Received August 12, 2019, accepted September 1, 2019, date of publication September 17, 2019, date of current version October 7, 2019.
Digital Object Identifier 10.1109/ACCESS.2019.2941915

On Secure Wireless Sensor Networks With Cooperative Energy Harvesting Relaying

ANH-NHAT NGUYEN[1], VAN NHAN VO[1,2], CHAKCHAI SO-IN[1], (Senior Member, IEEE), DAC-BINH HA[3], SURASAK SANGUANPONG[4], AND ZUBAIR AHMED BAIG[5]
[1]Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[2]International School, Duy Tan University, Da Nang 550000, Vietnam
[3]Faculty of Electrical and Electronics Engineering, Duy Tan University, Da Nang 550000, Vietnam
[4]Department of Computer Engineering, Faculty of Engineering, Kasetsart University, Bangkok 10900, Thailand
[5]School of Information Technology, Deakin University, Geelong, VIC 3220, Australia

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

This work was supported in part by the grants from Enthuse Company Limited and Khon Kaen University under Grant Ent-KKU-2560-01, and in part by the Thailand Research Fund under the International Research Network Program under Grant IRN61W0006.

ABSTRACT In this paper, we investigate the physical layer security (PLS) of a wireless sensor network (WSN) that consists of a base station (BS), multiple sensor nodes (SNs), and multiple energy-limited relays (ERs) in the presence of a passive eavesdropper (EAV). We adopt a time-switching/power-splitting (TSPS) mechanism for information transmission. The communication protocol is divided into two phases. The purpose of the first phase is to decode information, and energy harvesting (EH) is performed in accordance with the TSPS protocol. The purpose of the second phase is to transmit information to multiple destinations using the amplify-and-forward (AF) technique. In this study, we introduce a multirelay cooperative scheme (MRCS) to improve the secrecy performance. We derive analytical expressions for the secrecy outage probability (SOP) of the MRCS and that of the noncooperative relay scheme (NCRS) by using the statistical characteristics of the signal-to-noise ratio (SNR). Specifically, we propose an optimal relay selection scheme to guarantee the security of the system for the MRCS. In addition, Monte Carlo simulation results are presented to confirm the accuracy of our analysis based on simulations of the secrecy performance under various system parameters, such as the positions and number of ERs, the EH time, and the EH efficiency coefficients. Finally, the simulation results show that the secrecy performance of our MRCS is higher than that of the NCRS and the traditional cooperative relay scheme (TCRS).

INDEX TERMS Energy harvesting, cooperative relay, time-switching/power-splitting, physical layer security.

I. INTRODUCTION

Wireless sensor networks (WSNs) have attracted substantial attention in the research community over the last few years, driven by a wealth of theoretical and practical challenges as well as an increasing number of practical civilian applications [1]–[4]. WSN applications play important roles in everyday life, in manufacturing and in the military context, such as for weather monitoring, health care services, animal tracking, security and tactical surveillance, intrusion detection, and disaster management [5]. However, due to resource limitations, WSNs have suffered from various issues related to reachability, energy consumption, and security [6].

Therefore, to improve the reachability of WSNs, forwarding nodes have been proposed and deployed [7]–[11] for real-world cases in which the distances between a BS and the SNs are greater than the transmission range [8]. In such a case, the BS and SNs cannot directly communicate with each other; this leads to a need for intermediate nodes that can act as relays. For example, R. Liu *et al*. investigated a WSN in which the SNs are located at predetermined locations to collect information about an infrastructure to be monitored on a large scale; hence, the SNs use relays to forward the collected physical information to the BS [9]. A. Vallimayil *et al*. described the characteristics of relays, various deployment

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

methods, and the internal behaviors of relays in WSNs. These authors concluded that the use of relay nodes has mainly been proposed for maximizing the reachability and ensuring the fault tolerance of networks [10].

Another important problem facing WSNs is energy consumption due to the limited battery capacities of the SNs [12]–[14]. Once the energy of an SN is depleted, it can no longer fulfill its role in the network. Therefore, EH techniques have promised to improve the lifetime of WSNs [15]–[17]. EH can be understood as a mechanism for generating energy from ambient surroundings (such as solar rays, thermoelectricity, radio frequency (RF) waves, and other physical phenomena) and thus providing an uninterrupted power supply for WSNs [18]–[20].

RF EH has recently emerged as a promising solution for prolonging the lifetime of WSNs due to its constant energy production capabilities [21], [22]. An SN can collect energy from ambient RF signals to power its operations. RF EH is especially attractive for relay WSNs that rely on ERs to extend their coverage areas and improve their system performance [23]–[25]. For instance, A. Nasir *et al*. considered the application of RF EH in relay WSNs based on two practical receiver architectures for EH, namely, time-switching-based relaying (TSR) and power-splitting-based relaying (PSR) [23]. S. Zhong *et al*. investigated the outage performance of an EH relay network in which the BS transmits information to the SNs with the help of multiple ERs by using the AF technique. These authors concluded that the outage performance of the system can be improved by employing EH ERs [25].

The cooperative relay scheme (which we call the TCRS) is a multirelay technique that is traditionally used for wireless communications because of its promising gains in throughput and energy efficiency. The basic idea of this scheme is that when a BS transmits a data signal to a SN, an ER acts in parallel to assist with the communication between the BS and the SN. Thus, the SN receives two signals and combines them to improve its decoding performance by using maximum ratio combining (MRC) [26]–[28].

In addition, the security of the communication between the SNs and BS in a WSN is also a key concern due to the broadcast nature of such communication. However, the SNs in a WSN are often incapable of employing traditional cryptographic techniques due to practical constraints such as limited energy resources and computing power [29]. To mitigate this problem, PLS has emerged as one potential approach because of its low complexity and low computing requirements [3], [30]. PLS was first exploited by C. E. Shannon [31] and later extended by A. D. Wyner [32], thereby establishing an information theory framework based on a classical model consisting of a source and a destination in the presence of an EAV. For PLS, the secrecy capacity is defined as the difference between the channel capacity of the primary link from the BS to the destination and that of the eavesdropping link from the BS to the EAV [33]. For example, A. Mukherjee provided an overview of low-complexity PLS schemes that are suitable for a WSN by investigating two scenarios: uplink communications from the SNs to the BS and downlink communications from the BS to the SNs [34]. A. Soni *et al*. reviewed existing wireless attack approaches and wireless security techniques. Finally, these authors concluded that a wireless PLS technique can provide satisfactory security for WSNs [35]. However, the PLS of RF EH WSNs using cooperative ERs has yet to be fully clarified in the literature.

Therefore, in this paper, we investigate the secrecy performance of AF relaying in an RF EH WSN with a passive EAV over a Rayleigh fading channel. Accordingly, based on our security analysis, we also propose an effective protocol for cooperative relaying in which the signals from the ERs are combined before being forwarded to the SN to improve the secrecy performance. The main contributions of this paper are as follows:

- We investigate the communication protocol in an EH WSN with multiple AF ERs and multiple SNs, in which the ERs guarantee that all SNs can receive signals from the BS.
- We introduce a new MRCS in which the signals from multiple ERs are combined before being forwarded to an SN to improve the PLS.
- We derive analytical expressions for the PLS in terms of the SOP for the NCRS and the MRCS. Accordingly, we propose an optimal ER selection algorithm to guarantee the security of the system for the MRCS.

The remainder of this paper is organized as follows: In Section II, related work on the PLS of cooperative ERs is presented. In Section III, a system model, a communication protocol, and two communication schemes, i.e., the NCRS and MRCS, are introduced. In Section IV, the SOPs of the two schemes are analyzed. In Section V, numerical results are presented and discussed. Finally, conclusions and future work are presented in Section VI.

II. RELATED WORK

In this section, we briefly summarize the related work concerning the PLS of relay EH WSNs.

To improve the security of large-scale wireless communications, several researchers have investigated PLS for relay WSNs [36]–[42]. For example, Q. Xu *et al*. investigated secure relay communications in a WSN for which the system model consisted of a BS and a SN assisted by a relay under monitoring by multiple EAVs. They considered two scenarios: one in which the relays and EAVs were each equipped with a single antenna, and one in which each was equipped with multiple antennas. Finally, they derived an expression for the SOP of BS-SN transmission [36]. W. Li *et al*. addressed the PLS issue for a WSN in the presence of a passive EAV with a multiantenna relay. They proposed two optimal power allocation strategies for use under power-constrained and power-unconstrained conditions. Accordingly, they derived the SOPs for EAVs in different positions [37]. However, the studies discussed above focused only on simple systems with a single relay.

To extend the system model, Q. Y. Liau *et al*. investigated a WSN consisting of a BS, a SN, an EAV, and two relays. They proposed a two-path successive relaying secrecy protocol in which the relays operated alternately in a time-division mode to continuously forward signals from the BS to the SN. Accordingly, they derived the intercept probability to evaluate the security performance and concluded that relaying is a useful approach for improving wireless PLS [40]. Y. Deng *et al*. proposed a relaying technique for a three-tier WSN whose system model included multiple SNs, access points, BSs, and EAVs. The access points were used as the relays to help transmit information from the SNs to the BSs. These authors derived compact expressions for the average secrecy rate to evaluate the PLS of the system [39]. Notably, these works focused only on prespecified relays and did not analyze the impact of relay selection.

Building on previous work, M. Qian *et al*. studied the PLS of a WSN with multiple relays in the presence of an EAV. These authors proposed two relay selection strategies: an exponential-complexity exhaustive search strategy and a linear-complexity relay ordering strategy, in which a partial set of relays is selected for forwarding the source signal to the SN. They concluded that the proposed schemes significantly outperformed the conventional all-relay and best-relay strategies in terms of secrecy capacity [41]. However, EH at the relays to further enhance the secrecy performance was not considered.

V. N. Vo *et al*. investigated EH at the ERs in a WSN in the presence of EAVs. Specifically, multiple ERs were considered to be harvesting energy from multiple power transfer stations (PTSs) for forwarding signals to the BS. These authors proposed a best-relay-and-best-jammer scheme to combat the multiple EAVs. An expression for the SOP was derived to analyze the security of the system. The results indicated that the proposed scheme outperformed both the best-relay-and-random-jammer scheme and the random-relay-and-best-jammer scheme in terms of secrecy performance [42]. Nevertheless, this work did not consider cooperative relays for enhancing the secrecy performance of the system.

To address the limitations of the above works in particular, to consider cooperative ERs with EH, we investigate the PLS in a relay WSN in this paper. Here, the ERs cooperate with each other to forward information in order to improve the security performance. To the best of our knowledge, no previous publications have studied this problem.

III. SYSTEM AND CHANNEL MODEL

A. SYSTEM MODEL

In this paper, an RF EH relay WSN is considered, as illustrated in Fig. 1. The system model consists of a BS, denoted by S; M SNs, denoted by D_m, $m \in \{1, \ldots, M\}$; and N ERs, denoted by R_n, $n \in \{1, \ldots, N\}$, in the presence of a passive EAV, denoted by E. The EAV attempts to extract information being sent from the ERs to the SNs. The BS communicates with ERs and SNs via control messages [41], [51]. Each device is equipped with a single antenna and operates in half-duplex mode. The channel coefficients of the $S \to R_n$, $R_n \to D_m$, and $R_n \to E$ links are denoted by h_{SR_n}, $h_{R_nD_m}$, and h_{R_nE}, respectively. The distances of the $S \to R_n$, $R_n \to D_m$, and $R_n \to E$ links are denoted by d_{SR_n}, $d_{R_nD_m}$, and d_{R_nE}, respectively.

We assume that all channels are modeled as Rayleigh fading channels and that the channel coefficients are RVs distributed following the Rayleigh model [43]. The corresponding cumulative distribution function (CDF) and probability density function (PDF) of a channel are given as follows:

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

and

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

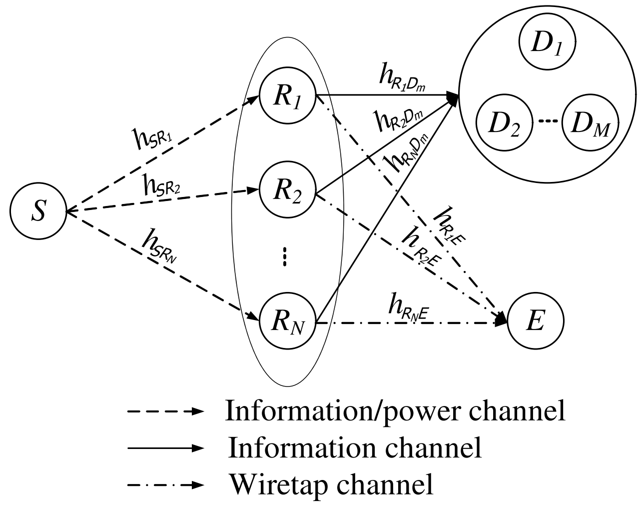

FIGURE 1. System model of an RF EH relay WSN.

TABLE 1. List of notations.

Notation	Description
h_{XY}	The channel coefficient of the link from $X \to Y$
d_{XY}	The distance of the link from $X \to Y$
g_{XY}	The random variable (RV) representing $\|h_{XY}\|^2/d_{XY}^{\sigma}$
Ω_{XY}	The mean channel gain of the link from $X \to Y$
α	The EH time proportion
ρ_{R_n}	The power splitting ratio (PS) of the BS for R_n
η	The EH efficiency coefficient
ε_{R_n}	The EH at R_n
$\mathcal{CN}(0, N_0)$	A scalar complex Gaussian distribution with zero mean and variance N_0
N_0	The noise power
P_{R_n}	The transmit power at R_n
γ_X	The end-to-end signal-to-noise ratio (SNR) at X
$C_{SEC_{D_m}}$	The instantaneous secrecy capacity at D_m
Θ_{D_m}	The SOP of D_m
Θ	The SOP of the considered system
Φ_{D_m}	The outage probability (OP) of D_m
Φ	The OP of the considered system
R_O	The target information rate
R_S	The target secrecy rate

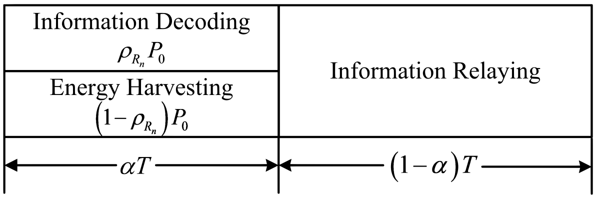

FIGURE 2. The TSPS mechanism at the ERs. A single time block T is used for both the information decoding and EH phase and the information relaying phase.

where $g_{XY} = |h_{XY}|^2/d_{XY}^{\sigma}$; the RVs h_{XY} and d_{XY} refer to the channel coefficient and the distance from $X \to Y$, respectively; σ is the path loss factor; and $\Omega_{XY} = \mathbf{E}\left[|h_{XY}|^2\right]/d_{XY}^{\sigma}$ is the mean channel gain, where $\mathbf{E}[\cdot]$ denotes the expectation operation.

B. COMMUNICATION PROTOCOL

In the considered system, we apply the TSPS protocol [24], where the communication protocol is divided into two phases, as illustrated in Fig. 2. First, the ERs receive information from the BS. Then, the selected ERs send information to the selected SN subject to eavesdropping by the EAV. Accordingly, the communication protocol is described as follows:

- In the first phase, a BS S transmits information to the ERs in αT time, where T is a time block and α $(0 < \alpha < 1)$ is the proportion of the time block dedicated to $S \to R_n$ transmission. As described in [24], the transmit power of the BS is split such that the received signal is split into two streams with PSs of ρ_{R_n} and $1 - \rho_{R_n}$ for information decoding and EH, respectively, where $0 < \rho_{R_n} < 1$. Thus, the information received at the n-th ER is written as follows:

$$y_{SR_n}(t) = \sqrt{\frac{\rho_{R_n} P_0}{d_{SR_n}^{\sigma}}} h_{SR_n} x(t) + n_{R_n}, \tag{3}$$

  where P_0 is the transmit power of the BS, $x(t)$ is a transmitted signal, and n_{R_n} is the additive white Gaussian noise (AWGN) at R_n, $n_{R_n} \sim \mathcal{CN}(0, N_0)$. The EH at R_n is expressed as follows:

$$\varepsilon_{R_n} = \frac{\eta\alpha\left(1 - \rho_{R_n}\right) P_0 \left|h_{SR_n}\right|^2 T}{d_{SR_n}^{\sigma}}, \tag{4}$$

  where η is the EH efficiency coefficient, which depends on the rectification $(0 < \eta < 1)$. Here, we assume that the EH efficiency coefficient is the same for all ERs [43].
- In the second phase, the n-th ER performs AF transmission of the signal $y_{SR_n}(t)$ to the SN D_m. Hence, the received signal at D_m is given by [44]

$$y_{R_n D_m}(t) = \sqrt{\frac{P_{R_n}}{\mathbf{E}\left|y_{SR_n}(t)\right|^2}} \frac{h_{R_n D_m}}{\sqrt{d_{R_n D_m}^{\sigma}}} y_{SR_n}(t) + n_{D_m}, \tag{5}$$

  where $n_{D_m} \sim \mathcal{CN}(0, N_0)$ is the AWGN at D_m and the transmit power at R_n in the remaining time $(1-\alpha)T$ is expressed as

$$P_{R_n} = \frac{\eta\alpha\left(1 - \rho_{R_n}\right) P_0 \left|h_{SR_n}\right|^2}{(1-\alpha)\, d_{SR_n}^{\sigma}} = c\left(1 - \rho_{R_n}\right) P_0 g_{SR_n}, \tag{6}$$

  where $c = \frac{\eta\alpha}{1-\alpha}$ and $g_{SR_n} = \frac{\left|h_{SR_n}\right|^2}{d_{SR_n}^{\sigma}}$.

C. CHANNEL CAPACITY

Based on the communication protocol, the end-to-end SNR at the m-th SN D_m for the signal received via the n-th ER R_n can be defined as follows:

$$\gamma_{D_m} = \frac{\delta \rho_{R_n} {P_0}^2 {g_{SR_n}}^2 g_{R_n D_m}}{\left(\delta P_0 g_{SR_n} g_{R_n D_m} + \rho_{R_n} P_0 g_{SR_n}\right) N_0 + N_0^2}, \tag{7}$$

where $\delta = c\left(1 - \rho_{R_n}\right)$ and $g_{R_n D_m} = \frac{\left|h_{R_n D_m}\right|^2}{d_{R_n D_m}^{\sigma}}$. Furthermore, the instantaneous legal channel capacity at D_m is expressed as follows:

$$C_{D_m} = (1-\alpha)\log_2\left(1 + \gamma_{D_m}\right). \tag{8}$$

Similar to (7) and (8), the end-to-end SNR and the instantaneous illegal channel capacity at E are given by

$$\gamma_E = \frac{\delta \rho_{R_n} {P_0}^2 {g_{SR_n}}^2 g_{R_n E}}{\left(\delta P_0 g_{SR_n} g_{R_n E} + \rho_{R_n} P_0 g_{SR_n}\right) N_0 + N_0^2}, \tag{9}$$

$$C_E = (1-\alpha)\log_2\left(1 + \gamma_E\right), \tag{10}$$

where $g_{R_n E} = \frac{\left|h_{R_n E}\right|^2}{d_{R_n E}^{\sigma}}$.

D. SCHEDULING SCHEMES

In this subsection, we present two schemes for selecting the best ER and cooperative ERs to forward the information from the BS to the SN.

- *The noncooperative ER scheme (NCRS)*: The best ER is selected from among the N ERs to help the BS send the signal to the SN such that the best possible channel gain of the $S \to R_n$ link is achieved [45], [46], i.e.,

$$|h_{SR^*}|^2 = \max_{n=1,\ldots,N}\left\{\left|h_{SR_n}\right|^2\right\}, \tag{11}$$

  where R^* is the best ER. Accordingly, the EH at R_n for the NCRS can be expressed as follows:

$$\varepsilon_{R^*}^{NCRS} = \frac{\eta\alpha\left(1 - \rho_{R^*}\right) P_0 |h_{SR^*}|^2 T}{d_{SR^*}^{\sigma}} = \eta\alpha\left(1 - \rho_{R^*}\right) P_0 g_{SR^*} T, \tag{12}$$

  where $g_{SR^*} = \frac{|h_{SR^*}|^2}{d_{SR^*}^{\sigma}}$. Furthermore, the CDF and PDF of g_{SR^*} are obtained as follows:

$$F_{g_{SR^*}}(x) = \left(1 - e^{-\frac{x}{\Omega_{SR^*}}}\right)^N, \tag{13}$$

$$f_{g_{SR^*}}(x) = \frac{N}{\Omega_{SR^*}} e^{-\frac{1}{\Omega_{SR^*}}} \left(1 - e^{-\frac{x}{\Omega_{SR^*}}}\right)^{N-1}, \quad (14)$$

where $\Omega_{SR^*} = \frac{\mathbf{E}\left[|h_{SR^*}|^2\right]}{d^{\sigma}_{SR^*}}$.

- *The multirelay cooperative scheme (MRCS)*: To improve the secrecy performance, we investigate the MRCS, i.e., the scheme in which the signals from multiple ERs are combined before being forwarded to D_m. Accordingly, the CDF and PDF of g_{RD_m} can be obtained as follows [47]:

$$F_{g_{RD_m}}(x) = \sum_{n=1}^{N} \prod_{\substack{j=1 \\ j \neq n}}^{N} \frac{\Omega_{R_nD_m} F_{g_{R_nD_m}}(x)}{\Omega_{R_nD_m} - \Omega_{R_jD_m}}, \quad \text{if } \Omega_{R_nD_m} \neq \Omega_{R_jD_m}; \quad (15)$$

$$f_{g_{RD_m}}(x) = \sum_{n=1}^{N} \prod_{\substack{j=1 \\ j \neq n}}^{N} \frac{\Omega_{R_nD_m} f_{g_{R_nD_m}}(x)}{\Omega_{R_nD_m} - \Omega_{R_jD_m}}, \quad \text{if } \Omega_{R_nD_m} \neq \Omega_{R_jD_m}; \quad (16)$$

where $g_{RD_m} = \sum_{n=1}^{N} g_{R_nD_m}$, $\Omega_{R_nD_m} = \frac{\mathbf{E}\left[\left|h_{R_nD_m}\right|^2\right]}{d^{\sigma}_{R_nD_m}}$, and $\Omega_{R_jD_m} = \frac{\mathbf{E}\left[\left|h_{R_jD_m}\right|^2\right]}{d^{\sigma}_{R_jD_m}}$.

IV. SECRECY PERFORMANCE ANALYSIS

In this section, we derive the expressions for the SOPs of the two scheduling schemes (i.e., NCRS and MRCS) to evaluate the secrecy performance of the considered system.

A. SECRECY CAPACITY

According to the definition of the secrecy capacity presented in [32], [48], the instantaneous secrecy capacity of a wireless transmission from S to D_m in the presence of a passive EAV is defined as

$$C_{SEC_{D_m}} = \left[C_{D_m} - C_E\right]^+ = \begin{cases} (1-\alpha)\log_2\left(\frac{1+\gamma_{D_m}}{1+\gamma_E}\right), & \gamma_{D_m} > \gamma_E \\ 0, & \gamma_{D_m} \leq \gamma_E, \end{cases} \quad (17)$$

where $C_{SEC_{D_m}} \in \left\{C^{NCRS}_{SEC_{D_m}}, C^{MRCS}_{SEC_{D_m}}\right\}$.

To guarantee that all SNs can receive signals from the BS, the selected SN is chosen such that the secrecy capacity is the lowest, i.e.,

$$C_{SEC} = \min_{m=1,\ldots,M} \left\{C_{SEC_{D_m}}\right\}, \quad (18)$$

where $C_{SEC} \in \left\{C^{NCRS}_{SEC}, C^{MRCS}_{SEC}\right\}$.

B. SECRECY PERFORMANCE ANALYSIS

Similar to what was done in [39], [49], the SOP is used to evaluate the secrecy performance of the WSN. For the m-th SN, this metric is defined as the probability of the instantaneous secrecy capacity dropping below a target secrecy rate R_S, i.e.,

$$\Theta_{D_m} = \Pr\left\{C_{SEC_{D_m}} < R_S\right\}, \quad (19)$$

where $\Theta_{D_m} \in \left\{\Theta^{NCRS}_{D_m}, \Theta^{MRCS}_{D_m}\right\}$ and $\Pr\{\cdot\}$ is a probability function. By substituting (17) into (19), the SOP for D_m can be rewritten as follows:

$$\Theta_{D_m} = \Pr\left\{(1-\alpha)\log_2\left(\frac{1+\gamma_{D_m}}{1+\gamma_E}\right) < R_S\right\}. \quad (20)$$

Note that we perform our analysis for the high-SNR regime because the signals from the BS to the ERs, from SNs to other SNs, and from the SNs to the EAVs are of much higher power than the background noise power, i.e., $\gamma_0 = \frac{P_0}{N_0} \to \infty$ [50], [51]. Thus, γ_{D_m} and γ_E can be approximated as

$$\gamma_{D_m} \simeq \frac{\delta\rho_{R_n}\gamma_0 g_{SR_n} g_{R_nD_m}}{\delta g_{R_nD_m} + \rho_{R_n}} = \underbrace{\delta\rho_{R_n}\gamma_0 g_{SR_n}}_{X_{SR_n}} \underbrace{\frac{g_{R_nD_m}}{\delta g_{R_nD_m} + \rho_{R_n}}}_{Y_{R_nD_m}}, \quad (21)$$

$$\gamma_E \simeq \frac{\delta\rho_{R_n}\gamma_0 g_{SR_n} g_{R_nE}}{\delta g_{R_nE} + \rho_{R_n}} = \underbrace{\delta\rho_{R_n}\gamma_0 g_{SR_n}}_{X_{SR_n}} \underbrace{\frac{g_{R_nE}}{\delta \gamma_{R_nE} + \rho_{R_n}}}_{Y_{R_nE}}. \quad (22)$$

By substituting (21) and (22) into (20), the SOP for the m-th SN Θ_{D_m} can be approximated as [51]

$$\begin{aligned} \Theta_{D_m} &= \Pr\left\{\frac{1+X_{SR_n}Y_{R_nD_m}}{1+X_{SR_n}Y_{R_nE}} < 2^{R_S/(1-\alpha)}\right\} \\ &= \Pr\left\{Y_{R_nD_m} < \frac{\theta}{X_{SR_n}} + (\theta+1)\,Y_{R_nE}\right\} \\ &= \int_0^\infty f_{Y_{R_nE}}(z) \int_0^\infty f_{X_{SR_n}}(x)\, F_{Y_{R_nD_m}}(\varphi)\,dxdz \\ &\simeq \int_0^{v_3} f_{Y_{R_nE}}(z) \int_0^\infty f_{X_{SR_n}}(x)\, F_{Y_{R_nD_m}}(\varphi)\,dxdz, \end{aligned} \quad (23)$$

where $\varphi = \theta/x + (\theta+1)\,z$ and $\theta = 2^{R_S/(1-\alpha)} - 1$. By setting $v_1 = \delta\rho_{R_n}\gamma_0$, the CDF and PDF of the RV X_{SR_n} can be expressed as

$$F_{X_{SR_n}}(x) = F_{g_{SR_n}}\left(\frac{x}{v_1}\right), \quad (24)$$

$$f_{X_{SR_n}}(x) = f_{g_{SR_n}}\left(\frac{x}{v_1}\right). \quad (25)$$

By applying probabilistic characteristics, the CDF of $Y_{R_n\xi}$, $\xi \in \{D_m, E\}$, can be expressed as

$$F_{Y_{R_n\xi}} = \Pr\left\{Y_{R_n\xi} < x\right\} = \Pr\left\{\frac{g_{R_n\xi}}{\delta g_{R_n\xi} + \rho_{R_n}} < x\right\}$$

$$= \Pr\left\{g_{R_n\xi}\left(1-\delta x\right) < x\rho_{R_n}\right\}$$
$$= \begin{cases} 1, & x \geq \delta^{-1} \\ \Pr\left\{g_{R_n\xi} < \dfrac{x\rho_{R_n}}{1-\delta x}\right\}, & x < \delta^{-1}. \end{cases} \quad (26)$$

After several calculation steps, the CDF and PDF of $Y_{R_n\xi}$ are obtained as follows:

$$F_{Y_{R_n\xi}}(x) = \begin{cases} 1, & x \geq v_3 \\ 1 - e^{-\frac{1}{\Omega_{R_n\xi}}\frac{v_2 x}{v_3 - x}}, & x < v_3, \end{cases} \quad (27)$$

$$f_{Y_{R_n\xi}}(x) = \begin{cases} 0, & x \geq v_3 \\ \dfrac{1}{\Omega_{R_n\xi}}\dfrac{v_2 v_3}{(v_3 - x)^2} e^{-\frac{1}{\Omega_{R_n\xi}}\frac{v_2 x}{v_3 - x}}, & x < v_3, \end{cases} \quad (28)$$

where $v_2 = \rho_{R_n}\delta^{-1}$ and $v_3 = \delta^{-1}$.

Furthermore, the SOP for the multiple SNs is expressed as follows [39]:

$$\Theta = \Pr\left\{C_{SEC} < R_S\right\}, \quad (29)$$

where $\Theta \in \left\{\Theta^{NCRS}, \Theta^{MRCS}\right\}$. By substituting (18) and (19) into (29), we can rewrite the SOP of the considered system as

$$\Theta = \Pr\left\{\min\left\{C_{SEC_{D_m}}\right\} < R_S\right\}$$
$$= 1 - \prod_{m=1}^{M}\left(1 - \Pr\left\{C_{SEC_{D_m}} < R_S\right\}\right)$$
$$= 1 - \prod_{m=1}^{M}\left(1 - \Theta_{D_m}\right). \quad (30)$$

Next, the SOPs for the NCRS and MRCS are given by the following two theorems.

Theorem 1: For the NCRS, the SOP of the m-th SN is expressed by equation (31)*, as shown at the top of the next page. Therefore, the SOP of the considered system for the NCRS is obtained as follows:*

$$\Theta^{NCRS} = 1 - \prod_{m=1}^{M}\left(1 - \Theta_{D_m}^{NCRS}\right). \quad (32)$$

Proof: The proof is given in Appendix A.

Theorem 2: For the MRCS, the SOP of the m-th SN is expressed by equation (33) *(see the next page). Therefore, the SOP of the considered system for the MRCS is obtained as follows:*

$$\Theta^{MRCS} = 1 - \prod_{m=1}^{M}\left(1 - \Theta_{D_m}^{MRCS}\right). \quad (34)$$

Proof: The proof is given in Appendix B.

Algorithm 1 Algorithm for Determining γ_0^*

Data: Predetermined system parameters, array $\gamma_0 \in (0, \psi)$, security constraint ω
Result: γ_0^*

Set the initial step: $i \leftarrow 1$;
Set the initial value: $\gamma_0^* \leftarrow 0$;
for $(i; \text{length}(\gamma_0); i++)$ **do**
  Calculate $\Theta^{(MRCS)}(i)$ in (34);
  if $\Theta^{(MRCS)}(i) = \omega$ **then**
    $\gamma_0^* = \gamma_0(i)$;
    break;
  end if
  if $\Theta^{(MRCS)}(i) < \omega$ **then**
    $\gamma_0^* = \gamma_0(i-1)$;
    break;
  end if
end for
return γ_0^*;

Algorithm 2 Algorithm for Determining N^*

Data: Predetermined system parameters, array $N \in (1, \kappa)$, security constraint ω
Result: N^*

Set the initial step: $i \leftarrow 1$;
Set the initial value: $N^* \leftarrow 1$;
for $(i; \text{length}(N); i++)$ **do**
  Calculate $\Theta^{(MRCS)}(i)$ in (34);
  if $\Theta^{(MRCS)}(i) = \omega$ **then**
    $N^* = N(i)$;
    break;
  end if
  if $\Theta^{(MRCS)}(i) < \omega$ **then**
    $N^* = N(i-1)$;
    break;
  end if
end for
return N^*;

Based on the secrecy performance analysis, we predict that the end-to-end SNRs at the SN and EAV will both include γ_0 (see (21) and (22)). Therefore, with the NCRS, the SOP will improve only negligibly with increasing γ_0 because both the numerator and denominator of the secrecy capacity expression given in (17) will increase. In contrast, with the MRCS, the SOP will significantly decrease when γ_0 increases because the SNR at the SN will be the result of combining the signals from multiple ERs, i.e., the numerator will be larger than the denominator in (17). Thus, an optimal γ_0 value exists in the MRCS such that the security of the considered system can be guaranteed.

Therefore, we propose an algorithm for determining the optimal transmit power to guarantee the security of the system as follows: the value of γ_0 is divided into an array, and the values in this array are substituted into (34) until the SOP for

$$\Theta_{D_m}^{NCRS} = 1 - \frac{N v_2 v_3}{\Omega_{SR^*}\Omega_{R_nE} v_1} \sum_{k=0}^{N-1} \frac{(-1)^k (N-1)!}{k!\,(N-1-k)!} e^{v_2\left(\frac{1}{\Omega_{R_nD_m}}+\frac{1}{\Omega_{R_nE}}\right)} 2\sqrt{\frac{\Omega_{SR^*} v_1 v_2 v_3 \theta}{\Omega_{R_nD_m}(k+1)}}$$
$$\times \int_0^{v_3/(\theta+1)} \frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2 v_3}{v_3-z}-\frac{1}{\Omega_{SR^*}\Omega_{R_nD_m}}\frac{\Omega_{R_nD_m}(k+1)\theta+\Omega_{SR^*}v_1v_2v_3}{v_1[v_3-(\theta+1)z]}}}{(v_3-z)^2\,[v_3-(\theta+1)z]} K_1\left(\frac{2\sqrt{(k+1)\,v_2v_3\theta/\Omega_{SR^*}\Omega_{R_nD_m}v_1}}{[v_3-(\theta+1)z]}\right) dz. \tag{31}$$

$$\Theta_{D_m}^{MRCS} = e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2[v_3/(\theta+1)]}{v_3-[v_3/(\theta+1)]}} + \frac{v_2 v_3}{\Omega_{SR_n}\Omega_{R_nE}v_1} e^{\frac{v_2}{\Omega_{R_nE}}} \int_0^{v_3/(\theta+1)} \int_0^{\theta/[v_3-(\theta+1)z]} \frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2v_3}{v_3-z}-\frac{1}{\Omega_{SR_n}}\frac{x}{v_1}}}{(v_3-z)^2} dxdz$$
$$+ \sum_{i=1}^{N}\prod_{\substack{j=1\\ j\neq i}}^{N} \frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m}-\Omega_{R_jD_m}} \frac{v_2v_3}{\Omega_{SR_n}\Omega_{R_nE}v_1} e^{\frac{v_2}{\Omega_{R_nE}}} \int_0^{v_3/(\theta+1)} \int_{\theta/[v_3-(\theta+1)z]}^{\infty} \frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2v_3}{v_3-z}-\frac{1}{\Omega_{SR_n}}\frac{x}{v_1}}}{(v_3-z)^2} dxdz$$
$$- \sum_{i=1}^{N}\prod_{\substack{j=1\\ j\neq i}}^{N} \frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m}-\Omega_{R_jD_m}} \frac{v_2v_3}{\Omega_{SR_n}\Omega_{R_nE}v_1} e^{v_2\left(\frac{1}{\Omega_{R_nE}}+\frac{1}{\Omega_{R_nD_m}}\right)} 2\sqrt{\frac{\Omega_{SR_n}v_1v_2v_3\theta}{\Omega_{R_nD_m}}}$$
$$\times \int_0^{v_3/(\theta+1)} \frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2v_3}{v_3-z}-\frac{1}{\Omega_{R_nD_m}\Omega_{SR_n}}\frac{\Omega_{R_nD_m}\theta+\Omega_{SR_n}v_1v_2v_3}{v_1[v_3-(\theta+1)z]}}}{(v_3-z)^2\,[v_3-(\theta+1)z]} K_1\left(\frac{2\sqrt{v_2v_3\theta/\Omega_{R_nD_m}\Omega_{SR_n}v_1}}{[v_3-(\theta+1)z]}\right) dz. \tag{33}$$

the MRCS satisfies the constraint $\Theta^{MRCS} < \omega$, where ω is the security constraint. The optimal transmit power algorithm is detailed in **Algorithm 1**.

The time complexity of **Algorithm 1** is exactly the time complexity of the "for" loop. First, in step 4, calculating $\Theta^{(MRCS)}(i)$ takes $O(n^2)$ time. Steps 5 to 12 take $O(n)$ time. Therefore, the "for" loop is computed in $O(\text{length}(\gamma_0)n^2)$ time, which is also the time complexity of **Algorithm 1**.

Similar to the approach of **Algorithm 1**, we also propose an algorithm for selecting the optimal number of ERs for the MRCS to reduce the implementation cost while still ensuring sufficient secrecy performance. The algorithm for selecting the optimal number of ERs for the MRCS is detailed in **Algorithm 2**.

C. THROUGHPUT ANALYSIS

In this subsection, the throughput is determined by evaluating the outage probability (OP) of the m-th SN, i.e., Φ_{D_m}, at a target information rate R_O (expressed in bits/sec/Hz), where $R_O = \log_2(1+\phi)$ and ϕ is the threshold value of the SNR for correct data detection at the SN. Specifically, Φ_{D_m} is given by [23]

$$\Phi_{D_m} = \Pr\left[\gamma_{D_m} < \phi\right] = \int_0^{\phi\delta/v_1} f_{g_{SR_n}}(x)\,dx + \int_{\phi\delta/v_1}^{\infty} f_{g_{SR_n}}(x) F_{g_{R_nD_m}}(\varsigma)\,dx, \tag{35}$$

where $\Phi_{D_m} \in \left\{\Phi_{D_m}^{NCRS}, \Phi_{D_m}^{MRCS}\right\}$, $C_{D_m} \in \left\{C_{D_m}^{NCRS}, C_{D_m}^{MRCS}\right\}$, $\phi = 2^{R_O/(1-\alpha)} - 1$, and $\varsigma = \frac{\phi\rho_{R_n}}{v_1x-\phi\delta}$. Similarly, the selected SN is chosen such that the channel capacity is the lowest, and we can rewrite the OP of the considered system as

$$\Phi = 1 - \prod_{m=1}^{M}\left(1-\Phi_{D_m}\right), \tag{36}$$

where $\Phi \in \left\{\Phi^{NCRS}, \Phi^{MRCS}\right\}$.

Theorem 3: For the NCRS, the OP of the m-th SN is expressed by equation (37) *(see the next page).*

Therefore, the OP of the considered system for the NCRS is obtained as follows:

$$\Phi^{NCRS} = 1 - \prod_{m=1}^{M}\left(1-\Phi_{D_m}^{NCRS}\right). \tag{38}$$

Proof: The proof is given in Appendix C.

Theorem 4: For the MRCS, the OP of the m-th SN is expressed by equation (39) *(see the next page).*

Therefore, the OP of the considered system for the MRCS is obtained as follows:

$$\Phi^{MRCS} = 1 - \prod_{m=1}^{M}\left(1-\Phi_{D_m}^{MRCS}\right). \tag{40}$$

Proof: The proof is given in Appendix D.

Given that $(1-\alpha)T$ is the effective communication time within the time block T (expressed in seconds), the throughput is given by [52], [53]

$$\tau = (1-\alpha)(1-\Phi) R_O, \tag{41}$$

where $\tau \in \{\tau^{NCRS}, \tau^{MRCS}\}$.

$$\Phi_{D_m}^{NCRS} = 1 - \frac{N}{\Omega_{SR^*}} \sum_{k=0}^{N-1} \frac{(-1)^k (N-1)!}{k! (N-1-k)!} e^{-\frac{(1+k)\phi\delta}{v_1 \Omega_{SR^*}}} 2\sqrt{\frac{\Omega_{SR^*}\phi\rho_{R_n} v_1}{\Omega_{R_n D_m}(1+k)}} K_1 \left(2\sqrt{\frac{\phi\rho_{R_n}(1+k)}{\Omega_{SR^*}\Omega_{R_n D_m} v_1}}\right). \quad (37)$$

$$\Phi_{D_m}^{MRCS} = \gamma\left(1, \frac{\phi\delta}{\Omega_{SR_n} v_1}\right) + \sum_{i=1}^{N} \prod_{\substack{j=1 \\ j\neq i}}^{N} \frac{\Omega_{R_n D_m}}{\Omega_{R_n D_m} - \Omega_{R_j D_m}} \Gamma\left(1, \frac{\phi\delta}{\Omega_{SR_n} v_1}\right) - \sum_{i=1}^{N} \prod_{\substack{j=1 \\ j\neq i}}^{N} \frac{\Omega_{R_n D_m}}{\Omega_{R_n D_m} - \Omega_{R_j D_m}} \frac{1}{\Omega_{SR_n} v_1} e^{-\frac{\phi\delta}{\Omega_{SR_n} v_1}} 2\sqrt{\frac{\Omega_{SR_n}\phi\rho_{R_n} v_1}{\Omega_{R_n D_m}}} K_1\left(2\sqrt{\frac{\phi\rho_{R_n}}{\Omega_{SR_n}\Omega_{R_n D_m} v_1}}\right). \quad (39)$$

V. NUMERICAL RESULTS

This section presents and discusses numerical results obtained from Monte Carlo simulations. Specifically, the effects of various system parameters, such as γ_0, the distance d_{SR} from the BS to an ER, the distance d_{RD} from an ER to an SN, the number of ERs N, the number of SNs M, the EH time proportion α, the EH efficiency coefficient η, and the PS ρ, are discussed. The following system parameters are used for both analysis and simulation [47], [49]: $d_{SR} \in [0.5, 2.5]$, $d_{RD} \in [0.5, 5]$, $d_{RE} = 2$, $R_S = 0.01$, $R_O = 0.5$, $\alpha \in [0.1, 0.9]$, $\eta \in [0.1, 0.9]$, $\omega = 0.01$, $\rho_{R_n} = \rho \in [0.1, 0.9]$, $\gamma_0 \in [0, 30]$ (dB), $M \in [1, 10]$, and $N \in [1, 10]$. We evaluate and compare the security performance of the following three schemes:

- The noncooperative ER scheme (NCRS): The best ER is chosen from among multiple ERs to forward the signal to the SN [45], [46].
- The traditional cooperative relay scheme (TCRS): The BS cooperates with the best ER to forward the signal to the SN [54].
- The multirelay cooperative scheme (MRCS): The ERs cooperate to forward the signal to the SN.

Fig. 3 illustrates the impact of γ_0 on the SOP. It can be seen that with increasing γ_0, the SOP decreases negligibly for the NCRS but decreases very quickly for the TCRS and MRCS. This behavior can be explained as follows: The channel capacities from the BS to the SN and from the BS to the EAV are functions of γ_0. In the NCRS, the expressions for the channel capacities of the BS-SN link and the BS-EAV link each contain a single instance of γ_0. In contrast, in the TCRS and MRCS, the channel capacity of the BS-SN link is obtained from multiple channel capacities that are functions of γ_0, while the channel capacity of the BS-EAV link is still a single function of γ_0. Therefore, the secrecy performances of the MRCS and TCRS are significantly improved.

Furthermore, when we set the secrecy constraint to 0.01 (i.e., set the probability of being monitored by the EAV to 1%), the MRCS can achieve secure transmission at $\gamma_0^* = 17.5$ (dB) (this value is found via **Algorithm 1**). Thus, we can conclude that the secrecy performance of the MRCS is better than those of both the NCRS and the TCRS, and this trend also holds for the remaining simulations.

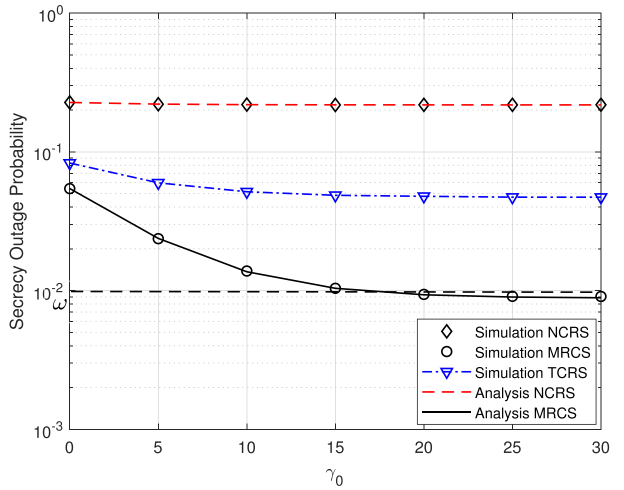

FIGURE 3. SOP versus γ_0 (dB), with $N = M = 5$, $\alpha = 0.4$, $\rho = 0.6$, $\eta = 0.7$, and $R_S = 0.01$.

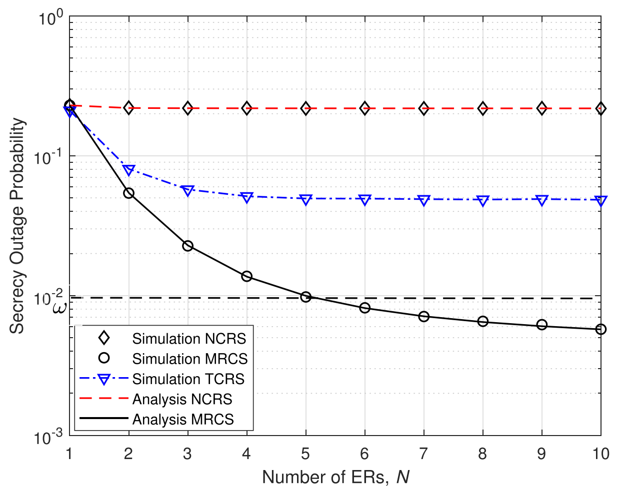

FIGURE 4. SOP versus the number of ERs N, with $M = 5$, $\gamma_0 = 10$ (dB), $\alpha = 0.4$, $\rho = 0.6$, $\eta = 0.7$, and $R_S = 0.01$.

Fig. 4 shows the impact of the number of relays on the SOP. We can see that as the number of SNs increases, the secrecy

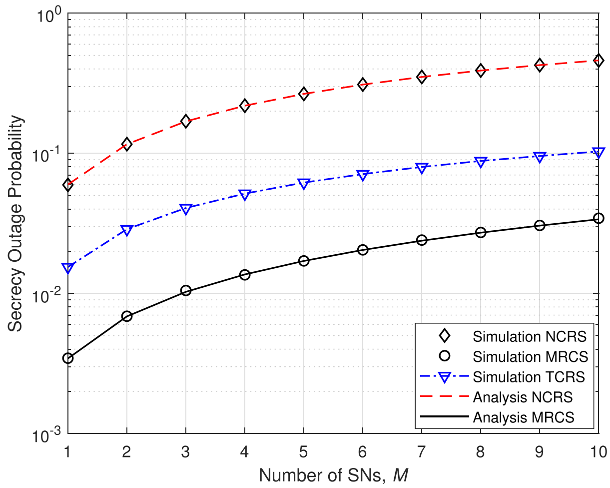

FIGURE 5. SOP versus the number of SNs M, with $N = 5$, $\gamma_0 = 10$ (dB), $\alpha = 0.4$, $\rho = 0.6$, $\eta = 0.7$, and $R_S = 0.01$.

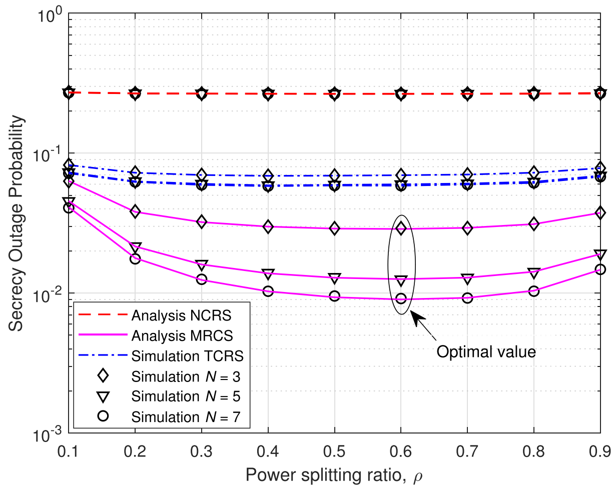

FIGURE 7. SOP versus the PS ρ, with $M = 5$, $\gamma_0 = 10$ (dB), $\alpha = 0.4$, $\eta = 0.7$, and $R_S = 0.01$.

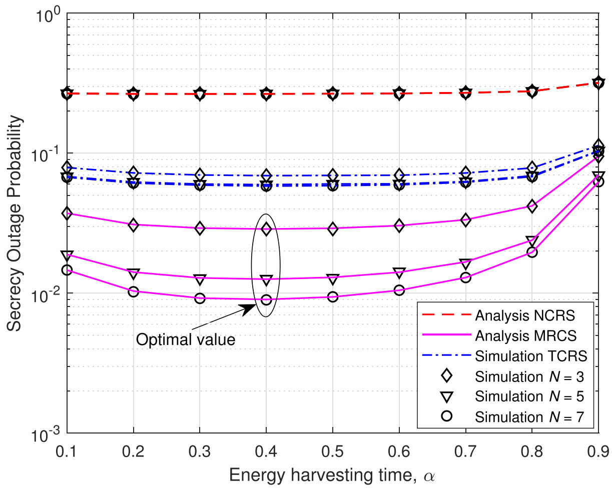

FIGURE 6. SOP versus the EH time proportion α, with $M = 5$, $\gamma_0 = 10$ (dB), $\rho = 0.6$, $\eta = 0.7$, and $R_S = 0.01$.

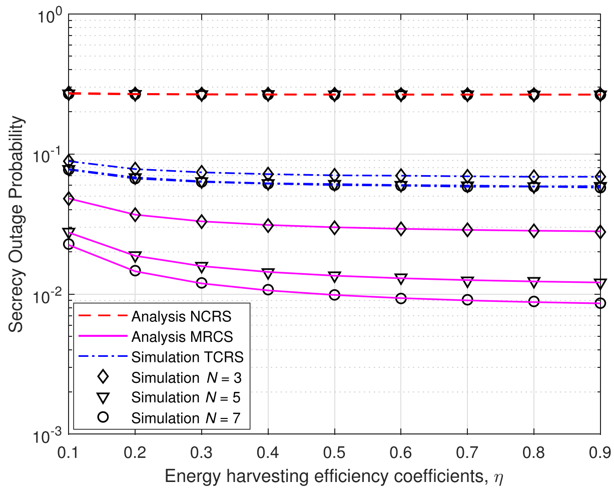

FIGURE 8. SOP versus the EH efficiency coefficient η, with $M = 5$, $\gamma_0 = 10$ (dB), $\alpha = 0.4$, $\rho = 0.6$, and $R_S = 0.01$.

performance shows minimal improvement for the NCRS but increases very quickly for the TCRS and MRCS. This is because in the NCRS, only the best ER is selected, while in both the TCRS and MRCS, multiple ERs are selected to contribute to the combined information that will be forwarded to the SN. Similar to Fig. 3, for the MRCS, there exists an optimal number of ERs that will guarantee the security of the considered system. Note that the optimal number of ERs for the MRCS, $N^* = 6$, is found via **Algorithm 2**.

Fig. 5 depicts the impact of the number of SNs on the SOP. As the number of SNs increases, the SOPs of the three schemes also increase. This is because the diversity gain at the SNs increases as the number of SNs increases. Furthermore, the ERs forward the signals to the worst SN to guarantee the transmission of information to all SNs. Thus, the probability of successful communication for all SNs decreases with an increasing number of SNs.

Fig. 6 illustrates the impact of the EH time proportion and the number of ERs on the secrecy performance. The SOP initially decreases as α increases, reaches an intermediate point, and then increases again. This result occurs because when the EH time proportion is too small, the ERs do not harvest a substantial amount of power; thus, the transmit power levels of the ERs are not sufficient. On the other hand, when α is very large, the transmit power levels at the ERs are quite high, allowing the EAV to more easily capture the signal.

Fig. 7 presents the impact of the PS ρ and the number of ERs on the SOP. Similar to Fig. 6, the SOP decreases to a certain point and then increases as ρ increases. This is because the ERs do not have sufficient power to decode the information when ρ is small, whereas when ρ is large, the transmit power of the ERs is not sufficient to forward the signal to the SN.

Fig. 8 shows the impact of the EH efficiency coefficient η and the number of ERs on the SOP. As the EH efficiency coefficient of the ERs increases, the SOP will decrease for the TCRS and MRCS, i.e., the secrecy performance will improve. This is because higher η values indicate that more energy is

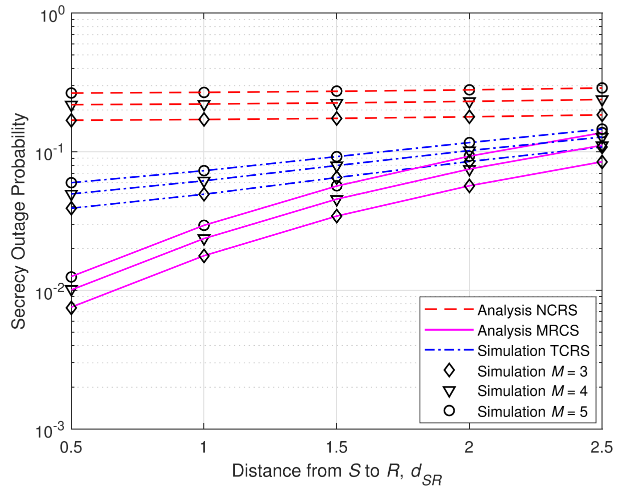

FIGURE 9. SOP versus the distance d_{SR} from S to R, with $N = 5$, $\alpha = 0.4$ (dB), $\rho = 0.6$, $\eta = 0.7$, and $R_S = 0.01$.

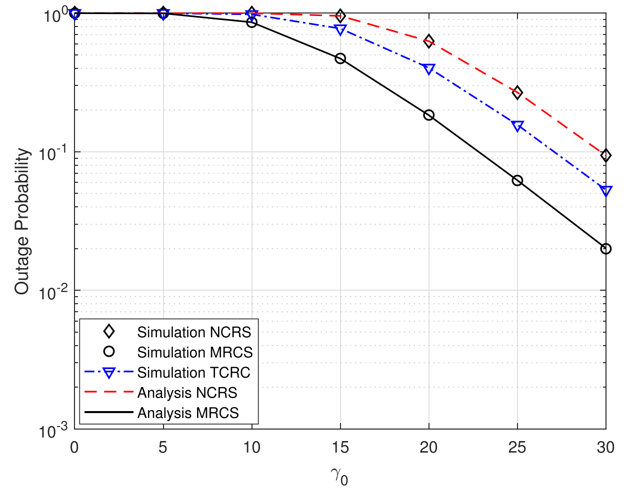

FIGURE 11. OP versus γ_0 (dB), with $N = 6$, $M = 5$, $\alpha = 0.4$, $\rho = 0.6$, $\eta = 0.7$ and $R_O = 0.5$.

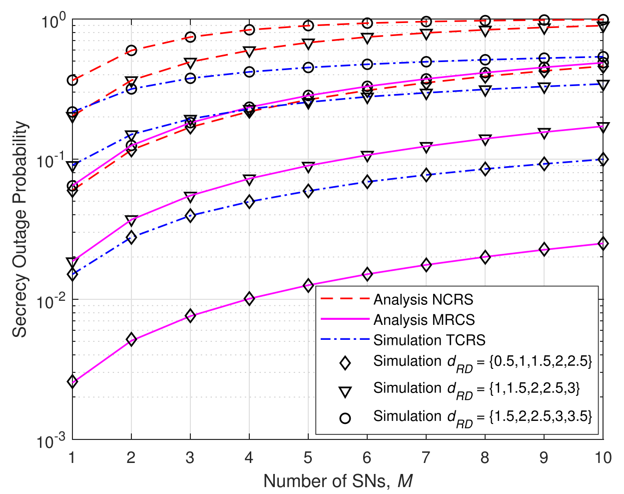

FIGURE 10. SOP versus the distance d_{RD} from R to D, with $N = 5$, $\alpha = 0.4$ (dB), $\rho = 0.6$, $\eta = 0.7$, and $R_S = 0.01$.

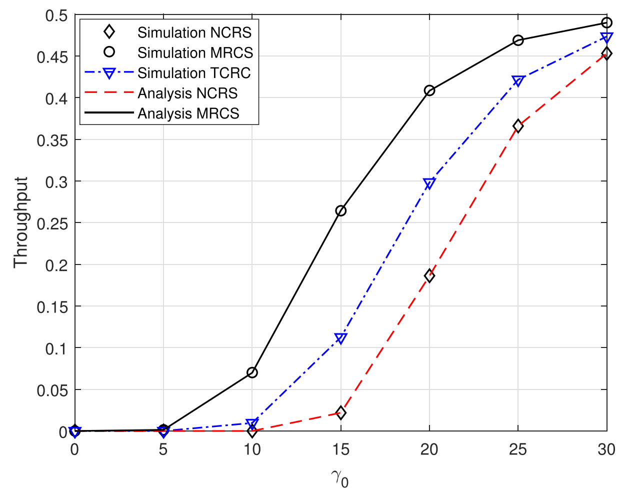

FIGURE 12. Throughput τ versus γ_0 (dB), with $N = 6$, $M = 5$, $\alpha = 0.4$, $\rho = 0.6$, $\eta = 0.7$, and $R_O = 0.5$.

being harvested at the ERs, which causes the BS-SN channel capacities to increase for the TCRS and MRCS.

In Figs. 9 and 10, we investigate the impacts on the SOP of the distance d_{SR} from the BS to an ER and of the distance d_{RD} from an ER to an SN. The SOP increases as either d_{SR} or d_{RD} increases. This is because when the ER is farther from the BS or the SN is farther from the ER, the channel conditions become poorer due to the higher path loss, causing the SN to have difficulty detecting the signal. Furthermore, as seen in Fig. 10, the SOP reaches 1 as d_{RD} increases (i.e., the system experiences an outage) under the NCRS, while it remains small under the TCRS and MRCS. Thus, it is concluded that both the TCRS and MRCS can be used in the case of long-distance transmission from the ERs to the SNs; however, the secrecy performance of the MRCS is better than that of the TCRS in this case.

Fig. 11 shows the impact of γ_0 on the OP of the m-th SN. As shown, an increase in γ_0 leads to a decrease in the OP. The reason for this result is that the higher the transmit power is, the more energy is harvested; thus, the SNs can more easily decode the signal. Furthermore, the OP under the MRCS is lower than those under the other schemes. This is because in the MRCS, information from multiple ERs is combined before being forwarded to the SN.

Fig. 12 depicts the impact of γ_0 on the throughput. Similarly, the throughput under the MRCS is better than those under the other schemes. The throughput gradually improves with increasing γ_0 and becomes stable when γ_0 is sufficiently large. This result occurs because the throughput is related to the SNR. As a consequence of the increase in the SNR, the OP will decrease, and thus, the throughput will be higher.

VI. CONCLUSION

The secrecy performance in terms of the SOP of an RF EH relay WSN in the presence of a passive EAV is studied in this paper. We investigate a communication protocol that is divided into two phases: one for information decoding and EH and one for information relaying. The MRCS is investigated to improve the secrecy performance. Accordingly,

$$\Theta_{D_m} = \int_0^{v_3/(\theta+1)} f_{Y_{R_nE}}(z) \int_0^{\infty} f_{X_{SR_n}}(x) F_{Y_{R_nD_m}}\left[\frac{\theta}{x} + (\theta+1) z\right] dxdz + \int_{v_3/(\theta+1)}^{v_3} f_{Y_{R_nE}}(z) \int_0^{\infty} f_{X_{SR_n}}(x) dxdz \tag{42}$$

$$\begin{aligned} \Theta_{D_m}^{NCRS} &= F_{Y_{R_nE}}(v_3) - F_{Y_{R_nE}}[v_3/(\theta+1)] + \int_0^{v_3/(\theta+1)} f_{Y_{R_nE}}(z) \int_0^{\theta/[v_3-(\theta+1)z]} f_{X_{SR^*}}(x) dxdz \\ &\quad + \int_0^{v_3/(\theta+1)} f_{Y_{R_nE}}(z) \int_{\theta/[v_3-(\theta+1)z]}^{\infty} f_{X_{SR^*}}(x) \left(1 - e^{-\frac{1}{\Omega_{R_nD_m}} \frac{v_2\left[\frac{\theta}{x}+(\theta+1)z\right]}{v_3-\left[\frac{\theta}{x}+(\theta+1)z\right]}}\right) dxdz \end{aligned} \tag{43}$$

$$\begin{aligned} \Theta_{D_m}^{NCRS} &= 1 - \frac{N v_2 v_3}{\Omega_{SR^*}\Omega_{R_nE} v_1} \sum_{k=0}^{N-1} \frac{(-1)^k (N-1)!}{k!(N-1-k)!} e^{v_2\left(\frac{1}{\Omega_{R_nD_m}}+\frac{1}{\Omega_{R_nE}}\right)} \\ &\quad \times \int_0^{v_3/(\theta+1)} \int_{\theta/[v_3-(\theta+1)z]}^{\infty} \frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2v_3}{v_3-z} - \frac{1}{\Omega_{SR^*}}\frac{(k+1)x}{v_1} - \frac{1}{\Omega_{R_nD_m}}\frac{v_2v_3x}{[v_3-(\theta+1)z]x-\theta}}}{(v_3-z)^2} dxdz \end{aligned} \tag{44}$$

$$\begin{aligned} \Theta_{D_m}^{NCRS} &= 1 - \frac{N v_2 v_3}{\Omega_{SR^*}\Omega_{R_nE} v_1} \sum_{k=0}^{N-1} \frac{(-1)^k (N-1)!}{k!(N-1-k)!} e^{v_2\left(\frac{1}{\Omega_{R_nD_m}}+\frac{1}{\Omega_{R_nE}}\right)} \\ &\quad \times \int_0^{v_3/(\theta+1)} \frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2v_3}{v_3-z} - \frac{1}{\Omega_{SR^*}\Omega_{R_nD_m}}\frac{\Omega_{R_nD_m}(k+1)\theta+\Omega_{SR^*}v_1v_2v_3}{v_1[v_3-(\theta+1)z]}}}{(v_3-z)^2[v_3-(\theta+1)z]} \int_0^{\infty} e^{-\frac{1}{\Omega_{SR^*}}\frac{(k+1)y}{v_1[v_3-(\theta+1)z]} - \frac{1}{\Omega_{R_nD_m}}\frac{v_2v_3\theta}{y[v_3-(\theta+1)z]}} dydz \end{aligned} \tag{45}$$

$$\begin{aligned} \Theta_{D_m}^{MRCS} &= F_{Y_{R_nE}}(v_3) - F_{Y_{R_nE}}(v_3/(\theta+1)) + \int_0^{v_3/(\theta+1)} f_{Y_{R_nE}}(z) \int_0^{\theta/[v_3-(\theta+1)z]} f_{X_{SR_n}}(x) dxdz \\ &\quad + \sum_{i=1}^{N} \prod_{\substack{j=1 \\ j\neq i}}^{N} \frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m} - \Omega_{R_jD_m}} \int_0^{v_3/(\theta+1)} f_{Y_{R_nE}}(z) \int_{\theta/[v_3-(\theta+1)z]}^{\infty} f_{X_{SR_n}}(x) \left(1 - e^{-\frac{1}{\Omega_{R_nD_m}} \frac{v_2\left[\frac{\theta}{x}+(\theta+1)z\right]}{v_3-\left[\frac{\theta}{x}+(\theta+1)z\right]}}\right) dxdz \end{aligned} \tag{46}$$

the SOP under the MRCS is compared with that under the NCRS. To guarantee the security of the system, two algorithms for determining the optimal γ_0 and selecting the optimal ERs are proposed. We also present numerical results obtained from Monte Carlo simulations. We find that the secrecy performance of the MRCS is superior to that of either the NCRS or the TCRS. The numerical results indicate that the secrecy performance of the MRCS is improved by increasing either the number of relays or the EH efficiency coefficient or by decreasing either the distance from the BS to the ERs or the distance from the ERs to the SNs. In future work, we will investigate the issue of imperfect channel state information (CSI); furthermore, we aim to explore the practical adoption of nonorthogonal multiple access (NOMA) to further enhance the system performance in a resource-constrained EH WSN [55]–[57] as well as to improve the PLS in a multihop scenario with multiple EAVs. Additionally, various metrics, e.g., the packet loss, transmission delay, and effective capacity can be further investigated [11], [58], [59].

APPENDIX A
PROOF OF THEOREM 1

By applying the characteristics of integrals and performing some mathematical manipulations in (23), the SOP for the m-th SN is rewritten as shown in (42), as shown at the top of this page. Next, by substituting (27) into (42), the integral $\Theta_{D_m}^{NCRS}$ is formulated as shown in (43), as shown at the top

$$\begin{aligned}\Theta_{D_m}^{MRCS} &= e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2[v_3/(\theta+1)]}{v_3-[v_3/(\theta+1)]}} + \frac{v_2 v_3}{\Omega_{SR_n}\Omega_{R_nE}v_1}e^{\frac{v_2}{\Omega_{R_nE}}}\int_0^{v_3/(\theta+1)}\int_0^{\theta/[v_3-(\theta+1)z]}\frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2 v_3}{v_3-z}-\frac{1}{\Omega_{SR_n}}\frac{x}{v_1}}}{(v_3-z)^2}dxdz\\ &+\sum_{i=1}^{N}\prod_{\substack{j=1\\ j\neq i}}^{N}\frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m}-\Omega_{R_jD_m}}\frac{v_2 v_3}{\Omega_{SR_n}\Omega_{R_nE}v_1}e^{\frac{v_2}{\Omega_{R_nE}}}\int_0^{v_3/(\theta+1)}\int_{\theta/[v_3-(\theta+1)z]}^{\infty}\frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2 v_3}{v_3-z}-\frac{1}{\Omega_{SR_n}}\frac{x}{v_1}}}{(v_3-z)^2}dxdz\\ &-\sum_{i=1}^{N}\prod_{\substack{j=1\\ j\neq i}}^{N}\frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m}-\Omega_{R_jD_m}}\frac{v_2 v_3}{\Omega_{SR_n}\Omega_{R_nE}v_1}e^{v_2\left(\frac{1}{\Omega_{R_nE}}+\frac{1}{\Omega_{R_nD_m}}\right)}\\ &\times\underbrace{\int_0^{v_3/(\theta+1)}\int_{\theta/[v_3-(\theta+1)z]}^{\infty}\frac{e^{-\frac{1}{\Omega_{R_nE}}\frac{v_2 v_3}{v_3-z}-\frac{1}{\Omega_{SR_n}}\frac{x}{v_1}-\frac{1}{\Omega_{R_nD_m}}\frac{v_2 v_3 x}{v_3 x-[\theta+(\theta+1)zx]}}}{(v_3-z)^2}dxdz}_{A}\end{aligned} \tag{47}$$

$$\Phi_{D_m}^{NCRS} = 1-\frac{N}{\Omega_{SR^*}}\sum_{k=0}^{N-1}\frac{(-1)^k(N-1)!}{k!(N-1-k)!}\int_{\frac{\phi\delta}{v_1}}^{\infty}e^{-\frac{(1+k)x}{\Omega_{SR^*}}-\frac{1}{\Omega_{R_nD_m}}\frac{\theta\rho R_n}{v_1 x-\phi\delta}}dx \tag{48}$$

$$\begin{aligned}\Phi_{D_m}^{MRCS} &= \int_0^{\phi\delta/v_1}\frac{1}{\Omega_{SR_n}}e^{-\frac{x}{\Omega_{SR_n}}}dx+\sum_{i=1}^{N}\prod_{\substack{j=1\\ j\neq i}}^{N}\frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m}-\Omega_{R_jD_m}}\int_{\phi\delta/v_1}^{\infty}\frac{1}{\Omega_{SR_n}}e^{-\frac{x}{\Omega_{SR_n}}}dx\\ &-\sum_{i=1}^{N}\prod_{\substack{j=1\\ j\neq i}}^{N}\frac{\Omega_{R_nD_m}}{\Omega_{R_nD_m}-\Omega_{R_jD_m}}\int_{\phi\delta/v_1}^{\infty}\frac{1}{\Omega_{SR_n}}e^{-\frac{x}{\Omega_{SR_n}}}e^{-\frac{1}{\Omega_{R_nD_m}}\frac{\phi\rho R_n}{v_1 x-\phi\delta}}dx\end{aligned} \tag{49}$$

of this page. Then, by applying formula (1.111) in [60] and substituting (14), (25), and (28) into (43), $\Theta_{D_m}^{NCRS}$ can be rewritten as the function presented in (44), as shown at the top of the previous page.

Let us set $y = (v_3 - (\theta + 1)\,z)\,x - \theta$; then, after a few steps of calculation, we arrive at the expression for $\Theta_{D_m}^{NCRS}$ shown in (45), as shown at the top of the previous page. Finally, $\Theta_{D_m}^{NCRS}$ is obtained from (31), where $K_v(x)$ is a v-order modified Bessel function of the second kind, Eq. (3.471.9) in [60]. The proof is complete.

APPENDIX B
PROOF OF THEOREM 2

Similar to what is shown in **Appendix A**, by substituting (15) and (27) into (42), the SOP for the m-th SN under the MRCS, denoted by $\Theta_{D_m}^{MRCS}$, is rewritten as shown in (46), as shown at the top of the previous page. Then, we substitute (25) and (28) into (46) to formulate the integral expression for $\Theta_{D_m}^{MRCS}$ shown in (47), as shown at the top of this page. Finally, let us set $y = (v_3 - (\theta + 1)\,z)\,x - \theta$ in A; then, after several steps of calculation, $\Theta_{D_m}^{MRCS}$ is rewritten as shown in (33). The proof is complete.

APPENDIX C
PROOF OF THEOREM 3

By substituting the PDF of g_{SR^*} given in (14) and the CDF of $g_{R_nD_m}$ given in (1) into (35), the OP for the m-th SN is rewritten as shown in (48), as shown at the top of this page. The integral is then solved using Eq. (3.471.9) in [60]. The proof is complete.

APPENDIX D
PROOF OF THEOREM 4

Similar to what is shown in **Appendix C**, by substituting the PDF of g_{SR_n} given in (2) and the CDF of g_{RD_m} given in (15) into (35), the OP for the m-th SN under the MRCS, denoted by $\Phi_{D_m}^{MRCS}$, is rewritten as shown in (49), as shown at the top of this page. Finally, the integrals from left to right are solved using Eq. (3.351.1), Eq. (3.351.2) and Eq. (3.471.9) in [60], respectively. The proof is complete.

REFERENCES

[1] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, "A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.

[2] P.-Y. Ting, J.-L. Tsai, and T.-S. Wu, "Signcryption method suitable for low-power IoT devices in a wireless sensor network," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2385–2394, Sep. 2018.
[3] 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.
[4] 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, Oct. 2018.
[5] M. Amarlingam, P. K. Mishra, K. V. V. D. Prasad, and P. Rajalakshmi, "Compressed sensing for different sensors: A real scenario for WSN and IoT," in *Proc. World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 289–294.
[6] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in *Proc. Int. Conf. Mach. Intell. Res. Advancement (ICMIRA)*, Dec. 2013, pp. 58–62.
[7] O. Dousse, M. Franceschetti, and P. Thiran, "On the throughput scaling of wireless relay networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2756–2761, Jun. 2006.
[8] G. A. Di Caro and E. Feo Flushing, "Optimal relay node placement for throughput enhancement in wireless sensor networks," in *Proc. FITCE Congr. ICT Bridging Ever Shifting Digit. Divide*, Aug. 2011, pp. 1–6.
[9] R. Liu, I. J. Wassell, and K. Soga, "Relay node placement for wireless sensor networks deployed in tunnels," in *Proc. Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Oct. 2010, pp. 144–150.
[10] A. Vallimayil, K. M. K. Raghunath, V. R. S. Dhulipala, and R. M. Chandrasekaran, "Role of relay node in wireless sensor network: A survey," in *Proc. Int. Conf. Electron. Comput. Technol.*, Kanyakumari, India, Apr. 2011, pp. 160–167.
[11] A. Zahedi, "Optimum beam forming in selective-relay cooperative communication using effective capacity approach," *AEU-Int. J. Electron. Commun.*, vol. 98, pp. 199–207, Jan. 2019.
[12] H.-C. Keh, Y.-H. Wang, K.-Y. Lin, and C.-C. Lin, "Power saving mechanism with optimal sleep control in wireless sensor networks," *Tamkang J. Sci. Eng.*, vol. 14, pp. 235–243, Sep. 2011.
[13] F. K. Shaikh and S. Zeadally, "Energy harvesting in wireless sensor networks: A comprehensive review," *Renew. Sustain. Energy Rev.*, vol. 55, pp. 1041–1054, Mar. 2016.
[14] S. Gupta, R. Zhang, and L. Hanzo, "Throughput maximization for a buffer-aided successive relaying network employing energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6758–6765, Aug. 2016.
[15] H. Jabbar, Y. S. Song, and T. T. Jeong, "RF energy harvesting system and circuits for charging of mobile devices," *IEEE Trans. Consum. Electron.*, vol. 56, no. 1, pp. 247–253, Feb. 2010.
[16] J. Taneja, J. Jeong, and D. Culler, "Design, modeling, and capacity planning for micro-solar power sensor networks," in *Proc. Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2008, pp. 407–418.
[17] D. Porcarelli, D. Spenza, D. Brunelli, A. Cammarano, C. Petrioli, and L. Benini, "Adaptive rectifier driven by power intake predictors for wind energy harvesting sensor networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 3, no. 2, pp. 471–482, Jun. 2015.
[18] F. Ingelrest, G. Barrenetxea, G. Schaefer, M. Vetterli, O. Couach, and M. Parlange, "SensorsCope: Application-specific sensor network for environmental monitoring," *ACM Trans. Sens. Netw.*, vol. 6, pp. 1–32, Jan. 2010.
[19] M. Song, S. Wang, and R. Fisher, "Transportation, iceberg costs and the adjustment of industrial structure in China," *Transp. Res. D, Transp. Environ.*, vol. 32, pp. 278–286, Oct. 2014.
[20] M. Song, J. Zhang, and S. Wang, "Review of the network environmental efficiencies of listed petroleum enterprises in China," *Renew. Sustain. Energy Rev.*, vol. 43, pp. 65–71, Mar. 2015.
[21] 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.
[22] V. V. Mai, W.-Y. Shin, and K. Ishibashi, "Wireless power transfer for distributed estimation in sensor networks," *IEEE J. Sel. Topics Signal Process.*, vol. 11, no. 3, pp. 549–562, Apr. 2017.
[23] 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.
[24] V. Singh and H. Ochiai, "An efficient time switching protocol with adaptive power splitting for wireless energy harvesting relay networks," in *Proc. Veh. Technol. Conf.*, Jun. 2017, pp. 1–5.
[25] S. Zhong, H. Huang, and R. Li, "Performance analysis of energy-harvesting-aware multi-relay networks in Nakagami-m fading," *EURASIP J. Wireless Commun. Netw.*, vol. 63, no. 1, pp. 1–9, Mar. 2018.
[26] M.-L. Ku, W. Li, Y. Chen, and K. J. R. Liu, "On energy harvesting gain and diversity analysis in cooperative communications," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2641–2657, Dec. 2015.
[27] D. Bapatla and S. Prakriya, "Performance of energy-buffer aided incremental relaying in cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3583–3598, Jul. 2019.
[28] J. Crawford and Y. Ko, "Cooperative OFDM-IM relay networks with partial relay selection under imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9362–9369, Oct. 2018.
[29] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2nd Quart., 2009.
[30] T. V. Truong, V. N. Vo, D. B. Ha, and D. D. Tran, "Secrecy performance analysis of energy harvesting wireless networks with multiple power transfer stations and destinations in the presence of multiple eavesdroppers," in *Proc. Nat. Found. Sci. Technol. Develop. Conf. Inf. Comput. Sci.*, Sep. 2016, pp. 107–112.
[31] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[32] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[33] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[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] 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.
[36] 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.
[37] W. Li, K. Liu, S. Wang, J. Lei, E. Li, and X. Li, "Full-duplex relay for enhancing physical layer security in wireless sensor networks: Optimal power allocation for minimizing secrecy outage probability," in *Proc. Int. Conf. Commun. Technol.*, Chengdu, China, Oct. 2017, pp. 906–910.
[38] X. Gong, H. Long, F. Dong, and Q. Yao, "Cooperative security communications design with imperfect channel state information in wireless sensor networks," *IET Wireless Sensor Syst.*, vol. 6, no. 2, pp. 35–41, Apr. 2016.
[39] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.
[40] Q. Y. Liau, C. Y. Leow, and Z. Ding, "Physical layer security using two-path successive relaying," *Sensors*, vol. 16, no. 6, pp. 1–13, Jun. 2016.
[41] M. Qian, C. Liu, and Y. Zou, "Cooperative beamforming for physical-layer security in power-constrained wireless sensor networks with partial relay selection," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 3, pp. 1–7, Mar. 2016.
[42] 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.
[43] D. B. Ha, D. D. Tran, T. V. Truong, and V. N. Vo, "Physical layer secrecy performance of energy harvesting networks with power transfer station selection," in *Proc. Int. Conf. Commun. Electron.*, Jul. 2016, pp. 451–456.
[44] D.-B. H. Ha, D.-D. Tran, V. Tran-Ha, and E.-K. Hong, "Performance of amplify-and-forward relaying with wireless power transfer over dissimilar channels," *Elektronika ir Elektrotechnika*, vol. 21, no. 5, pp. 90–95, Oct. 2015.
[45] 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.
[46] N.-P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5G wireless communications: A joint relay selection and wireless power transfer approach," *IEEE Access*, vol. 4, pp. 3349–3359, 2016.
[47] V. N. Vo, T. G. Nguyen, C. So-In, H. Tran, and S. Sanguanpong, "Secrecy performance in the Internet of Things: Optimal energy harvesting time under constraints of sensors and eavesdroppers," *Mobile Netw. Appl.*, pp. 1–18, Feb. 2019.

[48] D. B. Ha, T. Q. Duong, D. D. Tran, H. Zepernick, and T. T. Vu, "Physical layer secrecy performance over Rayleigh/Rician fading channels," in *Proc. Int. Conf. Adv. Technol. Commun.*, Oct. 2014, pp. 113–118.
[49] 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, Aug. 2018.
[50] D. H. Ha, D. B. Ha, J. Zdralek, and M. Voznak, "Performance analysis of hybrid energy harvesting AF relaying networks over Nakagami-*m* fading channels," in *Proc. Int. Conf. Adv. Technologies. Commun.*, Oct. 2018, pp. 157–162.
[51] P. N. Son and H. Y. Kong, "Cooperative communication with energy-harvesting relays under physical layer security," *IET Commun.*, vol. 9, no. 17, pp. 2131–2139, Oct. 2015.
[52] A. Zahedi, M. Lari, A. Albaaj, and Q. Alabkhat, "Simultaneous energy harvesting and information processing considering multi-relay multi-antenna using maximum ratio transmission and antenna selection strategies," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 11, pp. 1–13, May 2017.
[53] V. P. Tuan and H. Y. Kong, "Exploiting cooperative relays to enhance the performance of energy-harvesting systems over Nakagami-*m* fading channels," *Telecommun. Syst.*, vol. 69, no. 4, pp. 477–487, Dec. 2018.
[54] L. Sun, T. Zhang, L. Lu, and H. Niu, "Cooperative communications with relay selection in wireless sensor networks," *IEEE Trans. Consum. Electron.*, vol. 55, no. 2, pp. 513–517, May 2009.
[55] M. R. Zamani, M. Eslami, M. Khorramizadeh, and Z. Ding, "Energy-efficient power allocation for NOMA with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 1009–1013, Jan. 2019.
[56] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2nd Quart., 2017.
[57] F. Fang, H. Zhang, J. Cheng, and V. C. M. Leung, "Energy-efficient resource allocation for downlink non-orthogonal multiple access network," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3722–3732, Sep. 2016.
[58] D. Wu and R. Negi, "Effective capacity: A wireless link model for support of quality of service," *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 630–643, Jul. 2003.
[59] Q. Zhu and X. Zhang, "Effective-capacity based auctions for relay selection over wireless cooperative communications networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2016, pp. 1–6.
[60] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, A. Jeffrey and D. Zwillinger, Eds. New York, NY, USA: Academic, 2014.

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, radio-frequency energy harvesting, and wireless sensor networks.

VAN NHAN VO received the B.S. degree in computer science from Da Nang 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 the Internet of Things, information security, physical layer secrecy, radio-frequency energy harvesting, wireless sensor networks, and the security of other advanced communication systems.

CHAKCHAI SO-IN (SM'14) received the Ph.D. degree in computer engineering from Washington University in St. Louis, MO, USA, in 2010. He is currently a Professor with the Department of Computer Science, Khon Kaen University. He was an Interne with CNAP-NTU (SG), Cisco Systems, WiMAX Forums, and Bell Labs, USA. His research interests include mobile computing, wireless/sensor networks, signal processing, and computer networking and security He has authored over 100 publications and ten books, including some in IEEE JSAC, IEEE Magazines, and Computer Network/Network Security Labs. He is also a Senior Member of ACM. He has served as an Editor for *PLOS One*, *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 letters/magazines, and *Computer Networks*/*Computer Communications*.

DAC-BINH HA received the B.S. degree in radio techniques and the M.S. and Ph.D. degrees in communications and information systems from the Huazhong University of Science and Technology (HUST), China, in 1997, 2006, and 2009, respectively. He is currently the Dean of the Faculty of Electrical and Electronics Engineering, Duy Tan University, Vietnam.

SURASAK SANGUANPONG received the B.Eng. and M.Eng. degrees in electrical engineering from Kasetsart University, in 1985 and 1987, respectively. He is currently an Associate Professor with the Department of Computer Engineering and the Director of the Applied Network Research Laboratory, Kasetsart University. His research interests include network measurement, the Internet security, and high-speed networking.

ZUBAIR AHMED BAIG is currently a Senior Lecturer in cyber security with the School of Information Technology, Deakin University. He has authored over 65 journal and conference articles and book chapters. His research interests include cyber security, artificial intelligence, smart cities, and the Internet of Things. He has served on numerous technical program committees of international conferences and has delivered numerous keynote talks on cyber security. He serves as an Editor for the *IET Wireless Sensor Systems* journal and *PSU Research Review* (Emerald Publishing House).