2018

Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy

Van Nhan Vo

Tri Gia Nguyen

Chakchai So-In

Zubair Ahmed Baig
Edith Cowan University

Surasak Sanguanpong

10.1109/ACCESS.2018.2829485
Vo, V. N., Nguyen, T. G., So-In, C., Baig, Z. A., & Sanguanpong, S. (2018). Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy. *IEEE Access, 6*, 23406-23419.
https://doi.org/10.1109/ACCESS.2018.2829485

IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

SPECIAL SECTION ON SECURITY AND TRUSTED COMPUTING FOR INDUSTRIAL INTERNET OF THINGS

Received March 15, 2018, accepted April 11, 2018, date of publication April 23, 2018, date of current version May 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2829485

Secrecy Outage Performance Analysis for Energy Harvesting Sensor Networks With a Jammer Using Relay Selection Strategy

VAN NHAN VO[1], TRI GIA NGUYEN[2], (Member, IEEE), CHAKCHAI SO-IN[1], (Senior Member, IEEE), ZUBAIR AHMED BAIG[3], AND SURASAK SANGUANPONG[4]

[1]Applied Network Technology Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[2]Faculty of Information Technology, Duy Tan University, Da Nang 550000, Vietnam
[3]Security Research Institute, Edith Cowan University, Perth, WA 6027, Australia
[4]Department of Computer Engineering, Faculty of Engineering, Kasetsart University, Bangkok 10900, Thailand

Corresponding author: Surasak Sanguanpong (surasak.s@ku.ac.th)

This work was supported in part by Enthuse Company Ltd., under Grant Ent-KKU-2560-01, in part by the Khon Kaen University Grant, and in part by the Kasetsart University Grant.

ABSTRACT In this paper, we study radio frequency energy harvesting (EH) in a wireless sensor network in the presence of multiple eavesdroppers (EAVs). Specifically, the sensor source and multiple sensor relays harvest energy from multiple power transfer stations (PTSs), and then, the source uses this harvested energy to transmit information to the base station (BS) with the help of the relays. During the transmission of information, the BS typically faces a risk of losing information due to the EAVs. Thus, to enhance the secrecy of the considered system, one of the relays acts as a jammer, using harvested energy to generate interference with the EAVs. We propose a best-relay-and-best-jammer scheme for this purpose and compare this scheme with other previous schemes. The exact closed-form expression for the secrecy outage probability (SOP) is obtained and is validated through Monte Carlo simulations. A near-optimal EH time algorithm is also proposed. In addition, the effects on the SOP of key system parameters such as the EH efficiency coefficient, the EH time, the distance between the relay and BS, the number of PTSs, the number of relays, and the number of EAVs are investigated. The results indicate that the proposed scheme generally outperforms both the best-relay-and-random-jammer scheme and the random-relay-and-best-jammer scheme in terms of the secrecy capacity.

INDEX TERMS Energy harvesting, wireless sensor networks, relay networks, friendly jammer, physical layer security.

I. INTRODUCTION

Recently, wireless sensor networks (WSNs) have come to be considered key technologies for Internet of Things (IoTs) applications in which sensor nodes (SNs) are responsible for instantaneous or periodic data collection in various environments; such applications include manufacturing and precision agriculture [1]–[3]. However, the energy storage capacity of SNs is limited, and thus, SNs need to be replaced periodically to maintain SN operations [4]. This need for frequent replacement is very dangerous in hazardous environments such as nuclear reactors. Accordingly, prolonging the product life for SNs has become one of the most challenging problems for WSNs.

Fortunately, recent advances in energy harvesting (EH) techniques have enabled promising solutions that prolong the product life and increase the energy efficiency of SNs [5]–[8]. By means of EH techniques, SNs can harvest energy from ambient energy sources such as solar radiation, wind, and radio signals, which, in turn, allows the SNs to operate continuously [9]. However, the availability of these sources is difficult to predict and impossible to control [7]. An alternative solution, namely, radio frequencys (RFs) EH, has been proposed [10]. This approach is based on the fact that radio signals provide a sustainable power supply in wireless networks and can be harvested and converted into usable energy for SNs. RF EH has been shown to enhance the

system energy efficiency in WSNs [11], [12]. Because the SN lifetime is prolonged through the proposed scheme, the security of the underlying communication medium is also critical in WSNs [13]–[15]. The signals broadcast over wireless channels must be protected against tampering and/or modification by adversaries. Without an efficient and effective mechanism in place, WSNs may be easily compromised.

To mitigate this problem, a physical layer security (PLS) technique has been proposed that has attracted considerable attention from the research community [16]–[22]. This technique exploits the characteristics of wireless channels (e.g., fading, noise, and interference) and does not require complex computations to enable secure communication in wireless networks [20]. Hyadi *et al*. [21] presented a detailed overview of recent and ongoing research works on PLS with uncertain channel state information (CSI). Choi *et al*. [16] investigated PLS techniques for performing distributed detection in the presence of an eavesdropper (EAV) in the working environment. In [17], Zhu *et al*. proposed an optimal sensor scheduling scheme to enhance the PLS of industrial WSNs. Zheng *et al*. [22] proposed a hybrid full-duplex/half-duplex receiver deployment strategy to secure legitimate transmissions.

Taking advantage of a number of spatial and temporal techniques, cooperative relay communications and friendly jammers have been studied to achieve PLS improvements [23]–[26]. In particular, in [23], the secrecy performance under the influence of relays and jammers was evaluated in terms of the secrecy outage probability (SOP). In [24], Chen *et al*. considered a wireless model with two sources, one EAV, and intermediate nodes. The authors proposed algorithms for joint relay and jammer selection in two-way relay networks with the aim of improving the SOP.

In [25], Li *et al*. considered a cooperative wireless network under two specific schemes: a decode-and-forward (DF) relay scheme and cooperative jamming. The authors also proposed solutions to enhance the performance of secure transmission by maximizing the achievable secrecy rate and minimizing the total power transmit power. Zheng *et al.* [26] optimized the power allocation and transmission region under an SOP constraint and then analyzed the effect of a DF relay scheme on the secrecy performance. However, the combination of EH, PLS, and cooperative communication has not been commonly addressed in the literature.

Motivated by all of the works listed above and the references therein, in this paper, we study the secrecy performance of an RF EH-WSN and propose a best-relay-and-best-jammer scheme to enhance the secrecy performance. Our main contributions are summarized as follows:

- We propose a cooperative communication strategy for an EH-WSN in which the best relay and the best jammer are selected from among multiple relays. We compare this approach with previous schemes, such as the best relay with a random jammer and a random relay with the best jammer [27].
- Based on the proposed scheme, we derive an exact closed-form expression for the SOP. This formula enables the rapid evaluation of the secrecy performance. Moreover, we propose a near-optimal EH time algorithm for the best-relay-and-best-jammer scheme (BBS).
- Our numerical results indicate that 1) the proposed scheme outperforms both the best-relay-and-random-jammer scheme (BRS) and the random-relay-and-best-jammer scheme (RBS) and 2) the performance of the proposed scheme significantly improves as the number of relays and the number of power transfer stations (PTSs) increase and as the number of EAVs decreases.

The remainder of this paper is organized as follows: In Section II, some related work on the secrecy performance of relay-based WSNs is presented. In Section III, the system model, signal model, and three communication schemes are introduced. In Section IV, the SOPs corresponding to the three considered schemes are analyzed. In Section V, numerical results are presented and discussed. Finally, conclusions are given in Section VI.

II. RELATED WORK

Cooperative relay communication is a popular approach to improving PLS; thus, several works have investigated relay systems in WSNs [28]–[34]. For example, in 2016, Q. Xu *et al*. studied an IoT application with randomly distributed EAVs with the help of such a relay scheme. The authors investigated two scenarios: one in which each device was equipped with a single antenna and another in which the devices were equipped with multiple antennas for relaying and EAVs. Then, the SOP and the optimal power allocation in each of the two scenarios were derived [28]. X. Gong *et al*. investigated a system in which a source, multiple relays, a destination, and an EAV were deployed. Gong *et al.* [29] proposed a robust beamforming scheme to recover a fraction of the performance lost.

As an extension of the work done in [28] and [29], Q. Y. Liau *et al*. investigated a more complex model including a source, a destination, two half-duplex relays, and an EAV. Liau *et al.* [30] proposed two-path successive relaying (TPSR) to improve the security of the system. Y. Deng *et al*. considered a three-tier WSN using a DF relay scheme in which the considered system included multiple SNs, access points, sinks, and external EAVs. Based on this model, the authors proposed new expressions for the average secrecy rate to analyze the transmission security in practical WSNs [31]. However, the possibility of relay selection to further boost secrecy performance has not been considered.

With regard to friendly cooperative jammers, Araujo *et al*. [32] proposed a jamming strategy to address the problem of secure communication in WSNs. M. Yang *et al*. investigated the scenario of a WSN with one base station (BS), multiple users, one EAV, and one cooperative jammer. Each user and EAV was equipped with a single antenna, while the BS and jammer had multiple antennas. Accordingly, transmit antenna selection was performed for the BS and jamming signals to

achieve a satisfactory secrecy performance. An exact closed-form expression for the SOP was derived to evaluate the secrecy performance [33].

To improve the secrecy performance of WSNs, Zhang *et al*. [34] investigated a relay-based scheme with a friendly jammer. The authors focused on two schemes, one with cooperative jamming and one without, to evaluate the security of a two-way relay WSN in the presence of an EAV. The authors then proposed a near-optimal resource allocation algorithm for the first scheme and a heuristic algorithm based on alternating optimization for the second scheme to improve the secrecy performance. Zheng *et al*. [35] investigated a two-tier heterogeneous decentralized wireless network (DWN), in which the SNs and receivers (data collection stations) in each tier were organized in pairs. They studied the benefits of FD receiver jamming to enhance the PLS of the considered system. Notably, the works discussed above considered jamming only in WSNs without EH.

To explicitly identify and address the limitations of other works, particularly on relaying with jamming in the EH case, we investigate the PLS in an RF EH-WSN in which the SN source delivers packets to the BS via multiple relays while EAVs are jammed by a friendly jammer. To the best of our knowledge, no previous publication has addressed this problem.

III. SYSTEM AND CHANNEL MODEL

In this section, the system model, EH process, and signal model are presented.

A. SYSTEM MODEL

Let us consider a relay-based RF EH-WSN, as illustrated in Fig. 1, in which a packet is transmitted by a source S to a BS B with the help of multiple intermediate relays L_n, $n = 1, \ldots, N+1$, in the presence of multiple passive EAVs E_k, $k = 1, \ldots, K$. Under the assumption that the SNs are limited in energy, the SNs must harvest energy from multiple PTSs P_m, $m = 1, \ldots, M$, to support data transmission. Here, we consider the scenario presented in [36], in which S is far from both B and the E_k; thus, there are no direct $S \rightarrow B$ or $S \rightarrow E_k$ links. Therefore, $S \rightarrow B$ transmission can only be performed with the help of the intermediate relays. Due to size limitations, all SNs, EAVs, and the BS are each equipped with a single antenna, and all channels are modeled as Rayleigh fading channels.

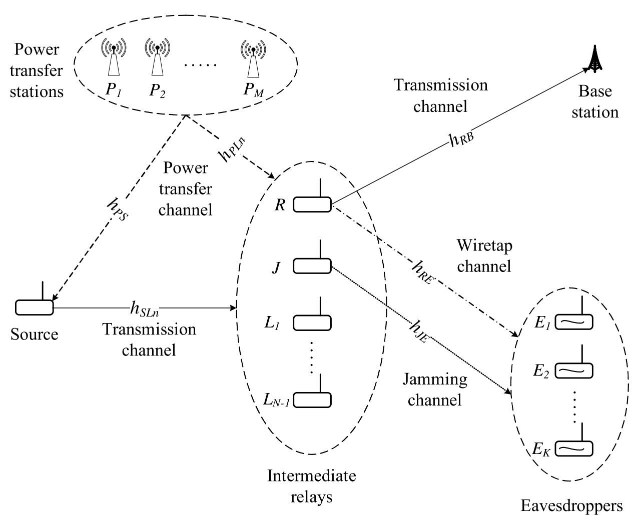

FIGURE 1. The system model of a relay-based RF EH-WSN.

Here, we follow [37]–[39] in that the CSI of the whole system is known at all nodes. This is rational even for passive EAVs because the SNs can estimate the CSI by detecting the local oscillator power that is inadvertently leaked from the front-end RF receivers of the EAVs [39].

For mathematical modeling purposes, the channel coefficients of the $P \rightarrow S$, $P \rightarrow L_n$, $S \rightarrow L_n$, $L_n \rightarrow E_k$, and $L_n \rightarrow B$ communication links are denoted by h_{PS}, h_{PL_n}, h_{SL_n}, $h_{L_nE_k}$, and h_{L_nB}, respectively. The distances of the $P \rightarrow S$, $P \rightarrow L_n$, $S \rightarrow L_n$, $L_n \rightarrow E_k$, and $L_n \rightarrow B$ communication links are denoted by d_{PS}, d_{PL_n}, d_{SL_n}, $d_{L_nE_k}$, and d_{L_nB}, respectively.

B. ENERGY HARVESTING

We deploy a time switching receiver (TSR) protocol to harvest energy and process information at S and the L_n [40]. Each SN is assumed to adopt the harvest-use (HU) mode for EH and information transmission [41]; i.e., the SNs neither save energy nor recharge their batteries, and all harvested energy is used immediately. This assumption is rational because the SNs are equipped only with small batteries for energy storage due to size limitations.

In Fig. 2, the symbol T represents the time block corresponding to one HU period, such that αT is the EH time of both the source and relay nodes, while $(1-\alpha)T$ is the time for information transmission, where $\alpha \in (0, 1)$. The time window for information transmission is divided into two phases as follows: $\frac{(1-\alpha)}{2}T$ is used for $S \rightarrow L_n$ communication, and the remaining time $\frac{(1-\alpha)}{2}T$ is simultaneously used for both $L_n \rightarrow B$ communication and $L_n \rightarrow E_k$ jamming.

In this paper, we consider the scenario presented in [42] and [43], in which only one PTS is selected as active for

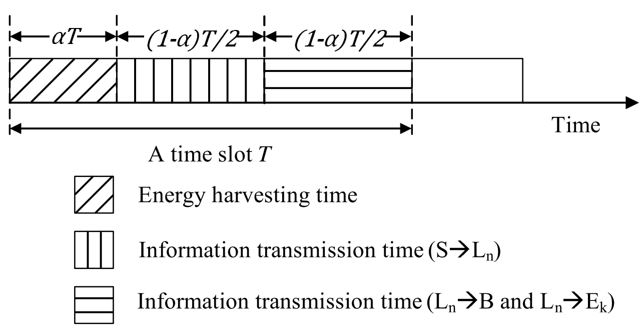

FIGURE 2. TSR protocol at a relay. The considered time block T is used for both EH and information transmission; the time αT is used to harvest energy from multiple PTSs, while the remaining time $(1-\alpha)T$ is used to transmit the packet from the source to the BS.

the purpose of calculating the computational cost and the energy demand reduction. Here, a particular PTS (with the best channel for the $P_m \rightarrow S$ link) is selected to transmit power to S, similar to the selection of a PTS for each L_n. Note that it is possible that the same PTS may be selected for both purposes depending on the channel gain. This selection can be interpreted as follows:

$$h_{PL_n} \triangleq \max_{m=1,\ldots,M} \left\{ |h_{P_m L_n}| \right\}, \tag{1}$$

and

$$h_{PS} \triangleq \max_{m=1,\ldots,M} \left\{ |h_{P_m S}| \right\}. \tag{2}$$

Accordingly, the energy harvested at L_n during the EH time αT is given by [44]

$$E_{PL_n} = \frac{\eta\alpha P_0 T \left|h_{PL_n}\right|^2}{d_{PL_n}^{\theta}} = \eta\alpha P_0 T \gamma_{PL_n}, \tag{3}$$

and the energy harvested at S is given by

$$E_{PS} = \frac{\eta\alpha P_0 T |h_{PS}|^2}{d_{PS}^{\theta}} = \eta\alpha P_0 T \gamma_{PS}, \tag{4}$$

where P_0 is the power transmitted from the PTSs; $\eta \in (0, 1)$ is the EH efficiency coefficient, which depends on the EH circuitry [44]; θ is the path loss exponent; $\gamma_{PS} = \frac{|h_{PS}|^2}{d_{PS}^{\theta}}$; and $\gamma_{PL_n} = \frac{|h_{PL_n}|^2}{d_{PL_n}^{\theta}}$.

Remark 1: We assume that each channel coefficient X_j, $j = 1, \ldots, J$, is a random variable that follows an exponential distribution. Thus, the probability density function (PDF) and the cumulative distribution function (CDF) of $X = \max_{j=1,\ldots,J} \{X_j\}$ are calculated as follows:

$$f_X(x) = \frac{J}{\lambda_X} e^{-\frac{x}{\lambda_X}} \left(1 - e^{-\frac{x}{\lambda_X}}\right)^{J-1} \tag{5}$$

and

$$F_X(x) = \left(1 - e^{-\frac{x}{\lambda_{\gamma X}}}\right)^J, \tag{6}$$

where λ_X is the mean channel gain.

With the help of **Remark 1**, we obtain the PDFs of γ_{PS} and γ_{PL_n} as follows:

$$f_{\gamma_{PS}}(x) = \frac{M}{\lambda_{PS}} e^{-\frac{x}{\lambda_{PS}}} \left(1 - e^{-\frac{x}{\lambda_{PS}}}\right)^{M-1} \tag{7}$$

and

$$f_{\gamma_{PL_n}}(x) = \frac{M}{\lambda_{PL_n}} e^{-\frac{x}{\lambda_{PL_n}}} \left(1 - e^{-\frac{x}{\lambda_{PL_n}}}\right)^{M-1}, \tag{8}$$

where $\lambda_{PL_n} = \frac{\mathbb{E}\left[|h_{PL_n}|^2\right]}{d_{PL_n}^{\theta}}$, $\lambda_{PS} = \frac{\mathbb{E}\left[|h_{PS}|^2\right]}{d_{PS}^{\theta}}$, and $\mathbb{E}[\cdot]$ is an expectation operator.

C. COMMUNICATION MODEL

Under the assumption that the channel fading coefficients remain constant during a given time slot but may change in the next time slot, the transmit power of S is obtained as [27]

$$P_{PS} = \frac{E_{PS}}{\frac{(1-\alpha)}{2}T} = \frac{2\eta\alpha P_0}{(1-\alpha)}\gamma_{PS}, \tag{9}$$

and the transmit power of L_n is obtained as

$$P_{PL_n} = \frac{E_{PL_n}}{\frac{(1-\alpha)}{2}T} = \frac{2\eta\alpha P_0}{(1-\alpha)}\gamma_{PL_n}. \tag{10}$$

Accordingly, information is communicated in two phases, as follows:

- In the first phase, S broadcasts packets to all SNs. Thus, the received signal at L_n is given by

$$y_{L_n}(t) = \sqrt{\frac{P_{PS}}{d_{SL_n}^{\theta}}} h_{SL_n} x(t) + n_{L_n}, \tag{11}$$

  where $x(t)$ is the transmitted signal and n_{L_n} is a complex additive white Gaussian noise (AWGN) component at L_n, $n_{L_n} \in \mathcal{CN}(0, N_0)$.
- In the second phase, the signal received at each SN L_n is fully decoded [45] and is then re-encoded before being forwarded to B. During this time, the jammer also injects additional jamming signals to interfere with the EAVs with the purpose of degrading their eavesdropping capability [46]. Thus, the received signals at B and at each E_k are as follows:

$$y_B(t) = \sqrt{\frac{P_{PR}}{d_{RB}^{\theta}}} h_{RB} x(t) + n_B \tag{12}$$

  and

$$y_{E_k}(t) = \sqrt{\frac{P_{PR}}{d_{RE_k}^{\theta}}} h_{RE_k} x(t) + \sqrt{\frac{P_{PJ}}{d_{JE_k}^{\theta}}} h_{JE_k} z(t) + n_{E_k}, \tag{13}$$

  where n_B and n_{E_k} are the complex AWGN components at B and the E_k, respectively, $n_B \in \mathcal{CN}(0, N_0)$ and $n_{E_k} \in \mathcal{CN}(0, N_0)$.

The instantaneous signal-to-noise ratios (SNRs) at each L_n and B and the instantaneous signal-to-interference-plus-noise ratio (SINR) at each E_k can be written as follows:

$$\gamma_{SL_n} = \frac{\left|h_{SL_n}\right|^2}{d_{SL_n}^{\theta}}, \tag{14}$$

$$\gamma_{L_nB} = \frac{\left|h_{L_nB}\right|^2}{d_{L_nB}^{\theta}}, \tag{15}$$

$$\gamma_{L_nE_k} = \frac{\left|h_{L_nE_k}\right|^2}{d_{L_nE_k}^{\theta}}. \tag{16}$$

Thus, the end-to-end SNR at B and the SINR at each E_k for each L_n are given as follows [47], [48]:

$$\gamma_B^{(n)} = \min\left\{\gamma_{SL_n}, \gamma_{L_nB}\right\} \tag{17}$$

and

$$\gamma_{E_k}^{(n)} = \min\left\{\gamma_{SL_n}, \gamma_{L_nE_k}\right\}. \tag{18}$$

Here, we consider the case presented in [27] and [36] in which the SNR at L_n is better than both the SNR at B and the SINR at E_k, i.e., $\gamma_{SL_n} > \gamma_{L_nB}$ and $\gamma_{SL_n} > \gamma_{L_nE_k}$. Note that further evaluations regarding the assumption of distance vs. channel gain are left for future investigations, as stated in the future work section. Therefore, the end-to-end SNR at B and the end-to-end SINR at E_k for L_n can be rewritten as

$$\gamma_B^{(n)} = \gamma_{L_nB} \tag{19}$$

and

$$\gamma_{E_k}^{(n)} = \gamma_{L_nE_k}. \tag{20}$$

Next, we focus on the secrecy performance of two schemes, namely, the best-relay-and-random-jammer scheme (BRS) and the random-relay-and-best-jammer (RBS) [27]; then, we propose a new strategy, the best-relay-and-best-jammer (BBS), and compare this strategy with the two previous ones in terms of the SOP metric.

1) DESCRIPTION OF THE BRS

Here, we investigate the BRS, in which jammer J is randomly selected from among $(N+1)$ intermediate relays to combat the EAVs and the best relay R^* is chosen from among the remaining N SNs serving as intermediate relays to forward packets to B, i.e.,

$$h_{R^*B} \triangleq \max_{n=1,\ldots,N}\left\{|h_{L_nB}|\right\}. \tag{21}$$

The CDFs of γ_{R^*B} and γ_{JE_k} are obtained with the help of **Remark 1** as follows:

$$F_{\gamma_{R^*B}}(x) = \left(1 - e^{-\frac{x}{\lambda_{\gamma_{R^*B}}}}\right)^N \tag{22}$$

and

$$F_{\gamma_{JE_k}}(x) = 1 - e^{-\frac{x}{\lambda_{\gamma_{JE_k}}}}, \tag{23}$$

where $\gamma_{R^*B} = \frac{|h_{R^*B}|^2}{d_{R^*B}^\theta}$, $\gamma_{JE_k} = \frac{|h_{JE_k}|^2}{d_{JE_k}^\theta}$, $\lambda_{R^*B} = \frac{\mathbb{E}\left[|h_{R^*B}|^2\right]}{d_{R^*B}^\theta}$, and $\lambda_{JE_k} = \frac{\mathbb{E}\left[|h_{JE_k}|^2\right]}{d_{JE_k}^\theta}$.

R^* forwards the encoded packet to B, while J transmits jamming signals to B and the E_k. Here, for synchronization purposes, the same set of Gaussian pseudorandom jamming signals is generated on both the BS and the jammer, allowing B to cooperate with J. Afterward, when the jammer transmits an interference signal to the BS, unlike the unknown EAVs, the BS can remove this signal by exploiting this prior information, while the EAVs will still receive interference from the jammer [49], [50].

Here, the EAVs are assumed to have perfect knowledge of the protocol for legitimate transmissions from the relay to B, including the coding, modulation scheme, and encryption algorithm; however, the encoded signal is confidential [51].

Consequently, with the help of (19) and (20), the instantaneous end-to-end SNR at B in the BRS is given by

$$\gamma_B^{(BRS)} = \frac{P_{PR^*}|h_{R^*B}|^2}{N_0 d_{R^*B}^\theta} = \varsigma\gamma_{PR^*}\gamma_{R^*B}, \tag{24}$$

and the end-to-end SINR at each E_k in the BRS can be calculated as follows:

$$\begin{aligned}\gamma_{E_k}^{(BRS)} &= \frac{P_{PR^*}\left|h_{R^*E_k}\right|^2}{d_{R^*E_k}^\theta\left(\frac{P_{PJ}}{d_{JE_k}^\theta}\left|h_{JE_k}\right|^2 + N_0\right)} \\ &= \frac{\varsigma\gamma_{PR^*}\gamma_{R^*E_k}}{\varsigma\gamma_{PJ}\gamma_{JE_k} + 1},\end{aligned} \tag{25}$$

where $\varsigma = \frac{2\eta\alpha P_0}{N_0(1-\alpha)}$, $\gamma_{PR^*} = \frac{|h_{PR^*}|^2}{d_{PR^*}^\theta}$, and $\gamma_{R^*E_k} = \frac{\left|h_{R^*E_k}\right|^2}{d_{R^*E_k}^\theta}$.

2) DESCRIPTION OF THE RBS

In this strategy, R is randomly selected from among $(N+1)$ SNs serving as intermediate relays to forward the encoded packet to B and the best J^* is then chosen from the remaining N SNs to combat the EAVs, i.e.,

$$h_{J^*E_k} \triangleq \max_{n=1,\ldots,N}\left\{|h_{L_nE_k}|\right\}. \tag{26}$$

Similar to the approach represented in (22), the CDFs of γ_{RB} and $\gamma_{J^*E_k}$ are obtained as follows:

$$F_{\gamma_{RB}}(x) = 1 - e^{-\frac{x}{\lambda_{\gamma_{RB}}}} \tag{27}$$

and

$$F_{\gamma_{J^*E_k}}(x) = \left(1 - e^{-\frac{x}{\lambda_{\gamma_{J^*E_k}}}}\right)^N, \tag{28}$$

where $\gamma_{RB} = \frac{|h_{RB}|^2}{d_{RB}^\theta}$, $\gamma_{J^*E_k} = \frac{\left|h_{J^*E_k}\right|^2}{d_{J^*E_k}^\theta}$, $\lambda_{RB} = \frac{\mathbb{E}[|h_{RB}|^2]}{d_{RB}^\theta}$, and $\lambda_{J^*E_k} = \frac{\mathbb{E}\left[\left|h_{J^*E_k}\right|^2\right]}{d_{J^*E_k}^\theta}$.

Furthermore, similar to (19) and (20), the instantaneous end-to-end SNR at B and the SINR at E_k in the RBS are given by

$$\gamma_B^{(RBS)} = \frac{P_{PR}|h_{RB}|^2}{N_0 d_{RB}^\theta} = \varsigma\gamma_{PR}\gamma_{RB} \tag{29}$$

and

$$\begin{aligned}\gamma_{E_k}^{(RBS)} &= \frac{P_{PR}\left|h_{RE_k}\right|^2}{d_{RE_k}^\theta\left[\frac{P_{PJ^*}}{d_{J^*E_k}^\theta}\left|h_{J^*E_k}\right|^2 + N_0\right]} \\ &= \frac{\varsigma\gamma_{PR}\gamma_{RE_k}}{\varsigma\gamma_{PJ^*}\gamma_{J^*E_k} + 1},\end{aligned} \tag{30}$$

where $\gamma_{PR} = \frac{|h_{PR}|^2}{d_{PR}^\theta}$ and $\gamma_{RE_k} = \frac{\left|h_{RE_k}\right|^2}{d_{RE_k}^\theta}$.

3) DESCRIPTION OF THE BBS

In this strategy, we propose to select the best SN as R^* from among $(N+1)$ SNs serving as intermediate relays to forward the encoded packet to B, i.e.,

$$h_{R^*B} \triangleq \max_{n=1,\ldots,N+1} \{|h_{L_nB}|\}, \tag{31}$$

and to choose the second-best SN from among the remaining N SNs to serve as J^* with the purpose of jamming the EAVs, i.e.,

$$h_{J^*E_k} \triangleq \max_{\tilde{n}=1,\ldots,N} \{|h_{L_{\tilde{n}}E_k}|\}. \tag{32}$$

The CDFs of γ_{R^*B} and $\gamma_{J^*E_k}$ are obtained with the help of **Remark 1** as follows:

$$F_{\gamma_{R^*B}}(x) = \left(1 - e^{-\frac{x}{\lambda\gamma_{R^*B}}}\right)^{N+1} \tag{33}$$

and

$$F_{\gamma_{J^*E_k}}(x) = \left(1 - e^{-\frac{x}{\lambda\gamma_{J^*E_k}}}\right)^{N}. \tag{34}$$

Similar to (24) and (25), the instantaneous end-to-end SNR at B and the SINR at E_k in the BBS are given by

$$\gamma_B^{(BBS)} = \frac{P_{PR^*}|h_{R^*B}|^2}{N_0 d_{R^*B}^{\theta}} = \varsigma\gamma_{PR^*}\gamma_{R^*B} \tag{35}$$

and

$$\begin{aligned}\gamma_{E_k}^{(BBS)} &= \frac{P_{PR^*}\left|h_{R^*E_k}\right|^2}{d_{R^*E_k}^{\theta}\left[\frac{P_{PJ^*}}{d_{J^*E_k}^{\theta}}\left|h_{J^*E_k}\right|^2 + N_0\right]} \\ &= \frac{\varsigma\gamma_{PR^*}\gamma_{R^*E_k}}{\varsigma\gamma_{PJ^*}\gamma_{J^*E_k}+1}.\end{aligned} \tag{36}$$

IV. SECRECY OUTAGE PROBABILITY ANALYSIS

In this section, the channel capacities and SOPs of the BRS, RBS, and BBS are analyzed.

A. CHANNEL CAPACITY

Using the Shannon capacity formula [52], the instantaneous channel capacity of the $S \to B$ link without jamming is given by

$$C_B = W\log_2(1+\gamma_B), \tag{37}$$

where W is the system bandwidth, $\gamma_B \in \{\gamma_B^{(BRS)}, \gamma_B^{(RBS)}, \gamma_B^{(BBS)}\}$, and $C_B \in \{C_B^{(BRS)}, C_B^{(RBS)}, C_B^{(BBS)}\}$.

Similarly, we can obtain the instantaneous channel capacity of each $S \to E_k$ link when affected by jamming signals as follows:

$$C_{E_k} = W\log_2(1+\gamma_{E_k}), \tag{38}$$

where $\gamma_{E_k} \in \{\gamma_{E_k}^{(BRS)}, \gamma_{E_k}^{(RBS)}, \gamma_{E_k}^{(BBS)}\}$ and $C_{E_k} \in \{C_{E_k}^{(BRS)}, C_{E_k}^{(RBS)}, C_{E_k}^{(BBS)}\}$.

As discussed in [42], [43], [53], and [54], the instantaneous secrecy capacity of a channel is a non-negative metric. Without loss of generality, the bandwidth is normalized to unity, i.e., $W=1$; hence, the instantaneous secrecy capacity of wireless transmission from S to B in the presence of passive EAVs E_k is formulated as follows:

$$\begin{aligned}C_{S_k} &= \left[C_B - C_{E_k}\right]^+ \\ &= \begin{cases}\log_2\left(\dfrac{1+\gamma_B}{1+\gamma_{E_k}}\right), & \gamma_B > \gamma_{E_k} \\ 0, & \gamma_B \le \gamma_{E_k},\end{cases}\end{aligned} \tag{39}$$

where $C_{S_k} \in \{C_{S_k}^{(BRS)}, C_{S_k}^{(RBS)}, C_{S_k}^{(BBS)}\}$.

B. SECRECY OUTAGE PROBABILITY

Based on [54], [55], and [56], the SOP is defined as the probability that the instantaneous secrecy capacity is below a predefined threshold value R_{th}.

The relay-based RF EH-WSN is considered to be suffering an outage if either the $S \to R$ link or the $R \to B$ link suffers an outage event. Consequently, the SOP of the considered system for each E_k is given by

$$\begin{aligned}SOP_k &= \Pr\left\{\frac{1-\alpha}{2}C_{S_k} < R_{th}\right\} \\ &= \Pr\left\{\frac{1-\alpha}{2}\log_2\left(\frac{\gamma_B+1}{\gamma_{E_k}+1}\right) < R_{th}\right\} \\ &= \Pr\left\{\gamma_B < 2^{\frac{2R_{th}}{1-\alpha}}\gamma_{E_k} + 2^{\frac{2R_{th}}{1-\alpha}} - 1\right\} \\ &= \Pr\left\{\gamma_B < \xi\gamma_{E_k} + \xi - 1\right\},\end{aligned} \tag{40}$$

where $SOP_k \in \{SOP_k^{(BRS)}, SOP_k^{(RBS)}, SOP_k^{(BBS)}\}$ and $\xi = 2^{\frac{2R_{th}}{1-\alpha}}$.

1) DERIVATION FOR THE BRS

By substituting (24) and (25) into (40), the SOP of the relay-based RF EH-WSN for the k-th EAV under the BRS can be expressed as

$$\begin{aligned}SOP_k^{(BRS)} &= \Pr\left\{\gamma_B^{(BRS)} < \xi\gamma_{E_k}^{(BRS)} + \xi - 1\right\} \\ &= \Pr\left\{\gamma_{R^*B} \le \frac{\xi\gamma_{R^*E_k}}{\varsigma\gamma_{PJ}\gamma_{JE_k}+1} + \frac{\xi-1}{\varsigma\gamma_{PR^*}}\right\}.\end{aligned} \tag{41}$$

By using [55, Formula (23)], the expression given in (41) can be rewritten as

$$SOP_k^{(BRS)} = \int_0^\infty \underbrace{\Pr\left\{\gamma_{R^*B} \le \frac{\xi\gamma_{R^*E_k}}{\varsigma\gamma_{PJ}\gamma_{JE_k}+1} + \frac{\xi-1}{\varsigma x}\right\}}_{\Psi_1} \times f_{\gamma_{PR^*}}(x)\,dx. \tag{42}$$

The probability in (42) can be further rewritten by setting $U = \varsigma\gamma_{PJ}\gamma_{JE_k}+1$, as follows:

$$\Psi_1 = \int_1^\infty \underbrace{\int_0^\infty F_{\gamma_{R^*B}}\left(\frac{\xi t}{u} + \frac{\xi-1}{\varsigma x}\right) f_{\gamma_{R^*E_k}}(t)\,dt}_{\Psi_2} f_U(u)\,du, \tag{43}$$

where $f_U(u)$ is the PDF of U. Substituting (22) into the function Ψ_2 expressed in (43) and using [57, Formula (3.310.11)] yields

$$\Psi_2 = \int_0^\infty \left[1 - e^{-\frac{1}{\lambda_{R^*B}}\left(\frac{\xi t}{u} + \frac{\xi-1}{\varsigma x}\right)}\right]^N \frac{1}{\lambda_{R^*E_k}} e^{-\frac{t}{\lambda_{R^*E_k}}} dt$$
$$= 1 - \sum_{\tilde{n}} \frac{e^{-\frac{\tilde{n}(\xi-1)}{\varsigma\lambda_{R^*B}x}} u}{u + \tilde{n}\xi\frac{\lambda_{R^*E_k}}{\lambda_{R^*B}}}, \quad (44)$$

where $\sum_{\tilde{n}} = \sum_{\tilde{n}=1}^{N} \frac{(-1)^{\tilde{n}-1}N!}{\tilde{n}!(N-\tilde{n})!}$.

By substituting the function Ψ_2 and the PDF of U (see (65) in appendix A) into (33) and using formula (73) in appendix C, the function Ψ_1 can be calculated as follows:

$$\Psi_1 = \int_1^\infty \left[1 - \sum_{\tilde{n}} \frac{e^{-\frac{\tilde{n}(\xi-1)}{\varsigma\lambda_{R^*B}x}} u}{u + \tilde{n}\xi\frac{\lambda_{R^*E_k}}{\lambda_{R^*B}}}\right] \sum_{\tilde{m}} \frac{2(\tilde{m}+1)}{\varsigma\lambda_{PJ}\lambda_{JE_k}}$$
$$\times K_0\left(2\sqrt{\frac{(\tilde{m}+1)(u-1)}{\varsigma\lambda_{PJ}\lambda_{JE_k}}}\right) du$$
$$= \sum_{\tilde{m}} \left\{1 - \sum_{\tilde{n}} e^{-\frac{\tilde{n}(\xi-1)}{\varsigma\lambda_{R^*B}x}} \left[1 - \omega_1\lambda_1 S_{-1,0}(\phi_1)\right]\right\}, \quad (45)$$

where

$$\sum_{\tilde{m}} = \sum_{\tilde{m}=0}^{M-1} \frac{(-1)^{\tilde{m}}M!}{(\tilde{m}+1)!(M-\tilde{m}-1)!},$$
$$\omega_1 = 4\tilde{n}(\tilde{m}+1)\xi,$$
$$\phi_1 = 2\sqrt{\frac{(\tilde{m}+1)\left(1 + \tilde{n}\xi\frac{\lambda_{R^*E_k}}{\lambda_{R^*B}}\right)}{\varsigma\lambda_{PJ}\lambda_{JE_k}}},$$
$$\lambda_1 = \frac{\lambda_{R^*E_k}}{\varsigma\lambda_{PJ}\lambda_{JE_k}\lambda_{R^*B}},$$

and $S_{-1,0}(\cdot)$ is the Lommel function [58].

By substituting (8) into (42) and solving this integral with the help of [57, Formula (3.324.1)], we obtain the following expression for $SOP_k^{(BRS)}$:

$$SOP_k^{(BRS)}$$
$$= \int_0^\infty \sum_{\tilde{m}} \left\{\begin{array}{l} 1 - \sum_{\tilde{n}} e^{-\frac{\tilde{n}(\xi-1)}{\varsigma\lambda_{R^*B}x}} \\ \times\left[1 - \omega_1\lambda_1 S_{-1,0}(\phi_1)\right]\end{array}\right\}$$
$$\times \frac{M}{\lambda_{PR^*}} e^{-\frac{x}{\lambda_{PR^*}}} \left(1 - e^{-\frac{x}{\lambda_{PR^*}}}\right)^{M-1} dx$$
$$= \sum_{\tilde{m}}\sum_{m} \left\{1 - \sum_{\tilde{n}} \varphi_1 K_1(\varphi_1)\left[1 - \omega_1\lambda_1 S_{-1,0}(\phi_1)\right]\right\}, \quad (46)$$

where

$$\sum_{m} = \sum_{m=0}^{M-1} \frac{(-1)^m M!}{(m+1)!(M-m-1)!},$$
$$\varphi_1 = 2\sqrt{\frac{\tilde{n}(\xi-1)(1+m)}{\varsigma\lambda_{PR^*}\lambda_{R^*B}}},$$

and the $K_n(\cdot)$ are the Bessel functions ($n = 0, 1, \ldots$).

In a relay-based RF EH-WSN with multiple EAVs, R can transmit confidential signals to B only if the instantaneous SNR at B is larger than all SINRs at the EAVs, i.e.,

$$\gamma_E \triangleq \max_{k=1,\ldots,K}\{\gamma_{E_k}\}. \quad (47)$$

Accordingly, the SOP under the BRS is calculated as follows:

$$SOP^{(BRS)} = \Pr\left\{\min_{1\le k\le K}\left\{C_{S_k}^{(BRS)}\right\} < R_{th}\right\}$$
$$= 1 - \Pr\left\{\min_{1\le k\le K}\left\{C_{S_k}^{(BRS)}\right\} \ge R_{th}\right\}$$
$$= 1 - \prod_{k=1}^{K}\left[1 - \Pr\left\{C_{S_k}^{(BRS)} < R_{th}\right\}\right]. \quad (48)$$

Finally, by substituting (46) into (48), we obtain the following expression for the SOP of the system under the BRS:

$$SOP^{(BRS)}$$
$$= 1 - \prod_{k=1}^{K}\left[1 - SOP_k^{(BRS)}\right]$$
$$= 1 - \prod_{k=1}^{K}\left\{1 - \sum_{\tilde{m}}\sum_{m}\left[\begin{array}{l} 1 - \sum_{\tilde{n}} \varphi_1 K_1(\varphi_1) \\ \times\left[1 - \omega_1\lambda_1 S_{-1,0}(\phi_1)\right]\end{array}\right]\right\}. \quad (49)$$

2) DERIVATION FOR THE RBS

By substituting (29) and (30) into (40), the SOP of the relay-based RF EH-WSN for EAV E_k under the RBS can be expressed as

$$SOP_k^{(RBS)} = \Pr\left\{\gamma_B^{(RBS)} < \xi\gamma_{E_k}^{(RBS)} + \xi - 1\right\}$$
$$= \int_0^\infty \underbrace{\Pr\left\{\gamma_{RB} \le \frac{\xi\gamma_{RE_k}}{\varsigma\gamma_{PJ^*}\gamma_{J^*E_k}+1} + \frac{\xi-1}{\varsigma x}\right\}}_{\Gamma_1}$$
$$\times f_{\gamma_{PR}}(x)\,dx. \quad (50)$$

The probability in (50) can be rewritten by setting $V = \varsigma\gamma_{PJ^*}\gamma_{J^*E_k} + 1$, as follows:

$$\Gamma_1 = \int_1^\infty \underbrace{\int_0^\infty F_{\gamma_{RB}}\left(\frac{\xi t}{v} + \frac{\xi-1}{\varsigma x}\right) f_{\gamma_{RE_k}}(t)\,dt f_V(v)\,dv}_{\Gamma_2}, \quad (51)$$

where $f_V(v)$ is the PDF of V. By substituting (27) into the function Γ_2 expressed in (51) and using formula (3.310.11) in [57], we obtain

$$\Gamma_2 = \int_0^\infty \left[1 - e^{-\frac{1}{\lambda_{RB}}\left(\frac{\xi t}{v}+\frac{\xi-1}{\varsigma x}\right)}\right]\frac{1}{\lambda_{RE_k}}e^{-\frac{t}{\lambda_{RE_k}}}dt = 1 - \frac{e^{-\frac{\xi-1}{\varsigma\lambda_{RB}x}}v}{v+\frac{\xi\lambda_{RE_k}}{\lambda_{RB}}}. \quad (52)$$

Now, by substituting Γ_2 and the PDF of V (see (69) in appendix B) into (51) and using (73) in appendix C, the integral function Γ_1 can be expressed as

$$\begin{aligned}\Gamma_1 &= \int_1^\infty \left[1 - \frac{e^{-\frac{\xi-1}{\varsigma\lambda_{RB}x}}v}{v+\frac{\xi\lambda_{RE_k}}{\lambda_{RB}}}\right]\sum_{\tilde m}\sum_{\tilde n}\frac{2\tilde n(\tilde m+1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}} \\ &\quad\times K_0\left(2\sqrt{\frac{(v-1)\tilde n(\tilde m+1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E}}}\right)du \\ &= \sum_{\tilde m}\sum_{\tilde n}\left\{1 - e^{-\frac{\xi-1}{\varsigma\lambda_{RB}x}}\left[1-\omega_1\lambda_2 S_{-1,0}(\phi_2)\right]\right\}, \quad (53)\end{aligned}$$

where

$$\phi_2 = 2\sqrt{\frac{\tilde n(\tilde m+1)\left(1+\frac{\xi\lambda_{RE_k}}{\lambda_{RB}}\right)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E}}}$$

and $\lambda_2 = \dfrac{\lambda_{RE_k}}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}\lambda_{RB}}$.

By substituting (8) and (53) into (50) and solving this integral using [57, Formula (3.324.1)], we can calculate $SOP_k^{(RBS)}$ as follows:

$$\begin{aligned}SOP_k^{(RBS)} &= \int_0^\infty \sum_{\tilde m}\sum_{\tilde n}\left\{\begin{array}{l}1 - e^{-\frac{\xi-1}{\varsigma\lambda_{RB}x}} \\ \times\left[1-\omega_1\lambda_2 S_{-1,0}(\phi_2)\right]\end{array}\right\} \\ &\quad\times\frac{M}{\lambda_{PR}}e^{-\frac{x}{\lambda_{PR}}}\left(1-e^{-\frac{x}{\lambda_{PR}}}\right)^{M-1}dx \\ &= \sum_{\tilde m}\sum_{\tilde n}\sum_{m}\left\{1-\varphi_2 K_1(\varphi_2)\left[1-\omega_1\lambda_2 S_{-1,0}(\phi_2)\right]\right\}, \quad (54)\end{aligned}$$

where $\varphi_2 = 2\sqrt{\frac{(\xi-1)(m+1)}{\varsigma\lambda_{PR}\lambda_{RB}}}$.

In the considered RF EH-WSN with multiple EAVs, $SOP_k^{(RBS)}$ can be formulated as

$$\begin{aligned}SOP^{(RBS)} &= \Pr\left\{\min_{1\le k\le K}\left\{C_{S_k}^{(RBS)}\right\} < R_{th}\right\} \\ &= 1-\prod_{k=1}^{K}\left\{1-\sum_{\tilde m}\sum_{\tilde n}\sum_{m}\left[\begin{array}{l}1-\varphi_2 K_1(\varphi_2) \\ \times\left[1-\omega_1\lambda_2 S_{-1,0}(\phi_2)\right]\end{array}\right]\right\}. \quad (55)\end{aligned}$$

3) DERIVATION FOR THE BBS

By substituting (35) and (36) into (40), the SOP of the relay-based RF EH-WSN for EAV E_k under the BBS can be expressed as

$$\begin{aligned}SOP_k^{(BBS)} &= \Pr\left\{\gamma_B^{(BBS)} < \xi\gamma_{E_k}^{(BBS)} + \xi - 1\right\} \\ &= \int_0^\infty \underbrace{\Pr\left\{\gamma_{R^*B} \le \frac{\xi\gamma_{R^*E_k}}{\varsigma\gamma_{PJ^*}\gamma_{J^*E_k}+1} + \frac{\xi-1}{\varsigma x}\right\}}_{\Phi_1} \\ &\quad\times f_{\gamma_{PR^*}}(x)\,dx. \quad (56)\end{aligned}$$

The probability in (56) can be calculated as follows:

$$\Phi_1 = \int_1^\infty \underbrace{\int_0^\infty F_{\gamma_{R^*B}}\left(\frac{\xi t}{v}+\frac{\xi-1}{\varsigma x}\right)f_{\gamma_{R^*E_k}}(t)\,dt}_{\Phi_2} f_V(v)\,dv. \quad (57)$$

By substituting (33) into the function Φ_2 expressed in (57) and using [57, Formula (3.310.11)], we obtain the following:

$$\begin{aligned}\Phi_2 &= \int_0^\infty \left[1-e^{-\frac{1}{\lambda_{R^*B}}\left(\frac{\xi t}{v}+\frac{\xi-1}{\varsigma x}\right)}\right]^{N+1}\frac{1}{\lambda_{R^*E_k}}e^{-\frac{t}{\lambda_{R^*E_k}}}dt \\ &= 1-\sum_{n}\frac{e^{-\frac{n(\xi-1)}{\varsigma\lambda_{R^*B}x}}v}{v+n\xi\frac{\lambda_{R^*E_k}}{\lambda_{R^*B}}}, \quad (58)\end{aligned}$$

where $\sum_n = \sum_{n=1}^{N+1}\frac{(-1)^{n-1}(N+1)!}{n!(N+1-n)!}$.

Then, by substituting the function Φ_2 and the PDF of V (see (69) in appendix B) into (56) and using (73) in appendix C, we can obtain the function Φ_1 as follows:

$$\begin{aligned}\Phi_1 &= \int_1^\infty\left[1-\sum_n\frac{e^{-\frac{n(\xi-1)}{\varsigma\lambda_{R^*B}x}}v}{v+n\xi\frac{\lambda_{R^*E_k}}{\lambda_{R^*B}}}\right]\sum_{\tilde m}\sum_{\tilde n}\frac{2\tilde n(\tilde m+1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}} \\ &\quad\times K_0\left(2\sqrt{\frac{(v-1)\tilde n(\tilde m+1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}}}\right)dv \\ &= \sum_{\tilde m}\sum_{\tilde n}\left\{1-\sum_n e^{-\frac{n(\xi-1)}{\varsigma\lambda_{R^*B}x}}\left[1-\omega_3\lambda_3 S_{-1,0}(\phi_3)\right]\right\}, \quad (59)\end{aligned}$$

where

$$\phi_3 = 2\sqrt{\frac{\tilde n(\tilde m+1)\left(1+n\xi\frac{\lambda_{R^*E_k}}{\lambda_{R^*B}}\right)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}}},$$

$$\lambda_3 = \frac{\lambda_{R^*E_k}}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}\lambda_{R^*B}},$$

and $\omega_3 = 4n\tilde n(\tilde m+1)\xi$.

By substituting (8) and (56) into (50) and solving this integral using [57, Formula (3.324.1)], we can calculate $SOP_k^{(BBS)}$ as follows:

$$\begin{aligned}
&SOP_k^{(BBS)} \\
&= \int_0^\infty \sum_{\tilde{m}} \sum_{\tilde{n}} \left\{ \begin{array}{l} 1 - \sum_n e^{-\frac{n(\xi-1)}{\varsigma \lambda_{R^*B} x}} \\ \times \left[1 - \omega_3 \lambda_3 S_{-1,0}(\phi_3)\right] \end{array} \right\} \\
&\quad \times \frac{M}{\lambda_{PR^*}} e^{-\frac{x}{\lambda_{PR^*}}} \left(1 - e^{-\frac{x}{\lambda_{PR^*}}}\right)^{M-1} \\
&= \sum_{\tilde{m}} \sum_{\tilde{n}} \sum_m \left\{ 1 - \sum_n \varphi_3 K_1(\varphi_3) \left[1 - \omega_3 \lambda_3 S_{-1,0}(\phi_3)\right] \right\},
\end{aligned} \tag{60}$$

where $\varphi_3 = 2\sqrt{\frac{n(m+1)(\xi-1)}{\varsigma \lambda_{PR^*} \lambda_{R^*B}}}$.

For the considered RF EH-WSN with multiple EAVs, $SOP^{(BBS)}$ can be expressed as follows:

$$\begin{aligned}
&SOP^{(BBS)} \\
&= \Pr\left\{ \min_{1 \le k \le K} \left\{ C_{S_k}^{(BBS)} \right\} < R_{th} \right\} \\
&= 1 - \prod_{k=1}^{K} \left\{ 1 - \sum_{\tilde{m}} \sum_{\tilde{n}} \sum_m \left[\begin{array}{l} 1 - \sum_n \varphi_3 K_1(\varphi_3) \\ \times \left[1 - \omega_3 \lambda_3 S_{-1,0}(\phi_3)\right] \end{array} \right] \right\}.
\end{aligned} \tag{61}$$

Accordingly, the proposed algorithm finds a near-optimal EH time by splitting the possible values of the EH time proportion (α) into an array (from 0.0 to 1.0) and substituting each value in the array until the lowest SOP (SOP^*) is found, thus yielding the optimal α (α^*). The near-optimal algorithm for selecting the EH time for the BBS is summarized in **Algorithm 1**.

Algorithm 1 Near-Optimal Energy Harvesting Time

procedure NOEHT
  Initialize $SOP^* = 1$, $i = 1$, and $\alpha(i) \in (0, 1)$;
  while $\alpha(i) < 1$ **do**
    $\xi = 2^{\frac{2R_{th}}{1-\alpha(i)}}$;
    $\varsigma = \frac{2\eta\alpha(i)P_0}{1-\alpha(i)}$;
    $\lambda_3 = \frac{\lambda_{R^*E_k}}{\varsigma \lambda_{PJ} \lambda_{J^*E_k} \lambda_{R^*B}}$;
    $\omega_3 = 4n\tilde{n}(\tilde{m}+1)\xi\lambda_3$;
    $\varphi_3 = 2\sqrt{\frac{n(m+1)(\xi-1)}{\varsigma \lambda_{PR^*} \lambda_{R^*B}}}$;
    $\sum_m = \sum_{m=0}^{M-1} \frac{(-1)^m M!}{(m+1)!(M-m-1)!}$;
    $\sum_{\tilde{m}} = \sum_{\tilde{m}=0}^{M-1} \frac{(-1)^{\tilde{m}} M!}{(\tilde{m}+1)!(M-\tilde{m}-1)!}$;
    $\sum_n = \sum_{n=1}^{N+1} \frac{(-1)^{n-1}(N+1)!}{n!(N+1-n)!}$;
    $\sum_{\tilde{n}} = \sum_{\tilde{n}=1}^{N} \frac{(-1)^{\tilde{n}-1} N!}{n!(N-\tilde{n})!}$;
    Calculate $SOP^{(BBS)}(i)$ according to (61);
    if $SOP^* < SOP^{(BBS)}(i)$ **then**
      $SOP^* = SOP^{(BBS)}(i-1)$;
      $\alpha^* = \alpha(i-1)$;
      break;
    else
      $SOP^* = SOP^{(BBS)}(i)$;
      $i = i + 1$;
    end if
  end while
  return α^* and SOP^*;
end procedure

V. NUMERICAL RESULTS

In this section, we present the numerical results of a Monte Carlo simulation to verify the closed-form expression for the secrecy performance of the proposed communication technique. Specifically, we evaluate the secrecy performance of the considered system by considering the effects on the SOP of the distance from R to B, d_{RB}; the EH time, α; the EH efficiency coefficient, η; the SNR, P_0/N_0; the number of PTSs, M; the number of EAVs, K; and the number of relays, N. Unless otherwise stated, the system parameters for both the analysis and the simulation are as follows [27]: $d_{PS} = d_{PL_n} = 2.5$, $d_{RB} \in (0.4, 1.2)$, $d_{RE_k} \in \{2, 3, 4\}$, $d_{JE_k} \in \{4, 3, 2\}$, $R_{th} = 1$ kbps, $\theta = 3$, $\alpha \in (0.0, 1.0)$, $\eta \in (0.0, 1.0)$, $SNR \in (-5.0, 15.0)$, $K \in \{1, 2, 3\}$, $M \in \{2, 4, 6\}$, and $N \in [1, 10]$. We evaluate the following three schemes:

- Best-relay-and-random-jammer scheme (BRS): J is randomly chosen from among $(N + 1)$ SNs, and R^* is the best SN chosen from among the remaining N SNs.
- Random-relay-and-best-jammer scheme (RBS): R is randomly chosen from among $(N + 1)$ SNs, and J^* is the best SN chosen from among the remaining N SNs.
- Best-relay-and-best-jammer scheme (BBS): R^* is the best SN chosen from among $(N + 1)$ SNs, and J^* is the second-best SN chosen from among the remaining N SNs.

In the first simulation, we study how the SOP changes with the SNR, and three conditions with various numbers of EAVs ($K = 1$, 2, and 3) are considered for the three schemes. Fig. 3 shows the simulation results. The RBS is worse than the BRS from the perspective of the secrecy performance because the effect of the relay on the SOP is higher than that of the jammer (this is proven by (25) and (30)).

We also observe that the proposed solution (BBS) outperforms both the BRS and the RBS because the best J^* is selected from among the N SNs serving as intermediate relays such that the SNRs at the EAVs under the BBS are higher than those under the other two schemes, consistent with (25), (30), and (36). This figure also demonstrates that as the number of EAVs decreases, the SOP of the proposed scheme also decreases; i.e., the secrecy performance is enhanced with decreasing K.

In the second simulation, we investigate how the SOP changes with the distance between R and B, d_{RB}, and we

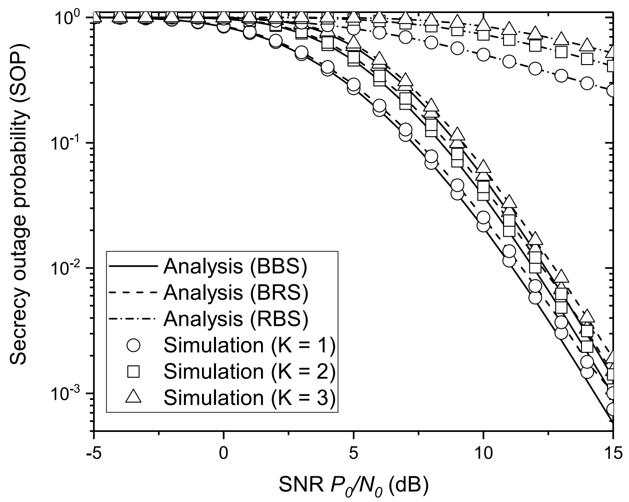

FIGURE 3. Effects on the SOP of various SNRs and various numbers of EAVs (K) with $\alpha = 0.41$, $\eta = 0.85$, $N = 10$, $SNR = 10$ dB, and $M = 4$.

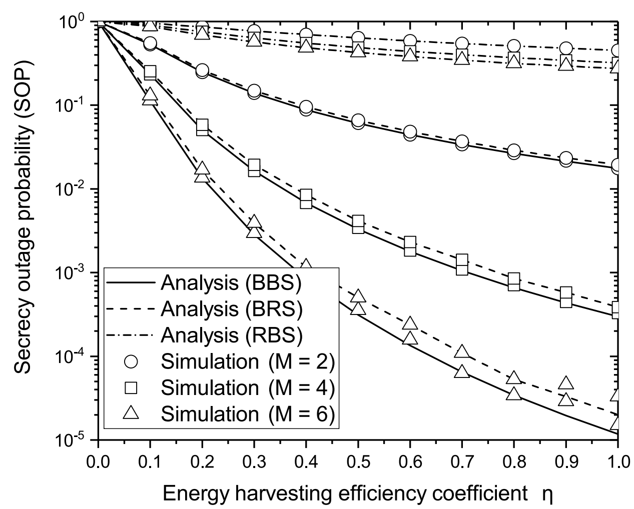

FIGURE 5. Effects on the SOP of various EH efficiency coefficients (η) and various numbers of PTSs (M) with $\alpha = 0.41$, $SNR = 10$ dB, $K = 2$, and $N = 10$.

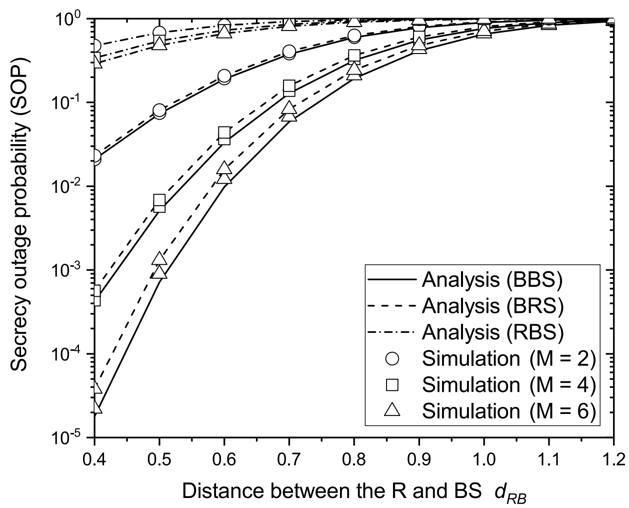

FIGURE 4. Effects on the SOP of various distances between R and B (d_{RB}) and various numbers of PTSs (M) with $\alpha = 0.41$, $\eta = 0.85$, $SNR = 10$ dB, $N = 10$, and $K = 2$.

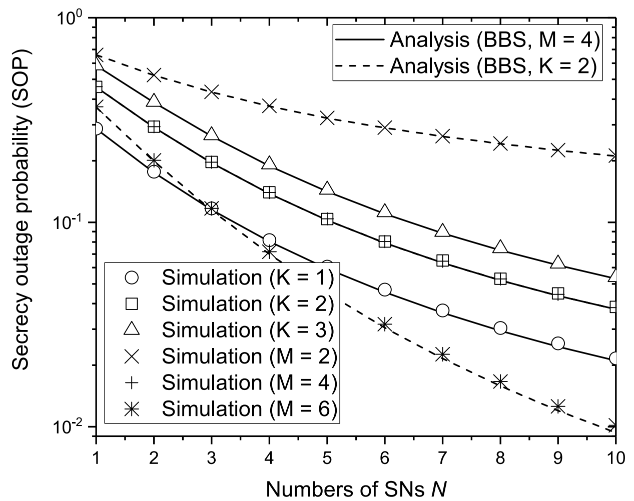

FIGURE 6. Effects on the SOP of various numbers of SNs (N), various numbers of EAVs (K), and various numbers of PTSs (M) with $\alpha = 0.41$, $\eta = 0.85$, and $SNR = 10$ dB.

evaluate three conditions with different numbers of PTSs ($M = 2, 4,$ and 6). The simulation results are plotted in Fig. 4. We can see that for each value of M, the SOP increases and approaches 1 as d_{RB} increases. In other words, the secrecy performance is improved with lower values of d_{RB}. This result may be attributed to the fact that as d_{RB} increases, the number of packets received by B rapidly decreases, consistent with (24), (29), and (35). Furthermore, with an increasing number of PTSs, a marked difference in the SOP arises between the BBS and the RBS and also between the BBS and the BRS.

In the third simulation, we study the effects on the SOP of various EH efficiency coefficients, η, and numbers of PTSs, M. The simulation results are shown in Fig. 5. For each value of M, the SOP decreases with higher values of η. This occurs because a higher EH efficiency coefficient means that more energy can be obtained (based on (10)).

We also investigate the effects on the SOP of various numbers of SNs, PTSs, and EAVs (N, M, and K, respectively). The simulation results are shown in Fig. 6. The SOP is improved as M and N increase, either separately or simultaneously, and as K decreases.

In the fifth simulation, we study the change in the SOP with the EH time α, as shown in Figs. 7 and 8. In Fig. 7, the SOP initially decreases at small values of α, peaks at a certain point, and then increases to a value near 1. This behavior occurs because when α is small, the relay harvests little power, causing the transmission power available at the relay to be insufficient and resulting in a higher

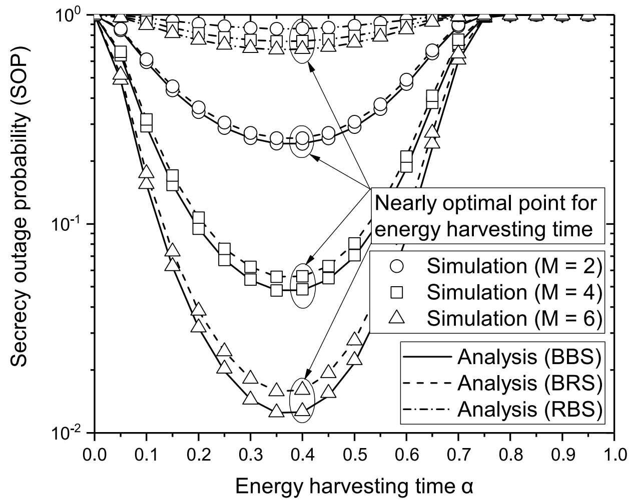

FIGURE 7. Effects on the SOP of various EH times (α) and various numbers of PTSs (M) with $\eta = 0.85$, $N = 10$, $SNR = 8$ dB, $N = 10$, and $K = 2$.

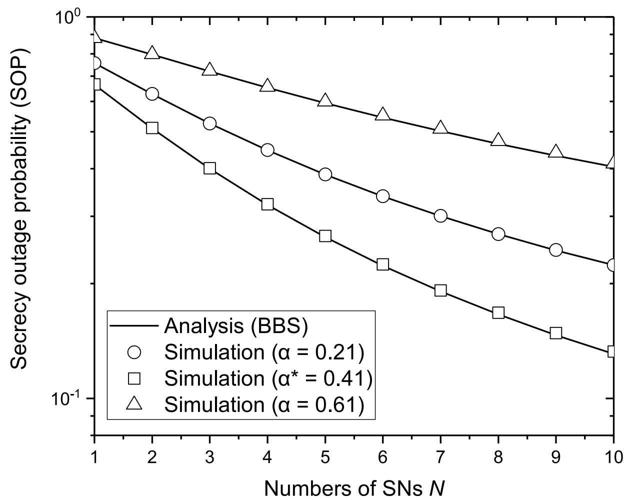

FIGURE 8. Effects on the SOP of various numbers of SNs (N) and various EH times (α) with $\eta = 0.85$, $M = 4$, $SNR = 8$ dB, and $K = 2$.

SOP. However, when α is too large, the secrecy capacity will be insufficient (according to (40)), and much of the power harvested for information transmission will be wasted. Consequently, the secrecy performance is highest for an intermediate value of α.

In addition, this figure shows that the SOP approaches 1 when $\alpha \to 0^+$ or $\alpha \to 1^-$. This result means that the secrecy performance of the system is not benefited by an excessively small or large α. This behavior occurs because $\xi \to 2^{2R_{th}}$ and $\varsigma \to 0$ when $\alpha \to 0$. From (24), (25), (29), (30), (35), and (36), the instantaneous SNRs at B and E_k are approximately 0; thus, the SOP of the considered system approaches 1 (based on (49), (55), and (61)).

In the final simulation, as shown in Fig. 8, we investigate the effects of various numbers of SNs and EH times α on the SOP. We can see that the SOP is lower with $\alpha^* = 0.41$ than it is with either $\alpha = 0.21$ or $\alpha = 0.61$; i.e., the considered RF EH-WSN is most secure when $\alpha^* = 0.41$ (the near-optimal EH time found by the proposed algorithm).

VI. CONCLUSION

In this paper, we proposed a best-relay-and-best-jammer scheme (BBS) as well as a near-optimal EH time algorithm to enhance the secrecy performance of a relay-based RF EH-WSN. We also derived an exact closed-form expression for the SOP of the considered system. Our numerical results show that in our proposed scheme, communication security can be improved by increasing the number of SNs and PTSs or by decreasing the number of EAVs, and that the BBS generally outperforms the best-relay-and-random-jammer (BRS) and the random-relay-and-best-jammer (RBS). The analytical results were verified by Monte Carlo simulations. Note, however, that because of the model simplifications adopted for the derivations and for the purpose of computational and energy cost reduction, there are some limitations that will require further investigation, i.e., the relationship between the distance and the channel gain and the case of only one active PTS. In addition, we are currently investigating a system with multiple relay clusters and a mobile charger to demonstrate a practical implementation of an RF EH-WSN.

APPENDIX

A. PROOF OF THE PDF OF $U = 1 + \varsigma\gamma_{PJ}\gamma_{JE_k}$

In accordance with the definition of conditional probability, the CDF of U can be written as

$$F_U(u) = \Pr\left\{1 + \varsigma\gamma_{PJ}\gamma_{JE_k} < u\right\} = \int_0^\infty F_{\gamma_{JE_k}}\left(\frac{u-1}{\varsigma x}\right) f_{\gamma_{PJ}}(x)\, dx, \tag{62}$$

where $u \geq 1$.

By substituting (8) and (23) into (62), we obtain

$$F_U(u) = \int_0^\infty \left(1 - e^{-\frac{u-1}{\varsigma\lambda_{JE_k}x}}\right)\frac{M}{\lambda_{PJ}}e^{-\frac{x}{\lambda_{PJ}}} \times \left(1 - e^{-\frac{x}{\lambda_{PJ}}}\right)^{M-1} dx. \tag{63}$$

After some mathematical manipulations, we obtain the CDF and PDF of U as follows:

$$F_U(u) = \sum_{\tilde{m}} \left\{ \begin{array}{l} 1 - 2\sqrt{\frac{(\tilde{m}+1)(u-1)}{\varsigma\lambda_{PJ}\lambda_{JE_k}}} \\ \times K_1\left[2\sqrt{\frac{(\tilde{m}+1)(u-1)}{\varsigma\lambda_{PJ}\lambda_{JE_k}}}\right] \end{array} \right\} \tag{64}$$

and

$$f_U(u) = \sum_{\tilde{m}} \frac{2(\tilde{m}+1)}{\varsigma\lambda_{PJ}\lambda_{JE_k}} K_0\left(2\sqrt{\frac{(\tilde{m}+1)(u-1)}{\varsigma\lambda_{PJ}\lambda_{JE_k}}}\right). \tag{65}$$

B. PROOF OF THE PDF OF $V = 1 + \varsigma\gamma_{PJ^*}\gamma_{J^*E_k}$

As in Appendix A, the CDF of V can be formulated as

$$F_V(v) = \Pr\left\{1 + \varsigma\gamma_{PJ^*}\gamma_{J^*E_k} < v\right\} = \int_0^\infty F_{\gamma_{J^*E_k}}\left(\frac{v-1}{\varsigma x}\right) f_{\gamma_{PJ^*}}(x)\,dx, \quad (66)$$

where $v \geq 1$.

By substituting (8) and (28) into (66), we obtain

$$F_V(v) = \left(1 - e^{-\frac{v-1}{\varsigma\lambda_{J^*E_k}x}}\right)^N \frac{M}{\lambda_{PJ^*}} e^{-\frac{x}{\lambda_{PJ^*}}} \times \left(1 - e^{-\frac{x}{\lambda_{PJ^*}}}\right)^{M-1} dx. \quad (67)$$

After some mathematical manipulations, we obtain the CDF and PDF of V as follows:

$$F_V(v) = \sum_{\tilde{m}} \left\{ \begin{array}{l} 1 - \sum_{\tilde{n}} 2\sqrt{\frac{\tilde{n}(\tilde{m}+1)(v-1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}}} \\ \times K_1\left[2\sqrt{\frac{\tilde{n}(\tilde{m}+1)(v-1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}}}\right] \end{array} \right\} \quad (68)$$

and

$$f_V(v) = \sum_{\tilde{m}}\sum_{\tilde{n}} \frac{2\tilde{n}(\tilde{m}+1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}} K_0\left(2\sqrt{\frac{(v-1)\tilde{n}(\tilde{m}+1)}{\varsigma\lambda_{PJ^*}\lambda_{J^*E_k}}}\right). \quad (69)$$

C. PROOF OF THE FORMULA USED IN (45), (53), AND (59)

We reproduce the two functions (6.561.16) and (6.565.7) presented in [57] as follows:

$$\int_0^\infty xK_0(bx)dx = b^{-2} \quad (70)$$

and

$$\int_0^\infty \frac{x}{x^2+a^2} K_0(bx)dx = S_{-1,0}(ab), \quad (71)$$

where $a > 0$ and $b > 0$ are constants.

From these formulas, we have

$$\int_0^\infty \left[K_0(bx)\left(x + \frac{x}{x^2+a^2}\right)\right]dx = b^{-2} + S_{-1,0}(ab). \quad (72)$$

After some mathematical manipulations, we derive (72) as follows:

$$\begin{aligned} \int_0^\infty \left[K_0(bx)\left(\frac{x^3+x}{x^2+a^2}\right)\right]dx &= b^{-2} + S_{-1,0}(ab) - a^2\int_0^\infty \frac{x}{x^2+a^2}K_0(bx)dx \\ &= b^{-2} + S_{-1,0}(ab)\left(1-a^2\right). \quad (73) \end{aligned}$$

ACKNOWLEDGMENTS

The authors would like to thank Dr. Hung Tran at Mälardalen University, Västerås, Sweden for providing us valuable comments.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[2] M. Gholami and R. W. Brennan, "A comparison of alternative distributed dynamic cluster formation techniques for industrial wireless sensor networks," *Sensors*, vol. 16, no. 1, p. 65, Jan. 2016.

[3] T. G. Nguyen, C. So-In, N. 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.

[4] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 8. Jan. 2000, pp. 1–10.

[5] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless-powered communication network," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.

[6] D. Gunduz, K. Stamatiou, N. Michelusi, and M. Zorzi, "Designing intelligent energy harvesting communication systems," *IEEE Commun. Mag.*, vol. 52, no. 1, pp. 210–216, Jan. 2014.

[7] Z. Hadzi-Velkov, I. Nikoloska, G. K. Karagiannidis, and T. Q. Duong, "Wireless networks with energy harvesting and power transfer: Joint power and time allocation," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 50–54, Jan. 2016.

[8] K. W. Choi, L. Ginting, P. A. Rosyady, A. A. Aziz, and D. I. Kim, "Wireless-powered sensor networks: How to realize," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 221–234, Jan. 2017.

[9] T. Ruan, Z. J. Chew, and M. Zhu, "Energy-aware approaches for energy harvesting powered wireless sensor nodes," *IEEE Sensors J.*, vol. 17, no. 7, pp. 2165–2173, Apr. 2017.

[10] H. Tran, J. Åkerberg, M. Björkman, and H.-V. Tran, "RF energy harvesting: An analysis of wireless sensor networks for reliable communication," *Wireless Netw.*, pp. 1–15, Jun. 2017.

[11] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2014.

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

[13] 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.

[14] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2016.

[15] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016.

[16] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," in *Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 1–6.

[17] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[18] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[19] 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, p. 2023, Sep. 2017.

[20] 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. Sens. Netw.*, vol. 12, no. 3, p. 9740750, Mar. 2016.

[21] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, Sep. 2016.

[22] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[23] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[24] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[25] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[26] T. X. Zheng, H. M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.

[27] 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.

[28] 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.

[29] X. Gong, H. Long, F. Dong, and Q. Yao, "Cooperative security communications design with imperfect channel state information in wireless sensor networks," *IET Wireless Sensors Syst.*, vol. 6, no. 2, pp. 35–41, Apr. 2016.

[30] Q. Y. Liau, C. Y. Leow, and Z. Ding, "Physical layer security using two-path successive relaying," *Sensors*, vol. 16, no. 6, p. 846, Jun. 2016.

[31] 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.

[32] A. Araujo, J. Blesa, E. Romero, and O. Nieto-Taladriz, "Cooperative jam technique to increase physical-layer security in CWSN," in *Proc. 2nd Int. Conf. Adv. Cognit. Radio*, Jan. 2012, pp. 11–14.

[33] M. Yang, B. Zhang, Y. Huang, N. Yang, D. Guo, and B. Gao, "Secure multiuser communications in wireless sensor networks with TAS and cooperative jamming," *Sensors*, vol. 16, no. 11, pp. 1908, Nov. 2016.

[34] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. M. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1714–1725, Oct. 2016.

[35] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.

[36] H. Zhang, H. Lei, I. S. Ansari, G. Pan, Z. Ren, and K. A. Qaraqe, "Secrecy performance analysis with optimal DF relay selection of underlay CR networks over Nakagami-m fading channels," in *Proc. IEEE Int. Conf. Commun.*, May 2017, pp. 1–6.

[37] 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: https://doi.org/10.1007/s11036-017-0922-x

[38] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[39] Y. Wan, Q. Li, Q. Zhang, and J. Qin, "Optimal and suboptimal full-duplex secure beamforming designs for MISO two-way communications," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 493–496, Oct. 2015.

[40] 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.

[41] S. Sudevalayam and P. Kulkarni, "Energy harvesting sensor nodes: Survey and implications," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp. 443–461, 3rd Quart., 2010.

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

[43] T.-V. Truong, N.-V. Vo, D.-B. Ha, and D.-D. Tran, "Secrecy performance analysis of energy harvesting wireless networks with multiple power transfer stations and destinations in the presence of multiple eavesdroppers," in *Proc. Nat. Found. Sci. Technol. Develop. Conf. Inform. Comput. Sci.*, Oct. 2016, pp. 107–112.

[44] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4754–4767, Nov. 2013.

[45] V.-D. Nguyen, H. V. Nguyen, and O.-S. Shin, "Wireless energy harvesting for cognitive multihop wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 8, pp. 1–9, Aug. 2015.

[46] J. Liu, Z. Liu, Y. Zeng, and J. Ma, "Cooperative jammer placement for physical layer security enhancement," *IEEE Netw.*, vol. 30, no. 6, pp. 56–61, Dec. 2016.

[47] H. Tran, H.-J. Zepernick, and H. Phan, "Cognitive cooperative networks with decode-and-forward relay selection under interference constraints of multiple primary users," *Wireless Commun. Mobile Comput.*, vol. 15, no. 10, pp. 1433–1443, Sep. 2013.

[48] T. Q. Duong, P. L. Yeoh, V. N. Q. Bao, M. Elkashlan, and N. Yang, "Cognitive relay networks with multiple primary transceivers under spectrum-sharing," *IEEE Signal Process. Lett.*, vol. 19, no. 11, pp. 741–744, Nov. 2012.

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

[50] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

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

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

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

[54] J. Zhang, G.-F. Pan, and Y.-Y. Xie, "Secrecy outage performance for wireless-powered relaying systems with nonlinear energy harvesters," *Frontiers Inform. Technol. Electron. Eng.*, vol. 18, no. 2, pp. 246–252, Feb. 2017.

[55] 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.

[56] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[57] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, A. Jeffrey and D. Zwillinger, Eds. New York, NY, USA: Academic, 2007.

[58] G. N. Watson, *A Treatise on the Theory of Bessel Functions*. Cambridge, U.K.: Cambridge Univ. Press, 1996.

VAN NHAN VO received the B.S. degree in computer science from the University of Da Nang, Da Nang, Vietnam, in 2006, and the M.S. degree, 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 been teaching and studying with Duy Tan University. He is also a member of Cisco Systems, Juniper Systems, and ComPTIA Systems. His research interests include information security, physical-layer security, RF-EH, wireless sensor networks, and the security of other advanced communication systems.

TRI GIA NGUYEN received the B.Ed. degree from the Hue University of Education, Vietnam, in 2011, the M.Sc. degree from Duy Tan University, Vietnam, in 2013, and the Ph.D. degree from Khon Kaen University, Thailand, in 2017, in computer science. He is currently a Post-Doctoral Researcher with the Department of Computer Science, Faculty of Science, Khon Kaen University.

His research interests include the Internet of Things, sensor networks, wireless communications, wireless energy harvesting networks, mobile computing, computer systems, network security, and modeling and analysis.

CHAKCHAI SO-IN (SM'14) received the Ph.D. degree in computer engineering from Washington University at St. Louis, MO, USA, in 2010. He has interned at CNAP-NTU, Singapore, 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 IEEE JSAC, 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 and journals, such as GLOBECOM, ICC, VTC, WCNC, ICNP, ICNC, PIMRC, the IEEE TRANSACTIONS, IEEE letters/magazines, and the *Journal of Computer Networks and Communications*.

ZUBAIR AHMED BAIG is currently a Senior Lecturer in cybersecurity with the School of Science, Edith Cowan University, Perth, WA, Australia, where he is also with the Security Research Institute. He has authored over 50 journal and conference articles and book chapters. His research interests include cybersecurity, artificial intelligence, smart cities, and the Internet of Things. He has served on numerous technical program committees for international conferences and has delivered numerous keynote talks on cybersecurity. He is currently serving as an Editor for the *IET Wireless Sensor Systems* Journal and the *PSU Research Review* Journal, Emerald Publishing House.

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 focuses on network measurement, Internet security, and high-speed networking.