IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 10, 2019, accepted October 3, 2019, date of publication October 11, 2019, date of current version October 25, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2946600*

# On Security and Throughput for Energy Harvesting Untrusted Relays in IoT Systems Using NOMA

**VAN NHAN VO[1], CHAKCHAI SO-IN[2], (Senior Member, IEEE), HUNG TRAN[3], DUC-DUNG TRAN[4], SOVANNARITH HENG[2,5], PHET AIMTONGKHAM[2], AND ANH-NHAT NGUYEN[2]**

[1]International School, Duy Tan University, Da Nang 550000, Vietnam
[2]Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[3]School of Innovation, Design and Engineering, Mälardalen University, 72123 Västerås, Sweden
[4]Faculty of Electrical and Electronics Engineering, Duy Tan University, Da Nang 550000, Vietnam
[5]Department of Computer Science, Faculty of Science, Royal University of Phnom Penh, Phnom Penh 12100, Cambodia

Corresponding author: Chakchai So-In (chakso@kku.ac.th)

This work was supported in part by the Thailand Research Fund, in part by the Thai Network Information Center Foundation under Grant RSA6180067, in part by the Khon Kaen University, and in part by the SSF Framework Grant Serendipity, Sweden.

**ABSTRACT** In this paper, we analyze the secrecy and throughput of multiple-input single-output (MISO) energy harvesting (EH) Internet of Things (IoT) systems, in which a multi-antenna base station (BS) transmits signals to IoT devices (IoTDs) with the help of relays. Specifically, the communication process is separated into two phases. In the first phase, the BS applies transmit antenna selection (TAS) to broadcast the signal to the relays and IoTDs by using non-orthogonal multiple access (NOMA). Here, the relays use power-splitting-based relaying (PSR) for EH and information processing. In the second phase, the selected relay employs the amplify-and-forward (AF) technique to forward the received signal to the IoTDs using NOMA. The information transmitted from the BS to the IoTD risks leakage by the relay, which is able to act as an eavesdropper (EAV) (i.e., an untrusted relay). To analyze the secrecy performance, we investigate three schemes: random-BS-best-relay (RBBR), best-BS-random-relay (BBRR), and best-BS-best-relay (BBBR). The physical layer secrecy (PLS) performance is characterized by deriving closed-form expressions of secrecy outage probability (SOP) for the IoTDs. A BS transmit power optimization algorithm is also proposed to achieve the best secrecy performance. Based on this, we then evaluate the system performance of the considered system, i.e., the outage probability and throughput. In addition, the impacts of the EH time, the power-splitting ratio, the numbers of BS antennas, and the numbers of untrusted relays on the SOP and throughput are investigated. The Monte Carlo approach is applied to verify our analytical results. Finally, the numerical examples indicate that the system performance of BBBR is greater than that of RBBR and BBRR.

**INDEX TERMS** Energy harvesting, Internet of Things, physical layer secrecy, throughput, NOMA, MISO, untrusted relay.

## I. INTRODUCTION

The Internet of Things (IoT) has attracted the attention of many researchers worldwide [1]–[3]; the main drive behind the future IoT relates to smart sensor technologies, including in farm monitoring, vehicular tracking, healthcare, and industrial environments [4]–[6]. Although the term IoT has been around for almost a decade, the corresponding technologies and protocols, such as massive connectivity, energy constraints, scalability and reliability limitations, and security, are still open research issues [7]–[9].

An important problem caused by the usage of massive IoT devices (IoTDs) is spectrum scarcity [5]. The non-orthogonal multiple access (NOMA) technique has been used as a promising solution to overcome this drawback. This is because NOMA can increase the connectivity and improve spectrum utilization in IoT systems [10]. For example, E. Hossain *et al*. investigated the system on a large scale

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wu.

using NOMA and concluded that NOMA not only improves spectral efficiency but also increases power efficiency [10]. I. Khan *et al*. proved that NOMA is a promising approach for future mobile Internet and IoT applications, which will require handling enormous increases in data traffic, massive connectivity, and low latency [9].

Furthermore, NOMA is able to simultaneously support users with good channel conditions as well as users with poor channel conditions by using the same bandwidth resources [11]. In addition, some works have compared the system performance of orthogonal multiple access (OMA) and NOMA [12]–[14]. For instance, Z. Chen *et al*. evaluated the system performance of NOMA and OMA by mathematical proof [12], while M. Zeng *et al*. compared NOMA and OMA for multiple-input multiple-output (MIMO) systems [13]. They concluded that the system performance of NOMA is better than that of OMA.

Energy consumption is actually another critical issue in IoT systems because of IoTDs' resource limitations [15]. Energy harvesting (EH) has emerged as a possible solution to meet the energy demands of IoT systems [7]. Thus, many works have focused on the perspective of EH usage in the IoT era [15]–[18]. For instance, N. Garg *et al*. introduced a survey on EH for IoTDs. They presented EH considering different energy sources and their comparisons. They then concluded that EH using solar or wind can obtain energy with very high efficiency; however, such harvesting is not available during night or in high-density building areas, respectively; in addition, EH from radio frequency (RF) is suitable for the IoTs due to its high availibility [15].

B. Alzahrani *et al*. introduced a resource management scheme for IoT systems with RF EH. The simulation results indicated that RF EH can increase the energy efficiency of IoT systems [16]. X. Song *et al*. investigated down-link NOMA networks and proposed a power allocation scheme to improve the energy efficiency with imperfect channel state information (CSI) [18]. Furthermore, D. D. Tran *et al*. investigated a multiple-input single-out (MISO) IoT system with simultaneous wireless information and power transfer, where the considered system consists of a multiantenna BS, multiple energy-limited relay clusters, and multiple IoTDs. Through Monte Carlo simulations, they showed that better system performance is obtained as the number of transmit antennas and relays increases [19].

To improve the scalability and reliability of IoT systems, cooperative relaying in which relays can be employed to support transmission from a base station (BS) to an IoTD, has been shown to be an effective method [20]. Note that relays can operate in two ways: to amplify and transmit the signal received from the source with a suitable power amplification coefficient by using amplify-and-forward (AF) techniques or to transmit the decoded signal using decode-and-forward (DF) techniques [19].

Unfortunately, the relays do not have the same security characteristics as the BS-IoTD pair since they belong to a heterogeneous network in certain scenarios [21], such as in a network consisting of networks used by a government or a financial institution whereby not all IoTD have the same level of security [20]. Thus, the relay can become an eavesdropper (EAV), i.e., an untrusted relay [22], [23]. This leads to confidential information possibly being monitored by the untrusted relay. Therefore, DF is not recommended since this technique requires that the untrusted relay decode the message before forwarding it to the IoTDs, i.e., AF is preferred [20], [21].

Due to the presence of untrusted relays, communication security is also a major challenge to IoT systems [20]. Traditional cryptographic encryption has been applied to overcome this reliability limitation. However, key distribution and management issues in IoT systems are difficult to control since these systems have massive numbers of resource-constrained IoTDs and different subsystems controlled by distinct operators [5].

As a result, physical layer secrecy (PLS) with high efficiency is an appealing approach for enhancing the secrecy performance in the IoT [5], [24]–[26]. The primary idea of PLS is exploiting the wireless channel characteristics to keep the confidential message from the EAV. For example, H. Hu *et al*. focused on the problem of secure communication between the IoTD and BS via the EH untrusted relay with the AF technique. The secrecy performances of the system were evaluated through the PLS in terms of the probability of successfully securing transmission [5]. L. Lv *et al*. introduced a novel NOMA-inspired relaying scheme using the AF technique to improve the PLS of untrusted relay networks. They then evaluated the PLS of their considered system by deriving an analytical expression for a lower bound on the ergodic secrecy sum rate [26].

To the best of our knowledge, RF EH untrusted relays in MISO IoT system using NOMA have not been studied extensively in recent works. Thus, in this paper, we consider PLS and throughput for a NOMA IoT system that consists of multi-antenna BS, multiple untrusted relays, multiple IoTDs with imperfect CSI. The primary contributions of this paper are summarized as follows:

- We introduce a communication process in a MISO IoT system with multiple AF EH untrusted relays.
- We investigate three cooperative TAS and relay selection schemes, i.e., the best-BS-random-relay scheme (RBBR), random-BS-best-relay scheme (BBRR), and best-BS-best-relay scheme (BBBR), to analyze and compare the considered system securities.
- We derive closed-form expressions of the secrecy outage probability (SOP) with imperfect CSI by using statistical characteristics of end-to-end signal-to-interference-plus-noise ratio (SINR) for the three considered schemes. Based on the SOP, an optimal and convergent transmit power algorithm for the BS is proposed.
- We derive closed-form expressions of the outage probability and throughput for the three considered schemes. Accordingly, the system performance is evaluated by the

outage probability and throughput metrics based on the optimal SOP.

The remainder of this paper is organized as follows: In Section II, some related works on EH, NOMA, and the PLS of untrusted relays in IoT systems are presented. In Section III, a system model, a communication process, the end-to-end SINR, and the three communication schemes are introduced. In Section IV, the SOPs corresponding to the three considered schemes are analyzed. In Section V, the outage probability and throughput are derived. In Section VI, numerical results are shown and discussed. Finally, conclusions and directions for future research are presented in Section VII.

## II. RELATED WORK

In this section, the summary of recent work on PLS and EH untrusted relay in IoT with NOMA transmission is introduced.

To enhance the reliability and secrecy performance, the PLS in IoT systems using untrusted relays has been considered [5], [21], [27], [28]. For example, D. Chen *et al*. focused on the secrecy performance of uplink transmission in an IoT system, where multiple IoTDs communicate with a BS with the help of an untrusted relay. Based on the maximum end-to-end signal-to-noise ratio (SNR), they proposed the optimal scheduling scheme to improve the secrecy throughput [21]. Nevertheless, this work focused on a simple system with one untrusted relay, and the authors did not investigate the impact of EH on the secrecy performance of the considered system.

Therefore, to investigate the impact of EH on secrecy performance, H. Hu *et al*. considered a cognitive IoT system, where the problem of secure communication between the IoTD and a BS via an EH untrusted relay was analyzed. They derived the closed-form expressions of the probability of successful secure transmission to evaluate the secrecy performances [5]. Furthermore, to extend the system, V. N. Vo *et al*. considered an IoT system whereby multiple IoTD and untrusted relays harvested energy from multiple power transfer stations (PTSs), and the IoTDs then transmited the signal to the BS with the help of untrusted relays. The authors then studied the secrecy performance of three relay selection schemes based on the SOP and throughput metrics [27]. However, the spectrum scarcity in the case of a large number of IoTDs was not investigated in those works.

To increase the connectivity and ensure effective spectrum utilization, the application of NOMA to an IoT system has been considered. For example, L. Lv *et al*. introduced a novel NOMA relaying scheme to improve the PLS of untrusted relay networks. Analytical expressions of an ergodic secrecy sum rate (ESSR) are derived to evaluate the secrecy performance, and the numerical results show that the significant ESSR improvement of the NOMA scheme is better than that of conventional orthogonal multiple access [26].

D.-T. Do *et al*. investigated a system in a scenario consisting of an untrusted relay required by users at far distances, where the NOMA is used to serve a large number of users.

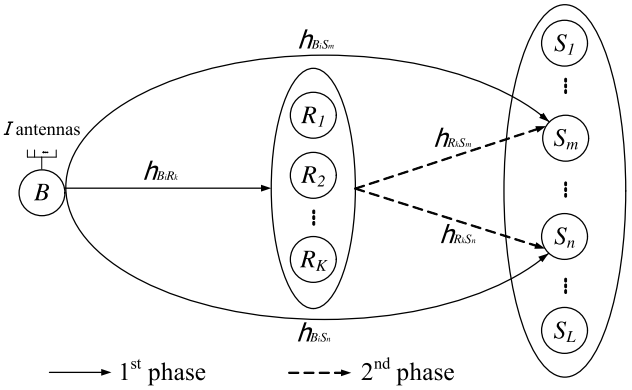


**FIGURE 1.** A system model for the EH untrusted relays in the IoT.

The SOP is derived to evaluate the secrecy performance [29]. Note that the above works assume that the CSIs of the communication links are perfectly known to the receiver; nevertheless, the perfect CSI is difficult to obtain because of the channel estimation errors, feedback, and quantization errors [18]. Thus, considering imperfect CSI in wireless communication systems is essential to investigating a system that well models a real-world application.

T. A. Le *et al*. studied a NOMA system with imperfect successive interference cancellation (SIC) using EH untrusted relays. In this context, the relays use a power-switching architecture to harvest energy and AF to forward signals. The closed-form expressions of the SOP are derived to analyze the secrecy performance. The numerical results indicated that NOMA offers better secrecy performance with multiple users [30]. However, cooperation between direct links and the relay as well as the multi-antenna BS to improve the secrecy performance and throughput was not considered. Likewise, the trade-off between the secrecy performance and throughput was also not investigated in that work.

Based on the above survey, no publication has investigated the SOP optimization with imperfect CSI; thus, we focus on this issue to evaluate the throughput performance of a secure IoT system consisting of a BS with multiple antennas, multiple untrusted relays, and multiple IoTDs.

## III. SYSTEM MODEL

In this section, we introduce the system model, channel assumptions, communication protocol, and scheduling schemes.

### A. SYSTEM MODEL AND CHANNEL ASSUMPTIONS

We consider the IoT architecture as in Fig. 1, where the system consists of a BS (e.g., controller), multiple EH relays, and multiple IoTDs (e.g., sensors). The BS transmits signals to the IoTDs by using NOMA and utilizes the relays for forwarding the signal to the IoTDs to improve the throughput. The relays then use the AF technique to send the collected information to the IoTDs by using NOMA. Here, we investigate the case in which the relays are not authenticated by a legitimate BS and IoTDs, i.e., an untrusted relay. This means

**TABLE 1. Notations.**

| Notation | Definition |
|---|---|
| $L$ | The number of IoTDs |
| $K$ | The number of untrusted relays |
| $I$ | The number of antennas possessed by the BS |
| $B_i$ | The BS with the $i$-th antenna, where $1 \leq i \leq I$ |
| $R_k$ | The $k$-th untrusted relay, where $1 \leq k \leq K$ |
| $S_\pi$ | The $\pi$-th IoTD, where $1 \leq \pi \leq L$ and $\pi \in \{m, n\}$ |
| $h_{XY}$ | The channel coefficient of the $X \to Y$ link |
| $d_{XY}$ | The distance corresponding to $h_{XY}$ |
| $(A_\pi, B_\pi)$ | The coordinate of the $\pi$-th IoTD |
| $(A_k, B_k)$ | The coordinate of the $k$-th untrusted relay |
| $\upsilon$ | The path-loss exponent, $2 \leq \upsilon \leq 6$ [31]–[33] |
| $\mathbf{E}[\cdot]$ | The expectation operator |
| $\Omega_{\lvert h_{XY}\rvert^2}$ | The main channel gain , $\Omega_{\lvert h_{XY}\rvert^2} = d_{XY}^{-\upsilon}$ |
| $\mathcal{P}$ | The transmit power |
| $P$ | The probability function |
| $\lambda_{sec_{S_\pi}}$ | The predefined secrecy threshold of the $\pi$-th IoTD |
| $\lambda_{op_{S_\pi}}$ | The target rate of the $\pi$-th IoTD |
| $\widehat{h}_{XY}$ | The channel coefficient estimated using minimum mean square error (MMSE) for $h_{XY}$ |
| $\mathcal{O}_{sec}$ | The SOP |
| $\mathcal{O}_{asym}$ | The asymptotic expressions of the SOP in the high SNR regime |
| $\mathcal{O}_{op}$ | The outage probability |
| $\Gamma$ | The throughput |

that the reliable communication of the considered IoT system can be improved significantly by utilizing multiple relays; however, the end-to-end information should not be revealed to untrusted relays.

Note that the BS is equipped with multiple antennas, and the IoTDs and untrusted relays have a single antenna due to their size and capability limitations. Without loss of generality, all channels are assumed to be mutually independent [34] and are described in Table 1. We also assume that channels in each block of time (from the BS to the untrusted relays, from the untrusted relays to the IoTDs, and from the BS to the IoTDs) are independent and modeled as block flat Rayleigh fading channels, i.e., the channel gains are random variables (RVs) distributed following an exponential distribution [35]–[37]. Accordingly, the probability density function (PDF) and cumulative distribution function (CDF) are expressed as follows [31]–[33]:

$$f_{|h_{XY}|^2}(x) = \frac{1}{\Omega_{|h_{XY}|^2}} \exp\left(-\frac{x}{\Omega_{|h_{XY}|^2}}\right), \quad (1)$$

$$F_{|h_{XY}|^2}(x) = 1 - \exp\left(-\frac{x}{\Omega_{|h_{XY}|^2}}\right), \quad (2)$$

where RV $h_{XY} \in \left\{h_{B_iR_k}, h_{B_iS_\pi}, h_{R_kS_\pi}\right\}$ is an exponential RV with a mean value $\Omega_{|h_{XY}|^2}$.

### B. COMMUNICATION PROCESS

Adopting the PSR protocol [5], [38], the communication process is shown in Fig. 2, which is divided into 2 phases as follows:

- Phase 1: In a block time $\tau T$: The BS selects one of $I$ antennas to broadcast superimposed mixed signals, i.e., $x_B = \sqrt{\alpha_m}x_m + \sqrt{\alpha_n}x_n$, to the IoTDs and untrusted relays using TAS [19], where $x_m$ and $x_n$ are the signals received by $S_m$ (far IoTD) and $S_n$ (near IoTD), and $\alpha_m$ and $\alpha_n$ are the power allocation coefficients that satisfy the condition $\alpha_m + \alpha_n = 1$ and $\alpha_m > \alpha_n$ [39]. Note that we adopt the assumption given in [40], [41] that the destination node pairs are selected arbitrarily but that they must satisfy the characteristics of NOMA, i.e., the near sensors having good channel condition are allocated a lower power level than the far sensors (which have bad channel conditions). Thus, the received signals in the first phase at $S_\pi$ are expressed as

$$y_{S_\pi}^{(1)} = \sqrt{\mathcal{P}_B}\left(\sqrt{\alpha_m}x_m + \sqrt{\alpha_n}x_n\right)h_{B_iS_\pi} + n_{S_\pi}^{(1)}, \quad (3)$$

where $n_{S_\pi}^{(1)} \sim \mathcal{CN}(0, N_0)$, $N_0$ is additive white Gaussian noise (AWGN), and $\mathcal{P}_B$ is the transmit power of the BS. Note that imperfect CSI of the communication link between the BS and the IoTD is considered, i.e., the channel coefficient of the BS-IoTD link is estimated by using MMSE estimation error as follows [42]–[45]:

$$h_{B_iS_\pi} = \widehat{h}_{B_iS_\pi} + e_{B_iS_\pi}, \quad (4)$$

where $\widehat{h}_{B_iS_\pi}$ is the channel coefficient estimated using MMSE for $h_{B_iS_\pi}$, $e_{B_iS_\pi} \sim \mathcal{CN}(0, \Omega_e)$ is the channel estimation error, and $\Omega_e$ is defined as the correctness of the channel estimation. According to the NOMA technique, $S_m$ decodes the message $x_m$ by treating $S_n$'s message as noise. Therefore, the instantaneous SINR at the $m$-th IoTD from the BS is written as follows:

$$\gamma_{B_iS_m}^{(1)} = \frac{\alpha_m\rho_B|\widehat{h}_{B_iS_m}|^2}{\alpha_n\rho_B|\widehat{h}_{B_iS_m}|^2 + \rho_B\Omega_e + 1}, \quad (5)$$

where $\rho_B = \mathcal{P}_B/N_0$. Furthermore, at the $n$-th IoTD, $S_n$ first decodes the message $x_m$ and then removes this element to obtain its message by using SIC. Here, we assume that $S_n$ can decode $x_m$ successfully by adopting the method proposed in [43], [46]. Thus, the SINR at $S_n$ necessary to detect $x_n$ from the BS is expressed as

$$\gamma_{B_iS_n}^{(1)} = \frac{\alpha_n\rho_B|\widehat{h}_{B_iS_n}|^2}{\rho_B\Omega_e + 1}. \quad (6)$$

At untrusted relay $R_k$, power-splitting-based relaying (PSR) is deployed by dividing the transmit power of the BS into two streams: $\mu\mathcal{P}_B$ for EH and $(1-\mu)\mathcal{P}_B$ for information processing, where $0 < \mu < 1$ is the power-splitting ratio [38]. Thus, the harvested energy at $R_k$ can be formulated as

$$E_{R_k} = \mathbf{E}\left[\tau T\eta\mu\mathcal{P}_B\left|h_{B_iR_k}\right|^2\right], \quad (7)$$

where $\tau$ is the fraction of the block time $T$ for EH, $\eta$ is the energy conversion efficiency of the $k$-th untrusted relay, and $\mathcal{P}_B$ is the transmit power of the BS. Here, due to the short distance, the untrusted relays apply a constant gain to the received signal from the BS [47]–[49], i.e., the fixed-gain between BS and the untrusted relay is

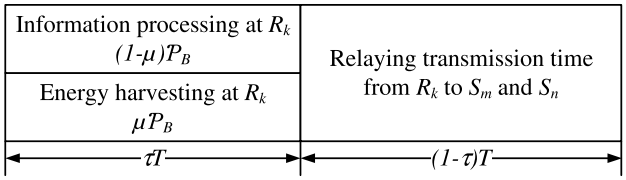


**FIGURE 2.** The communication process with the PSR protocol.

known. This reduces the amount of mathematical computation (in practical scenarios, the fixed-gain is known, as the channel is less variable and can be calculated by statistical information collected by the operator). Thus, we apply the fixed-gain EH and relay at the untrusted relays, i.e., $\mathbf{E}\left[\left|h_{B_iR_k}\right|^2\right] = \Omega_{\left|h_{B_iR_k}\right|^2}$ [41], [50]–[52]. Accordingly, the harvested energy at $R_k$ can be rewritten as

$$E_{R_k} = \tau T \eta \mu \mathcal{P}_B \Omega_{\left|h_{B_iR_k}\right|^2}. \tag{8}$$

Furthermore, the received signal at the $k$-th untrusted relay is expressed as

$$y_{R_k} = \sqrt{(1-\mu)\mathcal{P}_B}\left(\sqrt{\alpha_m}x_m + \sqrt{\alpha_n}x_n\right)h_{B_iR_k} + n_{R_k}, \tag{9}$$

where $n_{R_k} \sim \mathcal{CN}(0, N_0)$. Therefore, the received SINRs at the $k$-th untrusted relay for detecting $x_m$ and $x_n$ are expressed as follows:

$$\gamma_{B_iR_k}^{x_m} = \frac{\alpha_m (1-\mu)\rho_B \left|h_{B_iR_k}\right|^2}{\alpha_n (1-\mu)\rho_B \left|h_{B_iR_k}\right|^2 + (1-\mu)\rho_B\Omega_e + 1}, \tag{10}$$

$$\gamma_{B_iR_k}^{x_n} = \frac{\alpha_n (1-\mu)\rho_B \left|h_{B_iR_k}\right|^2}{(1-\mu)\rho_B\Omega_e + 1}. \tag{11}$$

- Phase 2: In the remaining time of $(1-\tau)T$, the selected untrusted relay uses the harvested energy in the first phase for relaying the signal to the IoTDs by applying AF with NOMA. Here, the transmit power and the variable amplifying coefficient at $R_k$ are expressed as follows:

$$\mathcal{P}_{R_k} = \frac{E_{R_k}}{(1-\tau)T}, \tag{12}$$

$$\mathcal{G}_k = \frac{1}{\sqrt{\mathcal{P}_B\left|\widehat{h}_{B_iR_k}\right|^2 + N_0}}. \tag{13}$$

Consequently, the received signal at $S_\pi$ in the second phase is formulated as

$$\begin{aligned} y_{S_\pi}^{(2)} &= \mathcal{G}_k\sqrt{\mathcal{P}_{R_k}}y_{R_k}h_{R_kS_\pi} + n_{S_\pi}^{(2)} \\ &= \mathcal{G}_k\sqrt{(1-\mu)\mathcal{P}_B\mathcal{P}_{R_k}}\left(\sqrt{\alpha_m}x_m + \sqrt{\alpha_n}x_n\right) \\ &\quad \times h_{B_iR_k}h_{R_kS_\pi} + \mathcal{G}_k\sqrt{\mathcal{P}_{R_k}}h_{R_kS_\pi}n_{R_k} + n_{S_\pi}^{(2)}, \end{aligned} \tag{14}$$

where $n_{S_\pi}^{(2)} \sim \mathcal{CN}(0, N_0)$. Note that we consider the imperfect CSI of the communication link between the selected untrusted relay and $S_\pi$, i.e.,

$$h_{R_kS_\pi} = \widehat{h}_{R_kS_\pi} + e_{R_kS_\pi}, \tag{15}$$

where $\widehat{h}_{R_kS_\pi}$ is the channel coefficient estimated using MMSE for $h_{R_kS_\pi}$ and $e_{R_kS_\pi} \sim \mathcal{CN}(0, \Omega_e)$ is the channel estimation error. Thus, the SINRs for detecting $x_m$ and $x_n$ transmitted from $R_k$ at $S_m$ and $S_n$ are expressed as (16) and (17), as shown at the bottom of this page, where $\rho_{R_k} = \mathcal{P}_{R_k}/N_0$.

### C. THE END-TO-END SINR AND CHANNEL CAPACITY

At the IoTDs, selection combining (SC) are utilized to process the received signals [38], [53]. Thus, the end-to-end SINRs at $S_m$ and $S_n$ for decoding $x_m$ and $x_n$ are formulated as follows:

$$\gamma_{S_m} = \max\left\{\frac{\alpha_m\rho_B\left|\widehat{h}_{B_iS_m}\right|^2}{\alpha_n\rho_B\left|\widehat{h}_{B_iS_m}\right|^2 + \Delta_5}, \frac{\alpha_m\Delta_1\left|\widehat{h}_{R_kS_m}\right|^2}{\left|\widehat{h}_{R_kS_m}\right|^2\Delta_2 + \Delta_3}\right\}, \tag{18}$$

$$\gamma_{S_n} = \max\left\{\frac{\alpha_n\rho_B\left|\widehat{h}_{B_iS_n}\right|^2}{\Delta_5}, \frac{\alpha_n\Delta_1\left|\widehat{h}_{R_kS_n}\right|^2}{\left|\widehat{h}_{R_kS_n}\right|^2\Delta_4 + \Delta_3}\right\}, \tag{19}$$

where $\Delta_1$, $\Delta_2$, $\Delta_3$, $\Delta_4$, and $\Delta_5$ are defined as follows:

$$\Delta_1 = \rho_{R_k}(1-\mu)\rho_B\Omega_{\left|\widehat{h}_{B_iR_k}\right|^2}, \tag{20}$$

$$\Delta_2 = \alpha_n\Delta_1 + \rho_{R_k}(1-\mu)\rho_B\Omega_e + \rho_{R_k}, \tag{21}$$

$$\begin{aligned} \Delta_3 &= \rho_{R_k}(1-\mu)\rho_B\left(\Omega_{\left|\widehat{h}_{B_iR_k}\right|^2}\Omega_e + \Omega_e^2\right) + \rho_{R_k}\Omega_e \\ &\quad + \rho_B\Omega_{\left|\widehat{h}_{B_iR_k}\right|^2} + 1, \end{aligned} \tag{22}$$

$$\Delta_4 = \rho_{R_k}(1-\mu)\rho_B\Omega_e + \rho_{R_k}, \tag{23}$$

$$\Delta_5 = \rho_B\Omega_e + 1. \tag{24}$$

Note that we consider the case in which the relays are not authenticated by legitimate BS or IoTDs, i.e., the relays may become EAVs. This means that confidential information may be revealed to untrusted relays. Thus, to measure the secrecy performance under the threat of an untrusted relay,

$$\gamma_{R_kS_m}^{(2)} = \frac{\rho_{R_k}\alpha_m(1-\mu)\rho_B\left|\widehat{h}_{B_iR_k}\right|^2\left|\widehat{h}_{R_kS_m}\right|^2}{\rho_{R_k}(1-\mu)\rho_B\left(\alpha_n\left|\widehat{h}_{B_iR_k}\right|^2\left|\widehat{h}_{R_kS_m}\right|^2 + \left|\widehat{h}_{R_kS_m}\right|^2\Omega_e + \left|\widehat{h}_{B_iR_k}\right|^2\Omega_e + \Omega_e^2\right) + \rho_{R_k}\left(\left|\widehat{h}_{R_kS_m}\right|^2 + \Omega_e\right) + 1/\mathcal{G}_k^2}, \tag{16}$$

$$\gamma_{R_kS_n}^{(2)} = \frac{\rho_{R_k}\alpha_n(1-\mu)\rho_B\left|\widehat{h}_{B_iR_k}\right|^2\left|\widehat{h}_{R_kS_n}\right|^2}{\rho_{R_k}(1-\mu)\rho_B\left(\left|\widehat{h}_{R_kS_n}\right|^2\Omega_e + \left|\widehat{h}_{B_iR_k}\right|^2\Omega_e + \Omega_e^2\right) + \rho_{R_k}\left(\left|\widehat{h}_{R_kS_n}\right|^2 + \Omega_e\right) + 1/\mathcal{G}_k^2}. \tag{17}$$

we employ the secrecy capacity concept given in [5], [21], i.e., the secrecy capacity at $S_m$ and $S_n$ can be formulated, respectively, as follows:

$$C_{sec_{S_m}} = \tau \log\left(\frac{1+\gamma_{S_m}}{1+\gamma_{B_iR_k}^{x_m}}\right), \tag{25}$$

$$C_{sec_{S_n}} = \tau \log\left(\frac{1+\gamma_{S_n}}{1+\gamma_{B_iR_k}^{x_n}}\right). \tag{26}$$

Substituting (10) and (18) into (25) and substituting (11) and (19) into (26), we have the SINRs for decoding $x_m$ and $x_n$ at $S_m$ and $S_n$ as (27) and (28), as shown at the bottom of this page, respectively, where $\Delta_6$ and $\Delta_7$ are defined as

$$\Delta_6 = 1 + \frac{\alpha_m(1-\mu)\rho_B\Omega_{|h_{B_iR_k}|^2}}{\alpha_n(1-\mu)\rho_B\Omega_{|h_{B_iR_k}|^2} + (1-\mu)\rho_B\Omega_e + 1}, \tag{29}$$

$$\Delta_7 = 1 + \frac{\alpha_n(1-\mu)\rho_B\Omega_{|h_{B_iR_k}|^2}}{(1-\mu)\rho_B\Omega_e + 1}. \tag{30}$$

### D. SCHEDULE SCHEME

- The RBBR: A transmit antenna at the BS is randomly chosen among $\{B_i\}_{i=1}^{I}$. Furthermore, the condition of the channel $R_k \to S_m$ is worse than that of $R_k \to S_n$. Thus, to improve the secrecy performance and throughput, this scheme intends to select the best untrusted relay $R^*$ among the $K$ intermediate nodes to maximize the channel gain of the link from $R^*$ to the $m$-th IoTD. Mathematically, the selected untrusted relay in RBBR is written as
$$R^* = \arg\max_{k=1,\cdots,K}\left\{\left|h_{R_kS_m}\right|^2\right\}. \tag{31}$$
- The BBRR: An untrusted relay is randomly chosen among $\{R_k\}_{k=1}^{K}$. Furthermore, the condition of the channel $B \to S_m$ is worse than that of $B \to S_n$. Thus, to improve the secrecy performance and throughput, this scheme intends to select a transmit antenna of the BS to maximize the channel gain of the direct link from the BS to the $m$-th IoTD, i.e., the BS with the selected transmit antenna is given by
$$B^* = \arg\max_{i=1,\cdots,I}\left\{\left|h_{B_iS_m}\right|^2\right\}. \tag{32}$$
- The BBBR: To improve the system performance, an antenna is chosen among $I$ antennas of the BS such that the channel gain from that antenna to the $m$-th IoTD is the best. Similarly, an untrusted relay is chosen among $K$ intermediate nodes such that the channel gain from that relay to the $m$-th IoTD is the best, i.e., the selected antenna and the selected untrusted relay are chosen as (31) and (32), respectively.

## IV. OPTIMAL POWER ALLOCATION IN THE PRESENCE OF UNTRUSTED RELAYS BASED ON THE SOP

In this section, the SOP will be analyzed over Rayleigh fading channels [35], and the optimal power allocation algorithm will be introduced.

### A. SECRECY OUTAGE PROBABILITY

Following [29], [39], the SOP for decoding $x_m$ and $x_n$ of an IoT system in the presence of an EH untrusted relay is defined as either the channel secrecy capacity probability of transmission links for decoding $x_m$ or that for decoding $x_n$ must be lower than predefined thresholds, $\lambda_{sec_{S_m}}$ or $\lambda_{sec_{S_n}}$, respectively, i.e.,

$$\mathcal{O}_{sec}^{\Psi} = \Pr\left\{C_{sec_{S_m}} < \lambda_{sec_{S_m}} \text{ or } C_{sec_{S_n}} < \lambda_{sec_{S_n}}\right\}, \tag{33}$$

where $\Psi \in \{\text{RBBR, BBRR, BBBR}\}$ and Pr{.} is a probability function. In accordance with the definition of conditional probabilities, the SOP of the considered system can be rewritten as

$$\mathcal{O}_{sec}^{\Psi} = 1 - \left(1 - \underbrace{\Pr\left\{C_{sec_{S_m}} < \lambda_{sec_{S_m}}\right\}}_{\mathcal{O}_{sec_{S_m}}^{\Psi}}\right) \times \left(1 - \underbrace{\Pr\left\{C_{sec_{S_n}} < \lambda_{sec_{S_n}}\right\}}_{\mathcal{O}_{sec_{S_n}}}\right). \tag{34}$$

Next, we introduce the closed-form for the SOP of the three considered schemes.

#### 1) DERIVATION FOR THE RBBR

Based on (27) and (34), the term $\mathcal{O}_{sec_{S_m}}^{\text{RBBR}}$ can be rewritten as follows:

$$\mathcal{O}_{sec_{S_m}}^{\text{RBBR}} = \underbrace{\Pr\left\{\frac{\alpha_m\rho_B\left|\widehat{h}_{B_iS_m}\right|^2}{\alpha_n\rho_B\left|\widehat{h}_{B_iS_m}\right|^2 + \Delta_5} < \Delta_6^m\right\}}_{P_{sec_{S_m}}^{\text{RBBR}(1)}} \times \underbrace{\Pr\left\{\frac{\alpha_m\Delta_1\left|\widehat{h}_{R^*S_m}\right|^2}{\Delta_2\left|\widehat{h}_{R^*S_m}\right|^2 + \Delta_3} < \Delta_6^m\right\}}_{P_{sec_{S_m}}^{\text{RBBR}(2)}}, \tag{35}$$

where $\Delta_6^m = 2^{\lambda_{sec_{S_m}}/\tau}\Delta_6 - 1$.

$$C_{sec_{S_m}} = \tau \log\left[\left(1 + \max\left\{\frac{\alpha_m\rho_B|\widehat{h}_{B_iS_m}|^2}{\alpha_n\rho_B|\widehat{h}_{B_iS_m}|^2 + \Delta_5}, \frac{\alpha_m\Delta_1\left|\widehat{h}_{R_kS_m}\right|^2}{\left|\widehat{h}_{R_kS_m}\right|^2\Delta_2 + \Delta_3}\right\}\right)/\Delta_6\right], \tag{27}$$

$$C_{sec_{S_n}} = \tau \log\left[\left(1 + \max\left\{\frac{\alpha_n\rho_B|\widehat{h}_{B_iS_n}|^2}{\Delta_5}, \frac{\alpha_n\Delta_1\left|\widehat{h}_{R_kS_n}\right|^2}{\left|\widehat{h}_{R_kS_n}\right|^2\Delta_4 + \Delta_3}\right\}\right)/\Delta_7\right]. \tag{28}$$

*Remark 1: Assume that $V_j$ ($j \in \{1, \cdots, J\}$) is an exponentially distributed independent RV with mean values $\Omega_{V_j}$. The CDF of $U = aV_j/(bV_j + c)$ is formulated as*

$$F_U = \begin{cases} 1 - \exp\left[-\dfrac{c_1 u}{\Omega_{V_j}(a_1 - b_1 u)}\right], & \text{if } a_1 - b_1 u > 0 \\ 0, & \text{if } a_1 - b_1 u < 0, \end{cases} \tag{36}$$

*where $a_1, b_1$, and $c_1$ are constants.*

*For the proof, see Appendix A.*

Using **Remark 1** with $a_1 = \alpha_m \rho_B$, $b_1 = \alpha_n \rho_B$, $c_1 = \Delta_5$, and $u = \Delta_6^m$, the expression $P_{sec_{S_m}}^{\text{RBBR}(1)}$ is obtained as

$$P_{sec_{S_m}}^{\text{RBBR}(1)} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_5 \Delta_6^m}{\Omega_{|\widehat{h}_{B_i S_m}|^2}\left(\alpha_m \rho_B - \alpha_n \rho_B \Delta_6^m\right)}\right], \\ \quad \text{if } \alpha_m - \alpha_n \Delta_6^m > 0 \\ 0, \quad \text{if } \alpha_m - \alpha_n \Delta_6^m \le 0. \end{cases} \tag{37}$$

*Remark 2: Assuming $V^* = \max\limits_{j=1,\cdots,J}\{V_j\}$, the CDF of $U^* = a_2 V^*/(b_2 V^* + c_2)$ is formulated as*

$$F_{U^*} = \begin{cases} \prod\limits_{j=1}^{J}\left\{1 - \exp\left[-\dfrac{c_2 u}{\Omega_{V_j}(a_2 - b_2 u)}\right]\right\}, \\ \quad \text{if } a_2 - b_2 u > 0 \\ 0, \quad \text{if } a_2 - b_2 u < 0, \end{cases} \tag{38}$$

*where $a_2, b_2$, and $c_2$ are constants.*

*For the proof, see Appendix A.*

Applying **Remark 2** with $a_2 = \alpha_m \Delta_1$, $b_2 = \Delta_2$, $c_2 = \Delta_3$, and $u = \Delta_6^m$, the probability function in terms of $P_{sec_{S_m}}^{\text{RBBR}(2)}$ is obtained as follows:

$$P_{sec_{S_m}}^{\text{RBBR}(2)} = \begin{cases} \prod\limits_{k=1}^{K}\left\{1 - \exp\left[-\dfrac{\Delta_3 \Delta_6^m}{\Omega_{|\widehat{h}_{R_k S_m}|^2}\left(\alpha_m \Delta_1 - \Delta_2 \Delta_6^m\right)}\right]\right\}, \\ \quad \text{if } \alpha_m \Delta_1 - \Delta_2 \Delta_6^m > 0 \\ 0, \quad \text{if } \alpha_m \Delta_1 - \Delta_2 \Delta_6^m < 0. \end{cases} \tag{39}$$

Based on (27) and (34), the term $\mathcal{O}_{sec_{S_n}}$ can be rewritten as follows:

$$\mathcal{O}_{sec_{S_n}} = \underbrace{\Pr\left\{\frac{\alpha_n \rho_B |\widehat{h}_{B_i S_n}|^2}{\Delta_5} < \Delta_7^n\right\}}_{P_{sec_{S_n}}^{(1)}} \times \underbrace{\Pr\left\{\frac{\alpha_n \Delta_1 |\widehat{h}_{R_k S_n}|^2}{\Delta_4 |\widehat{h}_{R_k S_n}|^2 + \Delta_3} < \Delta_7^n\right\}}_{P_{sec_{S_n}}^{(2)}}, \tag{40}$$

where $\Delta_7^n = 2^{\lambda_{sec_{S_n}}/\tau}\Delta_7 - 1$. Substituting (2) into $P_{sec_{S_n}}^{(1)}$ and applying **Remark 1** with $a_1 = \alpha_n \Delta_1$, $b_1 = \Delta_4$, $c_1 = \Delta_3$, and $u = \Delta_7^m$ to $P_{sec_{S_n}}^{(2)}$, the functions $P_{sec_{S_n}}^{(1)}$ and $P_{sec_{S_n}}^{(2)}$ are derived as follows:

$$P_{sec_{S_n}}^{(1)} = 1 - \exp\left(-\frac{\Delta_7^n \Delta_5}{\Omega_{|\widehat{h}_{B_i S_n}|^2}\alpha_n \rho_B}\right), \tag{41}$$

$$P_{sec_{S_n}}^{(2)} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_3 \Delta_7^n}{\Omega_{|\widehat{h}_{R_k S_n}|^2}\left(\alpha_n \Delta_1 - \Delta_4 \Delta_7^n\right)}\right], \\ \quad \text{if } \alpha_n \Delta_1 - \Delta_4 \Delta_7^n > 0 \\ 0, \quad \text{if } \alpha_n \Delta_1 - \Delta_4 \Delta_7^n \le 0. \end{cases} \tag{42}$$

Finally, the SOP in the case of using RBBR is obtained as

$$\mathcal{O}_{sec}^{\text{RBBR}} = 1 - \left(1 - P_{sec_{S_m}}^{\text{RBBR}(1)} P_{sec_{S_m}}^{\text{RBBR}(2)}\right) \times \left(1 - P_{sec_{S_n}}^{(1)} P_{sec_{S_n}}^{(2)}\right). \tag{43}$$

### 2) DERIVATION FOR THE BBRR

Similar to the RBBR, the SOP for the BBRR is derived as follows:

$$\mathcal{O}_{sec}^{\text{BBRR}} = 1 - \left(1 - P_{sec_{S_m}}^{\text{BBRR}(1)} P_{sec_{S_m}}^{\text{BBRR}(2)}\right) \times \left(1 - P_{sec_{S_n}}^{(1)} P_{sec_{S_n}}^{(2)}\right), \tag{44}$$

where $P_{sec_{S_n}}^{(1)}$ and $P_{sec_{S_n}}^{(2)}$ are defined as (41) and (42), respectively; and $P_{sec_{S_m}}^{\text{BBRR}(1)}$ and $P_{sec_{S_m}}^{\text{BBRR}(2)}$ are defined as

$$P_{sec_{S_m}}^{\text{BBRR}(1)} = \prod_{i=1}^{I} P_{sec_{S_m}}^{\text{RBBR}(1)}, \tag{45}$$

$$P_{sec_{S_m}}^{\text{BBRR}(2)} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_3 \Delta_6^m}{\Omega_{|\widehat{h}_{R^* S_m}|^2}\left(\alpha_m \Delta_1 - \Delta_2 \Delta_6^m\right)}\right], \\ \quad \text{if } \alpha_m \Delta_1 - \Delta_2 \Delta_6^m > 0 \\ 0, \quad \text{if } \alpha_m \Delta_1 - \Delta_2 \Delta_6^m \le 0. \end{cases} \tag{46}$$

### 3) DERIVATION FOR THE BBBR

Following the definition of BBBR, the best antenna of the BS and the best untrusted relay are selected; thus, the SOP for the BBBR is obtained as

$$\mathcal{O}_{sec}^{\text{BBBR}} = 1 - \left(1 - P_{sec_{S_m}}^{\text{BBBR}(1)} P_{sec_{S_m}}^{\text{BBBR}(2)}\right) \times \left(1 - P_{sec_{S_n}}^{(1)} P_{sec_{S_n}}^{(2)}\right), \tag{47}$$

where $P_{sec_{S_n}}^{(1)}$ and $P_{sec_{S_n}}^{(2)}$ are defined as (41) and (42), respectively; $P_{sec_{S_m}}^{\text{BBBR}(1)} = P_{sec_{S_m}}^{\text{BBRR}(1)}$ and $P_{sec_{S_m}}^{\text{BBBR}(2)} = P_{sec_{S_m}}^{\text{RBBR}(2)}$.

### B. ASYMPTOTIC SOP ANALYSIS

Based on the analytical expressions of the SOP for RBBR, BBRR, and BBBR, we can see that the secrecy performance at high $\rho_B$, i.e., $\rho_B \to \infty$, tends to be a constant. Thus, the asymptotic expressions of the SOP for RBBR, BBRR, and BBBR are analyzed to observe insights into the effect of the high SNR regime as follows:

$$\mathcal{O}_{asym}^{\mathrm{RBBR}} = 1 - \left(1 - P_{asym_{S_m}}^{\mathrm{RBBR}(1)} P_{asym_{S_m}}^{\mathrm{RBBR}(2)}\right) \times \left(1 - P_{asym_{S_n}}^{(1)} P_{asym_{S_n}}^{(2)}\right), \quad (48)$$

$$\mathcal{O}_{asym}^{\mathrm{BBRR}} = 1 - \left(1 - P_{asym_{S_m}}^{\mathrm{BBRR}(1)} P_{asym_{S_m}}^{\mathrm{BBRR}(2)}\right) \times \left(1 - P_{asym_{S_n}}^{(1)} P_{asym_{S_n}}^{(2)}\right), \quad (49)$$

$$\mathcal{O}_{asym}^{\mathrm{BBBR}} = 1 - \left(1 - P_{asym_{S_m}}^{\mathrm{BBBR}(1)} P_{asym_{S_m}}^{\mathrm{BBBR}(2)}\right) \times \left(1 - P_{asym_{S_n}}^{(1)} P_{asym_{S_n}}^{(2)}\right), \quad (50)$$

where $P_{asym_{S_m}}^{\mathrm{BBRR}(2)}$ is defined as in (51), as shown at the bottom of this page; $P_{asym_{S_m}}^{\mathrm{BBBR}(1)} = P_{asym_{S_m}}^{\mathrm{BBRR}(1)}$ and $P_{asym_{S_m}}^{\mathrm{BBBR}(2)} = P_{asym_{S_m}}^{\mathrm{RBBR}(2)}$; and $\Delta_6^{asym}$, $\Delta_7^{asym}$, $P_{asym_{S_m}}^{\mathrm{RBBR}(1)}$, $P_{asym_{S_m}}^{\mathrm{BBRR}(1)}$, $P_{asym_{S_m}}^{\mathrm{RBBR}(2)}$, $P_{asym_{S_n}}^{(1)}$, and $P_{asym_{S_n}}^{(2)}$ are defined as

$$\Delta_6^{asym} = 2^{\lambda_{sec_{S_m}}/\tau}\left(1 + \frac{\alpha_m \Omega_{|h_{B_i R_k}|^2}}{\alpha_n \Omega_{|h_{B_i R_k}|^2} + \Omega_e}\right) - 1, \quad (52)$$

$$\Delta_7^{asym} = 2^{\lambda_{sec_{S_n}}/\tau}\left(1 + \frac{\alpha_m \Omega_{|h_{B_i R_k}|^2}}{\Omega_e}\right) - 1, \quad (53)$$

$$P_{asym_{S_m}}^{\mathrm{RBBR}(1)} = \begin{cases} 1 - \exp\left[-\dfrac{\Omega_e \Delta_6^{asym}}{\Omega_{|\widehat{h}_{B_i S_m}|^2}\left(\alpha_m - \alpha_n \Delta_6^{asym}\right)}\right], \\ \quad \text{if } \alpha_m - \alpha_n \Delta_6^{asym} > 0 \\ 0, \quad \text{if } \alpha_m - \alpha_n \Delta_6^{asym} \le 0, \end{cases} \quad (54)$$

$$P_{asym_{S_m}}^{\mathrm{BBRR}(1)} = \prod_{i=1}^{I} P_{asym_{S_m}}^{\mathrm{RBBR}(1)}, \quad (55)$$

$$P_{asym_{S_m}}^{\mathrm{RBBR}(2)} = \prod_{k=1}^{K} P_{asym_{S_m}}^{\mathrm{BBRR}(2)}, \quad (56)$$

$$P_{asym_{S_n}}^{(1)} = 1 - \exp\left(-\frac{\Delta_7^{asym} \Omega_e}{\Omega_{|\widehat{h}_{B_i S_n}|^2} \alpha_n}\right), \quad (57)$$

$$P_{asym_{S_n}}^{(2)} = \begin{cases} 1 - \exp\left[-\dfrac{\left(\Omega_{|\widehat{h}_{B_i R_k}|^2}\Omega_e + \Omega_e^2\right)\Delta_7^{asym}}{\Omega_{|\widehat{h}_{R_k S_n}|^2}\left(\alpha_n \Omega_{|\widehat{h}_{B_i R_k}|^2} - \Omega_e \Delta_7^{asym}\right)}\right], \\ \quad \text{if } \alpha_n \Delta_1 - \Delta_4 \Delta_7^n > 0 \\ 0, \quad \text{if } \alpha_n \Delta_1 - \Delta_4 \Delta_7^n \le 0. \end{cases} \quad (58)$$

### C. OPTIMAL SOP IN THE PRESENCE OF UNTRUSTED RELAYS

Based on the communication process, we predict that when the transmit power is small, the channel capacities at the untrusted relay and IoTD are also small, i.e., the probability that the IoTDs receive the messages without eavesdropping is low. This leads to a low secrecy capacity, i.e., the secrecy performance is improved as the transmit power is increased. Nevertheless, the secrecy capacity will decrease if the transmit power of the BS is high since the untrusted relay can become an EAV and steal the confidential communications between the BS and the IoTDs. Thus, the SOP will increase again. Therefore, an optimal transmit power exists such that the considered system can achieve the best secrecy performance.

Accordingly, we propose the algorithm illustrated in **Algorithm 1** to determine the optimal transmit power at the BS such that the SOP is the lowest and that the transmit power at the BS is such that the SOP converges. In particular, the values of $\rho_B$ are split into an array $(\delta_b, \delta_e)$ with $\mathcal{I}$ elements, where $\delta_1 < \delta_2$ are the smallest and largest values of $\rho_B$, and the starting point of the SOP $\mathcal{O}_{sec}^{\Psi}$ is set to 1. Next, we update $\mathcal{O}_{sec}^{\Psi}(\ell_1)$ with respect to $\rho_B(\ell_1)$, where $\ell_1 \in (1, \mathcal{I})$. The iteration loop process will be stopped when $\mathcal{O}_{sec}^{\Psi}(\ell_1 + 1) > \mathcal{O}_{sec}^{\Psi}(\ell_1)$ with $\rho_B^*$, and the optimized transmit power is found using the formula $\mathcal{P}_B^{\Psi^*} = \rho_B^* N_0$.

Similarly, to determine the transmit power convergence, we update $\mathcal{O}_{sec}^{\Psi}(\ell_2)$ with respect to $\rho_B(\ell_2)$, where $\ell_2 \in (1, \mathcal{I})$. The iteration loop process will be stopped when $\mathcal{O}_{sec}^{\Psi}(\ell_1) - \mathcal{O}_{asym}^{\Psi} = \varepsilon$ ($\varepsilon \to 0$) with $\rho_{B_{conv}}$, and the converged transmit power is $\mathcal{P}_{B_{conv}}^{\Psi} = \rho_{B_{conv}} N_0$. Note that the aforementioned iteration process (lines 4-9 and 11-14) attempts to improve the accuracy of the approximations to a particular minimum in the original feasible region by using the element $\mathcal{I}$ and $\varepsilon$, i.e., the accuracy of the algorithm convergence is higher for larger $\mathcal{I}$ and smaller $\varepsilon$.

$$P_{asym_{S_m}}^{\mathrm{BBRR}(2)} = \begin{cases} 1 - \exp\left\{-\dfrac{\left(\Omega_{|\widehat{h}_{B_i R_k}|^2}\Omega_e + \Omega_e^2\right)\Delta_6^{asym}}{\Omega_{|\widehat{h}_{R_k S_m}|^2}\left[\alpha_m \Omega_{|\widehat{h}_{B_i R_k}|^2} - \left(\alpha_n \Omega_{|\widehat{h}_{B_i R_k}|^2} + \Omega_e\right)\Delta_6^{asym}\right]}\right\}, & \text{if } \alpha_m \Delta_1 - \Delta_2 \Delta_6^m > 0 \\ 0, & \text{if } \alpha_m \Delta_1 - \Delta_2 \Delta_6^m < 0. \end{cases} \quad (51)$$

**Algorithm 1** Algorithm for Determining the Optimized Transmit Power and Convergence

1: Set the initial array: $\rho_B(\ell) \in (\delta_b, \delta_e)$;
2: Set the initial step: $\ell_1, \ell_2 \leftarrow 1$;
3: Set the initial value: $\mathcal{O}^* \leftarrow 1$ and $\varepsilon \leftarrow 0.001$;
4: Set the initial value: $\mathcal{O}^{\Psi}_{asym}$ according to (48)−(50);
5: **repeat**
6: Update $\mathcal{O}^{\Psi}_{sec}(\ell_1)$ with respect to $\rho_B(\ell_1)$ according to (43), (44), and (47);
7: $\mathcal{O}^{\Psi} \leftarrow \mathcal{O}^{\Psi}_{sec}(\ell_1)$
8: $\ell_1 = \ell_1 + 1$;
9: Update $\mathcal{O}^{\Psi}_{sec}(\ell_1)$ with respect to $\rho_B(\ell_1)$ according to (43), (44), and (47);
10: **until** $\mathcal{O}^{\Psi}_{sec}(\ell_1) > \mathcal{O}^{\Psi}$;
11: $\mathcal{P}^{\Psi^*}_B = N_0\rho_B(\ell_1)$ and $\mathcal{O}^{\Psi^*}_{sec} = \mathcal{O}^{\Psi}_{sec}(\ell_1)$;
12: **repeat**
13: $\ell_2 = \ell_2 + 1$;
14: Update $\mathcal{O}^{\Psi}_{sec}(\ell_2)$ with respect to $\rho_B(\ell_2)$ according to (43), (44), and (47);
15: **until** $\mathcal{O}^{\Psi}_{sec}(\ell_2) - \mathcal{O}^{\Psi}_{asym} = \varepsilon$;
16: $\mathcal{P}^{\Psi}_{B_{conv}} = N_0\rho_B(\ell_2)$ and $\mathcal{O}^{\Psi}_{conv} = \mathcal{O}^{\Psi}_{conv}(\ell_2)$;
17: **return** $\mathcal{P}^{\Psi^*}_B$, $\mathcal{O}^{\Psi^*}_{sec}$, $\mathcal{P}^{\Psi}_{B_{conv}}$, and $\mathcal{O}^{\Psi}_{conv}$.

## V. SYSTEM PERFORMANCE ANALYSIS

### A. OUTAGE PROBABILITY

The IoTDs combine the signals from the BS and the selected untrusted relay by using SC at the second phase in the communication process. Therefore, an outage event for the pair IoTDs, i.e., $m$-th IoTD $S_m$ and $n$-th IoTD $S_n$, can be interpreted as either $S_m$ or $S_n$ cannot decode its own message [41]. Based on the above explanation, the outage probability of the considered IoT system is expressed as follows:

$$\mathcal{O}^{\Psi}_{op} = 1 - \left(1 - \underbrace{\Pr\left\{C_{op_{S_m}} < \lambda_{op_{S_m}}\right\}}_{\mathcal{O}^{\Psi}_{op_{S_m}}}\right) \times \left(1 - \underbrace{\Pr\left\{C_{op_{S_n}} < \lambda_{op_{S_n}}\right\}}_{\mathcal{O}_{op_{S_n}}}\right), \quad (59)$$

where $\lambda_{op_{S_m}}$ and $\lambda_{op_{S_n}}$ are the target rates at $S_m$ and $S_n$, respectively. Here, without loss of generality, we set $\tau = 1/2$, which is the similar to conventional relay systems [5], [38]; thus, $C_{op_{S_m}}$ and $C_{op_{S_n}}$ are defined as

$$C_{op_{S_m}} = \tau \log\left(1 + \max\left\{\frac{\alpha_m\rho_B|\widehat{h}_{B_iS_m}|^2}{\alpha_n\rho_B|\widehat{h}_{B_iS_m}|^2+\Delta_5}, \frac{\alpha_m\Delta_1|\widehat{h}_{R_kS_m}|^2}{|\widehat{h}_{R_kS_m}|^2\Delta_2+\Delta_3}\right\}\right), \quad (60)$$

$$C_{op_{S_n}} = \tau \log\left(1 + \max\left\{\frac{\alpha_n\rho_B|\widehat{h}_{B_iS_n}|^2}{\Delta_5}, \frac{\alpha_n\Delta_1|\widehat{h}_{R_kS_n}|^2}{|\widehat{h}_{R_kS_n}|^2\Delta_4+\Delta_3}\right\}\right). \quad (61)$$

Similar to (43), (44), and (47), the outage probabilities of $S_m$ and $S_n$ pair for RBBR, BBRR, and BBBR are obtained as follows:

$$\mathcal{O}^{\text{RBBR}}_{op} = 1 - \left(1 - P^{\text{RBBR}(1)}_{op_{S_m}}P^{\text{RBBR}(2)}_{op_{S_m}}\right) \times \left(1 - P^{(1)}_{op_{S_n}}P^{(2)}_{op_{S_n}}\right), \quad (62)$$

$$\mathcal{O}^{\text{BBRR}}_{op} = 1 - \left(1 - P^{\text{BBRR}(1)}_{op_{S_m}}P^{\text{BBRR}(2)}_{op_{S_m}}\right) \times \left(1 - P^{(1)}_{op_{S_n}}P^{(2)}_{op_{S_n}}\right), \quad (63)$$

$$\mathcal{O}^{\text{BBBR}}_{op} = 1 - \left(1 - P^{\text{BBRR}(1)}_{op_{S_m}}P^{\text{RBBR}(2)}_{op_{S_m}}\right) \times \left(1 - P^{(1)}_{op_{S_n}}P^{(2)}_{op_{S_n}}\right), \quad (64)$$

where $P^{\text{BBBR}(1)}_{op_{S_m}} = P^{\text{BBRR}(1)}_{op_{S_m}}$, $P^{\text{BBBR}(2)}_{op_{S_m}} = P^{\text{RBBR}(2)}_{op_{S_m}}$, $\Delta_8 = 2^{\lambda_{op_{S_m}}/\tau} - 1$, and $\Delta_9 = 2^{\lambda_{op_{S_n}}/\tau} - 1$; and $P^{\text{RBBR}(1)}_{op_{S_m}}$, $P^{\text{RBBR}(2)}_{op_{S_m}}$, $P^{\text{BBRR}(1)}_{op_{S_m}}$, $P^{\text{BBRR}(2)}_{op_{S_m}}$, $P^{(1)}_{op_{S_n}}$, and $P^{(2)}_{op_{S_n}}$ are respectively defined as follows:

$$P^{\text{RBBR}(1)}_{op_{S_m}} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_5\Delta_8}{\Omega_{|\widehat{h}_{B_iS_m}|^2}(\alpha_m\rho_B - \alpha_n\rho_B\Delta_8)}\right], \\ \quad \text{if } \alpha_m - \alpha_n\Delta_8 > 0 \\ 0, \quad \text{if } \alpha_m - \alpha_n\Delta_8 \le 0, \end{cases} \quad (65)$$

$$P^{\text{BBBR}(2)}_{op_{S_m}} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_3\Delta_8}{\Omega_{|\widehat{h}_{R^*S_m}|^2}(\alpha_m\Delta_1 - \Delta_2\Delta_8)}\right], \\ \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 > 0 \\ 0, \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 \le 0, \end{cases} \quad (66)$$

$$P^{\text{RBBR}(2)}_{op_{S_m}} = \prod_{k=1}^{K} P^{\text{BBBR}(2)}_{S_m}, \quad (67)$$

$$P^{\text{BBRR}(1)}_{op_{S_m}} = \prod_{i=1}^{I} P^{\text{RBBR}(1)}_{S_m}, \quad (68)$$

$$P^{\text{BBBR}(2)}_{op_{S_m}} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_3\Delta_8}{\Omega_{|\widehat{h}_{R^*S_m}|^2}(\alpha_m\Delta_1 - \Delta_2\Delta_8)}\right], \\ \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 > 0 \\ 0, \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 \le 0, \end{cases} \quad (69)$$

$$P^{(1)}_{op_{S_n}} = 1 - \exp\left(-\frac{\Delta_9\Delta_5}{\Omega_{|\widehat{h}_{B_iS_n}|^2}\alpha_n\rho_B}\right), \quad (70)$$

Similar to (43), (44), and (47), the outage probabilities of $S_m$ and $S_n$ pair for RBBR, BBRR, and BBBR are obtained as follows:

$$\mathcal{O}^{\text{RBBR}}_{op} = 1 - \left(1 - P^{\text{RBBR}(1)}_{op_{S_m}}P^{\text{RBBR}(2)}_{op_{S_m}}\right) \times \left(1 - P^{(1)}_{op_{S_n}}P^{(2)}_{op_{S_n}}\right), \quad (62)$$

$$\mathcal{O}^{\text{BBRR}}_{op} = 1 - \left(1 - P^{\text{BBRR}(1)}_{op_{S_m}}P^{\text{BBRR}(2)}_{op_{S_m}}\right) \times \left(1 - P^{(1)}_{op_{S_n}}P^{(2)}_{op_{S_n}}\right), \quad (63)$$

$$\mathcal{O}^{\text{BBBR}}_{op} = 1 - \left(1 - P^{\text{BBRR}(1)}_{op_{S_m}}P^{\text{RBBR}(2)}_{op_{S_m}}\right) \times \left(1 - P^{(1)}_{op_{S_n}}P^{(2)}_{op_{S_n}}\right), \quad (64)$$

where $P^{\text{BBBR}(1)}_{op_{S_m}} = P^{\text{BBRR}(1)}_{op_{S_m}}$, $P^{\text{BBBR}(2)}_{op_{S_m}} = P^{\text{RBBR}(2)}_{op_{S_m}}$, $\Delta_8 = 2^{\lambda_{op_{S_m}}/\tau} - 1$, and $\Delta_9 = 2^{\lambda_{op_{S_n}}/\tau} - 1$; and $P^{\text{RBBR}(1)}_{op_{S_m}}$, $P^{\text{RBBR}(2)}_{op_{S_m}}$, $P^{\text{BBRR}(1)}_{op_{S_m}}$, $P^{\text{BBRR}(2)}_{op_{S_m}}$, $P^{(1)}_{op_{S_n}}$, and $P^{(2)}_{op_{S_n}}$ are respectively defined as follows:

$$P^{\text{RBBR}(1)}_{op_{S_m}} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_5\Delta_8}{\Omega_{|\widehat{h}_{B_iS_m}|^2}(\alpha_m\rho_B - \alpha_n\rho_B\Delta_8)}\right], \\ \quad \text{if } \alpha_m - \alpha_n\Delta_8 > 0 \\ 0, \quad \text{if } \alpha_m - \alpha_n\Delta_8 \le 0, \end{cases} \quad (65)$$

$$P^{\text{BBBR}(2)}_{op_{S_m}} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_3\Delta_8}{\Omega_{|\widehat{h}_{R^*S_m}|^2}(\alpha_m\Delta_1 - \Delta_2\Delta_8)}\right], \\ \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 > 0 \\ 0, \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 \le 0, \end{cases} \quad (66)$$

$$P^{\text{RBBR}(2)}_{op_{S_m}} = \prod_{k=1}^{K} P^{\text{BBBR}(2)}_{S_m}, \quad (67)$$

$$P^{\text{BBRR}(1)}_{op_{S_m}} = \prod_{i=1}^{I} P^{\text{RBBR}(1)}_{S_m}, \quad (68)$$

$$P^{\text{BBBR}(2)}_{op_{S_m}} = \begin{cases} 1 - \exp\left[-\dfrac{\Delta_3\Delta_8}{\Omega_{|\widehat{h}_{R^*S_m}|^2}(\alpha_m\Delta_1 - \Delta_2\Delta_8)}\right], \\ \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 > 0 \\ 0, \quad \text{if } \alpha_m\Delta_1 - \Delta_2\Delta_8 \le 0, \end{cases} \quad (69)$$

$$P^{(1)}_{op_{S_n}} = 1 - \exp\left(-\frac{\Delta_9\Delta_5}{\Omega_{|\widehat{h}_{B_iS_n}|^2}\alpha_n\rho_B}\right), \quad (70)$$

$$P_{op_{S_n}}^{(2)} = \begin{cases} 1-\exp\left[-\dfrac{\Delta_3\Delta_9}{\Omega_{|\widehat{h}_{R_k S_n}|^2}(\alpha_n\Delta_1-\Delta_4\Delta_9)}\right], \\ \quad \text{if } \alpha_n\Delta_1-\Delta_4\Delta_9 > 0 \\ 0, \quad \text{if } \alpha_n\Delta_1-\Delta_4\Delta_9 \le 0. \end{cases} \quad (71)$$

### B. THROUGHPUT ANALYSIS

In this subsection, we study the throughput to estimate how fast the system can be achieved under the optimal SOP. The BS and untrusted relays transmit signals at a constant rate, and the system throughput is subjective to the impact of outage probability. To consider the delay-limited mode for practical implementations, the system throughput is investigated, and this important metric is formulated as [41]

$$\Gamma^{\Psi} = \left(1-\mathcal{O}_{op_{S_m}}^{\Psi}\right)\Delta_8 + \left(1-\mathcal{O}_{op_{S_n}}^{\Psi}\right)\Delta_9. \quad (72)$$

## VI. NUMERICAL RESULTS

In this section, we provide insightful numerical results for evaluating the secrecy performance and throughput of the EH untrusted relay IoT system. In particular, we investigate the impacts of $\rho_B$, the EH time, the number of BS antennas, the number of untrusted relays, and the predefined threshold on the SOP, the outage probability, and the throughput of the pairs of IoTDs $S_m$ and $S_n$.

Unless otherwise stated, we investigate the considered system in a square of unit area. The coordinates of the gateway and $\pi$-th IoTD are $B$ (0.0, 0.0) and $S_\pi$ $(A_\pi, B_\pi)$, respectively. The selected untrusted relay is collocated at $R_k$ $(A_k, B_k)$. The path-loss exponent of the considered system that is placed in free space is equal to 2 [33]. The following system parameters are used for both the analysis and simulation [31], [43], [54]: $(A_m, B_m) \in \{(0.6, 0.0), (0.6, 0.1), (0.6, 0.2)\}$, $(A_n, B_n) \in \{(0.5, 0.0), (0.5, 0.1), (0.5, 0.2)\}$, and $(A_k, B_k) \in \{(0.4,0.0),(0.4,0.1), (0.4,0.2), (0.4,0.3), (0.4,0.4), (0.4, 0.5), (0.4, 0.55), (0.4, 0.6)\}$; the EH efficiency coefficients $\eta \in (0, 1)$; the fractions of the EH time $\tau \in (0, 1)$; the power-splitting ratio $\mu \in (0, 1)$; $\rho_B \in [-20, 40]$ (dB); the secrecy thresholds for decoding $x_m$ and $x_n$ are $\lambda_{sec_{S_m}} = 0.01$ (kbps) and $\lambda_{sec_{S_n}} = 0.02$ (kbps), respectively; the predefined thresholds of IoTDs for successfully decoding $x_m$ and $x_n$ are $\lambda_{op_{S_m}} \in (0.01, 0.5)$ (kbps) and $\lambda_{op_{S_n}} \in (0.01, 0.5)$ (kbps), respectively; the number of BS antennas $I \in \{2, 5, 8\}$; and the number of untrusted relays $K \in \{2, 5, 8\}$. Note that we evaluated and compared the three schemes as follows:

- RBBR: A random antenna and the best untrusted relay from $I$ antennas of the BS and from $K$ untrusted relays, respectively, are selected to transfer information to the IoTDs.
- BBRR: The best antenna and a random untrusted relay from $I$ antennas of the BS and from $K$ untrusted relays, respectively, are selected to transfer information to the IoTDs.
- BBBR: The best antenna and the best untrusted relay from $I$ antennas of the BS and from $K$ untrusted relays, respectively, are selected to transfer information to the IoTDs.

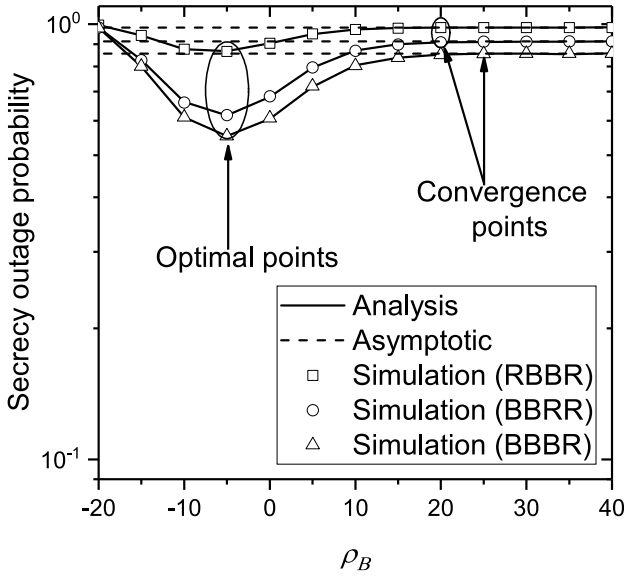


**FIGURE 3.** The effects of $\rho_B$ on the SOP with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\mu = 0.6$, $\tau = 0.4$, $\eta = 0.8$, $I = 5$, and $K = 5$.

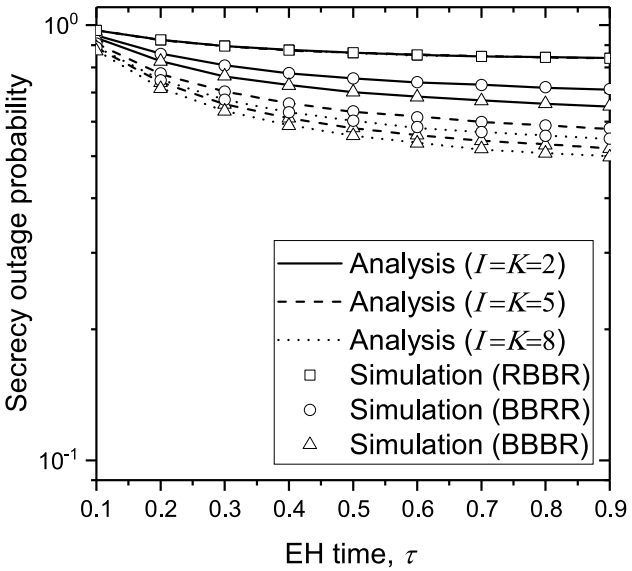


**FIGURE 4.** The effects of the EH time $\tau$ on the SOP with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\mu = 0.6$, $\rho_B = -5$ (dB), $\eta = 0.8$, $I = 5$, and $K = 5$.

Fig. 3 plots the SOP curves for different $\rho_B$ of the RBBR, BBRR, and BBBR. The SOP of the BBBR is better than that of the BBRR and RBBR. This is because the BBBR chooses the best antenna of the BS and the best untrusted relay to send signals to the IoTDs, i.e., this scheme obtains the best diversity gain among the three schemes. Furthermore, the secrecy performance of BBRR outperforms that of RBBR. This is because the untrusted relays can steal the confidential communications from the BS-to-IoTD links; hence, the BS's antenna selection is more effective than untrusted relay selection. This trend applies to all SOP simulations.

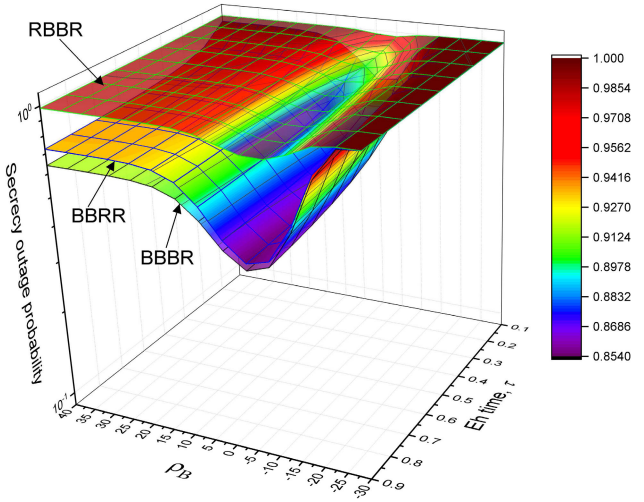


**FIGURE 5.** The effects of $\rho_B$ and the EH time $\tau$ on the SOP with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\mu = 0.6$, $\eta = 0.8$, $I = 5$, and $K = 5$.

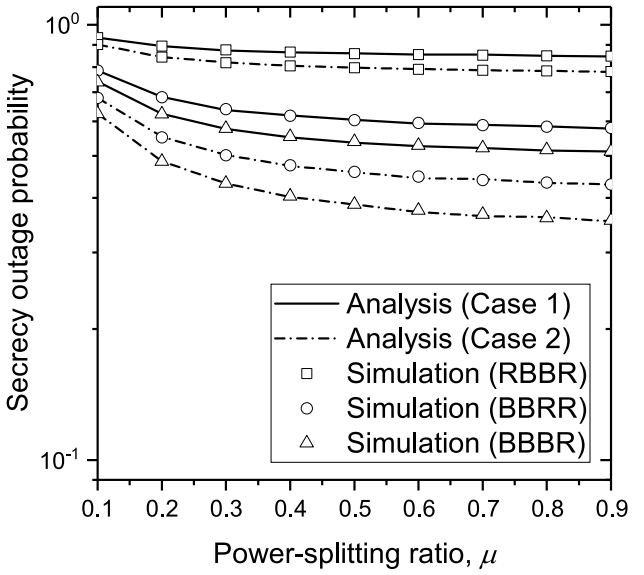


**FIGURE 6.** The effects of the power-splitting ratio $\mu$ on the SOP with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\tau = 0.4$, $\rho_B = -5$ (dB), $\eta = 0.8$, $I = 5$, and $K = 5$.

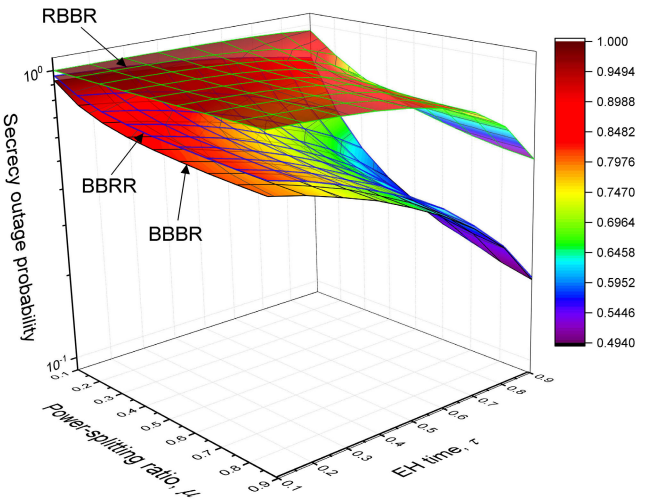


**FIGURE 7.** The effects of the power-splitting ratio $\mu$ and the EH time $\tau$ on the SOP with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\rho_B = -5$ (dB), $\eta = 0.8$, $I = 5$, and $K = 5$.

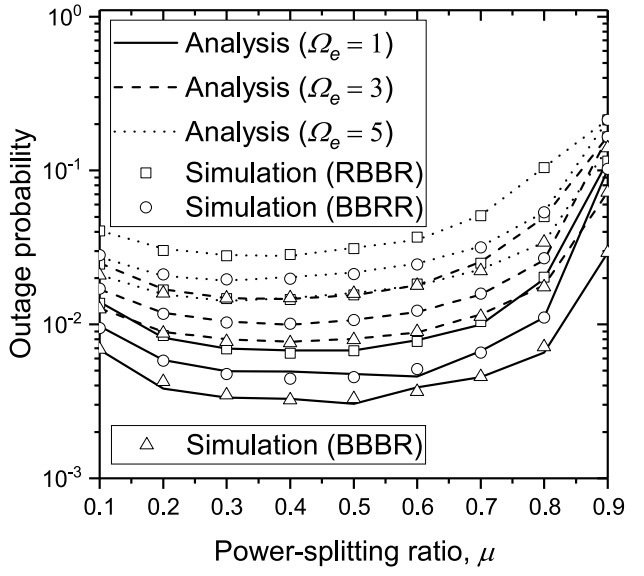


**FIGURE 8.** The effects of the power-splitting ratio $\mu$ and the channel estimation error $\Omega_e$ on the outage probability with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\rho_B = -5$ (dB), $\eta = 0.8$, $I = 5$, and $K = 5$.

In addition, the SOP of $\rho_B$ tends to 40 (dB), and the SOPs of the three schemes all decrease to the optimal point ($\rho_B = -5$(dB)) and then increase to close to the convergence point ($\rho_B = 20$(dB) for RBBR and BBRR and $\rho_B = 25$(dB) for BBBR), which is consistent with **Algorithm 1**.

Fig. 4 investigates the impact of the EH time on the SOP of RBBR, BBRR, and BBBR. It is obvious that the secrecy performance is improved as the EH time is increased. This is because the untrusted relays will harvest more energy when the EH time is higher. Furthermore, when the numbers of antennas of the BS and untrusted relays increases, the SOP is improved. It is easy to understand that the diversity gain will increase at the BS with the higher numbers of antennas and untrusted relays. In addition, to investigate the effects of both $\rho_B$ and $\tau$, we plot the 3-D figure in Fig. 5. Again, we can see that the SOP obtains the optimal point of $\rho_B = -5$(dB), and this point will decrease with increasing EH time.

Fig. 6 displays the curves of the SOP versus the power-splitting ratio $\mu$ under the three schemes in two cases. Case 1: the untrusted relays are near the BS, i.e., the coordinates of the relays are (0.4,0.0), (0.4,0.1), (0.4,0.2), (0.4,0.3), and (0.4,0.4). Case 2: the untrusted relays are far the BS, i.e., the coordinates of the relays are (0.4,0.2), (0.4,0.3), (0.4,0.4), (0.4,0.5), and (0.4,0.6). We can see that the SOP of case 1 is higher than that of case 2. This is because although the untrusted relays in case 1 harvest energy better than do those in case 2, the untrusted relays in case 1 also capture the confidential signal more easily than do those in case 2.

Furthermore, the SOPs of the three considered schemes decrease with increasing $\mu$. This result occurs because the EH

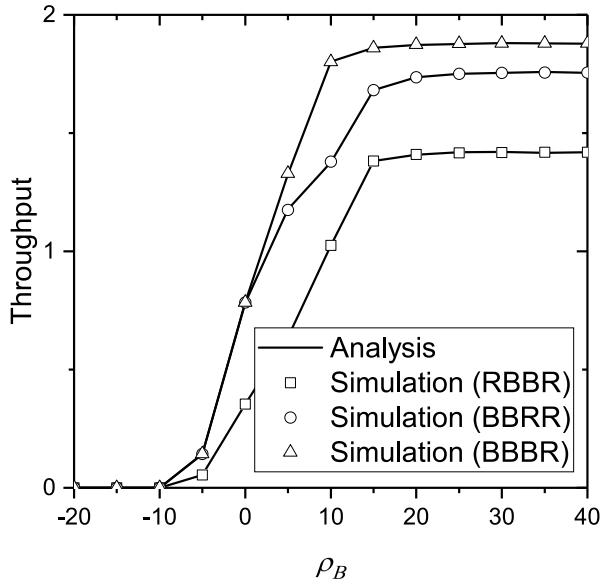


**FIGURE 9.** The effects of $\rho_B$ on the throughput with $\alpha_m = 0.7$, $\alpha_n = 0.3$, $\eta = 0.8$, $I = 5$, and $K = 5$.

power increases while the power for information processing decreases. This leads to a reduction in the received signal strength at the untrusted relays, and hence, the SOP decreases.

To illustrate this more clearly, we show the impact of $\mu$ and $\tau$ on the SOP in the 3-D figure in Fig. 7. We can see that the SOP is improved as either $\mu$ or $\tau$ increases. Furthermore, the SOP of the BBRR decreases to close to that of the BBBR as $\mu$ increases. When $\mu$ tends nearly to 1, the untrused relays do not have power for information process, i.e., the received signal at the IoTDs is only affected by the BS's antenna selection.

Fig. 8 depicts the outage probability variation with respect to the power-splitting ratio and the channel estimation error under three schemes, in which the optimal transmit power for ensuring satisfactory secrecy performance is fixed. It is observed that the outage probabilities of BBRR and BBBR are the same and better than that of RBBR. Furthermore, the outage probability decreases as the channel estimation error improves. The secrecy performance is better when the CSI is predicted to be more accurate.

Fig. 9 shows the impact of $\rho_B$ on the throughput for the three considered schemes. Similar to the SOP, we can see that the throughput of the BBBR is better than that of the remaining schemes. Furthermore, in contrast to the SOP, the throughputs are improved with increasing $\rho_B$ and unchanged when $\rho_B$ is sufficiently large. This is because the IoTDs more easily obtain the signal given the higher power of the BS. From Figs. 3 and 9, we can observe that the SOP is improved under the small transmit power, while this leads to low throughput. This is the trade-off between secrecy performance and throughput.

## VII. CONCLUSION

In this work, the secrecy and throughput of a cooperative EH untrusted relays IoT system using NOMA with imperfect CSI were analyzed. Three cooperative schemes (i.e., RBBR, BBRR, and BBBR) were introduced to analyze the secrecy and throughput of the considered IoT system. The closed-form expressions for the exact and asymptotic SOP were derived. Based on that, an algorithm for determining the transmit power optimization and convergence was proposed. The closed-form expressions for the throughput of the three considered schemes were also obtained and verified by Monte Carlo simulation results. The numerical examples show that the BBBR outperforms RBBR and BBRR when the secrecy performance and throughput metrics are investigated. In addition, the SOP and the throughput for the three schemes improves as the number of BS antennas and untrusted relays increase. For future work, we are currently considering the issue of adaptive power allocation for NOMA in IoT systems that consist of multiple relay clusters to improve the SOP and throughput for IoT application systems.

## APPENDIX A
## PROOF THE REMARK 1

Following the definition of conditional probability, the CDF of $U$ can be written as

$$F_U = \Pr\left\{\frac{a_1 V}{b_1 V + c_1} < u\right\} = \begin{cases} \Pr\left\{V < \dfrac{c_1 u}{a_1 - b_1 u}\right\}, & \text{if } a_1 - b_1 u > 0 \\ 0, & \text{if } a_1 - b_1 u < 0. \end{cases} \quad (73)$$

Substituting (2) into (73), the proof is complete.

## APPENDIX B
## PROOF THE REMARK 2

Similar to **Remark 1**, the CDF of $U^*$ can be written as

$$F_{U^*} = \begin{cases} \Pr\left\{\max\limits_{j=1,\cdots,J}\{V_j\} < \dfrac{c_2 u}{a_2 - b_2 u}\right\}, \\ \quad \text{if } a_2 - b_2 u > 0 \\ 0, \quad \text{if } a_2 - b_2 u < 0. \end{cases} \quad (74)$$

Adopting the definition of conditional probability, we have

$$F_{U^*} = \begin{cases} \prod\limits_{j=1}^{J} \Pr\left\{V_j < \dfrac{c_2 u}{a_2 - b_2 u}\right\}, \\ \quad \text{if } a_2 - b_2 u > 0 \\ 0, \quad \text{if } a_2 - b_2 u < 0. \end{cases} \quad (75)$$

Substituting (2) into (75), the proof is complete.

## REFERENCES

[1] Y. Wang, W. Yang, X. Shang, J. Hu, Y. Huang, and Y. Cai, "Energy-efficient secure transmission for wireless powered Internet of things with multiple power beacons," *IEEE Access*, vol. 6, pp. 75086–75098, 2018.
[2] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.
[3] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Information*, vol. 7, no. 3, p. 49, Aug. 2016.
[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[5] H. Hu, Z. Gao, X. Liao, and V. C. M. Leung, "Secure communications in CIoT networks with a wireless energy harvesting untrusted relay," *Sensors*, vol. 17, no. 9, pp. 1–21, Sep. 2017.

[6] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[7] L. Li, Y. Xu, Z. Zhang, J. Yin, W. Chen, and Z. Han, "A prediction-based charging policy and interference mitigation approach in the wireless powered Internet of Things," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 439–451, Feb. 2019.

[8] B. Ji, Y. Li, B. Zhou, C. Li, K. Song, and H. Wen, "Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting," *IEEE Access*, vol. 7, pp. 38738–38747, 2019.

[9] I. Khan, "Performance analysis of 5G cooperative-NOMA for IoT-intermittent communication," *Int. J. Commun. Netw. Inf. Secur.*, vol. 9, no. 3, pp. 314–322, Dec. 2017.

[10] E. Hossain and Y. Al-Eryani, "Large-scale NOMA: Promises for massive machine-type communication," in *Proc. IEEE COMSOC TCCN Newslett.*, Richmond, VA, USA, Jan. 2019, pp. 1–5.

[11] R. Abozariba, M. K. Naeem, M. Patwary, M. Seyedebrahimi, and P. Bull, "NOMA-based resource allocation and mobility enhancement framework for IoT in next generation cellular networks," *IEEE Access*, vol. 7, pp. 29158–29172, 2019.

[12] Z. Chen, Z. Ding, X. Dai, and R. Zhang, "A mathematical proof of the superiority of NOMA compared to conventional OMA," *IEEE Trans. Signal Process.*, pp. 1–28, Oct. 2016. [Online]. Available: https://arxiv.org/abs/1612.01069

[13] M. Zeng, A. Yadav, O. A. Dobre, G. I. Tsiropoulos, and H. V. Poor, "On the sum rate of MIMO-NOMA and MIMO-OMA systems," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 534–537, Aug. 2017.

[14] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, Jan. 2014, pp. 1–5.

[15] N. Garg and R. Garg, "Energy harvesting in IoT devices: A survey," in *Proc. Int. Conf. Intell. Sustain. Syst.*, Palladam, India, Dec. 2017, pp. 127–131.

[16] B. Alzahrani and W. Ejaz, "Resource management for cognitive IoT systems with RF energy harvesting in smart cities," *IEEE Access*, vol. 6, pp. 62717–62727, 2018.

[17] A. Rauniyar, P. Engelstad, and O. N. Østerbø, "RF energy harvesting and information transmission based on NOMA for wireless powered IoT relay systems," *Sensors*, vol. 18, p. 3254, Sep. 2018.

[18] X. Song, L. Dong, J. Wang, L. Qin, and X. Han, "Energy efficient power allocation for downlink NOMA heterogeneous networks with imperfect CSI," *IEEE Access*, vol. 7, pp. 39329–39340, 2019.

[19] D.-D. Tran, D.-B. Ha, V. N. Vo, C. So-In, H. Tran, T. G. Nguyen, Z. Baig, and S. Sanguanpong, "Performance analysis of DF/AF cooperative MISO wireless sensor networks with NOMA and SWIPT over Nakagami-*m* fading," *IEEE Access*, vol. 6, pp. 56142–56161, 2018.

[20] 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.

[21] 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. 11862–11872, 2018.

[22] 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.

[23] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Telecommun. Conf.*, New Orleans, LO, USA, Nov./Dec. 2008, pp. 1–5.

[24] V. N. Vo, T. G. Nguyen, C. So-In, and H. Tran, "Outage performance analysis of energy harvesting wireless sensor networks for NOMA transmissions," *Mobile Netw. Appl.*, pp. 1–19, Dec. 2018, to be published. doi: 10.1007/s11036-018-1188-7.

[25] Z. Xiang, W. Yang, Y. Cai, Y. Cheng, H. Wu, and M. Wang, "Exploiting uplink NOMA to improve sum secrecy throughput in IoT networks," *Wireless Commun. Mobile Comput.*, vol. 2018, Jul. 2018, Art. no. 9637610.

[26] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, "Secure cooperative communications with an untrusted relay: A NOMA-inspired jamming and relaying approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3191–3205, Dec. 2019.

[27] V. N. Vo, D.-D. Tran, C. So-In, and H. Tran, "Secrecy performance analysis for fixed-gain energy harvesting in an Internet of Things with untrusted relays," *IEEE Access*, vol. 6, pp. 48247–48258, 2018.

[28] M. T. Mamaghani, A. Kuhestani, and K.-K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Trans. Veh. Technol.*, pp. 1–14, Feb. 2018.

[29] D.-T. Do and M.-S. Van Nguyen, "Impact of untrusted relay on physical layer security in non-orthogonal multiple access networks," *Wireless Pers. Commun.*, vol. 106, no. 3, pp. 1353–1372, Jun. 2019.

[30] T. A. Le and H. Y. Kong, "Secrecy analysis of a cooperative NOMA network using an EH untrusted relay," *Int. J. Electron.*, vol. 106, pp. 799–815, Feb. 2019.

[31] T. D. Hieu, T. T. Duy, and B.-S. Kim, "Performance enhancement for multihop harvest-to-transmit WSNs with path-selection methods in presence of eavesdroppers and hardware noises," *IEEE Sensors J.*, vol. 18, no. 12, pp. 5173–5186, Jun. 2018.

[32] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[33] J. Miranda, R. Abrishambaf, T. Gomes, P. Gonçalves, J. Cabral, A. Tavares, and J. Monteiro, "Path loss exponent analysis in wireless sensor networks: Experimental evaluation," in *Proc. IEEE Int. Conf. Ind. Inform.*, Bochum, Germany, Jul. 2013, pp. 54–58.

[34] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[35] 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.

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

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

[38] Y. Ye, Y. Li, F. Zhou, N. Al-Dhahir, and H. Zhang, "Power splitting-based SWIPT with dual-hop DF relaying in the presence of a direct link," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1316–1319, Jun. 2019.

[39] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[40] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[41] X. Yue, Y. Liu, S. Kang, and A. Nallanathan, "Performance analysis of NOMA with fixed gain relaying over Nakagami-*m* fading channels," *IEEE Access*, vol. 5, pp. 5445–5454, 2017.

[42] V. N. Q. Bao, T. Q. Duong, and C. Tellambura, "On the performance of cognitive underlay multihop networks with imperfect channel state information," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4864–4873, Dec. 2013.

[43] D.-T. Do, M. Vaezi, and T.-L. Nguyen, "Wireless powered cooperative relaying using NOMA with imperfect CSI," in *Proc. IEEE Globecom Workshops*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.

[44] W. Cai, C. Chen, L. Bai, Y. Jin, and J. Choi, "User selection and power allocation schemes for downlink NOMA systems with imperfect CSI," in *Proc. IEEE Veh. Technol. Conf.*, Montreal, QC, Canada, Sep. 2016, pp. 1–5.

[45] S. Guo and X. Zhou, "Robust resource allocation with imperfect channel estimation in NOMA-based heterogeneous vehicular networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2321–2332, Mar. 2019.

[46] D.-B. Ha and S. Q. Nguyen, "Outage performance of energy harvesting DF relaying NOMA networks," *Mobile Netw. Appl.*, vol. 23, no. 6, pp. 1572–1585, Dec. 2017. doi: 10.1007/s11036-017-0922-x.

[47] M. O. Hasna and M. S. Alouini, "A performance study of dual-hop transmissions with fixed gain relays," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1963–1968, Nov. 2004.

[48] O. S. Badarneh, "On the performance of fixed-gain amplify-and-forward dual-hop relaying in wireless networks with beamforming," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Istanbul, Turkey, Apr. 2014, pp. 3112–3117.
[49] T.-N. Tran and M. Voznak, "HD/FD and DF/AF with fixed-gain or variable-gain protocol switching mechanism over cooperative NOMA for green-wireless networks," *Sensors*, vol. 19, no. 8, p. 1845, Apr. 2019.
[50] A. Koç, İ. Altunbac, and A. Yongaçoğlu, "Outage performance of fixed-gain and variable-gain AF full-duplex relaying in non-identical Nakagami-*m* fading channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2017, Jun. 2017, Art. no. 110.
[51] G. K. Karagiannidis, "Performance bounds of multihop wireless communications with blind relays over generalized fading channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 3, pp. 498–503, Mar. 2006.
[52] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.
[53] Q. Wang, J. Liu, C. Zhai, S. Ma, and S. Yu, "Outage probability analysis of selection combining over generalized correlated Weibull fading channels," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process.*, Chengdu, China, Jul. 2015, pp. 591–595.
[54] N. T. Van, T. N. Do, V. N. Q. Bao, and B. An, "Performance analysis of wireless energy harvesting multihop cluster-based networks over Nakagami-*m* fading channels," *IEEE Access*, vol. 6, pp. 3068–3084, 2017.

**VAN NHAN VO** received the B.S. degree from in computer science from Danang University, Da Nang, Vietnam, in 2006, and the M.S. degree in computer science from Duy Tan University, Da Nang, in 2014. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Faculty of Science, Khon Kaen University, Thailand. Since 2009, he has taught and studied at Duy Tan University. His research interests include information security, physical layer secrecy, radio frequency energy harvesting, nonorthogonal multiple access, wireless sensor networks, the Internet of Things, and the security of other advanced communication systems.

**CHAKCHAI SO-IN** (SM'14) received the Ph.D. degree in computer engineering from the Washington University in St. Louis, MO, USA, in 2010. He was an Intern with CNAP-NTU (SG), Cisco Systems, WiMAX Forums, and Bell Labs, USA. He is currently a Professor with the Department of Computer Science, Khon Kaen University. He has authored over 100 publications and ten books, including some in the IEEE JSAC, IEEE magazines, and *Computer Networks/Network Security*. His research interests include mobile computing, wireless/sensor networks, signal processing, and computer networking and security. He has served as a Committee Member for many conferences/journals, such as Globecom, ICC, VTC, WCNC, ICNP, ICNC, PIMRC, IEEE Transactions, IEEE letter/magazines, and *Computer Networks and Communications*. He has served as an Editor for *PLOS One*, *SpringerPlus*, *PeerJ*, and ECTI-CIT.

**HUNG TRAN** received the B.S. and M.S. degrees in information technology from Vietnam National University, Hanoi, in 2002 and 2006, respectively, and the Ph.D. degree from the School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden, in 2013. In 2014, he joined the Electrical Engineering Department, École de Technologie Supérieure, Montreal, Canada. He is currently a Postdoctoral Researcher with Mälardalen University, Sweden. His research interests include cognitive radio networks, cooperative communication systems, millimeter-wave communications, energy harvesting, and security communications at the physical layer.

**DUC-DUNG TRAN** received the B.E. degree in electronics and telecommunications from Hue University of Sciences, Vietnam, in 2013, and the M.Sc. degree in computer sciences from Duy Tan University, Da Nang, Vietnam, in 2016. He joined the Faculty of Electrical and Electronics Engineering, Duy Tan University, in 2015. From 2013 to 2014, he was an Assistant Researcher with the Institute of Research and Development, Duy Tan University. His research interests include the secrecy of physical layer communications, wireless communications, MIMO systems, and wireless energy harvesting networks.

**SOVANNARITH HENG** received the B.S. degree from the Royal University of Phnom Penh, in 2005, and the M.S. degree from the Ateneo de Manila University, in 2010. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Khon Kaen University, Thailand. His research interests include image processing, wireless multimedia sensor networks, computer networks, and distributed systems.

**PHET AIMTONGKHAM** received the B.S. and M.S. degrees in computer science and information technology from Khon Kaen University, Thailand, in 2013 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the Department of Computer Science, Faculty of Science. He is the Founder of Advanced Internetworking Company Ltd. His research interests include computer networking, multimedia networks, wireless sensor networks, and the Internet of Things.

**ANH-NHAT NGUYEN** received the B.S. degree in computer science from Duy Tan University, Da Nang, Vietnam, in 2012, and the M.S. degree in computer science from the Huazhong University of Science and Technology (HUST), China, in 2018. He is currently pursuing the Ph.D. degree with the Department of Information Technology, Faculty of Science, Khon Kaen University, Thailand. His research interests include image processing, information security, physical layer secrecy, RF-EH, and wireless sensor networks.