sensors

MDPI

Article

Exploiting Opportunistic Scheduling Schemes and WPT-Based Multi-Hop Transmissions to Improve Physical Layer Security in Wireless Sensor Networks †

Kyusung Shim [1], Toan-Van Nguyen [1] and Beongku An [2,*]

[1] Department of Electronics and Computer Engineering, Hongik University, Sejong City 30016, Korea; shimkyusung@outlook.kr (K.S.); vannguyentoan@gmail.com (T.-V.N.)

[2] Department of Software and Communications Engineering, Hongik University, Sejong City 30016, Korea

* Correspondence: beongku@hongik.ac.kr; Tel.: +82-44-860-2243

† This paper is an extended version of our paper published in Shim, K.; Nguyen, T.-V.; An, B. Secrecy Improvement for Wireless-Powered Multihop D2D Communication in Wireless Sensors Networks. In Proceedings of the 7th International Conference on Green and Human Information Technology (ICGHIT 2019), Kuala Lumpur, Malaysia, 16–18 January 2019; pp. 209–214.

Received: 26 November 2019; Accepted: 9 December 2019; Published: 11 December 2019

Abstract: This paper studies the secrecy performance of wireless power transfer (WPT)-based multi-hop transmissions in wireless sensors networks (WSNs), where legitimate nodes harvest energy from multiple power beacons (PBs) to support the multi-hop secure data transmission to a destination in the presence of an eavesdropper. Specifically, the PBs not only transfer radio frequency energy to the legitimate nodes but also act as friendly jammers to protect data transmission. To improve secrecy performance, we propose two secure scheduling schemes, named minimum node selection (MNS) scheme and optimal node selection (ONS) scheme. We then evaluate the performance of the proposed schemes in terms of the exact closed-form for secrecy outage probability (SOP) and asymptotic SOP. The developed analyses are verified by Monte-Carlo simulations. The numerical results show that the ONS scheme outperforms the MNS scheme emerging as an effective protocol for secure multi-hop transmission in WSNs. Furthermore, the effects of the number of PBs, number of hops, time switching ratio, and the secure target data rate on the system performance are also investigated.

Keywords: artificial noise; multi-hop transmission; opportunistic scheduling; physical layer security; secrecy outage probability; wireless sensor networks

1. Introduction

Wireless sensor networks (WSNs) has been emerged as a networking solution for future wireless networks supporting Internet-of-thing (IoT) ecosystems [1,2]. In practice, WSNs are deployed in the battlefield or hazardous environments to allow collecting and monitoring the physical phenomena without human interaction [3,4]. However, one of the most challenges faced by traditional WSNs is how to maintain the network lifetime since the sensor nodes are low cost, small size, and have limited power supply [5]. Moreover, energy for encoding and protecting information against eavesdropping is also raising a significant burden on the traditional WSNs and IoT systems. Wireless power transfer (WPT) is a sustainable energy solution to efficiently solve such a problem in WSNs since each sensor node can harvest energy from multiple power beacons (PBs) to maintain their operation [6–8]. Specifically, the authors in [9] introduced the time-switching-based relaying (TSR) and power splitting-based relaying (PSR) architectures to allow energy harvesting and information processing at a battery-less relay node, which enables a wide range of attractive applications with stringent quality of services in future IoT systems and WSNs. Recently, the researches on energy harvesting address the harvesting energy from the light-emitting diode (LED) as well as the radio frequency (RF) in indoor IoT systems [10].

Multi-hop transmission has been identified as an effective technique to extend the networks coverage in WSNs by leveraging information transmission from a source node to a destination node via multiple intermediate sensor nodes. However, the broadcast of the wireless signals in multi-hop transmissions is easily wiretapped by illegitimate users [11]. Physical layer security (PLS) is one of the most effective approaches to protect the information against eavesdroppers by exploiting physical characteristics of wireless channels [12]. Moreover, the PLS concept can be naturally applied to the WPT-based multi-hop transmission in WSNs, where the PBs not only radiate RF signals to power to the sensor nodes but also generate artificial noise to degrade the eavesdropping channels. The secrecy outage probability (SOP) is one of the system metrics to evaluate secure performance, and is defined as the probability that the difference between capacity of the main channel and that of the eavesdropper channel falls below a predefined secrecy target data rate [13,14]. Additionally, perfect secure transmission is achieved when the channel state information (CSI) of the main channel is higher than that of the eavesdropper channel [15].

1.1. Related Works and Motivations

In this subsection, we discuss the most recent works for the PLS and WPT-based enabling multi-hop transmission in WSNs. Do et al. in [16] proposed the relay selection schemes to enhance the system performance under independent and non-identical distribution (i.n.i.d.) fading channel. The paper also proposed the PSR mechanism for relays to harvest energy from the source RF radiation. The authors in [17] proposed two antenna selection schemes by using the CSI to improve secrecy performance in underlay cognitive radio network. Additionally, the secondary transmitter can harvest energy from the primary transmitter's signal to transmit the message to a secondary receiver. In [18], the authors considered the cooperative relaying system, where the relay is equipped with TSR architecture to support data transmission from a source and a destination with maximal ratio combining (MRC) technique. In [19], the authors considered the wireless energy harvesting (EH) multi-hop cluster-based networks, where the destination in the considered networks is equipped with multiple antenna and proposed relay selection schemes to enhance the system performance. In our previous work [20], we proposed the WPT-based multi-hop transmission model in the presence of an eavesdropper. More specifically, the power beacons radiated the jamming signal during the data transmission phase to reduce the eavesdropper's CSI. However, reference [20] did not consider cluster networks.

The authors in [21] considered multi-hop transmission under multiple eavesdroppers over Nakagami-m fading channel. However, the authors did not consider node selection to enhance secrecy performance in the considered model. The author in [22] studied the secrecy performance in multi-hop relaying systems, where the relays worked on full-duplex mode. However, this work had some limitations that the full-duplex relay could cancel the self-interference, and the author did not consider any technique to enhance the secrecy performance on the considered system similar to [21]. The authors in [23] exploited the secrecy performance in multi-hop transmission under the underlay cognitive radio networks. The authors addressed that the CSI of interference link is imperfect. Interestingly, in the case of one primary user, the imperfect CSI did not affect the secrecy performance. From the aforementioned works [21–23], the multi-hop transmission shows that the system secrecy performance decreases when the number of hops increases.

In order to enhance the secrecy performance in multi-hop transmission, some authors have addressed the opportunistic scheduling in multi-hop transmission systems. The authors in [24] proposed opportunistic scheduling scheme in cluster networks to improve the secrecy performance. The nodes were selected to improve the main channel performance. Additionally, the eavesdropper employed the MRC technique to enhance wiretapping performance. Recently, the authors in [25] addressed the path-selection method to enhance the secrecy performance in multi-hop transmission for wireless sensor networks. Additionally, the authors exploited the impact of hardware impairment in secrecy performance. In [26], the authors exploited the cooperative multi-hop transmission protocol in underlay cognitive radio networks. The authors considered hardware impairments for a more practical scenario. However, the authors did not propose any technique to improve the system secrecy performance. From the numerical results, in spite of node/path selection schemes, the considered system achieves very low secrecy performance. The PLS is addressed in multi-hop transmission in [23–26]. Thus, future research needs to consider not only opportunistic scheduling scheme but also some techniques to enhance the secrecy performance in multi-hop scenarios.

The aforementioned works [16,18–20] mainly focused on EH-based multi-hop transmission or [21–26] considered multi-hop secure transmission, which is not feasible in practice. In practical WSNs, because of the limited antenna performance of sensor nodes and deep shadowing, the direct link between source node and destination node is not available. The sensor nodes cooperate with other sensor nodes in order to overcome the channel attenuation between the source node and destination node. However, different from the legitimate users transmission, the eavesdropper overhears the legitimate users transmission in the vicinity. Thus, in the WSNs, sensor nodes are densely deployed and grouped into clusters as well as the existing wiretapping attacks. The study of PLS in WPT-based multi-hop transmissions is necessary for WSNs. Additionally, from [23–26], the multi-hop transmissions show low secrecy performance when the number of hops is increased. Thus, the PLS in WPT-based multi-hop transmissions plays a vital role in the future WSNs and IoT systems.

1.2. Contributions and Organization

In this paper, we study the effects of node selection on the performance of WPT-based multi-hop transmissions in WSNs. Specifically, we propose two node selection schemes to improve the secrecy performance, named the minimum node selection (MNS) scheme and optimal node selection (ONS) scheme. In particular, the MNS scheme selects the sensor node in each cluster based on the minimization of the eavesdropper channel capacity, while the ONS scheme tries to choose the best sensor node that maximizes the secrecy capacity in each hop transmission. Furthermore, the power beacons are deployed to not only charge the sensor nodes in energy harvesting phase but also generate the jamming signal to confuse the eavesdropper in data transmission phase. By employing the randomize-and-forward strategy [27,28], the considered cooperative relaying prevents the eavesdropper from combining the wiretapped information during the data transmission phase. The main contributions of this paper can be summarized as follows:

- We deploy an effective secure model for WPT-based multi-hop transmission to improve the energy capability of sensor nodes and reduce the decoding ability of eavesdropper in WSNs. Specifically, the dedicated RF signal for powering sensor nodes can be used to interfere the wiretapping channels. The considered WPT-based multi-hop transmission has been reported in this literature.
- We propose two scheduling schemes to improve the secrecy performance in WSNs. We then derive the new exact closed-form expressions for the SOP of the proposed schemes. The asymptotic analyses of the SOP are further provided to show some insight information into the considered system. The analytical results are verified by Monte-Carlo simulations confirming the correctness of our analysis.
- We show through the numerical results that the ONS scheme provides the best secrecy performance among the proposed schemes. Additionally, the effects of the number of sensor nodes, the number of PBs, and time switching ratio on the secrecy performance are also evaluated and discussed.

The rest of the paper is organized as follows. Section 2 describes the system model. Section 3 analyzes the exact closed-form expression for SOP of the proposed schemes. Section 4 presents the numerical results based on the derived analytical results. Finally, the paper is concluded in Section 5.

2. System Model

2.1. System Description and Channel Modeling

Let us consider a WPT-based multi-hop transmission in wireless sensor networks, as depicted in Figure 1, where a desired source in the first cluster transmits its information to a destination with the help of intermediate nodes located in K-1 cluster, with $K > 1$, while an eavesdropper overhears the signals transmitted by the source and relays. In this paper, we assume that sources and intermediate nodes have a limited power supply; thus, they must harvest energy from RF signal radiated by a set of M power beacons, i.e., $\mathcal{P} = \{\mathrm{PB}_m \mid m = 1, 2, ..., M\}$. We assume that the power beacons have the same structure and transmit the power at the same level, i.e., $P_m = P$ [19]. Moreover, all sensor nodes are equipped with a single antenna and operated in half-duplex mode. We further assume that the direct link from the source node to the destination node is not available due to the limited radio range of each sensor node and deep shadowing [19,25,29].

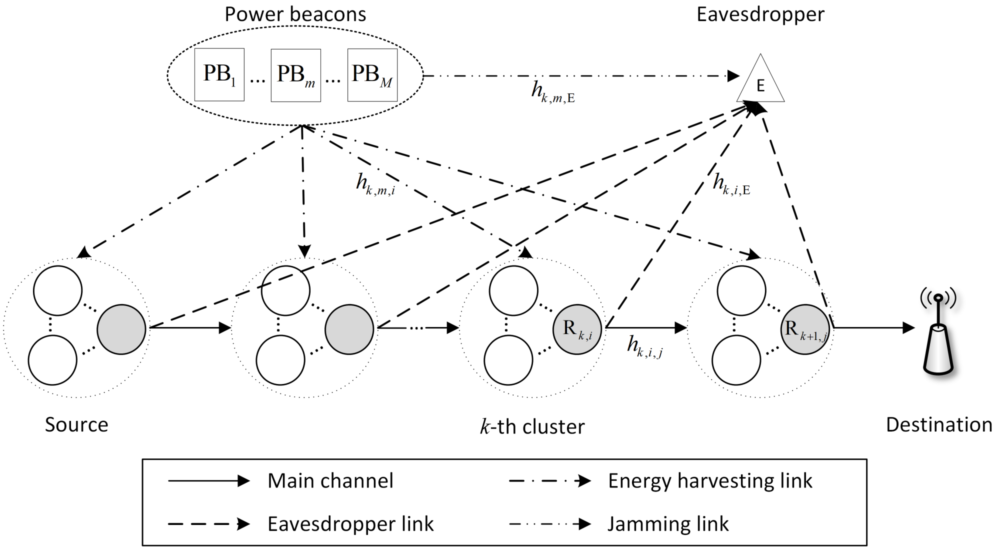


Figure 1. Illustration of the proposed multi-hop transmissions in wireless sensor network.

The main notations used in this paper are summarized in Table 1. Moreover, we assume that all channels exhibit flat and block Rayleigh fading. Let u_{XY} be the channel coefficient from X to Y, where $\mathrm{X} \in \{\mathrm{S}_i, \mathrm{R}_{k,i}, \mathrm{PB}_m\}$ and $\mathrm{Y} \in \{\mathrm{S}_i, \mathrm{R}_{k,i}, \mathrm{D}, \mathrm{E}\}$ with $\mathrm{X} \neq \mathrm{Y}$. Thus, the channel gain $|u_{\mathrm{XY}}|^2$ follows the exponential distribution whose cumulative distribution function (CDF), $F_{|u_{\mathrm{XY}}|^2}(u) = 1 - \exp(-\frac{u}{\lambda_{\mathrm{XY}}})$, and probability density function (PDF), $f_{|u_{\mathrm{XY}}|^2}(u) = \frac{1}{\lambda_{\mathrm{XY}}} \exp(-\frac{u}{\lambda_{\mathrm{XY}}})$, respectively, where λ_{XY} indicates the mean of $|u_{\mathrm{XY}}|^2$ and can be expressed as $\lambda_{\mathrm{XY}} = (d_{\mathrm{XY}}/d_0)^{-\epsilon}$, where d_{XY} presents the Euclidean distance between X and Y, d_0 and ϵ denote the reference distance and path-loss exponent, respectively.

The operation of the considered system can be divided into two consecutive phases including energy harvesting and data transmission which are presented in the next subsection. Additionally, the aims of the power beacons in each phase, called energy harvesting and data transmission phase, can be summarized as follows:

- Energy harvesting phase: According to wireless power transfer technique [9], the power beacons support the sensor nodes to harvest energy. Thus, in the energy harvesting phase, sensor nodes can harvest energy from the power beacons.
- Data transmission phase: In multi-hop transmission, sensor nodes transmit information by consuming the harvested energy. Thus, the eavesdropper can overhear the legitimate user's information. In order to enhance the secrecy performance, the power beacons radiate the jamming signal to degrade the received signal-to-noise ratio (SNR) of the eavesdropper.

Table 1. Summary of main notations.

Symbol	Definition
PB_m	Power beacons m with $m \in \{1, 2, ..., M\}$.
S_i	Source node in the first cluster, where $i \in \{1, ..., N_0\}$.
D	Destination node.
N_k	The number of relay in the k-th cluster, $k \in$ {0,1,..., K-1} and $N_k \geq 1$.
$\mathsf{R}_{k,i}$	The i-th sensor node in the k-th cluster., $\mathsf{R}_{0,i} \equiv \mathsf{S}_i$ and $\mathsf{R}_{K,1} \equiv \mathsf{D}$ with $k \in \{0, ..., K\}$.
E	The eavesdropper node.
$\lvert h_{k,m,i}\rvert^2$	The channel gain of link $\mathsf{PB}_m \to \mathsf{R}_{k-1,i}$.
$\lvert h_{k,m,\mathsf{E}}\rvert^2$	The channel gain of link $\mathsf{PB}_m \to \mathsf{E}$.
$\lvert h_{k,i,j}\rvert^2$	The channel gain of link $\mathsf{R}_{k-1,i} \to \mathsf{R}_{k,j}$.
$\lvert h_{k,i,\mathsf{E}}\rvert^2$	The channel gain of link $\mathsf{R}_{k-1,i} \to \mathsf{E}$.
$\lambda_{k,m,i}$, $\lambda_{k,i,j}$, $\lambda_{k,i,\mathsf{E}}$ and $\lambda_{k,m,\mathsf{E}}$	Mean of $\lvert h_{k,m,i}\rvert^2$, $\lvert h_{k,i,j}\rvert^2$, $\lvert h_{k,i,\mathsf{E}}\rvert^2$ and $\lvert h_{k,m,\mathsf{E}}\rvert^2$, respectively.
α with $\alpha \in [0,1]$	Time switching ratio.
η with $\eta \in (0,1)$	The energy conversion efficiency.

2.2. Energy Harvesting Phase

Figure 2 illustrates the time block structure of the considered system employing time switching architecture [9], where all sensor nodes simultaneously harvest energy from the M PBs in duration of αT while the data transmissions is taken place in K orthogonal sub-time slots. The harvested energy at $\mathsf{R}_{k,i}$ can be expressed as

$$E_{k,i} = \sum_{m=1}^{M} \eta \alpha T P \lvert h_{k,m,i}\rvert^2. \tag{1}$$

Therefore, the average transmit power of $\mathsf{R}_{k,i}$ in a sub-time slot can be calculated as

$$\begin{aligned} P_{k,i} &= \frac{E_{k,i}}{(1-\alpha)T/K} \\ &= \sum_{m=1}^{M} \frac{K\eta\alpha P \lvert h_{m,k,i}\rvert^2}{1-\alpha}. \end{aligned} \tag{2}$$

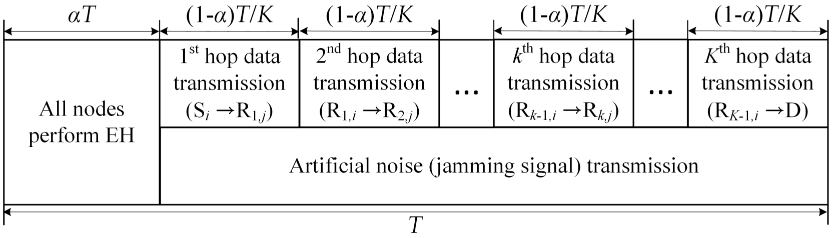

αT
(1-α)T/K
(1-α)T/K
(1-α)T/K
(1-α)T/K
All nodes perform EH
1st hop data transmission (S$_i$ →R$_{1,j}$)
2nd hop data transmission (R$_{1,i}$ →R$_{2,j}$)
...
kth hop data transmission (R$_{k-1,i}$ →R$_{k,j}$)
...
Kth hop data transmission (R$_{K-1,i}$ →D)
Artificial noise (jamming signal) transmission
T

Figure 2. The transmission time block structure of the wireless power transfer (WPT)-based multi-hop transmissions in wireless sensor network for energy harvesting and data transmission.

2.3. Data Transmission Phase

In this phase, the source nodes transmit their data to the destination node via multiple intermediate sensor nodes while the power beacons generate the artificial noise to degrade the wiretapping channel of the eavesdropper. More specifically, as can be seen in Figure 2, k-th hop data transmission slot indicates that the transmission between a sensor node, called i node in (k-1)-th relay cluster, and an other sensor node, named j node in k-th relay cluster. Because each sensor node equips with half-duplex mode, in k-th time slot, the received sensor node in k-th relay cluster can transmit its message to an other sensor node in the next transmission slot. Simultaneously, the power beacon radiates the jamming signal as a role of friendly jammer in data transmission phase. We assume that each legitimate user and PBs cooperate such that the jamming signal can be nulled out at legitimate users [30,31]. Thus, the received signal at $\mathsf{R}_{k+1,j}$ can be expressed as

$$y_{k,i,j} = \sqrt{P_{k,i}} h_{k,i,j} x_{k,i} + n_j, \tag{3}$$

where the $h_{k,i,j}$ denotes the channel coefficients of $\mathsf{R}_{k,i} \rightarrow \mathsf{R}_{k+1,j}$ link and n_j presents the additive white Gaussian noise (AWGN) at $\mathsf{R}_{k+1,j}$ with zero mean and variance $\sigma^2_{\mathsf{R}_{k+1,j}}$. Without loss of generality, we assume that the each node has the same variance of noise, i.e., $\sigma^2_{\mathsf{R}_{k+1,j}} = \sigma^2$. The instantaneous SNR of the main channel at k hop can be expressed as

$$\gamma_{k,i,j} = \frac{P_{k,i} |h_{k,i,j}|^2}{\sigma^2}. \tag{4}$$

Meanwhile, the eavesdropper can overhear the information from the legitimate users due to the nature broadcast of the wireless signals. Thus, the wiretapped signals in k-th hop transmission at E can be expressed as

$$y_{k,i,\mathsf{E}} = \sqrt{P_{k,i}} h_{k,i,\mathsf{E}} x_{k,i} + \sum_{m=1}^{M} \sqrt{P} h_{k,m,\mathsf{E}} s_m + n_{\mathsf{E}}. \tag{5}$$

Since the power beacons generate the jamming signals to degrade the decoding ability of the eavesdropper. Thus, the instantaneous signal-to-interference-plus-noise ratio (SINR) of k-th hop at E can be expressed as

$$\gamma_{k,i,\mathsf{E}} = \frac{P_{k,i} |h_{k,i,\mathsf{E}}|^2}{\sum_{m=1}^{M} P |h_{k,m,\mathsf{E}}|^2 + \sigma^2}. \tag{6}$$

In order to facilitate the analysis and highlight the secure performance under different opportunistic scheduling schemes, we assume that the perfect CSI is available at all receivers [24–26,32,33] (In [34], the authors proposed the method of the eavesdropper channel estimation without eavesdropper feedback. The other legitimate users, called torch nodes, feedback their channel information instead of the eavesdropper. Since we mainly focus on the impact of the node selection schemes in the considered SOP performance of WPT-based multi-hop transmission. The study of imperfect CSI of eavesdropper link in our system model is indeed an interesting topic and will be considered in our future works).

2.4. Opportunistic Scheduling Scheme

In this subsection, we explain the proposed opportunistic scheduling schemes for multi-hop transmission in WSNs. In order to analyze the impacts of scheduling schemes on the secure performance, we assume that various techniques, e.g., clustering protocols [35,36], eavesdropper channel estimation [34], distributed coordination function (DCF) in IEEE 802.11 [37,38], etc., perfectly support the proposed node selection schemes as in [24,26,32,33].

2.4.1. Random Node Selection Scheme

We consider the random node selection scheme as a baseline scheme for comparison purpose. In particular, the RNS scheme randomly selects a relay in each cluster for multi-hop transmission [19]. Thus, the instantaneous SNRs of main channel and eavesdropper channel can be expressed, respectively, as

$$\gamma^{\mathsf{RNS}}_{k,i^*,j^*} = \frac{P_{k,i} |h_{k,i,j}|^2}{\sigma^2}, \tag{7}$$

$$\gamma^{\mathsf{RNS}}_{k,i^*,\mathsf{E}} = \frac{P_{k,i} |h_{k,i,\mathsf{E}}|^2}{\sum_{m=1}^{M} P |h_{k,m,\mathsf{E}}|^2 + \sigma^2}. \tag{8}$$

2.4.2. Minimum Node Selection Scheme

In MNS scheme, the selected node is the least vulnerable node among the nodes in each cluster, which minimizes the channel capacity of eavesdropper channel in each cluster. Thus, MNS scheme can be mathematically described as

$$\mathrm{R}_{k,i^*}^{\mathsf{MNS}} = \arg\min_{i\in N_k} \left\{ \log_2(1+\gamma_{k,i,\mathsf{E}}) \right\}. \tag{9}$$

The instantaneous SNRs of main channel and eavesdropper channel can be expressed, respectively, as

$$\gamma_{k,i^*,j^*}^{\mathsf{MNS}} = \frac{P_{k,i^*}|h_{k,i^*,j^*}|^2}{\sigma^2}, \tag{10}$$

$$\gamma_{k,i^*,\mathsf{E}}^{\mathsf{MNS}} = \arg\min_{i\in N_k} \left\{ \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sum_{m=1}^{M} P|h_{k,m,\mathsf{E}}|^2+\sigma^2} \right\}. \tag{11}$$

where P_{k,i^*} and $|h_{k,i^*,j^*}|^2$ indicate the average transmit power and channel gain of the selected sensor node in k-th cluster through the MNS scheme, respectively.

2.4.3. Optimal Node Selection Scheme

In this scheme, the main and eavesdropper channels are jointly considered, thus, ONS scheme can achieve the most robust performance [33,39]. Since the ONS scheme utilizes both the main and eavesdropper channel to enhance secrecy performance, the selection criteria can be mathematically described as

$$\mathrm{R}_{k,i^*}^{\mathsf{ONS}} = \arg\max_{i\in N_k} \left\{ \log_2\left(\frac{1+\gamma_{k,i,j^*}}{1+\gamma_{k,i,\mathsf{E}}} \right) \right\}, \tag{12}$$

where j^* indicates the selected node which has already chosen in the previous hop.

3. Outage Performance Analysis

In this section, we analyze the effects of each scheduling scheme on the secrecy performance of the considered system setup. We evaluate the secrecy outage probability which is defined as [23,33,40]

$$P_{out}^{\mathsf{sch}} = \Pr\left(\frac{1-\alpha}{K} \min_{k\in K} \log_2\left(\frac{1+\gamma_{k,i^*,j^*}^{\mathsf{sch}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\mathsf{sch}}} \right) < R_{th}^{\mathsf{sch}} \right), \tag{13}$$

where $\mathsf{sch} \in \{\mathsf{RNS}, \mathsf{MNS}, \mathsf{ONS}\}$ and R_{th}^{sch} (bps/Hz) indicate the secrecy target data rate of each node selection scheme. For the sake of notational convenience, $\kappa \triangleq \frac{K\eta\alpha}{(1-\alpha)}$, $\gamma \triangleq P/\sigma^2$, $X_{k,m,i} \triangleq |h_{k,m,i}|^2$, $Y_{k,i,j} \triangleq |h_{k,i,j}|^2$, $Z_{k,i,\mathsf{E}} \triangleq |h_{k,i,\mathsf{E}}|^2$, $T_{k,m,\mathsf{E}} \triangleq |h_{k,m,\mathsf{E}}|^2$, $W_{k,i} \triangleq \sum_{m=1}^{M} X_{k,m,i}$, and $V_{k,\mathsf{E}} \triangleq \sum_{m=1}^{M} T_{k,m,\mathsf{E}}$, respectively.

3.1. Exact Closed-Form Expression for SOP Analysis

3.1.1. RNS Scheme

Theorem 1. *The exact closed-form expression for the SOP of RNS scheme can be derived as*

$$\begin{aligned} P_{\mathrm{out}}^{\mathsf{RNS}} = 1 - \prod_{k=1}^{K} \Bigg[& \left(\frac{1}{\lambda_{k,m,i}\lambda_{k,m,\mathsf{E}}} \right)^{M} \frac{2}{\Gamma(M)\Gamma(M)} \left(\frac{\lambda_{k,m,i}(\gamma_{th}^{\mathsf{RNS}}-1)}{\kappa\gamma\lambda_{k,i,j}} \right)^{M/2} K_M\left(2\sqrt{\frac{(\gamma_{th}^{\mathsf{RNS}}-1)}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}} \right) \\ & \times \left(\Gamma(M)\lambda_{k,m,\mathsf{E}}^{M} - \frac{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathsf{E}}}{\gamma\lambda_{k,i,j}} \beta_1^{M-1} \exp\left(\frac{\beta_1}{\lambda_{k,m,\mathsf{E}}} \right) \Gamma(M)\Gamma(1-M, \frac{\beta_1}{\lambda_{k,m,\mathsf{E}}}) \right) \Bigg], \end{aligned} \tag{14}$$

where $\gamma_{th}^{\mathsf{RNS}} \triangleq 2^{\frac{KR_{th}^{\mathsf{RNS}}}{(1-\alpha)}}$, $\beta_1 = (\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathsf{E}} + \lambda_{k,i,j})/\,\gamma\lambda_{k,i,j}$, $K_\nu(\cdot)$ *is the modified Bessel function of the second kind with order* ν *([41], eq. 8.342.6),* $\Gamma(z)$ *is the Gamma function ([41], 8.310.1), and* $\Gamma(\alpha, x)$ *is the upper incomplete Gamma function ([41], eq. 8.350.2), respectively.*

Proof. See Appendix A. □

3.1.2. MNS Scheme

Theorem 2. *The exact closed-form expression for the SOP of MNS scheme can be derived as*

$$\begin{aligned} P_{out}^{\mathsf{MNS}} = \quad & 1 - \prod_{k=1}^{K}\left[\left(\tfrac{1}{\lambda_{k,m,i}\lambda_{k,m,\mathsf{E}}}\right)^{M} \tfrac{2}{\Gamma(M)\Gamma(M)} \left(\tfrac{(\gamma_{th}^{\mathsf{MNS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\tfrac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\right. \\ & \left.\times\left[\Gamma(M)\lambda_{k,m,\mathsf{E}}^{M} - \tfrac{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}}}{\gamma N\lambda_{k,i,j}}\beta_2^{M-1}\exp\left(\tfrac{\beta_2}{\lambda_{k,m,\mathsf{E}}}\right)\Gamma(M)\Gamma(1-M, \tfrac{\beta_2}{\lambda_{k,m,\mathsf{E}}})\right]\right], \end{aligned} \tag{15}$$

where $\gamma_{th}^{\mathsf{MNS}} \triangleq 2^{\frac{KR_{th}^{\mathsf{MNS}}}{(1-\alpha)}}$ *and* $\beta_2 = (\ \gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}} + N\lambda_{k,i,j}\ )/\ \gamma N\lambda_{k,i,j}$.

Proof. See Appendix B. □

3.1.3. ONS Scheme

Theorem 3. *The exact closed-form expression for the SOP of ONS scheme can be derived as*

$$\begin{aligned} P_{out}^{\mathsf{ONS}} = 1 - \prod_{k=1}^{K}\Bigg[1 - & \left(\frac{1}{\lambda_{k,m,\mathsf{E}}}\right)^{M}\frac{1}{\Gamma(M)}\sum_{n=0}^{N}\sum_{i=0}^{n}\binom{N}{n}\binom{n}{i}(-1)^{n+i}\left(\frac{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}} + \lambda_{k,i,j}}{\gamma\lambda_{k,i,j}}\right)^{i} \\ & \times\left[\left(\frac{1}{\lambda_{k,m,i}}\right)^{M}\frac{2}{\Gamma(M)}\left(\frac{(\gamma_{th}^{\mathsf{MNS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\right]^{n} \\ & \times\exp\left(\frac{\beta_3}{\lambda_{k,m,\mathsf{E}}}\right)\left(\frac{1}{\lambda_{k,m,\mathsf{E}}}\right)^{-\frac{M-i+1}{2}}\beta_3^{\frac{M-i-1}{2}}\Gamma(M)\exp\left(-\frac{\beta_3}{2\lambda_{k,m,\mathsf{E}}}\right)W_{\frac{-i+1-M}{2},\frac{i-M}{2}}\left(\frac{\beta_3}{\lambda_{k,m,\mathsf{E}}}\right)\Bigg], \end{aligned} \tag{16}$$

where $\gamma_{th}^{\mathsf{ONS}} \triangleq 2^{\frac{KR_{th}^{\mathsf{ONS}}}{(1-\alpha)}}$, $\beta_3 = (\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}} + \lambda_{k,i,j})/\gamma\lambda_{k,i,j}$ *and* $W_{\lambda,\mu}(z)$ *presents the Whittaker function ([41], eq. 9.220.4).*

Proof. See Appendix C. □

3.2. Asymptotic SOP Analysis

In this subsection, we consider the asymptotic expressions of SOP with both schemes in order to insights when $P_m \to \infty$. In order to obtain asymptotic SOP, we apply the following approximation for small z_k as [18]

$$\prod_{k=1}^{K}(1 - z_k) \approx 1 - \sum_{k=1}^{K} z_k. \tag{17}$$

3.2.1. RNS Scheme

Corollary 1. *The asymptotic SOP of RNS scheme can be derived as*

$$P_{Asym}^{\mathsf{RNS}} = \sum_{k=1}^{K}\Delta_{asym}, \tag{18}$$

where

$$\Delta_{asym} = 1 - \left(\frac{1}{\lambda_{k,m,\mathrm{E}}\lambda_{m,k,i}}\right)^{M} \frac{2}{\Gamma(M)} \left(\frac{(\gamma_{th}^{\mathsf{RNS}}-1)\lambda_{m,k,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{(\gamma_{th}^{\mathsf{RNS}}-1)}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right) \times \left[\lambda_{k,m,\mathrm{E}}^{M} - \frac{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}}{\gamma\lambda_{k,i,j}}\beta_1^{M-1}\exp\left(\frac{\beta_1}{\lambda_{k,m,\mathrm{E}}}\right)\Gamma(1-M,\frac{\beta_1}{\lambda_{k,m,\mathrm{E}}})\right]. \tag{19}$$

Proof. From (14), we apply (17), P_{Asym}^{RNS} can be further written as

$$\begin{aligned} P_{Asym}^{\mathsf{RNS}} &= 1 - \left[1 - \sum_{k=1}^{K}\Delta_{asym}\right] \\ &= \sum_{k=1}^{K}\Delta_{asym}, \end{aligned} \tag{20}$$

where Δ_{asym} is defined as in (19). The proof of Corollary 1 is concluded. □

3.2.2. MNS Scheme

Corollary 2. *The asymptotic SOP of MNS scheme can be derived as*

$$P_{Asym}^{\mathsf{MNS}} = \sum_{k=1}^{K}\Phi_{asymn}, \tag{21}$$

where the following notation is adopted

$$\Phi_{asym} = 1 - \left(\frac{1}{\lambda_{k,m,i}\lambda_{k,m,\mathrm{E}}}\right)^{M} \frac{2}{\Gamma(M)} \left(\frac{(\gamma_{th}^{\mathsf{MNS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right) \times \left[\left(\frac{1}{\lambda_{k,m,\mathrm{E}}}\right)^{-M} - \frac{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathrm{E}}}{\gamma N\lambda_{k,i,j}}\beta_2^{M-1}\exp\left(\frac{\beta_2}{\lambda_{k,m,\mathrm{E}}}\right)\Gamma\left(1-M,\frac{\beta_2}{\lambda_{k,m,\mathrm{E}}}\right)\right]. \tag{22}$$

Proof. Similar to Corollary 1, the asymptotic SOP of MNS scheme can easily obtained as (21). The proof of Corollary 2 is concluded. □

3.2.3. ONS Scheme

Corollary 3. *The asymptotic SOP of ONS scheme can be derived as*

$$P_{Asym}^{\mathsf{ONS}} = \sum_{k=1}^{K}\Psi, \tag{23}$$

where Ψ *is defined as in* (A50).

Proof. Similar to Corollary 1, the asymptotic SOP of ONS scheme can easily obtained as (23). The proof of Corollary 3 is concluded. □

4. Numerical Results

In this section, we present representative numerical results to illustrate the achieve secrecy outage performance of the proposed schemes. Unless otherwise stated, the simulation parameters are presented in Table 2 [19,20].

Table 2. Summary of simulation parameters.

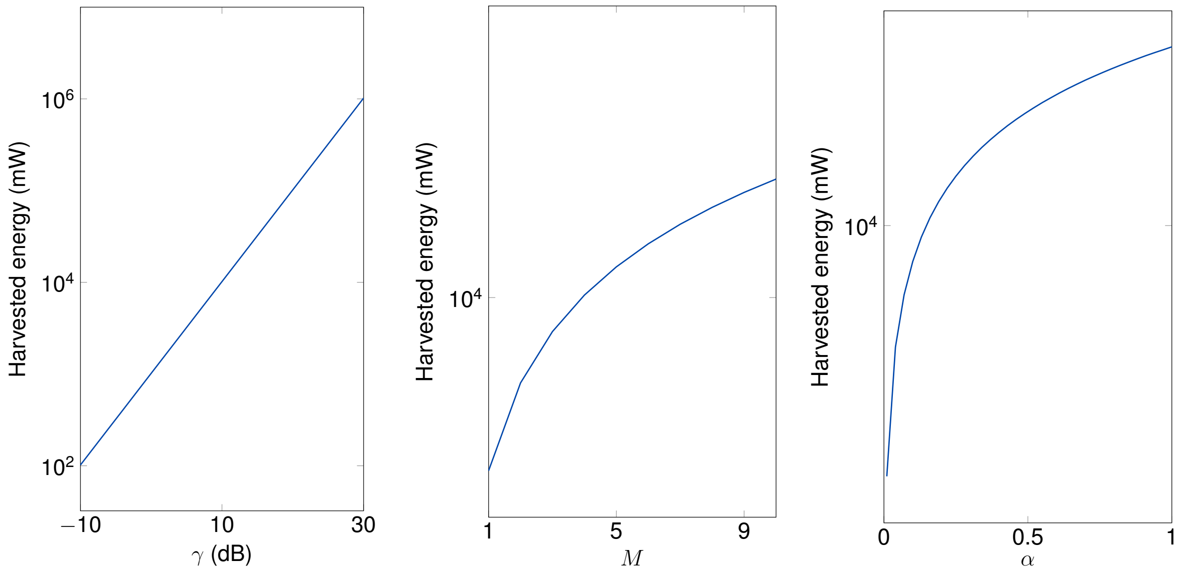
Parameters	**Value**
The distance between S and D, d_{SD}	10 m
The reference distance, d_0	1 m
The position of S	(0, 0)
The position of R_k	$(d_{\mathsf{SD}}\ k/K, 0)$
The position of D	(10, 0)
The position of PB_m	(7.5, 5.5)
The position of E	(−5, 5)
The number of relays in each cluster, N_k	2
The secrecy target data rate, R_{th}^{sch}	1 bps/Hz
Pathloss exponent, β	2.7
Pathloss at reference distance, $\mathcal{L}$ at d_0	−30 dB
Energy conversion efficiency, η	0.7
Time switching ratio, α	0.15

First of all, we exploit the impact of the energy parameters, i.e., transmit SNR of power beacons, the number of power beacons, and time switching ratio, to the average harvested energy of sensor node cluster. As can be seen in Figure 3, the average harvested energy of the sensor node cluster increases when the energy parameters is increased. In detail, in Figure 3a, the average harvested energy is linearly increased when transmit SNR of power beacons increases. Different from Figure 3a, when the number of power beacons increases, the slope of the harvested energy of sensor node cluster is decreased as shown in Figure 3b. The slope of the average harvested energy of sensor node cluster is decreased when the time switching ratio increases as shown in Figure 3c. From Figure 3, when transmit SNR of power beacons, the number of power beacons and time switching ratio increases, the sensor node can harvest enough energy to operate the sensor node [42]. It is noted that, as can be seen Table 2, the sensor node cluster is located at the most farthest from the power beacons. Thus, other clusters can naturally harvest more energy from the power beacons to transmit message and sense. Additionally, during the networks planning step, the engineers or administrators can make a network that the sensor nodes can sufficiently harvest the energy to transmit pilot and data messages or other source consumption.

We turn our attention to the impact of the system parameters on the secrecy outage performance. We studied the impact of transmit SNR, γ, on the SOP of the proposed schemes. As can be observed in Figure 4, the secrecy performances of all schemes were enhanced when the transmit SNR was increased. The reason is that the jamming signals significantly interfere with the eavesdropper channel when the transmit SNR of the power beacons is large. Additionally, the ONS scheme shows the robust performance among the proposed schemes since the ONS scheme required both CSI of the main and eavesdropper channels as in (12). In Figure 4, when the transmit SNR of power beacons was increased, the secrecy outage performance of the considered system model was significantly increased. One of possible reasons is that, in data transmission phase, the power beacons radiate the jamming signal to degrade the received SINR of the eavesdropper links.

Figure 5 illustrates the effect of the time switching ratio, α, on the SOP of the proposed schemes. The pattern of SOP presents the convex function that means the proposed scheme makes an adequate time switching ratio to improve system secrecy performance. When the time switching ratio was higher than 0.8, the system performance seemed to be saturated. Finally, the appropriately selected time switching ratio played an important role in network planning to enhance the overall system performance.

The effect of the secrecy target data rate, R_{th}, on the SOP is presented in Figure 6. A high secrecy target data means that the system requires a high system secrecy level. Thus, the outage event frequently occurs when system requires a high threshold. Furthermore, the SOPs of all schemes are increased when the secrecy target data rate increases. Different from the RNS and MNS schemes, the ONS scheme significantly enhances the system performance under the same channel settings. The reason is that the ONS scheme requires both main and eavesdropper channel information to select the node in each cluster to perform multi-hop transmission. Moreover, the results from Figure 4 to Figure 6 show that the theoretical results are in good agreement with the simulation ones validating the correctness of our derivation approaches.



(**a**) (**b**) (**c**)

Figure 3. The impact of energy parameters on the average harvested energy of the cluster of sensor nodes with $M = 4$, $N_k = 2$, $K = 3$, $\eta = 0.7$, $\alpha = 0.15$, $\gamma = 10$ dB and $R_{th} = 1$ bps/Hz. (**a**) Energy harvesting (EH) versus γ; (**b**) EH versus M; (**c**) EH versus α.

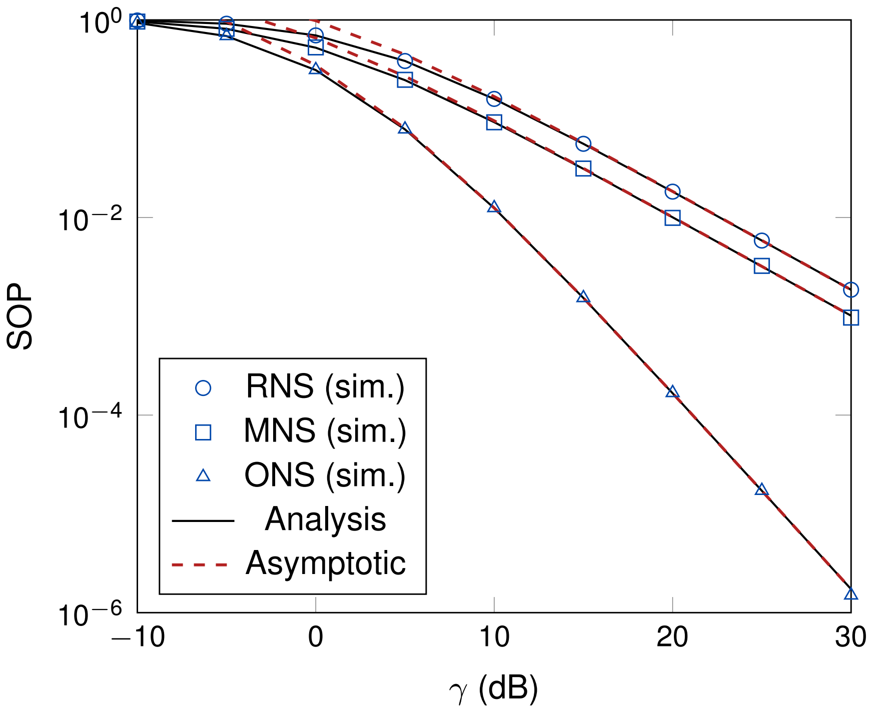


Figure 4. The illustration of the effect of γ on the secrecy outage probability (SOP) with $M = 4$ and $K = 3$.

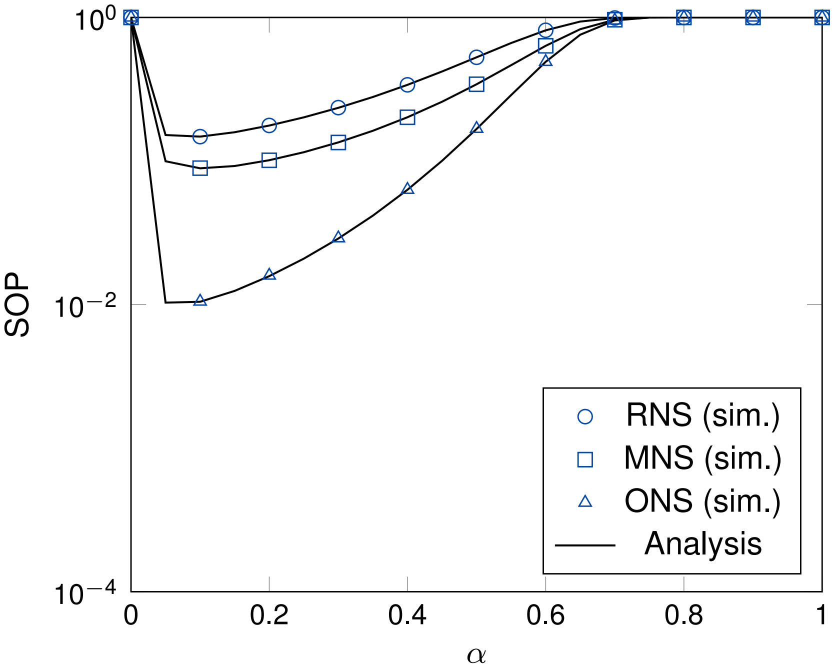


Figure 5. The SOP versus α with γ = 10 dB, M = 4 and K = 3.

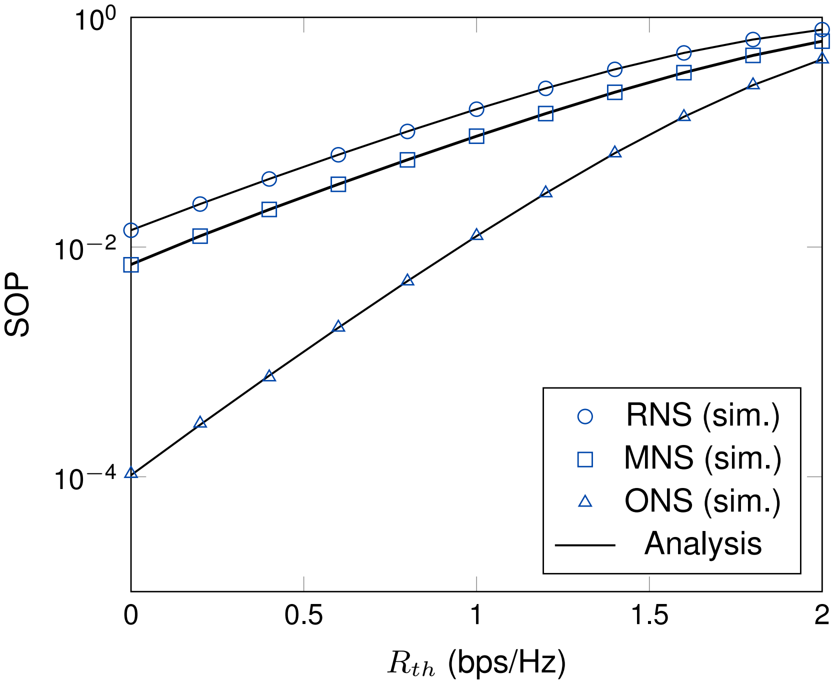


Figure 6. The effect of the SOP versus R_{th} with γ = 10 dB, M = 4, K = 3.

Now, we turn our attention to the effects of the number of hops, number of nodes in each cluster and number of power beacons on the system secrecy performance. Figure 7 plots the SOPs as a function of the number of hops. As can be observed, ONS scheme showed better secrecy performance than that of MNS and RNS schemes. The reason is that the RNS scheme does not consider the channel information to select the sensor node in each hop while MNS scheme only considers the eavesdropper channel. Differently, ONS scheme considers both main and eavesdropper channel information to select the best sensor node in each hop to perform the multi-hop transmission. Thus, the secrecy performance of ONS scheme outperforms the other proposed schemes in the same system setup. Similar to the time switching ratio, the number of hops shows the convex patterns in all node selection schemes; thus, appropriately selecting the number of hops plays an important role in network planning to enhance the system secrecy performance.

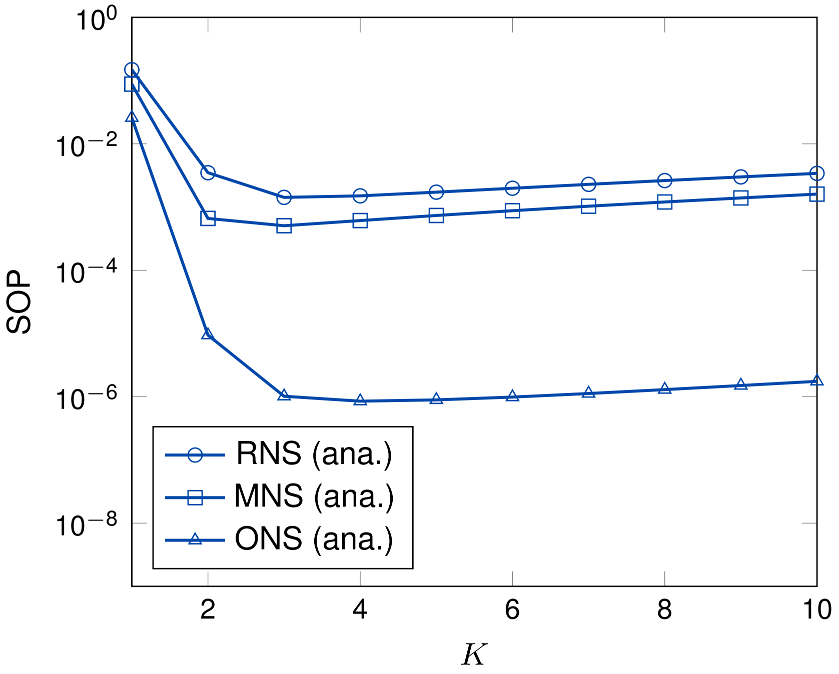


Figure 7. The SOP versus K with γ = 5 dB, R_{th} = 0.1 bps/Hz, M = 4.

Figure 8 presents the SOPs as a function of the number of sensor node in each cluster. As can be observed, when the number of nodes in each cluster was increased, the SOPs of ONS and MNS schemes were increased, while the SOP of RNS scheme was still unchanged. The reason is that RNS scheme randomly selects a node in each cluster for multi-hop transmission. More specifically, the MNS scheme requires the eavesdropper channel information to select the sensor node in each hop. Thus, the SOP of MNS scheme shows better performance than that of RNS scheme. Different from other schemes, since ONS scheme utilizes both main and eavesdropper channel information to select the node, ONS scheme dramatically enhances the secrecy performance compared to that of the other schemes when the number of node in each cluster increases.

Figure 9 illustrates the SOP as a function of the number of power beacons. The SOPs of the proposed schemes were enhanced when the number of power beacons was increased. The reason is that the SINR of eavesdropper channel degrades when the number of power beacons increases in (6). As can be observed, the SOPs of MNS and ONS schemes are significantly improved compared to that of RNS scheme. The reason is that MNS scheme consider the CSI of eavesdropper channel to select the sensor node in a each cluster while the ONS scheme utilizes both the CSI of main channel and eavesdropper channels to select the best sensor node in a each cluster. Thus, the secrecy performance is significantly enhanced under the same system setup. In Figures 8 and 9, when the number of sensor nodes in each cluster and the number of power beacons is increased, the system secrecy performance is increased excepted the RNS scheme. It is noted that increasing the number of sensor nodes in each cluster significantly enhances the secrecy performance compared to that of increasing the number of power beacons in the same network settings.

Finally, we exploit the complexity order of each node selection scheme as in Table 3. Complexity order represents the required channel estimation to select the node and transmit information [43,44]. As can be seen in Table 3, the amount of channel information of the RNS scheme was the smallest among the proposed scheduling schemes. The reason is that the RNS scheme does not require the channel information to select the node. Thus, the total required channel information is K. Differently, MNS scheme needs to estimate the channel information to select the best node. Thus, the total complexity order is $(M + N_k + 1)K$. Optimally, ONS scheme utilizes both main and eavesdropper channels information to select the best node. Since the nodes are sequentially selected from the destination node, the amount of the required channel information at a certain hop transmission is $2N_k + MN_k + M$, and the amount of the required channel information for K hops transmission is $(2N_k + MN_k + M)K$. Through Table 3, each scheme has a specific advantage and drawback. Thus, in network planning perspective, each scheme can be cleverly applied in the practice to achieve a good trade-off between secrecy performance and complexity.

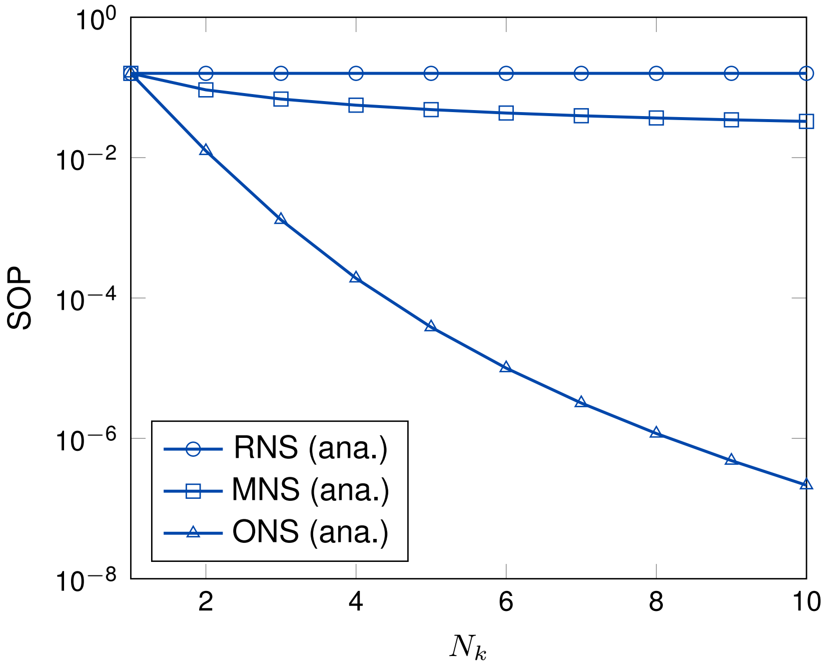


Figure 8. The SOP versus N_k with γ = 10 dB, M = 4, K = 3.

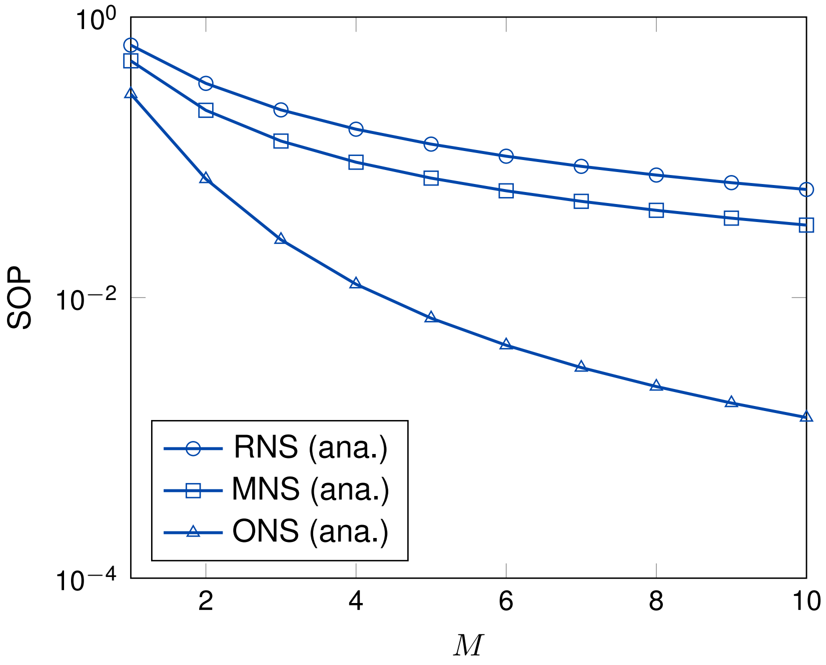


Figure 9. The SOP versus M with γ = 15 dB, K = 3.

Table 3. The comparison of complexity order in the proposed schemes.

Scheme	RNS	MNS	ONS
Complexity Order	K	$(M+N_k+1)K$	$(2N_k+MN_k+M)K$

5. Conclusions

This paper proposed the system model and the scheduling scheme to enhance the secrecy performance for WPT-based multi-hop transmission in WSNs. More specifically, the power beacon served as a friendly jammer to reduce the CSI of eavesdropper as well as the radiation energy to harvest the sensor node. We proposed two kinds of node selection schemes, called as MNS and ONS schemes, to improve the secrecy performance. The MNS scheme selected the sensor node to minimize the eavesdropper channel information in each cluster while ONS schemes utilized both main and eavesdropper channel information to select the best cooperative node in each cluster. We derived the exact closed-form expression for SOP of the proposed schemes. In addition, to provide more insights into the proposed schemes, we derived asymptotic SOP. From the numerical results, the secrecy performance of the ONS scheme outperformed compared to that of MNS scheme under the same system setup. However, through the complexity order analysis, the ONS scheme showed the more required channel information to select the sensor node and transmit information than that of MNS scheme.

Author Contributions: The main contributions of K.S. were to create the main ideas and execute performance evaluations by theoretical analysis and simulation. T.-V.N. worked on the related works to review the idea, supporting the theoretical analysis, and improved the writing of the paper. B.A. worked as the advisor of K.S. and T.-V.N. to discuss, create and advise the main ideas and performance evaluations together.

Funding: This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant no. 2016R1D1A1B03934898) and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1A2C1083996).

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

Appendix A. The Proof of Theorem 1

From (13), the SOP of RNS scheme, $P_{\text{out}}^{\text{RNS}}$, can be expressed as

$$P_{\text{out}}^{\text{RNS}} = 1 - \prod_{k=1}^{K}\left[1 - \underbrace{\Pr\left(\frac{1+\gamma_{k,i^*,j^*}^{\text{RNS}}}{1+\gamma_{k,i^*,\text{E}}^{\text{RNS}}} < \gamma_{th}^{\text{RNS}}\right)}_{\Delta}\right]. \tag{A1}$$

From (7) and (8), Δ in (A1) can be rewritten as

$$\begin{aligned}\Delta &= \Pr\left[\frac{1+\kappa W_{k,i}Y_{k,i,j}}{1+\kappa W_{k,i}Z_{k,i,\text{E}}/(1+\gamma V_{k,\text{E}})} < \gamma_{th}^{\text{RNS}}\right] \\ &= \Pr\left[Y_{k,i,j} < \frac{\gamma_{th}^{\text{RNS}}-1}{\kappa\gamma W_{k,i}} + \frac{\gamma_{th}^{\text{RNS}}Z_{k,i,\text{E}}}{1+\gamma V_{k,\text{E}}}\right].\end{aligned} \tag{A2}$$

We then calculate Δ in (A2) as

$$\Delta = \int_0^\infty\int_0^\infty \underbrace{\int_0^\infty F_{Y_{k,i,j}}\left(\frac{\gamma_{th}^{\text{RNS}}-1}{\kappa\gamma w} + \frac{\gamma_{th}^{\text{RNS}}z}{1+\gamma v}\right) f_{Z_{k,i,\text{E}}}(z)dz}_{\Delta_1}\, f_{W_{k,i}}(w)dw f_{V_{k,\text{E}}}(v)dv. \tag{A3}$$

Next, Δ_1 can be calculated as

$$\Delta_1 = \int_0^\infty \left[1 - \exp\left(-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{th}^{\mathsf{RNS}}-1}{\kappa\gamma w} + \frac{\gamma z}{1+\gamma v}\right)\right)\right]\frac{1}{\lambda_{k,i,\mathrm{E}}}\exp\left(-\frac{1}{\lambda_{k,i,\mathrm{E}}}z\right)dz. \tag{A4}$$

With the help of ([41], eq.(3.310)), we obtain Δ_1 as

$$\Delta_1 = 1 - \frac{\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}+\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}\exp\left(-\frac{\gamma_{th}^{\mathsf{RNS}}-1}{\kappa\gamma w\lambda_{k,i,j}}\right). \tag{A5}$$

Substituting (A5) into (A3), Δ can be expressed as

$$\Delta = \int_0^\infty \underbrace{\int_0^\infty \left[1 - \frac{\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}+\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}\exp\left(-\frac{\gamma_{th}^{\mathsf{RNS}}-1}{\kappa\gamma\lambda_{k,i,j}w}\right)\right]f_{W_{k,i}}(w)dw}_{\Delta_2}\, f_{V_{k,\mathrm{E}}}(v)dv. \tag{A6}$$

Since $W_{k,i}$ is the summation of M exponential random variables, $W_{k,i}$ follows the Gamma distribution [14,19]. Hence, the CDF and PDF of $W_{k,i}$ can be expressed as

$$F_{W_{k,i}}(w) = 1 - \exp\left(-\frac{w}{\lambda_{k,m,i}}\right)\sum_{t=0}^{M-1}\frac{1}{t!}\left(\frac{w}{\lambda_{k,m,i}}\right)^t, \tag{A7}$$

$$f_{W_{k,i}}(w) = {\frac{1}{\lambda_{k,m,i}}}^{M}\frac{w^{M-1}}{\Gamma(M)}\exp\left(-\frac{w}{\lambda_{k,m,i}}\right). \tag{A8}$$

Plugging the PDF of $W_{k,i}$ into (A6), along with the helps of ([41], eq. (3.351.3)) and ([41], eq. (3.471.9)), Δ_2 in (A6) can be obtained as

$$\Delta_2 = 1 - \frac{\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}+\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}\left(\frac{1}{\lambda_{k,m,i}}\right)^M\frac{2}{\Gamma(M)}\left(\frac{(\gamma_{th}^{\mathsf{RNS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2}K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{RNS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right). \tag{A9}$$

Next, substituting (A9) into (A6) and applying ([41], eq. 3.351.3), Δ can be expressed as

$$\begin{aligned}\Delta =& 1 - \left(\frac{1}{\lambda_{k,m,i}\lambda_{k,m,\mathrm{E}}}\right)^M\frac{2}{\Gamma(M)\Gamma(M)}\left(\frac{(\gamma_{th}^{\mathsf{RNS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2}K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{RNS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\\ &\times\underbrace{\int_0^\infty\left(1-\frac{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}}{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}+\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}\right)v^{M-1}\exp\left(-\frac{v}{\lambda_{k,m,\mathrm{E}}}\right)dv}_{\Delta_3}.\end{aligned} \tag{A10}$$

Relying on ([41], eq. 3.351.3) and ([41], eq. 3.383.10), Δ_3 in (A10) can be obtained as

$$\begin{aligned}\Delta_3 =& \int_0^\infty v^{M-1}\exp\left(-\frac{v}{\lambda_{k,m,\mathrm{E}}}\right)dv - \frac{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}}{\gamma\lambda_{k,i,j}}\int_0^\infty\frac{1}{\beta_1+v}v^{M-1}\exp\left(-\frac{v}{\lambda_{k,m,\mathrm{E}}}\right)dv\\ =&\Gamma(M)\left(\frac{1}{\lambda_{k,m,\mathrm{E}}}\right)^{-M} - \frac{\gamma_{th}^{\mathsf{RNS}}\lambda_{k,i,\mathrm{E}}}{\gamma\lambda_{k,i,j}}\beta_1^{M-1}\exp\left(\frac{\beta_1}{\lambda_{k,m,\mathrm{E}}}\right)\Gamma(M)\Gamma\left(1-M,\frac{\beta_1}{\lambda_{k,m,\mathrm{E}}}\right).\end{aligned} \tag{A11}$$

Plugging (A11) into (A10) and after some mathematical manipulations, we can obtain (14). The proof of Theorem 1 is concluded.

Appendix B. The Proof of Theorem 2

From (13), the SOP of the MNS scheme, P_{out}^{MNS}, can be rewritten as

$$P_{out}^{\text{MNS}} = 1 - \prod_{k=1}^{K} \Pr\left[1 - \underbrace{\Pr\left(\frac{1+\gamma_{k,i^*,j^*}^{\text{MNS}}}{1+\gamma_{k,i^*,\text{E}}^{\text{MNS}}} < \gamma_{th}^{\text{MNS}}\right)}_{\Phi}\right]. \tag{A12}$$

Similar to RNS scheme, Φ in (A12) can be rewritten as

$$\Phi = \Pr\left[Y_{k,i^*,j^*} < \frac{\gamma_{th}^{\text{MNS}}-1}{\kappa\gamma W_{k,i^*}} + \frac{\gamma_{th}^{\text{MNS}} Z_{k,i^*,\text{E}}}{1+\gamma V_{k,\text{E}}}\right]. \tag{A13}$$

As can be observed, the events of the probability (A13) are not mutually exclusive since they include the same components $Z_{k,i^*,\text{E}}$ [33,45]. Thus, by conditioning $Z_{k,i^*,\text{E}} = z$, Φ can be further rewritten as

$$\Phi = \int_0^\infty \Pr\left[Y_{k,i^*,j^*} < \frac{\gamma_{th}^{\text{MNS}}-1}{\kappa\gamma W_{k,i^*}} + \frac{\gamma_{th}^{\text{MNS}} z}{1+\gamma V_{k,\text{E}}}\right] f_{Z_{k,i^*,\text{E}}}(z)dz. \tag{A14}$$

Based on the total probability [46], Φ can be calculated as

$$\Phi = \int_0^\infty \int_0^\infty \underbrace{\int_0^\infty \sum_{i=1}^{N} \Pr(i^*=i) \Pr\left[Y_{k,i,j^*} < \frac{\gamma_{th}^{\text{MNS}}-1}{\kappa\gamma w} + \frac{\gamma_{th}^{\text{MNS}} z}{1+\gamma v}\right] f_{Z_{k,i^*,\text{E}}}(z)dz}_{\Phi_1} f_{W_{k,i}}(w)dw f_{V_{k,\text{E}}}(v)dv. \tag{A15}$$

The following lemmas will help to calculate (A15). First, Lemma A1 helps to obtain the probability of a certain node based on the criterion (9).

Lemma A1. $\Pr(i^* = i)$ *in* (A15) *can be written as*

$$\Pr(i^* = i) = \frac{1}{N}. \tag{A16}$$

Proof. The proof can be found in [33]. □

Next, the CDF and PDF of Y_{k,i,j^*} can be obtained by the following lemma.

Lemma A2. *The CDF and PDF of* Y_{k,i,j^*} *can be, respectively, derived as*

$$F_{Y_{k,i,j^*}}(y) = 1 - \exp\left(-\frac{y}{\lambda_{Y_{k,i,j}}}\right), \tag{A17}$$

$$f_{Y_{k,i,j^*}}(y) = \frac{1}{\lambda_{Y_{k,i,j}}} \exp\left(-\frac{y}{\lambda_{Y_{k,i,j}}}\right). \tag{A18}$$

Proof. From the node selection criterion (9), the CDF of Y_{k,i,j^*} can be expressed as

$$F_{Y_{k,i,j^*}}(y) = \sum_{j=1}^{N} \underbrace{\Pr(j^*=j)}_{\Phi_{1A}} \Pr\left(Y_{k,i,j} < y\right). \tag{A19}$$

Next, Φ_{1B} in (A19) can be written as

$$\Phi_{1A} = \Pr\left(\bigcap_{u=1,u\neq i}^{N} \left(Y_{k,u,\text{E}} > Y_{k,i,\text{E}}\right)\right). \tag{A20}$$

By conditioning $Y_{k,i,\mathrm{E}} = y$, $F_{Y_{k,i,j^*}}(y)$ can be rewritten as

$$\begin{aligned}\Phi_{1A} &= \int_0^\infty \exp\left(-\frac{(N-1)y}{\lambda_{Y_{k,i,j}}}\right)\frac{1}{\lambda_{Y_{k,i,j}}}\exp\left(-\frac{y}{\lambda_{Y_{k,i,j}}}\right)dy,\\ &= 1/N.\end{aligned} \tag{A21}$$

Plugging (A21) into (A19) and after some careful manipulations, we can easily obtain the (A17) and (A18). This proof of Lemma A2 is concluded. □

Next, the CDF and PDF of $Z_{k,i^*,\mathrm{E}}$ can be obtained by the following lemma.

Lemma A3. *The CDF and PDF of the $Z_{k,i^*,\mathrm{E}}$ can be, respectively, derived as*

$$F_{Z_{k,i^*,\mathrm{E}}}(z) = 1 - \exp\left(-\frac{Nz}{\lambda_{k,i,\mathrm{E}}}\right), \tag{A22}$$

$$f_{Z_{k,i^*,\mathrm{E}}}(z) = \frac{N}{\lambda_{k,i,\mathrm{E}}}\exp\left(-\frac{Nz}{\lambda_{k,i,\mathrm{E}}}\right). \tag{A23}$$

Proof. From the (9), the CDF of $Z_{k,i^*,\mathrm{E}}$ can be rewritten as

$$F_{Z_{k,i^*,\mathrm{E}}}(z) = \Pr\left(\min_{1\le i\le N} Z_{k,i,\mathrm{E}} < z\right). \tag{A24}$$

After some manipulations, (A24) can be further expressed as

$$\begin{aligned}F_{Z_{k,i^*,\mathrm{E}}}(z) &= 1 - \Pr\left(\min_{1\le i\le N} Z_{k,i,\mathrm{E}} < z\right)\\ &= 1 - \prod_{i=1}^{N}\left[1 - \Pr\left(Z_{k,i,\mathrm{E}} < z\right)\right].\end{aligned} \tag{A25}$$

Applying ([41], eq. 3.310), the CDF and PDF of $Z_{k,i^*,\mathrm{E}}$ can be obtained as in (A22) and (A23), respectively. The proof of Lemma A3 is concluded. □

Next, plugging (A16), (A17) and (A23) into (A15), Φ_1 in (A15) can be expressed as

$$\Phi_1 = \int_0^\infty \frac{N}{\lambda_{k,i,\mathrm{E}}}\exp\left(-\frac{Nz}{\lambda_{k,i,\mathrm{E}}}\right)dz - \frac{N}{\lambda_{k,i,\mathrm{E}}}\exp\left(-\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma w\lambda_{k,i,j}}\right)\int_0^\infty \exp\left(-(\frac{\gamma_{th}^{\mathsf{MNS}}}{(1+\gamma v)\lambda_{k,i,j}} + \frac{N}{\lambda_{k,i,\mathrm{E}}})z\right)dz. \tag{A26}$$

Applying ([41], eq. 3.310), Φ_1 can be obtained as

$$\Phi_1 = 1 - \frac{N(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathrm{E}} + N(1+\gamma v)\lambda_{k,i,j}}\exp\left(-\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma w\lambda_{k,i,j}}\right). \tag{A27}$$

By substituting (A27) into (A15), Φ can be rewritten as

$$\Phi = \int_0^\infty \underbrace{\int_0^\infty \left[1 - \frac{N(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathrm{E}} + N(1+\gamma v)\lambda_{k,i,j}}\exp\left(-\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma w\lambda_{k,i,j}}\right)\right] f_{W_{k,i}}(w)dx}_{\Phi_2}\, f_{V_{k,\mathrm{E}}}(v)dv. \tag{A28}$$

From (A28), Φ_2 can be further expressed as

$$\begin{aligned}\Phi_2 =& \underbrace{\int_0^\infty \left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{w^{M-1}}{\Gamma(M)} \exp\left(-\frac{w}{\lambda_{k,m,i}}\right) dw}_{\Phi_{2A}} \\ &- \frac{N(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}} + N(1+\gamma v)\lambda_{k,i,j}} \frac{1}{\Gamma(M)} \left(\frac{1}{\lambda_{k,m,i}}\right)^M \underbrace{\int_0^\infty w^{M-1} \exp\left(-\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{k,i,j}}\frac{1}{w} - \frac{1}{\lambda_{k,m,i}}w\right) dw}_{\Phi_{2B}}.\end{aligned} \tag{A29}$$

In order to further calculate (A29), we apply ([41], eq. 3.351.3) and ([41], eq. 3.471.9) for Φ_{2A} and Φ_{2B}, respectively. We can obtain the results as

$$\begin{aligned}\Phi_{2A} &= \int_0^\infty \left(\frac{1}{\lambda_{m,k,i}}\right)^M \frac{w^{M-1}}{\Gamma(M)} \exp\left(-\frac{w}{\lambda_{m,k,i}}\right) dw = 1, \\ \Phi_{2B} &= \int_0^\infty w^{M-1} \exp\left(-\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{k,i,j}}\frac{1}{w} - \frac{1}{\lambda_{m,k,i}}w\right) dw \\ &= 2\left(\frac{(\gamma_{th}^{\mathsf{MNS}-1})\lambda_{m,k,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{m,k,i}\lambda_{k,i,j}}}\right).\end{aligned} \tag{A30}$$

By plugging (A30) into (A29), along with the help of ([41], eq. 3.351.3), Φ can be calculated as

$$\begin{aligned}\Phi =& 1 - \left(\frac{1}{\lambda_{m,k,i}\lambda_{k,m,\mathsf{E}}}\right)^M \frac{2}{\Gamma(M)\Gamma(M)} \left(\frac{(\gamma_{th}^{\mathsf{MNS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{MNS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right) \\ & \times \underbrace{\int_0^\infty \frac{N(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}} + N(1+\gamma v)\lambda_{k,i,j}} v^{M-1} \exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right) dv}_{\Phi_3}.\end{aligned} \tag{A31}$$

In order to further calculate the integration in (A31), Φ_3 can be calculated as

$$\begin{aligned}\Phi_3 &= \int_0^\infty \left(1 - \frac{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}}}{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}} + N\lambda_{k,i,j} + \gamma N\lambda_{k,i,j}v}\right) v^{M-1} \exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right) dv \\ &= \int_0^\infty v^{M-1} \exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right) dt - \frac{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}}}{\gamma N\lambda_{k,i,j}} \int_0^\infty \frac{v^{M-1}}{\beta_2 + v} \exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right) dv,\end{aligned} \tag{A32}$$

where β_2 is defined as (15). Similar to (A11) in RNS scheme, we utilize ([41], eq. 3.351.3) and ([41], 3.383.10) to obtain Φ_3 as

$$\Phi_3 = \Gamma(M)\left(\frac{1}{\lambda_{k,m,\mathsf{E}}}\right)^{-M} - \frac{\gamma_{th}^{\mathsf{MNS}}\lambda_{k,i,\mathsf{E}}}{\gamma N\lambda_{k,i,j}} \beta_2^{M-1} \exp\left(\frac{\beta_2}{\lambda_{k,m,\mathsf{E}}}\right) \Gamma(M) \Gamma\left(1-M, \frac{\beta_2}{\lambda_{k,m,\mathsf{E}}}\right). \tag{A33}$$

Plugging (A33) into (A31) and after some careful manipulations, the exact closed-form expression for the SOP of MNS scheme can be obtained as (15). The proof of Theorem 2 is concluded.

Appendix C. The Proof of Theorem 3

From (13), the SOP of ONS scheme can be expressed as

$$P_{out}^{\mathsf{ONS}} = 1 - \prod_{k=1}^{K} \left[1 - \underbrace{\Pr\left(\frac{1+\gamma_{k,i^*,j^*}^{\mathsf{ONS}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\mathsf{ONS}}} < \gamma_{th}\right)}_{\Psi}\right]. \tag{A34}$$

Similar to the MNS scheme, Ψ in (A34) can be further rewritten as

$$\Psi = \Pr\left(\frac{1+\kappa\gamma W_{k,i^*}Y_{k,i^*,j^*}}{1+\frac{\kappa\gamma W_{k,i^*}Z_{k,i^*,\mathsf{E}}}{1+\gamma V_{k,\mathsf{E}}}} < \gamma_{th}^{\mathsf{ONS}}\right). \tag{A35}$$

As can be seen, the events of the probability in (A35) are not mutually exclusive since they include the same components $T_{k,m,\mathsf{E}}$ [33,45]. By conditioning on $T_{k,m,\mathsf{E}} = t$, Ψ can be further expressed as

$$\Psi = \int_0^\infty \Pr\left(\max_{i\in N}\left\{\frac{1+\kappa\gamma X_{k,i}Y_{k,i,j^*}}{1+\frac{\kappa\gamma X_{k,i}Z_{k,i,\mathsf{E}}}{1+\gamma v}}\right\} < \gamma_{th}^{\mathsf{ONS}}\right) f_{V_{k,\mathsf{E}}}(v)dv. \tag{A36}$$

Based on the criterion in (12), (A36) can be expressed as

$$\Psi = \int_0^\infty \prod_{i=1}^{N}\Bigg[\underbrace{\Pr\left(Y_{k,i,j^*} < \frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma W_{k,i}} + \frac{\gamma_{th}^{\mathsf{ONS}}Z_{k,i,\mathsf{E}}}{1+\gamma v}\right)}_{\Psi_1}\Bigg] f_{V_{k,\mathsf{E}}}(v)dv. \tag{A37}$$

In order to further calculate the integration in (A37), Ψ_1 can be rewritten as

$$\Psi_1 = \int_0^\infty \underbrace{\int_0^\infty F_{Y_{k,i,j^*}}\left(\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma w} + \frac{\gamma_{th}^{\mathsf{ONS}}z}{1+\gamma v}\right) f_{Z_{k,i,\mathsf{E}}}(z)dz}_{\Psi_2}\, f_{W_{k,i}}(w)dw. \tag{A38}$$

Recalling Lemma A2, Ψ_2 in (A38) can be calculated as

$$\Psi_2 = \int_0^\infty \left[1-\exp\left(-\frac{1}{\lambda_{k,i,j}}(\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma w} + \frac{\gamma_{th}^{\mathsf{ONS}}z}{1+\gamma v})\right)\right]\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{z}{\lambda_{k,i,\mathsf{E}}}\right)dz. \tag{A39}$$

Applying ([41], 3.310), we can obtain as

$$\Psi_2 = 1 - \frac{(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}} + (1+\gamma v)\lambda_{k,i,j}}\exp\left(-\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma w\lambda_{k,i,j}}\right). \tag{A40}$$

By substituting (A40) into (A38), Ψ_1 can be further written as

$$\begin{aligned}\Psi_1 =& \underbrace{\int_0^\infty \left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{w^{M-1}}{\Gamma(M)}\exp\left(-\frac{w}{\lambda_{k,m,i}}\right)dw}_{\Psi_{1A}} \\ &-\left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{1}{\Gamma(M)}\frac{(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}} + (1+\gamma v)\lambda_{k,i,j}}\underbrace{\int_0^\infty w^{M-1}\exp\left(-\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,i,j}}\frac{1}{w} - \frac{1}{\lambda_{k,m,i}}w\right)dw}_{\Psi_{1B}}.\end{aligned} \tag{A41}$$

By applying ([41], 3.351.3) and ([41], 3.471.9) for Ψ_{1A} and Ψ_{1B}, respectively, we can obtain as

$$\begin{aligned}\Psi_{1A} =& \int_0^\infty \left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{w^{M-1}}{\Gamma(M)}\exp\left(-\frac{w}{\lambda_{k,m,i}}\right)dw = 1, \\ \Psi_{1B} =& \int_0^\infty w^{M-1}\exp\left(-\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,i,j}}\frac{1}{w} - \frac{1}{\lambda_{k,m,i}}w\right)dw \\ =&2\left(\frac{(\gamma_{th}^{\mathsf{ONS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right).\end{aligned} \tag{A42}$$

Consequently, Ψ_1 can be obtained as

$$\begin{aligned}\Psi_1 =& 1-\left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{2}{\Gamma(M)} \frac{(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}}+(1+\gamma v)\lambda_{k,i,j}} \\ &\times \left(\frac{(\gamma_{th}^{\mathsf{ONS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right). \end{aligned} \tag{A43}$$

By plugging (A43) into (A37) and after some mathematical steps, Ψ can be written as

$$\begin{aligned}\Psi =& \int_0^\infty \left[1-\left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{2}{\Gamma(M)} \frac{(1+\gamma v)\lambda_{k,i,j}}{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}}+(1+\gamma v)\lambda_{k,i,j}} \left(\frac{(\gamma_{th}^{\mathsf{ONS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2}\right. \\ &\left.\times K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\right]^N \left(\frac{1}{\lambda_{k,m,\mathsf{E}}}\right)^M \frac{v^{M-1}}{\Gamma(M)} \exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right)dv. \end{aligned} \tag{A44}$$

Based on the binomial theorem, (A44) can be further expressed as

$$\begin{aligned}\Psi =& \left(\frac{1}{\lambda_{k,m,\mathsf{E}}}\right)^M \frac{1}{\Gamma(M)} \sum_{n=0}^{N}\binom{N}{n}(-1)^n \\ &\times \left[\left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{2}{\Gamma(M)} \left(\frac{(\gamma_{th}^{\mathsf{ONS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\right]^n \\ &\underbrace{\times \int_0^\infty \left(1-\frac{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}}}{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}}+\lambda_{k,i,j}+\gamma\lambda_{k,i,j}v}\right)^n v^{M-1}\exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right)dv\,.}_{\Psi_3} \end{aligned} \tag{A45}$$

Again, utilizing the binomial theorem, Ψ_3 in (A45) can be further expressed as

$$\Psi_3 = \sum_{i=0}^{n}\binom{n}{i}(-1)^i\left(\frac{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}}}{\gamma\lambda_{k,i,j}}\right)^i \int_0^\infty \frac{v^{M-1}}{(\beta_3+v)^i}\exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right)dv, \tag{A46}$$

where β_3 is defined as (16) and by plugging (A46) into (A45), Ψ can be written as

$$\begin{aligned}\Psi =& \left(\frac{1}{\lambda_{k,m,\mathsf{E}}}\right)^M \frac{1}{\Gamma(M)} \sum_{n=0}^{N}\sum_{i=0}^{n}\binom{N}{n}\binom{n}{i}(-1)^{n+i} \\ &\times \left[\left(\frac{1}{\lambda_{k,m,i}}\right)^M \frac{2}{\Gamma(M)} \left(\frac{(\gamma_{th}^{\mathsf{ONS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathsf{ONS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\right]^n \\ &\times \left(\frac{\gamma_{th}^{\mathsf{ONS}}\lambda_{k,i,\mathsf{E}}+\lambda_{k,i,j}}{\gamma\lambda_{k,i,j}}\right)^i \underbrace{\int_0^\infty \frac{v^{M-1}}{(\beta_3+v)^i}\exp\left(-\frac{v}{\lambda_{k,m,\mathsf{E}}}\right)dv\,.}_{\Psi_4} \end{aligned} \tag{A47}$$

In order to calculate the integration in (A47), we change the variable as $u = \beta_3 + v$; Ψ_4 can be rewritten as

$$\begin{aligned}\Psi_4 =& \int_{\beta_3}^\infty u^{-i}(u-\beta_3)^{M-1}\exp\left(-\frac{u-\beta_3}{\lambda_{k,m,\mathsf{E}}}\right)du \\ =& \exp\left(\frac{\beta_3}{\lambda_{k,m,\mathsf{E}}}\right)\int_{\beta_3}^\infty u^{-i}(u-\beta_3)^{M-1}\exp\left(-\frac{u}{\lambda_{k,m,\mathsf{E}}}\right)du. \end{aligned} \tag{A48}$$

Making use of ([41], 3.383.4), Ψ_4 can be calculated as

$$\Psi_4 = \exp\left(\frac{\beta_3}{\lambda_{k,m,\mathrm{E}}}\right)\left(\frac{1}{\lambda_{k,m,\mathrm{E}}}\right)^{-\frac{M-i+1}{2}} \beta_3^{\frac{M-i-1}{2}} \Gamma(M) \exp\left(-\frac{\beta_3}{2\lambda_{k,m,\mathrm{E}}}\right) W_{\frac{-i+1-M}{2},\frac{i-M}{2}}\left(\frac{\beta_3}{\lambda_{k,m,\mathrm{E}}}\right), \tag{A49}$$

where $W_{\lambda,\mu}(z)$ is defined as (16). By plugging (A49) into (A47), Ψ can be obtained as

$$\begin{aligned}\Psi =& \left(\frac{1}{\lambda_{k,m,\mathrm{E}}}\right)^{M} \frac{1}{\Gamma(M)} \sum_{n=0}^{N}\sum_{i=0}^{n}\binom{N}{n}\binom{n}{i}(-1)^{n+i}\left(\frac{\gamma_{th}^{\mathrm{ONS}}\lambda_{k,i,\mathrm{E}}+\lambda_{k,i,j}}{\gamma\lambda_{k,i,j}}\right)^{i} \\ &\times\left[\left(\frac{1}{\lambda_{k,m,i}}\right)^{M}\frac{2}{\Gamma(M)}\left(\frac{(\gamma_{th}^{\mathrm{ONS}}-1)\lambda_{k,m,i}}{\kappa\gamma\lambda_{k,i,j}}\right)^{M/2} K_M\left(2\sqrt{\frac{\gamma_{th}^{\mathrm{ONS}}-1}{\kappa\gamma\lambda_{k,m,i}\lambda_{k,i,j}}}\right)\right]^{n} \\ &\times\exp\left(\frac{\beta_3}{\lambda_{k,m,\mathrm{E}}}\right)\left(\frac{1}{\lambda_{k,m,\mathrm{E}}}\right)^{-\frac{M-i+1}{2}}\beta_3^{\frac{M-i-1}{2}}\Gamma(M)\exp\left(-\frac{\beta_3}{2\lambda_{k,m,\mathrm{E}}}\right)W_{\frac{-i+1-M}{2},\frac{i-M}{2}}\left(\frac{\beta_3}{\lambda_{k,m,\mathrm{E}}}\right).\end{aligned} \tag{A50}$$

By plugging (A50) into (A34), the exact closed-form expression of ONS scheme can be obtained as (16). The proof of Theorem 3 is concluded.

References

1. Fodor, G.; Dahlman, E.; Mildh, G.; Parkvall, S.; Reider, N.; Miklós, G.; Turányi, Z. Design aspects of network assisted device-to-device communications. *IEEE Commun. Mag.* **2012**, *50*, 170–177. [CrossRef]
2. Xie, L.; Shi, Y.; Hou, Y.T.; Lou, A. Wireless power transfer and applications to sensor networks. *IEEE Wirel. Commun.* **2013**, *20*, 140–145. [CrossRef]
3. Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. *J. Netw. Comput. Appl.* **2016**, *60*, 192–219. [CrossRef]
4. Awan, K.M.; Shah, P.A.; Iqbal, K.; Gillani, S.; Ahmad, W.; Nam, Y. Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 6470359. [CrossRef]
5. Pan, G.; Lei, H.; Yuan, Y.; Ding, Z. Performance Analysis and Optimization for SWIPT Wireless Sensor Networks. *IEEE Trans. Commun.* **2017**, *65*, 2291–2302. [CrossRef]
6. Kurs, A.; Karalis, A.; Moffatt, R.; Joannopoulos, J.D.; Fisher, P.; Soljačić, M. Wireless Power Transfer via Strongly Coupled Magnetic Resonances. *Science* **2007**, *317*, 83–86. [CrossRef]
7. Lumpkins, W. Nikola Tesla's Dream Realized: Wireless power energy harvesting. *IEEE Consum. Electron. Mag.* **2014**, *3*, 39–42. [CrossRef]
8. Zhong, C.; Chen, X.; Zhang, Z.; Karagiannidis, G.K. Wireless-Powered Communications: Performance Analysis and Optimization. *IEEE Trans. Commun.* **2015**, *63*, 5178–5190. [CrossRef]
9. 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]
10. Pan, G.; Lei, H.; Ding, Z.; Ni, Q. 3-D Hybrid VLC-RF Indoor IoT Systems With Light Energy Harvesting. *IEEE Trans. Green Commun. Netw.* **2019**, *3*, 853–865. [CrossRef]
11. Atapattu, S.; Ross, N.; Jing, Y.; He, Y.; Evans, J.S. Physical-Layer Security in Full-Duplex Multi-Hop Multi-User Wireless Network With Relay Selection. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1216–1232. [CrossRef]
12. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 19–26. [CrossRef] [PubMed]
13. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
14. da Costa, D.; Ferdinand, N.; Dias, U.; de Sousa Júnior, R.; Latva-aho, M. Secrecy Outage Performance of MIMO Wiretap Channels with Multiple Jamming Signals. *J. Commun. Inf. Syst.* **2016**, *31*. [CrossRef]
15. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
16. Do, N.T.; Bao, V.N.Q.; An, B. Outage Performance Analysis of Relay Selection Schemes in Wireless Energy Harvesting Cooperative Networks over Non-Identical Rayleigh Fading Channels. *Sensors* **2016**, *16*, 295. [CrossRef]

17. Lei, H.; Xu, M.; Ansari, I.S.; Pan, G.; Qaraqe, K.A.; Alouini, M. On Secure Underlay MIMO Cognitive Radio Networks with Energy Harvesting and Transmit Antenna Selection. *IEEE Trans. Green Commun. Netw.* **2017**, *1*, 192–203. [CrossRef]
18. Van, N.T.; Tan, H.M.; Hoang, T.M.; Duy, T.T.; Bao, V.N.Q. Exact outage probability of energy harvesting incremental relaying networks with MRC receiver. In Proceedings of the 2016 International Conference on Advanced Technologies for Communications (ATC), Hanoi, Vietnam, 12–14 October 2016; pp. 120–125. [CrossRef]
19. Van, N.T.; Do, T.N.; Bao, V.N.Q.; An, B. Performance Analysis of Wireless Energy Harvesting Multihop Cluster-Based Networks Over Nakagami-*m* Fading Channels. *IEEE Access* **2018**, *6*, 3068–3084. [CrossRef]
20. Shim, K.; Nguyen, T.V.; An, B. Secrecy Improvement for Wireless-Powered Multihop D2D Communication in Wireless Sensors Networks. In Proceedings of the 2019 International Conference on Green and Human Information Technology (ICGHIT), Kuala Lumpur, Malaysia, 16–18 January 2019; pp. 209–214.
21. Tran, D.; Vo, N.; Vo, T.; Ha, D. Physical Layer Secrecy Performance of Multi-hop Decode-and-Forward Relay Networks with Multiple Eavesdroppers. In Proceedings of the 2015 International Conference on Advanced Information Networking and Applications Workshops (AINA), Gwangju, Korea, 25–27 March 2015; pp. 430–435. [CrossRef]
22. Lee, J. Full-Duplex Relay for Enhancing Physical Layer Security in Multi-Hop Relaying Systems. *IEEE Commun. Lett.* **2015**, *19*, 525–528. [CrossRef]
23. Shim, K.; Do, N.T.; An, B.; Nam, S. Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information. In Proceedings of the 2016 International Conference on Electronics, Information, and Communications (ICEIC), Da Nang, Vietnam, 27–30 January 2016; pp. 1–4. [CrossRef]
24. Duy, T.T.; Kong, H.Y. Secrecy Performance Analysis of Multihop Transmission Protocols in Cluster Networks. *Wirel. Pers. Commun.* **2015**, *82*, 2505 – 2518. [CrossRef]
25. Hieu, T.D.; Duy, T.T.; Kim, B. Performance Enhancement for Multihop Harvest-to-Transmit WSNs with Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises. *IEEE Sens. J.* **2018**, *18*, 5173–5186. [CrossRef]
26. Tran Tin, P.; The Hung, D.; Nguyen, T.N.; Duy, T.T.; Voznak, M. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-Hop Transmission with and without Presence of Hardware Impairments. *Entropy* **2019**, *21*, 217. [CrossRef]
27. Mo, J.; Tao, M.; Liu, Y. Relay Placement for Physical Layer Security: A Secure Connection Perspective. *IEEE Commun. Lett.* **2012**, *16*, 878–881. [CrossRef]
28. Dung, C.T.; Van, N.T.; Duy, T.T.; Bao, V.N.Q.; Nhat, N.L. Security enhancement for dual-hop RF protocols with Nth-best partial relay and EH-based jammer. In Proceedings of the 2015 International Conference on Communications, Management and Telecommunications (ComManTel), DaNang, Vietnam, 28–30 December 2015; pp. 111–115. [CrossRef]
29. Bao, V.N.Q.; Duy, T.T.; Van, N.T. Exact outage analysis of energy-harvesting multihop cluster-based networks with multiple power beacons over Nakagami-m fading channels. In Proceedings of the 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications Computing (SigTelCom), Ho Chi Minh City, Vietnam, 29–31 January 2018; pp. 1–6.
30. 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]
31. Hoang, T.M.; Duong, T.Q.; Vo, N.; Kundu, C. Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 174–177. [CrossRef]
32. Fan, L.; Yang, N.; Duong, T.Q.; Elkashlan, M.; Karagiannidis, G.K. Exploiting Direct Links for Physical Layer Security in Multiuser Multirelay Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3856–3867. [CrossRef]
33. Shim, K.; Do, N.T.; An, B. Performance Analysis of Physical Layer Security of Opportunistic Scheduling in Multiuser Multirelay Cooperative Networks. *Sensors* **2017**, *17*, 377. [CrossRef] [PubMed]
34. Choi, Y.; Kim, D. Performance analysis with and without torch node in secure communications. In Proceedings of the 2015 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 14–16 October 2015; pp. 84–87. [CrossRef]

35. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 7 January 2000. [CrossRef]
36. Park, G.Y.; Kim, H.; Jeong, H.W.; Youn, H.Y. A Novel Cluster Head Selection Method based on K-Means Algorithm for Energy Efficient Wireless Sensor Network. In Proceedings of the 2013 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, Spain, 25–28 March 2013; pp. 910–915. [CrossRef]
37. Liu, P.; Tao, Z.; Lin, Z.; Erkip, E.; Panwar, S. Cooperative wireless communications: A cross-layer approach. *IEEE Wirel. Commun.* **2006**, *13*, 84–92. [CrossRef]
38. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012); IEEE: New York, NY, USA, 2016; pp. 1–3534. [CrossRef]
39. Shim, K.; An, B. Exploiting Opportunistic Scheduling for Physical-Layer Security in Multitwo User NOMA Networks. *Wirel. Commun. Mobile Comput.* **2018**, *2018*, 2797824. [CrossRef]
40. Tang, C.; Pan, G.; Li, T. Secrecy Outage Analysis of Underlay Cognitive Radio Unit Over Nakagami-*m* Fading Channels. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 609–612. [CrossRef]
41. Gradshteyn, I.; Ryzhik, I. *Table of Integrals, Series, and Products*, 7th ed.; Academic Press: Cambridge, MA, USA, 2007.
42. Liu, T.; Lui, J.C.S.; Ma, X.; Jiang, H. Enabling Relay-Assisted D2D Communication for Cellular Networks: Algorithm and Protocols. *IEEE Internet Things* **2018**, *5*, 3136–3150. [CrossRef]
43. Gui, B.; Dai, L.; Cimini, L.J. Routing strategies in multihop cooperative networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 843–855. [CrossRef]
44. Do, N.T.; da Costa, D.B.; Duong, T.Q.; Bao, V.N.Q.; An, B. Exploiting Direct Links in Multiuser Multirelay SWIPT Cooperative Networks With Opportunistic Scheduling. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 5410–5427. [CrossRef]
45. Ding, H.; Ge, J.; da Costa, D.B.; Jiang, Z. A New Efficient Low-Complexity Scheme for Multi-Source Multi-Relay Cooperative Networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 716–722. [CrossRef]
46. Papoulis, A.; Pillai, S.U. *Probability, Random Variables, and Stochastic Processes*, 4th ed.; McGraw-Hill: New York, NY, USA, 2002.