{th,4} = R_{th,2} - \frac{1}{2}\Big\{&(R_{th,2} - R_{th,1})^2[f(R_{th,2}) - f(R_{th,3})] \\ &-(R_{th,2} - R_{th,3})^2[f(R_{th,2}) - f(R_{th,1})]\Big\} \\ &\div \big\{(R_{th,2} - R_{th,1})[f(R_{th,2}) - f(R_{th,3})] \\ &- (R_{th,2} - R_{th,3})[f(R_{th,2}) - f(R_{th,1})]\big\}. \end{aligned} \tag{29}$$

If the fitting is invalid or $R_{th,4}$ is located outside of the interval between $R_{th,1}$ and $R_{th,2}$, $R_{th,4}$ will be obtained by gold section search. Afterwards, compare the $T_s^{(\mathrm{sch})}(R_{th,4})$ and $T_s^{(\mathrm{sch})}(R_{th,3})$. If $T_s^{(\mathrm{sch})}(R_{th,4})$ is larger, the triplet will be updated as $\upsilon_1 = (R_{th,3}, R_{th,4}, R_{th,2})$, otherwise, $\upsilon_1 = (R_{th,1}, R_{th,3}, R_{th,4})$. Finally, at each iteration, the interval of the triple becomes smaller, until the interval is smaller than the predefined tolerance.

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, we present numerical results to evaluate the secrecy performance of the HR-assisted WPCCN with FD-DBJ in this section. As [29], we adopt a simulation environment of linear topology, where the destination, the HR, and the multiple source users in a localized group are placed in horizontal way. Unless stated otherwise, we set the activation threshold as $\Gamma_{th} = \Gamma_A/N_0 = 2$ dB, the predetermined transmission rate as $R_{th} = 0.1$ bit/s/Hz, the number of the users as $N = 4$, the time-switching factor as $\alpha = 0.5$, and the energy conversion efficiency as $\eta = 0.8$, $\gamma_R = P_R/N_0 = 30$ dB, $\gamma_D = P_D/N_0 = 20$ dB, $\lambda_{SR} = \lambda_{RS} = \lambda_{RD} = 5$, $\lambda_{SE} = \lambda_{RE} = 10$ and $\lambda_{DE} = 1$. By comparison, we denote the optimal multiuser selection strategy (i.e., $n^* = \arg\max_n (C_{s1}(n))$) as the benchmark scheme.

In Fig.3, we plot $P_{\text{HOP}}^{(\text{sch})}$ versus γ_R with different numbers of users N. At first, we observe that N plays a positive role on the performance of the system. Then, we observe that the BUS scheme can acquire much better secrecy performance than the RUS scheme. In contrast, we observe that the secrecy performance of the proposed BUS scheme is slightly worse than that of the benchmark scheme. However, it is noted that the benchmark scheme is hard to achieve in practice due to the fact that the source users and the HR are difficult to acquire the CSI relative to the eavesdropper. Thus, the proposed BUS scheme is still an efficient way to achieve the secure transmission. Meanwhile, we can further observe that for BUS scheme, the secrecy performance improves as N increases. In contrast, the value of N has no effect on the RUS scheme. It is because that the RUS scheme randomly selects the source from multiple users for information transmission, which means that the number of sources and the selection scheme are independent of each other.

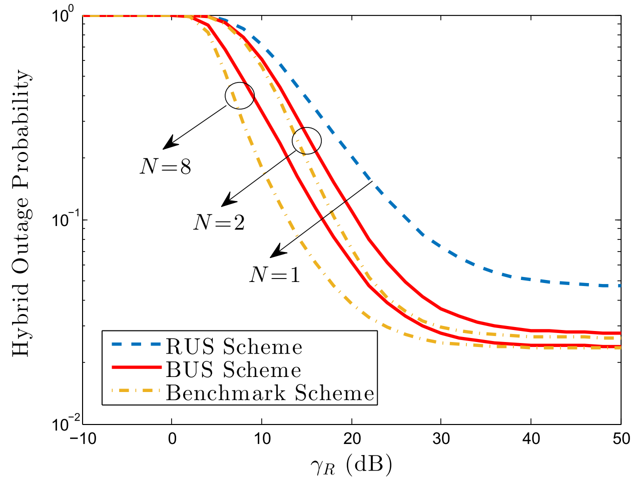


FIGURE 3. HOP versus the transmit SNR at HR with $N = \{1, 2, 8\}$.

In Fig. 4, we plot $P_{\text{HOP}}^{(\text{sch})}$ versus γ_R with different energy conversion efficiency factors η. It is illustrated in Fig. 4 that for a given N, η plays a positive role on the secrecy performance. This is due to the fact that the energy conversion efficiency of the considered WPCCN is dependent on the η. On the one hand, the increase of energy conversion efficiency enables more source users to exceed the energy threshold, which activates more users to participate in information transmission. On the other hand, larger η can ensure that the source nodes harvest more energy, which decreases the energy outage probability, i.e., $P_{\text{EOP}}^{(\text{sch})}$, resulting in the decrease of $P_{\text{HOP}}^{(\text{sch})}$. Moreover, we can also observe that the BUS scheme can achieve better secrecy performance than the RUS scheme, which demonstrates the validity of the BUS scheme again.

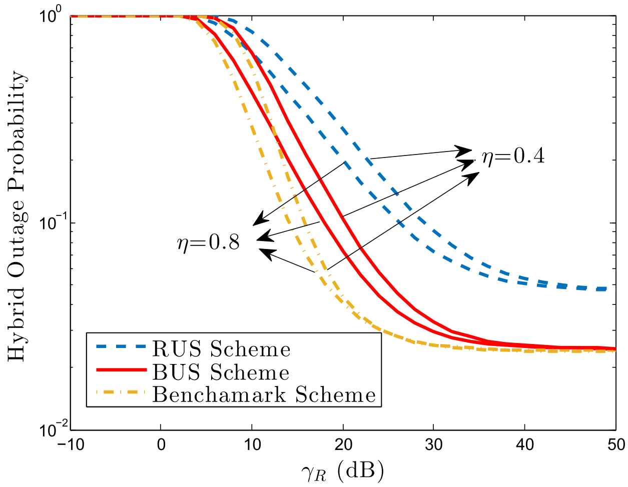


FIGURE 4. HOP versus the transmit SNR at HR with $\eta = \{0.4, 0.8\}$.

In Fig. 5, we plot the $P_{\text{HOP}}^{(\text{sch})}$ versus γ_R with/without the DBJ (i.e., destination-based jamming). At first, we observe that the secrecy performance without the DBJ is considerable terrible, which is almost unacceptable for secure transmission in the considered system. In contrast, we find that $P_{\text{HOP}}^{(\text{sch})}$ in the case with the DBJ is relatively small, which illustrates the positive impact of the DBJ on the secrecy performance. Actually, the introduction of the DBJ can confuse malicious

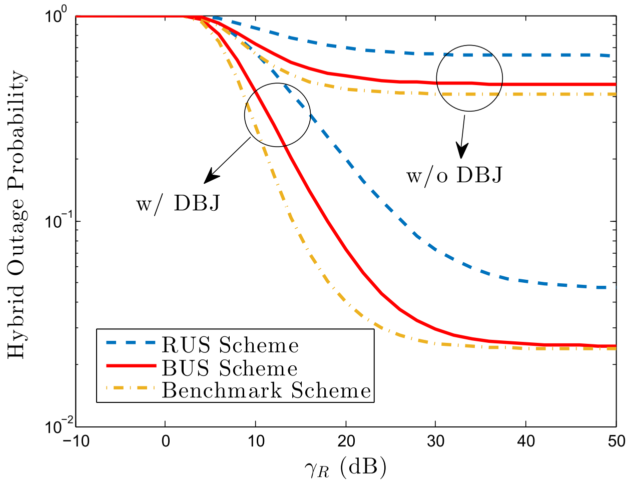


FIGURE 5. The impact of the DBJ (i.e., destination-based jamming) on HOP.

eavesdroppers effectively. In other words, stronger DBJ enables the channel quality of the eavesdropper to a lower level. It is worth mentioning that there exist feedback links between the HR and the destination, and hence the DBJ can be eliminated at the HR and the destination by the interference cancellation techniques. Thus, the introduction of the DBJ is conductive to improve the secrecy performance of the considered system.

In Fig.6, we plot $T_s^{(\text{sch})}$ versus α. We first observe that the function of $T_s^{(\text{sch})}$ with respect to α is an unimodal function. It can be explained by the fact that the source users cannot harvest sufficient energy to maintain their function when α is too small. In contrast, when α is exceedingly large, the transmission time is very short leading to large HOP, which causes the small value of the ST. Furthermore, we plot $T_s^{(\text{sch})}$ versus R_{th} in Fig.7. Similarly, we also find that the function of $T_s^{(\text{sch})}$ with respect to R_{th} is also an unimodal function, which proves that there exists a optimal predetermined transmission rate R_{th}^{opt} to maximum ST. It is consistent with the deduction in Remark 5.

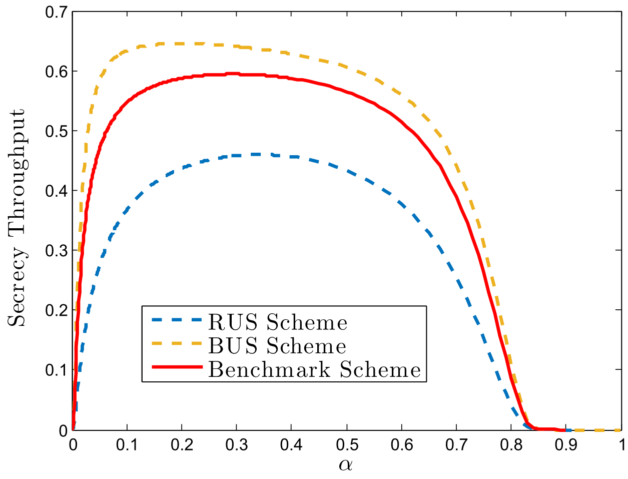


FIGURE 6. ST versus the time-switching factor.

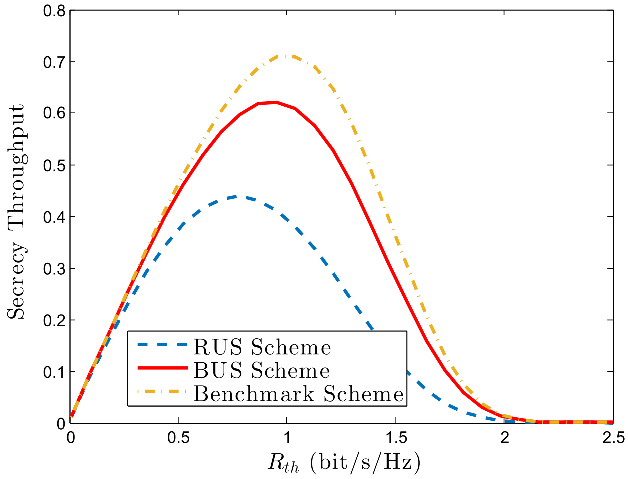


FIGURE 7. ST versus the predetermined transmission rate.

V. CONCLUSION

In this paper, we explore the PLS of a HR-assisted multiuser WPCCN with FD-DBJ. In particular, two secure multiuser scheduling strategies are proposed for the improvement of the secrecy performance. The analytical closed-form expressions of EOP, SOP and HOP are derived for each scheme, and the maximization problem of ST is solved with help of the Brent method. For getting a deeper insight, the influence of key parameters on secrecy performance of the system is further discussed. Simulation results are provided to validate the correctness of our analysis.

APPENDIX A

Firstly, as per (22), $P_{\text{SOP}}^{(\text{RUS})}$ is given by

$$P_{\text{SOP}}^{(\text{RUS})} = 1 - \bar{P}_{\text{SOP1}}^{(\text{RUS})} \bar{P}_{\text{SOP2}}^{(\text{RUS})}, \tag{30}$$

where $\bar{P}_{\text{SOP1}}^{(\text{RUS})} = 1 - P_{\text{SOP1}}^{(\text{RUS})}$ and $\bar{P}_{\text{SOP2}}^{((\text{RUS}))} = 1 - P_{\text{SOP2}}^{(\text{RUS})}$, respectively.

Then, with the help of (23), we have

$$\begin{aligned}\bar{P}_{\text{SOP1}}^{(\text{RUS})} &= \Pr\left\{\left|h_{RS_{n*}}\right|^2 \left|h_{S_{n*}R}\right|^2 > \frac{\beta \left|h_{RS_{n*}}\right|^2 \left|h_{S_{n*}E}\right|^2}{\bar{\gamma}_D \left|h_{DE_{m1}}\right|^2 + 1} + \frac{\xi}{\bar{\gamma}_R}\right\} \\ &= \Pr\left\{\left|h_{S_{n*}R}\right|^2 > \frac{\beta \left|h_{S_{n*}E}\right|^2}{\bar{\gamma}_D \left|h_{DE_1}\right|^2 + 1} + \frac{\xi}{\bar{\gamma}_R \left|h_{RS_{n*}}\right|^2}\right\} \\ &= \int_0^{+\infty} P_1 \cdot f_{\left|h_{DE_1}\right|^2}(y)\, dy, \end{aligned} \tag{31}$$

where $P_1 = \Pr\left\{\left|h_{S_{n*}R}\right|^2 > \frac{\beta \left|h_{S_{n*}E}\right|^2}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R \left|h_{RS_{n*}}\right|^2}\right\}$.

Furthermore, P_1 can be shown as:

$$P_1 = \int_0^{+\infty} P_2 \cdot f_{\left|h_{S_{n*}E}\right|^2}(x)\, dx, \tag{32}$$

where $P_2 = \Pr\left\{\left|h_{S_{n*}R}\right|^2 > \frac{\beta x}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R \left|h_{RS_{n*}}\right|^2}\right\}$.

Then, P_2 is given by

$$P_2 = \int_0^{+\infty} f_{\left|h_{RS_{n*}}\right|^2}(z) \underbrace{\int_{\frac{\beta x}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R z}}^{+\infty} f_{\left|h_{S_{n*}R}\right|^2}(v)\, dv}_{P_3}\, dz, \tag{33}$$

where P_3 is given by

$$\begin{aligned} P_3 &= \int_{\frac{\beta x}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R z}}^{+\infty} f_{\left|h_{S_{n*}R}\right|^2}(v)\, dv \\ &= \exp\left\{-\lambda_{SR}\left(\frac{\beta x}{\bar{\gamma}_D y + 1} + \frac{\xi}{\bar{\gamma}_R z}\right)\right\}, \end{aligned} \tag{34}$$

It is noted that in line with (13), we have

$$f_{\left|h_{S_{n*}R}\right|^2}(v) = \lambda_{SR} e^{-\lambda_{SR} v}. \tag{35}$$

The reason is that for the RUS scheme, the optimal source user is selected randomly, which means that the RUS scheme have no diversity gain.

Therefore, by inserting (34) into (33), P_2 is given by

$$\begin{aligned}P_2 &= \int_0^{+\infty} \lambda_{RS} \exp\left\{-\left(\frac{\lambda_{SR}\xi}{\bar{\gamma}_R z} + \lambda_{RS} z + \frac{\lambda_{SR}\beta x}{\bar{\gamma}_D y + 1}\right)\right\} dz \\ &= 2\lambda_{RS}\sqrt{\frac{\lambda_{SR}\xi}{\lambda_{RS}\bar{\gamma}_R}} K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi}{\bar{\gamma}_R}}\right) \exp\left(-\frac{\lambda_{SR}\beta x}{\bar{\gamma}_D y + 1}\right),\end{aligned} \tag{36}$$

where $K_1(\cdot)$ denotes the modified Bessel function of the second kind [62].

By inserting (36) into (32), P_1 is given by

$$\begin{aligned}P_1 &= \int_0^{+\infty} \lambda_{RS}\lambda_{SE} \exp\left(-\frac{\lambda_{SR}\beta x}{\bar{\gamma}_D y + 1} - \lambda_{SE} x\right) dx \\ &\quad \times 2\sqrt{\frac{\lambda_{SR}\xi}{\lambda_{RS}\bar{\gamma}_R}} K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi}{\bar{\gamma}_R}}\right) \\ &= \frac{\lambda_{SE}\lambda_{RS}\left(\bar{\gamma}_D y + 1\right)}{\lambda_{SR}\beta + \lambda_{SE}\left(\bar{\gamma}_D y + 1\right)} 2\sqrt{\frac{\lambda_{SR}\xi}{\lambda_{RS}\bar{\gamma}_R}} K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi}{\bar{\gamma}_R}}\right).\end{aligned} \tag{37}$$

By substituting $y = \frac{\left(\tilde{\lambda}_{SE} + \lambda_{SR}\right)t}{\bar{\gamma}_D \tilde{\lambda}_{SE}}$ into (37), utilizing [62, Eq. (9.211.4)], i.e., $\int_0^{+\infty} \exp\{-zt\}\, t^{\alpha-1}(1+t)^{\gamma-\alpha-1} dt = \Psi(\alpha, \gamma; z) \cdot \Gamma(\alpha)$, in which $\alpha = 1$, $\gamma = 1$ and $z = \frac{\lambda_{DE}\left(\tilde{\lambda}_{SE} + \lambda_{SR}\right)}{\tilde{\lambda}_{SE}\bar{\gamma}_D}$, and performing some mathematical manipulations, $\bar{P}_{\text{SOP1}}^{(\text{RUS})}$ in (31) is given by

$$\begin{aligned}\bar{P}_{\text{SOP1}}^{(\text{RUS})} &= 2\lambda_{RS}\left(1 - \frac{\lambda_{SR}\lambda_{DE}}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\right)\sqrt{\frac{\lambda_{SR}\xi}{\lambda_{RS}\bar{\gamma}_R}} K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi}{\bar{\gamma}_R}}\right) \\ &\quad \times \int_0^{+\infty} \frac{1}{1+t} \exp\left\{-\frac{t\lambda_{DE}\left(\tilde{\lambda}_{SE} + \lambda_{SR}\right)}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\right\} dt \\ &= 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}\xi}{\bar{\gamma}_R}}\left(1 - \frac{\lambda_{SR}\lambda_{DE}}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\right) \\ &\quad \times K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}\xi}{\bar{\gamma}_R}}\right) \\ &\quad \times \Psi\left\{1, 1; \frac{\lambda_{DE}\left(\tilde{\lambda}_{SE} + \lambda_{SR}\right)}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\right\}.\end{aligned} \tag{38}$$

On the other hand, as per (24), we have

$$\begin{aligned}\bar{P}_{\text{SOP2}}^{(\text{RUS})} &= \Pr\left\{|h_{RD}|^2 > \frac{\beta|h_{RE}|^2}{\bar{\gamma}_D\left|h_{DE_2}\right|^2 + 1} + \frac{\beta - 1}{\bar{\gamma}_R}\right\} \\ &= \int_0^{+\infty} P_a \cdot f_{\left|h_{DE_2}\right|^2}(y)\, dy,\end{aligned} \tag{39}$$

where $P_a = \Pr\left\{|h_{RD}|^2 > \frac{\beta|h_{RE}|^2}{\bar{\gamma}_D y + 1} + \frac{\beta-1}{\bar{\gamma}_R}\right\}$.

Then, P_a is given by

$$\begin{aligned}P_a &= \int_0^{+\infty} \Pr\left\{|h_{RD}|^2 > \frac{\beta x}{\bar{\gamma}_D y + 1} + \frac{\beta - 1}{\bar{\gamma}_R}\right\} f_{|h_{RE}|^2}(x)\, dx \\ &= \int_0^{+\infty} f_{|h_{RE}|^2}(x) \int_{\frac{\beta x}{\bar{\gamma}_D y+1} + \frac{\beta-1}{\bar{\gamma}_R}}^{+\infty} f_{|h_{RD}|^2}(v)\, dv dx \\ &= \int_0^{+\infty} \lambda_{RE} \exp\left\{-\left(\lambda_{RE} + \frac{\beta\lambda_{RD}}{\bar{\gamma}_D y + 1}\right) x - \frac{\lambda_{RD}(\beta - 1)}{\bar{\gamma}_R}\right\} dx \\ &= \left(1 - \frac{\lambda_{RD}}{\lambda_{RD} + \tilde{\lambda}_{RE}\bar{\gamma}_D y + \tilde{\lambda}_{RE}}\right) \exp\left(-\frac{\lambda_{RD}(\beta - 1)}{\bar{\gamma}_R}\right).\end{aligned} \tag{40}$$

Similarly, by inserting (40) into (39), with the help of $y = \frac{\tilde{\lambda}_{RE} + \lambda_{RD}}{\tilde{\lambda}_{RE}\bar{\gamma}_D} t$ and [62, Eq. (9.211.4)], $\bar{P}_{\text{SOP2}}^{(\text{RUS})}$ is given by

$$\begin{aligned}\bar{P}_{\text{SOP2}}^{(\text{RUS})} &= \left(1 - \frac{\lambda_{RD}\lambda_{DE}}{\tilde{\lambda}_{RE}\bar{\gamma}_D}\right) \Psi\left\{1, 1; \frac{\lambda_{DE}\left(\tilde{\lambda}_{RE} + \lambda_{RD}\right)}{\tilde{\lambda}_{RE}\bar{\gamma}_D}\right\} \\ &\quad \times \exp\left(-\frac{\lambda_{RD}(\beta - 1)}{\bar{\gamma}_R}\right).\end{aligned} \tag{41}$$

Finally, by substituting (38) and (41) into (30) and performing some mathematical manipulations, $P_{\text{SOP}}^{(\text{RUS})}$ in (25) can be derived.

APPENDIX B

Following the same line of derivation used for obtaining $P_{\text{SOP}}^{(\text{RUS})}$, similar with (30), $P_{\text{SOP}}^{(\text{BUS})}$ is given by

$$P_{\text{SOP}}^{(\text{BUS})} = 1 - \bar{P}_{\text{SOP1}}^{(\text{BUS})}\bar{P}_{\text{SOP2}}^{(\text{BUS})}, \tag{42}$$

where $\bar{P}_{SOP1}^{(\text{BUS})} = 1 - P_{\text{SOP1}}^{(\text{BUS})}$ and $\bar{P}_{\text{SOP2}}^{(\text{BUS})} = 1 - P_{\text{SOP2}}^{(\text{BUS})}$, respectively.

Meanwhile, with the help of (23), we have

$$\begin{aligned}\bar{P}_{\text{SOP1}}^{(\text{BUS})} &= \Pr\left\{\left|h_{RS_{n^*}}\right|^2\left|h_{S_{n^*}R}\right|^2 > \frac{\beta\left|h_{RS_{n^*}}\right|^2\left|h_{S_{n^*}E}\right|^2}{\bar{\gamma}_D\left|h_{DE_1}\right|^2 + 1} + \frac{\xi}{\bar{\gamma}_R}\right\} \\ &= \Pr\left\{\left|h_{S_{n^*}R}\right|^2 > \frac{\beta\left|h_{S_{n^*}E}\right|^2}{\bar{\gamma}_D\left|h_{DE_1}\right|^2 + 1} + \frac{\xi}{\bar{\gamma}_R\left|h_{RS_{n^*}}\right|^2}\right\} \\ &= \int_0^{+\infty} P_4 \cdot f_{\left|h_{DE_1}\right|^2}(y)\, dy,\end{aligned} \tag{43}$$

where $P_4 = \Pr\left\{\left|h_{S_{n^*}R}\right|^2 > \frac{\beta\left|h_{S_{n^*}E}\right|^2}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R\left|h_{RS_{n^*}}\right|^2}\right\}$.

Furthermore, P_4 is given by

$$P_4 = \int_0^{+\infty} P_5 \cdot f_{\left|h_{S_{n^*}E}\right|^2}(x)\, dx, \tag{44}$$

where $P_5 = \Pr\left\{\left|h_{S_{n^*}R}\right|^2 > \frac{\beta x}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R\left|h_{RS_{n^*}}\right|^2}\right\}$.

Then, P_5 is given by

$$P_5 = \int_0^{+\infty} f_{\left|h_{RS_{n^*}}\right|^2}(z) \underbrace{\int_{\frac{\beta x}{\bar{\gamma}_D y+1} + \frac{\xi}{\bar{\gamma}_R z}}^{+\infty} f_{\left|h_{S_{n^*}R}\right|^2}(v)\, dv}_{P_6} dz. \tag{45}$$

where P_6 can be calculated as

$$\begin{aligned}P_6 &= \int_{\frac{\beta x}{\bar{\gamma}_D y+1}+\frac{\xi}{\bar{\gamma}_R z}}^{+\infty} f_{\left|h_{S_{n^*}R}\right|^2}(v)\,dv \\ &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\lambda_{SR}l\int_{\frac{\beta x}{\bar{\gamma}_D y+1}+\frac{\xi}{\bar{\gamma}_R z}}^{+\infty}\exp\left(-\lambda_{SR}lv\right)dv \\ &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\exp\left\{-\lambda_{SR}l\left(\frac{\beta x}{\bar{\gamma}_D y+1}+\frac{\xi}{\bar{\gamma}_R z}\right)\right\}.\end{aligned} \tag{46}$$

As per (17), we have

$$f_{\left|h_{S_{n^*}R}\right|^2}(v) = \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\lambda_{SR}le^{-\lambda_{SR}lv}. \tag{47}$$

It is due to the fact that for the BUS scheme, the best user is scheduled on the main channel quality between S_n and HR, which means that the BUS can obtain the diversity gain, resulting in the improving of the secrecy performance.

By inserting (46) into (45), P_5 is given by

$$\begin{aligned}P_5 &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1} \\ &\quad\times\int_0^{+\infty}\lambda_{RS}\exp\left\{-\left(\lambda_{RS}z+\frac{\lambda_{SR}l\xi}{\bar{\gamma}_R z}+\frac{\lambda_{SR}l\beta x}{\bar{\gamma}_D y+1}\right)\right\}dz \\ &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\lambda_{RS}\exp\left(-\frac{\lambda_{SR}l\beta x}{\bar{\gamma}_D y+1}\right) \\ &\quad\times\int_0^{+\infty}\exp\left\{-\frac{4\lambda_{SR}l\xi}{4z\bar{\gamma}_R}-\lambda_{RS}z\right\}dz \\ &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\exp\left(-\frac{\lambda_{SR}l\beta x}{\bar{\gamma}_D y+1}\right) \\ &\quad\times 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}l\xi}{\bar{\gamma}_R}}K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}l\xi}{\bar{\gamma}_R}}\right).\end{aligned} \tag{48}$$

By inserting (48) into (44), P_4 is given by

$$\begin{aligned}P_4 &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\lambda_{SE} \\ &\quad\times 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}l\xi}{\bar{\gamma}_R}}K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}l\xi}{\bar{\gamma}_R}}\right) \\ &\quad\times\int_0^{+\infty}\exp\left\{-\left[\frac{\lambda_{SR}l\beta}{\bar{\gamma}_D y+1}+\lambda_{SE}\right]x\right\}dx \\ &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\left(1-\frac{\lambda_{SR}l}{\lambda_{SR}l+\tilde{\lambda}_{SE}\left(\bar{\gamma}_D y+1\right)}\right) \\ &\quad\times 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}l\xi}{\bar{\gamma}_R}}K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}l\xi}{\bar{\gamma}_R}}\right).\end{aligned} \tag{49}$$

Similarly, with the help of $y = \frac{\tilde{\lambda}_{SE}+\lambda_{SR}l}{\tilde{\lambda}_{SE}\bar{\gamma}_D}t$ and [62, Eq. (9.211.4)], by substituting (49) into (43), $\bar{P}_{\text{SOP1}}^{(\text{BUS})}$ is given by

$$\begin{aligned}\bar{P}_{\text{SOP1}}^{(\text{BUS})} &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}2\sqrt{\frac{\lambda_{RS}\lambda_{SR}l\xi}{\bar{\gamma}_R}} \\ &\quad\times\left(1-\frac{\lambda_{SR}l\lambda_{DE}}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\right)K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}l\xi}{\bar{\gamma}_R}}\right) \\ &\quad\times\Psi\left\{1,1;\frac{\lambda_{DE}\left[\tilde{\lambda}_{SE}+\lambda_{SR}l\right]}{\tilde{\lambda}_{SE}\bar{\gamma}_D}\right\}.\end{aligned} \tag{50}$$

On the other hand, as per (24), $\bar{P}_{\text{SOP2}}^{(\text{BUS})}$ is given by

$$\bar{P}_{\text{SOP2}}^{(\text{BUS})} = \int_0^{+\infty}P_b\cdot f_{\left|h_{DE_2}\right|^2}(y)\,dy, \tag{51}$$

where $P_b = \Pr\left\{|h_{RD}|^2 > \frac{\beta|h_{RE}|^2}{\bar{\gamma}_D y+1}+\frac{\beta-1}{\bar{\gamma}_R}\right\}$.

Then, P_b is given by

$$\begin{aligned}P_b &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\lambda_{SE} \\ &\quad\times 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}l\xi}{\bar{\gamma}_R}}K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}l\xi}{\bar{\gamma}_R}}\right) \\ &\quad\times\int_0^{+\infty}\exp\left\{-\left[\frac{\lambda_{SR}l\beta}{\bar{\gamma}_D y+1}+\lambda_{SE}\right]x\right\}dx \\ &= \sum_{l=1}^{N}\binom{N}{l}(-1)^{l+1}\left(1-\frac{\lambda_{SR}l}{\lambda_{SR}l+\tilde{\lambda}_{SE}\left(\bar{\gamma}_D y+1\right)}\right) \\ &\quad\times 2\sqrt{\frac{\lambda_{RS}\lambda_{SR}l\xi}{\bar{\gamma}_R}}K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RS}l\xi}{\bar{\gamma}_R}}\right).\end{aligned} \tag{52}$$

Similarly, by inserting (52) into (51), with the help of $y = \frac{\tilde{\lambda}_{RE}+\lambda_{RD}}{\tilde{\lambda}_{RE}\bar{\gamma}_D}t$ and [62, Eq. (9.211.4)], $\bar{P}_{\text{SOP2}}^{(\text{BUS})}$ is given by

$$\begin{aligned}\bar{P}_{\text{SOP2}}^{(\text{BUS})} &= \left(1-\frac{\lambda_{RD}\lambda_{DE}}{\tilde{\lambda}_{RE}\bar{\gamma}_D}\right)\Psi\left\{1,1;\frac{\lambda_{DE}\left(\tilde{\lambda}_{RE}+\lambda_{RD}\right)}{\tilde{\lambda}_{RE}\bar{\gamma}_D}\right\} \\ &\quad\times\exp\left(-\frac{\lambda_{RD}\left(\beta-1\right)}{\bar{\gamma}_R}\right).\end{aligned} \tag{53}$$

Finally, by substituting (50) and (53) into (42) and performing some mathematical manipulations, $P_{\text{SOP}}^{(\text{BUS})}$ in (26) can be derived.

REFERENCES

[1] S. Mattisson, "An overview of 5G requirements and future wireless networks: Accommodating scaling technology," *IEEE Solid State Circuits Mag.*, vol. 10, no. 3, pp. 54–60, 2018.

[2] P. Zhang, X. Yang, J. Chen, and Y. Huang, "A survey of testing for 5G: Solutions, oppurtunities, and challenges," *China Commun.*, vol. 16, no. 1, pp. 69–85, Jan. 2019.

[3] A. Froytlog, T. Foss, O. Bakker, G. Jevne, M. A. Haglund, F. Y. Li, J. Oller, and G. Y. Li, "Ultra-low power wake-up radio for 5G IoT," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 111–117, Mar. 2019.

[4] X. Liu and N. Ansari, "Toward green IoT: Energy solutions and key challenges," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 104–110, Mar. 2019.

[5] K. Liang, L. Zhao, G. Zhang, and H.-H. Chen, "Non-uniform deployment of power beacons in WPCN," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1887–1899, Mar. 2019.

[6] T. N. Do, V. D. Nguyen, O. S. Shin, and D. Au, "Simultaneous uplink and downlink transmissions for WPCN," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 374–377, Feb. 2019.

[7] K.-G. Nguyen, Q.-D. Vu, L.-N. Tran, and M. Juntti, "Energy efficiency fairness for multi-pair wireless-powered relaying systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 357–373, Feb. 2019.

[8] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[9] 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.

[10] J. Ren, J. Hu, D. Zhang, H. Guo, Y. Zhang, and X. Shen, "RF energy harvesting and transfer in cognitive radio sensor networks: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 104–110, Jan. 2018.

[11] V. Nhan 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.

[12] 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, Nov. 2018.

[13] J. Chen, L. Zhang, Y. Liang, X. Kang, and R. Zhang, "Resource allocation for wireless powered IoT networks with short packet communicationr," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 1447–1661, Feb. 2019.

[14] 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.

[15] 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.

[16] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[17] 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.

[18] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[19] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

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

[21] S. Bi, Y. Zeng, and R. Zhang, "Wireless powered communication networks: An overview," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 10–18, Apr. 2016.

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

[23] 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.

[24] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[25] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[26] 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.

[27] 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.

[28] 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.

[29] 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, Jun. 2016.

[30] J. Zhang, G. Pan, and Y. Xie, "Secrecy analysis of wireless-powered multi-antenna relaying system with nonlinear energy harvesters and imperfect CSI," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 2, pp. 460–470, Jun. 2018.

[31] P. Yan, Y. Zou, and J. Zhu, "Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2084–2096, Mar. 2018.

[32] X. Ding, Y. Zou, G. Zhang, X. Chen, X. Wang, and L. Hanzo, "The security–reliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networks," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 3890–3904, Jun. 2019.

[33] J. Choi, C. Song, and J. Joung, "Wireless powered information transfer based on zero-forcing for multiuser MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8561–8570, Sep. 2018.

[34] H. Lee, H. Kin, K.-J. Lee, and I. Lee, "Asynchronous designs for multiuser MIMO wireless powered communication networks," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2420–2430, Sep. 2019.

[35] H. Chen, X. Zhou, Y. Li, P. Wang, and B. Vucetic, "Wireless-powered cooperative communications via a hybrid relay," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014, pp. 666–670.

[36] N. Zlatanov, D. W. K. Ng, and R. Schober, "Capacity of the two-hop relay channel with wireless energy transfer from relay to source and energy transmission cost," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 647–662, Jan. 2017.

[37] M. Liu and Y. Liu, "Relay-assisted multiuser wireless powered communication with processing costs," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[38] M. Liu and Y. Liu, "Charge-then-forward: Wireless-powered communication for multiuser relay networks," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5155–5167, Nov. 2018.

[39] F. Yang, W. Xu, Z. Zhang, L. Guo, and J. Lin, "Energy efficiency maximization for relay-assisted WPCN: Joint time duration and power allocation," *IEEE Access*, vol. 6, pp. 78297–78307, Dec. 2018.

[40] E. Chen, M. Xia, and S. Aissa, "Coverage probability of hierarchical wireless networks with hybrid powering/relaying nodes (invited paper)," in *Proc. 15th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2018, pp. 1–6.

[41] S. Luo, G. Yang, and K. Chan Teh, "Throughput of wireless-powered relaying systems with buffer-aided hybrid relay," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4790–4801, Jul. 2016.

[42] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and Z. Han, "Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1528–1544, Mar. 2018.

[43] R. Zhao, X. Tan, D.-H. Chen, Y.-C. He, and Z. Ding, "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11511–11524, Dec. 2018.

[44] T.-X. Zheng, Q. Yang, Y. Zhang, H.-M. Wang, and P. Mu, "Secure transmissions in wireless ad hoc networks using hybrid half and full duplex receivers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[45] Y. Huang, P. Zhang, Q. Wu, and J. Wang, "Secrecy performance of wireless powered communication networks with multiple eavesdroppers and outdated CSI," *IEEE Access*, vol. 6, pp. 33774–33788, May 2018.

[46] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 335–346, Jan. 2017.

[47] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082–2085, Dec. 2015.

[48] Y. Dong, M. J. Hossain, and J. Cheng, "Performance of wireless powered amplify and forward relaying over Nakagami- fading channels with non-linear energy harvester," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 672–675, Apr. 2016.

[49] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[50] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[51] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.

[52] Y. Wang, H. Yin, W. Yang, T. Zhang, Y. Shen, and H. Zhu, "Secure wireless powered cooperative communication networks with finite energy storage," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1008–1022, Jan. 2020.

[53] 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.

[54] Y. Liu, L. Wang, S. A. Raza 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.

[55] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2018.

[56] J. Wan, D. Qiao, H.-M. Wang, and H. Qian, "Buffer-aided two-hop secure communications with power control and link selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7635–7647, Nov. 2018.

[57] Y. Zou and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*. Cham, Switzerland: Springer, 2016.

[58] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[60] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

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

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

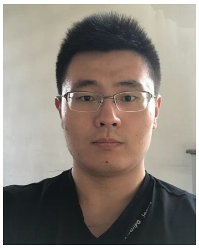
[63] R. P. Brent, *Algorithms for Minimization Without Derivatives*. Chelmsford, MA, USA: Courier Corporation, 2013.

[64] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C: The Art of Scientific Computing*. Cambridge, U.K.: Cambridge Univ. Press, 2007.

XIAOHUI SHANG received the B.E. degree in communication engineering from the Harbin Institute of Technology (HIT), in 2009, and the M.S. degree in communication and information system from the PLA University of Science and Technology (PLAUST), in 2012. He is currently pursuing the Ph.D. degree with the College of Communications Engineering, Army Engineering University of PLA, Nanjing, China. His research interests include physical layer security, cooperative communications, wireless powered communication networks, and energy harvesting.

HAO YIN received the B.S. degree in microwave communication and the M.S. degree in communication and information systems from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 1982 and 1987, respectively, and the Ph.D. degree in communication and information systems from the Beijing Institute of Technology, Beijing, China, in 2008. He is currently an Adjunct Professor with the Army Engineering University of PLA, Nanjing, China, and a Researcher with the Institute of China Electronic System Engineering. His research interests include wireless communication networks and information systems.

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.



MU LI received the B.S. degree in system engineering 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 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree in communication and information systems with the Army Engineering University of PLA, Nanjing, China. His current research interests include cooperative communications, wireless sensor networks, physical layer security, and cognitive radio systems.

YONG WANG received the B.S. and M.S. degrees from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2007 and 2012, respectively. He is currently pursuing the Ph.D. degree in communications and information systems from the College of Communication Engineering, Army Engineering University of PLA. His current research interests include cooperative communications, physical layer security, wireless sensor networks, and the Internet of Things.