sensors

MDPI

Article

Secrecy Performance of TAS/SC-Based Multi-Hop Harvest-to-Transmit Cognitive WSNs Under Joint Constraint of Interference and Hardware Imperfection

Phu Tran Tin [1,2], Pham Minh Nam [2,3], Tran Trung Duy [4], Phuong T. Tran [5,*] and Miroslav Voznak [1]

1 VSB, Technical University of Ostrava, 17. listopadu 15/2172, 708 33 Ostrava, Poruba, Czech Republic; phutrantin@iuh.edu.vn (P.T.T.); miroslav.voznak@vsb.cz (M.V.)
2 Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City 700000, Vietnam; 1727002@student.hcmute.edu.vn
3 Faculty of Electrical and Electronics Engineering, HCMC University of Technology and Education, Ho Chi Minh City 700000, Vietnam
4 Department of Telecommunications, Posts and Telecommunications Institute of Technology, Ho Chi Minh City 700000, Vietnam; trantrungduy@ptithcm.edu.vn
5 Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
* Correspondence: tranthanhphuong@tdtu.edu.vn

Received: 11 February 2019; Accepted: 4 March 2019; Published: 7 March 2019

Abstract: In this paper, we evaluate the secrecy performance of multi-hop cognitive wireless sensor networks (WSNs). In the secondary network, a source transmits its data to a destination via the multi-hop relaying model using the transmit antenna selection (TAS)/selection combining (SC) technique at each hop, in the presence of an eavesdropper who wants to receive the data illegally. The secondary transmitters, including the source and intermediate relays, have to harvest energy from radio-frequency signals of a power beacon for transmitting the source data. Moreover, their transmit power must be adjusted to satisfy the quality of service (QoS) of the primary network. Under the joint impact of hardware imperfection and interference constraint, expressions for the transmit power for the secondary transmitters are derived. We also derive exact and asymptotic expressions of secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC) for the proposed protocol over Rayleigh fading channel. The derivations are then verified by Monte Carlo simulations.

Keywords: multi-hop wireless sensor networks; physical-layer security; transmit antenna selection; selection combining; cognitive radio; energy harvesting; hardware impairments

1. Introduction

Security is one of the important issues in wireless sensor networks (WSNs) due to the broadcast nature of wireless medium. Conventionally, encryption/decryption algorithms that generate public/private keys are used to guarantee security [1,2]. Recently, a security framework for the physical layer, called the wiretap channel or physical-layer security (PLS) [3–7], has been introduced as a potential solution. In PLS, the difference between the channel capacity of the data link and the channel capacity of the eavesdropping link, named secrecy capacity, is commonly used to evaluate secrecy performance such as average secrecy capacity (ASC), secrecy outage probability (SOP), and probability of non-zero secrecy capacity (PNSC). Hence, to enhance the secrecy performance, the quality of the data and eavesdropping links should be increased and decreased, respectively. To enhance the

channel capacity of the data links, diversity transmit and receive methods [8–10] can be used. In [8], the transmit antenna selection (TAS) technique is employed at a multi-antenna base station (BS) to maximize the instantaneous signal-to-noise ratios (SNRs) obtained between BS and intended users. References [9,10] considered MIMO secure communication systems, where the transmitter uses the TAS technique, while the legitimate receiver and eavesdropper can use selection combining (SC) or maximal ratio combining (MRC) for reception. In [11–15], cooperative relaying strategies were proposed to improve secrecy performance via increasing the channel capacity for the data links. Moreover, to avoid the eavesdropper combining the data with MRC, a randomize-and-forward (RF) strategy [16] can be employed, where the source and relays generate different code-books to confuse the eavesdropper. For significantly degrading the eavesdropping channels, cooperative jamming (CJ) methods were reported in [17–19]. The basic idea of the CJ method is that jammer nodes are employed to generate artificial noises on the eavesdropper. In addition, the legitimate receivers have to cooperate with the jammers to remove the interference appeared in their received signals. However, the implementation of this technique can be a difficult work due to the requirement of high synchronization between the nodes.

Recently, wireless energy harvesting (EH) [20,21] has emerged as a potential solution to prolong the lifetime of WSNs. In wireless EH, the energy-constrained devices can harvest energy from radio frequency signals generated by ambient nodes. In [21], EH amplify-and-forward (AF) relaying protocols were proposed and analyzed, where the relay node harvests energy from the source for transmitting the source data to the destination. The authors of [22] considered both AF and decode-and-forward (DF) relaying schemes employed a hybrid power splitting (PS) and time switching (TS) EH relay. In [23–25], power beacons (PBs) are deployed in the networks to charge energy for wireless devices. The PB-aided wireless power transfer models are suitable for large-scale WSNs or wireless ad-hoc networks. Moreover, to avoid causing the co-channel interference to the receivers, channels used for harvesting energy from the wireless signals of PBs are different from those used for the data transmission. In [23–25], the authors studied the performance of secondary networks in PB-assisted underlay cognitive radio (PB-UCR), where the transmit power of secondary users was limited by both the harvested energy and the maximum interference levels required by primary users. In [26], a secure communication scenario in cognitive sensor radio networks with an EH eavesdropper was introduced. Reference [27] proposed various path-selection protocols in multi-path multi-hop relaying networks in the presence of active eavesdroppers. Moreover, in [27], all of the terminals whose transceiver hardware is low-cost suffered from hardware imperfection due to phase noise, I/Q imbalance (IQI), amplifier nonlinearities, etc. [28–30].

This paper deals with multi-hop secure communication networks in PB-UCR under impact of hardware impairments. In [31], the authors first evaluated the secrecy capacity in the presence of IQI for OFDMA communication systems. Reference [32] proposed a secure massive MIMO system with a passive multiple-antenna eavesdropper and hardware noises. The results in [31,32] showed that the hardware impairments significantly impact of the secrecy performance. Next, unlike [27], our scheme considers the PB-URC networks using the MIMO-based TAS/SC relaying technique. In [33–35], cooperative multi-hop full-duplex relaying networks were proposed to enhance the end-to-end secrecy performance. However, it is too difficult to apply these schemes into WSNs due to the complexity of full-duplex operation. References [36–38] introduced simple multi-hop secure relaying scenarios in which all of the nodes are equipped with a single antenna. In [39], PLS in downlink MIMO multi-hop heterogeneous cellular networks were investigated. In particular, the data transmission between base stations and mobile users is realized via direct or multi-hop mode. In [40], a multi-hop multicasting secure transmission protocol with multi-antenna DF relays in the presence of multiple eavesdroppers was proposed and analyzed. However, in [36–40], the authors did not consider the cognitive environment as well as the wireless EH technique.

To the best of our knowledge, there is no published work related to multi-hop secure transmission in PB-UCR under the impact of hardware noises. In the proposed protocol, a secondary source

transmits its data to a secondary destination using the multi-hop mode in the presence of a secondary eavesdropper. To support the reliable communication at each hop, the TAS/SC technique is used to forward the source data. Operating on the underlay spectrum sharing method, the transmit power of the secondary source and relay nodes must be adjusted to satisfy the required QoS of the primary network. Moreover, the secondary transmitters have to harvest energy from PB deployed in the secondary network for the data transmission. The main contribution of this paper can be summarized as follows:

- We propose a simple multi-hop MIMO relaying protocol using the TAS/SC technique for PB-UCR WSNs. The proposed protocol can obtain energy efficiency and spectrum usage efficiency, enhance the reliability of data transmission, and improve the secrecy performance.
- In almost published works related to EH and UCR (see [23–25]), the transmitters adjust their transmit power following the instantaneous channel state information. As a result, the transmit power is a random variable (RV), which is not feasible. In this paper, the secondary source and relay nodes are assumed to transmit the source data at fixed transmit power levels. In addition, we derive an exact closed-form expression of the average transmit power of the secondary transmitters under the joint impacts of the energy harvested, the interference constraint, and the maximum transmit power level.
- We investigate the impact of hardware impairments on the end-to-end SOP and PNSC of the proposed scheme. Indeed, the obtained results presented that the hardware imperfection has a significant impact on the secrecy performance. Moreover, the analytical results showed that different values of the hardware impairment levels of the data and eavesdropping links lead to different secrecy performance trend. Finally, it is worth noting that the proposed scheme is a generalized case of the existing schemes in which the transceiver hardware is assumed to be perfect [11,41–43].
- We derive new exact and asymptotic expressions of the end-to-end SOP and PNSC over Rayleigh fading channels, which are then verified by Monte Carlo simulations.

The rest of this paper is organized as follows. The system model of the considered protocol is described in Section 2. In Section 3, the expressions of SOP are derived. The simulation results are shown in Section 4. Finally, this paper is concluded in Section 5.

2. System Model

Figure 1 illustrates the system model of the proposed scheme, in which a secondary source (T_0) wants to transmit its data to a destination (T_K) via $K-1$ intermediate nodes denoted by $\mathrm{T}_1, \mathrm{T}_2, \ldots, \mathrm{T}_{K-1}$. The data transmission between T_0 and T_K is realized via K orthogonal time slots, exploiting the TAS/SC technique. In particular, at the $(k+1)$-th hop, the node T_k selects an antenna to transmit the source data to the node T_{k+1}, which uses the SC technique to combine the signals received from T_k, where $k = 0, 1, \ldots, K$. We assume that all of the nodes including the source, the destination and the relays are equipped with N_D antennas. The transmitter T_k has to harvest energy from wireless signals of a single-antenna power beacon (PB) deployed in the secondary network. Moreover, T_k must adjust the transmit power to satisfy a maximal interference threshold (I_th) required by a single-antenna primary user (PU). Also in the secondary network, there exists an N_E-antenna eavesdropper (E) who uses the SC technique to decode the source data obtained at each hop. Similar to [16], the secondary transmitters randomly generate code-book to confuse the eavesdropper.

Comment 1: Due to the size limitation and complexity constraint, it is assumed that all of the receivers can only use the SC combiner for decoding the data. In addition, the secrecy performance of the proposed protocol is same with that of the corresponding one with multiple non-colluding single-antenna eavesdroppers [44,45]. Finally, in the case where the eavesdropper can employ the MRC technique, the expressions derived in this paper can be used as bound expressions of the secrecy performance.

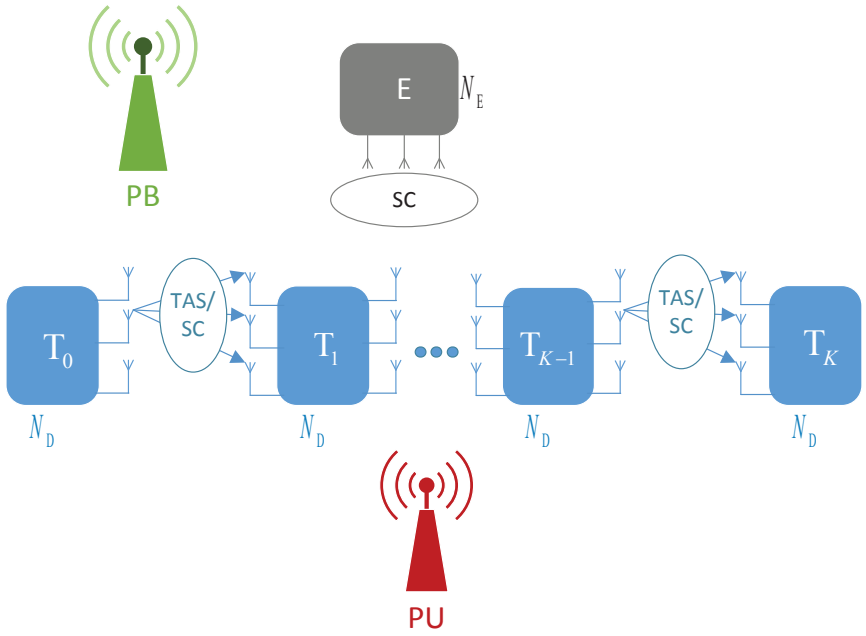

Figure 1. System model of the proposed scheme.

Let us denote $\gamma_{X,Y}$ as the channel gain of the link, where $X, Y \in \{T_k, E, PB, PU\}$. Assume that all of the channels are Rayleigh fading; hence the channel gain $\gamma_{X,Y}$ is an exponential RV. The cumulative distribution function (CDF) and probability density function (PDF) of $\gamma_{X,Y}$ can be expressed, respectively, as

$$F_{\gamma_{X,Y}}(u) = 1 - \exp(-\lambda_{X,Y} u), \; f_{\gamma_{X,Y}}(u) = \lambda_{X,Y} \exp(-\lambda_{X,Y} u), \tag{1}$$

where $\lambda_{X,Y}$ is parameter of the exponential RV $\gamma_{X,Y}$, i.e., $\lambda_{X,Y} = 1/\mathcal{E}\{\gamma_{X,Y}\} = 1/\sqrt{Var\{\gamma_{X,Y}\}}$, where $\mathcal{E}$ is expected operator and $Var\{X\}$ is variance of X. To take path-loss into account, we can model $\lambda_{X,Y}$ as $\lambda_{X,Y} = d_{X,Y}^{\beta}$ [46], where $d_{X,Y}$ is the distance between X and Y, and β is the path-loss exponent.

We denote $\gamma_{T_{k,m},Y}$ as the channel gain between the m-th antenna of T_k and Y, where $m = 1, 2, \ldots, N_D$. Assume that RVs $\gamma_{T_{k,m},Y}$ are independent and identical, i.e., $\lambda_{T_{k,m},Y} = \lambda_{T_k,Y}$ for all m. Also, let $\gamma_{X,T_{k+1,n}}$ and γ_{X,E_p} as channel gain between X and the n-th antenna of T_{k+1}, and that between X and the p-th antenna of E, respectively, where $n = 1, 2, \ldots, N_D$ and $p = 1, 2, \ldots, N_E$. Similarly, $\gamma_{X,T_{k+1,n}}$ and γ_{X,E_p} are independent and identically distributed (i.i.d.) RVs, i.e., $\lambda_{X,T_{k+1,n}} = \lambda_{X,T_{k+1}}$ and $\lambda_{X,E_p} = \lambda_{X,E}$ for all n and p.

Let $\mathcal{T}$ denote the total transmission time between T_0 and T_K, and hence the time allocated for each time slot is given as $\tau = \mathcal{T}/K$. Considering the $(k+1)$-th hop; a duration of $\varepsilon\tau$ is used for T_k to harvest energy, and the remaining duration, i.e., $(1-\varepsilon)\tau$, is spent for the data transmission between T_k and T_{k+1}, where $0 \le \varepsilon \le 1$. Then, the amount of energy that T_K can harvest is given by

$$EH_k = \eta \varepsilon \tau P_B \sum_{v=1}^{N_D} \gamma_{PB,T_{k,v}}, \tag{2}$$

where η $(0 \le \eta \le 1)$ is energy conversion efficiency, and P_B is transmit power of PB.

From (2), we can formulate the transmit power that T_k can use in the data transmission phase by

$$Q_{EH,k} = \frac{EH_k}{(1-\varepsilon)\tau} = \chi P_B \varphi_{sum,k}, \tag{3}$$

where $\chi = \eta\varepsilon/\left(1-\varepsilon\right)$ and $\varphi_{\text{sum},k} = \sum_{v=1}^{N_\text{D}} \gamma_{\text{PB,T}_{k,v}}$. Using (Equation (A.7) [25]), we can write the CDF of $\varphi_{\text{sum},k}$ as

$$F_{\varphi_{\text{sum},k}}\left(z\right) = 1 - \sum_{t=0}^{N_\text{D}-1} \frac{1}{t!}\left(\lambda_{\text{PB,T}_k} z\right)^t \exp\left(-\lambda_{\text{PB,T}_k} z\right). \tag{4}$$

Considering the data transmission between the transmitter A and the receiver B; under the impact of the hardware impairments, the instantaneous SNR received at B can be expressed as in [30,33,34,47,48]:

$$\Psi_{\text{A,B}} = \frac{P_\text{A}\gamma_{\text{A,B}}}{\left(\kappa_\text{A}^2 + \kappa_\text{B}^2\right) P_\text{A}\gamma_{\text{A,B}} + \sigma^2} = \frac{P_\text{A}\gamma_{\text{A,B}}}{\kappa_{\text{A,B}}^2 P_\text{A}\gamma_{\text{A,B}} + \sigma^2}, \tag{5}$$

where $\text{A,B} \in \{\text{T,E,PB,PU}\}$, P_A is transmit power of the transmitter A, $\gamma_{\text{A,B}}$ is channel gain between A and B, σ^2 is the variance of additive white Gaussian noise (AWGN), κ_A^2 and κ_B^2 are constants characterizing the level of the hardware impairments at A and B, respectively, and $\kappa_{\text{A,B}}^2 = \kappa_\text{A}^2 + \kappa_\text{B}^2$ is the total hardware impairment level. The values of κ_A^2, κ_B^2, $\kappa_{\text{A,B}}^2$, which depend on the structure of the transceiver hardware at A and B, can be determined by practical experiments.

Moreover, in the URC network, if T_k uses the m-th antenna to transmit the data, the transmit power must satisfy the interference constraint required by PU as in [25,49]:

$$Q_{\text{IN},k,m} = \frac{I_\text{th}}{\left(1+\kappa_\text{P}^2\right)\gamma_{\text{T}_{k,m},\text{PU}}}, \tag{6}$$

where κ_P^2 is total hardware impairment level at T_k and PU (see [25,49]).

Let P_S denote the maximum transmit power of each antenna; by combining (3) and (6), the transmit power of the m-th antenna at T_k can be formulated by

$$\begin{aligned} P_{k,m} &= \min\left(Q_{\text{EH},k}, Q_{\text{IN},k,m}, P_\text{S}\right) = P_\text{S}\min\left(\mu_1\varphi_{\text{sum},k}, \frac{\mu_2}{\gamma_{\text{T}_{k,m},\text{PU}}}, 1\right) \\ &= \begin{cases} P_\text{S}\min\left(\mu_1\varphi_{\text{sum},k}, \frac{\mu_2}{\gamma_{\text{T}_{k,m},\text{PU}}}\right), & \text{if } \min\left(\mu_1\varphi_{\text{sum},k}, \frac{\mu_2}{\gamma_{\text{T}_{k,m},\text{PU}}}\right) < 1 \\ P_\text{S}, & \text{if } \min\left(\mu_1\varphi_{\text{sum},k}, \frac{\mu_2}{\gamma_{\text{T}_{k,m},\text{PU}}}\right) \geq 1 \end{cases} \end{aligned} \tag{7}$$

where

$$\mu_1 = \frac{\chi P_\text{B}}{P_\text{S}},\ \mu_2 = \frac{I_\text{th}}{\left(1+\kappa_\text{P}^2\right)P_\text{S}}.$$

We can observe from (7) that when $\min\left(\mu_1\varphi_{\text{sum},k}, \mu_2/\gamma_{\text{T}_{k,m},\text{PU}}\right) < 1$, then $P_{k,m} = P_\text{S}\min\left(\mu_1\varphi_{\text{sum},k}, \mu_2/\gamma_{\text{T}_{k,m},\text{PU}}\right)$ is a RV, which is not feasible (although this assumption was widely used in many published literature, e.g., [23–25] and references therein). In practice, the transmit power $P_{k,m}$ should be fixed at pre-determined levels. Indeed, assume that there are $W+1$ fixed levels denoted by L_v $(v = 0, 1, \ldots, W)$ with $L_v = vP_\text{S}/W$. For example, $L_0 = 0$ is the lowest level, and $L_W = P_\text{S}$ is the highest one. Now, by combining with (7), we can write the expression of $P_{k,m}$ as

$$P_{k,m} = \begin{cases} 0, & \text{if } P_{\mathrm{S}} \min\left(\mu_1 \varphi_{\mathrm{sum},k}, \frac{\mu_2}{\gamma_{\mathrm{T}_{k,m},\mathrm{PU}}}\right) < L_1 \\ L_v, & \text{if } v < W,\ L_v \le P_{\mathrm{S}} \min\left(\mu_1 \varphi_{\mathrm{sum},k}, \frac{\mu_2}{\gamma_{\mathrm{T}_{k,m},\mathrm{PU}}}\right) < L_{v+1} \\ L_W, & \text{if } L_W \le P_{\mathrm{S}} \min\left(\mu_1 \varphi_{\mathrm{sum},k}, \frac{\mu_2}{\gamma_{\mathrm{T}_{k,m},\mathrm{PU}}}\right) \end{cases} \tag{8}$$

Now, we consider the data transmission between T_k and T_{k+1}. Employing the TAS/SC technique, the transmit antenna at T_k and the receive antenna at T_{k+1} are selected by the following strategy (see [9]):

$$\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} = \max_{m=1,2,\ldots,N_{\mathrm{D}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} \left(\gamma_{\mathrm{T}_{k,m},\mathrm{T}_{k+1,n}} \right) \right), \tag{9}$$

where b and c are the selected antennas at T_k and T_{k+1}, respectively, $b \in \{1, 2, \ldots, N_{\mathrm{D}}\}$ and $c \in \{1, 2, \ldots, N_{\mathrm{D}}\}$. Since $\gamma_{\mathrm{T}_{k,m},\mathrm{T}_{k+1,n}}$ are i.i.d. RVs, CDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}$ can be obtained by

$$\begin{aligned} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}(x) &= \prod_{m=1}^{N_{\mathrm{D}}} \prod_{n=1}^{N_{\mathrm{D}}} F_{\gamma_{\mathrm{T}_{k,m},\mathrm{T}_{k+1,n}}}(x) = \left(1 - \exp\left(-\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}} x\right)\right)^{N_{\mathrm{D}}^2} \\ &= 1 + \sum_{v=1}^{N_{\mathrm{D}}^2} (-1)^v \begin{pmatrix} N_{\mathrm{D}}^2 \\ v \end{pmatrix} \exp\left(-v \lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}} x\right). \end{aligned} \tag{10}$$

With the presence of hardware impairments, the channel capacity of the $\mathrm{T}_k \rightarrow \mathrm{T}_{k+1}$ link is calculated as

$$C_{\mathrm{D},k} = (1 - \varepsilon)\, \tau \log_2 \left(1 + \frac{P_{k,b} \gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}{\kappa_{\mathrm{D}}^2 P_{k,b} \gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} + \sigma^2}\right), \tag{11}$$

where κ_{D}^2 is the total hardware impairment level at T_k and T_{k+1}, which is assumed to be the same for all values of k.

Let us consider the eavesdropping link at the $(k+1)$-th hop; the channel capacity of the $\mathrm{T}_k \rightarrow \mathrm{E}$ link can be obtained by

$$C_{\mathrm{E},k} = (1 - \varepsilon)\, \tau \log_2 \left(1 + \frac{P_{k,b} \gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\kappa_{\mathrm{E}}^2 P_{k,b} \gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} + \sigma^2}\right), \tag{12}$$

where κ_{E}^2 is the total hardware impairment level at T_k and E. In addition, since E uses the SC combiner, the channel gain $\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}$ can be written as

$$\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} = \max_{p=1,2,\ldots,N_{\mathrm{E}}} \left(\gamma_{\mathrm{T}_{k,b},\mathrm{E}_p} \right), \tag{13}$$

where $g \in \{1, 2, \ldots, N_{\mathrm{E}}\}$. In addition, CDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}$ can be expressed by

$$F_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}(x) = \prod_{p=1}^{N_{\mathrm{E}}} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_p}}(x) = \left(1 - \exp\left(-\lambda_{\mathrm{T}_k,\mathrm{E}} x\right)\right)^{N_{\mathrm{E}}}. \tag{14}$$

From (14), we obtain PDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}$ as

$$\begin{aligned} f_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}(x) &= N_{\mathrm{E}}\lambda_{\mathrm{T}_k,\mathrm{E}}\exp\left(-\lambda_{\mathrm{T}_k,\mathrm{E}}x\right)\left(1-\exp\left(-\lambda_{\mathrm{T}_k,\mathrm{E}}x\right)\right)^{N_{\mathrm{E}}-1} \\ &= \sum_{u=0}^{N_{\mathrm{E}}-1}(-1)^u\begin{pmatrix} N_{\mathrm{E}}-1 \\ u \end{pmatrix}N_{\mathrm{E}}\lambda_{\mathrm{T}_k,\mathrm{E}}\exp\left(-(u+1)\lambda_{\mathrm{T}_k,\mathrm{E}}x\right). \end{aligned} \tag{15}$$

Next, from (11) and (12), the secrecy capacity at the $(k+1)$-th hop is obtained by

$$\begin{aligned} C_{\mathrm{Sec},k} &= \max\left(0, C_{\mathrm{D},k}-C_{\mathrm{E},k}\right) \\ &= \max\left(0,(1-\alpha)\tau\left[\log_2\left(1+\frac{P_{k,b}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}{\kappa_{\mathrm{D}}^2 P_{k,b}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}+\sigma^2}\right)-\log_2\left(1+\frac{P_{k,b}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\kappa_{\mathrm{E}}^2 P_{k,b}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}+\sigma^2}\right)\right]\right). \end{aligned} \tag{16}$$

With the random-and-forward strategy, the end-to-end secrecy capacity of the proposed protocol is given as in [37]:

$$C_{\mathrm{Sec}}^{\mathrm{e2e}} = \min_{k=1,2,\ldots,K}\left(C_{\mathrm{Sec},k}\right). \tag{17}$$

3. Performance Analysis

In this section, we analyze the average transmit power of the secondary transmitters and the secrecy performance of the proposed protocol in terms of SOP and PNSC.

3.1. Average Transmit Power of the Secondary Transmitters

From (8), the average transmit power of T_k can be given by the following formula:

$$\begin{aligned} \mathcal{E}\left\{P_{k,b}\right\} = &\sum_{v=1}^{W-1}\Pr\left(\frac{v}{W}\le\min\left(\mu_1\varphi_{\mathrm{sum},k},\frac{\mu_2}{\gamma_{\mathrm{T}_{k,b},\mathrm{PU}}}\right)<\frac{v+1}{W}\right)\frac{v}{W}P_{\mathrm{S}} \\ &+\Pr\left(1\le\min\left(\mu_1\varphi_{\mathrm{sum},k},\frac{\mu_2}{\gamma_{\mathrm{T}_{k,b},\mathrm{PU}}}\right)\right)P_{\mathrm{S}}, \end{aligned} \tag{18}$$

where $\mathcal{E}\{.\}$ is an expectation operator. To calculate $\mathcal{E}\left\{P_{k,b}\right\}$, we attempt to find CDF of $\min\left(\mu_1\varphi_{\mathrm{sum},k},\mu_2/\gamma_{\mathrm{T}_{k,b},\mathrm{PU}}\right)$. Setting $Z_{\min,k} = \min\left(\mu_1\varphi_{\mathrm{sum},k},\mu_2/\gamma_{\mathrm{T}_{k,b},\mathrm{PU}}\right)$, the CDF of $Z_{\min,k}$ is obtained by

$$F_{Z_{\min,k}}(z) = 1-\left(1-F_{\varphi_{\mathrm{sum},k}}\left(\frac{z}{\mu_1}\right)\right)F_{\gamma_{\mathrm{T}_{k,b},\mathrm{PU}}}\left(\frac{\mu_2}{z}\right). \tag{19}$$

Substituting $F_{\gamma_{\mathrm{T}_{k,b},\mathrm{PU}}}(x) = 1-\exp\left(-\lambda_{\mathrm{T}_k,\mathrm{PU}}x\right)$ and (4) into (19) yields

$$F_{Z_{\min,k}}(z) = 1-\left[\sum_{t=0}^{N_{\mathrm{D}}-1}\frac{1}{t!}\left(\lambda_{\mathrm{PB},\mathrm{T}_k}\frac{z}{\mu_1}\right)^t\exp\left(-\lambda_{\mathrm{PB},\mathrm{T}_k}\frac{z}{\mu_1}\right)\right]\left(1-\exp\left(-\frac{\lambda_{\mathrm{T}_k,\mathrm{PU}}\mu_2}{z}\right)\right). \tag{20}$$

Therefore, the average transmit power of T_k is written by

$$E\left\{P_{k,b}\right\} = \sum_{v=1}^{W-1}\left(F_{Z_{\min,k}}\left(\frac{v+1}{W}\right)-F_{Z_{\min,k}}\left(\frac{v}{W}\right)\right)\frac{v}{W}P_{\mathrm{S}}+\left(1-F_{Z_{\min,k}}(1)\right)P_{\mathrm{S}}. \tag{21}$$

3.2. Secrecy Outage Probability (SOP)

The end-to-end SOP of the proposed protocol can be calculated by

$$\begin{aligned}\mathrm{SOP} &= \Pr(C_{\mathrm{Sec}}^{\mathrm{e2e}}<C_{\mathrm{th}}) = \Pr\left(\min_{\mathrm{k}=1,2,\ldots,\mathrm{K}}(C_{\mathrm{Sec},k}) < C_{\mathrm{th}}\right)\\ &= 1-\prod_{k=1}^{K}\left(1-\Pr\left(C_{\mathrm{Sec},k}<C_{\mathrm{th}}\right)\right)\\ &= 1-\prod_{k=1}^{K}\left(1-\mathrm{SOP}_k\right),\end{aligned} \tag{22}$$

where C_{th} ($C_{\mathrm{th}}>0$) is a predetermined outage threshold, and $\mathrm{SOP}_k=\Pr\left(C_{\mathrm{Sec},k}<C_{\mathrm{th}}\right)$ is the secrecy outage probability at the k-th hop. Using (8) and (16), we can formulate SOP_k by

$$\mathrm{SOP}_k = \sum_{v=1}^{W}\Pr\left(P_{k,b}=L_v\right)\times \underbrace{\Pr\left(\frac{1+\frac{L_v\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}{\kappa_{\mathrm{D}}^2L_v\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}+\sigma^2}}{1+\frac{L_v\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\kappa_{\mathrm{E}}^2L_v\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}+\sigma^2}}<\rho\right)}_{\mathrm{SOP}_k(L_v)}, \tag{23}$$

where $\rho=2^{C_{\mathrm{th}}/(1-\varepsilon)\tau}$.

It is noted from (23) that the secrecy outage event is only considered in the cases where the transmit power $P_{k,b}$ is higher than zero, i.e., $P_{k,b}=L_v$ and $v\geq 1$.

For the probability $\Pr\left(P_{k,b}=L_v\right)$ in (23), it can be calculated by

$$\Pr\left(P_{k,b}=L_v\right)=\begin{cases}F_{Z_{\min,k}}\left(\frac{v+1}{W}\right)-F_{Z_{\min,k}}\left(\frac{v}{W}\right), & \text{if } v<W\\ 1-F_{Z_{\min,k}}(1), & \text{if } v=W\end{cases} \tag{24}$$

Next, let us consider the SOP conditioned on $P_{k,b}=L_v$ as marked in (23); we have

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) &= \Pr\left(\frac{L_v\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}{\kappa_{\mathrm{D}}^2L_v\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}+\sigma^2}<\rho-1+\frac{L_v\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\kappa_{\mathrm{E}}^2L_v\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}+\sigma^2}\rho\right)\\ &= \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}<\alpha_{1,v}+\alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}+\alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right),\end{aligned} \tag{25}$$

where

$$\begin{aligned}&\alpha_0=1-(\rho-1)\kappa_{\mathrm{D}}^2,\ \alpha_{1,v}=\frac{\sigma^2(\rho-1)}{L_v},\ \alpha_2=(\rho-1)\kappa_{\mathrm{E}}^2+\rho,\\ &\alpha_{3,v}=\frac{L_v}{\sigma^2}\left((\rho-1)\kappa_{\mathrm{D}}^2\kappa_{\mathrm{E}}^2+\kappa_{\mathrm{D}}^2\rho-\kappa_{\mathrm{E}}^2\right).\end{aligned} \tag{26}$$

We can observe from (25) that if $\alpha_0\leq 0$ (or $\kappa_{\mathrm{D}}^2\geq 1/(\rho-1)$), $\mathrm{SOP}_k\left(L_v\right)$ always equals 1 for all values of k and v.

In the following, we derive the exact expressions of $\mathrm{SOP}_k\left(L_v\right)$ as given in Lemmas 1–3 below.

Lemma 1. *When $\alpha_0>0$ and $\alpha_{3,v}>0$ $\left(\text{ or } \kappa_{\mathrm{D}}^2>\kappa_{\mathrm{E}}^2/\left(\rho+(\rho-1)\kappa_{\mathrm{E}}^2\right)\right)$, the exact expression of SOP can be given as*

$$\mathrm{SOP}_k\left(L_v\right)=1+\sum_{n=1}^{N_{\mathrm{D}}^2}\sum_{m=0}^{N_{\mathrm{E}}-1}(-1)^{n+m}\beta_0\int_0^{\alpha_0}\exp\left(\beta_1 y\right)\exp\left(-\frac{\beta_2}{y}\right)dy. \tag{27}$$

Proof. At first, when $\alpha_0 > 0$ and $\alpha_{3,v} > 0$, we can rewrite $\mathrm{SOP}_k\left(L_v\right)$ as

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) &= \Pr\left(\left(\alpha_0 - \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\\ &= \Pr\left(\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} \geq \frac{\alpha_0}{\alpha_{3,v}}\right) + \Pr\left(\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} < \frac{\alpha_0}{\alpha_{3,v}}, \gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \frac{\alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\alpha_0 - \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}\right)\\ &= 1 - F_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}\left(\frac{\alpha_0}{\alpha_{3,v}}\right) + \int_0^{\alpha_0/\alpha_{3,v}} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}\left(\frac{\alpha_{1,v} + \alpha_2 x}{\alpha_0 - \alpha_{3,v}x}\right) f_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}(x)\, dx. \end{aligned} \tag{28}$$

By substituting the CDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}$ in (10), and the PDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}$ in (15) into (28), after some manipulations, we arrive at

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) = 1 + \sum_{n=1}^{N_\mathrm{D}^2}\sum_{m=0}^{N_\mathrm{E}-1}(-1)^{n+m}\binom{N_\mathrm{D}^2}{n}\binom{N_\mathrm{E}-1}{m} N_\mathrm{E}\lambda_{\mathrm{T}_k,\mathrm{E}}\\ \times\int_0^{\alpha_0/\alpha_{3,v}} \exp\left(-\left(m+1\right)\lambda_{\mathrm{T}_k,\mathrm{E}}x\right)\exp\left(-n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\frac{\alpha_{1,v}+\alpha_2 x}{\alpha_0 - \alpha_{3,v}x}\right)dx.\end{aligned} \tag{29}$$

By changing variable $y = \alpha_0 - \alpha_{3,v}x$, we have

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) = 1 + \sum_{n=1}^{N_\mathrm{D}^2}\sum_{m=0}^{N_\mathrm{E}-1}(-1)^{n+m}\binom{N_\mathrm{D}^2}{n}\binom{N_\mathrm{E}-1}{m}\frac{N_\mathrm{E}\lambda_{\mathrm{T}_k,\mathrm{E}}}{\alpha_{3,v}}\\ \times\exp\left(n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\frac{\alpha_2}{\alpha_{3,v}} - \left(m+1\right)\lambda_{\mathrm{T}_k,\mathrm{E}}\frac{\alpha_0}{\alpha_{3,v}}\right)\\ \times\int_0^{\alpha_0}\exp\left(\frac{\left(m+1\right)\lambda_{\mathrm{T}_k,\mathrm{E}}}{\alpha_{3,v}}y\right)\exp\left(-n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\frac{\alpha_{1,v}\alpha_{3,v}+\alpha_0\alpha_2}{\alpha_{3,v}y}\right)dy.\end{aligned} \tag{30}$$

With $\alpha_{1,v}\alpha_{3,v} + \alpha_0\alpha_2 = \rho$, we can rewrite (30) as

$$\mathrm{SOP}_k\left(L_v\right) = 1 + \sum_{n=1}^{N_\mathrm{D}^2}\sum_{m=0}^{N_\mathrm{E}-1}(-1)^{n+m}\beta_0\int_0^{\alpha_0}\exp\left(\beta_1 y\right)\exp\left(-\frac{\beta_2}{y}\right)dy. \tag{31}$$

where

$$\begin{aligned}\beta_0 &= \binom{N_\mathrm{D}^2}{n}\binom{N_\mathrm{E}-1}{m}\frac{N_\mathrm{E}\lambda_{\mathrm{T}_k,\mathrm{E}}}{\alpha_{3,v}}\exp\left(\frac{n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\alpha_2 - \left(m+1\right)\lambda_{\mathrm{T}_k,\mathrm{E}}\alpha_0}{\alpha_{3,v}}\right),\\ \beta_1 &= \frac{\left(m+1\right)\lambda_{\mathrm{T}_k,\mathrm{E}}}{\alpha_{3,v}}, \beta_2 = \frac{n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\rho}{\alpha_{3,v}}.\end{aligned} \tag{32}$$

We finish the proof of Lemma 1 here. We note that the integrals in (27) can be easily calculated by computer software such as Matlab or Mathematica. □

Comment 2: We can observe from (27) that the exact expression of $\mathrm{SOP}_k\left(L_v\right)$ is still in integral form, which does not provide any insights into the system performance. Therefore, our next objective is to find an asymptotic expression at high transmit SNR as given in Corollary 1 below.

Corollary 1. *When $\alpha_0 > 0$ and $\alpha_{3,v} > 0$, we can approximate $\mathrm{SOP}_k\left(L_v\right)$ at high transmit SNR $\left(P_\mathrm{S}/\sigma^2 \to +\infty\right)$ by a closed-form expression as*

$$\mathrm{SOP}_k\left(L_v\right) \overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} 1 - \left(1 - \exp\left(-\lambda_{\mathrm{T}_k,\mathrm{E}}\frac{\alpha_0}{\alpha_{3,v}}\right)\right)^{N_\mathrm{E}}. \tag{33}$$

Proof. At high transmit SNR, we can approximate (25) in this case as follows:

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) &= \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} + \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\\ &\overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right) = \Pr\left(\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} > \frac{\alpha_0}{\alpha_{3,v}}\right)\\ &\overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} 1 - F_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}\left(\frac{\alpha_0}{\alpha_{3,v}}\right).\end{aligned} \tag{34}$$

Substituting (14) into (34), we obtain (33). □

Comment 3: Combining (22), (23), (27), and (33), we obtain exact and asymptotic formulas of the end-to-end SOP when $\alpha_0 > 0$ and $\alpha_{3,v} > 0$. Equation (33) implies that $\mathrm{SOP}_k\left(L_v\right)$ at high transmit SNR only depends on $\lambda_{\mathrm{T}_k,\mathrm{E}}$, α_0, and $\alpha_{3,v}$. Moreover, $\mathrm{SOP}_k\left(L_v\right)$ (and the end-to-end SOP) increases when P_S/σ^2 increases.

Lemma 2. *When $\alpha_0 > 0$ and $\alpha_{3,v} < 0$, an exact expression of $\mathrm{SOP}_k\left(L_v\right)$ can be given as*

$$\mathrm{SOP}_k\left(L_v\right) = 1 + \sum_{n=1}^{N_\mathrm{D}^2}\sum_{m=0}^{N_\mathrm{E}-1}(-1)^{n+m+1}\beta_0\int_{\alpha_0}^{+\infty}\exp\left(\beta_1 y\right)\exp\left(-\frac{\beta_2}{y}\right)dy. \tag{35}$$

Proof. Similar to (28), $\mathrm{SOP}_k\left(L_v\right)$ in this case can be written by

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) &= \Pr\left(\left(\alpha_0 - \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\\ &= \Pr\left(\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \frac{\alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\alpha_0 - \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}\right)\\ &= \int_0^{+\infty} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}\left(\frac{\alpha_{1,v} + \alpha_2 x}{\alpha_0 - \alpha_{3,v}x}\right)f_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}\left(x\right)dx.\end{aligned} \tag{36}$$

With the same manner as deriving $\mathrm{SOP}_k\left(L_v\right)$ in (28), we can obtain (35). □

Corollary 2. *At high transmit SNR, $\mathrm{SOP}_k\left(L_v\right)$ in (35) can be approximated by*

$$\mathrm{SOP}_k\left(L_v\right) \overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} \left(1 - \exp\left(\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\frac{\alpha_2}{\alpha_{3,v}}\right)\right)^{N_\mathrm{D}^2}. \tag{37}$$

Proof. Similar to the proof of Corollary 1, we have

$$\begin{aligned}\mathrm{SOP}_k\left(L_v\right) &= \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} + \alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\\ &\overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} \Pr\left(-\alpha_{3,v}\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} < \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right)\\ &\overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}\left(-\frac{\alpha_2}{\alpha_{3,v}}\right).\end{aligned} \tag{38}$$

Substituting (10) into (38), we then obtain (37). □

Comment 4: Combining (22), (23), (35), and (37), we obtain exact and asymptotic expressions of the end-to-end SOP when $\alpha_0 > 0$ and $\alpha_{3,v} < 0$. Equation (37) also shows that at high transmit SNR, $\mathrm{SOP}_k\left(L_v\right)$ (and the end-to-end SOP) decreases as P_S/σ^2 increases.

Lemma 3. *When $\alpha_0 > 0$ and $\alpha_{3,v} = 0$, $\mathrm{SOP}_k(L_v)$ is given by an exact closed-form expression as*

$$\mathrm{SOP}_k(L_v) = 1 + \sum_{n=1}^{N_\mathrm{D}^2} \sum_{m=0}^{N_\mathrm{E}-1} (-1)^{n+m} \binom{N_\mathrm{D}^2}{n} \binom{N_\mathrm{E}-1}{m} \frac{N_\mathrm{E}\lambda_{\mathrm{T}_k,\mathrm{E}}}{(m+1)\lambda_{\mathrm{T}_k,\mathrm{E}} + n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\alpha_2/\alpha_0} \exp\left(-n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\frac{\alpha_{1,v}}{\alpha_0}\right). \quad (39)$$

Proof. In this case, we have

$$\begin{aligned}\mathrm{SOP}_k(L_v) &= \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right) \\ &= \int_0^{+\infty} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}\left(\frac{\alpha_{1,v}}{\alpha_0} + \frac{\alpha_2}{\alpha_0}x\right) f_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}(x)\,dx. \end{aligned} \quad (40)$$

Substituting CDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}$ in (10), and PDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}$ in (15) into (40), after some manipulations, we can obtain (39), and finish the proof. □

Corollary 3. *When $\alpha_0 > 0$ and $\alpha_3 = 0$, $\mathrm{SOP}_k(L_v)$ can be approximated by*

$$\mathrm{SOP}_k(L_v) \overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} 1 + \sum_{n=1}^{N_\mathrm{D}^2} \sum_{m=0}^{N_\mathrm{E}-1} (-1)^{n+m} \binom{N_\mathrm{D}^2}{n} \binom{N_\mathrm{E}-1}{m} \frac{N_\mathrm{E}\lambda_{\mathrm{T}_k,\mathrm{E}}}{(m+1)\lambda_{\mathrm{T}_k,\mathrm{E}} + n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\alpha_2/\alpha_0}. \quad (41)$$

Proof. In this case, we have the following approximation:

$$\begin{aligned}\mathrm{SOP}_k(L_v) &= \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_{1,v} + \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right) \\ &\overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} \Pr\left(\alpha_0\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} < \alpha_2\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}\right) \\ &\overset{P_\mathrm{S}/\sigma^2\to+\infty}{\approx} \int_0^{+\infty} F_{\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}\left(\frac{\alpha_2}{\alpha_0}x\right) f_{\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}(x)\,dx. \end{aligned} \quad (42)$$

□

Substituting CDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}$, and PDF of $\gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}$ into (42), after some manipulations, we can obtain (41).

Comment 5: Equation (41) shows that $\mathrm{SOP}_k(L_v)$, as well as the end-to-end SOP at high transmit SNR, do not depend on P_S/σ^2. It is worth noting that this paper considers a generalized system model where the hardware impairment levels on the data links and eavesdropping links can be different or the same. Moreover, we can observe from Lemmas 1–3 that the secrecy outage probability of the proposed protocol is only expressed by an exact closed-form formula when $\alpha_3 = 0$.

3.3. Probability of Non-Zero Secrecy Capacity (PNSC)

In this subsection, we analyze the end-to-end PNSC of the proposed protocol, which can be formulated by

$$\begin{aligned}\mathrm{PNSC} &= \Pr(C_\mathrm{Sec}^\mathrm{e2e} > 0) = \Pr\left(\min_{k=1,2,\ldots,K}(C_{\mathrm{Sec},k}) > 0\right) \\ &= \prod_{k=1}^{K} \Pr(C_{\mathrm{Sec},k} > 0) \\ &= \prod_{k=1}^{K} \mathrm{PNSC}_k, \end{aligned} \quad (43)$$

where $\mathrm{PNSC}_k = \Pr(C_{\mathrm{Sec},k} > 0)$ is the probability of non-zero secrecy capacity at the k-th hop.

Lemma 4. *The exact expressions of* PNSC_k *can be given by*

$$\mathrm{PNSC}_k = \sum_{v=1}^{M} \Pr\left(P_{k,b} = L_v\right) \times \begin{cases} \sum_{n=1}^{N_\mathrm{D}^2} \sum_{m=0}^{N_\mathrm{E}-1} (-1)^{n+m+1} \chi_0 \int_0^1 \exp\left(\chi_1 y\right) \exp\left(-\frac{\chi_2}{y}\right) dy, & \text{if } \kappa_\mathrm{D}^2 > \kappa_\mathrm{E}^2 \\ \sum_{n=1}^{N_\mathrm{D}^2} \sum_{m=0}^{N_\mathrm{E}-1} (-1)^{n+m+1} \chi_0 \int_1^{+\infty} \exp\left(\chi_1 y\right) \exp\left(-\frac{\chi_2}{y}\right) dy, & \text{if } \kappa_\mathrm{D}^2 < \kappa_\mathrm{E}^2 \\ \sum_{n=1}^{N_\mathrm{D}^2} \sum_{m=0}^{N-1} (-1)^{n+m} \binom{N_\mathrm{D}^2}{n} \binom{N_\mathrm{E}-1}{m} \frac{N_\mathrm{E} \lambda_{\mathrm{T}_k,\mathrm{E}}}{(m+1)\lambda_{\mathrm{T}_k,\mathrm{E}} + n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}}, & \text{if } \kappa_\mathrm{D}^2 = \kappa_\mathrm{E}^2 \end{cases} \tag{44}$$

where $\Pr\left(P_{k,b} = L_v\right)$ *is calculated as in* (24)*, and*

$$\chi_0 = \binom{N_\mathrm{D}^2}{n} \binom{N_\mathrm{E}-1}{m} \frac{N_\mathrm{E} \lambda_{\mathrm{T}_k,\mathrm{E}} \sigma^2}{L_v\left(\kappa_\mathrm{D}^2 - \kappa_\mathrm{E}^2\right)} \exp\left(\frac{\left(n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}} - (m+1)\lambda_{\mathrm{T}_k,\mathrm{E}}\right)\sigma^2}{L_v\left(\kappa_\mathrm{D}^2 - \kappa_\mathrm{E}^2\right)}\right),$$
$$\chi_1 = \frac{(m+1)\lambda_{\mathrm{T}_k,\mathrm{E}}\sigma^2}{L_v\left(\kappa_\mathrm{D}^2 - \kappa_\mathrm{E}^2\right)}, \chi_2 = \frac{n\lambda_{\mathrm{T}_k,\mathrm{T}_{k+1}}\sigma^2}{L_v\left(\kappa_\mathrm{D}^2 - \kappa_\mathrm{E}^2\right)}. \tag{45}$$

Proof. Similar to (23), we can formulate PNSC_k as

$$\mathrm{PNSC}_k = \sum_{v=1}^{M} \Pr\left(P_{k,b} = L_v\right) \times \Pr\left(\frac{1 + \frac{L_v \gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}}}{\kappa_\mathrm{D}^2 L_v \gamma_{\mathrm{T}_{k,b},\mathrm{T}_{k+1,c}} + \sigma^2}}{1 + \frac{L_v \gamma_{\mathrm{T}_{k,b},\mathrm{E}_g}}{\kappa_\mathrm{E}^2 L_v \gamma_{\mathrm{T}_{k,b},\mathrm{E}_g} + \sigma^2}} > 1\right)$$
$$= \sum_{v=1}^{M} \Pr\left(P_{k,b} = L_v\right) \times \left[1 - \lim_{\rho \to 1} \left(\mathrm{SOP}_k\left(L_v\right)\right)\right]. \tag{46}$$

Next, by substituting $\rho = 1$, $\alpha_0 = 1$, $\alpha_{1,v} = 0$, $\alpha_2 = 1$ into $\alpha_{3,v} = L_v\left(\kappa_\mathrm{D}^2 - \kappa_\mathrm{E}^2\right)/\sigma^2$ in (27), (35), and (39), we can obtain (45). □

Comment 6: Similar to [37], the end-to-end PNSC can be obtained with three different cases, i.e., $\kappa_\mathrm{D}^2 > \kappa_\mathrm{E}^2$, $\kappa_\mathrm{D}^2 < \kappa_\mathrm{E}^2$, and $\kappa_\mathrm{D}^2 = \kappa_\mathrm{E}^2$. Moreover, when $\kappa_\mathrm{D}^2 = \kappa_\mathrm{E}^2$, we obtain the exact closed-form expression of the end-to-end PNSC. Finally, with $\kappa_\mathrm{D}^2 = \kappa_\mathrm{E}^2$, the end-to-end PNSC value does not depend on the transmit SNR as well as the hardware impairment levels.

4. Simulation Results

In this section, we present Monte Carlo simulations to verify the theoretical results obtained in Section 3 by using MATLAB 2014a. For Monte Carlo experiments, we perform 10^5–$5 * 10^6$ independent trials, and in each trial, the Rayleigh channel coefficients for all of the links are generated to obtain the end-to-end secrecy performance. For the theoretical results, the expressions derived in Section 3 are used to present them.

In the simulation environment, a two-dimensional Oxy plane is considered, where the primary user (PU), the power beacon (PB), the secondary eavesdropper (E), and the secondary node (T_k) are located at $(x_\mathrm{P}, y_\mathrm{P})$, $(x_\mathrm{B}, y_\mathrm{B})$, $(x_\mathrm{E}, y_\mathrm{E})$, and $(k/K, 0)$, respectively, where $k = 0, 1, \ldots, K$. In all of the simulations, we fix the path-loss exponent (β) by 3, the number of transmit power levels (W) by 8, the variance of Gaussian noises $\left(\sigma^2\right)$ by 1, and the block time $(\mathcal{T})$ by 1. Moreover, we assume that $P_\mathrm{B} = 2P_\mathrm{S} = 4I_\mathrm{th}$, and the total hardware impairment level κ_P^2 equals 0. It is noted from figures that simulation results (Sim) are presented by markers, while the theoretical results including exact ones (Exact) and asymptotic ones (Asym) are presented by solid and dash lines, respectively.

In Figure 2, we present the average transmit power of the secondary transmitters as a function of P_S. In this simulation, the number of hops (K) is 3, the number of antennas at the node T_k (N_D) equals 3, the energy conversion efficiency (η) by 0.25, and the fraction of time spent for the EH phase (ε) is 0.25. In addition, the co-ordinates of PB and PU are $(0.4, 0.3)$ and $(0.6, -0.5)$, respectively. We can observe from Figure 2 that the average transmit power of the source (T_0) is highest because the Euclidean distance between T_0 and PU is farthest. We also see that the average transmit power of T_0, T_1, and T_2 linearly increases as P_S increases. It is worth noting that the simulation results match very well with the theoretical ones, which validates our derivations.

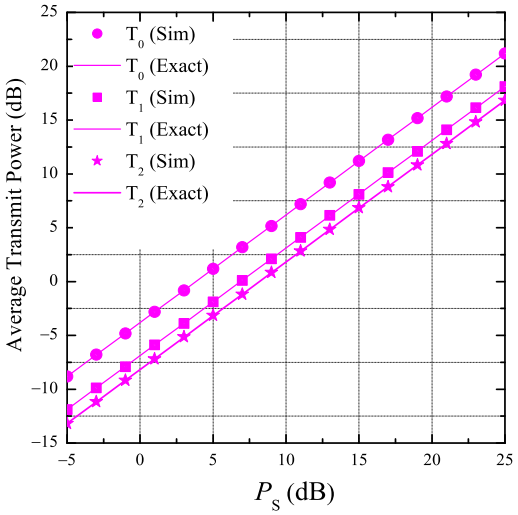

Figure 2. Average transmit power of the secondary transmitters as a function of P_S when $K = 3$, $N_D = 3$, $\varepsilon = 0.25$, $\eta = 0.25$, $x_B = 0.4$, $y_B = 0.3$, $x_P = 0.6$, and $y_P = -0.5$.

Figure 3 investigates the impact of the positions of PU and PB on the average transmit power of the secondary transmitters. Particularly, we change x_B from 0.1 to 0.9, and x_P is calculated by $x_P = 1 - x_B$. Moreover, we fix the values of y_B and y_P by 0.3 and –0.5, respectively. It can be seen from Figure 3 that the average transmit power of T_0, T_1, and T_2 varies with different positions of PB and PU. For example, when $x_B = 0.1$, the positions of PB and PU are (0.1, 0.3) and (0.9, –0.5), respectively. In this case, the average transmit power of T_2 is lowest because this node is nearest to PU. For another example, $x_B = 0.5$, the distances between T_1 and PU, and between T_2 and PU are the same, and hence the average transmit power of T_1 and T_2 is almost the same. For the nodes T_1 and T_2, we see that there exist positions of PB and PU at which their average transmit power is lowest. However, the average transmit power of T_0 always decreases as x_B increases.

Figure 4 presents the end-to-end SOP as a function of P_S with different number of antennas at E. In this simulation, the total hardware impairment levels of the data and eavesdropping links are given as $\kappa_D^2 = 0.01$ and $\kappa_E^2 = 0$, respectively, and hence the conditions in Lemma 1 are satisfied, i.e., $\alpha_0 > 0$ and $\alpha_{3,v} > 0$. It can be seen from this figure that simulation results match very well with theoretical ones. Moreover, we see that the exact end-to-end SOP converges to the approximate one at high P_S values, which verifies the derived expressions obtained in Lemma 1 and Corollary 1. As proved in Corollary 1, the end-to-end SOP at high P_S regime increases with the increasing of P_S. In addition, Figure 4 shows that there exists an optimal value of P_S at which the SOP value is lowest. Finally, we can see that the secrecy performance of the proposed protocol is worse with higher number of antennas at E.

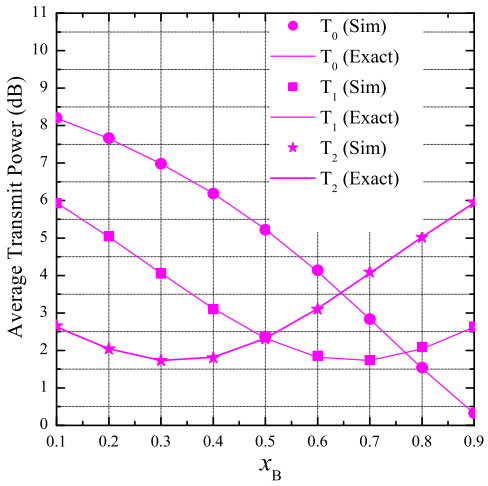

Figure 3. Average transmit power of the secondary transmitters as a function of x_B when $P_S = 10$ dB, $K = 3$, $N_D = 3$, $\varepsilon = 0.25$, $\eta = 0.25$, $y_B = 0.3$, $x_P = 1 - x_B$, and $y_P = -0.5$.

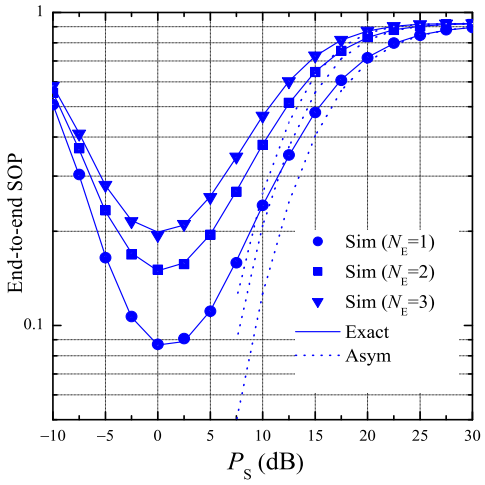

Figure 4. End-to-end secrecy outage probability as a function of P_S when $K = 3$, $N_D = 2$, $\varepsilon = 0.25$, $\eta = 0.25$, $C_{th} = 0.2$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, $y_E = 0.5$, $\kappa_D^2 = 0.01$, and $\kappa_E^2 = 0$.

In Figure 5, we present the end-to-end SOP as a function of P_S with various number of hops (K). In this figure, we assume that the transceiver hardware of the authorized nodes is better than that of the eavesdropper, i.e., $\kappa_D^2 = 0$ and $\kappa_E^2 = 0.01$, which satisfy the conditions in Lemma 2, i.e., $\alpha_0 > 0$ and $\alpha_{3,v} < 0$. It is seen from Figure 5 that the end-to-end SOP rapidly decreases as P_S increases. Moreover, the secrecy performance significantly enhances with higher number of hops. Finally, the simulation results again validate the theoretical results obtained from Lemma 2 and Corollary 2.

In Figure 6, we consider the cases where $\alpha_{3,v} = 0$ or $(\rho - 1)\kappa_D^2\kappa_E^2 + \kappa_D^2\rho - \kappa_E^2 = 0$. As proved in Lemma 3 and Corollary 3, we can see from Figure 6 that the exact end-to-end SOP rapidly converges to the asymptotic one which does not depend on P_S. It is also seen that the hardware impairment levels κ_D^2 and κ_E^2 significantly impact on the secrecy performance. In this figure, the value of SOP is lowest when the transceiver hardware of the authorized nodes and the eavesdropper is perfect, i.e., $\kappa_D^2 = \kappa_E^2 = 0$.

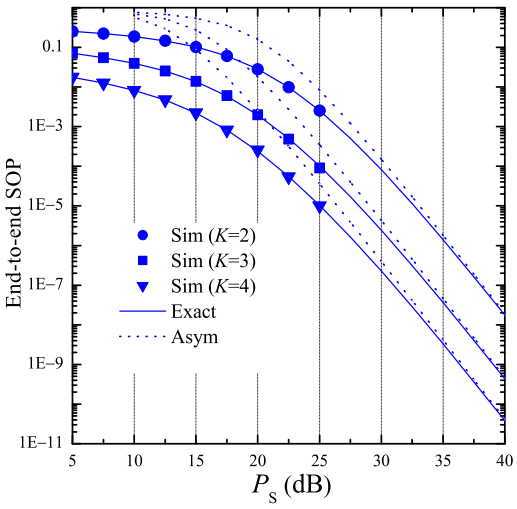

Figure 5. End-to-end secrecy outage probability as a function of P_S when $N_D = 2$, $N_E = 2$, $\varepsilon = 0.25$, $\eta = 0.25$, $C_{th} = 0.2$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, $y_E = 0.5$, $\kappa_D^2 = 0$, and $\kappa_E^2 = 0.01$.

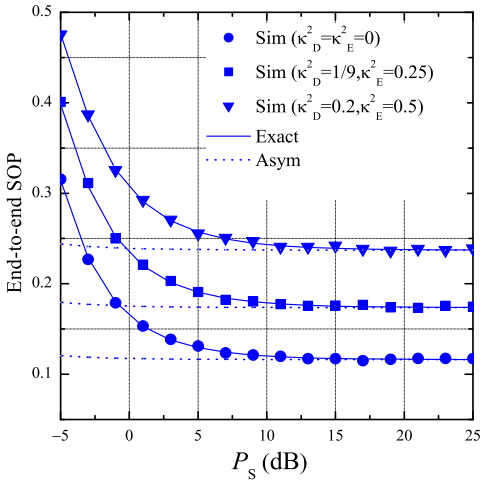

Figure 6. End-to-end secrecy outage probability as a function of P_S when $K = 3$, $N_D = 2$, $N_E = 2$, $\varepsilon = 0.25$, $\eta = 0.25$, $C_{th} = 0.25$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, and $y_E = 0.5$.

Figure 7 presents the SOP performance of the proposed protocol as a function of the fraction of time spent for the EH process (ε). As illustrated in this figure, the end-to-end SOP increases with higher value of ε. Moreover, when ε is very small, the probability $\Pr(P_{k,b} = L_v)$ in (23) $(v \geq 1)$ converges to zero, and hence the end-to-end SOP also goes to zero. Next, similar to Figure 5, the secrecy performance significantly enhances when the hardware impairment level of the data links (κ_D^2) is lower than that of the eavesdropping links (κ_E^2).

In Figure 8, we investigate the impact of the number of hops (K) on the end-to-end SOP. In this simulation, we assume that the number of antennas at the T_k and E nodes is same, i.e., $N_D = N_E$, and the transceiver hardware of these nodes is perfect, i.e., $\kappa_D^2 = \kappa_E^2 = 0$. As we can see, the values of SOP almost decrease as increasing the number of hops. However, in the case that $N_D = N_E = 1$, the end-to-end SOP is highest when the number of hops equals 2. When $K \geq 2$, it is seen that the SOP performance in case that $N_D = N_E = 3$ is best. Moreover, the value of SOP in this case rapidly decreases with the increasing of K.

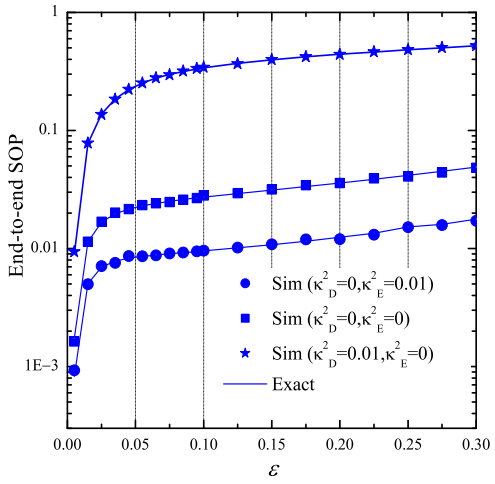

Figure 7. End-to-end secrecy outage probability as a function of ε when $P_S = 10$ dB, $K = 4$, $N_D = 2$, $N_E = 2$, $\eta = 0.1$, $C_{th} = 0.25$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, and $y_E = 0.5$.

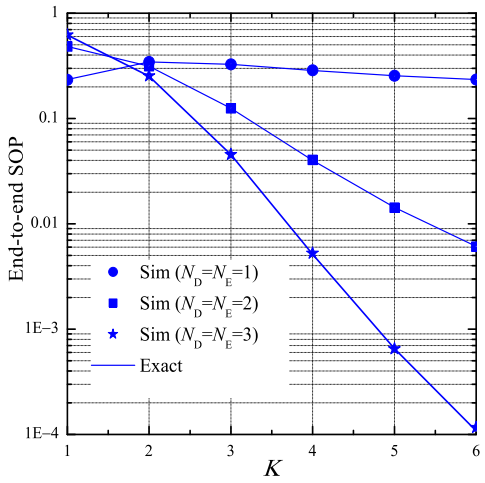

Figure 8. End-to-end secrecy outage probability as a function of K when $P_S = 0$ dB, $\varepsilon = 0.1$, $\eta = 0.1$, $C_{th} = 0.25$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, $y_E = 0.5$, $\kappa_D^2 = 0$, and $\kappa_E^2 = 0$.

In Figure 9, we present the end-to-end PNSC as a function of P_S with various values of κ_D^2 as κ_E^2 is fixed by 0.05. As observed, the PNSC performance is better with the decreasing of κ_D^2. Moreover, as $\kappa_D^2 < \kappa_E^2$ $(\kappa_D^2 > \kappa_E^2)$, the value of PNSC increases (decreases) with higher value of P_S, and in the case that $\kappa_D^2 = \kappa_E^2$, this value does not depend on P_S. It is worth noting that the simulation and theoretical results match very well with each other, which validates the formulas derived in Lemma 4.

Figure 10 presents the end-to-end PNSC as a function of κ_D^2 with different number of hops (K). As shown in this figure, the PNSC performance significantly decreases when the hardware impairment level of the data link increases. Moreover, at high κ_D^2 values, the end-to-end PNSC is worse with high number of hops.

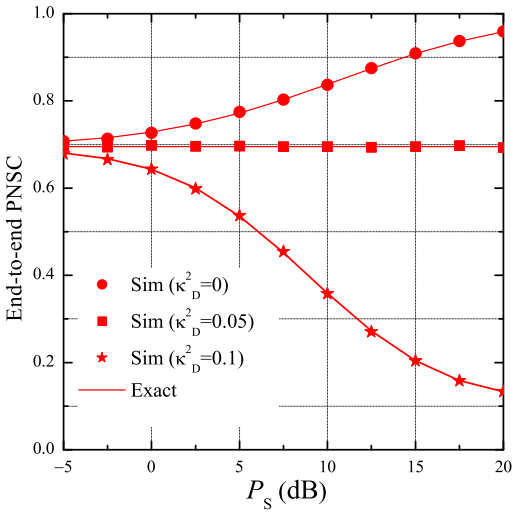

Figure 9. End-to-end probability of non-zero secrecy capacity as a function of P_S when $K = 3$, $\varepsilon = 0.25$, $\eta = 0.25$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, $y_E = 0.5$, $\kappa_E^2 = 0.05$, $N_D = 1$, and $N_E = 2$.

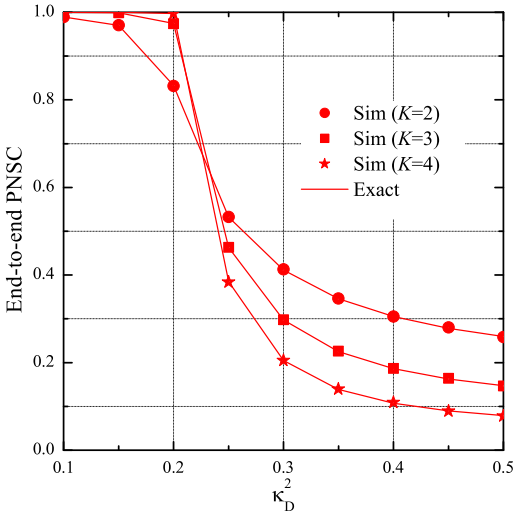

Figure 10. End-to-end probability of non-zero secrecy capacity as a function of κ_D^2 when $K = 3$, $\varepsilon = 0.1$, $\eta = 0.25$, $x_B = 0.5$, $y_B = 0.3$, $x_P = 0.5$, $y_P = -0.5$, $x_E = 0.5$, $y_E = 0.5$, $\kappa_E^2 = 0.2$, $N_D = 2$, and $N_E = 2$.

5. Conclusions

This paper proposed and evaluated the secrecy performance of the TAS/SC-based multi-hop harvest-to-transmit cognitive WSNs under the joint impact of the interference constraint, the limited-energy source, and the hardware impairments. The main contribution of this paper is to derive new exact and asymptotic expressions of the end-to-end SOP and PNSC over Rayleigh fading channel, which can be used to design and optimize the performance of the considered networks, with any hardware impairment levels, as well as other system parameters, in the practical considerations. The interesting results obtained in this paper can be listed as follows:

- The hardware impairments have a significant impact on the secrecy performance. Particularly, when the transceiver hardware of the authorized nodes is better than that of the eavesdropper, the proposed protocol obtains high secrecy performance. Otherwise, the SOP and PNSC performance is significantly degraded.
- The secrecy performance of the proposed protocol can be enhanced with higher number of antennas equipped at the authorized nodes.
- By optimally designing the number of hops and the fraction of time spent for the energy harvesting phase, the secrecy performance of the proposed protocol can be significantly improved.

Author Contributions: The main contributions of P.T.T. (Phu Tran Tin) and P.M.N. were to create the main ideas and execute performance evaluation by extensive simulations, while T.T.D., P.T.T. (Phuong T. Tran) and M.V. worked as the advisers of P.T.T. (Phu Tran Tin) and P.M.N. to discuss, create, and advise the main ideas and performance evaluations together.

Funding: This research received no external funding.

Acknowledgments: This work was supported by the grant SGS reg. No. SP2019/41 conducted at VSB Technical University of Ostrava, Czech Republic, and partially was funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.317.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ledwaba, L.P.I.; Hancke, G.P.; Venter, H.S.; Isaac, S.J. Performance Costs of Software Cryptography in Securing New-Generation Internet of Energy Endpoint Devices. *IEEE Access* **2018**, *6*, 9303–9323. [CrossRef]
2. Liu, Z.; Choo, K.-K.R.; Grossschadl, J. Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography. *IEEE Commun. Mag.* **2018**, *56*, 158–162. [CrossRef]
3. Wyner, A.D. The Wire-tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
4. Csiszar, I.; Korner, J. Broadcast Channels With Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
5. Gopala, P.K.; Lai, L.; Gamal, H.E. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 4687–4698. [CrossRef]
6. Li, Z.; Jing, T.; Ma, L.; Huo, Y.; Qian, J. Worst-Case Cooperative Jamming for Secure Communications in CIoT Networks. *Sensors* **2016**, *16*, 339. [CrossRef] [PubMed]
7. Tang, X.; Cai, Y.; Yang, W.; Yang, W.; Chen, D.; Hu, J. Secure Transmission of Cooperative Zero-Forcing Jamming for Two-User SWIPT Sensor Networks. *Sensors* **2018**, *18*, 331. [CrossRef]
8. Yang, M.; Zhang, B.; Huang, Y.; Yang, N.; Guo, D.; Gao, B. Secure Multiuser Communications in Wireless Sensor Networks with TAS and Cooperative Jamming. *Sensors* **2016**, *16*, 1908. [CrossRef]
9. Yang, N.; Yeoh, P.L.; Elkashlan, M.; Schober, R.; Collings, I.B. Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels. *IEEE Trans. Commun.* **2013**, *61*, 144–154. [CrossRef]
10. Xiong, J.; Tang, Y.; Ma, D.; Xiao, P.; Wong, K.-K. Secrecy Performance Analysis for TAS-MRC System with Imperfect Feedback. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1617–1629. [CrossRef]
11. Krikidis, I. Opportunistic Relay Selection For Cooperative Networks with Secrecy Constraints. *IET Commun.* **2010**, *4*, 1787–1791. [CrossRef]
12. Liu, Y.; Wang, L.; Tran, T.D.; Elkashlan, M.; Duong, T.Q. Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 46–49. [CrossRef]
13. Duy, T.T.; Duong, T.Q.; Thanh, T.L.; Bao, V.N.Q. Secrecy Performance Analysis with Relay Selection Methods under Impact of Co-channel Interference. *IET Commun.* **2015**, *9*, 1427–1435. [CrossRef]
14. Zhong, B.; Zhang, Z. Secure Full-Duplex Two-Way Relaying Networks With Optimal Relay Selection. *IEEE Commun. Lett.* **2017**, *21*, 1123–1126. [CrossRef]
15. Kuhestani, A.; Mohammadi, A.; Mohammadi, M. Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems With Untrusted Relays and Passive Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 341–355. [CrossRef]
16. Mo, J.; Tao, M.; Liu, Y. Relay Placement for Physical Layer Security: A Secure Connection Perspective. *IEEE Commun. Lett.* **2012**, *16*, 878–881.

17. Hu, L.; Wen, H.; Wu, B.; Pan, F.; Liao, R.-F.; Song, H.; Tang, J.; Wang, X. Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 219–228. [CrossRef]
18. Ma, H.; Cheng, J.; Wang X.; Ma, P. Robust MISO Beamforming with Cooperative Jamming for Secure Transmission From Perspectives of QoS and Secrecy Rate. *IEEE Trans. Commun.* **2018**, *66*, 767–780. [CrossRef]
19. Zhang, G.; Xu, J.; Wu, Q.; Cui, M.; Li X.; Lin, F. Wireless Powered Cooperative Jamming for Secure OFDM System. *IEEE Trans. Veh. Technol.* **2018**, *67*, 1331–1346. [CrossRef]
20. Zhou, X.; Zhang, R.; Ho, C.-K. Wireless information and power transfer: Architecture design and rate-energy tradeoff. *IEEE Trans. Commun.* **2013**, *61*, 4754–4767. [CrossRef]
21. Nasir, A.A.; Zhou, X.; Durrani, S.; Kennedy, R.A. Relaying protocols for wireless energy harvesting and information processing. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 3622–3636. [CrossRef]
22. Atapattu, S.; Evans, J. Optimal Energy Harvesting Protocols for Wireless Relay Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5789–5803. [CrossRef]
23. Xu, C.; Zheng, M.; Liang, W.; Yu, H.; Liang, Y.-C. Outage Performance of Underlay Multihop Cognitive Relay Networks with Energy Harvesting. *IEEE Commun. Lett.* **2016**, *20*, 1148–1151. [CrossRef]
24. Xu, C.; Zheng, M.; Liang, W.; Yu, H.; Liang, Y.-C. End-to-end Throughput Maximization for Underlay Multi-hop Cognitive Radio Networks with RF Energy Harvesting. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3561–3572. [CrossRef]
25. Hieu, T.D.; Duy, T.T.; Dung, L.T.; Choi, S.G. Performance Evaluation of Relay Selection Schemes in Beacon-Assisted Dual-hop Cognitive Radio Wireless Sensor Networks under Impact of Hardware Noises. *Sensors* **2018**, *18*, 1843. [CrossRef] [PubMed]
26. Sun, A.; Liang, T.; Li, B. Secrecy Performance Analysis of Cognitive Sensor Radio Networks with an EH-Based Eavesdropper. *Sensors* **2017**, *17*, 1026. [CrossRef] [PubMed]
27. Hieu, T.D.; Duy, T.T.; Kim, B.-S. Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs with Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises. *IEEE Sens. J.* **2018**, *18*, 5173–5186. [CrossRef]
28. Mokhtar, M.; Gomaa, A.; Al-Dhahir, N. OFDM AF relaying under I/Q imbalance: Performance analysis and baseband compensation. *IEEE Trans. Commun.* **2013**, *61*, 1304–1313. [CrossRef]
29. Björnson, E.; Matthaiou, M.; Debbah, M. A new look at dual-hop relaying: Performance limits with hardware impairments. *IEEE Trans. Commun.* **2013**, *61*, 4512–4525. [CrossRef]
30. Solanki, S.; Upadhyay, P.K.; da Costa, D.B.; Bithas, P.S.; Kanatas, A.G.; Dias, U.S. Joint Impact of RF Hardware Impairments and Channel Estimation Errors in Spectrum Sharing Multiple-Relay Networks. *IEEE Trans. Commun.* **2018**, *66*, 3809–3824. [CrossRef]
31. Boulogeorgos, A.A.; Karas, D.S.; Karagiannidis, G.K. How much does I/Q Imbalance affect secrecy capacity? *IEEE Commun. Lett.* **2016**, *20*, 1305–1308. [CrossRef]
32. Zhu, J.; Ng, D.W.K.; Wang, N.; Schober, R.; Bhargava, V.K. Analysis and Design of Secure Massive MIMO Systems in the Presence of Hardware Impairments. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2001–2016. [CrossRef]
33. Lee, J.-H. Full-Duplex Relay for Enhancing Physical Layer Security in Multi-Hop Relaying Systems. *IEEE Commun. Lett.* **2015**, *19*, 525–528. [CrossRef]
34. Lee, J.-H.; Sohn, I.; Kim, Y.-H. Transmit Power Allocation for Physical Layer Security in Cooperative Multi-Hop Full-Duplex Relay Networks. *Sensors* **2016**, *16*, 1726. [CrossRef] [PubMed]
35. Tian, F.; Chen, X.; Liu, S.; Yuan, X.; Li, D.; Zhang, X.; Yang, Z. Secrecy Rate Optimization in Wireless Multi-Hop Full Duplex Networks. *IEEE Access* **2018**, *6*, 5695–5704. [CrossRef]
36. Alotaibi, E.R.; Hamdi, K.A. Secure Relaying in Multihop Communication Systems. *IEEE Commun. Lett.* **2016**, *20*, 1120–1123. [CrossRef]
37. Tin, P.T.; Hung, D.T.; Duy, T.T.; Voznak, M. Analysis of Probability of Non-zero Secrecy Capacity for Multi-hop Networks in Presence of Hardware Impairments over Nakagami-m Fading Channels. *Radio Eng.* **2016**, *25*, 774–782.
38. Yao, J.; Liu, Y. Secrecy Rate Maximization with Outage Constraint in Multihop Relaying Networks. *IEEE Commun. Lett.* **2018**, *22*, 304–307. [CrossRef]
39. Qi, X.; Huang, K.; Zhong, Z.; Kang, X.; Zhong, Z. Physical layer security of multi-hop aided downlink MIMO heterogeneous cellular networks. *Chin. Commun.* **2016**, *13*, 120–130. [CrossRef]

40. Lee, J.-H. Confidential Multicasting Assisted by Multi-Hop Multi-Antenna DF Relays in the Presence of Multiple Eavesdroppers. *IEEE Trans. Commun.* **2016**, *64*, 4295–4304. [CrossRef]
41. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
42. Bao, V.N.Q.; Trung, N.L.; Debbah, M. Relay selection scheme for dual-hop networks under security constraints with multiple eavesdroppers. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 6076–6085. [CrossRef]
43. Vo, V.N.; Tran, D.-D.; Chakchai, S.-I.; Tran, H. Secrecy Performance Analysis for Fixed-Gain Energy Harvesting in an Internet of Things with Untrusted Relays. *IEEE Access* **2018**, *6*, 48247–48258.
44. Huang, Y.; Zhang, P.; Wu, Q.; Wang, J. Secrecy Performance of Wireless Powered Communication Networks with Multiple Eavesdroppers and Outdated CSI. *IEEE Access.* **2018**, *6*, 33774–33788. [CrossRef]
45. Lee, K.; Choi, H.-H. Secure Analog Network Coding with Wireless Energy Harvesting under Multiple Eavesdroppers. *IEEE Access.* **2018**, *6*, 76289–76301. [CrossRef]
46. Laneman, J.N.; Tse, D.N.; Wornell, G.W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Trans. Inf. Theory* **2004**, *50*, 3062–3080. [CrossRef]
47. Matthaiou, M.; Papadogiannis, A. Two-way relaying under the presence of relay transceiver hardware impairments. *IEEE Commun. Lett.* **2013**, *17*, 1136–1139. [CrossRef]
48. Duy, T.T.; Duong, Q.T.; da Costa, D.B.; Bao, V.N.Q.; Elkashlan M. Proactive Relay Selection with Joint Impact of Hardware Impairment and Co-channel Interference. *IEEE Trans. Commun.* **2015**, *63*, 1594–1606. [CrossRef]
49. Sharma, P.K.; Upadhyay, P.K. Cognitive relaying with transceiver hardware impairments under interference constraints. *IEEE Commun. Lett.* **2016**, *20*, 820–823. [CrossRef]

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).