Exploiting Secure Multi-Hop Transmissions with NOMA Networks: Performance Analysis

Yushintia Pramitarini*, Ridho Hendra Yoga Perdana* Kyusung Shim†, and Beongku An‡
*Dept. of Software and Communications Engineering in Graduate School, Hongik University, Republic of Korea
†School of Computer Engineering and Applied Mathematics, Hankyong National University, Republic of Korea
‡Dept. of Software and Communications Engineering, Hongik University, Republic of Korea
Emails: yushintia@mail.hongik.ac.kr, hendra@mail.hongik.ac.kr, kyusung.shim@hknu.ac.kr, beongku@hongik.ac.kr

***Abstract*—In this paper, we analyze the secrecy performance of secure multi-hop transmission for the NOMA system. More specifically, the multi-hop transmission can extend the coverage of wireless transmission. However, according to the principle of the wireless medium, an eavesdropper can overhear the legitimate users' transmission, which leads to serious security issues. In order to analyze the relationship between network parameters and secrecy outage probability, we derive exact closed-form expressions for the secrecy outage probability (SOP) of cell center and cell edge users, respectively. The numerical results show that the simulation and analysis results are tightly matched. Additionally, we investigate the impact of the number of hops and the distance on the secrecy performance.**

***Index Terms*—Non-orthogonal multiple access (NOMA), closed-form expression, multi-hop transmission, performance analysis, physical layer security**

I. Introduction

Recently, non-orthogonal multiple access (NOMA) is considered as an essential technology for evolving mobile networks beyond 5G [1]. Specifically, NOMA uses superimposed coding techniques to transmit simultaneously multiple users' information [2]. Additionally, NOMA system can improve spectral efficiency and massive connectivity [3]. However, when an eavesdropper intercepts a signal, the eavesdropper can wiretap multiple users' messages. Thus, in the viewpoint of security, it is very serious problem. Physical layer security (PLS) is considered as one of the efficient solutions to protect messages against intercept attacks. The main advantage of PLS is can protect messages by relying on the characteristics of the wireless medium. As a result, PLS does not require additional processes such as encryption and decryption processes to protect messages against malicious users [4]. However, the authors in [4] did not consider the multi-hop transmissions issue.

To extend the transmission coverage, the cooperative transmission is considered as one of the possible solutions that other nodes can help data transmission between a source node and destination node [2], [5], [6]. The authors in [7] investigated the multi-hop cognitive wireless-powered D2D communication in wireless sensor networks. In [7], the authors did not consider the security issue.

Indeed, authors in [8] studied the PLS for cooperative NOMA system. Authors in [6] addressed the multi-hop transmission in cognitive radio networks. However, the authors did not consider the multi-hop transmission. Besides, the impact of imperfect channel state information on the performance of multi-hop NOMA networks has been studied in [9]. Meanwhile, in [10] authors explored multi-hop transmission under various eavesdropping attacks for wireless sensor networks (WSNs). However, the authors did not consider multi-hop in cooperative NOMA.

The above mentioned works motivate us to study the impact of the secrecy performance in multi-hop transmission with NOMA system. In this paper, we study the secrecy performance on secure multi-hop transmission in cooperative NOMA, where the passive eavesdropper can overhear each hop transmission. The main contributions of this paper can be summarized as follows:

- We exploit the secrecy performance on secure multi-hop transmission in NOMA networks. In detail, an eavesdropper can overhear the confidential message at each hop.
- We derive the closed-form expression for the secrecy outage performance (SOP) of the cell-center and cell-edge users, respectively. Based on the closed-form expression for SOP, we can capture the relationship between secrecy performance and network parameters.
- The numerical results show that the effect of the number of hops and the distance between source to cell-center and cell-edge users on the secrecy performance is also evaluated.

The rest of this paper is organized as follows: Section II introduces the system model, channel description, and data transmission process. Section III derives the exact closed-form expression for SOP. Section IV presents the numerical results from the derived analysis and simulations. Finally, Section V concludes the paper.

Notation: The probability density function (PDF) and cumulative distribution function (CDF) of the random variable X are denoted $f_X(\cdot)$ and $F_X(\cdot)$, respectively. $\mathcal{CN}(0,1)$ represents a complex Gaussian distribution with zero mean and one variance.

II. System Model

A. System and Channel Description

We consider a secure multihop transmission in NOMA consisting of a source node denoted by S transmitting messages to

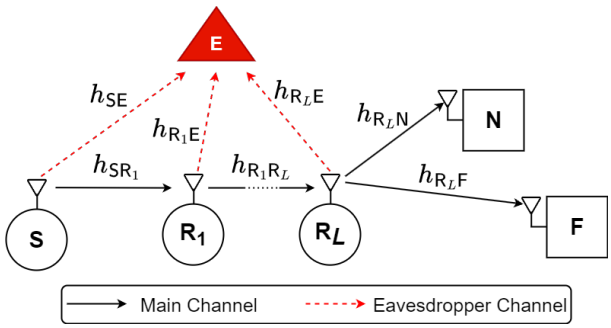

Fig. 1. Illustration of the proposed secure multi-hop transmissions in cooperative NOMA network.

cell-center User N and cell-edge User F aided by L relay nodes denoted by R_L, $l \in \{1, \cdots, L\}$ as illustrated in Fig. 1. Due to limited radio ranges, obstacles, or deep shadowing effects, we assume that the direct connection between S to N and S to F can not establish. Thus, R_L nodes help data transmission from the S to N and F users, respectively. Meanwhile, an eavesdropper denoted by E equipped with a single antenna can overhear the confidential message at each hop. Besides, we suppose that each node is operated in half-duplex mode to transmit and receive signals since each node is equipped with a single antenna.

Let us consider a channel coefficient from $\mathsf{X} \rightarrow \mathsf{Y}$ where $\mathsf{X} \in \{\mathsf{S}, \mathsf{R}_l, \cdots \mathsf{R}_L\}$, and $\mathsf{Y} \in \{\mathsf{R}_l, \cdots, \mathsf{R}_L, \mathsf{N}, \mathsf{F}, \mathsf{E}\}$. The channel coefficient consists of two parts small-scale fading and large-scale path loss effects. Let $\tilde{h}_{\mathsf{XY}}$ and $|\tilde{h}_{\mathsf{XY}}|^2$ denote the small-scale fading by following the Rayleigh distribution and the corresponding channel gain, respectively. Furthermore, the large-scale path loss effect can be expressed as $\lambda_{\mathsf{XY}} = (d_{\mathsf{XY}}/d_0)^{-\epsilon}$, where d_{XY} presents the Euclidean distance between X and Y, d_0 and ϵ denote the reference distance and path-loss exponent, respectively [11]. Consequently, the channel coefficient considers $h_{\mathsf{XY}} \triangleq \tilde{h}_{\mathsf{XY}}\lambda_{\mathsf{XY}}$ the small-scale fading and large-scale path loss effect, respectively.

B. Data Transmission Process

1) Relay transmission phases: In the relay transmission process, S transmits the superposed signal that is represented as $\sqrt{\theta_{\mathsf{N}}}\zeta_{\mathsf{N}} + \sqrt{\theta_{\mathsf{F}}}\zeta_{\mathsf{F}}$ via multiple intermediate relay. Here, ζ_{N} and ζ_{F} are the signals for User N and User F, respectively. According to NOMA principles, the terms θ_{N} and θ_{F} are power allocation coefficient for User N and User F with $\theta_{\mathsf{N}} \geq \theta_{\mathsf{F}}$ with $\theta_{\mathsf{N}} + \theta_{\mathsf{F}} = 1$, respectively. As can be seen in Fig. 1, we assume S as R_0, then every l-th hop transmission slot indicates that the transmission from $\mathsf{R}_{(l-1)}$ to R_l. The received signal at R_{l+1} can be expressed as

$$y_{\mathsf{R}_l} = \sqrt{P_{\mathsf{R}_l}}(\sqrt{\theta_{\mathsf{N}}}\zeta_{\mathsf{N}} + \sqrt{\theta_{\mathsf{F}}}\zeta_{\mathsf{F}})\mathsf{h}_{\mathsf{R}_l} + n_{\mathsf{R}_l}, \tag{1}$$

where $\mathsf{h}_{\mathsf{R}_l}$ denotes the channel coefficient of $\mathsf{h}_{\mathsf{R}_l} \rightarrow \mathsf{h}_{\mathsf{R}_{l+1}}$ link, P_{R_l} denotes the transmit power at R_l node and n_{R_l} is channel noise at R_{l+1} which is represented as an additive white Gaussian noise (AWGN) model followed as $\mathcal{CN}(0,1)$. In order to distinguish the cell-center and cell-edge user message from the received message, by performing the successive interference cancellation (SIC) process, each relay in every hop R_l can decode the cell-edge user's message from the received signal. The signal-to-interference-plus-noise ratio (SINR) to decode the F message at l hop relay can be expressed as

$$\gamma_{\mathsf{R}_l}^{\zeta_{\mathsf{F}}} = \frac{P_{\mathsf{R}_l}\theta_{\mathsf{F}}|h_{\mathsf{R}_l}|^2}{P_{\mathsf{R}_l}\theta_{\mathsf{N}}|h_{\mathsf{R}_l}|^2 + \sigma_{\mathsf{R}_l}^2}, \tag{2}$$

then, R_l can decode the N's message from the received signal, the signal-to-noise ration (SNR) to decode the N's message at R_l can be expressed as

$$\gamma_{\mathsf{R}_l}^{\zeta_{\mathsf{N}}} = \frac{P_{\mathsf{R}_l}\theta_{\mathsf{N}}|h_{\mathsf{R}_l}|^2}{\sigma_{\mathsf{R}_l}^2}. \tag{3}$$

2) Destination transmission phases: In the destination transmission phases, the received signal at User N and F from the last relay R_L can be expressed, respectively, as

$$y_{\mathsf{N}} = \sqrt{P_{\mathsf{R}_L}}(\sqrt{\theta_{\mathsf{N}}}\zeta_{\mathsf{N}} + \sqrt{\theta_{\mathsf{F}}}\zeta_{\mathsf{F}})\mathsf{h}_{\mathsf{R}_L\mathsf{N}} + n_{\mathsf{N}}, \tag{4}$$

$$y_{\mathsf{F}} = \sqrt{P_{\mathsf{R}_L}}(\sqrt{\theta_{\mathsf{N}}}\zeta_{\mathsf{N}} + \sqrt{\theta_{\mathsf{F}}}\zeta_{\mathsf{F}})\mathsf{h}_{\mathsf{R}_L\mathsf{F}} + n_{\mathsf{F}}, \tag{5}$$

where $\mathsf{h}_{\mathsf{R}_L\mathsf{N}}$ and $\mathsf{h}_{\mathsf{R}_L\mathsf{F}}$ denote the channel coefficient from R_L to User N and F, respectively, P_{R_L} denotes the transmit power at R_L and the channel noise at User N and F is represented by n_{N} and n_{F}, respectively, those are modeled with $\mathcal{CN}(0,1)$. Similar to relay, the SINR at User N to remove User F's message by performing the SIC process can be expressed as

$$\gamma_{\mathsf{N}}^{\zeta_{\mathsf{F}}} = \frac{P_{\mathsf{R}_L}\theta_{\mathsf{F}}|h_{\mathsf{R}_L\mathsf{N}}|^2}{P_{\mathsf{R}_L}\theta_{\mathsf{N}}|h_{\mathsf{R}_L\mathsf{N}}|^2 + \sigma_{\mathsf{N}}^2}, \tag{6}$$

then, the SNR for decoding the User N's message, ζ_{N}, at the user Ncan be expressed as

$$\gamma_{\mathsf{N}}^{\zeta_{\mathsf{N}}} = \frac{P_{\mathsf{R}_L}\theta_{\mathsf{N}}|h_{\mathsf{R}_L\mathsf{N}}|^2}{\sigma_{\mathsf{N}}^2}. \tag{7}$$

Different from User N, User F can directly decode its message from the received signal because its power allocation coefficients are larger than that of User N. The SINR to decode User F's message at User F can be expressed as

$$\gamma_{\mathsf{F}}^{\zeta_{\mathsf{F}}} = \frac{P_{\mathsf{R}_L}\theta_{\mathsf{F}}|h_{\mathsf{R}_L\mathsf{F}}|^2}{P_{\mathsf{R}_L}\theta_{\mathsf{N}}|h_{\mathsf{R}_L\mathsf{F}}|^2 + \sigma_{\mathsf{F}}^2}. \tag{8}$$

3) Eavesdropper transmission phases: The E can overhear a legitimate user's transmission from each transmission process. Thus, the wiretapped signal at E in every l hop transmission can be expressed as

$$y_{\mathsf{R}_l\mathsf{E}} = \sqrt{P_{\mathsf{R}_l}}(\sqrt{\theta_{\mathsf{N}}}\zeta_{\mathsf{N}} + \sqrt{\theta_{\mathsf{F}}}\zeta_{\mathsf{F}})\mathsf{h}_{\mathsf{R}_l\mathsf{E}} + n_{\mathsf{E}}, \tag{9}$$

where $\mathsf{h}_{\mathsf{R}_l,\mathsf{E}}$ denotes channel coefficient of l-th hop to E and n_{E} denotes as channel noise at E which is modeled with $\mathcal{CN}(0,1)$. In this paper, we assume that the eavesdropper has a strong signal encoding process. The eavesdropper perfectly distinguishes each user's message from the received signal. The received SNR of l-th hop at E to wiretap the message of User N and F can be expressed, respectively, as

$$\gamma_{\mathsf{R}_l\mathsf{E}}^{\zeta_{\mathsf{N}}} = \frac{P_{\mathsf{R}_l}\theta_{\mathsf{N}}|h_{\mathsf{R}_l\mathsf{E}}|^2}{\sigma_{\mathsf{E}}^2}, \tag{10}$$

$$\gamma_{\mathsf{R}_l\mathsf{E}}^{\zeta_\mathsf{F}} = \frac{P_{\mathsf{R}_l}\theta_\mathsf{F}|h_{\mathsf{R}_l\mathsf{E}}|^2}{\sigma_\mathsf{E}^2}. \tag{11}$$

III. Secrecy Outage Performance Analysis

In this section, we derive the closed-form expression for secrecy outage probability (SOP) of User N and User F. The SOP is defined as the probability that the secrecy rate is below the target secrecy data rate, which can be mathematically expressed as [6]

$$\mathrm{P}_{\mathtt{SOP}}^{\mathsf{N}} = \Pr\left[\frac{1}{L+1}\min_{1\le l\le L+1}\left\{\log_2\left(\frac{1+\gamma_\mathsf{N}^{\zeta_\mathsf{N}}}{1+\gamma_\mathsf{E}^{\zeta_\mathsf{N}}}\right)\right\} < \bar{\mathsf{R}}\right], \tag{12}$$

where $\bar{\mathsf{R}}$ denotes the secrecy target data rate. For convenience, we define the channel gains as $X_{l\mathsf{N}} \triangleq |h_{\mathsf{R}_l,\mathsf{N}}|^2$, $Z_{l\mathsf{E}} \triangleq |h_{\mathsf{R}_l,\mathsf{E}}|^2$. We can further suppose $\hat{\gamma} = P_{\mathsf{R}_l}/\sigma^2$, $a_\mathsf{n} = \hat{\gamma}\theta_\mathsf{N}$, and $\bar{\gamma} = 2^{(L+1)\bar{\mathsf{R}}}$. The $\mathrm{P}_{\mathtt{SOP}}^{\mathsf{N}}$ can be re-expressed as

$$\begin{aligned}\mathrm{P}_{\mathtt{SOP}}^{\mathsf{N}} &= 1 - \prod_{l=1}^{L+1}\left[1 - \Pr\left(\frac{1+a_\mathsf{n}X_{l,\mathsf{N}}}{1+a_\mathsf{n}Z_{l\mathsf{E}}} < \bar{\gamma}\right)\right] \\ &= 1 - \prod_{l=1}^{L+1}\left[1 - \underbrace{\int_0^\infty F_X\left(\frac{\bar{\gamma}-1}{a_\mathsf{n}} + \bar{\gamma}z\right) f_z(z)dz}_{\Phi}\right].\end{aligned} \tag{13}$$

Φ in (13) can be re-expressed as

$$\begin{aligned}\Phi &= \int_0^\infty \left[1 - e^{-\frac{1}{\lambda_{X_{l\mathsf{N}}}}\left(\frac{\bar{\gamma}-1}{a_\mathsf{n}} + \bar{\gamma}z\right)}\right]\frac{1}{\lambda_{X_{l\mathsf{N}}}}e^{-\frac{1}{\lambda_{Z_{l\mathsf{E}}}}z}dz \\ &= \underbrace{\int_0^\infty \frac{1}{\lambda_Z}e^{-\frac{1}{\lambda_{Z_{l\mathsf{E}}}}z}d_z}_{\Phi_1} - e^{-\frac{\bar{\gamma}-1}{\lambda_{X_{l\mathsf{N}}}a_\mathsf{N}}} \\ &\quad \times \underbrace{\int_0^\infty \frac{1}{\lambda_{Z_{l\mathsf{E}}}}e^{-\frac{\bar{\gamma}z}{\lambda_{X_{l\mathsf{N}}}} - \frac{1}{\lambda_{Z_{l\mathsf{E}}}}z}dz}_{\Phi_2}\end{aligned} \tag{14}$$

Relying on the fact [12, eq. 3.310], Φ_1 and Φ_2 in (14) can be respectively, re-written as

$$\Phi_1 = \int_0^\infty \frac{1}{\lambda_{Z_{l\mathsf{E}}}}e^{-\frac{1}{\lambda_{Z_{l\mathsf{E}}}}z}dz = 1 \tag{15}$$

$$\Phi_2 = \int_0^\infty \frac{1}{\lambda_{Z_{l\mathsf{E}}}}e^{-\frac{\bar{\gamma}z}{\lambda_{X_{l\mathsf{N}}}} - \frac{1}{\lambda_{Z_{l\mathsf{E}}}}z}dz = \frac{\lambda_{X_{l\mathsf{N}}}}{\bar{\gamma}\lambda_{Z_{l\mathsf{E}}} + \lambda_{X_{l\mathsf{N}}}} \tag{16}$$

By plugging Φ_1 and Φ_2 into (14), Φ can be further written as

$$\Phi = 1 - \frac{\lambda_{X_{l\mathsf{N}}}}{\bar{\gamma}\lambda_{Z_{l\mathsf{E}}} + \lambda_{X_{l\mathsf{N}}}}e^{-\frac{\bar{\gamma}-1}{\lambda_{X_{l\mathsf{N}}}a_\mathsf{N}}} \tag{17}$$

and $\mathrm{P}_{\mathtt{SOP}}^{\mathsf{N}}$ can be further written as

$$\mathrm{P}_{\mathtt{SOP}}^{\mathsf{N}} = 1 - \prod_{l=1}^{L+1}\left[\frac{\lambda_{X_{l\mathsf{N}}}}{\bar{\gamma}\lambda_{Z_{l\mathsf{E}}} + \lambda_{X_{l\mathsf{N}}}}e^{-\frac{\bar{\gamma}-1}{\lambda_{X_{l\mathsf{N}}}a_\mathsf{N}}}\right] \tag{18}$$

At User F, the SOP can be mathematically expressed as

$$\mathrm{P}_{\mathtt{SOP}}^{\mathsf{F}} = \Pr\left[\frac{1}{L+1}\min_{1\le l\le L+1}\left\{\log_2\left(\frac{1+\gamma_\mathsf{F}^{\zeta_\mathsf{F}}}{1+\gamma_\mathsf{E}^{\zeta_\mathsf{F}}}\right)\right\} < \bar{\mathsf{R}}\right]. \tag{19}$$

For convenience, let define the channel gain as $Y_{l\mathsf{F}} \triangleq |h_{\mathsf{R}_l\mathsf{F}}|^2$. Assuming $a_\mathsf{f} = \hat{\gamma}\theta_\mathsf{F}$, (19) can then be further re-written as:

$$\begin{aligned}&\mathrm{P}_{\mathtt{SOP}}^{\mathsf{F}} \\ &= 1 - \prod_{l=1}^{L+1}\left[1 - \Pr\left(\frac{1+\frac{a_\mathsf{f}Y_{l,\mathsf{F}}}{a_\mathsf{n}Y_{l\mathsf{F}}+1}}{1+a_\mathsf{f}Z_{l\mathsf{E}}}\right) < \bar{\gamma}\right] \\ &= 1 - \prod_{l=1}^{L+1}\left[1 - \int_0^\infty F_Y\left(Y_{l,\mathsf{F}} < \frac{(\bar{\gamma}-1) + \bar{\gamma}a_\mathsf{f}Z_{l\mathsf{E}}}{a_\mathsf{f} - a_\mathsf{n}((\bar{\gamma}-1) + \bar{\gamma}a_\mathsf{f}Z_{l\mathsf{E}})}\right)\right. \\ &\quad \left.\times f_z(z)dz\right]\end{aligned} \tag{20}$$

Given that the random variable $Y_{l,\mathsf{F}}$ is always non-negative, the expression on the right-side of (20) is consistently larger than zero, denoted as $\theta_\mathsf{F} - \theta_\mathsf{N}((\bar{\gamma}-1) + \bar{\gamma}a_\mathsf{f}Z_{l\mathsf{E}}) > 0$. Therefore, when $\frac{1-\theta_\mathsf{N}\bar{\gamma}}{\theta_\mathsf{N}\theta_\mathsf{F}\bar{\gamma}} > z$, the value on the right-side remains positive. Thus, (20) can be re-expressed as (21) top of the next page. By using the Gaussian-Chebyshev quadrature [13, eq. 25.4.38], the SOP of user F can be expressed as (22) top of the next page. We will explain how to approximate the (22) using the Gaussian-Chebyshev quadrature in the following lemma.

Lemma 1. *Suppose the integral of a function $g(x)$ does not recognize closed-form expression at $[a,b]$. The integral $\int_a^b g(x)dx$ can be approximated by:*

$$\begin{aligned}&\int_a^b g(x)dx \\ &= \frac{b-a}{2}\sum_{i=1}^{N} w_i\sqrt{1-x_i^2}\,g\left(\frac{b-a}{2}x_i + \frac{b+a}{2}\right),\end{aligned} \tag{23}$$

where N present the number of term, $w_i = \frac{\pi}{N}$, $x_i = cos((2i-1)\frac{\pi}{N})$.

Proof. With the Gaussian-Chebyshev quadrature, an integral over $[a,b]$ can be transformed into an integral over $[-1,1]$. The change of interval can be expressed as

$$\int_a^b g(x)dx = \frac{b-a}{2}\underbrace{\int_{-1}^{1} g\left(\frac{b-a}{2}x + \frac{b+a}{2}\right)dx}_{\Xi}. \tag{24}$$

To utilize the Gaussian-Chebyshev, (24) can be re-written as

$$\begin{aligned}\Xi &= \int_{-1}^{1}\underbrace{\int_{-1}^{1} g\left(\frac{b-a}{2}x + \frac{b+a}{2}\right)\sqrt{1-x^2}}_{p_{(x)}}\frac{1}{\sqrt{1-x^2}}dx \\ &= \int_{-1}^{1} p_{(x)}\frac{1}{\sqrt{1-x^2}}dx.\end{aligned} \tag{25}$$

By applying [13, eq. 25.4.38],then plugging (25) into (24), $\int_a^b g(x)dx$ can be further defined as:

$$\begin{aligned}&\int_a^b g(x)dx \\ &= \frac{b-a}{2}\sum_{i=1}^{N} w_i\sqrt{1-x_i^2}\,g\left(\frac{b-a}{2}x_i + \frac{b+a}{2}\right).\end{aligned} \tag{26}$$

$$\mathrm{P}_{\mathsf{SOP}}^{\mathsf{F}} = 1 - \prod_{l=1}^{L+1}\left[1 - \int_0^{\frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{\theta_{\mathsf{N}}\bar{\gamma}a_{\mathsf{f}}}} F_Y\left(Y_{l,\mathsf{F}} < \frac{(\bar{\gamma}-1)+\bar{\gamma}a_{\mathsf{f}}z}{a_{\mathsf{f}} - a_{\mathsf{n}}((\bar{\gamma}-1)+\bar{\gamma}a_{\mathsf{f}}z)}\right) f_Z(z)dz + \int_{\frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{\theta_{\mathsf{N}}\bar{\gamma}a_{\mathsf{f}}}}^{\infty} f_Z(z)dz\right]$$
$$= 1 - \prod_{l=1}^{L+1}\left[1 - \int_0^{\frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{\theta_{\mathsf{N}}\bar{\gamma}a_{\mathsf{f}}}} f_z(z)dz + \int_{\frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{\theta_{\mathsf{N}}\theta_{\mathsf{F}}\bar{\gamma}}}^{\infty} f_Z(z)dz - \int_0^{\frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{\theta_{\mathsf{N}}\bar{\gamma}a_{\mathsf{f}}}} e^{-\frac{1}{\lambda_{Y_{l\mathsf{F}}}}\frac{(\bar{\gamma}-1)+\bar{\gamma}a_{\mathsf{f}}z}{a_{\mathsf{f}}-a_{\mathsf{n}}((\bar{\gamma}-1)+\bar{\gamma}a_{\mathsf{f}}z)}} f_Z(z)dz\right] \tag{21}$$

$$\mathrm{P}_{\mathsf{SOP}}^{\mathsf{F}} = 1 - \prod_{l=1}^{L+1}\left[\int_0^{\frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{\theta_{\mathsf{N}}\bar{\gamma}a_{\mathsf{f}}}} e^{-\frac{1}{\lambda_{Y_{l,\mathsf{F}}}}\frac{(\bar{\gamma}-1)+\bar{\gamma}a_{\mathsf{f}}Z}{a_{\mathsf{f}}-a_{\mathsf{n}}((\bar{\gamma}-1)+\bar{\gamma}a_{\mathsf{f}}Z)}} f_Z(z)dz\right]$$
$$= 1 - \prod_{l=1}^{L+1}\left[\frac{1}{\lambda_{Z_{l,\mathsf{E}}}}\sum_{i=1}^{N}\xi\omega_i\sqrt{1-\chi_i^2}e^{-\frac{\delta+\beta\xi\chi_i+\xi}{\lambda_{Y_{l,\mathsf{F}}}(a_{\mathsf{f}}-a_{\mathsf{n}}(\delta+\beta\xi\chi_i+\xi))} - \frac{1}{\lambda_{Z_{l\mathsf{E}}}}(\xi\chi_i+\xi)}\right], \tag{22}$$

where

$$\xi = \frac{1-\theta_{\mathsf{N}}\bar{\gamma}}{2\theta_{\mathsf{N}}\bar{\gamma}a_{\mathsf{f}}}, \quad \delta = \bar{\gamma}-1, \quad \beta = \bar{\gamma}a_{\mathsf{f}}.$$

The proof of Lemma 1 is concluded. □

IV. Numerical Results

In this section, we present representative numerical results to demonstrate the achieved secrecy performance. Unless otherwise noted, the simulation configurations are outlined in Table I.

TABLE I
Simulation Parameters

Parameters	Value
Distance between S and N (d_{SN})	10 m
Distance between S and F (d_{SF})	12.5 m
Position of S	(0, 0)
Position of N	(10, 0)
Position of F	(12.5, 0)
Position of E	(5, -5)
Position of R_L	(d_{SN}/L, 0)
Number of hops (L)	4
Target secrecy rate $\bar{\mathsf{R}}$	0.1 bps/Hz
Transmit SNR $\hat{\gamma} \in \{\gamma_{\mathsf{S}}, \gamma_{\mathsf{R}}\}$	[-10:10:10] dB

Fig. 2 represents the impact of $\hat{\gamma}$ on the SOP of cell-center user with different number of hops (L). As can be seen in Fig. 2, the SOP is decreased when the γ increases. The reason is that when the $\hat{\gamma}$ increases, the main and the eavesdropper channel capacity improves. However, the impact of $\hat{\gamma}$ of the main channel capacity is more than that of the eavesdropper channel capacity. Moreover, when the number of hops increases, the SOP also decreases. The reason is that with more available hops, the system can potentially select a path with a lower secrecy capacity. Additionally, the SOP is inversely proportional to the number of hops corresponding to (12).

Fig 3 illustrates the impact of $\hat{\gamma}$ on the SOP with varying numbers of hops (L) at User F. The presence of a minimum SOP value around the -10 dB region for both ($L = 4$) and ($L = 6$) is significant. When the $\hat{\gamma}$ increases from -30 dB to -10 dB, the main and the eavesdropper channel

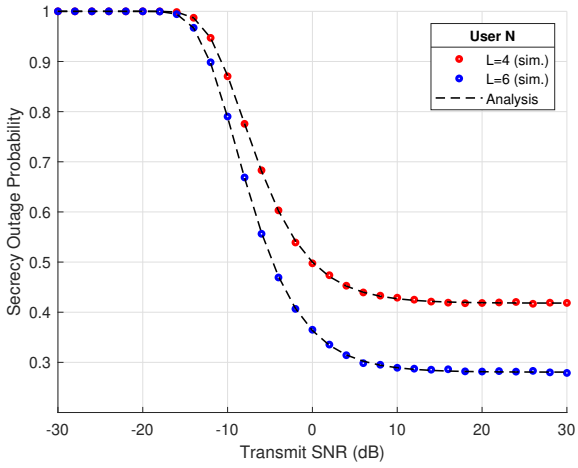

Fig. 2. The impact of transmit SNR ($\hat{\gamma}$) on the SOP with L = 4 and 6 at User N

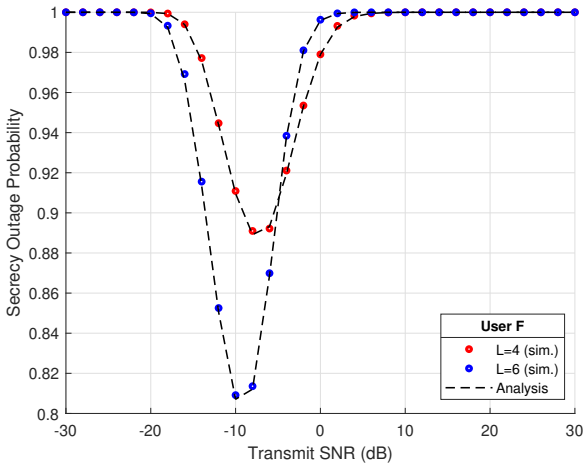

Fig. 3. The impact of transmit SNR ($\hat{\gamma}$) on the SOP with L = 4 and 6 at User F

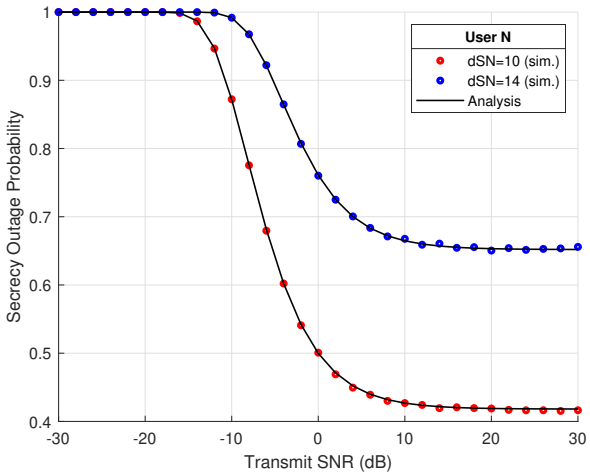

Fig. 4. The impact of transmit SNR ($\hat{\gamma}$) on the SOP with d_{SN} = 10 and 14 at User N

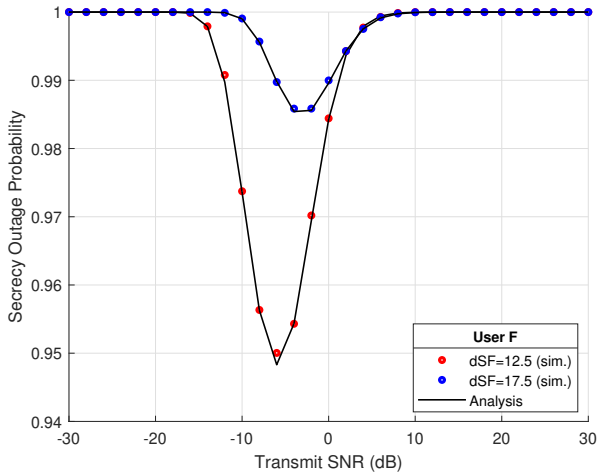

Fig. 5. The impact of transmit SNR ($\hat{\gamma}$) on the SOP with d_{SN} = 10 and 14 at User F

capacity improves. And as described before, the main channel capacity is more improved than the eavesdropper capacity. However, when the $\hat{\gamma}$ is greater than -10 dB, the interference from near user increases, which is corresponds to (8). In contrast, the eavesdropper channel capacity improves because the eavesdropper can decode all user messages perfectly, which is related to (10) and (11). Consequently, the secrecy performance is dropped. Furthermore, for any given $\hat{\gamma}$, the scenario with $L = 6$ maintains a lower SOP than the situation with $L = 4$. As described before, when the number of hops increases, the system can potentially select a path with a lower secrecy capacity because it corresponds to (12).

Fig. 4 illustrates the impact of $\hat{\gamma}$ on the SOP with various distances between source to User N. As can be observed in Fig. 4, when the distance between the source and the near user increases, the SOP increases. Corresponds to the channel gain when the distance increases, the channel gain decreases. Thus, the channel capacity is decreased. However, when the distance between the source and User N increases, the distance between the transmitter (source and relay) and eavesdropper is increased. This also results in decreased eavesdropper channel capacity, but the effect of the decreased main channel capacity is more than decreasing eavesdropper channel capacity.

Fig. 5 shows the transmit SNR, $\hat{\gamma}$, as a function of SOP performance with various distances between the source and User F. As can be observed in Fig. 5, when the distance increases from 12.5 m to 17.5 m, the SOP increases. As described before, when the distance increases, the channel gain decreases. Consequently, the main channel capacity is decreased. In addition, when the $\hat{\gamma}$ increases, the interference from the User N signal increases, thus making the main channel capacity decrease.

V. Conclusion

In this paper, we investigate the secrecy performance of multi-hop transmission with NOMA system. To analyze the relationship between network parameters and secrecy capacity performance, we derive exact closed-form expressions for the SOP for both cell-center and cell-edge users. From the numerical results, we evaluate the impact of the number of hops and the distance between the source to the cell-center and cell-edge users on the confidentiality performance. The comparison between simulation and analysis are closely matched. Furthermore, the impact of the number of hops and the distance between the source and cell-center and cell-edge users are evaluated thoroughly. However, it is important to note that while our work primarily concentrates on the secrecy performance of multi-hop transmission within the NOMA system, it does not encompass the consideration of additional security mechanisms or countermeasures commonly employed in practical scenarios such as encryption, authentication, or intrusion detection. In future work, we aim to further enhance the security of multi-hop transmissions by developing a secure routing protocol that harnesses the principles of physical layer security and blockchain technology to protect confidential packets against potential sniffing attacks.

Acknowledgement

This work was supported by National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2022R1A2B5B01001190). Prof. Beongku An is the corresponding author.

References

[1] K. Kavitha and S. Vappangi, "Performance Analysis of Novel User Pairing-Based Hybrid NOMA System With Fixed/Optimal Power Allocation Strategy," *IEEE Access*, vol. 11, pp. 106 037–106 053, 2023.

[2] Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "Exploiting TAS schemes to Enhance the PHY-security in Cooperative NOMA Networks: A Deep Learning Approach," in *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Bali, Indonesia, 2023, pp. 199–204.

[3] R. H. Y. Perdana, T. V. Nguyen, and B. An, "Adaptive User Pairing in Multi-IRS-aided Massive MIMO-NOMA Networks: Spectral Efficiency Maximization and Deep Learning Design," *IEEE Trans. Commun.*, vol. 71, no. 7, pp. 4377–4390, 2023.

[4] K. Shim, T.-V. Nguyen, and B. An, "Exploiting Opportunistic Scheduling Schemes to Improve Physical-Layer Security in MU-MISO NOMA Systems," *IEEE Access*, vol. 7, pp. 180 867–180 886, 2019.

[5] P. T. Tin, N. V. Hien, M. Voznak, and L. Sevcik, "Performance Comparison Between NOMA and OMA Relaying Protocols in Multi-Hop Networks over Nakagami-m Fading Channels under Impact of Hardware Impairments," in *2019 IEEE/ACM 23rd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, Cosenza, Italy, 2019, pp. 1–4.

[6] K. Shim and B. An, "Exploiting Secure Multihop Transmission in Underlying Cognitive Radio Networks: Analysis and Deep Learning Approaches," in *5th Int. Conf. Artif. Intell. Inf. Commun. ICAIIC 2023*. Bali, Indonesia: IEEE, 2023, pp. 281–285.

[7] T. V. Nguyen, T.-N. Do, V. N. Q. Bao, D. B. d. Costa, and B. An, "On the Performance of Multihop Cognitive Wireless Powered D2D Communications in WSNs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2684–2699, 2020.

[8] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative noma systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.

[9] L.-T. Tu, V.-D. Phan, T. N. Nguyen, P. T. Tran, T. T. Duy, Q.-S. Nguyen, N.-T. Nguyen, and M. Voznak, "Performance Analysis of Multihop Full-Duplex NOMA Systems with Imperfect Interference Cancellation and Near-Field Path-Loss," *Sensors*, vol. 23, no. 1, 2023.

[10] Y. Triwidyastuti, R. H. Y. Perdana, K. Shim, and B. An, "Secrecy Performance Analysis of Cooperative Multihop Transmission for WSNs under Eavesdropping Attacks," *Sensors*, vol. 23, no. 17, pp. 1–25, 2023.

[11] T. N. Do, D. B. Da Costa, T. Q. Duong, and B. An, "Improving the Performance of Cell-Edge Users in NOMA Systems Using Cooperative Relaying," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 1883–1901, 2018.

[12] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products Seventh Edition*. Elsevier Academic Press, 2007.

[13] M. Abramowitz, I. A. Stegun, and D. M. Miller, "Handbook of Mathematical Functions With Formulas, Graphs and Mathematical Tables (National Bureau of Standards Applied Mathematics Series No. 55)," *Journal of Applied Mechanics*, vol. 32, pp. 239–239, 1965.