IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 1, 2018, accepted August 15, 2018, date of publication August 28, 2018, date of current version September 21, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2867500

Secrecy Performance Analysis for Fixed-Gain Energy Harvesting in an Internet of Things With Untrusted Relays

VAN NHAN VO[1,2], DUC-DUNG TRAN[3], CHAKCHAI SO-IN[2], (Senior Member, IEEE), AND HUNG TRAN[4]

[1]International School, Duy Tan University, Danang 550000, Vietnam
[2]Applied Network Technology Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[3]Faculty of Electrical and Electronics Engineering, Duy Tan University, Danang 550000, Vietnam
[4]School of Innovation, Design and Engineering, Mälardalen University, 72123 Västerås, Sweden

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

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

ABSTRACT In this paper, the radio frequency energy harvesting (EH) and security issues in Internet of Things (IoT) sensor networks with multiple untrusted relays are considered. In particular, the communication protocol is divided into two phases. The first phase is used for EH, in which the IoT sensor nodes (SNs) and relays harvest energy from multiple power transfer stations. The second phase is used for information transmission in two steps: 1) the selected SN uses the harvested energy to broadcast information to the controller and the relays, and 2) the selected relay forwards information to the controller by applying the amplify-and-forward protocol to improve the quality of the communication between the SN and the controller. During information transmission, the controller is at risk of losing information because the relay may act as an eavesdropper (namely, an untrusted relay). Thus, to improve the secrecy performance of the considered system, we propose an optimal scheme, namely, best-sensor-best-untrusted-relay (BSBR) and compare this scheme with random-sensor-random-untrusted-relay and a threshold-based scheme. The closed-form expressions for the secrecy outage probability (SOP) and secrecy throughput (ST) are obtained and verified through Monte Carlo simulations to confirm the superior performance of our approach. EH time optimization and the target secrecy rate optimization algorithms are also proposed. In addition, the impacts of the EH time, the EH efficiency coefficient, the numbers of SNs and untrusted relays, and the target secrecy rate on the SOP and the ST are investigated. The results indicate that the BSBR generally outperforms the two baseline schemes in terms of the SOP and ST.

INDEX TERMS Energy harvesting, Internet of Things sensor networks, untrusted relay, physical layer security.

I. INTRODUCTION

IoT has recently received considerable interest from the research community [1]–[5]. IoT is expected to improve human life because IoT connects various physical objects (e.g., sensors, robots, and mobile phones) to provide information and track the activity of monitored objects at any time and place [6]. However, IoT devices have faced energy limitations due to resource constraints [7]. Thus, EH and relay transmission are potential solutions to prolong the lifetimes of IoT devices [8], [9].

The EH in IoT sensor networks (ISNs) is a process by which the energy from the surrounding environment (e.g., solar, wind, and radio frequency (RF)) is converted into electrical energy to maintain an IoT device's operations [10]. Among such processes, RF EH is of high interest due to its availability and flexible characteristics for transmitting energy [11]–[13].

For example, Wang *et al*. studied the EH issue in IoT by investigating three types of IoT devices, i.e., devices that only receive information, that only receive energy, and that can receive information and energy simultaneously from a controller [12]. More generally, Kamalinejad *et al*. surveyed technologies and strategies to enable wireless EH for ISNs. They considered two different scenarios, i.e., uniform

distribution in a ring topology and randomly distributed multihop topology, and then investigated the performance of the wireless EH unit and the energy consumption of IoT devices [13].

Relay transmission is a potential technique for saving transmit power for SNs to further enhance the network lifetime [14]–[16]. For instance, Luo *et al*. investigated the network lifetime in a multihop ISN-based IoT consisting of multiple SNs and a sink. They first proposed the optimal energy strategy, and then the optimal energy strategy was designed for the relay node to prolong the lifetime for the ISN [15]. Guo *et al*. considered an ISN with a source, a relay node, and a destination to investigate the energy efficiency of information transfer between SNs. They then adopted state-of-the-art research in simultaneous wireless energy and information transfer to improve the energy performance [16].

However, in some cases, the SN and controller do not have the same security clearance as the relay because they belong to a heterogeneous network [17]. Thus, the relay can also be viewed as a potential eavesdropper, which is called an untrusted relay [18]. Confidential information in the system can be leaked due to monitoring by the untrusted relay [19]. To mitigate this problem, information-theoretic security, physical layer security (PLS), has been recognized as a promising method due to its low complexity and effective characteristics [20]–[25].

Mukherjee provided an overview of low-complexity PLS schemes that are suitable for an ISN, which is modeled as two scenarios: uplink communications from SNs to the controller and downlink communications from the controller to actuators [23]. Soni *et al*. presented IoT concepts such as IoT elements, architecture, and communication standards. They then surveyed existing wireless attack approaches and wireless security techniques. Subsequently, they considered the applicability of wireless PLS techniques to achieve security for ISNs [24].

Zhong *et al*. investigated the PLS for IoT in multitier ultradense heterogeneous networks. They derived the cumulative distribution function (CDF) of the receiving signal-to-interference-plus-noise ratio (SINR) for IoT users and eavesdroppers, and then, they derived the SOP for an arbitrary IoT user to investigate secrecy performance [25]. However, studies conducting PLS analysis for RF EH with multiple untrusted relays in ISNs remain limited.

Motivated by the above works, in this paper, we consider an EH ISN in the presence of untrusted relays and then propose EH time and target secrecy rate algorithms to improve secrecy performance. The main contributions of this research are summarized as follows:

- We propose a communication protocol in an EH ISN with multiple untrusted relays; here, the untrusted relay is not only a relay to support communication between a SN and the controller but also a potential eavesdropper to steal confidential information.
- We propose an optimization scheme, i.e., BSBR, to improve the PLS against an untrusted relay once it becomes an eavesdropper.
- We evaluate the PLS of the considered system by deriving the closed-form expressions of the SOP and ST metrics for BSBR and its traditional metric, random-sensor-random-untrusted-relay (RSRR). Accordingly, optimal EH time and optimal secrecy rate algorithms are proposed.

The remainder of this paper is organized as follows. In Section II, some related works on the PLS of ISNs with untrusted relays are presented. In Section III, a system model, two communication schemes, and a communication protocol are introduced. In Section IV, the SOPs and STs corresponding to the two considered schemes are analyzed. In Section V, numerical results are provided and discussed. Finally, conclusions and directions for future research are presented in Section VI.

II. RELATED WORK

In this section, recent works about PLS analysis in IoT with untrusted relays are presented.

To enhance secrecy performance, some works have investigated the PLS for IoT [9], [20], [26]–[28]. For instance, Naira *et al*. considered cooperative communication in an ISN comprising a source-destination pair, multiple relays, and multiple eavesdroppers. The authors focused on performance analysis by evaluating the PLS [20]. Zhang *et al*. studied an uplink ISN including controllers, IoT devices, and eavesdroppers. They proposed a low-complexity secure on-off scheme to improve the secrecy performance and used the packet delay and packet secrecy outage probability to evaluate the delay and secrecy performance of the ISN [28].

To enhance the SN devices' coverage and save transmit power, an ISN with untrusted relays was investigated [9], [27], [29]. For example, D. Cheng *et al*. considered an untrusted relay ISN consisting of multiple SNs, a controller, and a single relay. In this case, the relay could be a potential eavesdropper to capture the IoT device's information. Three different scheduling schemes, i.e., optimal scheduling, threshold-based scheduling, and random scheduling, were implemented to evaluate the secrecy performance by deriving the closed-form expressions for SOP, ST, and secure energy efficiency. They also described the tradeoff between implementation complexity and secrecy performance [27]. However, the authors did not consider EH for the SNs and untrusted relay to prolong their lifetimes, and a limitation of their work was the assumption of only 1 relay.

Hu *et al*. studied a cognitive IoT in which the system included an untrusted relay that has EH capability to improve the coverage for the ISN. The authors investigated two main schemes: secure schemes based on power-splitting and time-splitting policies. Accordingly, they then derived the closed-form expressions for the probability of successfully secure transmissions for both schemes to evaluate the secrecy

performance [9]. Mamaghani *et al*. considered communication using a wireless-powered untrusted amplify-and-forward (AF) untrusted relay. They proposed three phases for the communication protocol based on the time-switching architecture at the untrusted relay. Accordingly, the closed-form lower-bound expressions for the ergodic secrecy sum rate in the high signal-to-noise ratio (SNR) regime were derived to evaluate the secure communication [29].

However, the above works considered EH only for untrusted relays, whereas the SN also needs power to maintain its operations, and the optimal EH time for untrusted relays was not mentioned. Thus, in this work, we study an RF EH ISN in which the SN and untrusted relay can harvest energy. We also propose an optimal EH time algorithm to improve the secrecy performance.

III. SYSTEM AND CHANNEL MODEL

In this section, the system model, communication protocol, and SN and untrusted relay selection schemes are introduced.

A. SYSTEM MODEL

We consider an ISN as illustrated in Fig. 1. The considered system includes N power transfer stations (PTSs) denoted by P_n (e.g., TV/radio broadcasters, mobile base stations, and handheld radios [8], [11], [13]), M SNs denoted by S_m, and one controller denoted by B with the presence of K relays R_k, where $n \in \{1, \cdots, N\}$, $m \in \{1, \cdots, M\}$, and $k \in \{1, \cdots, K\}$. Here, the SNs, controller, and relays are investigated in heterogeneous networks; thus, R_k can operate in two modes, namely as a relay or an eavesdropper; i.e., R_k not only supports the delivery of information from the SNs to the controller but also listens to the information from S_m.

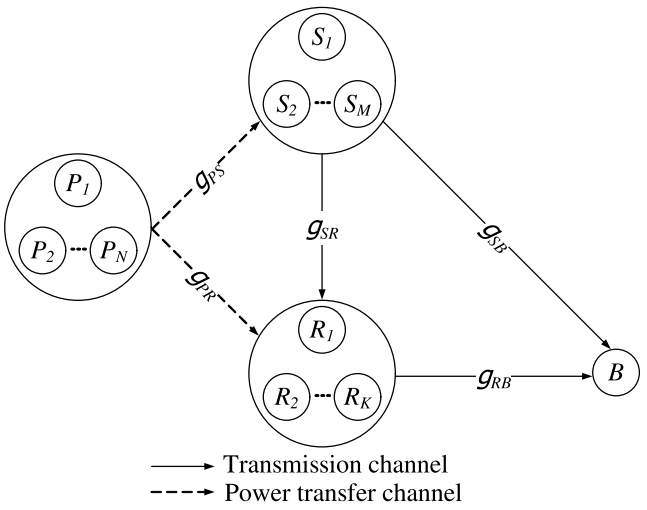

FIGURE 1. System model of the untrusted relay IoT sensor network.

Without loss of generality, the channel coefficients of the $P_n \to S_m$, $P_n \to R_k$, $S_m \to R_k$, $S_m \to B$, and $R_k \to B$ links are expressed by $g_{P_nS_m}$, $g_{P_nR_k}$, $g_{S_mR_k}$ g_{S_mB}, and g_{R_kB}, respectively. The distances of the $P_n \to S_m$, $P_n \to R_k$, $S_m \to R_k$, $S_m \to B$, and $R_k \to B$ links are denoted by $d_{P_nS_m}$, $d_{P_nR_k}$, $d_{S_mR_k}$, d_{S_mB}, and d_{R_kB}, respectively.

Following [30]–[32], we assume that all channels are modeled as Rayleigh fading channels and that the channel coefficients are random variables (RVs) distributed following the Rayleigh model. Accordingly, the CDF and probability density function (PDF) of the channel gains are respectively given as follows:

$$F_{\gamma_{XY}}(x) = 1 - e^{-\frac{x}{\Omega_{XY}}}, \tag{1}$$

and

$$f_{\gamma_{XY}}(x) = \frac{1}{\Omega_{XY}} e^{-\frac{x}{\Omega_{XY}}}, \tag{2}$$

where $\gamma_{XY} = |g_{XY}|^2 / d_{XY}^{\theta}$; RV g_{XY} and d_{XY} refer to the channel gain and the distance from $X \to Y$, respectively; the symbol θ is the path loss exponent, which is influenced by the terrain contours, environment (urban or rural, vegetation and foliage), and propagation medium; and $\Omega_{XY} = E[\gamma_{XY}]$ is the mean channel gain, where $E[\cdot]$ denotes the expectation operation. Moreover, in this considered system, the SNs do not know that the relays are eavesdroppers in the case of a relay node from a different network [18]. Thus, the SNs should provide the channel state information (CSI) for relays to achieve successful communication. Thus, we also assume that the CSI is known at all SNs, untrusted relays, and the controller [19], [26], [27].

B. COMMUNICATION PROTOCOL

In the considered system, a time-switching-based relaying (TSR) protocol is utilized for the communication process, in which two phases, i.e., EH and information transmission (see Fig. 2), are implemented [33]. At this point, the communication protocol is detailed as follows:

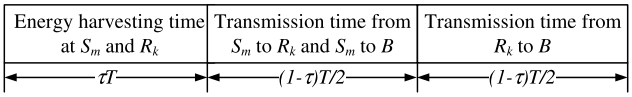

FIGURE 2. A total block time is used for the TSR protocol.

In the first phase, the SNs and relays harvest energy from the broadcasting signal of multiple PTSs in time τT. Here, we use the fixed-gain EH at S_m and R_k, i.e., $\Omega_{P_nS_m} = E\left[\frac{|g_{P_nS_m}|^2}{d_{P_nS_m}^{\theta}}\right]$ and $\Omega_{P_nR_k} = E\left[\frac{|g_{P_nR_k}|^2}{d_{P_nR_k}^{\theta}}\right]$ following [34]–[36]. Hence, the harvested energies at S_m and R_k are respectively as follows:

$$\mathcal{E}_{S_m} = E\left[\sum_{n=1}^{N} \frac{\tau T \eta \mathcal{P}_0 |g_{P_nR_k}|^2}{d_{P_nS_m}^{\theta}}\right] = \tau T \eta \mathcal{P}_0 \sum_{n=1}^{N} \Omega_{P_nS_m}, \tag{3}$$

and

$$\mathcal{E}_{R_k} = E\left[\sum_{n=1}^{N} \frac{\tau T \eta \mathcal{P}_0 |g_{P_nR_k}|^2}{d_{P_nR_k}^{\theta}}\right] = \tau T \eta \mathcal{P}_0 \sum_{n=1}^{N} \Omega_{P_nR_k}, \tag{4}$$

where $\mathcal{P}_0$ is the transmit power of PTSs; the symbols T and τ ($0 < \tau < 1$) denote the total block and fraction of block time for EH, respectively; and the symbol η is the EH conversion efficiency of the SNs and untrusted relays.

In the second phase, the remaining time slot $(1-\tau)T$ is used for information transmission, which is separated into the following two steps:

- Step 1: The selected SN broadcasts a signal x_S to a selected untrusted relay and controller during time $(1-\tau)T/2$. From (3), the transmit power of S_m is as follows:

$$\mathcal{P}_{S_m} = \frac{\mathcal{E}_{S_m}}{(1-\tau)\,T/2} = \frac{2\tau\eta\mathcal{P}_0}{1-\tau}\sum_{n=1}^{N}\Omega_{P_nS_m}. \tag{5}$$

  Hence, the received signals at untrusted relay R_k and controller B are respectively expressed as

$$y_{R_k}(t) = \sqrt{\frac{\mathcal{P}_{S_m}}{d^{\theta}_{S_mR_k}}}g_{S_mR_k}x_S + n_{R_k}, \tag{6}$$

  and

$$y^{(1)}_B(t) = \sqrt{\frac{\mathcal{P}_{S_m}}{d^{\theta}_{S_mB}}}g_{S_mB}x_S + n_B, \tag{7}$$

  where $n_{R_k}, n_B \in \mathcal{CN}(0, N_0)$ are additive white Gaussian noises (AWGNs) at R_k and B and N_0 is noise power.
- Step 2: We employ the AF protocol [35] in which the selected untrusted relay amplifies the received signal and then forwards it to the controller in the remaining time $(1-\tau)T/2$. Here, the variable amplifying coefficient G and transmit power $\mathcal{P}_{R_k}$ are respectively given by

$$G = \frac{1}{\sqrt{\frac{\mathcal{P}_{S_m}\left|g_{S_mR_k}\right|^2}{d^{\theta}_{S_mR_k}} + N_0}}, \tag{8}$$

  and

$$\mathcal{P}_{R_k} = \frac{\mathcal{E}_{R_k}}{(1-\tau)\,T/2} = \frac{2\alpha\eta\mathcal{P}_0}{1-\tau}\sum_{n=1}^{N}\Omega_{P_nR_k}. \tag{9}$$

  Accordingly, the signal received at the controller during this step is expressed as

$$\begin{aligned} y^{(2)}_B(t) &= G\sqrt{\frac{\mathcal{P}_{R_k}}{d^{\theta}_{R_kB}}}g_{R_kB}y_{R_k} + n_B \\ &= G\sqrt{\frac{\mathcal{P}_{R_k}}{d^{\theta}_{R_kB}}}g_{R_kB}\sqrt{\frac{\mathcal{P}_{S_m}}{d^{\theta}_{S_mR_k}}}g_{S_mR_k}x_S \\ &\quad + G\sqrt{\frac{\mathcal{P}_{R_k}}{d^{\theta}_{R_kB}}}g_{R_kB}n_{R_k} + n_B. \end{aligned} \tag{10}$$

C. CHANNEL CAPACITY

From (6), the instantaneous received SNR at the selected untrusted relay R_k is given by

$$\gamma_{R_k} = \frac{\mathcal{P}_{S_m}\left|g_{S_mR_k}\right|^2}{d^{\theta}_{S_mR_k}N_0} = \mathcal{A}_{S_m}\gamma_{S_mR_k}, \tag{11}$$

where $\mathcal{A}_{S_m} = \mathcal{P}_{S_m}/N_0$ and $\gamma_{S_mR_k} = \left|g_{S_mR_k}\right|^2/d^{\theta}_{S_mR_k}$.

Similar to (11), from (7) and (10), the instantaneous received SNRs at the controller in steps 1 and 2 are respectively expressed as

$$\gamma^{(1)}_B = \frac{\mathcal{P}_{S_m}\left|g_{S_mB}\right|^2}{d^{\theta}_{S_mB}N_0} = \mathcal{A}_{S_m}\gamma_{S_mB}, \tag{12}$$

and

$$\begin{aligned} \gamma^{(2)}_B &= \frac{P_{R_k}P_{S_m}G^2\left|h_{R_kB}\right|^2\left|h_{S_mR_k}\right|^2}{d^{\theta}_{R_kB}d^{\theta}_{S_mR_k}\left(G^2\frac{P_{R_k}\left|h_{R_kB}\right|^2N_0}{d^{\theta}_{R_kB}} + N_0\right)} \\ &= \frac{\mathcal{A}_{S_m}\mathcal{A}_{R_k}\gamma_{R_kB}\gamma_{S_mR_k}}{\mathcal{A}_{R_k}\gamma_{R_kB} + \mathcal{A}_{S_m}\gamma_{S_mR_k} + 1}, \end{aligned} \tag{13}$$

where $\gamma_{R_kB} = \left|g_{R_kB}\right|^2/d^{\theta}_{R_kB}$ and $\mathcal{A}_{R_k} = \mathcal{P}_{R_k}/N_0$.

Therefore, the end-to-end SNR at the controller B can be rewritten as follows:

$$\gamma_B = \mathcal{A}_{S_m}\gamma_{S_mB} + \frac{\mathcal{A}_{S_m}\mathcal{A}_{R_k}\gamma_{R_kB}\gamma_{S_mR_k}}{\mathcal{A}_{R_k}\gamma_{R_kB} + \mathcal{A}_{S_m}\gamma_{S_mR_k} + 1}. \tag{14}$$

Following the Shannon capacity formula [37], the instantaneous channel capacity from $S_m \to R_k$ link and from $S_m \to B$ are respectively given as follows:

$$\begin{aligned} C_{R_k} &= \frac{1-\tau}{2}\log_2\left(1+\gamma_{R_k}\right) \\ &= \frac{1-\tau}{2}\log_2\left(1+\mathcal{A}_{S_m}\gamma_{S_mR_k}\right), \end{aligned} \tag{15}$$

and

$$\begin{aligned} C_B &= \frac{1-\tau}{2}\log_2\left(1+\gamma_B\right) \\ &= \frac{1-\tau}{2}\log_2\Bigg(1+\mathcal{A}_{S_m}\gamma_{S_mB} \\ &\qquad + \frac{\mathcal{A}_{S_m}\mathcal{A}_{R_k}\gamma_{R_kB}\gamma_{S_mR_k}}{\mathcal{A}_{R_k}\gamma_{R_kB} + \mathcal{A}_{S_m}\gamma_{S_mR_k} + 1}\Bigg), \end{aligned} \tag{16}$$

where the term $(1-\tau)/2$ appears because the EH SN broadcasts a packet to the untrusted relay and controller in the first step and the relay forwards the SN information to the controller in the second step for the same effective time of $(1-\tau)/2$ part of the total block time T only.

Here, the untrusted relay can be an eavesdropper. Thus, according to [38]–[40], the secrecy capacity of the considered system is defined by the difference between the capacity of the channel from the selected SN to the controller and that of the channel from the selected SN to the untrusted relay, which can be expressed as follows:

$$\begin{aligned} C_{\text{secrecy}} &= \left[C_B - C_{R_k}\right]^+ \\ &= \begin{cases} \dfrac{1-\tau}{2}\log_2\left(\gamma\right), & \text{if } C_B > C_{R_k} \\ 0, & \text{if } C_B \le C_{R_k}, \end{cases} \end{aligned} \tag{17}$$

where γ is defined as

$$\gamma = \frac{1 + \mathcal{A}_{S_m}\gamma_{S_mB} + \frac{\mathcal{A}_{S_m}\mathcal{A}_{R_k}\gamma_{R_kB}\gamma_{S_mR_k}}{\mathcal{A}_{R_k}\gamma_{R_kB}+\mathcal{A}_{S_m}\gamma_{S_mR_k}+1}}{1+\mathcal{A}_{S_m}\gamma_{S_mR_k}}. \tag{18}$$

D. SCHEDULING SCHEME

In this subsection, two schemes, i.e., the BSBR and the RSRR, are investigated as follows:

- *Description of the BSBR*: A selected S (S^*) is chosen from M SNs such that γ_{S_mB} is the best, and a selected R (R^*) is also chosen from K untrusted relays such that γ_{R_kB} is the best, which can be described as follows:

$$S^* = \underset{1\le m\le M}{\arg\max} \left\{\gamma_{S_mB}\right\}, \tag{19}$$

and

$$R^* = \underset{1\le m\le K}{\arg\max} \left\{\gamma_{R_kB}\right\}. \tag{20}$$

Therefore, the CDF of γ_{S^*B} and the PDF of γ_{R^*B} are obtained as [41]

$$F_{\gamma_{S^*B}}(x) = \left(1 - e^{\frac{x}{\Omega_{S^*B}}}\right)^M, \tag{21}$$

and

$$f_{\gamma_{R^*B}}(x) = \frac{K}{\Omega_{R^*B}} e^{-\frac{x}{\Omega_{R^*B}}} \left(1 - e^{-\frac{x}{\Omega_{R^*B}}}\right)^{K-1}, \tag{22}$$

where $\Omega_{S^*B} = E\left[\frac{|g_{S^*B}|^2}{d_{S^*B}^{\theta}}\right]$ and $\Omega_{R^*B} = E\left[\frac{|g_{R^*B}|^2}{d_{R^*B}^{\theta}}\right]$.

- *Description of the RSRR*: A selected S and R (S^r and R^r) are randomly chosen from M SNs and K untrusted relays for each transmission. This scheme is used as a baseline for comparison with the BSBR scheme.

IV. SECRECY PERFORMANCE ANALYSIS

In this section, we derive the closed-form expressions of the SOP and secrecy throughput metrics to evaluate and compare the effects of the two schemes on the secrecy performance of the network scenario.

A. SECRECY OUTAGE PROBABILITY

As discussed in [42], the SOP is an important measure for evaluating the secrecy performance of the considered system, and it is defined as the probability of the instantaneous secrecy capacity dropping below a target secrecy rate R_{th}, i.e.,

$$\mathcal{O} = \Pr\left\{C_{\text{secrecy}} < R_{th}\right\}, \tag{23}$$

where $\Pr\{\cdot\}$ is a probability function; and $\mathcal{O}$ and C_{secrecy} are respectively defined as

$$\mathcal{O} \in \left\{\mathcal{O}^{(BSBR)}, \mathcal{O}^{(RSRR)}\right\},$$

and

$$C_{\text{secrecy}} \in \left\{C_{\text{secrecy}}^{(RSRR)}, C_{\text{secrecy}}^{(RSRR)}\right\}.$$

Let $U = \gamma_{R_kB}$ and $\varsigma = 2^{\frac{2R_{th}}{1-\tau}}$; then, the SOP of the considered system can be expressed as

$$\mathcal{O} = \int_0^{\infty} (\Phi_1 + \Phi_2) f_U(u)\, du, \tag{24}$$

where Φ_1 and Φ_2 are respectively expressed as follows:

$$\Phi_1 = \Pr\left\{\frac{1 + \mathcal{A}_{S_m}\gamma_{S_mB} + \mathcal{A}_{R_k}u}{1 + \mathcal{A}_{S_m}\gamma_{S_mR_k}} < \varsigma, \gamma_{S_mR_k} > \frac{\mathcal{A}_{R_k}u}{\mathcal{A}_{S_m}}\right\}, \tag{25}$$

and

$$\Phi_2 = \Pr\left\{1 + \frac{\mathcal{A}_{S_m}\gamma_{S_mB}}{1 + \mathcal{A}_{S_m}\gamma_{S_mR_k}} < \varsigma, \gamma_{S_mR_k} < \frac{\mathcal{A}_{R_k}u}{\mathcal{A}_{S_m}}\right\}. \tag{26}$$

Proof: See Appendix.

1) DERIVATION FOR THE BSBR

By substituting (2) and (21) into (25), the function $\Phi_1^{(RSRR)}$ can be rewritten as

$$\begin{aligned}\Phi_1^{(BSBR)} &= \Pr\left\{\gamma_{S^*B} < \frac{\varsigma\left(1 + \mathcal{A}_{S^*}\gamma_{S^*R^*}\right) - 1 - \mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}}, \right.\\ &\quad \left.\frac{\mathcal{A}_{S^*}\gamma_{S^*R^*}}{\mathcal{A}_{R^*}} > u^*\right\}\\ &= \frac{1}{\Omega_{S^*R^*}} \int_{\frac{\mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}}}^{\infty} \left[1 - e^{-\frac{\varsigma\left(1+\mathcal{A}_{S^*}h\right)-1-\mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}\Omega_{S^*B}}}\right]^M e^{-\frac{h}{\Omega_{S^*R^*}}} dh,\end{aligned} \tag{27}$$

where $u^* = \gamma_{R^*B}$.

Using the series of the power function representation in [43, eq. (1.111)], the integral $\Phi_1^{(BSBR)}$ can be obtained as

$$\Phi_1^{(BSBR)} = \Sigma_M \Delta_1 e^{-\left[\frac{m(\varsigma-1)}{\Omega_{S^*B}} + \frac{1}{\Omega_{S^*R^*}}\right]\frac{\mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}}}, \tag{28}$$

where $\Omega_{S^*R^*} = E\left[\frac{|g_{S^*R^*}|^2}{d_{S^*R^*}^{\theta}}\right]$; Σ_M and Δ_1 are respectively defined as

$$\Sigma_M = \sum_{m=0}^{M} \frac{(-1)^m M!}{m!\,(M-m)!}, \tag{29}$$

and

$$\Delta_1 = \frac{\Omega_{S^*B} e^{-\frac{\varsigma-1}{\mathcal{A}_{S^*}\Omega_{S^*B}}m}}{\varsigma m \Omega_{S^*R^*} + \Omega_{S^*B}}. \tag{30}$$

Similar to (28), the integral $\Phi_2^{(BSBR)}$ is calculated as

$$\begin{aligned}\Phi_2^{(BSBR)} &= \Pr\left\{\gamma_{S^*B} < \frac{\varsigma - 1 + (\varsigma - 1)\mathcal{A}_{S^*}t}{\mathcal{A}_{S^*}}, \gamma_{S^*R^*} < \frac{\mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}}\right\}\\ &= \frac{1}{\Omega_{S^*R^*}} \int_0^{\frac{\mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}}} \left[1 - e^{-\frac{\varsigma-1+(\varsigma-1)\mathcal{A}_{S^*}t}{\Omega_{S^*B}\mathcal{A}_{S^*}}}\right]^M e^{-\frac{t}{\Omega_{S^*R^*}}} dt\\ &= \Sigma_M \Delta_2 \left\{1 - e^{-\left[\frac{(\varsigma-1)m}{\Omega_{S^*B}} + \frac{1}{\Omega_{S^*R^*}}\right]\frac{\mathcal{A}_{R^*}u^*}{\mathcal{A}_{S^*}}}\right\},\end{aligned} \tag{31}$$

where Δ_2 is defined as

$$\Delta_2 = \frac{\Omega_{S^*B} e^{-\frac{\varsigma-1}{\Omega_{S^*B}\mathcal{A}_{S^*}} m}}{(\varsigma-1)\, m\Omega_{S^*R^*} + \Omega_{S^*B}}. \quad (32)$$

By substituting (22), (28), and (31) into (24), we can rewrite the SOP for BSBR as (33) on the bottom of this page, where Δ_3 is defined as

$$\Delta_3 = \left[\frac{m(\varsigma-1)}{\Omega_{S^*B}} + \frac{1}{\Omega_{S^*R^*}}\right] \frac{\sum_{n=1}^{N} \Omega_{P_n R^*}}{\sum_{n=1}^{N} \Omega_{P_n S^*}}. \quad (34)$$

Based on (33) and after some calculation steps, the SOP of the considered system for BSBR is obtained as follows:

$$\mathcal{O}^{(BSBR)} = \Sigma_K \Sigma_M \left(\Delta_2 + \frac{\Delta_1 - \Delta_2}{\Delta_3 \Omega_{R^*B} + k + 1}\right), \quad (35)$$

where Σ_K is defined as

$$\Sigma_K = \sum_{k=0}^{K-1} \frac{(-1)^k K!}{(k+1)!\,(K-k-1)!}. \quad (36)$$

2) DERIVATION FOR THE RSRR

Similar to the case of BSBR, the SOP for RSRR can be characterized by

$$\mathcal{O}^{(RSRR)} = 1 - \frac{\Omega_{S^rB} e^{-\frac{\varsigma-1}{\Omega_{S^rB}\mathcal{A}_{S^r}}}}{(\varsigma-1)\,\Omega_{S^rR^r} + \Omega_{S^rB}} - \frac{\Delta_4}{\Delta_5}, \quad (37)$$

where Ω_4 and Ω_5 are respectively defined as

$$\Delta_4 = \frac{\Omega_{S^rB} e^{-\frac{\varsigma-1}{\mathcal{A}_{S^r}\Omega_{S^rB}}}}{\varsigma\Omega_{S^rR^r} + \Omega_{S^rB}} - \frac{\Omega_{S^rB} e^{-\frac{\varsigma-1}{\mathcal{A}_{S^r}\Omega_{S^rB}}}}{(\varsigma-1)\,\Omega_{S^rR^r} + \Omega_{S^rB}}, \quad (38)$$

and

$$\Delta_5 = \left[\frac{\varsigma-1}{\Omega_{S^rB}} + \frac{1}{\Omega_{S^rR^r}}\right] \frac{\sum_{n=1}^{N} \Omega_{P_n R^r}}{\sum_{n=1}^{N} \Omega_{P_n S^r}} \Omega_{R^rB} + 1. \quad (39)$$

Based on the communication protocol, we predict that when the EH time τ is small, the transmission power at the untrusted relay is also small because it only harvests a small amount of energy. This leads to a high SOP, which will decrease with increasing τ. However, the secrecy capacity will decrease if the EH time of the untrusted relay is large because the untrusted relay can be viewed as an eavesdropper. Hence, the SOP of the ISN will increase again. Thus, an optimal EH time τ^* exists such that the considered system can achieve the best secrecy performance.

Algorithm 1 Algorithm for Determining τ^*

```
procedure
    Set the initial array: τ(i) ∈ (a, b);
    Set the initial step: i ← 1;
    Set the initial value: O* ← 1;
    while i < I do
        Update O(i) with respect to τ(i) according to (35) or (37);
        if O* > O(i) then
            Update O* ← O(i);
            Update i ← i + 1;
        else
            Calculate τ* = τ(i − 1);
            Calculate O* = O(i − 1);
            Exit the loop;
        end if
    end while
    return τ* and O*;
end procedure
```

To determine τ^*, we propose the algorithm illustrated in **Algorithm 1**. Specifically, we split the values of the EH time proportion into an array (a, b) with $\mathcal{I}$ elements, in which $a < b$ is the EH time and the starting point of SOP $\mathcal{O}^*$ is set to 1. The algorithm then performs the iteration process as follows:

- Update $\mathcal{O}(i)$ with respect to $\tau(i)$, where $\mathcal{O}(i) \in \{\mathcal{O}(i)^{(BSBR)}, \mathcal{O}(i)^{(RSRR)}\}$.
- The aforementioned iteration process will be stopped when $\mathcal{O}^* < \mathcal{O}(i)$.

B. ASYMPTOTIC SOP ANALYSIS

To obtain insights into the impact of a high SNR regime on the secrecy of multi-SN transmissions, the asymptotic expressions of the SOP for BSBR and RSRR are derived and analyzed in this subsection.

1) DERIVATION FOR THE BSBR

The asymptotic SOP for BSBR when the average SNR increases to infinity, i.e., $\gamma_0 = \mathcal{P}_0/N_0 \to \infty$, is obtained as

$$\lim_{\gamma_0 \to \infty} \mathcal{O}^{(BSBR)} = \Sigma_K \Sigma_M \left[\Delta_7 + \frac{\Delta_6 - \Delta_7}{\Delta_3 \Omega_{R^*B} + k + 1}\right], \quad (40)$$

where Ω_6 and Ω_7 are as follows:

$$\Delta_6 = \frac{\Omega_{S^*B}}{\varsigma m \Omega_{S^*R^*} + \Omega_{S^*B}}, \quad (41)$$

$$\mathcal{O}^{(BSBR)} = \frac{K}{\Omega_{R^*B}} \int_0^{\infty} \left[\Sigma_M \Delta_2 + \Sigma_M (\Delta_1 - \Delta_2) e^{-\Delta_3 u^*}\right] e^{-\frac{u^*}{\Omega_{R^*B}}} \left(1 - e^{-\frac{u^*}{\Omega_{R^*B}}}\right)^{K-1} du^*. \quad (33)$$

and

$$\Delta_7 = \frac{\Omega_{S^*B}}{(\varsigma - 1)\, m\Omega_{S^*R^*} + \Omega_{S^*B}}. \tag{42}$$

2) DERIVATION FOR THE RSRR

Similar to (40), the asymptotic SOP for RSRR is expressed as follows:

$$\lim_{\gamma_0 \to \infty} \mathcal{O}^{(RSRR)} = 1 - \frac{\Omega_{S^rB}}{(\varsigma - 1)\, \Omega_{S^rR^r} + \Omega_{S^rB}} - \frac{\Delta_8}{\Delta_5}, \tag{43}$$

where Ω_8 is defined as

$$\Delta_8 = \frac{\Omega_{S^rB}}{\varsigma \Omega_{S^rR^r} + \Omega_{S^rB}} - \frac{\Omega_{S^rB}}{(\varsigma - 1)\, \Omega_{S^rR^r} + \Omega_{S^rB}}. \tag{44}$$

C. SECRECY THROUGHPUT

The above SOP metric evaluates the reliability and security of the ISN. However, ST is still needed to characterize the overall efficiency of the considered system in achieving reliable and secure transmission. Following [44], the ST is defined as

$$\Psi = R_{th}\,(1 - \mathcal{O})\,, \tag{45}$$

where $\Psi \in \left\{\Psi^{(BSBR)}, \Psi^{(RSRR)}\right\}$. Therefore, the STs of the considered system for BSBR and RSRR are respectively obtained as follows:

$$\Psi^{(BSBR)} = R_{th}\left[1 - \Sigma_K \Sigma_M \left(\Delta_2 + \frac{\Delta_1 - \Delta_2}{\Delta_3 \Omega_{R^*B} + k + 1}\right)\right], \tag{46}$$

and

$$\Psi^{(RSRR)} = R_{th}\left[\frac{\Omega_{S^rB} e^{-\frac{\varsigma - 1}{\Omega_{S^rB} A_{S^r}}}}{(\varsigma - 1)\, \Omega_{S^rR^r} + \Omega_{S^rB}} + \frac{\Delta_4}{\Delta_5}\right]. \tag{47}$$

Based on (45), we realize that the ST is small with a small target secrecy rate R_{th}. However, based on the SOP definition, when R_{th} is large, the secrecy outage probability of the considered system is high, i.e., SOP will be large; this leads to decreasing ST. From this observation, we propose an algorithm to determine the optimal target secrecy rate R^*_{th} that achieves the maximum ST Ψ^*. Similar to **Algorithm 1**, the algorithm to determine the R^*_{th} is presented in **Algorithm 2**, where $\mathcal{J}$ is the number of elements of array (c, d), $c < d$ is the target secrecy rate, and $\Psi(j) \in \left\{\Psi(j)^{(BSBR)}, \Psi(j)^{(RSRR)}\right\}$.

Algorithm 2 Algorithm for Determining R^*_{th}

```
procedure
    Set the initial array: R_th(j) ∈ (c, d);
    Set the initial step: j ← 1;
    Set the initial value: Ψ* ← 0;
    while j < J do
        Update Ψ(j) with respect to R_th(j) according to (46) or (47);
        if Ψ* < Ψ(j) then
            Update Ψ* ← Ψ(j);
            Update j ← j + 1;
        else
            Calculate R*_th = R_th(j − 1);
            Calculate Ψ* = Ψ(j − 1);
            Exit the loop;
        end if
    end while
    return R*_th and Ψ*;
end procedure
```

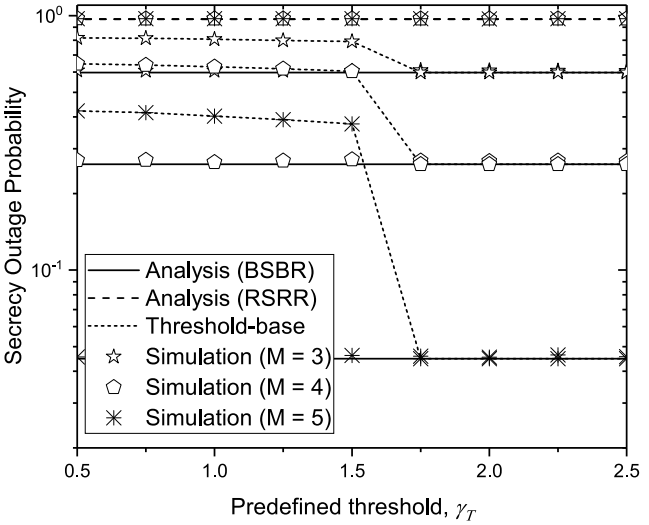

FIGURE 3. Secrecy outage probability versus predefined threshold γ_T with $K = 3$, $\gamma_0 = 10$ (dB), $R_{th} = 0.5$, and $\eta = 0.7$.

V. NUMERICAL RESULTS

In this section, we use Monte Carlo simulations to verify the analysis, and we then present the numerical results and discussion of the secrecy performance of the considered system. In particular, the impact of the optimal EH time on the SOP and the impact of the optimal target secrecy rate on the ST are investigated. Furthermore, the impact of the SNR transmitted from PTSs, γ_0; the EH conversion efficiency, η; the distance from the SN to the untrusted relay, d_{SR}; the number of SNs, M; and the number of untrusted relays, K, on the secrecy performance of the considered system are evaluated by two metrics: SOP, $\mathcal{O}$, and ST, Ψ. Moreover, we also compare the security performance between BSBR and RSRR. Unless otherwise stated, the system parameters for both the analysis and simulation are as follows [20], [36]: $d_{PS} \in [2, 5]$, $d_{SB} \in [2, 5]$, $d_{SR} \in [2, 5]$, $d_{RB} \in [2, 5]$, $R_{th} \in (0, 1)$, $\theta = 2$, $\alpha \in (0, 1)$, $\eta \in (0, 1)$, $\gamma_0 \in [-10, 30]$ (dB), $K \in [3, 5]$, $M \in [3, 5]$, $a = c = 0.1$, $b = d = 0.9$, $\mathcal{I} = \mathcal{J} = 10^2$, and $\sum_{n=1}^{N} \Omega_{P_nS_m} = \sum_{n=1}^{N} \Omega_{P_nR_k} = 2$. We evaluated and compared the following three schemes:

- *Best-sensor-best-untrusted-relay (BSBR)*: The best SN and the best untrusted relay are chosen from M SNs and K untrusted relays, respectively, to transmit information to the controller.

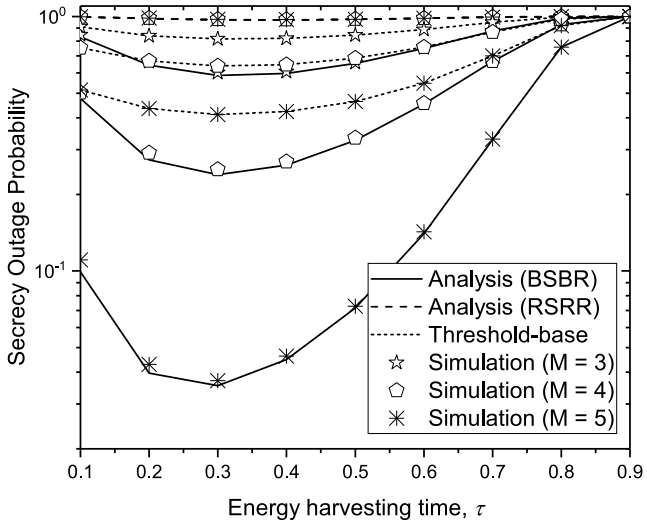

FIGURE 4. Secrecy outage probability versus energy harvesting time τ with $K = 3$, $\gamma_0 = 10$ (dB), $R_{th} = 0.5$, and $\eta = 0.7$.

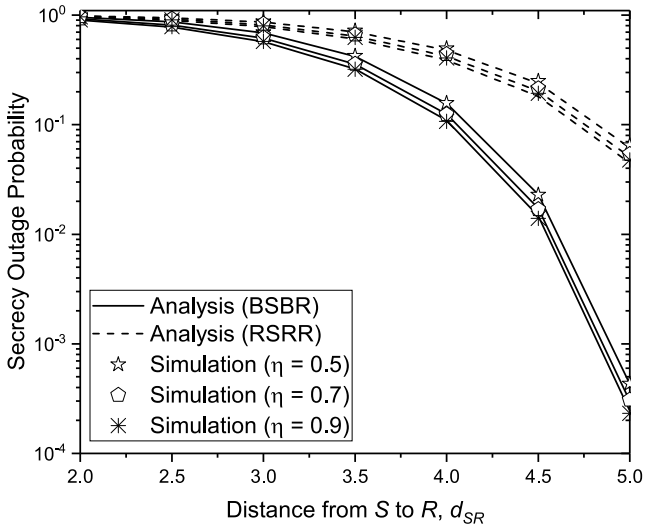

FIGURE 6. Secrecy outage probability versus distance from $S \to R$ d_{SR} with $K = 3$, $M = 3$, $\gamma_0 = 10$ (dB), $\tau = 0.3$, and $R_{th} = 0.5$.

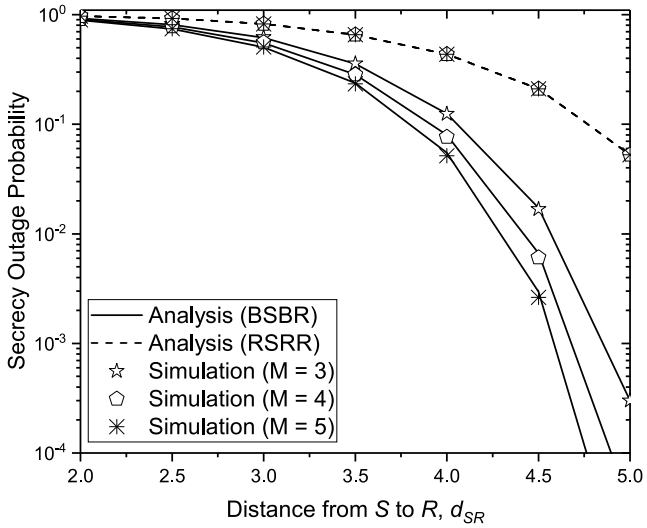

FIGURE 5. Secrecy outage probability versus distance from $S \to R$ d_{SR} with $K = 3$, $\gamma_0 = 10$ (dB), $R_{th} = 0.5$, and $\eta = 0.7$.

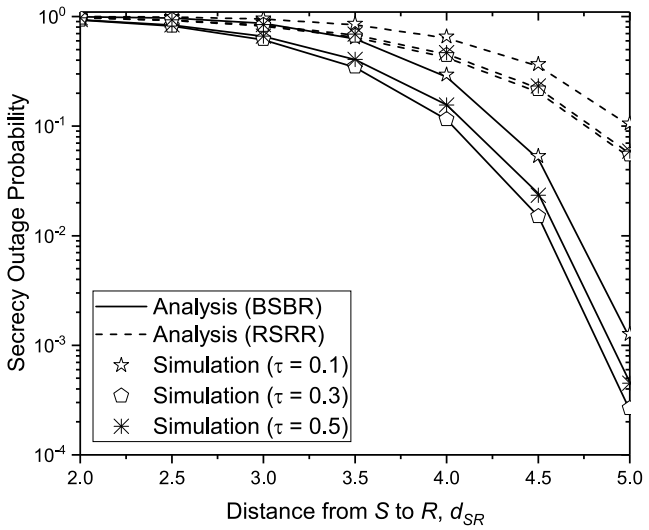

FIGURE 7. Secrecy outage probability versus distance from $S \to R$ d_{SR} with $K = 3$, $M = 3$, $\gamma_0 = 10$ (dB), $\eta = 0.7$, and $R_{th} = 0.5$.

- *Random-sensor-random-untrusted-relay (RSRR)*: The selected SN and the selected untrusted relay are randomly chosen from M SNs and K untrusted relays, respectively, to transmit information to the controller.
- *Threshold-based scheduling (TS)*: Here, we compare the proposed schemes with TS in [27]. The scenario of TS can be described as follows. The first SN is used for data transmission if its end-to-end SNR exceeds the predefined threshold, γ_T. Otherwise, the m-th SN is adopted for data transmission when the end-to-end SNR for the $(m-1)$-th SN is lower than γ_T but the end-to-end SNR for the m-th SN is above the predefined threshold. In the case where all end-to-end SNRs for SNs are lower than the predefined threshold, the best SN is employed for data transmission.

Fig. 3 shows the SOP of BSBR, RSRR, and TS versus the predefined threshold, γ_T. The SOP of the TS is nearly the same as that of the RSRR with small γ_T and is close to the SOP of the BSBR once $\gamma_T > \varsigma$. This result occurs because when γ_T is small, the first SN is selected for data transmission, which is similar to the RSRR. By contrast, if the predefined threshold is larger than ς, then the SN with the maximum end-to-end SNR will be selected for data transmission, which is equivalent to the BSBR.

Fig. 4 shows the SOP along with the EH time of BSBR and RSRR. As the EH time tends to be nearly 1, the SOPs of both schemes all decrease to the optimal point ($\tau^* = 0.3$) and then increase to nearly 1, which is consistent with **Algorithm 1**. Furthermore, we find that the SOP of RSRR corresponding to $M = 3$ is the same as that of the $\mathcal{O}^{(RSRR)}$ corresponding

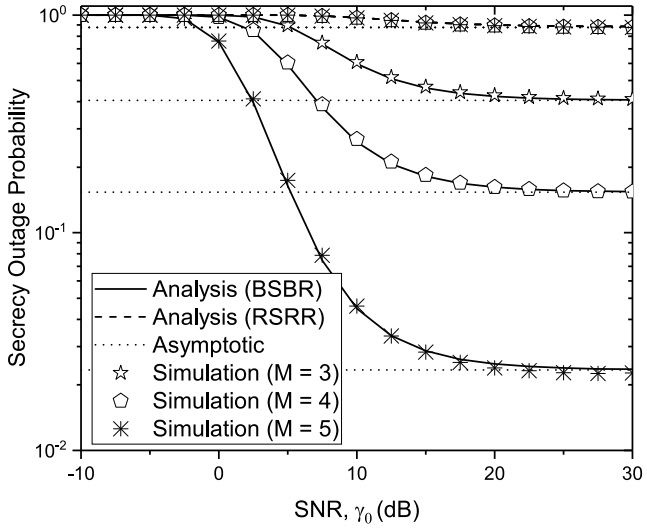

FIGURE 8. Secrecy outage probability versus transmit SNR γ_0 with $K = 3$, $\eta = 0.7$, $\tau = 0.3$, and $R_{th} = 0.5$.

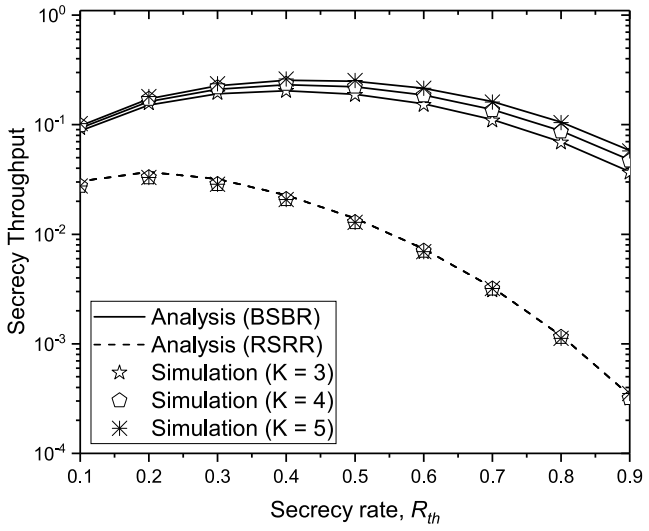

FIGURE 10. Secrecy throughput versus target secrecy rate R_{th} with $M = 3$, $\gamma_0 = 10$ (dB), $\tau = 0.3$, and $\eta = 0.7$.

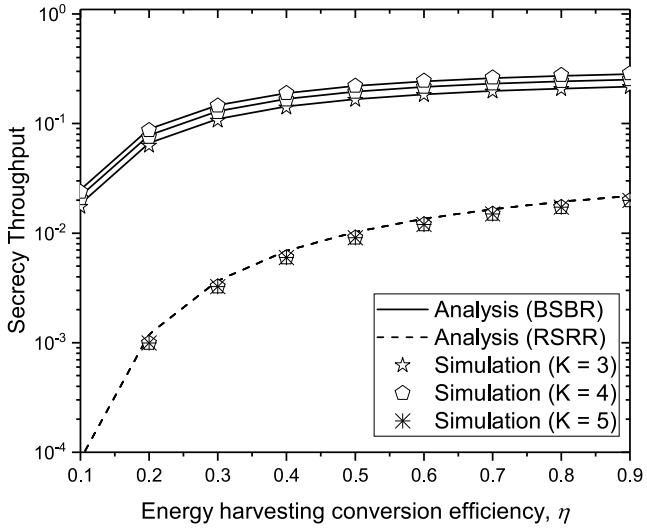

FIGURE 9. Secrecy throughput versus energy harvesting time conversion efficiency η with $M = 3$, $\gamma_0 = 10$ (dB), $\tau = 0.3$, and $R_{th} = 0.5$.

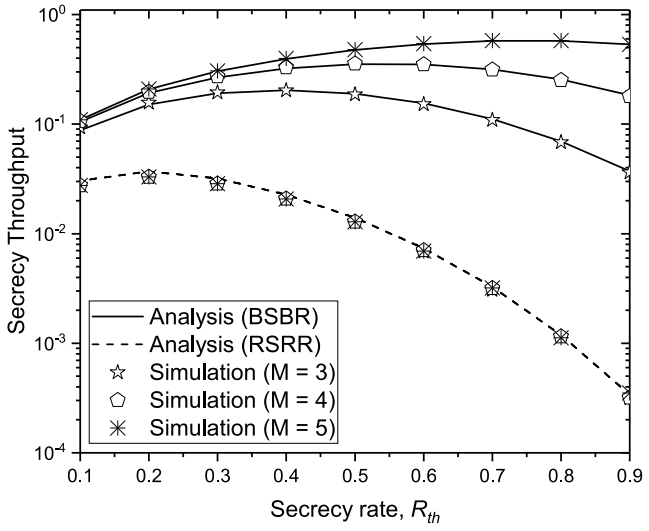

FIGURE 11. Secrecy throughput versus target secrecy rate R_{th} with $K = 3$, $\gamma_0 = 10$ (dB), $\tau = 0.3$, and $\eta = 0.7$.

to $M = 4$ and $M = 5$, and thus the number of SNs does not affect the SOP of RSRR. Note that $\mathcal{O}^{(BSBR)}$ decreases as M increases from $M = 3$ to $M = 5$. This result occurs because the diversity gain will increase at the SNs with higher M. In addition, we can observe that the secrecy performance of the BSBR is better than that of both TS and RSRR, and this trend applies for the remaining simulations.

Figs. 5, 6, and 7 depict the SOP along with distance from $S \rightarrow R$, d_{SR}. As shown in Fig. 5, as the untrusted relay is placed far from the SN, the SOP decreases because the untrusted relay can steal the confidential information from SN. When the distance d_{SR} is higher, i.e., the path loss is higher, the untrusted relays hardly monitor the information, and therefore the secrecy performance of the considered system will be improved, i.e., the SOP is decreased.

As shown in Fig. 6, the SOPs of RSRR with $\eta = 0.5$ is different from that with $\eta = 0.7$ and $\eta = 0.9$. The $\mathcal{O}^{(BSBR)}$ and $\mathcal{O}^{(RSRR)}$ all decrease with increasing η because more energy is harvested at the SN with higher η. Fig. 7 shows that the SOPs of both BSBR and RSRR are best at $\tau^* = 0.3$ because this τ value is the optimal EH time found by **Algorithm 1**.

Fig. 8 illustrates the SOP along with transmit SNR, γ_0. The $\mathcal{O}^{(BSBR)}$ and $\mathcal{O}^{(RSRR)}$ all decrease with increasing γ_0 because the SN will harvest more energy when the transmit SNR is higher. Furthermore, we find that the SOPs of both schemes with $M = 3$, $M = 4$, and $M = 5$ all converge gradually to a nonzero constant as γ_0 tends to infinity. This result indicates that none of the other parameters will affect the SOP at a sufficiently high transmit SNR value.

$$\mathcal{O} = \int_0^{\infty} \Pr\left\{ \frac{1-\tau}{2}\log_2\left(\frac{1+\mathcal{A}_{S_m}\gamma_{S_mB}+\frac{\mathcal{A}_{S_m}\mathcal{A}_{R_k}\gamma_{R_kB}\gamma_{S_mR_k}}{\mathcal{A}_{R_k}\gamma_{R_kB}+\mathcal{A}_{S_m}\gamma_{S_mR_k}+1}}{1+\mathcal{A}_{S_m}\gamma_{S_mR_k}} \right) < R_{th} \right\}$$
$$\approx \int_0^{\infty} \underbrace{\Pr\left\{ \frac{1+\mathcal{A}_{S_m}\gamma_{S_mB}+\min\left(\mathcal{A}_{R_k}u, \mathcal{A}_{S_m}\gamma_{S_mR_k}\right)}{1+\mathcal{A}_{S_m}\gamma_{S_mR_k}} < 2^{\frac{2R_{th}}{1-\tau}} \right\}}_{\Phi} f_U(u)\, du. \quad (49)$$

Fig. 9 shows the ST along with the EH conversion efficiency, η. The ST of the considered system for both BSBR and RSRR all increase with increasing η. This result occurs because as the EH conversion efficiency at SN tends to 1, the SN can harvest more energy from PTSs (based on (3)), leading to an improvement in secrecy performance.

Figs. 10 and 11 depict the ST along with the target secrecy rate, R_{th}. As shown in both figures, the $\Psi^{(BSBR)}$ and $\Psi^{(RSRR)}$ all first increase with increasing R_{th} to reach the maximum points $\Psi^{(BSBR)^*} = 0.2041$, $\Psi^{(BSBR)^*} = 0.2315$, and $\Psi^{(BSBR)^*} = 0.2562$ at $R_{th}^* = 0.41$, $R_{th}^* = 0.41$, and $R_{th}^* = 0.46$; $\Psi^{(RSRR)^*} = 0.0328$ at $R_{th}^* = 0.16$ with all M values with $K = 3$, $K = 4$, and $K = 5$, respectively, in Fig. 10; $\Psi^{(BSBR)^*} = 0.2041$, $\Psi^{(BSBR)^*} = 0.3618$, and $\Psi^{(BSBR)^*} = 0.588$ at $R_{th}^* = 0.41$, $R_{th}^* = 0.56$, and $R_{th}^* = 0.76$ with $M = 3$, $M = 4$, and $M = 5$; and $\Psi^{(RSRR)^*} = 0.0328$ at $R_{th}^* = 0.16$ with all M values, respectively, in Fig. 11 (these optimal points are found by **Algorithm 2**).

We can observe that the optimal STs for BSBR are not the same at the different values of the target secrecy rate R_{th} with different K and different M. This result is attributable to the change in the diversity gain of the considered system for BSBR with different K as well as M. By contrast, the optimal ST for RSRR is one at a single value of R_{th} with different K and different M. This value occurs is because the selected SN and the selected untrusted relay are randomly chosen from M SNs and K untrusted relays to send information to the controller, respectively. Hence, M and K do not affect the SOP of the RSRR scheme, which is consistent with (47). Then, the STs all decrease as R_{th} increases, which is consistent with **Algorithm 2**. Finally, from all simulations, we can conclude that the secrecy performance of BSBR outperforms that of RSRR.

VI. CONCLUSION

In this paper, a radio frequency (RF) energy-harvesting (EH) IoT sensor network (ISN) was investigated. The system consisted of multiple power transfer stations (PTSs), IoT sensor nodes (SNs), and a controller in the presence of multiple untrusted relays. The best-sensor-best-untrusted-relay (BSBR) was proposed and compared with the random-sensor-random-untrusted-relay (RSRR). Accordingly, the secrecy outage probability (SOP) and the ST were derived. We also proposed optimal EH time and optimal target secrecy rate algorithms for both schemes to improve the secrecy performance of the considered system. We then used Monte Carlo simulations to present the numerical results. Accordingly, the secrecy performance of the BSBR was superior to that of the RSRR, including threshold-based scheduling. In addition, the numerical results indicated that the secrecy performance analyses in terms of the SOP and the ST for both BSBR and RSRR improved as the numbers of SNs and untrusted relays increased. In future work, we will consider the issues of the optimal harvested energy, energy outage of SNs, and secrecy capacity in an ISN consisting of multiple relay clusters using the nonorthogonal multiple access (NOMA) technique to improve the SOP and ST for IoT application systems.

APPENDIX
PROOF FOR THE SOP IN (24)

By substituting (17) into (23), we obtain

$$\mathcal{O} = \Pr\left\{ \frac{1-\tau}{2}\log_2(\gamma) < R_{th} \right\}. \quad (48)$$

Using (18) and the approximation function $\frac{\alpha\beta}{\alpha+\beta+1} \approx \min(\alpha, \beta)$ [27], the SOP of the considered system can rewritten as (49) at the top of this page. Then, by applying the probability characteristics, the function Φ can expressed as

$$\Phi = \Pr\left\{ \frac{1+\mathcal{A}_{S_m}\gamma_{S_mB}+\mathcal{A}_{R_k}u}{1+\mathcal{A}_{S_m}\gamma_{S_mR_k}} < \varsigma, \gamma_{S_mR_k} > \frac{\mathcal{A}_{R_k}u}{\mathcal{A}_{S_m}} \right\}$$
$$+ \Pr\left\{ 1+\frac{\mathcal{A}_{S_m}\gamma_{S_mB}}{1+\mathcal{A}_{S_m}\gamma_{S_mR_k}} < \varsigma, \gamma_{S_mR_k} < \frac{\mathcal{A}_{R_k}u}{\mathcal{A}_{S_m}} \right\}. \quad (50)$$

REFERENCES

[1] F. Al-Turjman and A. Radwan, "Data delivery in wireless multimedia sensor networks: Challenging and defying in the IoT era," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 126–131, Oct. 2017.
[2] N. Kaur and S. K. Sood, "An energy-efficient architecture for the Internet of Things (IoT)," *IEEE Syst. J.*, vol. 11, no. 2, pp. 796–805, Jun. 2017.
[3] 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.
[4] S. Heng, C. So-In, and T. G. Nguyen, "Distributed image compression architecture over wireless multimedia sensor networks," *Wireless Commun. Mobile Comput.*, pp. 1–21, Dec. 2017.
[5] T. G. Nguyen, C. So-In, N. G. Nguyen, and S. Phoemphon, "A novel energy-efficient clustering protocol with area coverage awareness for wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 10, no. 3, pp. 519–536, May 2017.
[6] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the Internet of Things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, pp. 1–16, Aug. 2017.
[7] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT," *IEEE Access*, vol. 3, pp. 622–637, Jun. 2015.

[8] S. Mallick, A.-Z. S. B. Habib, A. S. Ahmed, and S. S. Alam, "Performance appraisal of wireless energy harvesting in IoT," in *Proc. Int. Conf. Elect. Inf. Commun. Technol.*, Dec. 2017, pp. 1–6.

[9] 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.

[10] H. Habibu, A. M. Zungeru, A. A. Susan, and I. Gerald, "Energy harvesting wireless sensor networks: Design and modeling," *Int. J. Wireless Mobile Netw.*, vol. 6, no. 5, pp. 17–31, Oct. 2014.

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

[12] D. Wang, H. Liu, X. Ma, J. Wang, Y. Peng, and Y. Wu, "Energy harvesting for Internet of Things with heterogeneous users," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–15, Jul. 2017, doi: 10.1155/2017/1858532.

[13] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 102–108, Jun. 2015.

[14] J.-H. Huang and S.-Y. Hsu, "Joint power assignment and relay location design for cooperative power-efficient networks with adaptive transmission mode selection," in *Proc. IEEE Wireless Commun. Netw. Conf.*, New Orleans, LA, USA, Jan. 2015, pp. 1141–1146.

[15] J. Luo, D. Wu, C. Pan, and J. Zha, "Optimal energy strategy for node selection and data relay in WSN-based IoT," *Mobile Netw. Appl.*, vol. 20, no. 2, pp. 169–180, Apr. 2015.

[16] W. Guo, S. Zhou, Y. Chen, S. Wang, X. Chu, and Z. Niu, "Simultaneous information and energy flow for IoT relay systems with crowd harvesting," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 143–149, Nov. 2016.

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

[18] 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.

[19] D. Chen, W. Yang, J. Hu, Y. Cai, and S. Zhu, "Cooperative secure transmission in the presence of untrusted relay," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 6, pp. 1–10, May 2016, doi: 10.1155/2016/3567323.

[20] A. K. Nair, S. Asmi, and A. Gopakumar, "Analysis of physical layer security via co-operative communication in Internet of Things," *Procedia Technol.*, vol. 24, no. 2016, pp. 896–903, May 2016.

[21] A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Proc. IEEE World Forum Internet Things*, Mar. 2014, pp. 67–72.

[22] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *Proc. IEEE Int. Conf. Privacy Secur. Mobile Syst.*, May 2014, pp. 1–8.

[23] 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.

[24] A. Soni, R. Upadhyay, and A. Jain, "Internet of Things and wireless physical layer security: A survey," *Comput. Commun., Netw. Internet Secur.*, vol. 5, pp. 115–123, May 2017.

[25] Z. Zhong, J. Peng, K. Huang, and Z. Zhong, "Analysis on physical-layer security for Internet of Things in ultra dense heterogeneous networks," in *Proc. Int. Conf. Internet Things, IEEE Green Comput. Commun., IEEE Cyber, Phys. Social Comput., IEEE Smart Data (iThings/GreenCom/CPSCom/SmartData)*, May 2017, pp. 39–43.

[26] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[27] 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, Feb. 2018.

[28] S. Zhang, J. Peng, K. Huang, X. Xu, and Z. Zhong, "Physical layer security in iot: A spatial-temporal perspective," in *Proc. Wireless Commun. Signal Process.*, Nanjing, China, Dec. 2017, pp. 1–6.

[29] 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, doi: 10.1109/TVT.2018.2848648.

[30] N. Wang, X. Song, J. Cheng, and V. C. M. Leung, "Enhancing the security of free-space optical communications with secret sharing and key agreement," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 6, no. 12, pp. 1072–1081, Dec. 2014.

[31] D.-B. Ha, D.-D. Tran, T.-V. Truong, and N.-V. Vo, "Physical layer secrecy performance of energy harvesting networks with power transfer station selection," in *Proc. IEEE Int. Conf. Commun. Electron.*, Jul. 2016, pp. 451–456.

[32] D.-B. Ha and S. Q. Nguyen, "Outage performance of energy harvesting DF relaying NOMA networks," *Mobile Netw. Appl.*, pp. 1–14, Oct. 2017, doi: 10.1007/s11036-017-0922-x.

[33] 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.

[34] 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, Mar. 2017.

[35] A. Koc, I. Altunbaş, 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, no. 2017, pp. 110-1–110-11, Jun. 2017, doi: 10.1186/s13638-017-0888-1.

[36] H. Tran, T. X. Quach, H. Tran, and E. Uhlemann, "Optimal energy harvesting time and transmit power in cognitive radio network under joint constraints of primary users and eavesdroppers," in *Proc. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Oct. 2017, pp. 1–8.

[37] P. Maji, S. D. Roy, and S. Kundu, "Secrecy outage analysis in a hybrid cognitive relay network with energy harvesting," *Int. J. Commun. Syst.*, vol. 30, no. 10, pp. 1–10, Jul. 2017.

[38] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[39] Q. Li, Y. Zhang, J. Lin, and S. X. Wu, "Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdropper's CSI," *IEEE Trans. Signal Process.*, vol. 65, no. 17, pp. 4684–4697, Sep. 2017.

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

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

[42] D. Chen, Y. Cheng, W. Yang, J. Hu, and Y. Cai, "Physical layer security in cognitive untrusted relay networks," *IEEE Access*, vol. 5, pp. 7055–7065, Oct. 2017.

[43] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, A. Jeffrey and D. Zwillinger, Eds. New York, NY, USA: Academic, 2014.

[44] X. Guan, Y. Cai, and W. Yang, "On the reliability-security tradeoff and secrecy throughput in cooperative ARQ," *IEEE Commun. Lett.*, vol. 18, no. 3, pp. 479–482, Mar. 2014.

VAN NHAN VO received the B.S. and M.S. degrees in computer science from Da Nang University, Duy Tan University, Da Nang, Vietnam, in 2006 and 2014, respectively. 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 Internet of Things, information security, physical layer secrecy, RF-EH, wireless sensor networks, and the security of other advanced communication systems.

DUC-DUNG TRAN received the B.E. degree in electronics and telecommunications from the Hue University of Sciences, Vietnam, in 2013, and the M.Sc. degree in computer sciences from Duy Tan University, Danang, 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 R&D, Duy Tan University. His research interests include secrecy of physical layer communications, wireless communications, MIMO systems, and wireless energy harvesting networks.

CHAKCHAI SO-IN (SM'14) received the Ph.D. degree in computer engineering from Washington University in St. Louis, St. Louis, MO, USA, in 2010. He was an Intern at 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 80 publications and 10 books, including some in the IEEE JSAC, the *IEEE Magazines*, and Computer Network/ Network Security Labs. His research interests include mobile computing, wireless/sensor networks, signal processing, and computer networking and security. He has served as an Editor at SpringerPlus, PeerJ, and ECTI-CIT, and as a committee member for many conferences/journals, such as Globecom, ICC, VTC, WCNC, ICNP, ICNC, PIMRC, the IEEE TRANSACTIONS, the IEEE Letter/Magazines, and Computer Networks/Communications.

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 Post-Doctoral Researcher with Mälardalen University, Sweden. His research interests include cognitive radio networks, cooperative communication systems, millimeter wave communications, energy harvesting, and secure communications at the physical layer.