sensors

MDPI

Article

Secrecy Performance Analysis of Cooperative Multihop Transmission for WSNs under Eavesdropping Attacks †

Yosefine Triwidyastuti [1], Ridho Hendra Yoga Perdana [1], Kyusung Shim [2] and Beongku An [3,*]

[1] Department of Software and Communications Engineering in Graduate School, Hongik University, Sejong City 30016, Republic of Korea; yosefine@mail.hongik.ac.kr (Y.T.); hendra@mail.hongik.ac.kr (R.H.Y.P.)
[2] School of Computer Engineering and Applied Mathematics, Hankyong National University, Anseong City 17579, Republic of Korea; kyusung.shim@hknu.ac.kr
[3] Department of Software and Communications Engineering, Hongik University, Sejong City 30016, Republic of Korea
* Correspondence: beongku@hongik.ac.kr
† This paper is an extended version of our paper published in Triwidyastuti, Y.; Perdana, R.H.Y.; Shim, K.; An, B. Cooperative Transmission with Friendly Jamming to Ensure Secrecy Performance. In Proceedings of the 11th International Conference on Green and Human Information Technology (ICGHIT 2023), Bangkok, Thailand, 31 January–2 February 2023; pp. 198–202.

Abstract: Multihop transmission is one of the important techniques to overcome the transmission coverage of each node in wireless sensor networks (WSNs). However, multihop transmission has a security issue due to the nature of a wireless medium. Additionally, the eavesdropper also attempts to interrupt the legitimate users' transmission. Thus, in this paper, we study the secrecy performance of a multihop transmission under various eavesdropping attacks for WSNs. To improve the secrecy performance, we propose two node selection schemes in each cluster, namely, minimum node selection (MNS) and optimal node selection (ONS) schemes. To exploit the impact of the network parameters on the secrecy performance, we derive the closed-form expression of the secrecy outage probability (SOP) under different eavesdropping attacks. From the numerical results, the ONS scheme shows the most robust secrecy performance compared with the other schemes. However, the ONS scheme requires a lot of channel information to select the node in each cluster and transmit information. On the other side, the MNS scheme can reduce the amount of channel information compared with the ONS scheme, while the MNS scheme still provides secure transmission. In addition, the impact of the network parameters on the secrecy performance is also insightfully discussed in this paper. Moreover, we evaluate the trade-off of the proposed schemes between secrecy performance and computational complexity.

Keywords: cooperative transmission; eavesdropper; multihop relay; node selection; physical layer security; secrecy outage probability

Citation: Triwidyastuti, Y.; Perdana, R.H.Y.; Shim, K.; An, B. Secrecy Performance Analysis of Cooperative Multihop Transmission for WSNs under Eavesdropping Attacks. *Sensors* **2023**, *23*, 7653. https://doi.org/10.3390/s23177653

Academic Editor: Jaime Lloret

Received: 4 August 2023
Revised: 29 August 2023
Accepted: 30 August 2023
Published: 4 September 2023

1. Introduction

The main focus of the next-generation network is on human-to-machine interactions and real-time communication by utilizing various tactile/haptic sensors and actuators that have a massive number with a small size but limited energy [1]. In 5G networks, the number of devices in a network can reach 1 million devices per square kilometer. Moreover, the connection density in 6G systems will reach 10^7 devices/km^2 [2]. However, a high density network is still prone to blockages when the destination is located in a far distance from the low-energy source, and there is no traffic distribution [3].

By using cooperative transmission, nodes in the network can be designated as relays that decode the received information from the source and retransmit the received information to the destination. Relay gives benefits to a communication network by extending its coverage, increasing the signal reception while reducing its energy consumption [4]. Due

to these advantages, cooperative transmission has been implemented in various wireless systems [5–7]. Specifically, sensor nodes in wireless sensor networks (WSNs) collect confidential and sensitive information to a gateway or server through a cooperative multihop communication [8].

In practice, WSN with cooperative transmission is widely implemented in various industries, such as disaster mitigation, vehicular network, and battlefield. Security has become the main issue for the large-scale application of WSNs [9]. Due to the broadcast nature of wireless nodes, illegitimate users can easily wiretap data transmission. An eavesdropper can disconnect the transmission between sensor nodes or send a wrong message and cause an error. In multihop WSN where intermediate nodes directly access the message and retransmit it to the next hop, the end-to-end security for confidential messages is difficult to achieve if there is no countermeasure in the data transmission [10].

A higher number of nodes that relay confidential information can surely reach the destination in a more remote area, but it is also more susceptible to eavesdropping attack [11]. An illegitimate node that is located within the relays' wireless range can overhear the broadcast messages [12]. The illegitimate node that only overhears the main channel transmission is known as a passive eavesdropper. On the other side, when the illegitimate node simultaneously transmits a jamming signal while overhearing the main channel transmission, it is known as an active eavesdropper and more advanced than a passive eavesdropper [13].

There are several considerable techniques to overcome an eavesdropper. The well-known technique is using data encryption in the network's application layer. However, encryption needs careful key management and distribution in the source node and destination node. Encryption can also be deciphered by brute-force computing in an advanced eavesdropper node [14]. The new emerging technique for overcoming an eavesdropper is physical layer security (PLS), which exploits communications' medium information to either enhance the main channel capacity, reduce the eavesdropper capacity, or both [15].

In this paper, we exploit the impact of secrecy performance on various eavesdropping attacks in multihop transmission. To enhance the secrecy performance, we propose two node selection schemes. The first node selection scheme can select the node in each cluster to minimize the eavesdropper channel. The second node selection scheme can select the node in each cluster to maximize the secrecy capacity. The main contributions of this paper can be summarized as follows:

- We exploit the impact of different eavesdropping attacks on the secure multihop transmission for WSNs. More specifically, in the passive eavesdropping attack, the eavesdropper only overhears legitimate users' transmission. Different from the passive eavesdropping attack, the active eavesdropping attack can overhear each hop transmission and radiate the jamming signal to reduce the main channel condition at the same time. This scenario has not been studied in this literature.
- To enhance the secrecy performance, we propose two node selection schemes. The first scheme can select the node that minimizes the eavesdropper channel gains, called the minimal node selection (MNS) scheme. The second scheme, namely, the optimal node selection (ONS) scheme, can maximize the secrecy capacity of each cluster. We also consider the random node selection (RNS) scheme, which randomly selects the node in each cluster as a benchmark to compare the secrecy performance with the proposed schemes in a multicluster network.
- In order to find the relation between the system parameters and the secrecy performance, we derive a closed-form expression of the secrecy outage probability (SOP) with different eavesdropping attacks and the proposed node selection schemes. Specifically, we obtain the end-to-end SOP as the function of the number of clusters, number of nodes, target secrecy rate, main channel transmit SNR, and eavesdropper jamming SNR.
- From the numerical results, the active eavesdropper seriously affects secrecy performance compared with that of a passive eavesdropping attack. Additionally, ONS

outperforms RNS and MNS secrecy performance in terms of SOP, while ONS requires a huge amount of channel information compared with that of other schemes.

The rest of this paper is organized as follows: Section 2 exploits previous works that motivate this research. Section 3 describes the system model of the proposed multihop relaying network, along with the passive and active scenarios of an eavesdropper attack and three node selection schemes. Section 4 analyzes the closed-form function of the system's SOP for all cases as the combination of eavesdropper scenarios and node selection schemes. Section 5 presents the numerical results obtained from the derived analysis and simulations. Finally, Section 6 concludes the paper.

2. Related Works

Studies on PLS mostly focus on three main strategies: optimized resource allocation, secure beamforming/precoding, and antenna/node selection [16]. Duo et al. proposed joint UAV trajectory and power control optimization for securing UAV communications [17]. However, finding an optimal resource allocation in a wireless network is a complicated task that needs a strategic game to formulate the interactions between all nodes. Wang et al. obtained a Stackelberg equilibrium in multiantenna cellular networks through an iterative algorithm [18]. Luo and Yang in [19] formulated the cooperation between cellular user, D2D user, and active eavesdropper as a secrecy antijamming game. Moreover, Luo et al. in [20] considered a multitier Stackelberg game to model the complex interaction among the nodes.

Regarding secure beamforming in PLS, Lin et al. investigated three different hybrid beamforming architectures to maximize the joint secrecy performance and energy efficiency in satellite–terrestrial integrated networks (STIN) [21]. Furthermore, the authors in [22–24] considered joint beamforming and optimization for cooperative STIN transmission. However, since the optimization problem is mathematically intractable, the beamforming strategy needs an iterative algorithm.

In the field of precoding strategy in PLS, Liu et al. employed a source with multiantennas to transmit artificial noise (AN) and information signals as secure precoding in an unmanned aerial vehicle (UAV) network [25]. The authors in [26] sent AN via random and null-space precoders from a massive MIMO base station. Meanwhile, the authors in [27,28] applied cooperative jamming from a multiantenna relay and source to overcome an active eavesdropper. In addition, the authors in [29] used another user in z satellite–terrestrial network as a friendly jammer. However, cooperative jamming requires an additional antenna/node and precoders to transmit the jamming signal aside from the information signal.

In a high-density network, a node selection strategy becomes the common technique to secure the cooperative transmission. The authors in [30–32] implemented relay selection to overcome an active eavesdropper, but only in dual-hop transmissions. On the other hand, a multihop network with a larger number of nodes makes the node selection process more complex. Shim et al. studied node selection for a source cluster and relay cluster in [33], while in [34], the authors utilized node selection for a multihop relaying network with power beacons. However, these two studies only studied the secrecy performance under a passive eavesdropper attack, while an active eavesdropper is more destructive to the system performance than a passive eavesdropper.

The authors in [35] proposed a node selection scheme to improve the end-to-end throughput without an eavesdropping attack. The authors in [36] proposed a train-to-train multihop transmission and next relay selection scheme. However, this work did not consider an eavesdropping attack. In [37], the authors exploited the outage performance for short packet communication in a multihop transmission with wireless energy transfer. This work also did not consider an eavesdropping attack. As can be observed, in the multihop transmission context, the improvements of secrecy performance and system throughput are studied. However, the study of a secure multihop transmission under active eavesdropping using a node selection strategy has not been conducted yet.

Different from previous works in [34–37] that studied various strategies to improve multihop transmission performance without considering an active eavesdropper attack, we propose a cooperative multihop relaying network in confronting a passive and active eavesdropper using node selection schemes. Other works in [30–32] only studied the secrecy performance of a dual-hop transmission under active eavesdropping attacks, while with the higher number of node clusters, the end-to-end security is harder to be deployed in multicluster WSNs [10].

3. System Model

3.1. System Description

Let us consider a multihop transmission in WSN consisting of K clusters with N nodes in every cluster, as depicted in Figure 1. The desired source (i-th node) in the first cluster ($\mathsf{R}_{1,i}$) transmits confidential information to a destination (D) through $K-1$ clusters of relay (R) as the main channel of cooperative transmission. We assume that all nodes in the main channel transmission have a single antenna. Meanwhile, the eavesdropper can overhear the legitimate users' transmission. If the eavesdropper is operated on the passive mode, the eavesdropper only wiretaps the confidential message since the eavesdropper is equipped with a single antenna. However, when the eavesdropper is operated on the active mode, the eavesdropper wiretaps the confidential message and radiates the jamming signal by using two antennas at the same time. In this paper, we exploit the impact of two eavesdropping "scenarios", called passive and active. Additionally, we propose node selection "schemes" to improve the system secrecy.

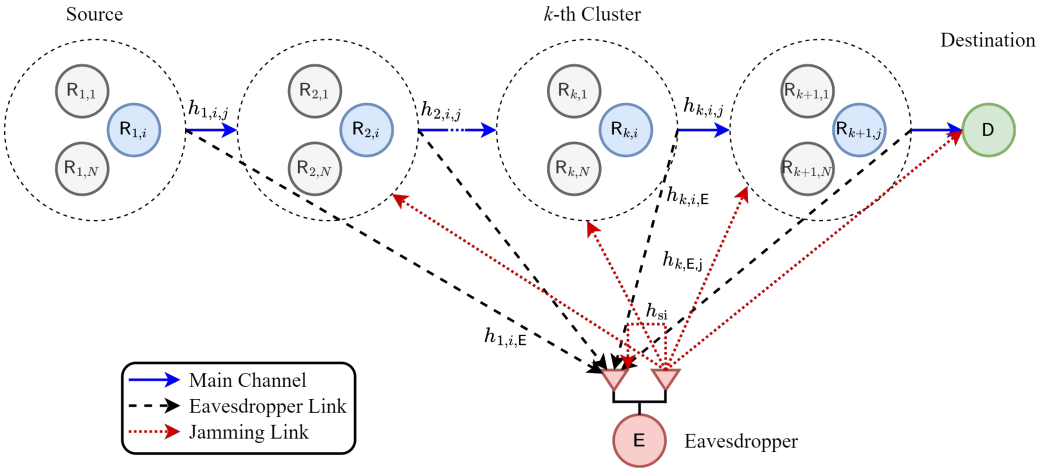

Figure 1. The proposed system model of the multihop transmission.

3.2. Scenario 1—Passive Eavesdropper

The received signal from the i-th node in the k-th cluster ($\mathsf{R}_{k,i}$) at the j-th node in the next cluster ($\mathsf{R}_{k+1,j}$) with a passive eavesdropper can be described as

$$y_{k,i,j}^{\text{pas}} = \sqrt{P_{k,i}} h_{k,i,j} x_{k,i} + n_{k+1,j}, \tag{1}$$

where $x_{k,i}$ and $P_{k,i}$ denote the transmit signal and power at the i-th node in the k-th cluster, respectively. $h_{k,i,j}$ denotes the channel coefficient of the $\mathsf{R}_{k,i} \rightarrow \mathsf{R}_{k+1,j}$ link. The channel noise at $\mathsf{R}_{k+1,j}$ is denoted by $n_{k+1,j}$ as an additive white Gaussian noise (AWGN) model with zero mean and variance $\sigma_{k+1,j}^2$. The signal-to-noise ratio (SNR) of the main channel at the k-th hop under a passive eavesdropper attack can be described as

$$\gamma_{k,i,j}^{\text{pas}} = \frac{P_{k,i}|h_{k,i,j}|^2}{\sigma_{k+1,j}^2}. \tag{2}$$

The received signal at E that only overhears the k-th hop data transmission can be expressed as

$$y_{k,i,\mathsf{E}}^{\text{pas}} = \sqrt{P_{k,i}} h_{k,i,\mathsf{E}} x_{k,i} + n_{\mathsf{E}}, \tag{3}$$

where $h_{k,i,\mathsf{E}}$ indicates the channel coefficient of the $\mathsf{R}_{k,i} \rightarrow \mathsf{E}$ link. n_{E} indicates the channel noise at E with an AWGN model and variance σ_{E}^2. The SNR of the eavesdropper link with a passive mode at the k-th hop can be expressed as

$$\gamma_{k,i,\mathsf{E}}^{\text{pas}} = \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sigma_{\mathsf{E}}^2}. \tag{4}$$

3.3. Scenario 2—Active Eavesdropper

In the active attack, the received signal at the k-th hop data transmission is interfered by the jamming signal from E, which can be described as

$$y_{k,i,j}^{\text{act}} = \underbrace{\sqrt{P_{k,i}} h_{k,i,j} x_{k,i}}_{\text{information}} + \underbrace{\sqrt{P_{\mathsf{E}}} h_{k,\mathsf{E},j} x_{\mathsf{E}}}_{\text{interference}} + \underbrace{n_{k+1,j}}_{\text{noise}}, \tag{5}$$

where $h_{k,\mathsf{E},\mathsf{j}}$ denotes the channel coefficient of the $\mathsf{E} \rightarrow \mathsf{R}_{k+1,j}$ link. The jamming signal and power from E are denoted by x_{E} and P_{E}, respectively. The signal-to-interference-plus-noise ratio (SINR) of the main channel at the k-th hop can be described as

$$\gamma_{k,i,j}^{\text{act}} = \frac{P_{k,i}|h_{k,i,j}|^2}{P_{\mathsf{E}}|h_{k,\mathsf{E},j}|^2 + \sigma_{k+1,j}^2}. \tag{6}$$

At E, the received signal is affected by the noise of the channel link and the self-interference (SI) from its jamming signal. The received signal at E can be expressed as

$$y_{k,i,\mathsf{E}}^{\text{act}} = \underbrace{\sqrt{P_{k,i}} h_{k,i,\mathsf{E}} x_{k,i}}_{\text{information}} + \underbrace{\sqrt{P_{\mathsf{E}}} h_{\mathsf{si}} x_{\mathsf{E}}}_{\text{self-interference}} + \underbrace{n_{\mathsf{E}}}_{\text{noise}}, \tag{7}$$

where h_{si} indicates the channel coefficient of the SI link. After different stages of mitigation, the residual SI (RSI) can be decreased to the noise level [38]. The observation with an RSI component at E can be expressed as

$$y_{k,i,\mathsf{E}}^{\text{RSI,act}} = \sqrt{P_{k,i}} h_{k,i,\mathsf{E}} x_{k,i} + n_{\mathsf{si}} + n_{\mathsf{E}}. \tag{8}$$

The SINR of the active eavesdropper at the k-th hop transmission can be expressed as

$$\gamma_{k,i,\mathsf{E}}^{\text{act}} = \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sigma_{\mathsf{si}}^2 + \sigma_{\mathsf{E}}^2}. \tag{9}$$

3.4. The Proposed Node Selection Scheme

3.4.1. Random Node Selection (RNS) Scheme

In this scheme, RNS selects a relay node randomly in each cluster without considering the channel information in every node. The SNR of the k-th hop main channel transmission with RNS and a passive eavesdropper can be described as

$$\gamma_{k,i^*,j*}^{\text{RNS,pas}} = \frac{P_{k,i}|h_{k,i,j}|^2}{\sigma_{k+1,j}^2}. \tag{10}$$

Meanwhile, the SNR of the passive eavesdropper link at the k-th hop can be written as

$$\gamma_{k,i^*,\mathsf{E}}^{\mathrm{RNS,pas}} = \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sigma_{\mathsf{E}}^2}. \tag{11}$$

The SINR of the k-th hop main channel transmission with RNS and an active eavesdropper can be described as

$$\gamma_{k,i^*,j*}^{\mathrm{RNS,act}} = \frac{P_{k,i}|h_{k,i,j}|^2}{P_{\mathsf{E}}|h_{k,\mathsf{E},j}|^2 + \sigma_{k+1,j}^2}. \tag{12}$$

Meanwhile, the SINR of the active eavesdropper link at the k-th hop can be written as

$$\gamma_{k,i^*,\mathsf{E}}^{\mathrm{RNS,act}} = \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sigma_{\mathrm{si}}^2 + \sigma_{\mathsf{E}}^2}. \tag{13}$$

We consider this scheme as a benchmark to compare the performance result with the following proposed schemes.

3.4.2. Minimum Node Selection (MNS) Scheme

We propose a minimum selection process to select a relay node in every cluster. The selection criteria of the node with the minimum eavesdropper's channel gain can be expressed as

$$\mathsf{R}_{k,i^*}^{\mathrm{MNS}} = \arg \min_{1 \le i \le N} \left\{ |h_{k,i,\mathsf{E}}|^2 \right\}. \tag{14}$$

The SNR of the k-th hop main channel transmission with minimum selection in the presence of a passive eavesdropper can be expressed as

$$\gamma_{k,i^*,j^*}^{\mathrm{MNS,pas}} = \frac{P_{k,i^*}|h_{k,i^*,j^*}|^2}{\sigma_{k+1,j^*}^2}, \tag{15}$$

where j^* denotes the selected node that has already chosen in the next hop. On the other side, the SNR of the passive eavesdropper link at the k-th hop becomes

$$\gamma_{k,i^*,\mathsf{E}}^{\mathrm{MNS,pas}} = \frac{P_{k,i} \min_{1 \le i \le N} \{|h_{k,i,\mathsf{E}}|^2\}}{\sigma_{\mathsf{E}}^2}. \tag{16}$$

The SINR of the k-th hop main channel transmission with minimum selection and an active eavesdropper can be expressed as

$$\gamma_{k,i^*,j^*}^{\mathrm{MNS,act}} = \frac{P_{k,i^*}|h_{k,i^*,j^*}|^2}{P_{\mathsf{E}}|h_{k,\mathsf{E},j^*}|^2 + \sigma_{k+1,j^*}^2}. \tag{17}$$

Meanwhile, the SINR of the active eavesdropper link at the k-th hop becomes

$$\gamma_{k,i^*,\mathsf{E}}^{\mathrm{MNS,act}} = \frac{P_{k,i} \min_{1 \le i \le N} \{|h_{k,i,\mathsf{E}}|^2\}}{\sigma_{\mathrm{si}}^2 + \sigma_{\mathsf{E}}^2}. \tag{18}$$

3.4.3. Optimal Node Selection (ONS) Scheme

In this selection process, we select the relay node in every cluster that can maximize the secrecy capacity of the system. The main and eavesdropper channels are both considered in an optimal selection process, which can be described by

$$\mathsf{R}_{k,i^*}^{\mathrm{ONS}} = \arg \max_{1 \le i \le N} \left\{ \log_2 \left(\frac{1 + \gamma_{k,i,j^*}}{1 + \gamma_{k,i,\mathsf{E}}} \right) \right\}. \tag{19}$$

The SNR of the k-th hop main channel transmission with ONS in the presence of a passive eavesdropper can be written as

$$\gamma_{k,i^*,j^*}^{\text{ONS,pas}} = \frac{P_{k,i}|h_{k,i,j^*}|^2}{\sigma_{k+1,j^*}^2}. \tag{20}$$

In addition, the SNR of the passive eavesdropper link at the k-th hop can be expressed as

$$\gamma_{k,i^*,\mathsf{E}}^{\text{ONS,pas}} = \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sigma_{\mathsf{E}}^2}. \tag{21}$$

The SINR of the k-th hop main channel transmission with ONS in the presence of an active eavesdropper can be written as

$$\gamma_{k,i^*,j*}^{\text{ONS,act}} = \frac{P_{k,i}|h_{k,i,j^*}|^2}{P_{\mathsf{E}}|h_{k,\mathsf{E},j^*}|^2 + \sigma_{k+1,j^*}^2}. \tag{22}$$

Lastly, the SINR of the active eavesdropper link at the k-th hop can be expressed as

$$\gamma_{k,i^*,\mathsf{E}}^{\text{ONS,act}} = \frac{P_{k,i}|h_{k,i,\mathsf{E}}|^2}{\sigma_{\text{si}}^2 + \sigma_{\mathsf{E}}^2}. \tag{23}$$

As can be seen, the SNR models with the proposed scheme and with passive eavesdropping are similar to the well-known selection scheme. However, as can be seen in (17), (18), (22) and (23), the SINR models with the proposed scheme and with an active eavesdropping attack are different since they have a jamming signal, which cause the derivation complexity that is very challenging. Thus, the proposed node selection schemes still have novel contributions.

4. Secrecy Outage Performance Analysis

The system's secrecy outage probability (SOP) is defined as the probability in which the system secrecy capacity is less than the target secrecy rate (R_{th}), which can be written as

$$P_{\text{SOP}}^{\text{case}} = \Pr\left(\frac{1}{K}\min_{1\le k\le K}\log_2\left(\frac{1+\gamma_{k,i^*,j^*}^{\text{case}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\text{case}}}\right) < R_{\text{th}}\right), \tag{24}$$

where case $\in \{\text{c1}, \text{c2}, \text{c3}, \text{c4}, \text{c5}, \text{c6}\}$. The SOP of the system is associated with the probability that the system cannot securely decode the information [39]. In other words, part of the secret information can be decoded by an eavesdropper. The SOP analysis of the proposed schemes will be presented in six different cases as the combination of the selection scheme and eavesdropper scenario that is shown in Table 1.

Table 1. Selection and scenario combinations.

Case	Node Selection Scheme	Eavesdropper Scenario
Case I (c1)	RNS	passive
Case II (c2)	RNS	active
Case III (c3)	MNS	passive
Case IV (c4)	MNS	active
Case V (c5)	ONS	passive
Case VI (c6)	ONS	active

We assume that all channels in the system undergo Rayleigh fading, in which the channel gain from X to Y ($|h_{\mathsf{XY}}|^2$) follows an exponential distribution with mean $\lambda_{\mathsf{XY}} = (d_{\mathsf{XY}}/d_0)^{-\epsilon}$. d_{XY} denotes the Euclidean distance between X and Y, while d_0 represents the reference distance, and ϵ represents the path-loss exponent. For convenience, we define

the channel gains as $X_{k,i,j} \triangleq |h_{k,i,j}|^2$, $Y_{k,i,\mathsf{E}} \triangleq |h_{k,i,\mathsf{E}}|^2$, and $Z_{k,\mathsf{E},j} \triangleq |h_{k,\mathsf{E},j}|^2$. Without loss of generality, we assume $P_{k,i} = P_{\mathsf{R}}$ and $\sigma^2_{k+1,j} = \sigma^2_{\mathsf{E}} = \sigma^2_{\mathsf{si}} = \sigma^2$. We can further suppose $\gamma_{\mathsf{R}} = P_{\mathsf{R}}/\sigma^2$ and $\gamma_{\mathsf{E}} = P_{\mathsf{E}}/\sigma^2$.

4.1. Case I: Random Node Selection Scheme under Passive Eavesdropper

From (24), the SOP with case I can be further written as

$$P^{\mathrm{c1}}_{\mathrm{SOP}} = 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{1+\gamma^{\mathrm{RNS,pas}}_{k,i^*,j^*}}{1+\gamma^{\mathrm{RNS,pas}}_{k,i^*,\mathsf{E}}} < \gamma_{\mathrm{th}}\right)\right], \tag{25}$$

where $\gamma_{\mathrm{th}} = 2^{KR_{\mathrm{th}}}$. By relying on the channel characteristic of each link with an RNS scheme, the SOP with case I can be rewritten as

$$\begin{aligned} P^{\mathrm{c1}}_{\mathrm{SOP}} &= 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{1+\gamma_{\mathsf{R}}X_{k,i,j}}{1+\gamma_{\mathsf{R}}Y_{k,i,\mathsf{E}}} < \gamma_{\mathrm{th}}\right)\right] \\ &= 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(X_{k,i,j} < \frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}} + \gamma_{\mathrm{th}}Y_{k,i,\mathsf{E}}\right)\right]. \end{aligned} \tag{26}$$

In order to further calculate $P^{\mathrm{c1}}_{\mathrm{SOP}}$, (26) can be re-expressed as

$$P^{\mathrm{c1}}_{\mathrm{SOP}} = 1 - \prod_{k=1}^{K}\Bigg[1 - \underbrace{\int_0^{\infty} F_{X_{k,i,j}}\left(\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}} + \gamma_{\mathrm{th}}y\right) f_{Y_{k,i,\mathsf{E}}}(y)dy}_{\Psi}\Bigg]. \tag{27}$$

Ψ in (27) can be rewritten as

$$\begin{aligned} \Psi &= \int_0^{\infty}\left[1 - \exp\left(-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}} + \gamma_{\mathrm{th}}y\right)\right)\right]\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{1}{\lambda_{k,i,\mathsf{E}}}y\right)dy \\ &= \underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{y}{\lambda_{k,i,\mathsf{E}}}\right)dy}_{\Psi_{1a}} - \exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right)\underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{\gamma_{\mathrm{th}}y}{\lambda_{k,i,j}} - \frac{y}{\lambda_{k,i,\mathsf{E}}}\right)dy}_{\Psi_{1b}}. \end{aligned} \tag{28}$$

Relying on the fact [40] (Equation 3.310), i.e., $\int_0^{\infty} e^{-px}dx = 1/p$, Ψ_{1a} and Ψ_{1b} can be, respectively, re-expressed as

$$\Psi_{1a} = \int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{1}{\lambda_{k,i,\mathsf{E}}}y\right)dy = 1, \tag{29}$$

$$\Psi_{1b} = \int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\left(\frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}} + \frac{1}{\lambda_{k,i,\mathsf{E}}}\right)y\right)dy = \frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + \lambda_{k,i,j}}. \tag{30}$$

By plugging Ψ_{1a} and Ψ_{1b} into (28), Ψ can be further expressed as

$$\Psi = 1 - \frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + \lambda_{k,i,j}}\exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right). \tag{31}$$

By substituting (31) into (27) and after some mathematical steps, the closed-form expression for the SOP under case I can be obtained as

$$P^{\mathrm{c1}}_{\mathrm{SOP}} = 1 - \prod_{k=1}^{K}\left[\frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + \lambda_{k,i,j}}\exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right)\right]. \tag{32}$$

4.2. Case II: Random Node Selection Scheme under Active Eavesdropper

The SOP under case II can be further written as

$$P_{\mathrm{SOP}}^{\mathrm{c2}} = 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{1+\gamma_{k,i^*,j^*}^{\mathrm{RNS,act}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\mathrm{RNS,act}}} < \gamma_{\mathrm{th}}\right)\right]. \tag{33}$$

From (12) and (13), the SOP of case II can be rewritten as

$$\begin{aligned} P_{\mathrm{SOP}}^{\mathrm{c2}} =& 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{1+\frac{\gamma_{\mathsf{R}}X_{k,i,j}}{\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j}+1}}{1+\frac{\gamma_{\mathsf{R}}Y_{k,i,\mathsf{E}}}{2}} < \gamma_{\mathrm{th}}\right)\right] \\ =& 1 - \prod_{k=1}^{K}\Bigg[1 - \underbrace{\Pr\left(\frac{\gamma_{\mathsf{R}}X_{k,i,j}}{\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j}+1} < (\gamma_{\mathrm{th}}-1) + \frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{R}}Y_{k,i,\mathsf{E}}}{2}\right)}_{\Phi}\Bigg]. \end{aligned} \tag{34}$$

Φ in (34) can be re-expressed as

$$\begin{aligned} \Phi =& \Pr\left(X_{k,i,j} < \frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}Z_{k,E,j}+1)}{\gamma_{\mathsf{R}}} + \frac{\gamma_{\mathrm{th}}Y_{k,i,\mathsf{E}}(\gamma_{\mathsf{E}}Z_{k,E,j}+1)}{2}\right) \\ =& \int_0^{\infty}\underbrace{\int_0^{\infty} F_{X_{k,i,j}}\left(\frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}z+1)}{\gamma_{\mathsf{R}}} + \frac{\gamma_{\mathrm{th}}y(\gamma_{\mathsf{E}}z+1)}{2}\right) f_{Y_{k,i,\mathsf{E}}}(y)dy}_{\Phi_1} f_{Z_{k,\mathsf{E},j}}(z)dz. \end{aligned} \tag{35}$$

Φ_1 in (35) can be rewritten as

$$\begin{aligned} \Phi_1 =& \int_0^{\infty}\left[1 - \exp\left(-\frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}z+1)}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} - \frac{\gamma_{\mathrm{th}}y(\gamma_{\mathsf{E}}z+1)}{2\lambda_{k,i,j}}\right)\right]\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{1}{\lambda_{k,i,\mathsf{E}}}y\right)dy \\ =& \underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{1}{\lambda_{k,i,\mathsf{E}}}y\right)dy}_{\Phi_{1a}} \\ & - \exp\left(-\frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}z+1)}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right)\underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\left(\frac{1}{\lambda_{k,i,\mathsf{E}}} + \frac{\gamma_{\mathrm{th}}(\gamma_{\mathsf{E}}z+1)}{2\lambda_{k,i,j}}\right)y\right)dy}_{\Phi_{1b}}. \end{aligned} \tag{36}$$

In order to further calculate Φ_1, we rely on the fact [40] (Equation 3.310). Φ_{1a} and Φ_{1b} in (36) can be, respectively, obtained as

$$\Phi_{1a} = \frac{1}{\lambda_{k,i,\mathsf{E}}}\int_0^{\infty}\exp\left(-\frac{1}{\lambda_{k,i,\mathsf{E}}}y\right)dy = \frac{1}{\lambda_{k,i,\mathsf{E}}}\lambda_{k,i,\mathsf{E}} = 1, \tag{37}$$

$$\begin{aligned} \Phi_{1b} =& \int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\left(\frac{2\lambda_{k,i,j}+\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}(\gamma_{\mathsf{E}}z+1)}{\lambda_{k,i,\mathsf{E}}2\lambda_{k,i,j}}\right)y\right)dy \\ =& \frac{2\lambda_{k,i,j}}{2\lambda_{k,i,j}+\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}(\gamma_{\mathsf{E}}z+1)}. \end{aligned} \tag{38}$$

Plugging Φ_{1a} and Φ_{1b} into Φ_1, (36) can be rewritten as

$$\Phi_1 = 1 - \frac{2\lambda_{k,i,j}}{2\lambda_{k,i,j}+\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}(\gamma_{\mathsf{E}}z+1)}\exp\left(-\frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}z+1)}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right). \tag{39}$$

By substituting Φ_1 into (35) and after some algebraic steps, Φ can be further expressed as

$$\begin{aligned}\Phi &= \int_0^\infty \left[1 - \frac{2\lambda_{k,i,j}}{2\lambda_{k,i,j} + \gamma_{\text{th}}\lambda_{k,i,\text{E}}(\gamma_\text{E} z + 1)} \exp\left(-\frac{(\gamma_{\text{th}} - 1)(\gamma_\text{E} z + 1)}{\gamma_\text{R}\lambda_{k,i,j}}\right)\right] \\ &\quad \times \frac{1}{\lambda_{k,\text{E},j}} \exp\left(-\frac{1}{\lambda_{k,\text{E},j}} z\right) dz \\ &= \underbrace{\int_0^\infty \frac{1}{\lambda_{k,\text{E},j}} \exp\left(-\frac{1}{\lambda_{k,\text{E},j}} z\right) dz}_{\Phi_{2a}} - \frac{1}{\lambda_{k,\text{E},j}} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_\text{R}\lambda_{k,i,j}}\right) \\ &\quad \times \underbrace{\int_0^\infty \frac{2\lambda_{k,i,j}}{2\lambda_{k,i,j} + \gamma_{\text{th}}\lambda_{k,i,\text{E}} + \gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}} z} \exp\left(-\frac{(\gamma_{\text{th}} - 1)\gamma_\text{E} z}{\gamma_\text{R}\lambda_{k,i,j}} - \frac{z}{\lambda_{k,\text{E},j}}\right) dz}_{\Phi_{2b}}.\end{aligned} \tag{40}$$

In order to further express Φ, we rely on the fact [40] (Equation 3.310) and [40] (Equation 3.352.4). Φ_{2a} and Φ_{2b} in (40) can be, respectively, obtained as

$$\Phi_{2a} = \frac{1}{\lambda_{k,\text{E,j}}} \int_0^\infty \exp\left(-\frac{1}{\lambda_{k,\text{E,j}}} z\right) dz = \frac{1}{\lambda_{k,\text{E,j}}} \lambda_{k,\text{E,j}} = 1, \tag{41}$$

$$\begin{aligned}\Phi_{2b} &= \frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}}} \int_0^\infty \frac{1}{\frac{2\lambda_{k,i,j} + \gamma_{\text{th}}\lambda_{k,i,\text{E}}}{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}}} + z} \exp\left(-\left(\frac{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,\text{E},j} - \gamma_\text{E}\lambda_{k,\text{E},j} + \gamma_\text{R}\lambda_{k,i,j}}{\gamma_\text{R}\lambda_{k,i,j}\lambda_{k,\text{E},j}}\right) z\right) dz \\ &= -\frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}}} \exp\left(\beta_k\mu_k\right) \text{Ei}(-\beta_k\mu_k),\end{aligned} \tag{42}$$

where $\beta_k = \frac{2\lambda_{k,i,j} + \gamma_{\text{th}}\lambda_{k,i,\text{E}}}{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}}}$, $\mu_k = \frac{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,\text{E},j} - \gamma_\text{E}\lambda_{k,\text{E},j} + \gamma_\text{R}\lambda_{k,i,j}}{\gamma_\text{R}\lambda_{k,i,j}\lambda_{k,\text{E},j}}$, and Ei(.) mean the exponential integral function [40] (Equation 8.211.1). Again, plugging Φ_{2a} and Φ_{2b} into (40), Φ can be obtained as

$$\Phi = 1 + \frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}}\lambda_{k,\text{E},j}} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_\text{R}\lambda_{k,i,j}} + \beta_k\mu_k\right) \text{Ei}(-\beta_k\mu_k). \tag{43}$$

After some algebraic steps, the closed-form expression for the SOP under case II ($P_{\text{SOP}}^{\text{c2}}$) can be obtained as

$$P_{\text{SOP}}^{\text{c2}} = 1 - \prod_{k=1}^{K} \left[-\frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_\text{E}\lambda_{k,i,\text{E}}\lambda_{k,\text{E},j}} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_\text{R}\lambda_{k,i,j}} + \beta_k\mu_k\right) \text{Ei}(-\beta_k\mu_k)\right]. \tag{44}$$

4.3. Case III: Minimal Node Selection with Passive Eavesdropper

The SOP with case III can be further written as

$$P_{\text{SOP}}^{\text{c3}} = 1 - \prod_{k=1}^{K} \left[1 - \Pr\left(\frac{1 + \gamma_{k,i^*,j^*}^{\text{MNS,pas}}}{1 + \gamma_{k,i^*,\text{E}}^{\text{MNS,pas}}} < \gamma_{\text{th}}\right)\right]. \tag{45}$$

From (15) and (16), the SOP under case III can be rewritten as

$$\begin{aligned}P_{\text{SOP}}^{\text{c3}} &= 1 - \prod_{k=1}^{K} \left[1 - \Pr\left(\frac{1 + \gamma_\text{R} X_{k,i^*,j^*}}{1 + \gamma_\text{R} Y_{k,i^*,\text{E}}} < \gamma_{\text{th}}\right)\right] \\ &= 1 - \prod_{k=1}^{K} \left[1 - \underbrace{\Pr\left(X_{k,i^*,j^*} < \frac{\gamma_{\text{th}} - 1}{\gamma_\text{R}} + \gamma_{\text{th}} Y_{k,i^*,\text{E}}\right)}_{\Omega}\right].\end{aligned} \tag{46}$$

As can be seen, the events of the probability (46) are not mutually exclusive since it includes $Y_{k,i^*,\mathsf{E}}$. Therefore, by conditioning $Y_{k,i^*,\mathsf{E}} = y$, Ω in (46) can be re-expressed as

$$\begin{aligned}\Omega &= \int_0^\infty \Pr\left(X_{k,i^*,j^*} < \frac{\gamma_{\text{th}} - 1}{\gamma_{\mathsf{R}}} + \gamma_{\text{th}} y\right) f_{Y_{k,i^*,\mathsf{E}}}(y)dy \\ &= \int_0^\infty \sum_{i=1}^{N} \Pr(i = i^*) \Pr\left(X_{k,i,j^*} < \frac{\gamma_{\text{th}} - 1}{\gamma_{\mathsf{R}}} + \gamma_{\text{th}} y\right) f_{Y_{k,i^*,\mathsf{E}}}(y)dy.\end{aligned} \tag{47}$$

The following lemmas will help to further calculate $P_{\text{SOP}}^{\text{sc3}}$. First, Lemma 1 helps to obtain the probability of one relay node, which is selected inside a cluster.

Lemma 1. *The probability of one node selected among N nodes can be expressed as*

$$\Pr(i^* = i) = \frac{1}{N}. \tag{48}$$

Proof. The probability of a node selected based on the criteria in (14) can be expressed as

$$\begin{aligned}\Pr\left(\mathsf{R}_{k,i^*} = \mathsf{R}_{k,i}\right) &= \Pr\left(\min_{m \in N_k} \{|h_{k,m,j}|^2\} > |h_{k,i,j}|^2\right) \\ &= \Pr\left(\bigcap_{m=1, m\neq i}^{N} \left(|h_{k,m,j}|^2 > |h_{k,i,j}|^2\right)\right).\end{aligned} \tag{49}$$

By conditioning $|h_{k,i,j}|^2 = w$ and assuming that nodes are independent, we can calculate the probability as

$$\begin{aligned}\Pr\left(\mathsf{R}_{k,i^*} = \mathsf{R}_{k,i}\right) &= \int_0^\infty \Pr\left(\bigcap_{m=1, m\neq i}^{N} \left(|h_{k,m,j}|^2 > w\right)\right) f_{|h_{k,i,j}|^2}(w)dw \\ &= \int_0^\infty \prod_{m=1, m\neq i}^{N} \left[1 - \Pr\left(|h_{k,m,j}|^2 < w\right)\right] f_{|h_{k,i,j}|^2}(w)dw \\ &= \int_0^\infty \frac{1}{\lambda_{k,i,j}} \exp\left(-\frac{Nw}{\lambda_{k,i,j}}\right) dw.\end{aligned} \tag{50}$$

Using [40] (Equation 3.310), we can obtain the probability of a node selected as in (48). The proof of Lemma 1 is concluded. □

The statistical characteristic of the channel gain from the selected node to the next hop will be presented in the following lemma.

Lemma 2. *Given the selected node* R_{k,i^*}*, the CDF and pdf of* $|h_{k,i,j^*}|^2$ *can be, respectively, expressed as*

$$F_{|h_{k,i,j^*}|^2}(x) = 1 - \exp\left(-\frac{x}{\lambda_{k,i,j}}\right), \tag{51}$$

$$f_{|h_{k,i,j^*}|^2}(x) = \frac{1}{\lambda_{k,i,j}} \exp\left(-\frac{x}{\lambda_{k,i,j}}\right). \tag{52}$$

Proof. Using the total probability theory, the CDF of $|h_{k,i,j^*}|^2$ can be written as

$$F_{|h_{k,i,j^*}|^2}(x) = \sum_{i=1}^{N} \Pr\left(\mathsf{R}_{k,i^*} = \mathsf{R}_{k,i}\right) \Pr\left(|h_{k,i,j}|^2 < x\right). \tag{53}$$

By relying on (48) in Lemma 1, (53) can be further expressed as

$$\begin{aligned} F_{|h_{k,i,j^*}|^2}(x) &= \sum_{i=1}^{N} \frac{1}{N} \Pr\left(|h_{k,i,j}|^2 < x\right) \\ &= 1 - \exp\left(-\frac{x}{\lambda_{k,i,j}}\right). \end{aligned} \tag{54}$$

After some mathematical steps, the pdf of $|h_{k,i,j^*}|^2$ can be obtained as in (52). The proof of Lemma 2 is concluded. □

Since the MNS scheme at every hop selects the node in a cluster that minimizes the eavesdropper's channel gain, the statistical characteristic of $|h_{k,i^*,\mathsf{E}}|^2$ will be presented in the following lemma.

Lemma 3. *Let* $|h_{k,i^*,\mathsf{E}}|^2 = \min_{1\le i\le N} |h_{k,i,\mathsf{E}}|^2$*; the CDF and pdf of* $|h_{k,i^*,\mathsf{E}}|^2$ *can be, respectively, expressed as*

$$F_{|h_{k,i^*,\mathsf{E}}|^2}(y) = 1 - \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y\right), \tag{55}$$

$$f_{|h_{k,i^*,\mathsf{E}}|^2}(y) = \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y\right). \tag{56}$$

Proof. From the criteria in (14), the CDF of $|h_{k,i^*,\mathsf{E}}|^2$ can be written as

$$\begin{aligned} F_{|h_{k,i^*,\mathsf{E}}|^2}(y) &= \Pr\left(\min_{1\le i\le N}\{|h_{k,i,\mathsf{E}}|^2\} < y\right) \\ &= 1 - \prod_{i=1}^{N}\Big[1 - \Pr\left(|h_{k,i,\mathsf{E}}|^2 < y\right)\Big]. \end{aligned} \tag{57}$$

Ref. (57) can be further calculated as

$$\begin{aligned} F_{|h_{k,i^*,\mathsf{E}}|^2}(y) =& 1 - \prod_{i=1}^{N}\left[1 - \left(1 - \exp\left(-\frac{y}{\lambda_{k,i,\mathsf{E}}}\right)\right)\right] \\ =& 1 - \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y\right). \end{aligned} \tag{58}$$

After some algebraic steps, the pdf of $|h_{k,i^*,\mathsf{E}}|^2$ can be obtained as in (56). The proof of Lemma 3 is concluded. □

By utilizing (48), (51), and (55), Ω in (47) can be rewritten as

$$\begin{aligned} \Omega &= \int_0^\infty \left[1 - \exp\left(-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}} + \gamma_{\mathrm{th}} y\right)\right)\right] \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y\right) dy \\ &= \underbrace{\int_0^\infty \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y\right) dy}_{\Omega_{1a}} \\ &\quad - \exp\left(-\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}} \lambda_{k,i,j}}\right) \underbrace{\int_0^\infty \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\left(\frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}} + \frac{N}{\lambda_{k,i,\mathsf{E}}}\right) y\right) dy}_{\Omega_{1b}}. \end{aligned} \tag{59}$$

Using [40] (Equation 3.310), Ω_{1a} and Ω_{1b} can be further expressed as

$$\Omega_{1a} = \int_0^{\infty} \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(- \frac{N}{\lambda_{k,i,\mathsf{E}}} y \right) dy = 1, \tag{60}$$

$$\Omega_{1b} = \int_0^{\infty} \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(- \left(\frac{\gamma_{\mathrm{th}} \lambda_{k,i,\mathsf{E}} + N\lambda_{k,i,j}}{\lambda_{k,i,j}\lambda_{k,i,\mathsf{E}}} \right) y \right) dy = \frac{N\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + N\lambda_{k,i,j}}. \tag{61}$$

After plugging (60) and (61) into (59), Ω in (59) can be further expressed as

$$\Omega = 1 - \frac{N\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + N\lambda_{k,i,j}} \exp\left(- \frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} \right). \tag{62}$$

By substituting Ω into (46) and after some mathematical calculation steps, the SOP with case III can be obtained as

$$P_{\mathrm{SOP}}^{\mathrm{c3}} = 1 - \prod_{k=1}^{K} \left[\frac{N\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + N\lambda_{k,i,j}} \exp\left(- \frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} \right) \right]. \tag{63}$$

4.4. Case IV: Minimal Node Selection with Active Eavesdropper

The SOP of the system with minimum selection in the presence of an active eavesdropper can be written as

$$\begin{aligned} P_{\mathrm{SOP}}^{\mathrm{c4}} =& 1 - \prod_{k=1}^{K} \left[1 - \Pr\left(\frac{1 + \gamma_{k,i^*,j^*}^{\mathrm{MNS,act}}}{1 + \gamma_{k,i^*,\mathsf{E}}^{\mathrm{MNS,act}}} < \gamma_{\mathrm{th}} \right) \right] \\ =& 1 - \prod_{k=1}^{K} \Bigg[1 - \underbrace{\Pr\left(\frac{\gamma_{\mathsf{R}} X_{k,i^*,j^*}}{\gamma_{\mathsf{E}} Z_{k,\mathsf{E},j^*} + 1} < (\gamma_{\mathrm{th}} - 1) + \frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{R}} Y_{k,i^*,\mathsf{E}}}{2} \right)}_{\Xi} \Bigg]. \end{aligned} \tag{64}$$

As can be seen in (64), the events of the probability (64) are not mutually exclusive since they include $Y_{k,i^*,\mathsf{E}}$. Thus, by conditioning $Y_{k,i^*,\mathsf{E}} = y$, Ξ in (64) can be further expressed as

$$\begin{aligned} \Xi =& \Pr\left(X_{k,i^*,j^*} < \frac{(\gamma_{\mathrm{th}} - 1)(\gamma_{\mathsf{E}} Z_{k,\mathsf{E},j^*} + 1)}{\gamma_{\mathsf{R}}} + \frac{\gamma_{\mathrm{th}} Y_{k,i^*,\mathsf{E}} (\gamma_{\mathsf{E}} Z_{k,\mathsf{E},j^*} + 1)}{2} \right) \\ =& \int_0^{\infty} \underbrace{\Pr\left(X_{k,i^*,j^*} < \frac{(\gamma_{\mathrm{th}} - 1)(\gamma_{\mathsf{E}} Z_{k,\mathsf{E},j^*} + 1)}{\gamma_{\mathsf{R}}} + \frac{\gamma_{\mathrm{th}} y (\gamma_{\mathsf{E}} Z_{k,\mathsf{E},j^*} + 1)}{2} \right)}_{\Xi_1} f_{Y_{k,i^*,\mathsf{E}}}(y) dy. \end{aligned} \tag{65}$$

In order to further represent $P_{\mathrm{SOP}}^{\mathrm{c4}}$, Ξ_1 can be expressed as

$$\begin{aligned} \Xi_1 =& \int_0^{\infty} F_{X_{k,i^*,j^*}} \left(\frac{(\gamma_{\mathrm{th}} - 1)\gamma_{\mathsf{E}} z}{\gamma_{\mathsf{R}}} + \frac{(\gamma_{\mathrm{th}} - 1)}{\gamma_{\mathsf{R}}} + \frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}} yz}{2} + \frac{\gamma_{\mathrm{th}} y}{2} \right) f_{Z_{k,\mathsf{E},j^*}}(z) dz \\ =& \underbrace{\int_0^{\infty} \frac{1}{\lambda_{k,\mathsf{E},j}} \exp\left(- \frac{z}{\lambda_{k,\mathsf{E},j}} \right) dz}_{\Xi_{1a}} - \exp\left(- \frac{1}{\lambda_{k,i,j}} \left(\frac{(\gamma_{\mathrm{th}} - 1)}{\gamma_{\mathsf{R}}} + \frac{\gamma_{\mathrm{th}} y}{2} \right) \right) \\ & \times \underbrace{\int_0^{\infty} \frac{1}{\lambda_{k,\mathsf{E},j}} \exp\left(- \left(\frac{(\gamma_{\mathrm{th}} - 1)\gamma_{\mathsf{E}}}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} + \frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}} y}{2\lambda_{k,i,j}} + \frac{1}{\lambda_{k,\mathsf{E},j}} \right) z \right) dz}_{\Xi_{1b}}. \end{aligned} \tag{66}$$

Relying on the fact [40] (Equation 3.310), Ξ_{1a} and Ξ_{1b} in (66) can be, respectively, obtained as

$$\Xi_{1a} = \int_0^{\infty} \frac{1}{\lambda_{k,\mathsf{E},j}} \exp\left(-\frac{z}{\lambda_{k,\mathsf{E},j}} \right) dz = \frac{1}{\lambda_{k,\mathsf{E},\mathsf{j}}} \lambda_{k,\mathsf{E},\mathsf{j}} = 1, \tag{67}$$

$$\begin{aligned} \Xi_{1b} &= \int_0^{\infty} \frac{1}{\lambda_{k,\mathsf{E},j}} \exp\left(-\left(\frac{2(\gamma_{\mathrm{th}} - 1)\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j} + 2\gamma_{\mathsf{R}}\lambda_{k,i,j} + \gamma_{\mathrm{th}}\gamma_{\mathsf{R}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j} y}{2\gamma_{\mathsf{R}}\lambda_{k,i,j}\lambda_{k,\mathsf{E},j}} \right) z \right) dz \\ &= \frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}\left(\frac{2(\gamma_{\mathrm{th}}-1)\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j} + 2\gamma_{\mathsf{R}}\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{R}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}} + y \right)} = \frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}(\eta_k + y)}, \end{aligned} \tag{68}$$

where $\eta_k = \frac{2(\gamma_{\mathrm{th}}-1)\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j} + 2\gamma_{\mathsf{R}}\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{R}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}}$. When plugging Ξ_{1a} and Ξ_{1b} into Ξ_1, (66) can be rewritten as

$$\Xi_1 = 1 - \frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}(\eta_k + y)} \exp\left(-\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} - \frac{\gamma_{\mathrm{th}} y}{2\lambda_{k,i,j}} \right). \tag{69}$$

By substituting Ξ_1 into (65) and after some algebraic steps, Ξ can be re-expressed as

$$\begin{aligned} \Xi &= \int_0^{\infty} \left[1 - \frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}(\eta_k + y)} \exp\left(-\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} - \frac{\gamma_{\mathrm{th}} y}{2\lambda_{k,i,j}} \right) \right] \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y \right) dy \\ &= \underbrace{\int_0^{\infty} \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y \right) dy}_{\Xi_{2a}} \\ &\quad - \frac{2N\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,i,\mathsf{E}}\lambda_{k,\mathsf{E},j}} \exp\left(-\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} \right) \underbrace{\int_0^{\infty} \frac{1}{(\eta_k + y)} \exp\left(-\left(\frac{\gamma_{\mathrm{th}}}{2\lambda_{k,i,j}} + \frac{N}{\lambda_{k,i,\mathsf{E}}} \right) y \right) dy}_{\Xi_{2b}}. \end{aligned} \tag{70}$$

Using the fact [40] (Equation 3.310), Ξ_{2a} can be obtained as

$$\Xi_{2a} = \int_0^{\infty} \frac{N}{\lambda_{k,i,\mathsf{E}}} \exp\left(-\frac{N}{\lambda_{k,i,\mathsf{E}}} y \right) dy = \frac{N}{\lambda_{k,i,\mathsf{E}}} \frac{\lambda_{k,i,\mathsf{E}}}{N} = 1. \tag{71}$$

In order to further expressed Ξ_{2b}, we utilize the fact [40] (Equation 3.352.4). Ξ_{2b} can be re-expressed as

$$\Xi_{2b} = \int_0^{\infty} \frac{1}{\eta_k + y} \exp\left(-\frac{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + 2N\lambda_{k,i,j}}{2\lambda_{k,i,j}\lambda_{k,i,\mathsf{E}}} y \right) dy = -\exp(\eta_k \nu_k) \mathrm{Ei}(-\eta_k \nu_k), \tag{72}$$

where $\nu_k = \frac{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}} + 2N\lambda_{k,i,j}}{2\lambda_{k,i,j}\lambda_{k,i,\mathsf{E}}}$. After plugging Ξ_{2a} and Ξ_{2b} into (70), Ξ can be obtained as

$$\Xi = 1 + \frac{2N\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,i,\mathsf{E}}\lambda_{k,\mathsf{E},j}} \exp\left(-\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} + \eta_k \nu_k \right) \mathrm{Ei}(-\eta_k \nu_k). \tag{73}$$

By inserting Ξ into (64), we obtain the SOP of case IV as

$$P_{\mathrm{SOP}}^{\mathrm{c4}} = 1 - \prod_{k=1}^{K} \left[-\frac{2N\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,i,\mathsf{E}}\lambda_{k,\mathsf{E},j}} \exp\left(-\frac{\gamma_{\mathrm{th}} - 1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}} + \eta_k \nu_k \right) \mathrm{Ei}(-\eta_k \nu_k) \right]. \tag{74}$$

4.5. Case V: Optimal Node Selection with Passive Eavesdropper

According to the definition of the SOP in (24), the SOP under case V can be further written as

$$\begin{aligned} P_{\mathrm{SOP}}^{\mathrm{c5}} =& 1-\prod_{k=1}^{K}\left[1-\Pr\left(\max_{1\le i\le N}\left\{\frac{1+\gamma_{k,i^*,j^*}^{\mathrm{ONS,pas}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\mathrm{ONS,pas}}}\right\}<\gamma_{\mathrm{th}}\right)\right] \\ =& 1-\prod_{k=1}^{K}\left[1-\prod_{i=1}^{N}\left\{\Pr\left(\frac{1+\gamma_{\mathsf{R}}X_{k,i,j^*}}{1+\gamma_{\mathsf{R}}Y_{k,i,\mathsf{E}}}<\gamma_{\mathrm{th}}\right)\right\}\right]. \end{aligned} \tag{75}$$

After some algebraic operations, the SOP under case V can be expressed as

$$P_{\mathrm{SOP}}^{\mathrm{c5}} = 1-\prod_{k=1}^{K}\left[1-\prod_{i=1}^{N}\underbrace{\left\{\Pr\left(X_{k,i,j}<\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}}+\gamma_{\mathrm{th}}Y_{k,i,\mathsf{E}}\right)\right\}}_{\Theta}\right]. \tag{76}$$

Θ in (76) can be rewritten as

$$\begin{aligned} \Theta =& \int_0^{\infty}\left[1-\exp\left(-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}}+\gamma_{\mathrm{th}}y\right)\right)\right]\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{y}{\lambda_{k,i,\mathsf{E}}}\right)dy \\ =& \underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{y}{\lambda_{k,i,\mathsf{E}}}\right)dy}_{\Theta_{1a}} \\ & -\exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right)\underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-(\frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}}+\frac{1}{\lambda_{k,i,\mathsf{E}}})y\right)dy}_{\Theta_{1b}}. \end{aligned} \tag{77}$$

Relying on the fact [40] (Equation 3.310), Θ_{1a} and Θ_{1b} can be, respectively, obtained as

$$\Theta_{1a} = \int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\frac{y}{\lambda_{k,i,\mathsf{E}}}\right)dy = 1, \tag{78}$$

$$\Theta_{1b} = \int_0^{\infty}\frac{1}{\lambda_{k,i,\mathsf{E}}}\exp\left(-\left(\frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}}+\frac{1}{\lambda_{k,i,\mathsf{E}}}\right)y\right)dy = \frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}+\lambda_{k,i,j}}. \tag{79}$$

By plugging Θ_{1a} and Θ_{1b} into (77), Θ can be further expressed as

$$\Theta = 1-\frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}+\lambda_{k,i,j}}\exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right). \tag{80}$$

By substituting (80) into (76) and using the binomial theorem [40] (Equation 1.111), we can obtain the closed-form expression for the SOP with case V, which can be expressed as

$$\begin{aligned} P_{\mathrm{SOP}}^{\mathrm{c5}} =& 1-\prod_{k=1}^{K}\left[1-\prod_{i=1}^{N}\left\{1-\frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}+\lambda_{k,i,j}}\exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right)\right\}\right] \\ =& 1-\prod_{k=1}^{K}\left[1-\sum_{m=0}^{N}\binom{N}{m}(-1)^m\left(\frac{\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,\mathsf{E}}+\lambda_{k,i,j}}\right)^m\exp\left(-\frac{m\gamma_{\mathrm{th}}-m}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}\right)\right]. \end{aligned} \tag{81}$$

4.6. Case VI: Optimal Node Selection with Active Eavesdropper

From (24), the SOP with case 6 can be further written as

$$P_{\mathrm{SOP}}^{\mathrm{c6}} = 1-\prod_{k=1}^{K}\left[1-\Pr\left(\max_{1\le i\le N}\left\{\frac{1+\gamma_{k,i^*,j^*}^{\mathrm{ONS,act}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\mathrm{ONS,act}}}\right\}<\gamma_{\mathrm{th}}\right)\right]. \tag{82}$$

The SOP in (82) can be re-expressed as

$$\begin{aligned} P_{\mathrm{SOP}}^{\mathrm{c6}} =& 1-\prod_{k=1}^{K}\left[1-\prod_{i=1}^{N}\left\{\Pr\left(\frac{1+\frac{\gamma_{\mathsf{R}}X_{k,i,j^*}}{\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j^*}+1}}{1+\frac{\gamma_{\mathsf{R}}}{2}Y_{k,i,\mathsf{E}}}<\gamma_{\mathrm{th}}\right)\right\}\right] \\ =& 1-\prod_{k=1}^{K}\left[1-\prod_{i=1}^{N}\left\{\underbrace{\Pr\left(\frac{\gamma_{\mathsf{R}}X_{k,i,j^*}}{\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j^*}+1}<\gamma_{\mathrm{th}}-1+\frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{R}}}{2}Y_{k,i,\mathsf{E}}\right)}_{\Delta}\right\}\right]. \end{aligned} \tag{83}$$

Δ in (83) can be given by

$$\begin{aligned} \Delta =& \Pr\left(X_{k,i,j^*}<\frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j^*}+1)}{\gamma_{\mathsf{R}}}+\frac{\gamma_{\mathrm{th}}Y_{k,i,\mathsf{E}}(\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j^*}+1)}{2}\right) \\ =& \int_0^{\infty}\underbrace{\Pr\left(X_{k,i,j^*}<\frac{(\gamma_{\mathrm{th}}-1)(\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j^*}+1)}{\gamma_{\mathsf{R}}}+\frac{\gamma_{\mathrm{th}}y(\gamma_{\mathsf{E}}Z_{k,\mathsf{E},j^*}+1)}{2}\right)}_{\Delta_1} f_{Y_{k,i,\mathsf{E}}}(y)dy. \end{aligned} \tag{84}$$

In order to further calculate (84), Δ_1 can be written as

$$\begin{aligned} \Delta_1 =& \int_0^{\infty} F_{X_{k,i,j^*}}\left(\frac{(\gamma_{\mathrm{th}}-1)\gamma_{\mathsf{E}}z}{\gamma_{\mathsf{R}}}+\frac{(\gamma_{\mathrm{th}}-1)}{\gamma_{\mathsf{R}}}+\frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}yz}{2}+\frac{\gamma_{\mathrm{th}}y}{2}\right) f_{Z_{k,\mathsf{E},j^*}}(z)dz \\ =& \underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,\mathsf{E},j}}\exp\left(-\frac{z}{\lambda_{k,\mathsf{E},j}}\right)dz}_{\Delta_{1a}}-\exp\left(-\frac{1}{\lambda_{k,i,j}}\left(\frac{(\gamma_{\mathrm{th}}-1)}{\gamma_{\mathsf{R}}}+\frac{\gamma_{\mathrm{th}}y}{2}\right)\right) \\ & \times\underbrace{\int_0^{\infty}\frac{1}{\lambda_{k,\mathsf{E},j}}\exp\left(-\left(\frac{(\gamma_{\mathrm{th}}-1)\gamma_{\mathsf{E}}}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}+\frac{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}y}{2\lambda_{k,i,j}}+\frac{1}{\lambda_{k,\mathsf{E},j}}\right)z\right)dz}_{\Delta_{1b}}. \end{aligned} \tag{85}$$

Relying on the fact [40] (Equation 3.310), Δ_{1a} and Δ_{1b} in (85) can be, respectively, expressed as

$$\Delta_{1a}=\int_0^{\infty}\frac{1}{\lambda_{k,\mathsf{E},j}}\exp\left(-\frac{z}{\lambda_{k,\mathsf{E},j}}\right)dz=\frac{1}{\lambda_{k,\mathsf{E},\mathsf{j}}}\lambda_{k,\mathsf{E},\mathsf{j}}=1, \tag{86}$$

$$\begin{aligned} \Delta_{1b} =& \int_0^{\infty}\frac{1}{\lambda_{k,\mathsf{E},j}}\exp\left(-\left(\frac{2(\gamma_{\mathrm{th}}-1)\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}+2\gamma_{\mathsf{R}}\lambda_{k,i,j}+\gamma_{\mathrm{th}}\gamma_{\mathsf{R}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}y}{2\gamma_{\mathsf{R}}\lambda_{k,i,j}\lambda_{k,\mathsf{E},j}}\right)z\right)dz \\ =& \frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}\left(\frac{2(\gamma_{\mathrm{th}}-1)\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}+2\gamma_{\mathsf{R}}\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{R}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}}+y\right)}=\frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}(\eta_k+y)}, \end{aligned} \tag{87}$$

where η_k is defined as (68). Again, when plugging Δ_{1a} and Δ_{1b} into (85), Δ_1 can be rewritten as

$$\Delta_1=1-\frac{2\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\gamma_{\mathsf{E}}\lambda_{k,\mathsf{E},j}(\eta_k+y)}\exp\left(-\frac{\gamma_{\mathrm{th}}-1}{\gamma_{\mathsf{R}}\lambda_{k,i,j}}-\frac{\gamma_{\mathrm{th}}y}{2\lambda_{k,i,j}}\right). \tag{88}$$

By substituting Δ_1 into (84) and after some algebraic steps, Δ can be re-expressed as

$$\begin{aligned}\Delta &= \int_0^\infty \left[1 - \frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_{\text{E}}\lambda_{k,\text{E},j}(\eta_k + y)} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_{\text{R}}\lambda_{k,i,j}} - \frac{\gamma_{\text{th}} y}{2\lambda_{k,i,j}}\right)\right] \frac{1}{\lambda_{k,i,\text{E}}} \exp\left(-\frac{1}{\lambda_{k,i,\text{E}}} y\right) dy \\ &= \underbrace{\int_0^\infty \frac{1}{\lambda_{k,i,\text{E}}} \exp\left(-\frac{1}{\lambda_{k,i,\text{E}}} y\right) dy}_{\Delta_{2a}} \\ &\quad - \frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_{\text{E}}\lambda_{k,i,\text{E}}\lambda_{k,\text{E},j}} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_{\text{R}}\lambda_{k,i,j}}\right) \underbrace{\int_0^\infty \frac{1}{(\eta_k + y)} \exp\left(-\left(\frac{\gamma_{\text{th}}}{2\lambda_{k,i,j}} + \frac{1}{\lambda_{k,i,\text{E}}}\right) y\right) dy}_{\Delta_{2b}}.\end{aligned} \tag{89}$$

Using the fact [40] (Equation 3.310), Δ_{2a} can be obtained as

$$\Delta_{2a} = \int_0^\infty \frac{1}{\lambda_{k,i,\text{E}}} \exp\left(-\frac{1}{\lambda_{k,i,\text{E}}} y\right) dy = \frac{1}{\lambda_{k,i,\text{E}}} \lambda_{k,i,\text{E}} = 1. \tag{90}$$

In order to further express Δ_{2b}, we utilize the fact [40] (Equation 3.352.4). Δ_{2b} can be re-expressed as

$$\Delta_{2b} = \int_0^\infty \frac{1}{\eta_k + y} \exp\left(-\frac{\gamma_{\text{th}}\lambda_{k,i,\text{E}} + 2\lambda_{k,i,j}}{2\lambda_{k,i,j}\lambda_{k,i,\text{E}}} y\right) dy = -\exp(\eta_k\alpha_k)\text{Ei}(-\eta_k\alpha_k), \tag{91}$$

where $\alpha_k = \frac{\gamma_{\text{th}}\lambda_{k,i,\text{E}} + 2\lambda_{k,i,j}}{2\lambda_{k,i,j}\lambda_{k,i,\text{E}}}$. After plugging Δ_{2a} and Δ_{2b} into (89), Δ can be obtained as

$$\Delta = 1 + \frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_{\text{E}}\lambda_{k,i,\text{E}}\lambda_{k,\text{E},j}} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_{\text{R}}\lambda_{k,i,j}} + \eta_k\alpha_k\right)\text{Ei}(-\eta_k\alpha_k). \tag{92}$$

By plugging Δ into (83) and using the binomial theorem [40] (Equation 1.111), we obtain the SOP of case VI as

$$\begin{aligned}P_{\text{SOP}}^{\text{c6}} &= 1 - \prod_{k=1}^{K}\left[1 - \prod_{i=1}^{N}\left\{1 + \frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_{\text{E}}\lambda_{k,i,\text{E}}\lambda_{k,\text{E},j}} \exp\left(-\frac{\gamma_{\text{th}} - 1}{\gamma_{\text{R}}\lambda_{k,i,j}} + \eta_k\alpha_k\right)\text{Ei}(-\eta_k\alpha_k)\right\}\right] \\ &= 1 - \prod_{k=1}^{K}\left[1 - \sum_{m=0}^{N}\binom{N}{m}\left(\frac{2\lambda_{k,i,j}}{\gamma_{\text{th}}\gamma_{\text{E}}\lambda_{k,i,\text{E}}\lambda_{k,\text{E},j}}\right)^m \exp\left(-\frac{m\gamma_{\text{th}} - m}{\gamma_{\text{R}}\lambda_{k,i,j}} + m\eta_k\alpha_k\right)\right. \\ &\qquad \left.\times \left(\text{Ei}(-\eta_k\alpha_k)\right)^m\right].\end{aligned} \tag{93}$$

5. Performance Evaluations

In this section, we exploit the impact of the active eavesdropping attack and the proposed node selection schemes on the secrecy performance. Unless otherwise stated, the simulation parameters are presented in Table 2.

Figure 2 shows the effect of γ_{R} on the SOP. As can be seen, when the transmitted SNR increases, the SOP is decreased. It can be explained by the SNR of the main channel, which is improved, as well as that of the eavesdropper channel. However, the impact of the SNR of the main channel is more than that of the eavesdropper channel. Additionally, when the eavesdropper generates a jamming signal, i.e., active eavesdropping attack, the SOP is higher than the passive eavesdropping attack. The reason is that the jamming signal can degrade the SINR of the main channel, which leads to reducing the difference between the main channel and eavesdropper channel capacities. In order to counteract the eavesdropper attack, different from the other node selection schemes that select the node randomly or utilize only eavesdropper channel information, the proposed ONS scheme uses both main channel and eavesdropper channel information. Thus, the proposed ONS scheme shows

the most robust secrecy performance compared with that of other node selection schemes. The comparison between simulation and analytical results is in good agreement, validating the correctness of our derivation approaches. Hence, the following results only provide the theoretical results.

Table 2. Simulation parameters.

Parameters	Value
Distance between S and D (d_{SD})	10 m
Position of S	(0, 0)
Position of D	(10, 0)
Position of E	(5, −5)
Position of R_k	($d_{\mathsf{SD}}k/K$, 0)
Number of hops (K)	4 hops
Number of nodes (N) in each cluster	6 nodes
Reference distance (d_0)	10 m
Path-loss exponent (ϵ)	2.7
Target secrecy rate (R_{th})	0.1 bps/Hz
Node transmit SNR (γ_{R})	10 dB
Eavesdropper jamming SNR (γ_{E})	0 dB

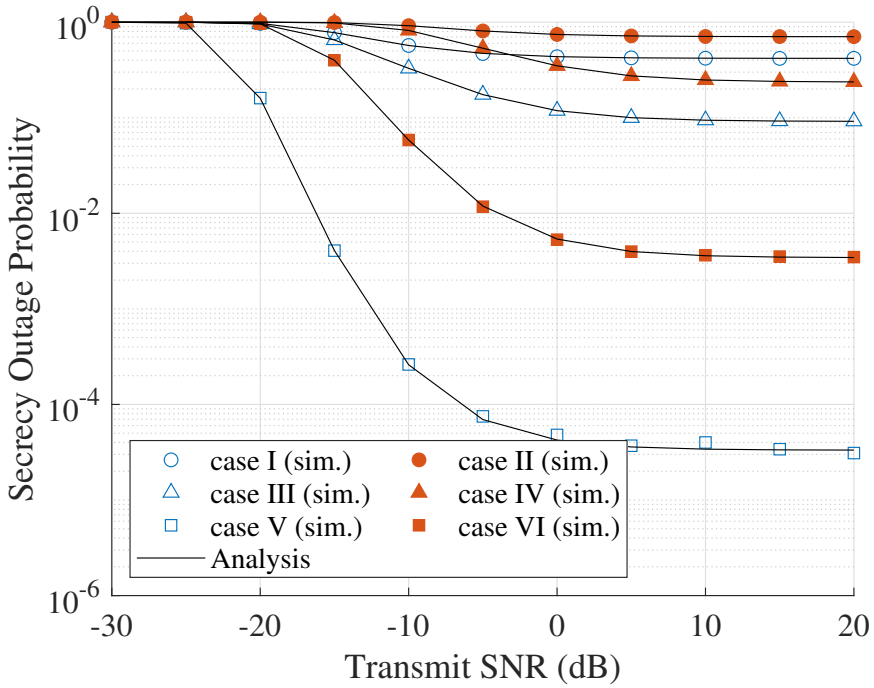

Figure 2. SOP versus node transmit SNR (γ_{R}).

Figure 3 shows the effect of γ_{E} towards the SOP of a cooperative multihop relaying network. As can be seen, the SOP for passive eavesdropper scenarios is constant. It can be explained by the fact that the eavesdropper does not radiate a jamming signal, only overhearing the legitimate users' transmission. In contrast, the active eavesdropper radiates the jamming signal. Thus, when the jamming SNR increases, the SOP with case II, case IV, and case VI is increased. It means that the difference between main channel and eavesdropper channel capacities is reduced. In Figure 3, ONS has the lowest SOP among all the node selection schemes because ONS selects a node in every cluster that gives the maximum secrecy rate. Therefore, the probability of the system secrecy being outage in an ONS scheme becomes minimum. On the contrary, RNS selects a node randomly, and MNS selects a node only based on the eavesdropper link that makes low system secrecy capacity and high SOP.

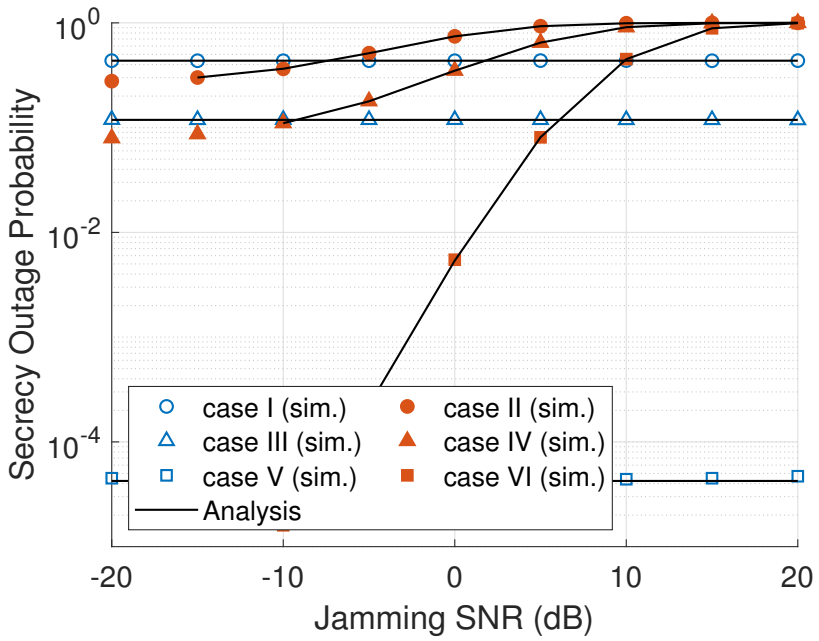

Figure 3. SOP versus eavesdropper's jamming SNR (γ_E).

Figure 4 shows the effect of R_{th} on the SOP. As shown in Figure 4, with the higher target secrecy data rate, the SOP is increased. The reason is that a higher target secrecy rate correlates with a higher threshold level of the system secrecy being outage. Therefore, the probability of the outage event becomes higher. In Figure 4, a passive eavesdropper scenario produces a better SOP than an active scenario because the system secrecy in a passive attack is higher; then the probability of an outage event is lower. Once again, ONS has the most robust SOP between all node selection schemes in Figure 4 because ONS utilizes both main channel and eavesdropper channel information to select a node. Case V with an ONS scheme and passive eavesdropper scenario has the lowest SOP among all cases. One of the reasons is that ONS selects the best node in every cluster that maximizes the secrecy capacity rate. Furthermore, the passive mode of an eavesdropper allows a less significant attack to the main channel capacity.

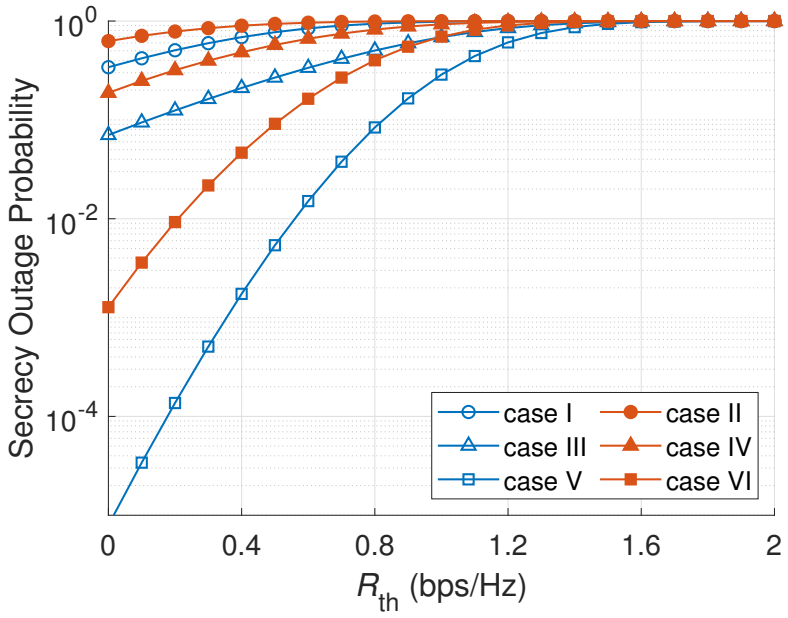

Figure 4. SOP versus target secrecy data rate (R_{th}).

Figure 5 illustrates the relation between the SOP and N. As can be seen, the number of nodes in a cluster does not have an impact on the SOP of an RNS scheme. An RNS scheme's SOP in cases I and II is constant for all N values because RNS only selects one node randomly regardless of many nodes that can be chosen. ONS and MNS schemes, on the other side, have a lower SOP when the number of nodes per cluster increases because there are more nodes that can be selected to relay the confidential information. In a cluster with more nodes, ONS and MNS schemes have more possibility to choose a node that has better secrecy capacity; then the probability of the secrecy being outage declines. Additionally, an active eavesdropper scenario yields a higher SOP due to more attacks on the main channel capacity than a passive eavesdropper scenario. An active eavesdropper radiates a jamming signal aiming to harm the main channel transmission. Hence, an active eavesdropper is more destructive.

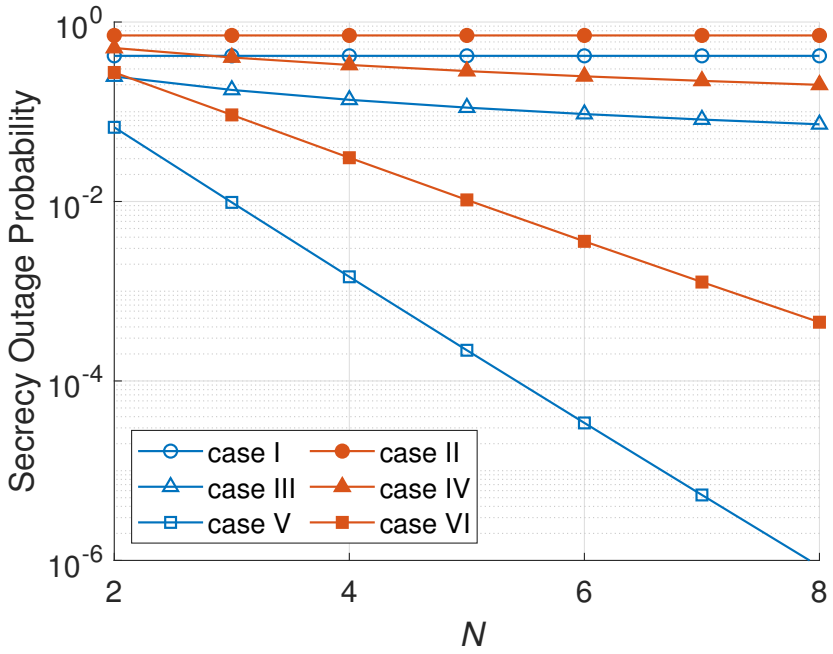

Figure 5. SOP versus number of nodes per cluster (N).

Figure 6 illustrates the impact of K on the SOPs. The SOP is decreased when the number of hops increases because there are more hops that can be chosen as the minimum system secrecy capacity rate. This corresponds to (24), where the SOP is inversely proportional to the number of hops. As can be observed more from Figure 6, a passive eavesdropper scenario produces a lower SOP due to its harmless attack on the main channel capacity than an active mode. The passive eavesdropping scenarios do not radiate a jamming signal, different from the active eavesdropping scenario. In Figure 6, an ONS scheme has the lowest SOP among all the node selection schemes since ONS selects the best node in every cluster that gives the maximum secrecy capacity based on the main channel and eavesdropper channel information. On the other hand, RNS selects a node randomly and MNS selects a node only based on the minimum eavesdropper channel gain that cannot increase the secrecy capacity significantly.

In order to further analyze the secrecy performance of the considered multihop transmission system, we calculate the system secrecy throughput, which is mathematically defined as [38]

$$\mathcal{T}_{\text{case}} = (1 - P_{\text{SOP}}^{\text{case}}) R_{\text{th}}. \tag{94}$$

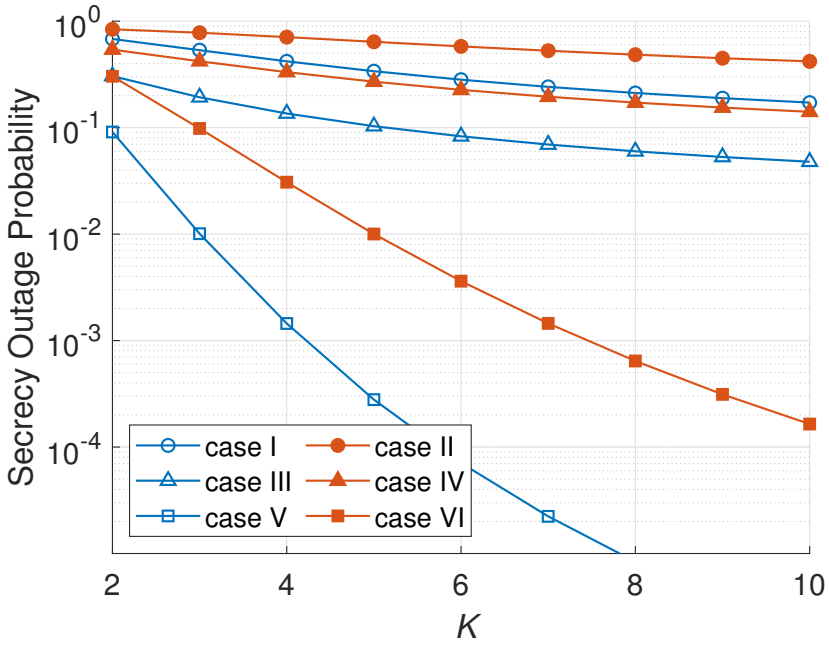

Figure 6. SOP versus number of hops (K).

Secrecy throughput is defined as the achievable secrecy rate of the system [41]. Figure 7 presents the system's secrecy throughput as a function of γ_R. The increment of the node transmit SNR results in the increase in the system's secrecy throughput. High SNR in the relay nodes increases the main channel capacity higher than the eavesdropper channel capacity because of the eavesdropping counteracting at the node selection process in every cluster. This eventually increases the overall system secrecy rate. The ONS scheme in Figure 7 has the highest secrecy throughput since ONS selects a node with the maximum secrecy capacity in every cluster. On the other hand, an RNS scheme has the lowest secrecy throughput because RNS selects a node randomly without considering the main channel and eavesdropper channel information. Active eavesdropping scenarios bring more destruction in the system secrecy throughput than passive eavesdropping scenarios due to the transmitted jamming signal that degrades the main channel capacity rate.

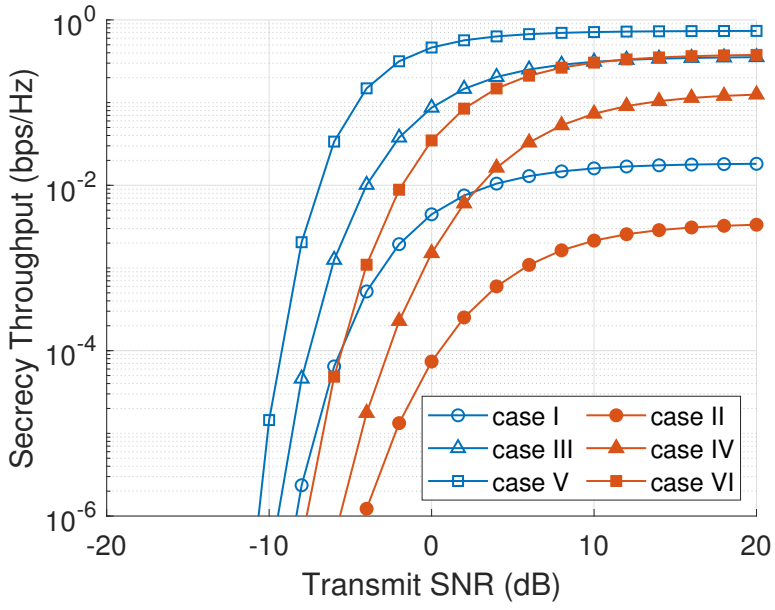

Figure 7. Secrecy throughput versus node transmit SNR (γ_R).

Figure 8 presents the system's secrecy throughput as a function of γ_E. As can be seen, a passive scenario of an eavesdropper in cases I, III, and V has a constant secrecy throughput because a passive eavesdropper only overhears the main channel information without transmitting any jamming signal. Cases II, IV, and VI under an active eavesdropper attack has a declination of secrecy throughput as a jamming SNR is increasing, since more jamming is interfering the main channel transmission, and eventually, the difference between main channel and eavesdropper channel capacities is decreasing. Case II with an RNS scheme has the lowest secrecy throughput because a node in every cluster is chosen randomly regardless of its channel information. However, the utilization of an ONS scheme can increase the secrecy throughput higher than RNS and MNS, since ONS selects the best node with the maximum secrecy capacity based on both main channel and eavesdropper channel information.

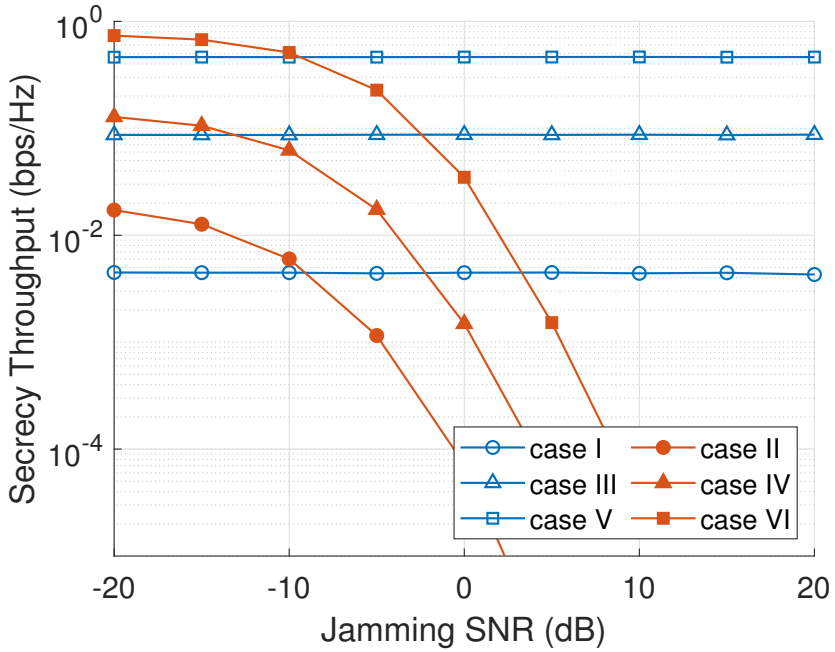

Figure 8. Secrecy throughput versus eavesdropper jamming SNR (γ_E).

Finally, we turn our attention to the complexity order. The complexity order is defined as the amount of channel information to select the node and transmit a signal. Table 3 presents the complexity order for every case of a system. Since an RNS scheme selects the node randomly, the RNS scheme does not utilize the channel information at the node selection step. Thus, the RNS scheme shows the lowest complexity order among the considered schemes. An MNS scheme only utilizes the eavesdropper channel information to select the node in each cluster, so the complexity for the selection process grows as $N \times K$. An ONS scheme utilizes both main channel and eavesdropper channel information to select a node in every cluster. Thus, an ONS scheme requires the most channel information among the considered schemes.

Table 3. Complexity order of the schemes.

Case	I	II	III	IV	V	VI
Scheme	RNS	RNS	MNS	MNS	ONS	ONS
Attack	passive	active	passive	active	passive	active
Complexity	$2K$	$3K$	$(N+2)K$	$(N+3)K$	$(2N+2)K$	$(2N+4)K$

Figure 9 visualizes the trade-off between the SOP and complexity as a function of K. As can be seen, when the number of hops increases, the complexity order of the proposed

node selection schemes is increased, while the SOP is decreased. More specifically, the RNS scheme's complexity order increases linearly, while the SOP is decreased. On the other hand, the ONS scheme's complexity order increases when the number of hops increases, while the SOP is decreased significantly. Finally, the complexity order of the MNS scheme is slightly increased, while the SOP of the MNS scheme is decreased and still providing secure transmission. From these phenomena, complexity order and SOP have a trade-off. However, though the complexity order of an ONS scheme is increased, the secrecy performance is significantly improved. Thus, we can conclude that the ONS scheme has advantage against complexity order.

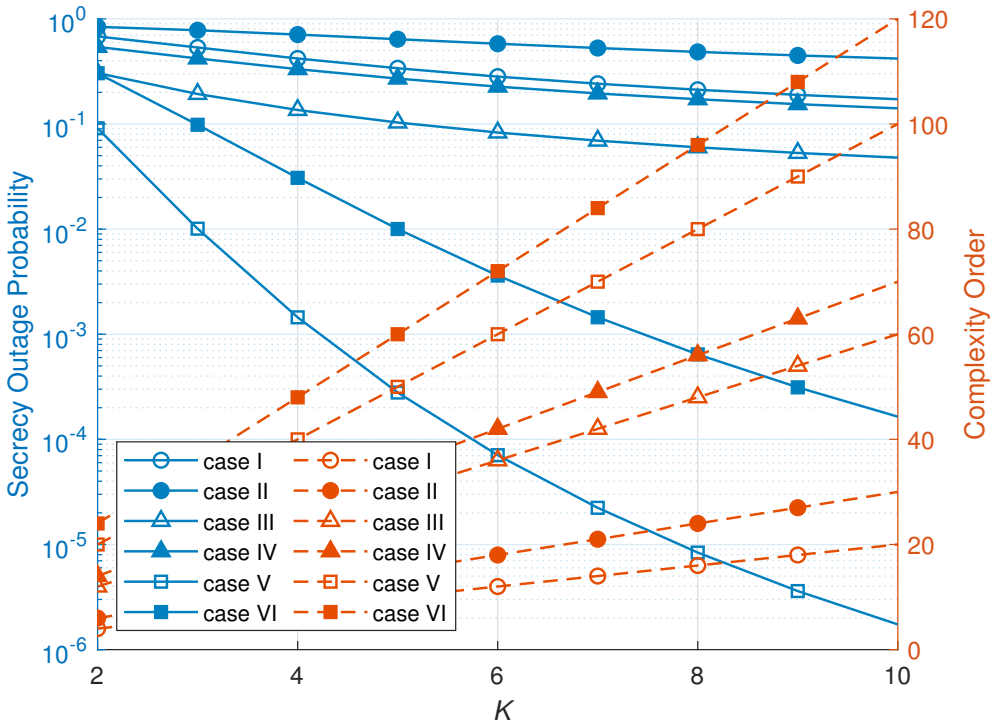

Figure 9. Complexity versus number of hops (K).

6. Conclusions

This paper studied the impact of the eavesdropping attack on the multihop transmission system for sensor networks. More specifically, we exploited the active and passive eavesdropping attacks. The active eavesdropping attack can overhear the legitimate users' transmission and radiate the jamming signal to degrade the main channel condition. The passive eavesdropping attack only overhears the legitimate users' transmission. As a counteraction, in order to protect the confidential message against various eavesdropping attacks, we proposed the node selection schemes called MNS scheme and ONS scheme. Since the MNS scheme only required the eavesdropper channel information to select the node in each cluster, it had low complexity and slightly improved the secrecy performance. Meanwhile, the ONS scheme selected the node in each cluster to maximize the secrecy capacity. Thus, the ONS scheme showed high complexity and significantly improved the secrecy performance. We derived the closed-form expression for the SOP with a different eavesdropping attack and node selection scheme. Numerical results showed that an active eavesdropping attack is more destructive compared with a passive attack since an active eavesdropper generated the jamming signal. The ONS scheme utilized both the main channel and eavesdropper channel to select the node in each cluster, which brought the most robust secrecy performance compared with the other node selection schemes. Additionally, through various numerical results, the proposed node selection scheme and different eavesdropping attack on the secrecy performance were discussed. In order to expand this

work, we try to develop the secure routing protocol that utilizes the physical layer security concept and blockchain to protect a confidential packet against a sniffing attack.

Author Contributions: Conceptualization, Y.T., R.H.Y.P., K.S. and B.A.; methodology, Y.T., K.S. and B.A.; software, Y.T., R.H.Y.P. and K.S.; validation, Y.T., R.H.Y.P., K.S. and B.A.; formal analysis, Y.T.; investigation, Y.T. and B.A.; resources, B.A.; writing—original draft preparation, Y.T.; writing—review and editing, R.H.Y.P., K.S. and B.A.; visualization, Y.T., K.S. and B.A.; supervision, B.A.; project administration, B.A.; funding acquisition, B.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2022R1A2B5B01001190).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Sharma, S.K.; Woungang, I.; Anpalagan, A.; Chatzinotas, S. Toward Tactile Internet in beyond 5G Era: Recent Advances, Current Issues, and Future Directions. *IEEE Access* **2020**, *8*, 56948–56991. [CrossRef]
2. Tataria, H.; Shafi, M.; Molisch, A.F.; Dohler, M.; Sjoland, H.; Tufvesson, F. 6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities. *Proc. IEEE* **2021**, *109*, 1166–1199. [CrossRef]
3. Lee, Y.L.; Qin, D.; Wang, L.C.; Sim, G.H. 6G Massive Radio Access Networks: Key Applications, Requirements and Challenges. *IEEE Open J. Veh. Technol.* **2021**, *2*, 54–66. [CrossRef]
4. Mao, Z.; Hu, F.; Sun, D.; Ma, S.; Liu, X. Fairness-Aware Intragroup Cooperative Transmission in Wireless Powered Communication Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6463–6472. [CrossRef]
5. Tuan, N.T.; Kim, D.S.; Lee, J.M. On the performance of cooperative transmission schemes in industrial wireless sensor networks. *IEEE Trans. Industr. Inform.* **2018**, *14*, 4007–4018. [CrossRef]
6. El-Banna, A.A.; Wu, K.; Elhalawany, B.M. Opportunistic Cooperative Transmission for Underwater Communication Based on the Water's Key Physical Variables. *IEEE Sens. J.* **2020**, *20*, 2792–2802. [CrossRef]
7. Ji, B.; Han, Y.; Wang, Y.; Cao, D.; Tao, F.; Fu, Z.; Li, P.; Wen, H. Relay Cooperative Transmission Algorithms for IoV under Aggregated Interference. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 9712–9725. [CrossRef]
8. Adil, M.; Khan, R.; Almaiah, M.A.; Al-Zahrani, M.; Zakarya, M.; Amjad, M.S.; Ahmed, R. MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks. *IEEE Access* **2020**, *8*, 44459–44469. [CrossRef]
9. Li, B.; Zou, Y.; Zhu, J.; Cao, W. Impact of hardware impairment and co-channel interference on security-reliability trade-off for wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 7011–7025. [CrossRef]
10. Mehmood, A.; Umar, M.M.; Song, H. ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks. *Ad Hoc Netw.* **2017**, *55*, 97–106. [CrossRef]
11. Hieu, T.D.; Duy, T.T.; Kim, B.S. 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]
12. Nguyen, V.L.; Lin, P.C.; Cheng, B.C.; Hwang, R.H.; Lin, Y.D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [CrossRef]
13. Ari, N.; Thomos, N.; Musavian, L. Active Eavesdropping in Short Packet Communication: Average Secrecy Throughput Analysis. In Proceedings of the 2021 IEEE International Conference on Communications Workshops, Montreal, Canada, 14–23 June 2021; pp. 1–6.
14. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
15. Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1773–1828. [CrossRef]
16. Wang, D.; Bai, B.; Zhao, W.; Han, Z. A Survey of Optimization Approaches for Wireless Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1878–1911. [CrossRef]
17. Duo, B.; Luo, J.; Li, Y.; Hu, H.; Wang, Z. Joint trajectory and power optimization for securing UAV communications against active eavesdropping. *China Commun.* **2021**, *18*, 88–99. [CrossRef]
18. Wang, W.; Teh, K.C.; Li, K.H.; Luo, S. On the Impact of Adaptive Eavesdroppers in Multi-Antenna Cellular Networks. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 269–279. [CrossRef]

19. Luo, Y.; Yang, Y. Secrecy Anti-jamming Game Learning in D2D Underlay Cellular Networks with an Active Eavesdropper. In Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, 8–11 October 2018; pp. 446–451.
20. Luo, Y.; Feng, Z.; Jiang, H.; Yang, Y.; Huang, Y.; Yao, J. Game-theoretic learning approaches for secure D2D communications against full-duplex active eavesdropper. *IEEE Access* **2019**, *7*, 41324–41335. [CrossRef]
21. Lin, Z.; Lin, M.; Champagne, B.; Zhu, W.P.; Al-Dhahir, N. Secrecy-Energy Efficient Hybrid Beamforming for Satellite-Terrestrial Integrated Networks. *IEEE Trans. Commun.* **2021**, *69*, 6345–6360. [CrossRef]
22. Lin, Z.; Lin, M.; Wang, J.B.; Cola, T.D.; Wang, J. Joint Beamforming and Power Allocation for Satellite-Terrestrial Integrated Networks with Non-Orthogonal Multiple Access. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 657–670. [CrossRef]
23. Lin, Z.; Lin, M.; Cola, T.D.; Wang, J.B.; Zhu, W.P.; Cheng, J. Supporting IoT with Rate-Splitting Multiple Access in Satellite and Aerial-Integrated Networks. *IEEE Internet Things J.* **2021**, *8*, 11123–11134. [CrossRef]
24. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS-Aided Hybrid Satellite-Terrestrial Relay Networks: Joint Beamforming Design and Optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [CrossRef]
25. Liu, C.; Lee, J.; Quek, T.Q. Safeguarding uav communications against full-duplex active eavesdropper. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2919–2931. [CrossRef]
26. Kudathanthirige, D.; Timilsina, S.; Baduge, G.A.A. Secure Communication in Relay-Assisted Massive MIMO Downlink with Active Pilot Attacks. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2819–2833. [CrossRef]
27. Lu, X.; Yang, W.; Guan, X.; Cai, Y. DCE-Based Secure Transmission for Massive MIMO Relay System against Active Eavesdropper. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13045–13059. [CrossRef]
28. Abdullah, Z.; Chen, G.; Abdullah, M.A.; Chambers, J.A. Enhanced Secrecy Performance of Multihop IoT Networks with Cooperative Hybrid-Duplex Jamming. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 161–172. [CrossRef]
29. Bouabdellah, M.; Bouanani, F.E. A PHY Layer Security of a Jamming-Based Underlay Cognitive Satellite-Terrestrial Network. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 1266–1279. [CrossRef]
30. Vahidian, S.; Hatamnia, S.; Champagne, B. On the Security Analysis of a Cooperative Incremental Relaying Protocol in the Presence of an Active Eavesdropper. *IEEE Access* **2019**, *7*, 181812–181828. [CrossRef]
31. Zhou, H.; He, D.; Wang, H.; Yang, D. Optimal Relay Selection with a Full-duplex Active Eavesdropper in Cooperative Wireless Networks. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
32. Liu, J.; Xu, X.; Han, S.; Zhang, Z.; Liu, C. Hybrid relay selection and cooperative jamming scheme for secure communication in healthcare-IoT. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 29 March–1 April 2021; pp. 1–7.
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]
34. Shim, K.; Nguyen, T.V.; An, B. Exploiting opportunistic scheduling schemes and wpt-based multi-hop transmissions to improve physical layer security in wireless sensor networks. *Sensors* **2019**, *19*, 5456. [CrossRef]
35. Nguyen, T.V.; Do, T.N.; Bao, V.N.Q.; Costa, D.B.d.; An, B. On the Performance of Multihop Cognitive Wireless Powered D2D Communications in WSNs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2684–2699. [CrossRef]
36. Ma, S.; Li, M.; Yang, R.; Sun, Y.; Wang, Z.; Si, P. Next-Hop Relay Selection for Ad Hoc Network-Assisted Train-to-Train Communications in the CBTC System. *Sensors* **2023**, *23*, 5883. [CrossRef] [PubMed]
37. Nguyen, T.V.; Nguyen, V.D.; da Costa, D.B.; Huynh-The, T.; Hu, R.Q.; An, B. Short-Packet Communications in Multihop Networks with WET: Performance Analysis and Deep Learning-Aided Optimization. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 439–456. [CrossRef]
38. Shim, K.; Do, T.N.; Nguyen, T.V.; Costa, D.B.D.; An, B. Enhancing PHY-Security of FD-Enabled NOMA Systems Using Jamming and User Selection: Performance Analysis and DNN Evaluation. *IEEE Internet Things J.* **2021**, *8*, 17476–17494. [CrossRef]
39. Ai, Y.; Mathur, A.; Verma, G.D.; Kong, L.; Cheffena, M. Comprehensive Physical Layer Security Analysis of FSO Communications over Málaga Channels. *IEEE Photon. J.* **2020**, *12*, 7906617. [CrossRef]
40. Gradshteyn, I.; Ryzhik, I. *Table of Integrals, Series, and Products Seventh Edition*; Elsevier Academic Press: Amsterdam, The Netherlands, 2007.
41. Lyu, J.; Wang, H.M.; Huang, K.W. Physical Layer Security in D2D Underlay Cellular Networks with Poisson Cluster Process. *IEEE Trans. Commun.* **2020**, *68*, 7123–7139. [CrossRef]