electronics

MDPI

Article

Improving Physical Layer Security for Multi-Hop Transmissions in Underlay Cognitive Radio Networks with Various Eavesdropping Attacks

Kyusung Shim [1,*] and Beongku An [2]

[1] School of Computer Engineering and Applied Mathematics, Hankyong National University, Anseong 17579, Republic of Korea
[2] Department of Software and Communications Engineering, Hongik University, Sejong 30016, Republic of Korea
* Correspondence: kyusung.shim@hknu.ac.kr; Tel.: +82-31-670-5355

Abstract

This paper investigates physical layer security (PHY-security) for multi-hop transmission in underlay cognitive radio networks under various eavesdropping attacks. To enhance secrecy performance, we propose two opportunistic scheduling schemes. The first scheme, called the minimal node selection (MNS) scheme, selects the node in each cluster that minimizes the eavesdropper's channel capacity. The second scheme, named the optimal node selection (ONS) scheme, chooses the node that maximizes secrecy capacity by using both the main and eavesdropper channel information. To reveal the relationship between network parameters and secrecy performance, we derive closed-form expressions for the secrecy outage probability (SOP) under different scheduling schemes and eavesdropping scenarios. Numerical results show that the ONS scheme provides the most robust secrecy performance among the considered schemes. Furthermore, we analyze the impact of key network parameters on secrecy performance. In detail, although the proposed ONS scheme requires more channel information than the MNS scheme, under a 20 dB interference threshold, the secrecy performance of the ONS scheme is 15% more robust than that of the MNS scheme.

Keywords: cognitive radio; eavesdropping attack; opportunistic scheduling; physical layer security

Academic Editor: Aryya Gangopadhyay

Received: 4 September 2025
Revised: 23 September 2025
Accepted: 27 September 2025
Published: 29 September 2025

Citation: Shim, K.; An, B. Improving Physical Layer Security for Multi-Hop Transmissions in Underlay Cognitive Radio Networks with Various Eavesdropping Attacks. *Electronics* **2025**, *14*, 3867. https://doi.org/10.3390/electronics14193867

1. Introductions

As the Internet of Things (IoT) continues to expand, the number of connected devices has grown exponentially [1,2]. However, the radio frequency spectrum available for interconnecting these devices is limited and almost allocated. Therefore, spectrum re-utilization has recently emerged as one of the key issues for future mobile networks. To address this challenge, several approaches have been proposed. Cognitive radio is one of the available efficient solutions to enhance network spectrum re-utilization [3–5].

A cognitive radio network consists of primary users, who are allocated licensed spectrum resources, and secondary users, who opportunistically utilize the spectrum without a license in the same location. Since both types of users can access the licensed spectrum, system spectral efficiency can be improved [6]. More specifically, cognitive radio can be classified into underlay and overlay approaches. In the overlay approach, secondary users may access the spectrum only when the primary users are not utilizing their allocated

bands. In contrast, in the underlay approach, primary users can allow simultaneous sharing of the licensed spectrum with secondary users, provided that they do not cause harmful interference. From the perspective of primary users, the secondary users' transmission is treated as interference and must be strictly limited under the primary user transmission guarantee [7,8]. Due to transmit power limitation, secondary users in underlay cognitive radio networks often require multi-hop transmission to reliably deliver messages. In such scenarios, when a secondary user needs to send a message from a transmitter to a receiver, multiple relay nodes are typically required to support the legitimate user's transmission. However, as more relay nodes participate in this transmission, malicious users can more easily intercept confidential messages due to the broadcast nature of the wireless medium [9]. As a result, security in underlay cognitive radio networks is even more critical than in other types of networks.

Encryption is a widely used solution for ensuring confidentiality by concealing the content of transmitted messages. Nevertheless, encryption and decryption processes bring additional overhead, leading to high latency, which is particularly critical in mobile networks. To overcome these limitations, physical layer security (PHY-security) [10], which leverages the inherent characteristics of wireless channels, has recently gained attention as a promising alternative security solution in wireless networks [9,11]. In order to enhance PHY-security, we can employ opportunistic scheduling schemes that use channel information to select users (or transmit antennas) based on the system's purpose [12–14]. For example, when a system aims to improve secrecy performance, it can select users (or transmit antennas) to minimize the eavesdropper's channel condition or maximize the secrecy capacity. As technology advances, eavesdroppers also try to improve their eavesdropping performance as well as the legitimate user performance [15–17]. More specifically, multiple eavesdroppers may collaborate to conduct eavesdropping, thereby enhancing their ability to intercept confidential transmissions. Consequently, various collaborative eavesdropping strategies have been investigated in the literature. A colluding attack occurs when multiple eavesdroppers cooperate to intercept the legitimate users' transmissions. By sharing the information they overhear, they are able to collectively exploit all intercepted data. In contrast, a non-colluding attack occurs when several eavesdroppers independently attempt to intercept the legitimate users' transmissions, and due to their independent operation, only the most effective eavesdropper is selected.

The authors in [18] proposed an anti-poisoning attack decentralized privacy-enhanced federated learning (APDPFL) scheme to protect flight operation data sharing. In [19], the authors proposed a method to solve the accurate recognition of named entities against spoken instructions for automatic speech recognition techniques in air traffic control. In these works [18,19], the authors address the advanced techniques for future mobile networks. However, they did not consider PHY-security. Different from the aforementioned works, in [20], although the considered network was not a cognitive radio network, the authors proposed a sub-optimal antenna selection scheme to enhance secrecy performance in multi-user single-input multi-output (MU-MISO) non-orthogonal multiple access (NOMA) networks under various eavesdropping scenarios. In [21], the authors proposed a novel network architecture to enhance the secrecy performance in vehicular networks with cooperative jamming helpers. The authors in [22] exploited secrecy performance in simultaneous wireless information and power transfer (SWIPT)-based cooperative vehicular relaying networks. The authors in [23] investigated the secrecy performance on intelligent reflecting surface (IRS) networks. This work had a research limitation in that it did not propose how to enhance the secrecy performance on the considered networks. These works [20–23] did not consider the secrecy performance in underlay cognitive radio network environments.

The authors in [24] exploited the impact of imperfect channel information on the secrecy performance in underlay cognitive radio multi-hop transmission. This work did not consider the impact of various eavesdropping attacks on the secrecy performance. The authors in [25] addressed the secure transmission in an underlay cognitive radio–NOMA system with a cooperative relay and an energy harvesting node. The authors in [26] considered secure transmission on cognitive radio networks with a full-duplex receiver. In [27], the authors studied reconfigurable intelligent surface (RIS)-assisted secure communication in cognitive radio systems. These works [24–27] considered secure transmission in underlay cognitive radio. However, they did not consider various eavesdropping attack scenarios.

From the aforementioned works [20–27], we conclude that enhancing secrecy performance in underlay cognitive radio networks is essential for future mobile networks. To this end, we raise two key research questions: (1) How can confidential messages be protected against various eavesdropping attacks? (2) How do different opportunistic scheduling schemes and/or eavesdropping strategies affect secrecy performance?

In this paper, we investigate the impact of various eavesdropping attacks on secrecy performance in multi-hop transmission architectures. To protect confidential messages in underlay cognitive radio networks, we propose two opportunistic scheduling schemes designed to enhance secrecy performance. In detail, the first scheduling scheme can select the relay at each cluster to minimize the eavesdropper channel condition. The second proposed scheme requires both the main channel and eavesdropper channel information to maximize the secrecy channel capacity. The main contributions of this paper are summarized as follows:

- In this work, we investigate the impact of various eavesdropping attacks on multi-hop transmission in underlay cognitive radio networks. Specifically, we consider a scenario where multiple eavesdroppers are present. These eavesdroppers may either collaborate by sharing intercepted information (colluding attack) or act independently (non-colluding attack). To the best of our knowledge, this network architecture has not been reported in the existing literature.
- We propose two types of opportunistic scheduling schemes to enhance secrecy performance. The first scheme, called the minimal node selection (MNS) scheme, selects a node in each cluster to minimize the eavesdropper's channel condition. This node selection scheme only requires the eavesdropper's channel information, which leads to lower computational complexity. The second scheme, called the optimal node selection (ONS) scheme, selects a node in each cluster to maximize secrecy performance. Since the ONS scheme requires both the main channel and eavesdropper channel information, it achieves more robust secrecy performance compared to the MNS scheme.
- To capture the relationship between network parameters and secrecy performance, we derive closed-form expressions for the secrecy outage probability (SOP) under the proposed scheduling schemes and various eavesdropping attacks. In addition, we analyze the complexity order to provide further insights into the amount of channel information required for node selection.
- To evaluate the impact of the proposed node selection schemes and various eavesdropping attacks on secrecy performance, we compare the proposed methods with a benchmark scheme that does not utilize channel state information for node selection within each cluster. Furthermore, we investigate the effects of key network parameters, including the interference threshold, target secrecy data rate, and the number of eavesdroppers, nodes per cluster, and hops, on secrecy performance. The results demonstrate that the proposed opportunistic scheduling schemes significantly

enhance secrecy performance compared to the benchmark scheme, while colluding attacks are shown to be more detrimental to secrecy performance.

The rest of the paper is organized as follows: Section 2 explains the considered multi-hop transmission scenario and the proposed opportunistic scheduling scheme. Section 3 analyzes the closed-form expression for SOP with the proposed opportunistic scheduling scheme and various eavesdropping attacks. Section 4 presents the performance evaluation based on the obtained closed-form expression and simulation results. Finally, we conclude this paper in Section 5.

2. System Model

Let us consider a multi-hop secure transmission in underlay cognitive radio networks, as depicted in Figure 1. According to the principle of underlay cognitive radio, the transmit power level of the secondary users is limited by the interference threshold. Thus, direct transmission between the source node and the destination node is difficult. In order to assist the transmission between the source node and the destination node, an intermediate node is located in the $(K-1)$th cluster, with $K > 1$. According to the principle of the wireless medium, eavesdroppers can overhear the legitimate users' transmissions. Furthermore, we assume that the legitimate users are equipped with a single antenna and operate in half-duplex mode. The main notations of this paper are summarized in Table 1.

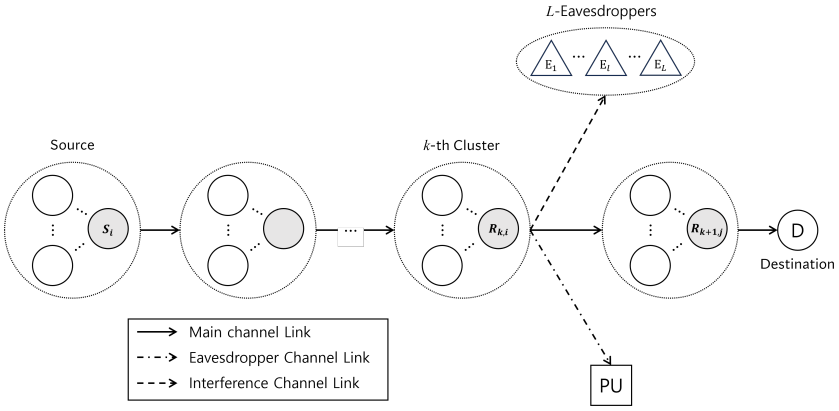

Figure 1. The illustration of the secure multi-hop transmission in the underlay cognitive radio network with multiple eavesdroppers.

Table 1. Notation summary.

Notation	Definition
S_i	The source node in the first cluster, where $i \in \{1, 2, N_0\}$.
$\mathsf{R}_{k,i}$	The i-th node in the k-th cluster; $\mathsf{R}_{0,1} \equiv \mathsf{S}_i$ and $\mathsf{R}_{K,1} \equiv \mathsf{D}$, with $k \in \{0, 1, \cdots, K\}$.
D	The destination node.
P	The primary node.
E_l	The l-th eavesdropper, where $l \in \{1, 2, \cdots, L\}$.
$\lvert h_{k,i,j} \rvert^2$	The channel gain of link $\mathsf{R}_{k-1,i} \to \mathsf{R}_{k,j}$.
$\lvert h_{k,i,\mathsf{P}} \rvert^2$	The channel gain of link $\mathsf{R}_{k-1,i} \to \mathsf{PU}$.
$\lvert h_{k,i,l} \rvert^2$	The channel gain of link $\mathsf{R}_{k-1,i} \to \mathsf{E}_l$.
$\lambda_{k,i,j}$, $\lambda_{k,i,\mathsf{P}}$, and $\lambda_{k,i,l}$	The means of $\lvert h_{k,i,j} \rvert^2$, $\lvert h_{k,i,\mathsf{P}} \rvert^2$, and $\lvert h_{k,i,l} \rvert^2$, respectively.
$P_{k,i}$	The transmit power level at the i-th node in the k-th cluster.
$\mathcal{I}_{\text{th}}$	The interference threshold.

In this paper, we consider the channel between X and Y, where $\mathsf{X} \in \{\mathsf{S}_i, \mathsf{R}_{k,i}\}$ and $\mathsf{Y} \in \{\mathsf{R}_{k,i}, \mathsf{D}, \mathsf{E}_l, \mathsf{P}\}$, with $\mathsf{X} \neq \mathsf{Y}$. $\hat{h}_{\mathsf{XY}}$ and G_{XY} represent the small-scale fading and large-scale path-loss effect, respectively. Since we suppose that the link can be described as independent and identical distributed (i.i.d.) Rayleigh block flat fading, the corresponding gain ($|h_{\mathsf{XY}}|^2$) follows an Exponential distribution. The large-scale path-loss effect can be defined as $G_{\mathsf{XY}} = \mathcal{L}(d_0/d_{\mathsf{XY}})^{\epsilon}$, where d_{XY} represents the Euclidean distance between X and Y, d_0 represents the reference distance, $\mathcal{L}$ represents the estimated power attenuation at d_0 (dB unit), and ϵ represents the path-loss exponent. In this paper, we consider both the small-scale fading and large-scale path-loss effect, i.e., $h_{\mathsf{XY}} \triangleq G_{\mathsf{XY}}\hat{h}_{\mathsf{XY}}$. The cumulative distribution function (CDF) and probability density function (PDF) of $|h_{\mathsf{XY}}|^2$ can be modeled as

$$F_{|h_{\mathsf{XY}}|^2}(h) = 1 - e^{-\frac{1}{\lambda_{\mathsf{XY}}}h}, \tag{1}$$

$$f_{|h_{\mathsf{XY}}|^2}(h) = \frac{1}{\lambda_{\mathsf{XY}}} e^{-\frac{1}{\lambda_{\mathsf{XY}}}h}, \tag{2}$$

where λ_{XY} indicates the average of $|h_{\mathsf{XY}}|^2$.

2.1. Data Transmission Phase

According to the principle of underlay cognitive radio, the transmit power level of each secondary user is limited under the interference threshold [16,24]. Thus, the transmit power at R_i ($P_{k,i}$) is mathematically expressed as

$$P_{k,i} = \frac{\mathcal{I}_{\text{th}}}{|h_{k,i,\mathsf{P}}|^2}. \tag{3}$$

The received signal at $\mathsf{R}_{k+1,j}$ can be expressed as

$$y_{k,i,j} = \sqrt{P_{k,i}} h_{k,i,j} x_{k,i} + n_j, \tag{4}$$

where $h_{k,i,j}$ stands for channel coefficient of link $\mathsf{R}_{k,i} \rightarrow \mathsf{R}_{k+1,j}$ and n_j is the channel noise, which follows the additive white Gaussian noise (AWGN) distribution with zero mean and σ_j^2. Thus, the instantaneous signal-to-noise ratio (SNR) of the main channel for k-hop transmission can be expressed as

$$\gamma_{k,i,j} = \frac{P_{k,i}|h_{k,i,j}|^2}{\sigma_j^2} = \frac{\mathcal{I}_{\text{th}}|h_{k,i,j}|^2}{|h_{k,i,\mathsf{P}}|^2\sigma_j^2}. \tag{5}$$

As can be observed in Figure 1, when the legitimate users transmit the confidential information, the l-th eavesdropper tries to intercept the information. In this paper, we exploit the impact of the eavesdropping attacks on the secrecy performance. Thus, the first scenario is called a colluding attack, where the eavesdroppers share the overheard information to enhance the wiretapping ability. The other scenario is a non-colluding attack, where the eavesdroppers work independently.

According to the principle of the wireless medium, the overheard k-th hop signal at the l-th eavesdropper can be expressed as

$$y_{k,i,l} = \sqrt{P_{k,i}} h_{k,i,l} x_{k,i} + n_l, \tag{6}$$

where $h_{k,i,l}$ indicates the channel coefficient at the l-th eavesdropper on the k-th hop signal and n_l is the channel noise, which follows the AWGN distribution with zero mean and σ_l^2 variance. In this paper, we can further assume that $\sigma_l^2 = \sigma_{\mathsf{E}}^2$.

2.1.1. Scenario 1: Colluding Attack

Since each eavesdropper can share the intercepted information, they can combine the intercepted information. Thus, the wiretapped SNR under the colluding attack can be expressed as

$$\gamma_{k,i,\mathsf{E}}^{\mathsf{co}} = \frac{P_{k,i}\sum_{l=1}^{L}|h_{k,i,l}|^2}{\sigma_{\mathsf{E}}^2} = \frac{\mathcal{I}_{\mathrm{th}}\sum_{l=1}^{L}|h_{k,i,l}|^2}{|h_{k,i,\mathsf{P}}|^2\sigma_{\mathsf{E}}^2}, \tag{7}$$

where the superscript "co" stands for the colluding attack.

2.1.2. Scenario 2: Non-Colluding Attack

Different from the colluding attack, the non-colluding attack does not share the intercepted information. Thus, we can further assume that the maximal intercepted information is the system intercepted information, in which the SNR can be mathematically expressed as

$$\gamma_{k,i,\mathsf{E}}^{\mathsf{nc}} = \frac{P_{k,i}\max_{1\le l\le L}\{|h_{k,i,l}|^2\}}{\sigma_{\mathsf{E}}^2} = \frac{\mathcal{I}_{\mathrm{th}}\max_{1\le l\le L}\{|h_{k,i,l}|^2\}}{|h_{k,i,\mathsf{P}}|^2\sigma_{\mathsf{E}}^2}, \tag{8}$$

where the superscript "nc" indicates the non-colluding attack.

In this study, the secrecy capacity is defined as the difference between the main channel capacity and the eavesdropper channel capacity. Thus, the end-to-end secrecy capacity can be mathematically expressed as [28]

$$C_{\mathrm{sec}}^{\mathsf{att}} = \frac{1}{K}\min_{k\in K}\left\{\log_2\left(\frac{1+\gamma_{k,i,j}}{1+\gamma_{k,i,\mathsf{E}}^{\mathsf{att}}}\right)\right\}, \tag{9}$$

where $\mathsf{att} \in \{\mathsf{co}, \mathsf{nc}\}$.

2.2. The Proposed Node Selection Schemes

In this subsection, we introduce several node selection schemes to enhance the end-to-end secrecy performance to protect the confidential message against various eavesdropper attacks.

2.2.1. The Minimal Node Selection (MNS) Scheme

This node selection scheme can select a node in each cluster to minimize the eavesdropper channel capacity, which can be mathematically expressed as

$$\mathsf{R}_{k,i^*} = \min_{i\in M}\{\log_2(1+\gamma_{k,i,\mathsf{E}}^{\mathsf{att}})\} = \min_{i\in M}\{|h_{k,i,j^*}|^2\}. \tag{10}$$

Then, the instantaneous SNR of the main channel and eavesdropper channel can be, respectively, expressed as

$$\gamma_{k,i,j}^{\mathsf{MNS}} = \frac{\mathcal{I}_{\mathrm{th}}|h_{k,i^*,j^*}|^2}{|h_{k,i^*,\mathsf{P}}|^2\sigma_j^2}, \tag{11}$$

$$\gamma_{k,i,\mathsf{E}}^{\mathsf{MNS,co}} = \frac{\mathcal{I}_{\mathrm{th}}\sum_{l=1}^{L}\min_{i\in M}\{|h_{k,i,l}|^2\}}{|h_{k,i^*,\mathsf{P}}|^2\sigma_{\mathsf{E}}^2}, \tag{12}$$

$$\gamma_{k,i,\mathsf{E}}^{\mathsf{MNS,nc}} = \frac{\mathcal{I}_{\mathrm{th}}\max_{1\le l\le L}\{\min_{i\in M}\{|h_{k,i,l}|^2\}\}}{|h_{k,i,\mathsf{P}}|^2\sigma_{\mathsf{E}}^2}. \tag{13}$$

2.2.2. The Optimal Node Selection (ONS) Scheme

The last node selection, named the optimal node selection (ONS) scheme, can select a node to maximize the secrecy capacity. The ONS scheme can be mathematically expressed as

$$\mathsf{R}_{k,i^*} = \max_{1\le i\le M}\left\{\log_2\left(\frac{1+\gamma_{k,i,j^*}}{1+\gamma^{\mathsf{att}}_{k,i,\mathsf{E}}}\right)\right\}. \tag{14}$$

Similar to the other node selection schemes, the SNR of the main channel and eavesdropper channel under the ONS scheme can be, respectively, expressed as

$$\gamma^{\mathsf{ONS}}_{k,i^*,j^*} = \frac{\mathcal{I}_{\mathrm{th}}|h_{k,i^*,j^*}|^2}{|h_{k,i^*,\mathsf{P}}|^2\sigma_j^2}, \tag{15}$$

$$\gamma^{\mathsf{ONS,co}}_{k,i^*,\mathsf{E}} = \frac{\mathcal{I}_{\mathrm{th}}\sum_{l=1}^{L}\{|h_{k,i^*,l}|^2\}}{|h_{k,i^*,\mathsf{P}}|^2\sigma_{\mathsf{E}}^2}, \tag{16}$$

$$\gamma^{\mathsf{ONS,nc}}_{k,i^*,\mathsf{E}} = \frac{\mathcal{I}_{\mathrm{th}}\max_{1\le l\le L}\{|h_{k,i^*,l}|^2\}}{|h_{k,i^*,\mathsf{P}}|^2\sigma_{\mathsf{E}}^2}. \tag{17}$$

3. Secrecy Outage Performance Analysis

In this context, the secrecy outage probability (SOP) is used for secrecy performance in the viewpoint of information theory. It is defined as the probability that the difference between the main channel and eavesdropper channel capacities is smaller than the predefined threshold, called the secrecy target data rate (R_{th}) (bps/Hz), and can be mathematically expressed as [29,30]

$$P^{\mathsf{sch,att}}_{\mathrm{out}} = \Pr\left[\frac{1}{K}\min_{k\in K}\left\{\log_2\left(\frac{1+\gamma^{\mathsf{sch}}_{k,i,j}}{1+\gamma^{\mathsf{sch,att}}_{k,i,\mathsf{E}}}\right)\right\} < R_{\mathrm{th}}\right], \tag{18}$$

where $\mathsf{sch}\in\{\mathsf{MNS},\mathsf{ONS}\}$. For the sake of simplicity, the self-defined constants are presented in Table 2.

Table 2. Self-defined constants.

$X_{k,i,j} = \lvert h_{k,i,j}\rvert^2$	$\gamma_{\mathrm{th}} = 2^{KR_{\mathrm{th}}}$
$Y_{k,i,\mathsf{E}_1} = \sum_{l=1}^{L}\lvert h_{k,i,l}\rvert^2$	$\bar{\gamma} = \mathcal{I}_{\mathrm{th}}$
$Y_{k,i,\mathsf{E}_e} = \max_{1\le l\le L}\{\lvert h_{k,i,l}\rvert^2\}$	$\sigma_1^2 = \cdots = \sigma_j^2 = \sigma^2$
$Z_{k,i\mathsf{P}} = \lvert h_{k,i,\mathsf{P}}\rvert^2$	$\sigma_{\mathsf{E}}^2 = \sigma^2$

3.1. MNS Scheme and Colluding Attack

The following lemmas will help to calculate the closed-form expression for SOP with the MNS scheme and a colluding attack.

Lemma 1. $\Pr(i^* = i)$ *can be formulated as*

$$\Pr(i^* = i) = \frac{1}{\Gamma(L)}\sum_{m=0}^{M_0} b_m^{M-1}\frac{\Gamma(L+m)}{M^{L+m}}, \tag{19}$$

where the following notation is adopted

$$b_m^{M-1} = \begin{cases} 1 & , \text{if } m{=}0 \\ M-1 & , \text{if } m{=}1 \\ \frac{1}{m}\sum_{j=1}^{J_0} \frac{jM-m}{\Gamma(j+1)} b_{m-j}^{M-1} & , \text{if } 1{<}m{<}M_0 \\ \left[\frac{1}{\Gamma(L)}\right]^{M-1} & , \text{if } m{=}M_0 \end{cases}$$

with $J_0 = \min\{m, L-1\}$ *and* $M_0 = (M-1)(L-1)$.

Proof. See [20]. □

Lemma 2. *The CDF and PDF of* Y_{k,i^*,E_1} *can be expressed as*

$$F_{Y_{k,i^*,\mathsf{E}_1}}(y) = 1 - \sum_{m=0}^{M(L-1)} \frac{b_m^M}{(\lambda_{k,i,l})^m} y^m e^{-\frac{M}{\lambda_{k,i,l}} y}, \tag{20}$$

$$f_{Y_{k,i^*,\mathsf{E}_1}}(y) = \frac{M}{\lambda_{k,i,l}\Gamma(L)} \sum_{m=0}^{M_0} \frac{b_m^{M-1}}{(\lambda_{k,i,l})^{L-1+m}} y^{L-1+m} e^{-\frac{M}{\lambda_{k,i,l}} y}, \tag{21}$$

where the following notation is adopted

$$b_m^M = \begin{cases} 1 & , \text{if } m{=}0 \\ M & , \text{if } m{=}1 \\ \frac{1}{m}\sum_{j=1}^{J_0} \frac{j(M+1)-m}{\Gamma(j+1)} b_{m-j}^{M} & , \text{if } 1{<}m{<}M_0 \\ \left[\frac{1}{\Gamma(L)}\right]^{M} & , \text{if } m{=}M_0 \end{cases}$$

with b_m^{M-1}, J_0, *and* M_0 *defined as in* (19).

Proof. See [20]. □

Theorem 1. *The closed-form expression for SOP with the MNS scheme and a colluding attack can be derived as*

$$\begin{aligned} P_{\text{out}}^{\mathsf{MNS,co}} = 1 - \prod_{k=1}^{K} \Bigg[& 1 - \frac{M}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{M^{L+m}} \\ & \times \left(\frac{M}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{M^{L+m}} - \frac{M}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}} \left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l} + M\lambda_{k,i,j}} \right)^{L+m} \right) \Bigg]. \end{aligned} \tag{22}$$

Proof. From (18), $P_{\text{out}}^{\mathsf{MNS,co}}$ can be further expressed as

$$P_{\text{out}}^{\mathsf{MNS,co}} = 1 - \prod_{k=1}^{K} \Bigg[1 - \underbrace{\Pr\left[\frac{1+\gamma_{k,i^*,j^*}^{\mathsf{MNS}}}{1+\gamma_{k,i^*,\mathsf{E}}^{\mathsf{MNS,co}}} < \gamma_{\text{th}} \right]}_{\Omega_{\mathsf{A}}} \Bigg]. \tag{23}$$

As can be seen, since it includes the same components, the events of the probability in (23) are not mutually exclusive. By conditioning $Y_{k,i^*,\mathsf{E}_1} = y$ and relying on the total probability [31], Ω_{A} in (23) can be further written as

$$\begin{aligned}\Omega_{\mathsf{A}} &= \Pr\left[X_{k,i^*,j^*} < \frac{\gamma_{\text{th}}-1}{\bar{\gamma}} Z_{k,i^*,\mathsf{P}} + \gamma_{\text{th}} Y_{k,i^*,\mathsf{E}}\right] \\ &= \sum_{i=1}^{M} \Pr[i^*=i] \int_0^{\infty} \underbrace{\Pr\left[X_{k,i^*,j^*} < \frac{\gamma_{\text{th}}-1}{\bar{\gamma}} Z_{k,i^*,\mathsf{P}} + \gamma_{\text{th}} y\right]}_{\Omega_{\mathsf{A}_1}} f_{Y_{k,i^*,\mathsf{E}_1}}(y)dy.\end{aligned} \tag{24}$$

In order to further express (24), Ω_{A_1} can be re-expressed as

$$\begin{aligned}\Omega_{\mathsf{A}_1} &= \int_0^{\infty} \left(1 - e^{-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{\text{th}}-1}{\bar{\gamma}} z + \gamma_{\text{th}} y\right)}\right) \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{1}{\lambda_{k,i,\mathsf{P}}} z} dz \\ &= \underbrace{\int_0^{\infty} \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{1}{\lambda_{k,i,\mathsf{P}}} z} dz}_{\Omega_{\mathsf{A}_2}} - \underbrace{\int_0^{\infty} \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y - \left(\frac{\gamma_{\text{th}}-1}{\bar{\gamma}\lambda_{k,i,j}} + \frac{1}{\lambda_{k,i,\mathsf{P}}}\right) z} dz}_{\Omega_{\mathsf{A}_3}}.\end{aligned} \tag{25}$$

When we rely on the facts from [32] (eq. 3.310), Ω_{A_2} and Ω_{A_3} can be expressed as

$$\Omega_{\mathsf{A}_2} = \int_0^{\infty} \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{1}{\lambda_{k,i,\mathsf{P}}} z} dz = 1, \tag{26}$$

$$\Omega_{\mathsf{A}_3} = \int_0^{\infty} \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y - \left(\frac{\gamma_{\text{th}}-1}{\bar{\gamma}\lambda_{k,i,j}} + \frac{1}{\lambda_{k,i,\mathsf{P}}}\right) z} dz = \frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y}. \tag{27}$$

By plugging (26) and (27) into (25), Ω_{A_1} can be re-written as

$$\Omega_{\mathsf{A}_1} = 1 - \frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y}. \tag{28}$$

Again, by substituting (19) and (28) into (24), Ω_{A_1} can be expressed as

$$\begin{aligned}\Omega_{\mathsf{A}_1} &= \sum_{m=1}^{M} \frac{1}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{M^{L+m}} \int_0^{\infty} \left(1 - \frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,j} + \bar{\gamma}\lambda_{k,i,j}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y}\right) \frac{M}{\lambda_{k,i,l}\Gamma(L)} \sum_{m=0}^{M_0} \frac{b_m^{M-1}}{\lambda_{k,i,l}^{L-1+m}} y^{L-1+m} e^{-\frac{M}{\lambda_{k,i,l}} y} dy \\ &= \sum_{m=1}^{M} \frac{1}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{M^{L+m}} \Bigg[\underbrace{\int_0^{\infty} \frac{M}{\lambda_{k,i,l}\Gamma(L)} \sum_{m=0}^{M_0} \frac{b_m^{M-1}}{\lambda_{k,i,l}^{L-1+m}} y^{L-1+m} e^{-\frac{M}{\lambda_{k,i,l}} y} dy}_{\Omega_{\mathsf{A}_4}} \\ &\quad - \underbrace{\int_0^{\infty} \frac{M\bar{\gamma}\lambda_{k,i,j}}{\lambda_{k,i,l}\Gamma(L)((\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j})} \sum_{m=0}^{M_0} \frac{b_m^{M-1}}{\lambda_{k,i,l}^{L-1+m}} y^{L-1+m} e^{-\left(\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} + \frac{M}{\lambda_{k,i,l}}\right)} dy}_{\Omega_{\mathsf{A}_5}} \Bigg].\end{aligned} \tag{29}$$

By using the fact from [32] (eq. 3.351.3), Ω_{A_4} and Ω_{A_5} in (29) can be, respectively, expressed as

$$\Omega_{\mathsf{A}_4} = \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{\Gamma(L) M^{L+m-1}}, \tag{30}$$

$$\Omega_{\mathsf{A}_5} = \sum_{m=0}^{M_0} b_m^{M-1} \frac{M\Gamma(L+m)}{\Gamma(L)} \left(\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}}\right) \left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l} + M\lambda_{k,i,j}}\right)^{L+m}. \tag{31}$$

By plugging (30) and (31) into (29), Ω_{A} can be expressed as

$$\begin{aligned}\Omega_{\mathsf{A}} =& \frac{M}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{M^{L+m}} \\ &\times \left(\frac{M}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)}{M^{L+m}} - \frac{M}{\Gamma(L)} \sum_{m=0}^{M_0} b_m^{M-1} \frac{\Gamma(L+m)\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}} \left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l} + M\lambda_{k,i,j}}\right)^{L+m}\right).\end{aligned} \tag{32}$$

By plugging (32) into (23), the closed-form expression for SOP with the MNS scheme and a colluding attack can be obtained as (22). The proof of Theorem 1 is concluded. □

3.2. MNS Scheme and Non-Colluding Attack

The following lemmas will help to calculate the closed-form expression for SOP with the MNS scheme and a non-colluding attack.

Lemma 3. $\Pr(i^* = i)$ *is derived as*

$$\Pr(i^* = i) = \sum_{A_1} \frac{L}{l_1 + l_2 + 1}, \tag{33}$$

where the following notation is adopted

$$\sum_{A_1} = \sum_{m=0}^{M-1} \sum_{l_1=0}^{mL} \sum_{l_2=0}^{L-1} \binom{M-1}{m} \binom{mL}{l_1} \binom{L-1}{l_2} (-1)^{m+l_1+l_2}.$$

Proof. See [20]. □

Lemma 4. *The CDF and PDF of* Y_{k,i^*,E_2} *can be derived as*

$$F_{Y_{k,i^*,\mathsf{E}_2}}(y) = 1 - \sum_{A_2} e^{-\frac{l}{\lambda_{k,i,l}} y}, \tag{34}$$

$$f_{Y_{k,i^*,\mathsf{E}_2}}(y) = \frac{ML}{\lambda_{k,i,l}} \sum_{A_1} e^{-\frac{l_1+l_2+1}{\lambda_{k,i,l}} y}, \tag{35}$$

where $\sum_{A_1}$ *is defined in* (33) *and the following notation is adopted as*

$$\sum_{A_2} = \sum_{m=0}^{M} \sum_{l=0}^{mL} \binom{M}{m} \binom{mL}{l} (-1)^{m+l}.$$

Proof. See [20]. □

Theorem 2. *The closed-form expression for SOP with the MNS scheme and a non-colluding attack can be derived as*

$$P_{\text{out}}^{\mathsf{MNS,nc}} = 1 - \prod_{k=1}^{K} \left[1 - \sum_{A_1} \frac{ML}{l_1 + l_2 + 1} \left(\sum_{A_1} \frac{ML}{l_1 + l_2 + 1} - \sum_{A_1} \left(\frac{\bar{\gamma} \lambda_{k,i,j}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma} \lambda_{k,i,j}} \right) \left(\frac{ML \lambda_{k,i,j}}{\gamma_{\text{th}} \lambda_{k,i,l} + (l_1 + l_2 + 1)\lambda_{k,i,j}} \right) \right) \right] \tag{36}$$

Proof. From (18), $P_{\text{out}}^{\mathsf{MNS,nc}}$ can be further expressed as

$$P_{\text{out}}^{\mathsf{MNS,nc}} = 1 - \prod_{k=1}^{K} \Bigg[1 - \underbrace{\Pr \left[\frac{1 + \gamma_{k,i^*,j^*}^{\mathsf{MNS}}}{1 + \gamma_{k,i^*,\mathsf{E}}^{\mathsf{MNS,nc}}} < \gamma_{\text{th}} \right]}_{\Omega_{\mathsf{B}}} \Bigg]. \tag{37}$$

Ω_{B} in (37) can be further expressed as

$$\Omega_{\mathsf{B}} = \Pr \left[X_{k,i^*,j^*} < \frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} Z_{k,i^*,\mathsf{P}} + \gamma_{\text{th}} Y_{k,i^*,\mathsf{E}_2} \right] \tag{38}$$

As can be observed, the events of the provability are not mutually exclusive. By condition-

ing $Y_{k,i^*,\mathsf{E}_2} = y$ and relying on the total probability [31], Ω_{B} can be re-written as

$$\Omega_{\mathsf{B}} = \sum_{i=1}^{M} \Pr[i^* = i] \int_0^{\infty} \underbrace{\Pr\left[X_{k,i,j^*} < \frac{\gamma_{\mathrm{th}} - 1}{\bar{\gamma}} Z_{k,i,\mathsf{P}} + \gamma_{\mathrm{th}} y\right]}_{\Omega_{\mathsf{B}_1}} f_{Y_{k,i^*,\mathsf{E}_2}}(y) dy. \tag{39}$$

Ω_{B_1} in (39) can be re-written as

$$\begin{aligned} \Omega_{\mathsf{B}_1} &= \int_0^{\infty} F_{k,i,j^*}\left(\frac{\gamma_{\mathrm{th}} - 1}{\bar{\gamma}} z + \gamma_{\mathrm{th}} y\right) f_{Z_{k,i,\mathsf{P}}}(z) dz \\ &= \int_0^{\infty} \left[1 - e^{-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{\mathrm{th}}-1}{\bar{\gamma}} z + \gamma_{\mathrm{th}} y\right)}\right] \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{1}{\lambda_{k,i,\mathsf{P}}} z} dz \end{aligned} \tag{40}$$

When we utilize the fact in [32] (eq. 3.310), Ω_{B_1} can be calculated as

$$\Omega_{\mathsf{B}_1} = 1 - \frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\mathrm{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}} e^{-\frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}} y}. \tag{41}$$

Plugging (35) and (41) into (39), Ω_{B} can be expressed as

$$\Omega_{\mathsf{B}} = \sum_{i=1}^{M} \sum_{A_1} \frac{L}{l_1 + l_2 + 1} \left[\underbrace{\int_0^{\infty} \sum_{A_3} \frac{ML}{\lambda_{k,i,l}} e^{-\frac{l_1+l_2+1}{\lambda_{k,i,l}} y} dy}_{\Omega_{\mathsf{B}_2}} - \underbrace{\int_0^{\infty} \sum_{A_3} \frac{ML}{\lambda_{k,i,l}} \frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\mathrm{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}} e^{-\left(\frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}} + \frac{\gamma_{\mathrm{th}}}{\lambda_{k,i,j}}\right) y} dy}_{\Omega_{\mathsf{B}_3}} \right] \tag{42}$$

Again, relying on the fact in [32] (eq. 3.310), Ω_{B_2} and Ω_{B_3} in (42) can be, respectively, written as

$$\Omega_{\mathsf{B}_2} = \sum_{A_3} \frac{ML}{l_1 + l_2 + 1}, \tag{43}$$

$$\Omega_{\mathsf{B}_3} = \sum_{A_3} \left(\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\mathrm{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma}\lambda_{k,i,j}}\right) \left(\frac{ML\lambda_{k,i,j}}{\gamma_{\mathrm{th}}\lambda_{k,i,l} + (l_1 + l_2 + 1)\lambda_{k,i,j}}\right). \tag{44}$$

By substituting (43) and (44) into (42) and after some mathematical steps, the closed-form expression for SOP with the MNS scheme and a non-colluding attack is obtained as (36). The proof of Theorem 2 is concluded. □

3.3. ONS Scheme and Colluding Attack

The following lemmas will help to analyze the closed-form expression for SOP with various eavesdropping attacks.

Lemma 5. *The CDF and PDF of Y_{k,i,E_1} can be calculated as*

$$F_{Y_{k,i,\mathsf{E}_1}}(y) = \frac{\gamma(L, y/\lambda_{k,i,l})}{\Gamma(L)} = 1 - \sum_{l=0}^{L-1} \frac{1}{l!(\lambda_{k,i,l})^l} t^l e^{-\frac{1}{\lambda_{k,i,l}} t}, \tag{45}$$

$$f_{Y_{k,i,\mathsf{E}_1}}(y) = \frac{1}{\lambda_{k,i,l}\Gamma(L)} \left(\frac{y}{\lambda_{k,i,l}}\right)^{L-1} e^{-\frac{y}{\lambda_{k,i,l}}}, \tag{46}$$

where $\gamma(\alpha, \beta)$ denotes the lower incomplete Gamma function and $\Gamma(\cdot)$ stands for the Gamma distribution [32].

Proof. See [20]. □

Theorem 3. *The closed-form expression for SOP with the ONS scheme and a colluding attack can be derived as*

$$P_{\text{out}}^{\text{ONS,co}} = 1 - \prod_{k=1}^{K} \left[1 - \sum_{m=0}^{M} \binom{M}{m} (-1)^m \left(\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\text{P}} + \bar{\gamma}\lambda_{k,i,j}} \right)^m \left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l} + \lambda_{k,i,j}} \right)^{mL} \right]. \tag{47}$$

Proof. From (18), $P_{\text{out}}^{\text{ONS,co}}$ can be re-written as

$$P_{\text{out}}^{\text{ONS,co}} = 1 - \prod_{k=1}^{K} \left[1 - \underbrace{\Pr\left[\frac{1 + \gamma_{k,i^*,j^*}}{1 + \gamma_{k,i^*,\text{E}_1}} < \gamma_{\text{th}} \right]}_{\Phi_{\text{A}}} \right]. \tag{48}$$

Relying on the principle of max probability [31], Φ_{A} in (48) can be re-formulated as

$$\begin{aligned} \Phi_{\text{A}} &= \Pr\left[\max_{m \in M} \left\{ \frac{1 + \frac{\bar{\gamma} X_{k,i,j^*}}{Z_{k,i,\text{P}}}}{1 + \frac{\bar{\gamma} Y_{k,i,\text{E}_1}}{Z_{k,i,\text{P}}}} \right\} < \gamma_{\text{th}} \right] \\ &= \prod_{m=1}^{M} \underbrace{\Pr\left[X_{k,i,j^*} < \frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} Z_{k,i,\text{P}} + \gamma_{\text{th}} Y_{k,i,\text{E}_1} \right]}_{\Phi_{\text{A}_1}}. \end{aligned} \tag{49}$$

Φ_{A_1} in (49) can be re-expressed as

$$\Phi_{\text{A}_1} = \int_0^\infty \underbrace{\int_0^\infty F_{X_{k,i,j^*}}\left(\frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} z + \gamma_{\text{th}} y \right) f_{Z_{k,i,\text{P}}}(z) dz}_{\Phi_{\text{A}_2}} f_{Y_{k,i,\text{E}_1}}(y) dy. \tag{50}$$

Since X_{k,i,j^*} and $Z_{k,i,\text{P}}$ follow an exponential distribution [33], Φ_{A_2} in (50) can be written as

$$\begin{aligned} \Phi_{\text{A}_2} &= \int_0^\infty \left[1 - e^{-\frac{1}{\lambda_{k,i,j}}\left(\frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} z + \gamma_{\text{th}} y \right)} \right] \frac{1}{\lambda_{k,i,\text{P}}} e^{-\frac{1}{\lambda_{k,i,\text{P}}} z} dz \\ &= \frac{1}{\lambda_{k,i,\text{P}}} \underbrace{\int_0^\infty e^{-\frac{1}{\lambda_{k,i,\text{P}}} z} dz}_{\Phi_{\text{A}_3}} - \frac{1}{\lambda_{k,i,\text{P}}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y} \underbrace{\int_0^\infty e^{-\left(\frac{\gamma_{\text{th}} - 1}{\bar{\gamma}\lambda_{k,i,j}} + \frac{1}{\lambda_{k,i,\text{P}}} \right) z} dz}_{\Phi_{\text{A}_4}}. \end{aligned} \tag{51}$$

Utilizing the fact from [32] (eq. 3.310), Φ_{A_3} and Φ_{A_4} can be calculated as

$$\Phi_{\text{A}_3} = \frac{1}{\lambda_{k,i,\text{P}}}, \tag{52}$$

$$\Phi_{\text{A}_4} = \frac{\bar{\gamma}\lambda_{k,i,j}\lambda_{k,i,\text{P}}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\text{P}} + \bar{\gamma}\lambda_{k,i,j}}. \tag{53}$$

By plugging (52) and (53) into (51), Φ_{A_2} can be expressed as

$$\Phi_{\text{A}_2} = 1 - \frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\text{P}} + \bar{\gamma}\lambda_{k,i,j}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y}. \tag{54}$$

Again, by plugging (46) and (54) into (50), Φ_{A_1} can be re-expressed as

$$\begin{aligned}\Phi_{\mathsf{A}_1} &= \int_0^{\infty}\left[1-\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}}+\bar{\gamma}\lambda_{k,i,j}}e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}}y}\right]\left(\frac{1}{\lambda_{k,i,l}}\right)^{L}\frac{1}{\Gamma(L)}y^{L-1}e^{-\frac{1}{\lambda_{k,i,l}}y}dy \\ &= \left(\frac{1}{\lambda_{k,i,l}}\right)^{L}\frac{1}{\Gamma(L)}\underbrace{\int_0^{\infty}y^{L-1}e^{-\frac{1}{\lambda_{k,i,l}}y}dy}_{\Phi_{\mathsf{A}_5}}-\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}}+\bar{\gamma}\lambda_{k,i,j}}\left(\frac{1}{\lambda_{k,i,l}}\right)^{L}\frac{1}{\Gamma(L)}\underbrace{\int_0^{\infty}y^{L-1}e^{-\left(\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}}+\frac{1}{\lambda_{k,i,l}}\right)y}dy}_{\Phi_{\mathsf{A}_6}}.\end{aligned} \tag{55}$$

When we rely on the fact from [32] (eq. 3.351.3), Φ_{A_5} and Φ_{A_6} in (55) can be expressed as

$$\Phi_{\mathsf{A}_5} = \Gamma(L)(\lambda_{k,i,l})^{L} \tag{56}$$

$$\Phi_{\mathsf{A}_6} = \Gamma(L)\left(\frac{\lambda_{k,i,j}\lambda_{k,i,l}}{\gamma_{\text{th}}\lambda_{k,i,l}+\lambda_{k,i,j}}\right)^{L} \tag{57}$$

By plugging (56) and (57) into (55), Φ_{A_1} can be expressed as

$$\Phi_{\mathsf{A}_1} = 1-\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}}+\bar{\gamma}\lambda_{k,i,j}}\left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l}+\lambda_{k,i,j}}\right)^{L} \tag{58}$$

Again, by substituting (58) into (49) and using the binomial theorem [34], Φ_{A} in (49) can be expressed as

$$\begin{aligned}\Phi_{\mathsf{A}} &= \left(1-\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}}+\bar{\gamma}\lambda_{k,i,j}}\left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l}+\lambda_{k,i,j}}\right)^{L}\right)^{M} \\ &= \sum_{m=0}^{M}\binom{M}{m}(-1)^{m}\left(\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}}+\bar{\gamma}\lambda_{k,i,j}}\right)^{m}\left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l}+\lambda_{k,i,j}}\right)^{mL}.\end{aligned} \tag{59}$$

By plugging (59) into (48) and some simple mathematical steps, the closed-form expression for SOP with the ONS scheme and a colluding attack can be obtained as (47). The proof of Theorem 3 is concluded. □

3.4. ONS Scheme and Non-Colluding Attack

Lemma 6. *The CDF and PDF of Y_{k,i,E_2} can be expressed as*

$$F_{Y_{k,i,\mathsf{E}_2}}(y) = \sum_{l=0}^{L}\binom{L}{l}(-1)^{l}e^{-\frac{1}{\lambda_{k,i,l}}y}, \tag{60}$$

$$f_{Y_{k,i,\mathsf{E}_2}}(y) = \frac{L}{\lambda_{k,i,l}}\sum_{l=0}^{L-1}\binom{L-1}{l}(-1)^{l}e^{-\frac{(l+1)}{\lambda_{k,i,l}}y}. \tag{61}$$

Proof. See [20]. □

Theorem 4. *The closed-form expression for SOP under the ONS scheme and a non-colluding attack can be derived as*

$$\begin{aligned}P_{\text{out}}^{\text{ONS,nc}} = 1-\prod_{k=1}^{K}\Bigg[1-\Bigg(&\sum_{l=0}^{L-1}\binom{L-1}{l}\frac{(-1)^{l}}{l+1} \\ &-\sum_{l=0}^{L-1}\binom{L-1}{l}(-1)^{l}\left(\frac{\bar{\gamma}\lambda_{k,i,j}}{(\gamma_{\text{th}}-1)\lambda_{k,i,\mathsf{P}}+\bar{\gamma}\lambda_{k,i,j}}\right)\left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}}\lambda_{k,i,l}+(l+1)\lambda_{k,i,j}}\right)\Bigg)^{M}\Bigg].\end{aligned} \tag{62}$$

Proof. From (18), $P_{\text{out}}^{\text{ONS,nc}}$ can be further expressed as

$$P_{\text{out}}^{\text{ONS,nc}} = 1 - \prod_{k=1}^{K} \Bigg[1 - \underbrace{\Pr\left[\max_{m \in M} \left\{ \frac{1 + \frac{\bar{\gamma} X_{k,i,j^*}}{Z_{k,i,\mathsf{P}}}}{1 + \frac{\bar{\gamma} Y_{k,i,\mathsf{E}_2}}{Z_{k,i,\mathsf{P}}}} \right\} < \gamma_{\text{th}} \right]}_{\Phi_{\mathsf{B}}} \Bigg]. \tag{63}$$

Φ_{B} in (63) can be re-written as

$$\Phi_{\mathsf{B}} = \prod_{m=1}^{M} \underbrace{\Pr\left[X_{k,i,j^*} < \frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} Z_{k,i,\mathsf{P}} + \gamma_{\text{th}} Y_{k,i,\mathsf{E}_2} \right]}_{\Phi_{\mathsf{B}_1}}. \tag{64}$$

In order to further express Φ_{B}, Φ_{B_1} in (64) can be re-expressed as

$$\Phi_{\mathsf{B}_1} = \int_0^\infty \underbrace{\int_0^\infty \Pr\left[X_{k,i,j^*} < \frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} z + \gamma_{\text{th}} y \right] f_{Z_{k,i,\mathsf{P}}}(z) dz}_{\Phi_{\mathsf{B}_2}} f_{Y_{k,i,\mathsf{E}_2}}(y) dy. \tag{65}$$

When we rely on the fact in ([32] (eq. 3.310), Φ_{B_2} can be further expressed as

$$\begin{aligned} \Phi_{\mathsf{B}_2} =& \int_0^\infty \frac{1}{\lambda_{k,i,\mathsf{P}}} e^{-\frac{1}{\lambda_{k,i,\mathsf{P}}} z} dz - \int_0^\infty e^{-\frac{1}{\lambda_{k,i,j}} \left(\gamma_{\text{th}} y + \frac{\gamma_{\text{th}} - 1}{\bar{\gamma}} z + \frac{\gamma_{\text{th}}}{\lambda_{k,i,\mathsf{P}}} z \right)} dz \\ =& 1 - \frac{\bar{\gamma} \lambda_{k,i,j}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma} \lambda_{k,i,j}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y}. \end{aligned} \tag{66}$$

By plugging (66) into (65), Φ_{B_1} can be expressed as

$$\begin{aligned} \Phi_{\mathsf{B}_1} =& \int_0^\infty \left(1 - \frac{\bar{\gamma} \lambda_{k,i,j}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma} \lambda_{k,i,j}} e^{-\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} y} \right) \frac{1}{\lambda_{k,i,l}} \sum_{l=0}^{L-1} \binom{L-1}{l} (-1)^l e^{-\frac{(l+1)}{\lambda_{k,i,l}} y} dy \\ =& \frac{1}{\lambda_{k,i,l}} \sum_{l=0}^{L-1} \binom{L-1}{l} (-1)^l \int_0^\infty e^{-\frac{(l+1)}{\lambda_{k,i,l}} y} dy - \frac{1}{\lambda_{k,i,l}} \sum_{l=0}^{L-1} \binom{L-1}{l} (-1)^l \int_0^\infty e^{-\left(\frac{\gamma_{\text{th}}}{\lambda_{k,i,j}} + \frac{(l+1)}{\lambda_{k,i,l}} \right) y} dy. \end{aligned} \tag{67}$$

Again, when we use the fact from ([32] (eq. 3.310) and some mathematical steps, Φ_{B} can be obtained as

$$\Phi_{\mathsf{B}} = \left[\sum_{l=0}^{L-1} \binom{L-1}{l} \frac{(-1)^l}{l+1} - \sum_{l=0}^{L-1} \binom{L-1}{l} (-1)^l \left(\frac{\bar{\gamma} \lambda_{k,i,j}}{(\gamma_{\text{th}} - 1)\lambda_{k,i,\mathsf{P}} + \bar{\gamma} \lambda_{k,i,j}} \right) \left(\frac{\lambda_{k,i,j}}{\gamma_{\text{th}} \lambda_{k,i,l} + (l+1)\lambda_{k,i,j}} \right) \right]^M. \tag{68}$$

By substituting (68) into (63), the closed-form expression for SOP with the ONS scheme and a non-colluding attack can be obtained as (62). The proof of Theorem 4 is concluded. □

4. Performance Evaluations

In this section, by comparing the simulation and analytical results, we investigate the impact of various network parameters on system secrecy performance. Unless otherwise specified, the simulation parameters are given in Table 3 [28,33]. To evaluate the impact of the proposed scheduling schemes and eavesdropping attacks on secrecy performance, we compare several cases, including a random node selection scheme as the benchmark, which are summarized in Table 4. As can be seen, the random node selection (RNS) scheme, which does not consider channel information to select nodes at each cluster, is utilized as the benchmark scheme.

Table 3. 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 P	$(-5, -5)$
The position of E	$(5, -5)$
The number of hops, K	5
The number of eavesdroppers, L	4
The number of relay nodes in each cluster, M	5
The path-loss exponent, β	2.7
The path loss at the reference distance, $\mathcal{L}$ at $d_0 = 1$	-30 dB
The interference threshold, $\mathcal{I}_{\text{th}}$	$[-30{:}5{:}30]$ dB
The target secrecy data rate, R_{out}	0.1 bps/Hz

Table 4. Schemes for performance comparison.

Cases	Scheme + Eavesdropping Attack
Case I	RNS + colluding attack
Case II	RNS + non-colluding attack
Case III	MNS + colluding attack
Case IV	MNS + non-colluding attack
Case V	ONS + colluding attack
Case VI	ONS + non-colluding attack

Firstly, Figure 2 illustrates the impact of the interference threshold on the secrecy outage probability (SOP). A higher interference threshold allows the secondary user to allocate more transmit power for message transmission. As can be seen in Figure 2, when the interference threshold increases, the secrecy performance decreases. However, at high interference threshold values, SOP converges to a performance floor, indicating that further increases in the interference threshold have little effect on the system performance.

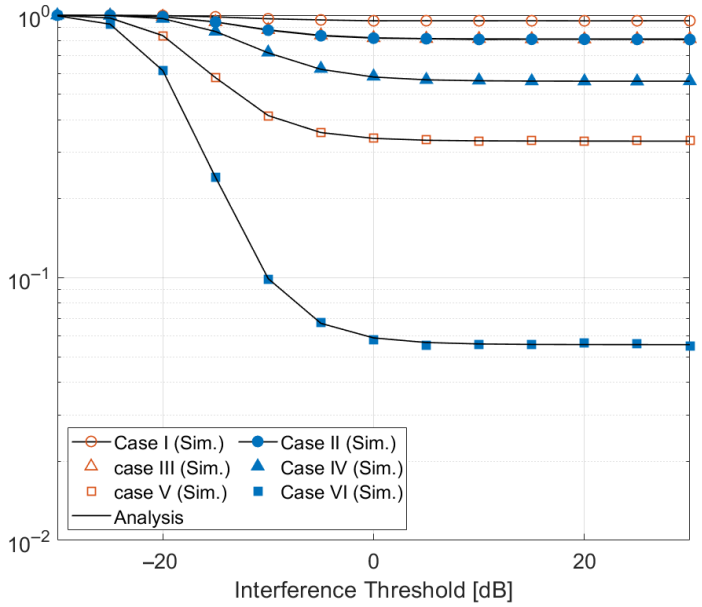

Figure 2. The SOP versus $\mathcal{I}_{\text{th}}$.

Figure 3 shows the impact of the target secrecy data rate on the SOP. The target secrecy data rate represents the required security level of the system. When the system demands a higher security level, it requires more robust protection against eavesdropping attacks. Therefore, as can be seen in Figure 3, since the system requires a higher security level, it becomes more frequently vulnerable to eavesdropping attacks. The results in Figures 2 and 3 show that the statistical approach (simulation results) is in good agreement with the model-based approach (analytical results), thereby validating the correctness of our derivations.

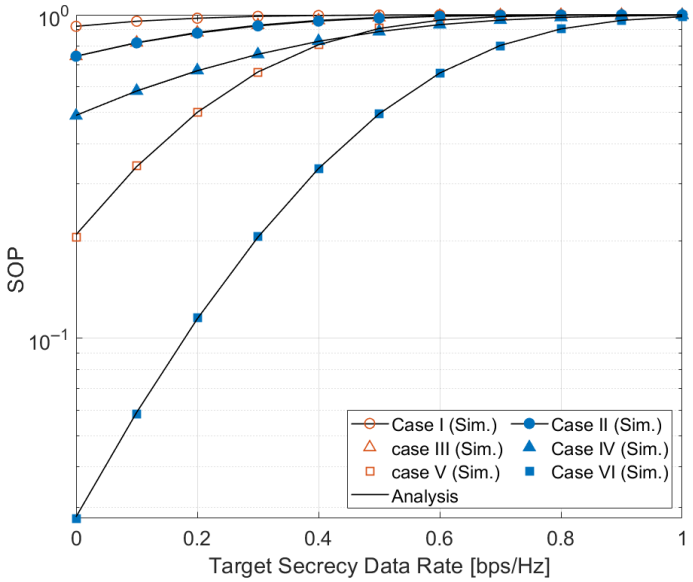

Figure 3. The SOP versus R_{th}.

Next, we turn our attention to the impact of the number of hops, eavesdroppers, and nodes in each cluster on secrecy performance. Figure 4 illustrates the effect of the number of hops on secrecy performance. As can be observed in Figure 4, when the number of hops increases, the secrecy performance improves. This phenomenon can be explained by the fact that increasing the number of hops reduces the distance between adjacent nodes, which enhances channel quality and thereby strengthens secrecy performance.

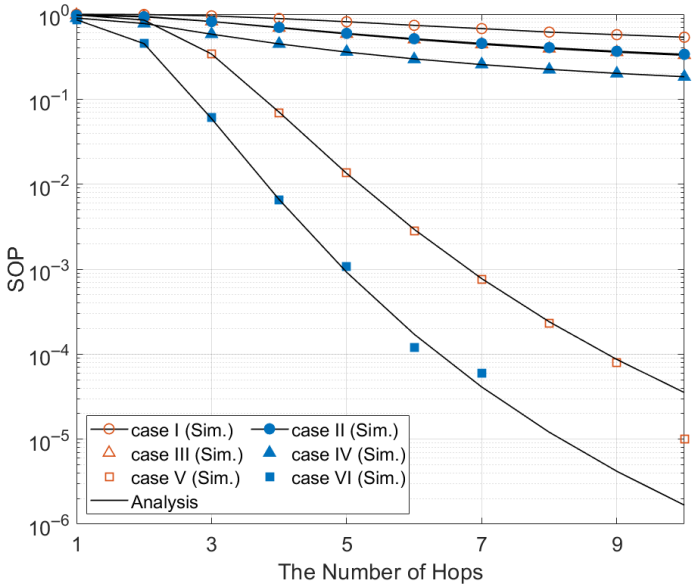

Figure 4. The SOP versus K.

Figure 5 illustrates the impact of the number of eavesdroppers on secrecy performance. As can be seen in Figure 5, when the number of eavesdroppers increases, the adversaries have more opportunities to intercept the legitimate users' transmissions, which leads to degraded secrecy performance.

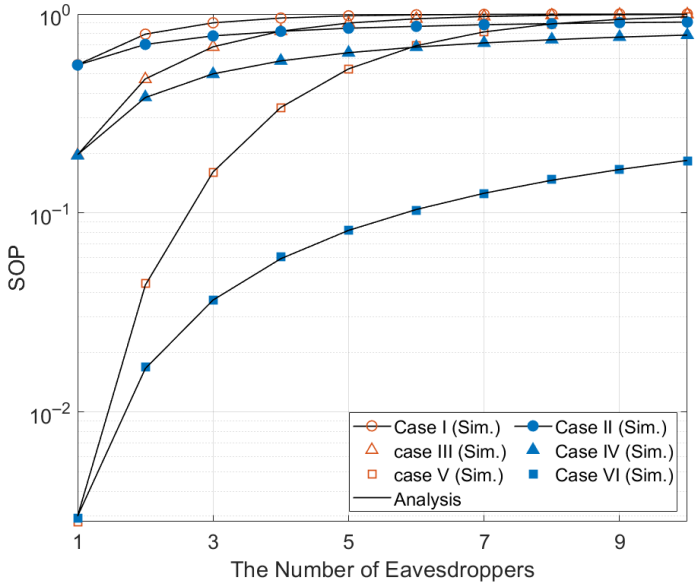

Figure 5. The SOP versus L.

The impact of the number of nodes in each cluster on secrecy performance is shown in Figure 6. As can be seen in Figure 6, when the number of nodes in each cluster increases, the secrecy performance improves. One possible reason is that a larger number of nodes provides more opportunities for each cluster to select better relay nodes, thereby enhancing secrecy performance.

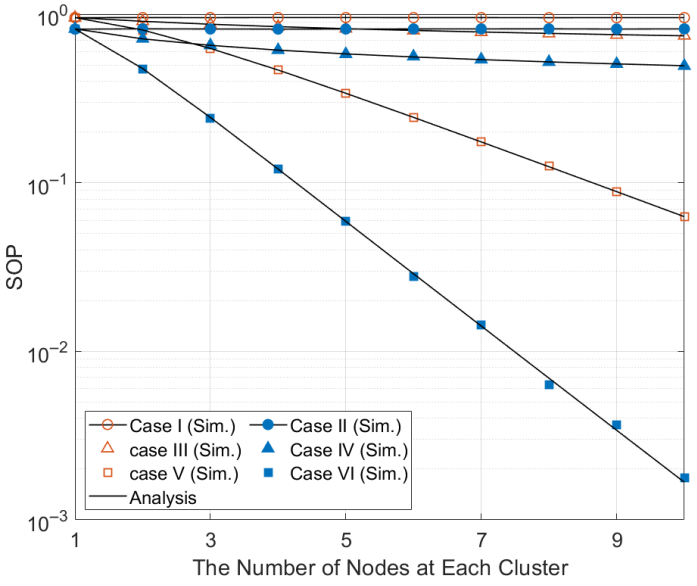

Figure 6. The SOP versus M.

From Figures 2–6, we investigate the impact of network parameters on secrecy performance. In addition, the ONS scheme demonstrates superior secrecy performance compared to the other selection schemes. This can be explained by the fact that the ONS scheme exploits both the main channel and the eavesdropper channel information to select the

node in each cluster, thereby achieving the most robust secrecy performance. Although the MNS scheme is less robust than the ONS scheme, it still enhances secrecy performance since it utilizes the eavesdropper channel information for node selection. Furthermore, since colluding attacks allow multiple eavesdroppers to collaborate and share their intercepted information, they are able to collect more comprehensive information. Therefore, colluding attacks result in more severe degradation of secrecy performance compared to non-colluding attacks.

Now, we analyze the complexity order of each case. In this context, the complexity order is defined as the number of channel information elements required to select a node and transmit a message [35,36]. As shown in Table 5, the ONS scheme requires the largest amount of channel information among the considered scheduling schemes since it exploits both the main channel and the eavesdropper channel information to maximize secrecy capacity. In contrast, the MNS scheme requires only the eavesdropper channel information to select the node in each cluster as it aims to minimize the eavesdropper's channel condition. From these results, we can conclude that opportunistic scheduling schemes requiring more channel information can achieve better secrecy performance. However, as the amount of required channel information increases, the scheduling scheme becomes more complex. Therefore, there exists a trade-off between complexity order and secrecy performance.

Table 5. Complexity order analysis.

	Complexity Order
Case I (RNS + colluding)	$3K$
Case II (RNS + non-colluding)	$3K$
Case III (MNS + colluding)	$K(ML + L + 2)$
Case IV (MNS + non-colluding)	$K(ML + L + 2)$
Case V (ONS + colluding)	$K(ML + 2M + L + 2)$
Case VI (ONS + non-colluding)	$K(ML + 2M + L + 2)$

In this paper, we evaluate secrecy performance from various perspectives. Based on this analysis, we investigate the impact of network parameters on secrecy performance and demonstrate that opportunistic scheduling can significantly enhance secrecy performance, albeit at the cost of increased computational complexity.

5. Conclusions

In this paper, to protect confidential messages against various eavesdropping attacks, we proposed opportunistic scheduling schemes to enhance secrecy performance for multi-hop transmission in underlay cognitive radio networks. The proposed MNS scheme does not need the eavesdropper's channel information to minimize the eavesdropper's channel gain, while providing a low complexity order. Different from the MNS scheme, the proposed ONS scheme not only requires both the main channel and the eavesdropper's channel to optimize the secrecy capacity but also shows a high complexity order. To capture the impact of network parameters, we derived closed-form expressions for the secrecy outage probability (SOP) under the proposed scheduling schemes and eavesdropping scenarios. Performance evaluations showed that the ONS scheme provides the most robust secrecy performance by leveraging both main and eavesdropper channel information, while the

MNS scheme also improves secrecy performance with lower computational complexity. Moreover, the results revealed that colluding attacks cause more severe degradation of secrecy performance than non-colluding attacks. Overall, our analysis emphasizes the fundamental trade-off between secrecy performance and computational complexity, offering valuable insights for the design of secure and efficient multi-hop cognitive radio networks. In addition, the proposed ONS scheme improves secrecy performance by 15% under a 20 dB interference threshold compared to the MNS scheme. We leave the investigation of the interaction between the PHY layer and the MAC layer on the system performance and node mobility on the system performance as a future research topic.

Author Contributions: Conceptualization, K.S. and B.A.; Validation, K.S. and B.A.; Formal analysis, K.S.; Writing—original draft, K.S.; Writing—review & editing, K.S. and B.A.; Supervision, B.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a research grant from Hankyong National University in the year of 2023.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

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

References

1. Pinto, R.P.; Silva, B.M.; Inácio, P.R. Federated learning for anomaly detection on Internet of Medical Things: A survey. *Internet Things* **2025**, *33*, 101677. [CrossRef]
2. Afrin, S.; Rafa, S.J.; Kabir, M.; Farah, T.; Alam, M.S.B.; Lameesa, A.; Ahmed, S.F.; Gandomi, A.H. Industrial Internet of Things: Implementations, challenges, and potential solutions across various industries. *Comput. Ind.* **2025**, *170*, 104317. [CrossRef]
3. Giral-Ramírez, D.A.; Hernández-Suarez, C.A.; García-Ubaque, C.A. Spectral decision analysis and evaluation in an experimental environment for cognitive wireless networks. *Results Eng.* **2021**, *12*, 100309. [CrossRef]
4. Le-Thanh, T.; Tran-Minh, C.; Ho-Van, K. Secrecy analysis of IRS-assisted NOMA cognitive radio networks with full-duplex energy scavenging jammer. *Phys. Commun.* **2025**, *72*, 102784. [CrossRef]
5. Narmadha, G.; Jeyalakshmi, M.; Ponnrajakumari, M.; Duraichi, N.; Sakthivel, B. Enhancing spectrum prediction in cognitive radio networks using an optimized generative adversarial network. *Results Eng.* **2025**, *26*, 105270. [CrossRef]
6. Goldsmith, A.; Jafar, S.A.; Maric, I.; Srinivasa, S. Breaking Spectrum Gridlock With Cognitive Radios: An Information Theoretic Perspective. *Proc. IEEE* **2009**, *97*, 894–914. [CrossRef]
7. Tu, N.H.; Hoang, T.D.; Lee, K. Short-Packet URLLCs for MIMO Underlay Cognitive Multihop Relaying with Imperfect CSI. *IEEE Access* **2023**, *11*, 81672–81689. [CrossRef]
8. Abilasha, V.; Karthikeyan, A. Metaheuristic-Based Cepstral Sensing Technique for Prolonging Network Lifetime and Mitigating Primary User Emulation Attacks in Cognitive Radio Sensor Network. *IEEE Access* **2025**, *13*, 100370–100391. [CrossRef]
9. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 19–26. [CrossRef]
10. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
11. Chorti, A.; Barreto, A.N.; Köpsell, S.; Zoli, M.; Chafii, M.; Sehier, P.; Fettweis, G.; Poor, H.V. Context-Aware Security for 6G Wireless: The Role of Physical Layer Security. *IEEE Commun. Stand. Mag.* **2022**, *6*, 102–108. [CrossRef]
12. Ajib, W.; Haccoun, D. An overview of scheduling algorithms in MIMO-based fourth-generation wireless systems. *IEEE Netw.* **2005**, *19*, 43–48. [CrossRef]
13. Zhang, Q.; Chen, Q.; Yang, F.; Shen, X.; Niu, Z. Cooperative and opportunistic transmission for wireless ad hoc networks. *IEEE Netw.* **2007**, *21*, 14–20. [CrossRef]
14. Asadi, A.; Mancuso, V. A Survey on Opportunistic Scheduling in Wireless Communications. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1671–1688. [CrossRef]
15. Abedi, M.R.; Mokari, N.; Saeedi, H.; Yanikomeroglu, H. Robust Resource Allocation to Enhance Physical Layer Security in Systems with Full-Duplex Receivers: Active Adversary. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 885–899. [CrossRef]
16. Shim, K.; An, B. Exploiting Secure Multihop Transmission in Underlying Cognitive Radio Networks: Analysis and Deep Learning Approaches. In Proceedings of the 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Bali, Indonesia, 20–23 February 2023; pp. 281–285. [CrossRef]

17. Shim, K.; An, B. Exploiting Impact of Eavesdropping Attacks on Secrecy Performance in WPT-based Secure Multi-hop Transmission. In Proceedings of the 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 4–7 July 2023; pp. 392–397. [CrossRef]
18. Li, X.; Zhao, H.; Xu, J.; Zhu, G.; Deng, W. APDPFL: Anti-Poisoning Attack Decentralized Privacy Enhanced Federated Learning Scheme for Flight Operation Data Sharing. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 19098–19109. [CrossRef]
19. Guo, D.; Zhang, S.; Zhang, J.; Yang, B.; Lin, Y. Exploring Contextual Knowledge-Enhanced Speech Recognition in Air Traffic Control Communication: A Comparative Study. *IEEE Trans. Neural Netw. Learn. Syst.* **2025**, *36*, 16085–16099. [CrossRef]
20. Shim, K.; Nguyen, T.V.; An, B. Exploiting Opportunistic Scheduling Schemes to Improve Physical-Layer Security in MU-MISO NOMA Systems. *IEEE Access* **2019**, *7*, 180867–180886. [CrossRef]
21. Huang, S.; Huang, X.; Chen, W.; Zhao, S. Physical layer security of vehicular networks with cooperative jamming helpers. *Phys. Commun.* **2022**, *53*, 101762. [CrossRef]
22. Odong, P.; Abd El-Malek, A.H.; Allam, A.; Abdel-Rahman, A.B. Physical layer security in SWIPT-based cooperative vehicular relaying networks. *Veh. Commun.* **2024**, *49*, 100835. [CrossRef]
23. Namdar, M.; Basgumus, A.; Ata, S.O.; Aldirmaz-Colak, S. Physical layer security in RIS-aided communication systems: Secrecy performance analyses. *Digit. Signal Process.* **2025**, *167*, 105417. [CrossRef]
24. Shim, K.; Do, N.T.; An, B.; Nam, S.Y. 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), Danang, Vietnam, 27–30 January 2016; pp. 1–4. [CrossRef]
25. Garcia, C.E.; Camana, M.R.; Koo, I. Secrecy Energy Efficiency Maximization in an Underlying Cognitive Radio–NOMA System with a Cooperative Relay and an Energy-Harvesting User. *Appl. Sci.* **2020**, *10*, 3630. [CrossRef]
26. Shang, Z.; Zhang, T.; Cai, Y.; Yang, W.; Wu, H.; Zhang, Y.; Tao, L. Secure Transmission in Cognitive Wiretap Networks with Full-Duplex Receivers. *Appl. Sci.* **2020**, *10*, 1840. [CrossRef]
27. Wang, X.; Wang, X.; Ge, J.; Liu, Z.; Ma, Y.; Li, X. Reconfigurable Intelligent Surface-Assisted Secure Communication in Cognitive Radio Systems. *Energies* **2024**, *17*, 515. [CrossRef]
28. 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]
29. Pramitarini, Y.; Perdana, R.H.Y.; Shim, K.; An, B. Opportunistic Scheduling Scheme to Improve Physical-Layer Security in Cooperative NOMA System: Performance Analysis and Deep Learning Design. *IEEE Access* **2024**, *12*, 58454–58472. [CrossRef]
30. Shim, K.; Park, S.H.; Kim, B.S.; An, B. Exploiting Opportunistic Scheduling Schemes on Cooperative NOMA Networks Under Active Eavesdropper. *IEEE Access* **2025**, *13*, 111484–111507. [CrossRef]
31. Alberto, L.G. *Probability, Statistics, and Random Processes for Electrical Engineering*, 3rd ed.; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2008; Volume 55.
32. Gradshteyn, I.; Ryzhik, I. *Table of Integrals, Series, and Products*, 7th ed.; Academic Press: Cambridge, MA, USA, 2007.
33. 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. [CrossRef]
34. Aigner, M. *Combinatorial Theory*; Springer: New York, NY, USA, 1979.
35. 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]
36. 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]