




Secrecy Performance in the Internet of Things: Optimal Energy Harvesting Time Under Constraints of Sensors and Eavesdroppers

Van Nhan Vo^{1,2} · Tri Gia Nguyen³ · Chakchai So-In²  · Hung Tran^{4,5} · Surasak Sanguanpong⁶

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

In this paper, we investigate the physical layer security (PLS) performance for the Internet of Things (IoT), which is modeled as an IoT sensor network (ISN). The considered system consists of multiple power transfer stations (PTSs), multiple IoT sensor nodes (SNs), one legitimate fusion center (LFC) and multiple eavesdropping fusion centers (EFCs), which attempt to extract the transmitted information at SNs without an active attack. The SNs and the EFCs are equipped with a single antenna, while the LFC is equipped with multiple antennas. Specifically, the SNs harvest energy from the PTSs and then use the harvested energy to transmit the information to the LFC. In this research, the energy harvesting (EH) process is considered in the following two strategies: 1) the SN harvests energy from all PTSs, and 2) the SN harvests energy from the best PTS. To guarantee security for the considered system before the SN sends the packet, the SN's power is controlled by a suitable power policy that is based on the channel state information (CSI), harvested energy, and security constraints. An algorithm for the nearly optimal EH time is implemented. Accordingly, the analytical expressions for the existence probability of secrecy capacity and secrecy outage probability (SOP) are derived by using the statistical characteristics of the signal-to-noise ratio (SNR). In addition, we analyze the secrecy performance for various system parameters, such as the location of system elements, the number of PTSs, and the number of EFCs. Finally, the results of Monte Carlo simulations are provided to confirm the correctness of our analysis and derivation.

Keywords Energy harvesting · Internet of things · Wireless sensor networks · Security constraint · Physical layer security

1 Introduction

The Internet of Things (IoT) is an indispensable part of the ongoing advances in the Fourth Industrial Revolution [1]. IoT technology is expected to provide ubiquitous connectivity and information-gathering abilities in healthcare, vehicular, smart city, and industrial environments, among others [2–4]. It is envisioned that physical devices with different types of sensors will be connected to communicate with each other [5]. In other words, an IoT platform can be obtained by integrating cooperative communication in the case of wireless sensor networks (WSNs) to the Internet [6, 7].

The major requirement for IoT applications is security because the IoT has a wide scope, which includes commercial, industrial, governmental, and military applications

[8–15]. Thus, traditional cryptographic protocols are implemented to resolve this problem by using key distribution or certificate management [8, 9]. For instance, R. Roman et al. presented open problems that remain to be addressed in secure IoT, such as cryptographic technologies and data identity management [14]. H. Suo et al. investigated security in the IoT and discussed the research statuses of key technologies, such as encryption mechanisms, communication security, sensor data protection, and cryptographic algorithms [15].

However, traditional cryptographic techniques can be challenging to implement in the IoT because IoT systems include a very large number of machine-type communication devices, heterogeneous radio access technologies, and different subsystems with distinct controlled operators [5]. Therefore, to supplement lightweight cryptographic protocols, physical layer security (PLS) is a promising solution for the IoT [7, 11, 16].

PLS exploits different channel conditions and interference environments without relying on private keys by applying a mathematical model to solve a class of problems

✉ Chakchai So-In
chakso@kku.ac.th

Extended author information available on the last page of the article.

in wireless communication. This approach may provide a fast evaluation of secrecy performance for similar practical systems, and it considers a low-cost solution before implementing a test bed [17–23]. For example, A. Soni et al. investigated recent wireless security techniques and then presented the applicability of wireless PLS techniques to achieve security for IoT devices [17]. T. Pecorella et al. surveyed the IoT threats, proposed a security framework for device initialization, and showed how to increase the security of IoT systems by using a PLS technique [20].

In addition to the security drawback, the energy constraint is also a challenging problem that needs to be resolved for IoT technology. Radio frequency (RF)-energy harvesting (EH) is a potential approach for solving the aforementioned problem because of its flexible and sustainable characteristics [24–30]. There are several environmental sources for harvesting energy, such as thermal, solar, and wireless RF energy sources [31].

However, RF-EH is more interesting for practical deployment because it is readily available in the form of transmitted energy (e.g., TV, radio, mobile base stations, and wireless local area networks) with a low cost [32]. For example, P. Kamalinejad et al. presented an overview of wireless EH units in the context of wireless EH IoT systems, which consist of multiple sensors that transmit data to a sink [24]. H. Hu et al. investigated cognitive IoT, where an IoT network works as the secondary system and an IoT device is a wireless EH node [25]. However, these works have not yet fully clarified PLS that combines with EH for IoT devices.

To the best of our knowledge, no works have investigated secrecy performance under the secure constraint in EH IoT sensor networks (ISNs). Therefore, in this paper, we study the secrecy performance of an RF-EH ISN in which the IoT sensor nodes (SNs) communicate with the multiantenna legitimate fusion center (LFC) in the presence of multiple eavesdropping fusion centers (EFCs). Here, to protect the confidential information of SNs from the EFCs, i.e., to not violate the secure constraint, the power allocation policy of SNs is investigated. Accordingly, our main contributions are as follows:

- We consider two strategies to harvest energy for the RF-EH ISN: 1) the SNs harvest energy from all the power transfer stations (PTSs), and 2) the SNs harvest energy from the best of the PTSs. We then propose a nearly optimal EH time algorithm under the overhearing of multiple EFCs to guarantee security for the considered system. Furthermore, we analyze the condition to determine the optimal PTSs considering the secrecy level.
- We analyze the secrecy performance by deriving an analytical expression for two metrics: the existence probability of secrecy capacity and the secrecy outage probability (SOP) for both strategies.

- We examine the secure performance under various parameters: the EH time; the numbers of PTSs, SNs, and EFCs; the transmit signal-to-noise ratio (SNR) of PTSs; the distance from SNs to LFC; and the EH efficiency coefficient.

The remainder of this paper is organized as follows. Section 2 presents a brief survey of the related work on PLS and EH in ISN. In Section 3, the two EH strategies are described, while the power allocation of the SNs, the nearly optimal EH time, and the number of PTS algorithms of the considered system are detailed in Section 4. In Section 5, the existence probability of secrecy capacity and SOP corresponding to the proposed schemes are analyzed. In Section 6, the numerical results and a discussion are presented. Finally, conclusions and future extensions are summarized in Section 7.

2 Related work

In this section, we summarize and discuss the related research on PLS and EH suitable for IoT applications.

There are several published works that have studied the PLS for IoT to improve secrecy performance [5, 6, 19, 33]. For example, A. Mukherjee et al. presented two system models for IoT: a LFC model and an IoT controller-to-actuator communication model, both applied to an ISN with single-input single-output (SISO) sensors and a multiantenna EFC. In this work, they only reviewed the state of the art in PLS for these models [5].

Z. Chen et al. considered secure uplink transmission in ISN, which consists of multiple SNs communicating with a LFC with the help of an untrusted relay. They presented three different scheduling schemes: an optimal scheduling (OS), a threshold-based scheduling (TS), and a random scheduling (RS). However, they only derived the closed form of the SOP and the secrecy throughput for these schemes without considering the optimal EH time [33].

A. K. Naira et al. investigated wireless communications in the presence of one or more EFCs. This work mainly focused on analyzing the performance of the PLS by exploiting all main fading phenomena, such as path loss, phase fading, and shadow fading. Furthermore, the authors used two heuristic algorithms, “hill climbing” and “random search”, to enhance the secrecy rate of the considered system [6].

Meanwhile, Q. Xu et al. examined secure communications in IoT networks by considering the SOP under two scenarios: SISO and multiple-input multiple-output (MIMO). Accordingly, the authors derived the optimal power allocation and codeword rate design to enhance security for IoT communications [19].

Note that the above two works did not consider EH in IoT; thus, H. Hu et al. considered a single secondary communication link to investigate the secrecy performance for a cognitive IoT, where a wireless EH node is used as an IoT device. Based on this model, they analyzed the proposed secure schemes in terms of the probability of a successful secure transmission metric to enhance secrecy performance [25].

In [34], V. N. Vo et al. investigated the PLS for a system model with multiple sensors that harvest energy from multiple PTSs to deliver packets to a single-antenna base station. Additionally, they proposed a sensor scheduling scheme to improve the secrecy performance. However, they considered a friendly jammer to protect the communication from EFCs, which means that its security depends on the assistance of the friendly jammer. The transmitter transmits the packet without knowing about the security threat, and there is no power allocation policy to protect the communication from EFCs.

Thus, in this paper, we investigate the RF-EH ISN in which SNs can harvest energy from PTSs and then use this energy to transmit the packet to a multiantenna LFC. Multiple EFCs exist that want to steal the packet transmitted from SNs to the LFC. Here, the security before transmission is considered; i.e., the information is protected by a secrecy constraint before sending packets. Accordingly, the transmitter will know its power level to transmit without revealing its information to the EFC. The optimal EH time is also determined by the proposed algorithm.

3 System model and communication protocol

In this section, the system model, the communication protocol, and the EH schemes are introduced.

3.1 System model

We consider the ISN illustrated in Fig. 1 [5]. The considered system, which has N PTSs, is denoted as P ; M SNs are denoted as S ; and one LFC is denoted as B . K passive EFCs are present, which illegally listen to information from the SNs to the LFC. Here, the SNs and the EFCs are equipped with a single antenna due to size limitations, while the LFC has L antennas.

For mathematical modeling purposes, the channel coefficients of $P_n \rightarrow S_m$, $S_m \rightarrow B_l$, and $S_m \rightarrow E_k$ communication links are expressed as $h_{P_n S_m}$, $h_{S_m B_l}$, and $h_{S_m E_k}$, respectively, where $n \in \{1, \dots, N\}$, $m \in \{1, \dots, M\}$, $k \in \{1, \dots, K\}$, and $l \in \{1, \dots, L\}$. The distances of the $P_n \rightarrow S_m$, $S_m \rightarrow B_l$, and $S_m \rightarrow$

E_k communication links are denoted as $d_{P_n S_m}$, $d_{S_m B_l}$, and $d_{S_m E_k}$, respectively. We assume that all channels are modeled as Rayleigh fading channels and that the channel coefficients are random variables distributed according to the Rayleigh model [35–37]. The corresponding cumulative distribution function (CDF) and probability density function (PDF) of the channel gains are given as follows:

$$F_X(x) = 1 - e^{-\frac{x}{\lambda_X}}, \tag{1}$$

$$f_X(x) = \frac{1}{\lambda_X} e^{-\frac{x}{\lambda_X}}, \tag{2}$$

where the random variable X refers to the channel gain and λ_X is the channel mean gain.

3.2 Communication protocol and EH schemes

In the considered system, we adopt wireless-powered communications (WPC) [32]. That is, the communication technique is implemented in two phases: the EH phase and the communication phase. The total time used for both EH and communication is given in Fig. 2. Accordingly, the communication protocol is described as follows:

- In the EH phase, the S_m harvests energy from the PTSs to support the communication phase. Here, we consider the best PTS as a reference case, while the summation of multiple PTSs as the preferred case can improve the system performance. However, we know that the second one always requires complex hardware and advanced processing techniques [38, 39]. This is considered a tradeoff between complexity and performance; i.e., high complexity and high cost will provide more processing efficiency. Accordingly, we focus on the EH phase of the two schemes, as follows:

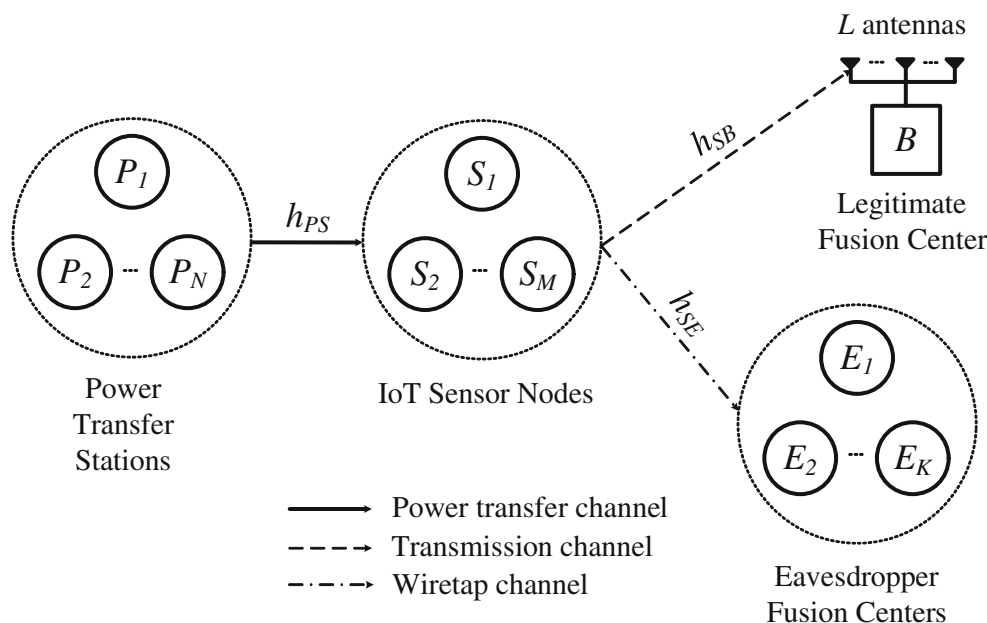
3.2.1 The summary PTS scheme (SPS)

The SNs harvest energy from all PTSs over N wireless links $h_{P_n S_m}$. The summation of harvested energy at the S_m can be given as follows:

$$\begin{aligned} E_{P_n S_m}^{SPS} &= \sum_{n=1}^N \eta \alpha T P_0 \frac{|h_{P_n S_m}|^2}{d_{P_n S_m}^\theta} \\ &= \eta \alpha T P_0 \sum_{n=1}^N \gamma_{P_n S_m}, \end{aligned} \tag{3}$$

where P_0 is the transmitted power of the PTSs; $0 < \eta < 1$ is the EH efficiency coefficient, which depends on the EH circuitry; $0 < \alpha < 1$ is a fraction of the time frame used to harvest energy; θ represents the path loss exponent; and

Fig. 1 System model of ISN with single-antenna SNs and a multi-antenna LFC under overhearing of EFCs



$\gamma_{P_n S_m} = \frac{|h_{P_n S_m}|^2}{d_{P_n S_m}^\theta}$. Accordingly, the PDF and CDF of $\gamma_{P S_m}$ can be obtained as follows:

$$f_{\gamma_{P S_m}}(x) = \sum_{n=1}^N \prod_{\substack{j=1 \\ j \neq n}}^N \frac{e^{-\frac{x}{\lambda_{P_n S_m}}}}{\lambda_{P_n S_m} - \lambda_{P_j S_m}}, \quad (4)$$

$$F_{\gamma_{P S_m}}(x) = \sum_{n=1}^N \prod_{\substack{j=1 \\ j \neq n}}^N \frac{\lambda_{P_n S_m} (1 - e^{-\frac{x}{\lambda_{P_n S_m}}})}{\lambda_{P_n S_m} - \lambda_{P_j S_m}} \quad (5)$$

if $\lambda_{P_n S_m} \neq \lambda_{P_j S_m}$,

where $\gamma_{P S_m} = \sum_{n=1}^N \gamma_{P_n S_m}$, $\lambda_{P_n S_m} = \frac{E[|h_{P_n S_m}|^2]}{d_{P_n S_m}^\theta}$, $\lambda_{P_j S_m} = \frac{E[|h_{P_j S_m}|^2]}{d_{P_j S_m}^\theta}$, and $E[\cdot]$ is the expectation operator.

Proof A detailed proof is presented in [Appendix](#). □

3.2.2 Best PTS scheme (BPS)

The PTS is selected from among N PTSs to transmit wireless energy to S_m such that the channel gain of the $P^* \rightarrow S_m$ link is the largest, i.e.,

$$|h_{P^* S_m}|^2 = \max_{n=1, \dots, N} \{|h_{P_n S_m}|^2\}. \quad (6)$$

Accordingly, the energy harvested at the S_m for BPS can be expressed as follows:

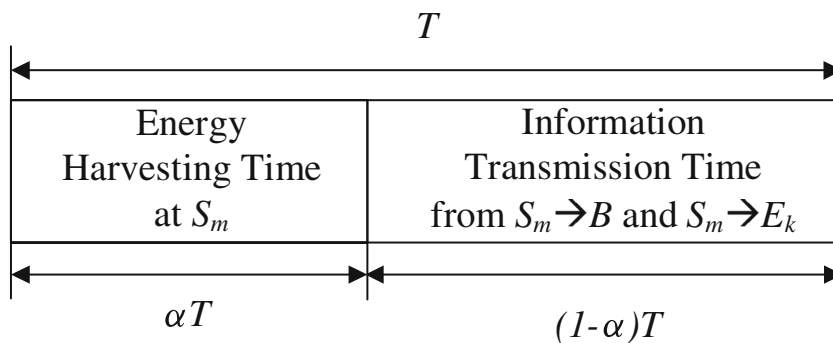
$$E_{P^* S_m}^{BPS} = \eta \alpha T P_0 \frac{|h_{P^* S_m}|^2}{d_{P^* S_m}^\theta} = \eta \alpha T P_0 \gamma_{P^* S_m}, \quad (7)$$

where $\gamma_{P^* S_m} = \frac{|h_{P^* S_m}|^2}{d_{P^* S_m}^\theta}$. Hence, we obtain the PDF and CDF of $\gamma_{P^* S_m}$ as follows [40]:

$$f_{\gamma_{P^* S_m}}(x) = \frac{N}{\lambda_{P^* S_m}} e^{-\frac{x}{\lambda_{P^* S_m}}} \left(1 - e^{-\frac{x}{\lambda_{P^* S_m}}}\right)^{N-1}, \quad (8)$$

$$F_{\gamma_{P^* S_m}}(x) = \left(1 - e^{-\frac{x}{\lambda_{P^* S_m}}}\right)^N, \quad (9)$$

Fig. 2 A time frame T is used for the EH and communication phases



where $\lambda_{P^*S_m} = \frac{E[|h_{P^*S_m}|^2]}{d_{P^*S_m}^\theta}$.

- In the communication phase, the SNs use the harvested energy to transmit information to the LFC; thus, the transmit powers of S_m for the SPS and the BPS are obtained as

$$P_{P^*S_m}^{SPS} = \frac{E_{P^*S_m}^{SPS}}{(1-\alpha)T} = \frac{\eta\alpha P_0}{1-\alpha} \gamma_{P^*S_m}, \tag{10}$$

$$P_{P^*S_m}^{BPS} = \frac{E_{P^*S_m}^{BPS}}{(1-\alpha)T} = \frac{\eta\alpha P_0}{1-\alpha} \gamma_{P^*S_m}. \tag{11}$$

Here, the SNs also estimate the channel state information (CSI) of all $S_m \rightarrow B_l$ links and know which one is the best channel for the $S \rightarrow B$ communication link [41]. To enhance the secrecy performance, the LFC employs selection combining (SC) to combine the received signals; i.e., the best channel gain is chosen to transmit the signals from SNs to the LFC [42, 43]. This can be interpreted as follows:

$$|h_{S^*B^*}|^2 = \max_{m=1, \dots, M} \left\{ \max_{l=1, \dots, L} \left\{ |h_{S_m B_l}|^2 \right\} \right\}. \tag{12}$$

Accordingly, the CDF of $\gamma_{S^*B^*}$ is formulated by using order statistics as follows:

$$F_{\gamma_{S^*B^*}}(x) = \left(1 - e^{-\frac{x}{\lambda_{S^*B^*}}}\right)^{M \times L}, \tag{13}$$

where $\gamma_{S^*B^*} = \frac{|h_{S^*B^*}|^2}{d_{S^*B^*}^\theta}$ and $\lambda_{S^*B^*} = \frac{E[|h_{S^*B^*}|^2]}{d_{S^*B^*}^\theta}$.

Furthermore, the received signals at B^* and E_k are given as follows:

$$y(t) = \sqrt{\frac{P_{P^*S^*}}{d_{S^*B^*}^\theta}} h_{S^*B^*} x(t) + n_{B^*}, \tag{14}$$

$$z(t) = \sqrt{\frac{P_{P^*S^*}}{d_{S^*E_k}^\theta}} h_{S^*E_k} x(t) + n_{E_k}, \tag{15}$$

where $x(t)$ is a transmitted signal; n_{B^*} and n_{E_k} are the additive white complex Gaussian noises at B^* and E_k , respectively; n_{B^*} and $n_{E_k} \in \mathcal{CN}(0, N_0)$; N_0 is the noise power; and $P_{P^*S^*} \in \{P_{P^*S^*}^{SPS}, P_{P^*S^*}^{BPS}\}$. Thus, the instantaneous received SNR at the B^* for the SPS is given by

$$\begin{aligned} \gamma_{P^*B^*}^{SPS} &= \frac{P_{P^*S^*}^{SPS} |h_{S^*B^*}|^2}{d_{S^*B^*}^\theta N_0} \\ &= \frac{\eta\alpha P_0}{(1-\alpha)N_0} \gamma_{P^*S^*} \gamma_{S^*B^*} \\ &= \zeta \gamma_0 \gamma_{P^*S^*} \gamma_{S^*B^*}, \end{aligned} \tag{16}$$

where $\zeta = \frac{\eta\alpha}{1-\alpha}$ and $\gamma_0 = \frac{P_0}{N_0}$.

Similarly, the SNR at the B^* for BPS and the SNRs at E_k for both the SPS and BPS are, respectively, shown as

$$\gamma_{P^*B^*}^{BPS} = \zeta \gamma_0 \gamma_{P^*S^*} \gamma_{S^*B^*}, \tag{17}$$

$$\gamma_{P^*E_k}^{SPS} = \zeta \gamma_0 \gamma_{P^*S^*} \gamma_{S^*E_k}, \tag{18}$$

$$\gamma_{P^*E_k}^{BPS} = \zeta \gamma_0 \gamma_{P^*S^*} \gamma_{S^*E_k}. \tag{19}$$

4 Power allocation of the SNs

In the considered model, the K EFCs can steal the information of the communication from the SNs to the LFC. Therefore, the SNs should regulate their powers to block exposure of the information to the EFCs. This can be interpreted in the constraint of security probability of the SNs as follows [41]:

$$\Pr \left\{ \max_{k \in \{1, 2, \dots, K\}} \{C_{E_k}\} \geq R_e \right\} \leq \omega, \tag{20}$$

where R_e and ω are the secrecy threshold and the secrecy constraint, respectively. $C_{E_k} \in \{C_{E_k}^{SPS}, C_{E_k}^{BPS}\}$ is the instantaneous channel capacity of the $S^* \rightarrow E_k$ link, and C_{E_k} is defined as follows:

$$C_{E_k} = \log_2(1 + \gamma_{PE_k}), \tag{21}$$

where $\gamma_{PE_k} \in \{\gamma_{PE_k}^{SPS}, \gamma_{PE_k}^{BPS}\}$.

By substituting Eq. 21 into Eq. 20, we obtain:

$$\Pr \left\{ \max_{k \in \{1, 2, \dots, K\}} \{\log_2(1 + \gamma_{PE_k})\} \geq R_e \right\} \leq \omega. \tag{22}$$

4.1 The constraint of security probability for the SPS

Since all channels are independent random variables, Eq. 23 can be formulated by substituting Eq. 18 into Eq. 22 as

$$\Theta^{SPS} = 1 - \prod_{k=1}^K \underbrace{\Pr \left\{ \gamma_{PS^*} \leq \frac{2^{R_e} - 1}{\zeta \gamma_0 \gamma_{S^*E_k}} \right\}}_{\Phi(x)} \leq \omega, \tag{23}$$

where Θ^{SPS} is the secrecy probability of SPS. The probability $\Phi(x)$ in Eq. 23 is derived as follows:

$$\begin{aligned} \Phi(x) &= \int_0^\infty F_{\gamma_{PS^*}} \left(\frac{2^{R_e} - 1}{\zeta \gamma_0 x} \right) f_{\gamma_{S^*E_k}}(x) dx \\ &= \sum_{n=1}^N \prod_{\substack{j=1 \\ j \neq n}}^N \frac{\lambda_{P_n S^*}}{\lambda_{P_n S^*} - \lambda_{P_j S^*}} \\ &\quad \times \int_0^\infty \left(1 - e^{-\frac{2^{R_e} - 1}{\zeta \gamma_0 \lambda_{P_n S^*} x}} \right) \frac{1}{\lambda_{S^*E_k}} e^{-\frac{x}{\lambda_{S^*E_k}}} dx. \end{aligned} \tag{24}$$

Using (3.324.1) in [44], the integral $\Phi(x)$ is obtained as follows:

$$\Phi(x) = \sum_N \left[1 - \beta^{SPS} K_1(\beta^{SPS}) \right], \tag{25}$$

where $K_1(\cdot)$ is the Bessel function. \sum_N and β^{SPS} are defined as

$$\sum_N = \sum_{n=1}^N \prod_{\substack{j=1 \\ j \neq n}}^N \frac{\lambda_{P_n S^*}}{\lambda_{P_n S^*} - \lambda_{P_j S^*}}, \tag{26}$$

$$\beta^{SPS} = 2\sqrt{\frac{2^{R_e} - 1}{\zeta \gamma_0 \lambda_{P_n S^*} \lambda_{S^* E_k}}}. \tag{27}$$

By substituting (25) into (23) and after performing some mathematical manipulations, we obtain the expression under the secure constraint to control the power of SNs for SPS as

$$\Theta^{SPS} = 1 - \prod_{k=1}^K \sum_N \left[1 - \beta^{SPS} K_1(\beta^{SPS}) \right] \leq \omega. \tag{28}$$

4.2 The constraint of security probability for the BPS

Similar to the approach for the SPS, the probability security constraint of the BPS is described by

$$\Theta^{BPS} = 1 - \prod_{k=1}^K \underbrace{\Pr \left\{ \gamma_{P^* S^*} \leq \frac{2^{R_e} - 1}{\zeta \gamma_0 \gamma_{S^* E_k}} \right\}}_{\Psi(x)} \leq \omega, \tag{29}$$

where Θ^{BPS} is the secrecy probability of the BPS. The probability $\Psi(x)$ is calculated as follows:

$$\begin{aligned} \Psi(x) &= \int_0^\infty F_{\gamma_{P^* S^*}} \left(\frac{2^{R_e} - 1}{\zeta \gamma_0 x} \right) f_{\gamma_{S^* E_k}}(x) dx \\ &= \int_0^\infty \left(1 - e^{-\frac{2^{R_e} - 1}{\zeta \gamma_0 \lambda_{P^* S^*} x}} \right)^N \frac{1}{\lambda_{S^* E_k}} e^{-\frac{x}{\lambda_{S^* E_k}}} (x) dx \\ &= 1 - \sum_{\tilde{N}} \left[\beta^{BPS} K_1(\beta^{BPS}) \right], \end{aligned} \tag{30}$$

where $\sum_{\tilde{N}}$ and β^{BPS} are defined as

$$\sum_{\tilde{N}} = \sum_{n=1}^N \frac{(-1)^{n+1} N!}{n! (N - n)!}, \tag{31}$$

$$\beta^{BPS} = 2\sqrt{\frac{n(2^{R_e} - 1)}{\zeta \gamma_0 \lambda_{P^* S^*} \lambda_{S^* E_k}}}. \tag{32}$$

Accordingly, the expression under the secure constraint to control the power of SNs for the BPS to protect against multiple EFCs is derived as follows:

$$\Theta^{BPS} = 1 - \prod_{k=1}^K \left[1 - \sum_{\tilde{N}} \beta^{BPS} K_1(\beta^{BPS}) \right] \leq \omega. \tag{33}$$

From Eqs. 28 and 33, we find that the power of SNs depends on the EH time; however, the optimal EH time expression is impossible to obtain due to the Bessel function $K_1(\cdot)$. Thus, we must apply an algorithm to find the nearly optimal EH time α^* by splitting the EH time into an array and substituting each value in this array until Eqs. 28 and 33 are true. Accordingly, the proposed algorithm for SPS and BPS to find α^* is outlined in **Algorithm 1**.

Algorithm 1 Nearly optimal EH time for secure RF-EHI SN.

```

1: procedure NOEHTISN
2:   Initialization
    $\Theta \leftarrow \{\Theta^{SPS}, \Theta^{BPS}\};$ 
    $i \leftarrow 1;$ 
   Array  $\alpha \in (a, b);$  %  $a < b$  are the EH times
3:   while  $\alpha(i) < b$  do
4:     Calculate  $\Theta(i)$  according to (28) or (33);
5:     if  $\Theta(i) = \omega$  then
6:        $\Theta^* \leftarrow \Theta(i);$ 
7:        $\alpha^* \leftarrow \alpha(i);$ 
8:       break;
9:     end if
10:    if  $\Theta^* > \omega$  then
11:       $\Theta^* \leftarrow \Theta(i - 1);$ 
12:       $\alpha^* \leftarrow \alpha(i - 1);$ 
13:      break;
14:    else
15:       $i \leftarrow i + 1;$ 
16:    end if
17:  end while
18:  for  $(i; \alpha(i) \leq b; i++)$  do
19:     $\Theta(i) \leftarrow \Theta^*;$ 
20:  end for
21:  return  $\alpha^*$  and  $\Theta;$ 
22: end procedure

```

Similarly to the approach of **Algorithm 1**, we also propose an algorithm to find the optimal number of PTSs in order to reduce the implementation cost; this algorithm is presented as **Algorithm 2**.

Algorithm 2 Nearly optimal number of PTSs for secure RF-EH ISN.

```

1: procedure NONPTSISN
2:   Initialization
    $\Theta \leftarrow \{\Theta^{SPS}, \Theta^{BPS}\};$ 
    $i \leftarrow 1;$ 
   Array  $N \in [1, c];$  %  $c$  is the number of PTSs
3:   while  $N(i) < c$  do
4:     Calculate  $\Theta(i)$  according to (28) or (33);
5:     if  $\Theta(i) = \omega$  then
6:        $\Theta^* \leftarrow \Theta(i);$ 
7:        $N^* \leftarrow N(i);$ 
8:       break;
9:     end if
10:    if  $\Theta(i) > \omega$  then
11:       $\Theta^* \leftarrow \Theta(i - 1);$ 
12:       $N^* \leftarrow N(i - 1);$ 
13:      break;
14:    else
15:       $i \leftarrow i + 1;$ 
16:    end if
17:  end while
18:  for  $(i; N(i) \leq c; i++)$  do
19:     $\Theta(i) \leftarrow \Theta^*;$ 
20:  end for
21:  return  $N^*$  and  $\Theta;$ 
22: end procedure

```

5 Secrecy performance analysis

In this section, we derive the exact closed-form expressions of secure performance measures for the network scenarios.

5.1 Secrecy capacity

According to the Shannon theorem, the instantaneous channel capacity of the $S^* \rightarrow B^*$ link is formulated as follows [38, 45–47]:

$$C_{B^*} = \log_2(1 + \gamma_{PB^*}), \tag{34}$$

where $C_{B^*} \in \{C_{B^*}^{SPS}, C_{B^*}^{BPS}\}$ and $\gamma_{PB^*} \in \{\gamma_{PB^*}^{SPS}, \gamma_{PB^*}^{BPS}\}$.

Hence, the instantaneous secrecy capacity of wireless transmission from S^* to B^* in the presence of passive E_k is obtained as [47]

$$C_{S_k} = \max\{0, C_{B^*} - C_{E_k}\} = \max\left\{0, \log_2\left(\frac{1 + \gamma_{PB^*}}{1 + \gamma_{PE_k}}\right)\right\}, \tag{35}$$

where $C_{S_k^*} \in \{C_{S_k^*}^{SPS}, C_{S_k^*}^{BPS}\}$.

5.1.1 The joint CDG of γ_{PB^*} and γ_{PE_k} for the SPS

Under Rayleigh fading, the joint CDF of γ_{PB^*} and γ_{PE_k} for SPS is formulated as follows [34]:

$$F_k^{SPS}(x, y) = \int_0^\infty F_{\gamma_{S^*B^*}}\left(\frac{x}{\zeta\gamma_0z}\right) F_{\gamma_{S^*E_k}}\left(\frac{y}{\zeta\gamma_0z}\right) \times f_{\gamma_{PS^*}}(z) dz. \tag{36}$$

By substituting Eqs. 1, 4 and 13 into Eq. 36 and using (3.324.1) in [44], we obtain

$$F_k^{SPS}(x, y) = \int_0^\infty \left(1 - e^{-\frac{x}{\zeta\gamma_0\lambda_{S^*B^*}z}}\right)^{M \times L} \times \left(1 - e^{-\frac{y}{\zeta\gamma_0\lambda_{S^*E_k}z}}\right) \sum_N \frac{1}{\lambda_{P_nS^*}} e^{-\frac{z}{\lambda_{P_nS^*}}} dz = \sum_N \left\{1 - \kappa K_1(\kappa) + \sum_{M \times L} [-\nu K_1(\nu) + \delta K_1(\delta)]\right\}, \tag{37}$$

where $\sum_{M \times L}, \kappa, \nu,$ and δ are defined as follows:

$$\sum_{M \times L} = \sum_{m=1}^{M \times L} \frac{(-1)^{m+1} (M \times L)!}{m! (M \times L - m)!}, \tag{38}$$

$$\kappa = 2\sqrt{\frac{y}{\zeta\gamma_0\lambda_{S^*E_k}\lambda_{P_nS^*}}}, \tag{39}$$

$$\nu = 2\sqrt{\frac{mx}{\zeta\gamma_0\lambda_{S^*B^*}\lambda_{P_nS^*}}}, \tag{40}$$

$$\delta = 2\sqrt{\frac{mx\lambda_{S^*E_k} + y\lambda_{S^*B^*}}{\zeta\gamma_0\lambda_{S^*B^*}\lambda_{S^*E_k}\lambda_{P_nS^*}}}. \tag{41}$$

5.1.2 The joint CDF of γ_{PB^*} and γ_{PE_k} for the BPS

Similarly, the joint CDF of γ_{PB^*} and γ_{PE_k} for BPS is formulated as follows:

$$F_k^{BPS}(x, y) = \int_0^\infty \left(1 - e^{-\frac{x}{\zeta\gamma_0\lambda_{S^*B^*}z}}\right)^{M \times L} \times \left(1 - e^{-\frac{y}{\zeta\gamma_0\lambda_{S^*E_k}z}}\right) \frac{N e^{-\frac{z}{\lambda_{P^*S^*}}}}{\lambda_{P^*S^*}} \left(1 - e^{-\frac{z}{\lambda_{P^*S^*}}}\right)^{N-1} dz = \sum_{\tilde{N}} \left\{1 - \sigma K_1(\sigma) + \sum_{M \times L} [-\psi K_1(\psi) + \chi K_1(\chi)]\right\}, \tag{42}$$

where $\sum_{\tilde{N}}$, σ , ψ , and χ are defined as follows:

$$\sum_{\tilde{N}} = \sum_{n=0}^{N-1} \frac{(-1)^n N!}{(n+1)!(N-n-1)!}, \tag{43}$$

$$\sigma = 2\sqrt{\frac{y(n+1)}{\zeta\gamma_0\lambda_{S^*E_k}\lambda_{P^*S^*}}}, \tag{44}$$

$$\psi = 2\sqrt{\frac{m(n+1)x}{\zeta\gamma_0\lambda_{S^*B^*}\lambda_{P^*S^*}(n+1)}}, \tag{45}$$

$$\chi = 2\sqrt{\frac{mx\lambda_{SE_k} + y\lambda_{S^*B^*}(n+1)}{\zeta\gamma_0\lambda_{S^*E_k}\lambda_{S^*B^*}\lambda_{P^*S^*}}}. \tag{46}$$

5.2 The existence probability of secrecy capacity

The existence probability of secrecy capacity represents the probability that the Shannon capacity of the main channel is greater than that of the EFC channel. Thus, the existence probability of secrecy capacity is defined as follows [34, 48]:

$$\mathcal{E}_k = \Pr \{C_{S_k} > 0\}, \tag{47}$$

where $\mathcal{E}_k \in \{\mathcal{E}_k^{SPS}, \mathcal{E}_k^{BPS}\}$.

5.2.1 The existence probability of secrecy capacity for the SPS

Under Rayleigh fading, the existence probability of secrecy capacity \mathcal{E}_k^{SPS} is calculated as follows:

$$\begin{aligned} \mathcal{E}_k^{SPS} &= \Pr \{C_{S_k}^{SPS} > 0\} \\ &= \int_0^\infty \int_0^x f_k^{SPS}(x, y) dx dy \\ &= \int_0^\infty \left[\frac{\partial F_k^{SPS}(x, y)}{\partial x} \right]_{y=x} dx. \end{aligned} \tag{48}$$

By substituting Eq. 37 into Eq. 48 and using (8.486.14) and (6.561.16) in [44], \mathcal{E}_k^{SPS} is derived as follows:

$$\mathcal{E}_k^{SPS} = \sum_N \sum_{M \times L} \frac{\lambda_{S^*B^*}}{m\lambda_{S^*E_k} + \lambda_{S^*B^*}}. \tag{49}$$

In the considered system with K EFCs, the probability of the existence of a nonzero secrecy capacity is defined as

$$\begin{aligned} \mathcal{E}^{SPS} &= \Pr \left\{ \min_{k=1, \dots, K} \{C_{S_k}^{SPS}\} > 0 \right\} \\ &= \prod_{k=1}^K \Pr \{C_{S_k}^{SPS} > 0\}. \end{aligned} \tag{50}$$

Finally, by substituting Eq. 49 into Eq. 50, we obtain the probability of the existence of a nonzero secrecy capacity

for the SPS as follows:

$$\mathcal{E}^{SPS} = \prod_{k=1}^K \sum_N \sum_{M \times L} \frac{\lambda_{S^*B^*}}{m\lambda_{S^*E_k} + \lambda_{S^*B^*}}. \tag{51}$$

5.2.2 The existence probability of secrecy capacity for the BPS

Similarly, the existence probability of secrecy capacity \mathcal{E}_k^{BPS} is derived as

$$\begin{aligned} \mathcal{E}_k^{BPS} &= \Pr \{C_{S_k}^{BPS} > 0\} \\ &= \sum_{\tilde{N}} \sum_{M \times L} \frac{\lambda_{S^*B^*}}{m\lambda_{S^*E_k} + \lambda_{S^*B^*}}. \end{aligned} \tag{52}$$

Accordingly, the existence probability of secrecy capacity of the considered system for BPS is obtained as

$$\mathcal{E}^{BPS} = \prod_{k=1}^K \sum_{\tilde{N}} \sum_{M \times L} \frac{\lambda_{S^*B^*}}{m\lambda_{S^*E_k} + \lambda_{S^*B^*}}. \tag{53}$$

5.3 Secrecy outage probability

The SOP is defined as the probability that the actual secrecy capacity is below the secure target rate R [36, 37, 49]; i.e.,

$$\mathcal{O}_k = \Pr \{C_{S_k} < R\}, \tag{54}$$

where $\mathcal{O}_k \in \{\mathcal{O}_k^{SPS}, \mathcal{O}_k^{BPS}\}$.

5.3.1 The secrecy outage probability for the SPS

Under Rayleigh fading, the SOP for SPS is formulated as

$$\begin{aligned} \mathcal{O}_k^{SPS} &= \Pr \{C_{S_k}^{SPS} < R\} \\ &= \int_0^\infty \int_0^{2^R(1+y)-1} f_k^{SPS}(x, y) dx dy \\ &= \int_0^\infty \left[\frac{\partial F_k^{SPS}(x, y)}{\partial y} \right]_{x=2^R(1+y)-1} dy. \end{aligned} \tag{55}$$

By substituting Eq. 37 into Eq. 55 and using (8.486.14) in [44], we obtain

$$\mathcal{O}_k^{SPS} = \sum_N \left[1 - \sum_{M \times L} \frac{\lambda_{S^*B^*}}{m\lambda_{S^*E_k}2^R + \lambda_{S^*B^*}} \mu K_1(\mu) \right], \tag{56}$$

where μ is defined as

$$\mu = 2\sqrt{\frac{m(2^R - 1)}{\zeta^*\gamma_0\lambda_{S^*B}\lambda_{P_n S^*}}}. \tag{57}$$

and $\zeta^* = \frac{\eta\alpha^*}{1-\alpha^*}$. For the considered system with multiple EFCs, the SOP for the SPS is derived as follows:

$$\begin{aligned} \mathcal{O}^{SPS} &= \Pr \left\{ \min_{k=1, \dots, K} \left\{ C_{S_k}^{SPS} \right\} < R \right\} \\ &= 1 - \prod_{k=1}^K \left(1 - \Pr \left\{ C_{S_k}^{SPS} < R \right\} \right) \\ &= 1 - \prod_{k=1}^K \left\{ 1 - \sum_N \left[1 - \sum_{M \times L} \lambda \mu K_1(\mu) \right] \right\}, \end{aligned} \tag{58}$$

where λ is defined as

$$\lambda = \frac{\lambda_{S^*B}}{m\lambda_{S^*E_k}2^R + \lambda_{S^*B^*}}. \tag{59}$$

5.3.2 The secrecy outage probability for the BPS

Similar to the approach of the \mathcal{O}^{SPS} , the SOP of the considered system for the BPS is expressed as

$$\mathcal{O}^{BPS} = 1 - \prod_{k=1}^K \left\{ 1 - \sum_{\tilde{N}} \left[1 - \sum_{M \times L} \lambda \phi K_1(\phi) \right] \right\}, \tag{60}$$

where ϕ is defined as

$$\phi = 2\sqrt{\frac{m(n+1)(2^R-1)}{\zeta^*\gamma_0\lambda_{S^*B^*}\lambda_{P^*S^*}}}. \tag{61}$$

6 Numerical results

This section presents and discusses the numerical results obtained through Monte Carlo simulations. Specifically, the impacts of various secrecy constraints (i.e., security level) on the optimal EH time and number of PTSs are investigated. Furthermore, the impacts of the SNR transmitted from PTSs γ_0 , the distance from the SN to LFC $d_{S^*B^*}$, the number of SNs M , the number of EFCs K , and the EH efficiency coefficient η on the secrecy performance are evaluated by two metrics: the existence probability of secrecy capacity and the SOP with the optimal EH time α^* and number of PTSs N^* . Unless otherwise stated, the system parameters for both the analysis and the simulation are as follows [6, 41]: $d_{PS} \in \{1, 2, 3, 4\}$, $d_{SB} \in [0.2, 1.2]$, $d_{SE_k} \in \{4.0, 4.5, 5.0\}$, $R_{th} = 1$, $\alpha \in (0.1, 0.9)$, $\eta \in \{0.75, 0.85, 0.95\}$, $\omega \in \{0.01, 0.02, 0.03\}$, $\gamma_0 \in [-10, 15]$ (dB), $L = 3$, $K \in \{1, 2, 3\}$, $M \in [1, 10]$, and $N \in [1, 12]$. We then evaluate and compare the security performances of the following two schemes:

- Summary power transfer station (SPS): SN harvests energy from all N PTSs.

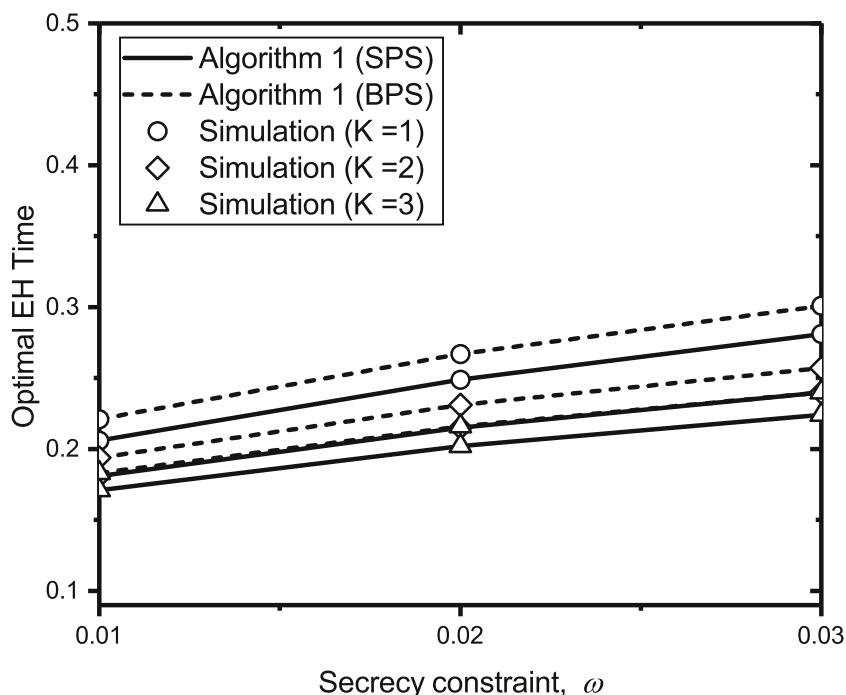
- Best power transfer station (BPS): SN harvests energy from the best PTS.

Figure 3 illustrates the impacts of the secrecy constraint and the number of EFCs on the optimal EH time that is found by Algorithm 1. Here, we define three levels of security: high, medium, and low, i.e., secrecy constraints $\omega = 0.01$, $\omega = 0.02$, and $\omega = 0.03$, respectively. When the secrecy level is decreased from high to low (i.e., the secrecy constraint increases from $\omega = 0.01$ to $\omega = 0.03$), the SNs can harvest more energy in the EH phase and still maintain the security. This result occurs because the EFCs have a higher opportunity to steal the signal at a low security level. However, the higher power of SN increases the EFCs' chance of successfully decoding the SN's signal, which increases the secrecy probability. Hence, the SNs' energy is harvested more as ω increases.

Figure 4 shows an example of the case specifically with a medium security level (i.e., $\omega = 0.02$), demonstrating the impact of the fraction of the EH time α and the number of EFCs ($K = 1, 2$, and 3) on the secrecy probability of SPS and BPS. As shown, when the number of EFCs is the lowest (i.e., $K = 1$), the secrecy probability slowly increases and converges as $\alpha^* = 0.249$ for SPS and as $\alpha^* = 0.267$ for BPS. Similarly, the saturated EH times in the cases of $K = 2$ and $K = 3$ are $\alpha^* = 0.215$ and $\alpha^* = 0.202$ for SPS and $\alpha^* = 0.231$ and $\alpha^* = 0.216$ for BPS, respectively. However, when the EH time is further increased (i.e., $\alpha > 0.267$), the secrecy probability does not change due to the fixed $\omega = 0.2$ (i.e., the harvested energy of SNs is saturated). This means that the SN is controlled such that the energy of SN is not harvested after the EH time reaches the optimal value α^* . In other words, the security is guaranteed by applying α^* to harvest energy for the SNs. Furthermore, we observe that the secrecy probability of the BPS reaches the security constraint more quickly than that of the SPS. This is because the SPS harvests more energy than the BPS.

Similar to Fig. 3, the impacts of the secrecy constraint and the number of EAVs on the optimal number of PTSs are presented in Fig. 5. As shown, the optimal number of PTSs will be increased by decreasing the security level. Specifically, for the case of security level $\omega = 0.02$, we show the impacts of the number of PTSs and the number of EFCs on the secrecy probability in Fig. 6. As shown, the secrecy probability is converged as $N^* = 6$ for the BPS and $N^* = 3$ for the SPS; i.e., the number of PTSs is saturated at the intermediate value to guarantee security. The secrecy probability is also increased as the number of EFCs increases; hence, with a higher number of EFCs, the power of the SN should be decreased to protect the considered

Fig. 3 Impacts of various secrecy constraints and various numbers of EFCs K on the optimal EH times with $\eta = 0.85$, $N = 2$, SNR $\gamma_0 = 5$ (dB), and $M = 4$



system. This is the tradeoff between security and reliability in ISNs.

Figure 7 shows the security probability without **Algorithm 2**. Compared to Fig. 6, when the number of PTSs reaches 6, the security probabilities of the SPS and the BPS overcome the security outage constraint $\omega = 0.02$; i.e., the system will be easy to attack using a higher number of PTSs

without **Algorithm 2**. This means that the system will be secured by using the optimal number of PTSs derived from **Algorithm 2**.

Next, we investigate the secure performance of the considered system by the existence probability of secrecy capacity and the SOP metrics with the optimal EH time and the number of PTSs, which are found by **Algorithm 1**

Fig. 4 Impacts of various EH times and various numbers of EFCs K on the secrecy probability with $\eta = 0.85$, $N = 2$, SNR $\gamma_0 = 5$ (dB), and $M = 4$

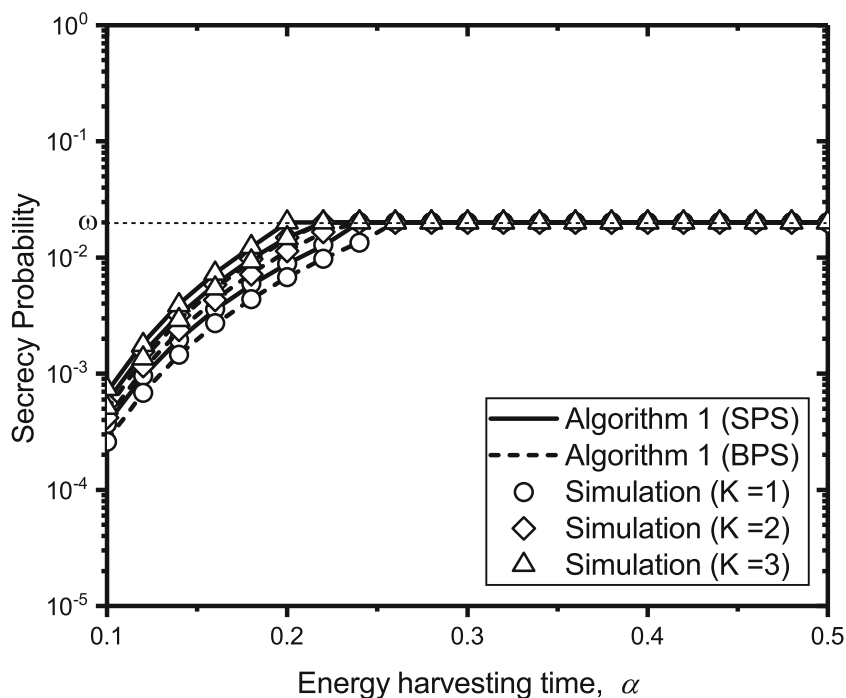
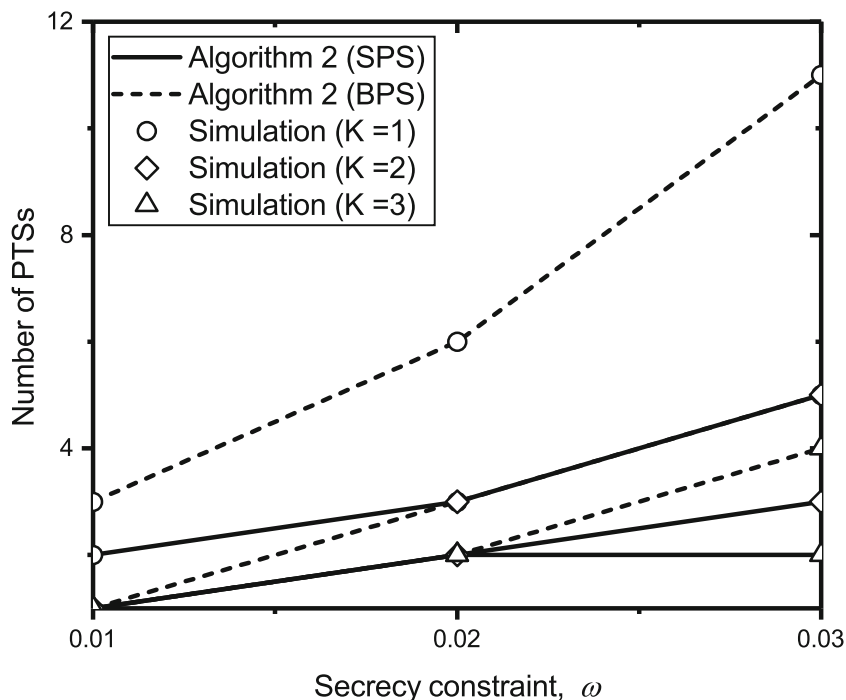


Fig. 5 Impacts of various secrecy constraints and various numbers of EFCs K on the optimal number of PTSs with $\eta = 0.85$, $\alpha = 0.15$, SNR $\gamma_0 = 5$ (dB), and $M = 4$



and **Algorithm 2**. Here, Figs. 8 and 9 provide valuable insights into the existence probability of secrecy capacity. As shown in Fig. 8, the existence probability of secrecy capacity is decreased by increasing the number of EFCs K . In contrast, the secrecy performance can be improved as the number of SNs M increases, as shown in Fig. 9:

When the EFC is increased, the possibility of information being stolen is high. In contrast, the diversity gain at the SNs will increase when we use a higher number of SNs.

As shown in Figs. 8 and 9, the existence probability of secrecy capacity for the SPS is the same as that for the

Fig. 6 Impacts of various numbers of PTSs and various numbers of EFCs K on the secrecy probability with **Algorithm 2** and $\eta = 0.85$, $\alpha = 0.15$, SNR $\gamma_0 = 5$ (dB), and $M = 4$

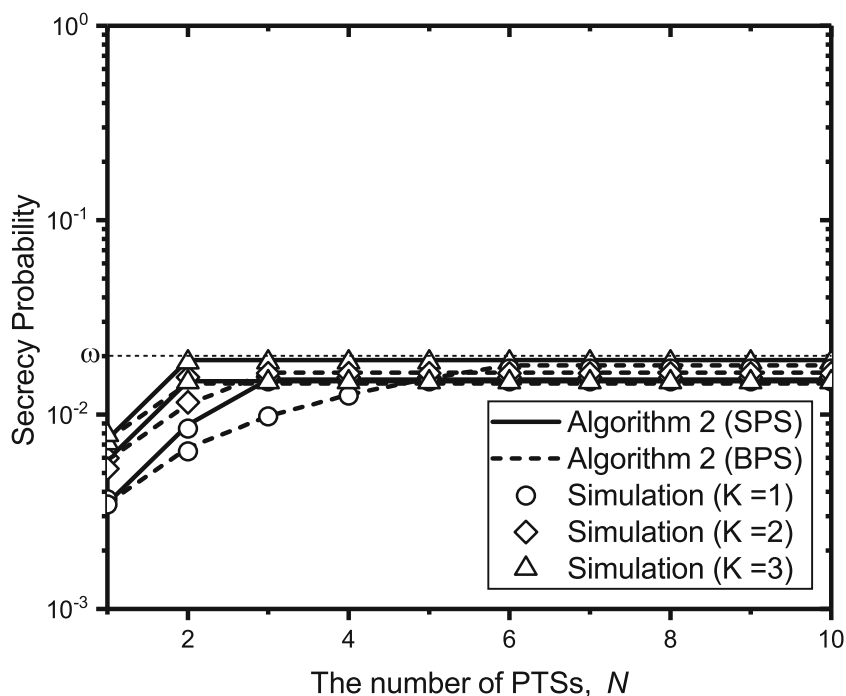
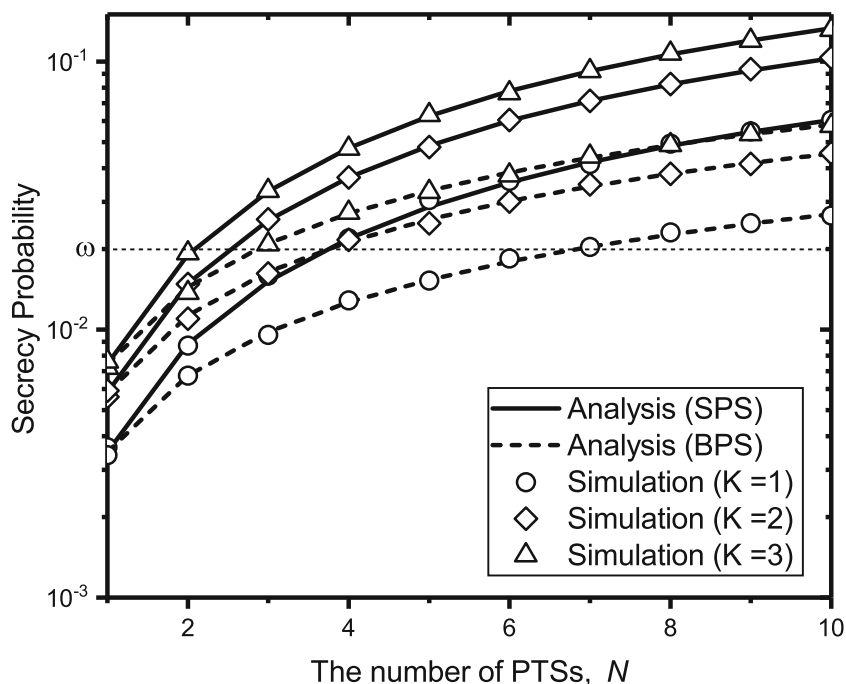


Fig. 7 Impacts of various numbers of PTSs and various numbers of EFCs K on the secrecy probability without **Algorithm 2** and $\eta = 0.85$, $\alpha = 0.15$, SNR $\gamma_0 = 5$ (dB), and $M = 4$



BPS. This result means that this metric is independent of the method of harvesting energy. This is confirmed by Eqs. 51 and 53, and it is not affected by the channel mean gain of the $P \rightarrow S^*$ link. Furthermore, the existence probability of secrecy capacity decreases as the distance from $S^* \rightarrow B^*$ increases. This is because the LFC hardly detects its desired signals under poor channel conditions.

Finally, we provide valuable insights into the SOP, as shown in Figs. 10, 11, 12 and 13. Figure 10 demonstrates the impacts of various SNRs γ_0 and the number of EFCs K on the SOP for the SPS and the BPS. As shown, the SOP decreases as SNRs γ_0 increases or the number of EFCs decreases. This result occurs because more energy is harvested with a higher γ_0 . In contrast, the information will

Fig. 8 Impacts of various distances from S^* to LFC and various numbers of EFCs K on the existence probability of secrecy capacity with $\eta = 0.85$, SNR $\gamma_0 = 5$ (dB), and $M = 4$

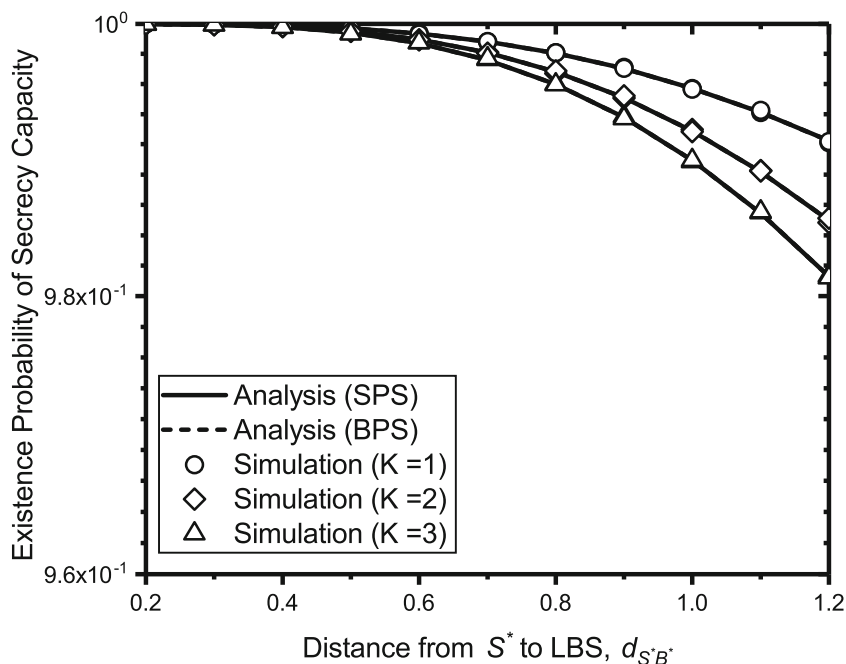
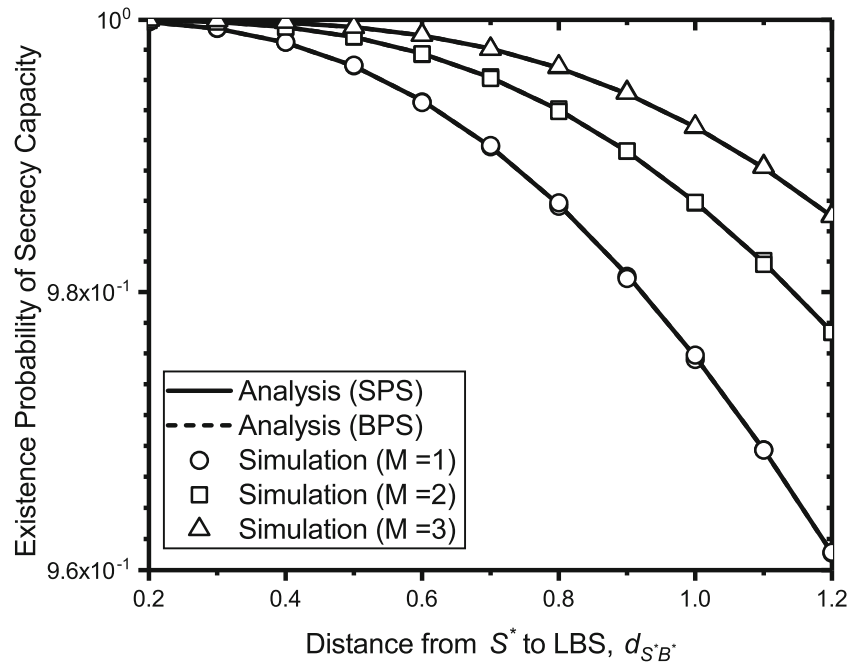


Fig. 9 Impacts of various distances from S^* to LFC and various numbers of SNs on the existence probability of secrecy capacity with $\eta = 0.85$ and SNR $\gamma_0 = 5$ (dB)



be easier to steal when there are more EFCs.

Meanwhile, Fig. 11 shows the effects of various SNRs γ_0 and the number of SNs M on the SOP. As shown, the SNRs γ_0 follows the same trend of the SOP in Fig. 10. However, the SOP will increase as the number of SNs decreases for both schemes. This is because the diversity gain becomes higher as the number of SNs increases.

Figure 12 shows the impacts of the number of SNs and the EH efficiency coefficient of the SNs on the SOP for both

the SPS and the BPS. As shown, when the number of SNs or the EH efficiency coefficient of the SNs is increased, the SOP will decrease; i.e., the secrecy performance improves. This result occurs because higher M or η values mean that more energy is harvested at the SNs (based on Eqs. 3 and 7); this leads to effectively reducing the SOP.

Figure 13 shows the impacts of the distance from S^* to LFC and the EH efficiency coefficient of the SNs on the SOP. As shown, the SOP decreases as the SN moves far

Fig. 10 Impacts of various SNRs γ_0 and various numbers of EFCs K on the SOP with $\eta = 0.85$, SNR $\gamma_0 = 5$ (dB), and $M = 4$

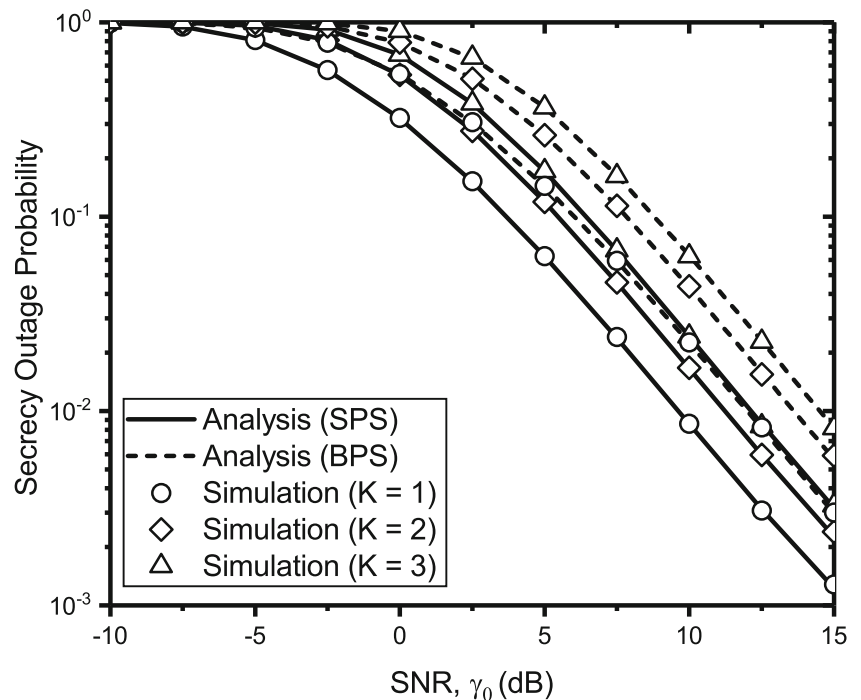
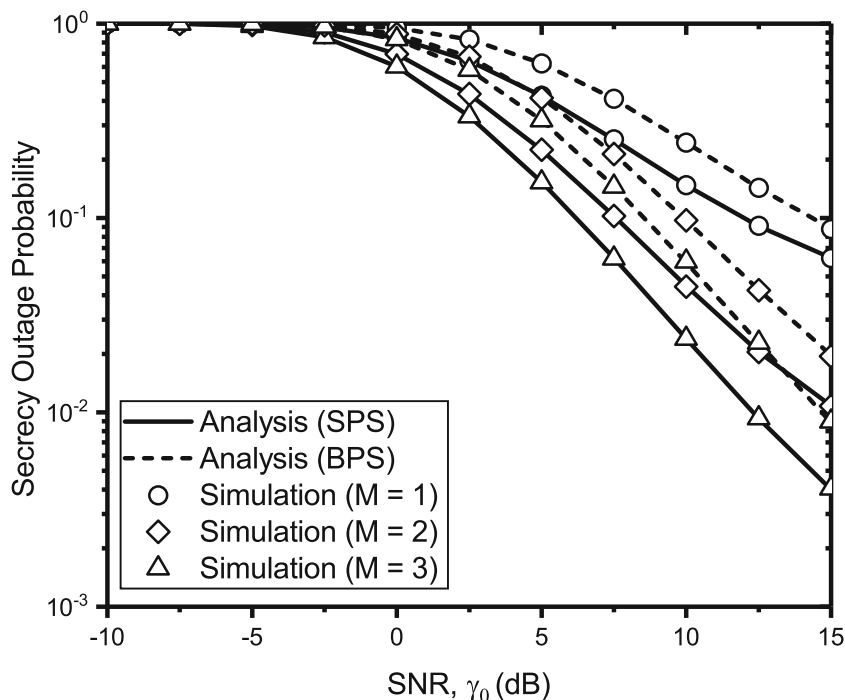


Fig. 11 Impacts of various SNRs γ_0 and various numbers of SNs M on the SOP with $\eta = 0.85$, SNR $\gamma_0 = 5$ (dB), and $M = 4$



away from the LFC. This result occurs because when the distance $d_{S^*B^*}$ is increased, the path loss is also increased. This leads to a decrease in the secrecy performance. The same trend applies to the impacts of $d_{S^*B^*}$ and η , γ_0 and M , and γ_0 and K for the simulations in Figs. 10, 12 and 13, respectively.

In addition, the SOP for the SPS is lower than that of the BPS in Figs. 10, 11, 12 and 13. It is clear that the SN in the SPS harvests energy from all PTSs. Meanwhile, only the best PTS is used for charging SN in the BPS; i.e., the SN's energy of the SPS is higher than that of the BPS. This leads to the SOP for the SPS outperforming the BPS.

Fig. 12 Impacts of various numbers of SNs M and various EH efficiency coefficients η on the SOP with $K = 2$ and SNR $\gamma_0 = 5$ (dB)

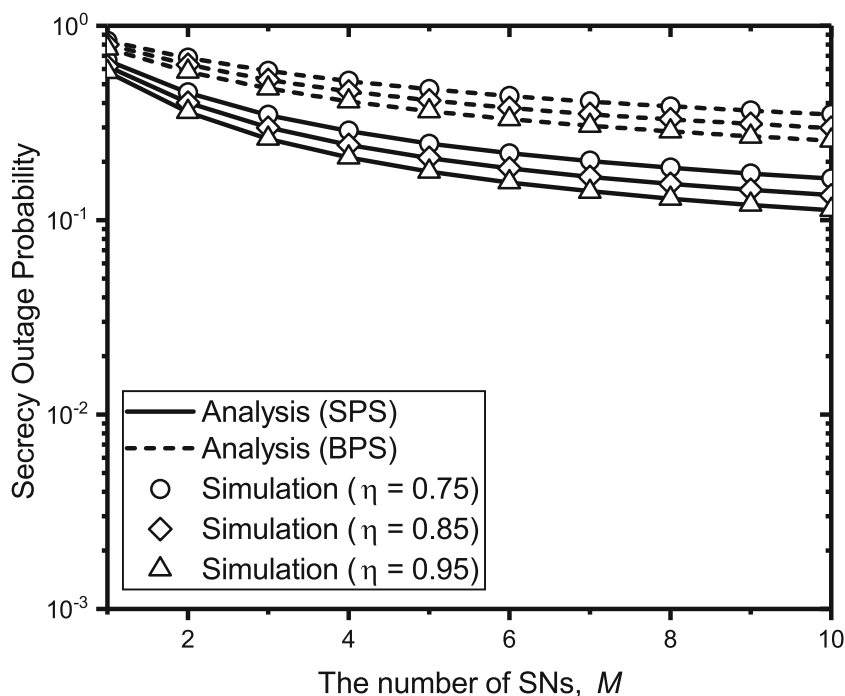
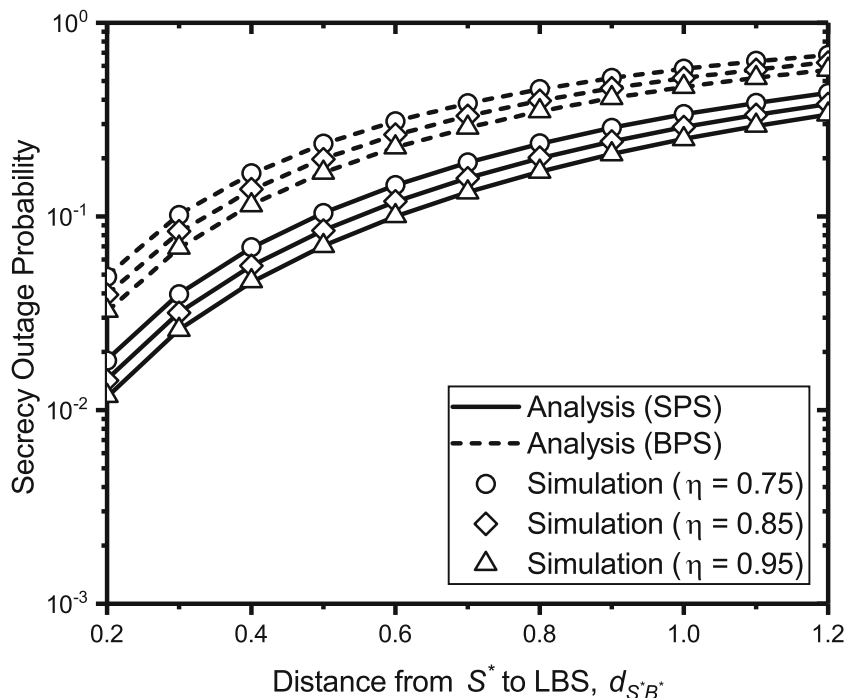


Fig. 13 Impacts of various distances from S^* to LFC and various EH efficiency coefficients η on the SOP with $K = 2$ and SNR $\gamma_0 = 5$ (dB)



7 Conclusion

In this paper, we considered the problem of transmit power allocation to guarantee security for an RF-EH ISN that includes multiple PTSs and SNs and a multiantenna LFC in the presence of multiple EFCs. To compare the tradeoff between signal processing and network performance, we investigated two schemes: SPS and BPS. Accordingly, we proposed a nearly optimal EH time and a nearly optimal number of PTSs algorithms for the RF-EH ISN, in which the SNs are subject to security constraints. Furthermore, the existence probability of secrecy capacity and the SOP for the SPS and the BPS are derived. The numerical results are verified through Monte Carlo simulations. Accordingly, the security of the considered system will be guaranteed by using the optimal EH time and the optimal number of PTS. The simulation results indicate that the secure performance analysis in terms of the existence probability of secrecy capacity and the SOP for both the SPS and the BPS is improved as the numbers of PTSs and SNs increase or the numbers of EFCs decrease. For future work, we will consider a real system with multiple relay clusters and friendly jammers to illustrate a practical implementation of RF-EH ISNs.

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

Appendix: Proofs for the PDF and the CDF of γ_{PS_m}

With the number of power transfer stations $N = 2$, we have

$$\gamma_{PS_m} = \gamma_{P_1S_m} + \gamma_{P_2S_m}. \tag{62}$$

Accordingly, the PDF of γ_{PS_m} is formulated as follows:

$$\begin{aligned} f_{\gamma_{PS_m}}(z) &= \int_{-\infty}^{\infty} \int_{-\infty}^{z-y} f_{\gamma_{P_1S_m} \cdot \gamma_{P_2S_m}}(x, y) dx dy \\ &= \frac{1}{\lambda_{P_1S_m} - \lambda_{P_2S_m}} e^{-\frac{z}{\lambda_{P_1S_m}}} \left[e^{\left(\frac{\lambda_{P_2S_m} - \lambda_{P_1S_m}}{\lambda_{P_2S_m} \lambda_{P_1S_m}}\right)z} - 1 \right] \\ &= \frac{\lambda_{P_1S_m}}{\lambda_{P_1S_m} - \lambda_{P_2S_m}} f_{\gamma_{P_1S_m}}(z) \\ &\quad + \frac{\lambda_{P_2S_m}}{\lambda_{P_2S_m} - \lambda_{P_1S_m}} f_{\gamma_{P_2S_m}}(z) \\ &\quad \text{if } \lambda_{P_nS_m} \neq \lambda_{P_jS_m}. \end{aligned} \tag{63}$$

Using the induction method [50], the PDF of γ_{PS_m} with N PTSs (i.e., the summary of N random variables having nonidentical exponential distributions) can be obtained as follows:

$$\begin{aligned} f_{\gamma_{PS_m}}(z) &= \sum_{n=1}^N \prod_{\substack{j=1 \\ j \neq n}}^N \frac{\lambda_{P_nS_m}}{\lambda_{P_nS_m} - \lambda_{P_jS_m}} f_{\gamma_{P_nS_m}}(z) \\ &\quad \text{if } \lambda_{P_nS_m} \neq \lambda_{P_jS_m}. \end{aligned} \tag{64}$$

Similarly, the CDF of $\gamma_{P_n S_m}$ with N PTSs can be derived:

$$F_{\gamma_{P_n S_m}}(z) = \sum_{n=1}^N \prod_{\substack{j=1 \\ j \neq n}}^N \frac{\lambda_{P_n S_m}}{\lambda_{P_n S_m} - \lambda_{P_j S_m}} F_{\gamma_{P_n S_m}}(z) \quad \text{if } \lambda_{P_n S_m} \neq \lambda_{P_j S_m} \quad (65)$$

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

- Wan J, Tang S, Shu Z, Li D, Wang S, Imran M, Vasilakos AV (2016) Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sens J* 16(20):7373–7380
- Zhang J, Duong TQ, Woods R, Marshall A (2017) Securing wireless communications of the internet of things from the physical layer, an overview. *Entropy* 19(8):1–16
- Heng S, So-In C, Nguyen TG (2017) Distributed image compression architecture over wireless multimedia sensor networks. *Wirel Commun Mob Comput* 2017:1–21
- Nguyen TG, So-In C, Nguyen NG, Phoemphon S (2017) A novel energy-efficient clustering protocol with area coverage awareness for wireless sensor networks. *Peer to Peer Netw Appl* 10(3):519–536
- Mukherjee A (2015) Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proc IEEE* 103(10):1747–1761
- Naira AK, Asmib S, Gopakumar A (2016) Analysis of physical layer security via co-operative communication in internet of things. *Procedia Technol* 24:896–903
- Abomhara M, Koien GM (2014) Security and privacy in the internet of things: Current status and open issues. In: *Proc. IEEE int. conf. privacy security mobile syst.*, pp 1–8
- Granjal J, Monteiro E, Silva JS (2015) Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Commun Survey Tuts* 17(3):1294–1312
- Zhou L, Chao H (2011) Multimedia traffic security architecture for the internet of things. *IEEE Netw* 25(3):35–40
- Jing Q, Vasilakos A, Wan J, Lu J, Qiu D (2014) Security of the internet of things: perspectives and challenges. *Wirel Netw* 20(8):2481–2501
- Zhang K, Liang X, Lu R, Shen X (2014) Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J* 1(5):372–383
- Abomhara M, Koien GM (2014) Security and privacy in the internet of things: Current status and open issues. In: *Proc. IEEE int. conf. privacy security mobile syst.*, pp 1–8
- Skarmeta AF, Ramos JLH, Moreno MV (2014) A decentralized approach for security and privacy challenges in the internet of things. In: *Proc IEEE world forum internet thing*, pp 67–72
- Roman R, Najera P, Lopez J (2011) Securing the internet of things. *Computer* 44(9):51–58
- Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: A review. *Proc IEEE Int Conf Comput Sci Electron Eng* 3:648–651
- Skarmeta AF, Hernandez-Ramos JL, Moreno MV (2014) A decentralized approach for security and privacy challenges in the internet of things. In: *Proc IEEE World Forum Internet Things*, no 67–72
- Soni A, Upadhyay R, Jain A (2017) Internet of things and wireless physical layer security: A survey. *Comput Commun Netw Internet Secur* 5:115–123
- Wang N, Jiang T, Li W, Lv S (2017) Physical-layer security in internet of things based on compressed sensing and frequency selection. *IET Commun* 11(9):1431–1437
- Xu Q, Ren P, Song H, Du Q (2016) Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* 4:2840–2853
- Pecorella T, Brilli L, Mucchi L (2016) The role of physical layer security in IoT: A novel perspective. *Information* 7(3):1–17
- Zhong Z, Peng J, Huang K, Zhong Z (2017) Analysis on physical-layer security for internet of things in ultra dense heterogeneous networks. In: *Proc. int. conf. on internet of things (iThings) and IEEE green computing and commun. (greencom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, pp 39–43
- Van NT, Do TN, Bao VNQ, An B (2017) Performance analysis of wireless energy harvesting multihop cluster-based networks over Nakagami-m fading channels. *IEEE Access* 6:3068–3084
- Vo VN, Nguyen TG, So-In C, Baig ZA, Sanguanpong S (2018) Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy. *IEEE Access*
- Kamalnejad P, Mahapatra C, Sheng Z, Mirabbasi S, Leung VCM, Guan YL (2015) Wireless energy harvesting for the internet of things. *IEEE Commun Mag* 53(6):102–108
- Hu H, Gao Z, Liao X, Leung VCM (2017) Secure communications in ciot networks with a wireless energy harvesting untrusted relay. *Sensors* 17(9):1–21
- Habibu H, Zungeru AM, Susan AA, Gerald I (2014) Energy harvesting wireless sensor networks: Design and modeling. *Int J Wireless Mobile Netw* 6(5):17–31
- Shaikh FK, Zeadally S (2016) Energy harvesting in wireless sensor networks: A comprehensive review. *Renew. Sustain Energy Rev* 55:1041–1054
- Li T, Dong Y, Fan P, Letaief KB (2017) Wireless communications with RF-based energy harvesting: From information theory to green systems. *IEEE Access* 5:27538–27550
- Smart G, Atkinson J, Mitchell J, Rodrigues M, Andreopoulos Y (2016) Energy harvesting for the internet-of-things: Measurements and probability models. In: *Proc int. conf. on telecommun.*, pp 1–6
- Mallick S, Habib A-Z, Ahmed AS, Alam SS (2017) Performance appraisal of wireless energy harvesting in IoT. In: *Proc int. conf. on elect. inform. and commun. technology*, pp 1–6
- Yang G, Ho CK, Guan YL (2014) Dynamic resource allocation for multiple-antenna wireless power transfer. *IEEE Trans Signal Process* 62(14):3565–3577
- Xiao L, Wang P, Niyato D, Kim DI, Han Z (2014) Wireless networks with RF energy harvesting: A contemporary survey. *IEEE Commun Surveys Tutorials* 17(2):757–789
- Chen Z, Ding Z, Dai X, Zhang R (2016) A mathematical proof of the superiority of NOMA compared to conventional OMA. *IEEE Trans. Signal Process.*, pp 1–28. arXiv:1612.01069
- Vo VN, Nguyen TG, So-In C, Ha D-B (2017) Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer. *IEEE Access* 5:25196–25206
- Wang N, Song X, Cheng J, Leung VCM (2014) Enhancing the security of free-space optical communications with secret sharing and key agreement. *J Opt Commun Netw* 6(12):1072–1081
- Ha D-B, Nguyen SQ (2017) Outage performance of energy harvesting DF relaying NOMA networks. *Mobile Networks and Applicat.*, pp 1–14. [Online]. Available: <https://doi.org/10.1007/s11036-017-0922-x>
- Ha D-B, Tran D-D, Truong T-V, Vo N-V (2016) Physical layer secrecy performance of energy harvesting networks with power

- transfer station selection. In: Proc IEEE Int. Conf. Commun. Electron., pp 451–456
38. Naderi MY, Chowdhury KR, Basagni S (2015) Wireless sensor networks with RF energy harvesting: Energy models and analysis. In: Proc IEEE Wireless Commun. and Networking Conf., pp 1494–1499
 39. Oliveira D, Oliveira R (2016) Modeling energy availability in RF energy harvesting networks. In: Proc Int. Symp. on Wireless Commun. Syst., pp 383–387
 40. Hoang TM, Duong TQ, Vo NS, Kundu C (2017) Physical layer security in cooperative energy harvesting networks with a friendly jammer. *IEEE Wireless Commun Lett* 6(2):174–177
 41. Tran H, Quach TX, Tran H, Uhlemann E (2017) Optimal energy harvesting time and transmit power in cognitive radio network under joint constraints of primary users and eavesdroppers. In: Proc. Int. Symp. on Personal, Indoor and Mobile Radio Commun., pp 1–8
 42. Yang N, Yeoh PL, Elkashlan M, Schober R, Collings IB (2013) Transmit antenna selection for security enhancement in mimo wiretap channels. *IEEE Trans Commun* 61(1):144–154
 43. Deng Y, Elkashlan M, Yeoh PL, Yang N, Mallik RK (2014) Cognitive mimo relay networks with generalized selection combining. *IEEE Trans Wireless Commun* 13(9):4911–4922
 44. Gradshteyn I, Ryzhik I, Zwillinger D (2007) Table of integrals, series, and products. In: Jeffrey A (ed). Academic Press, USA
 45. Tran H, Akerberg J, Bjorkman M, Tran H-V (2017) RF energy harvesting: an analysis of wireless sensor networks for reliable communication. *Wirel. Netw*, pp 1–15
 46. Zou Y, Wang G (2016) Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. *IEEE Trans Ind Informat* 12(2):780–787
 47. Barros J, Rodrigues MRD (2006) Secrecy capacity of wireless channels, Proc. IEEE Int. Symp. Inf. Theory, pp 356–360.
 48. Bhargav N, Cotton SL, Simmons DE (2016) Secrecy capacity analysis over κ - μ fading channels: Theory and applications. *IEEE Trans Commun* 64(7):1–26
 49. Toan HV, Bao VNQ, Le HN (2017) Cognitive two-way relay systems with multiple primary receivers: exact and asymptotic outage formulation. *IET Commun* 11(16):2490–2497
 50. Hine G (2017) Proof by mathematical induction: professional practice for secondary teachers. In: Australian Assoc. of Math. Teachers Biennial Conf., pp 1–8



Van Nhan Vo is a Ph.D. student in the Department of Computer Science, Faculty of Science, Khon Kaen University, Thailand. He received his B.S. and M.S. degrees in Computer Science from Da Nang University in 2006 and Duy Tan University, Da Nang, Vietnam, in 2014, respectively. Since 2009, he has taught and studied at Duy Tan University. His research interests include the Internet of Things, information security, physical layer secrecy, RF-

EH, wireless sensor networks, NOMA, and the security of other advanced communication systems.



Tri Gia Nguyen is a post-doctoral researcher in the Department of Computer Science, Faculty of Science, Khon Kaen University, Thailand. He received his B.Ed., M.Sc. and Ph.D. degrees in Computer Science from the Hue University of Education in 2011; Duy Tan University, Vietnam, in 2013; and Khon Kaen University, Thailand, in 2017. 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) is a Professor in the Department of Computer Science at Khon Kaen University, and he received his Ph.D. in Computer Engineering from Washington University in St. Louis, Missouri, USA, in 2010. He was an intern at CNAP-NTU (SG), Cisco Systems, WiMAX Forum and Bell Labs (USA). His research interests include mobile computing, wireless/sensor networks, signal processing, and computer

networking and security. He has served as an editor at SpringerPlus, PeerJ, and ECTI-CIT and as a committee member for many conferences/journals such as Globecom, ICC, VTC, WCNC, ICNP, ICNC, PIMRC, IEEE Transactions, IEEE Letter/Magazines, and Computer Networks/Communications. He has authored over 100 publications and 10 books, including some in IEEE JSAC, IEEE Magazines, and Computer Network/Network Security Labs.




Hung Tran received his B.S. and M.S. degrees in Information Technology from Vietnam National University, Hanoi, in 2002 and 2006, respectively, and his Ph.D. degree from the School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden, in 2013. In 2014, he joined the Electrical Engineering Department, École de Technologie Supérieure, Montreal, Canada. He is currently a postdoctoral researcher at Mälardalen University, Sweden. His research

interests include cognitive radio networks, cooperative communication systems, millimeter wave communications, energy harvesting and security communications at the physical layer.



Surasak Sanguanpong is an Associate Professor in the Department of Computer Engineering and the Director of the Applied Network Research Laboratory, Kasetsart University. He received his B.Eng. and M.Eng. degrees in Electrical Engineering from Kasetsart University in 1985 and 1987, respectively. His research focuses on network measurement, Internet security and high-speed networking.

Affiliations

Van Nhan Vo^{1,2} · Tri Gia Nguyen³ · Chakchai So-In²  · Hung Tran^{4,5} · Surasak Sanguanpong⁶

Van Nhan Vo
vonhanvan@dtu.edu.vn

Tri Gia Nguyen
nguyengiatri@duytan.edu.vn

Hung Tran
tran.hung@mdh.se

Surasak Sanguanpong
surasak.s@ku.ac.th

- ¹ International School, Duy Tan University, Danang 550000, Vietnam
- ² Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
- ³ Faculty of Information Technology, Duy Tan University, Danang 550000, Vietnam
- ⁴ School of Innovation, Design and Engineering, Mälardalen University, Västerås 72123, Sweden
- ⁵ Faculty of Information Technology, Nguyen Tat Thanh University, Ho Chi Minh, 700000, Vietnam
- ⁶ Department of Engineering, Faculty of Engineering, Kasetsart University, Bangkok 10900, Thailand