A Physical Layer Security-based Transmit Antenna Selection Scheme for NOMA Systems

Kyusung Shim*, Hyukchun Oh†, Tri Nhu Do*‡, and Beongku An†§
*Dept. of Electronics and Computer Engineering in Graduate School, Hongik University, Republic of Korea
†Dept. of Software and Communications Engineering, Hongik University, Republic of Korea
Emails: *shimkyusung@outlook.kr, †ohhyukchun@gmail.com, ‡dotrinhu@gmail.com, §beongku@hongik.ac.kr

***Abstract*—In this paper, we propose a novel transmit antenna selection (TAS) scheme to improve the physical layer security of two-user non-orthogonal multiple access (NOMA) systems. Specifically, the proposed TAS scheme aims to select an antenna that is the most robust against the interception of an eavesdropper, in particular, the antenna that minimizes the maximum capacity of the eavesdropper channels. To evaluate the performance of the proposed scheme, we derive an exact closed-form expression for the secrecy outage probability (SOP) of the near user and a tight approximated closed-form expression for the SOP of the far user. Numerical results reveals that the proposed TAS scheme improves the total secrecy outage probability compared to that of some existing schemes. We also provide some insightful discussions on the impact of the number of antenna and the location of the eavesdropper on the security capability of the considered system.**

I. Introduction

Non-orthogonal multiple access (NOMA) has been conceived as a key technique in the fifth generation (5G) networks to improve the spectral efficiency and support massive connectivity [1], [2]. Different from the conventional orthogonal multiple access (OMA) techniques, NOMA exploits power domain to conduct signal multiplexing. More specifically, the principle of NOMA is that a base station communicates with multiple users on the same frequency at the same time but with different power allocation coefficients. Please refer to the next section for a detailed operation of NOMA transmission.

On the other hand, downlink NOMA transmissions raise some concerns about security capability since messages of multiple users are superimposed and broadcasted at the same time [3]–[5]. Specifically, if a malicious user successfully intercepts the superposed message in down link NOMA transmissions, then the malicious user overhears multiple users' information. Thus, the security issue in NOMA systems is more important than that in conventional OMA systems. In order to deal with this issue, the authors in [4] took the advantage of spatial random deployment of both legitimate users and eavesdroppers to enhance the security of NOMA systems. Recently, in [5], the authors proposed to use artificial-noise performed by a full-duplex relay node to improve the secrecy performance of NOMA systems.

Another approach to improve the security capability of NOMA is to equip more antennas at the BS and then select the most robust one to perform NOMA. Indeed, in [6], the authors proposed a transmit antenna selection (TAS) scheme that was able to improve physical layer security of a considered NOMA scheme.

In this paper, we propose a novel TAS scheme aiming to enhance the robustness of the two-user NOMA transmissions. The main contributions and features of the paper can be summarized as:

- Considering two-user NOMA transmission, we propose a min-max criterion to select the best antenna, which has not been reported in the literature. In particular, the selected antenna is able to minimize the maximum capacity of the eavesdropper channels, consequently, achieves better security capability.
- We develop a performance analysis in terms of secrecy outage probability (SOP). Specifically, we derive the exact closed-form expression for the SOP of the near user and the tight approximated closed-form expression for the SOP of the far user. The developed analysis is verified by Monte Carlo simulation.
- From the numerical results, we show that the proposed TAS scheme achieves better secrecy performance than some existing schemes in the middle and high regime of transmit signal-to-noise ratio (SNR). Additional, as the number of the transmit antennas increases, the proposed scheme provides better secrecy outage performance than that of the other considered ones.

II. System Model

Let us consider a NOMA downlink transmission where a BS, denoted by S, simultaneously communicates with a cell-center user, named User N, and a cell-edge user, called User F, by employing a two-user NOMA scheme as shown in Fig. 1. The NOMA communication is overheard by an eavesdropper, denoted by E. The BS is equipped with K antennas while each user is equipped with single antenna.

Let $h_{i\mathsf{T}}$ denote the fading coefficient of a channel from an antenna $i, i = 1, \ldots, K$ to a User T, where $\mathsf{T} \in \{\mathsf{N}, \mathsf{F}, \mathsf{E}\}$. Assuming all wireless channels in the network exhibit Rayleigh block flat fading, $h_{i\mathsf{T}}$ can be modeled as independent and identically distributed (i.i.d.) complex Gaussian random variables with zero-mean and variance λ_{ST}. Additionally, let n_{T} denote the additive white Gaussian noise (AWGN) at User T, with zero-mean and variance σ^2_{T}. Thus, the channel gain $|h_{\mathsf{XY}}|^2$, where $\mathsf{X} \in \{i\}$ and $\mathsf{Y} \in \{\mathsf{N}, \mathsf{F}, \mathsf{E}\}$, is an exponential random variable with probability density function

(PDF), $f_{|h_{\mathsf{XY}}|^2}(z) = \frac{1}{\lambda_{\mathsf{XY}}} e^{-\frac{z}{\lambda_{\mathsf{XY}}}}, \forall z \geq 0$, otherwise, i.e., $z < 0$, $f_{|h_{\mathsf{XY}}|^2}(z) = 0$, where λ_{XY} denotes the mean of $|h_{\mathsf{XY}}|^2$. Additionally, the average channel gain can be written as $\mathrm{E}[|h_{\mathsf{XY}}|^2] = (d_{\mathsf{XY}}/d_0)^{-\epsilon}\mathcal{L}$ [7], where d_{XY} represents the distance between two nodes (in meters), ϵ stands for path-loss exponent, d_0 denotes the reference distance, and $\mathcal{L}$ is the average signal power attenuation at d_0.

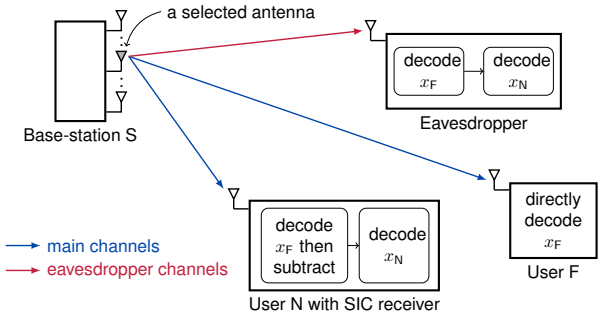

Fig. 1. An illustration of a two-user NOMA system with TAS under the present of an eavesdropper.

Suppose that antenna i on the BS has been selected for information transmission. According to the principle of NOMA, the intended transmit messages x_{N} and x_{F} of Users N and F, respectively, are superposed as $\sqrt{p_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{p_{\mathsf{F}}}x_{\mathsf{F}}$ and then broadcasted by the selected antenna at the beginning of the first sub-block time, where p_{N} and p_{F} denote the power allocation coefficients (PACs) for Users N and F, respectively. Following the principle of NOMA, we assume that $|h_{i\mathsf{N}}|^2 > |h_{i\mathsf{F}}|^2$, $0 < p_{\mathsf{N}} < p_{\mathsf{F}}$, and $p_{\mathsf{N}} + p_{\mathsf{F}} = 1$ [8].

1) At User N*:* The received observation at User N can be written as

$$y_{i\mathsf{N}} = (\sqrt{p_{\mathsf{N}}P_{\mathsf{S}}}x_{\mathsf{N}} + \sqrt{p_{\mathsf{F}}P_{\mathsf{S}}}x_{\mathsf{F}})h_{i\mathsf{N}} + n_{\mathsf{N}}. \tag{1}$$

According to the principle of NOMA, the SIC receiver at User N first decodes x_{F} and then subtracts this component from the received signal to detect its own message, i.e., x_{N} [8]. Thus, the received signal-to-interference-plus-noise ratio (SINR) at User N to decode x_{F} can be expressed as

$$\gamma_{i\mathsf{N}}^{x_{\mathsf{F}}} = \frac{p_{\mathsf{F}}P_{\mathsf{S}}|h_{i\mathsf{N}}|^2}{p_{\mathsf{N}}P_{\mathsf{S}}|h_{i\mathsf{N}}|^2 + \sigma_{\mathsf{N}}^2}, \tag{2}$$

and the received signal-to-noise ratio (SNR) at User N to decode x_{N} can be written as

$$\gamma_{i\mathsf{N}}^{x_{\mathsf{N}}} = \frac{p_{\mathsf{N}}P_{\mathsf{S}}|h_{i\mathsf{N}}|^2}{\sigma_{\mathsf{N}}^2}. \tag{3}$$

2) At User F*:* The received observation at User F can be expressed as

$$y_{i\mathsf{F}} = (\sqrt{p_{\mathsf{N}}P_{\mathsf{S}}}x_{\mathsf{N}} + \sqrt{p_{\mathsf{F}}P_{\mathsf{S}}}x_{\mathsf{F}})h_{i\mathsf{F}} + n_{\mathsf{F}}. \tag{4}$$

In contrast with User N, User F can directly decode its information signal since User F is allocated with higher transmit power and thus the interference introduced by the information signal of User N can be considered as noise [8]. Thus, the received SNR at User F to decode x_{F} that can be written as

$$\gamma_{i\mathsf{F}}^{x_{\mathsf{F}}} = \frac{p_{\mathsf{F}}P_{\mathsf{S}}|h_{i\mathsf{F}}|^2}{p_{\mathsf{N}}P_{\mathsf{S}}|h_{i\mathsf{F}}|^2 + \sigma_{\mathsf{F}}^2}. \tag{5}$$

3) At the Eavesdropper E*:* Due to the broadcast nature of wireless communications, the received observation at the eavesdropper E can be expressed as

$$y_{i\mathsf{E}} = (\sqrt{p_{\mathsf{N}}P_{\mathsf{S}}}x_{\mathsf{N}} + \sqrt{p_{\mathsf{F}}P_{\mathsf{S}}}x_{\mathsf{F}})h_{i\mathsf{E}} + n_{\mathsf{E}}. \tag{6}$$

Assuming that the eavesdropper is also equipped with the SIC receiver as in [3], [6], the SINR at E to decode x_{F} can be expressed as

$$\gamma_{i\mathsf{E}}^{x_{\mathsf{F}}} = \frac{p_{\mathsf{F}}P_{\mathsf{S}}|h_{i\mathsf{E}}|^2}{p_{\mathsf{N}}P_{\mathsf{S}}|h_{i\mathsf{E}}|^2 + \sigma_{\mathsf{E}}^2}, \tag{7}$$

and the SNR at E to decode x_{N} can be written as

$$\gamma_{i\mathsf{E}}^{x_{\mathsf{N}}} = p_{\mathsf{N}}P_{\mathsf{S}}|h_{i\mathsf{E}}|^2/\sigma_{\mathsf{E}}^2. \tag{8}$$

A. The Proposed Transmit Antenna Selection (TAS) Criteria

The proposed TAS schemes are conducted before data transmission through the signaling and channel state information (CSI) estimation/calculation system. We assume that the required CSI of each scheme is available [7], [9], [10].

The instantaneous transmission rate achieved by E associating with antenna i for x_{N} and x_{F} can be expressed as

$$C_{i\mathsf{E}}^{x_{\mathsf{N}}} = \log_2(1 + \gamma_{i\mathsf{E}}^{x_{\mathsf{N}}}), \tag{9}$$

$$C_{i\mathsf{E}}^{x_{\mathsf{F}}} = \log_2(1 + \gamma_{i\mathsf{E}}^{x_{\mathsf{F}}}), \tag{10}$$

respectively. It is noteworthy that the messages x_{N} and x_{F} are independent, and the eavesdropper aims to intercept them individually. Thus, from the perspective of the legitimate nodes, i.e., Users N and F, the potential achievable rate of the eavesdropper channel for a given antenna i can be written as

$$C_{i\mathsf{E}} = \max\left\{C_{i\mathsf{E}}^{x_{\mathsf{N}}}, C_{i\mathsf{E}}^{x_{\mathsf{F}}}\right\}. \tag{11}$$

Let i^* denote the selected antenna, the proposed TAS scheme aims to select an antenna whose eavesdropper channel is the most robust against the eavesdropper's interception. Mathematically, the criterion of the proposed TAS scheme can be expressed as

$$i^* = \arg \min_{1 \leq i \leq K} \max\left\{C_{i\mathsf{E}}^{x_{\mathsf{N}}}, C_{i\mathsf{E}}^{x_{\mathsf{F}}}\right\}. \tag{12}$$

The performance investigation of the the proposed TAS scheme in terms of SOP will be presented in the next section.

III. Performance Analysis

Without loss of generality, we assume that all nodes in the system have the same noise power, i.e., $\sigma_{\mathsf{N}}^2 = \sigma_{\mathsf{F}}^2 = \sigma_{\mathsf{E}}^2 \triangleq \sigma^2$ as in [6], [9], [10]. For the sake of notational convenience, let

$\bar{\gamma} \triangleq P_{\mathsf{S}}/\sigma^2$. Hence, (7), (8), and (12), the criterion to select the best antenna can be rewritten as

$$i^* = \arg \min_{1\le i\le K} \max \Bigg\{ \log_2 \left(1 + \frac{p_{\mathsf{F}}\bar{\gamma}|h_{i\mathsf{E}}|^2}{p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2 + 1}\right), \log_2\left(1 + p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2\right)\Bigg\}. \quad (13)$$

For the case $\log_2\left(1 + \frac{p_{\mathsf{F}}\bar{\gamma}|h_{i\mathsf{E}}|^2}{p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2+1}\right) < \log_2\left(1 + p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2\right)$, the criterion in (13) can be rewritten as

$$\begin{aligned} i^* &= \arg \min_{1\le i\le K} \log_2\left(1 + p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2\right), \\ &= \arg \min_{1\le i\le K} |h_{i\mathsf{E}}|^2. \end{aligned} \quad (14)$$

For the case $\log_2\left(1 + \frac{p_{\mathsf{F}}\bar{\gamma}|h_{i\mathsf{E}}|^2}{p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2+1}\right) > \log_2\left(1 + p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2\right)$, the criterion in (13) can be rewritten as

$$\begin{aligned} i^* &= \arg \min_{1\le i\le K} \log_2 \left(1 + \frac{p_{\mathsf{F}}\bar{\gamma}|h_{i\mathsf{E}}|^2}{p_{\mathsf{N}}\bar{\gamma}|h_{i\mathsf{E}}|^2 + 1}\right), \\ &= \arg \min_{1\le i\le K} |h_{i\mathsf{E}}|^2, \end{aligned} \quad (15)$$

where the second equal sign in (15) happens due to the fact that for non-negative constants c_1, c_2, X_1, X_2, it is straightforward that if $\frac{c_1X_1}{c_2X_1+1} \le \frac{c_1X_2}{c_2X_2+1}$, then $X_1 \le X_2$. For the sake of notational convenience, let $X_i \triangleq |h_{i\mathsf{N}}|^2$, $Y_i \triangleq |h_{i\mathsf{F}}|^2$, and $Z_i \triangleq |h_{i\mathsf{E}}|^2$. The following Lemma 1 and Lemma 2 help to analyze the secrecy outage probability in the proposed NOMA system.

Lemma 1. *Suppose that $|h_{i^*\mathsf{E}}|^2 = \min_{1\le i\le K}|h_{i\mathsf{E}}|^2$. the cumulative distribution function (CDF) and probability density function (PDF) of $|h_{i^*\mathsf{E}}|^2$ can be, respectively, written as:*

$$F_{|h_{i^*\mathsf{E}}|^2}(h) = 1 - e^{-\frac{K}{\lambda_{\mathsf{SE}}}h}, \quad (16)$$

$$f_{|h_{i^*\mathsf{E}}|^2}(h) = \frac{K}{\lambda_{\mathsf{SN}}} e^{-\frac{K}{\lambda_{\mathsf{SE}}}h}. \quad (17)$$

Proof. From the (12), the CDF of $|h_{i^*\mathsf{E}}|^2$ can be expressed as:

$$\begin{aligned} F_{|h_{i^*\mathsf{E}}|^2}(h) &= \Pr\left(\min_{1\le i\le K}\left\{|h_{i\mathsf{E}}|^2\right\} < h\right) \\ &= 1 - \Pr\left(\min_{1\le i\le K}\left\{|h_{i\mathsf{E}}|^2\right\} \ge h\right), \end{aligned} \quad (18)$$

since the event of $|h_{i\mathsf{E}}|^2$ is independent, The $F_{|h_{i^*\mathsf{E}}|^2}(z)$ can be expressed as:

$$\begin{aligned} F_{\gamma_{i^*\mathsf{E}}}(h) &= 1 - \Pr\left(\bigcap_{i=1}^{K}\left(\gamma_{i\mathsf{E}} \ge h\right)\right) \\ &= 1 - \prod_{i=1}^{K}\left(1 - \Pr(\gamma_{i\mathsf{E}} < h)\right). \end{aligned} \quad (19)$$

From the statistical characteristic of $|h_{i\mathsf{E}}|^2$, (19) can be further re-written as:

$$\begin{aligned} F_{|h_{i^*\mathsf{E}}|^2}(h) &= 1 - \prod_{i=1}^{K}\left[1 - \left(1 - \exp\left(-\frac{1}{\lambda_{\mathsf{SE}}}h\right)\right)\right] \\ &= 1 - \exp\left(-\frac{K}{\lambda_{\mathsf{SE}}}h\right). \end{aligned} \quad (20)$$

And after some algebraic manipulations, we can obtain the PDF of $|h_{i^*\mathsf{E}}|^2$ as shown in (17). This completes the proof of Lemma 1. □

From the results in Lemma 1, the probability of an selected antenna in each time slot is provided in the following lemma.

Lemma 2. *In a certain time slot, the probability that an selected antenna i as the best antenna i^* can be written as:*

$$\Pr(i^* = i) = \frac{1}{K}. \quad (21)$$

Proof. Using the total probability theory [11] and based on the criterion in (13), the probability that a antenna is the selected antenna can be expressed as:

$$F_{\gamma_{i^*\mathsf{U}}}(h) = \sum_{i=1}^{K} \underbrace{\Pr\left(i^* = i\right)}_{\Psi} \Pr\left(\gamma_{i\mathsf{U}} < h\right). \quad (22)$$

where $\mathsf{U} \in \{\mathsf{N}, \mathsf{F}\}$. From the proposed antenna selection scheme in (12), Ψ in (22) can be re-written as:

$$\begin{aligned} \Psi &= \Pr(\gamma_{1\mathsf{E}} > \gamma_{i\mathsf{E}}) \cap \cdots \cap \Pr(\gamma_{K\mathsf{E}} > \gamma_{i\mathsf{E}}) \\ &= \Pr\left(\bigcap_{j=1, j\ne i}^{K}\left(\gamma_{j\mathsf{E}} > \gamma_{i\mathsf{E}}\right)\right). \end{aligned} \quad (23)$$

We observe that the events of probability in (23) are not mutually exclusive since each events include the common component $\gamma_{i\mathsf{E}}$. Thus, by conditioning on $\gamma_{i\mathsf{E}} = h$, Ψ can be further re-expressed as

$$\begin{aligned} \Psi &= \int_0^\infty \prod_{j=1}^{K-1}\left[\Pr(\gamma_{j\mathsf{E}} > h)\right] f_{\gamma_{i\mathsf{E}}}(h)dh \\ &= \int_0^\infty \prod_{j=1}^{K-1}\left[1 - \Pr\left(\gamma_{j\mathsf{E}} \le h\right)\right] f_{\gamma_{i\mathsf{E}}}(h)dh. \end{aligned} \quad (24)$$

Similar to (20), Ψ can be further obtained as (16), specifically,

$$\begin{aligned} \Psi &= \int_0^\infty \prod_{j=1}^{K-1}\left[1 - \left(1 - \exp\left(-\frac{1}{\lambda_{\mathsf{SE}}}h\right)\right)\right] f_{\gamma_{i\mathsf{E}}}(h)dh \\ &= \int_0^\infty \exp\left(-\frac{K-1}{\lambda_{\mathsf{SE}}}h\right)\frac{1}{\lambda_{\mathsf{SE}}}\exp\left(-\frac{1}{\lambda_{\mathsf{SE}}}h\right)dh. \end{aligned} \quad (25)$$

After some basic manipulation, Ψ can be obtained as:

$$\Psi = \int_0^\infty \frac{1}{\lambda_{\mathsf{SE}}}\exp\left(-\frac{K}{\lambda_{\mathsf{SE}}}h\right)dh = \frac{1}{K}. \quad (26)$$

This completes the proof of Lemma 2. □

In physical layer security-based systems, the secrecy outage probability (SOP) can be defined as the probability that the secrecy capacity of a user falls below a predefined secrecy target rate (bps/Hz) [12].

1) At User N*:* In what follows, the SOP of User N can be expressed as

$$\begin{aligned} P_{\mathsf{SOP},x_\mathsf{N}} &= \Pr\left(C_{i^*\mathsf{N}}^{x_\mathsf{N}} - C_{i^*\mathsf{E}}^{x_\mathsf{N}} < R_{\mathsf{th},x_\mathsf{N}}\right), \\ &= \Pr\left(\log_2(1+\bar{\gamma}p_\mathsf{N}\gamma_{i^*\mathsf{N}})\right. \\ &\qquad \left. - \log_2(1+\bar{\gamma}p_\mathsf{N}\gamma_{i^*\mathsf{E}}) < R_{\mathsf{th},x_\mathsf{N}}\right) \\ &= \Pr\left(\frac{1+\bar{\gamma}p_\mathsf{N}\gamma_{i^*\mathsf{N}}}{1+\bar{\gamma}p_\mathsf{N}\gamma_{i^*\mathsf{E}}} < \gamma_{\mathsf{th},x_\mathsf{N}}\right), \end{aligned} \tag{27}$$

where $C_{i^*\mathsf{N}}^{x_\mathsf{N}}$, $C_{i^*\mathsf{E}}^{x_\mathsf{N}}$ denote the main channel capacity and eavesdropper channel capacity for User N, respectively. $R_{\mathsf{th},x_\mathsf{N}}$ presents the SNR threshold for correctly decoding the message x_N and $\gamma_{\mathsf{th},x_\mathsf{N}} \triangleq 2^{R_{\mathsf{th},x_\mathsf{N}}}$. As we can observe, the events of the probability in (27) are not mutually exclusive because they include the same components $\gamma_{i^*\mathsf{E}}$. Thus, the conditioning on $|h_{i^*\mathsf{E}}|^2 = z$ and after some algebraic manipulation, (27) can further expressed as

$$P_{\mathsf{SOP},x_\mathsf{N}} = \int_0^\infty \Pr\left(\gamma_{i^*\mathsf{N}} < \frac{\gamma_{\mathsf{th},x_\mathsf{N}}-1}{p_\mathsf{N}\bar{\gamma}} + \gamma_{\mathsf{th},x_\mathsf{N}} z\right) f_{\gamma_{i^*\mathsf{E}}}(z)dz. \tag{28}$$

Since the proposed antenna selection scheme selects the transmit antenna to minimize the $C_{i\mathsf{E}}$, the statistical characteristic of $|h_{i^*\mathsf{E}}|^2$ is presented in the Lemma 1. Additionally, The probability that an antenna is the selected antenna is presented at Lemma 2. Thus, the $P_{\mathsf{SOP},x_\mathsf{N}}$ can be further re-written as:

$$\begin{aligned} &P_{\mathsf{SOP},x_\mathsf{N}} \\ &= \int_0^\infty \sum_{i=1}^{K} \Pr(i^*=i) \Pr\left(|h_{i\mathsf{N}}|^2 < \frac{\gamma_{\mathsf{th},x_\mathsf{N}}-1}{p_\mathsf{N}\bar{\gamma}} + \gamma_{\mathsf{th},x_\mathsf{N}} z\right) \\ &\quad \times f_{\gamma_{i^*\mathsf{E}}}(z)dz \\ &= \underbrace{\int_0^\infty \frac{K}{\lambda_\mathsf{SE}} \exp\left(-\frac{K}{\lambda_\mathsf{SE}} z\right) dz}_{\Phi_1} - \frac{K}{\lambda_\mathsf{SE}} \exp\left(-\frac{1}{\lambda_\mathsf{SN}} \frac{(\gamma_{\mathsf{th},x_\mathsf{N}}-1)}{p_\mathsf{N}\bar{\gamma}}\right) \\ &\quad \times \underbrace{\int_0^\infty \exp\left(-\left(\frac{\gamma_{\mathsf{th},x_\mathsf{N}}}{\lambda_\mathsf{SN}} + \frac{K}{\lambda_\mathsf{SE}}\right) z\right) dz}_{\Phi_2}. \end{aligned} \tag{29}$$

In order to further simplify the (29), we rely on the integration property, i.e., $\int_0^\infty \exp(-px)dx = 1/p$ [13, Eq. (3.310)], Φ_1 and Φ_2 can be obtained as:

$$\Phi_1 = \int_0^\infty \frac{K}{\lambda_\mathsf{SE}} \exp\left(-\frac{K}{\lambda_\mathsf{SE}} z\right) dz = 1, \tag{30}$$

$$\begin{aligned} \Phi_2 &= \int_0^\infty \exp\left(-\left(\frac{\gamma_{\mathsf{th},x_\mathsf{N}}}{\lambda_\mathsf{SN}} + \frac{K}{\lambda_\mathsf{SE}}\right) z\right) dz \\ &= \frac{\lambda_\mathsf{SN}\lambda_\mathsf{SE}}{K\lambda_\mathsf{SN} + \gamma_{\mathsf{th},x_\mathsf{N}}\lambda_\mathsf{SE}}. \end{aligned} \tag{31}$$

respectively. By substituting (30) and (31) into (29), Consequently, the $P_{\mathsf{SOP},x_\mathsf{N}}$ can be written as:

$$P_{\mathsf{SOP},x_\mathsf{N}} = 1 - \frac{K\lambda_\mathsf{SN}}{K\lambda_\mathsf{SN} + \gamma_{\mathsf{th},x_\mathsf{N}}\lambda_\mathsf{SE}} \exp\left(-\frac{\gamma_{\mathsf{th},x_\mathsf{N}}-1}{\lambda_\mathsf{SN}}\right). \tag{32}$$

(32) is the exact closed-form expression of the near user with the proposed scheme for NONA system.

2) At User F*:* The SOP of User F can be expressed as

$$\begin{aligned} P_{\mathsf{SOP},x_\mathsf{F}} &= \Pr\left(C_{i^*\mathsf{F}}^{x_\mathsf{F}} - C_{i^*\mathsf{E}}^{x_\mathsf{F}} < R_{\mathsf{th},x_\mathsf{F}}\right), \\ &= \Pr\left(\log_2\left(1+\gamma_{i^*\mathsf{F}}\right) - \log_2(1+\gamma_{i^*\mathsf{E}}) < R_{\mathsf{th},x_\mathsf{F}}\right) \\ &= \Pr\left(\frac{1+\gamma_{i^*\mathsf{F}}}{1+\gamma_{i^*\mathsf{E}}} < \gamma_{\mathsf{th},x_\mathsf{F}}\right), \end{aligned} \tag{33}$$

where $C_{i^*\mathsf{F}}^{x_\mathsf{F}}$, $C_{i^*\mathsf{E}}^{x_\mathsf{F}}$ denote the main channel capacity and eavesdropper channel capacity for User F message, respectively. $R_{\mathsf{th},x_\mathsf{F}}$ presents the SNR threshold for correctly decoding the message x_F, and $\gamma_{\mathsf{th},x_\mathsf{F}} \triangleq 2^{R_{\mathsf{th},x_\mathsf{F}}}$. (33) can be further expressed as:

$$\begin{aligned} P_{\mathsf{SOP},x_\mathsf{F}} &= \Pr\left(\gamma_{i^*\mathsf{F}} < \gamma_{\mathsf{th},x_\mathsf{F}} - 1 + \gamma_{\mathsf{th},x_\mathsf{F}}\gamma_{i^*\mathsf{E}}\right) \\ &= \Pr\left(\frac{\bar{\gamma}p_\mathsf{F}|h_{i^*\mathsf{F}}|^2}{\bar{\gamma}p_\mathsf{N}|h_{i^*\mathsf{F}}|^2+1}\right. \\ &\qquad \left. < \gamma_{\mathsf{th},x_\mathsf{F}} \frac{\bar{\gamma}p_\mathsf{F}|h_{i^*\mathsf{E}}|^2}{\bar{\gamma}p_\mathsf{N}|h_{i^*\mathsf{E}}|^2+1} + \gamma_{\mathsf{th},x_\mathsf{F}} - 1\right). \end{aligned} \tag{34}$$

Similar to the case of the near user, the events of the probability in (34) are not mutually exclusive because they include the same component $\frac{\bar{\gamma}p_\mathsf{F}|h_{i^*\mathsf{E}}|^2}{\bar{\gamma}p_\mathsf{N}|h_{i^*\mathsf{E}}|^2+1}$. Thus, conditioning on $\frac{\bar{\gamma}p_\mathsf{F}|h_{i^*\mathsf{E}}|^2}{\bar{\gamma}p_\mathsf{N}|h_{i^*\mathsf{E}}|^2+1} = t$, the $P_{\mathsf{SOP},x_\mathsf{F}}$ can be expressed as:

$$\begin{aligned} &P_{\mathsf{SOP},x_\mathsf{F}} \\ &= \int_0^\infty \Pr\left(\frac{\bar{\gamma}p_\mathsf{F}|h_{i^*\mathsf{F}}|^2}{\bar{\gamma}p_\mathsf{N}|h_{i^*\mathsf{F}}|^2+1} < \gamma_{\mathsf{th},x_\mathsf{F}} t + \gamma_{\mathsf{th},x_\mathsf{F}} - 1\right) f_T(t)dt \\ &= \int_0^\infty \Pr\left(|h_{i^*\mathsf{F}}|^2 < \frac{\gamma_{\mathsf{th},x_\mathsf{F}} t + \gamma_{\mathsf{th},x_\mathsf{F}} - 1}{\bar{\gamma}\left[p_\mathsf{F} - p_\mathsf{F}(\gamma_{\mathsf{th},x_\mathsf{F}} t + \gamma_{\mathsf{th},x_\mathsf{F}} - 1)\right]}\right) f_T(t)dt. \end{aligned} \tag{35}$$

Since the $|h_{i^*\mathsf{F}}|^2$ and $|h_{i^*\mathsf{E}}|^2$ are non-negative random variables, and the statistical characteristic of $|h_{i^*\mathsf{F}}|^2$ and $|h_{i^*\mathsf{E}}|^2$ are given in Lemma 1, Lemma 2, respectively, after some algebraic manipulation, (35) is can be further re-written as:

$$\begin{aligned} P_{\mathsf{SOP},x_\mathsf{F}} &= \int_0^{\frac{1}{p_\mathsf{N}\gamma_{\mathsf{th},x_\mathsf{F}}}-1} \left[1 - \Omega(\lambda_\mathsf{SF}, \gamma_{\mathsf{th},x_\mathsf{F}} t + \gamma_{\mathsf{th},x_\mathsf{F}} - 1)\right] \\ &\qquad \times \Lambda\left(\frac{M}{\lambda_\mathsf{SE}}, t\right) dt + \int_{\frac{1}{p_\mathsf{N}\gamma_{\mathsf{th},x_\mathsf{F}}}-1}^{\frac{p_\mathsf{F}}{p_\mathsf{N}}} \Lambda\left(\frac{M}{\lambda_\mathsf{SE}}, t\right) dt, \\ &= 1 - \int_0^{\frac{1}{p_\mathsf{N}\gamma_{\mathsf{th},x_\mathsf{F}}}-1} \Lambda\left(\frac{M}{\lambda_\mathsf{SE}}, t\right) \\ &\qquad \times \Omega\left(\lambda_\mathsf{SF}, \gamma_{\mathsf{th},x_\mathsf{F}} t + \gamma_{\mathsf{th},x_\mathsf{F}} - 1\right) dt. \end{aligned} \tag{36}$$

where

$$\Omega(\alpha,\omega) = \exp\left(-\frac{\omega}{\alpha\bar{\gamma}(p_\mathsf{F} - p_\mathsf{N}\omega)}\right),$$

$$\Lambda\left(\frac{K}{\alpha},\omega\right) = \frac{K}{\alpha}\frac{p_\mathsf{F}}{\bar{\gamma}(p_\mathsf{F} - p_\mathsf{N}\omega)^2} \exp\left(-\frac{K}{\alpha}\frac{\omega}{\bar{\gamma}(p_\mathsf{F} - p_\mathsf{N}\omega)}\right),$$

where α and $\frac{K}{\alpha}$ present the average channel power gain with a single antenna, the average channel power gain with multiple antenna K, respectively. To the best of the authors' knowledge, it is very difficult to obtain the exact closed-form

expression. In this paper, we approximate the (36) using the Gaussian-Chebyshev quadrature [14, eq.(25.4.38)]. We explain how to approximate the (36) using the Gaussian-Chebyshev quadrature at the next Lemma.

Lemma 3. *For a given function $g(x)$, whose its integral on $[a, b]$ does not admit a closed-form expression, the integral $\int_a^b g(x)dx$ can be approximated as:*

$$\int_a^b g(x)dx = \frac{b-a}{2}\sum_{i=1}^{N} w_i\sqrt{1-x_i^2}\,g\left(\frac{b-a}{2}x_i+\frac{b+a}{2}\right)+R_N, \tag{37}$$

where N denotes the number of term, $w_i = \pi/N$, $x_i = \cos((2i-1)\pi/N)$, $R_N = \pi f^{(2N)}(\zeta)/(2N)!2^{2N-1}$ means the remainder. The range of ζ is $-1 < \zeta < 1$.

Proof. To use Gaussian-Chebyshev quadrature, an integral over [a,b] is changed into an integral over [-1,1]. The change of interval can be obtained as

$$\int_a^b g(x)dx = \frac{b-a}{2}\underbrace{\int_{-1}^{1} g\left(\frac{b-a}{2}x+\frac{b+a}{2}\right)dx}_{\Xi}. \tag{38}$$

To apply (38) to Gaussian-Chebyshev quadrature, (38) can be re-expressed as

$$\begin{aligned}\Xi &= \int_{-1}^{1}\underbrace{g\left(\frac{b-a}{2}x+\frac{b+a}{2}\right)\sqrt{1-x^2}}_{h(x)}\frac{1}{\sqrt{1-x^2}}dx \\ &= \int_{-1}^{1} h(x)\frac{1}{\sqrt{1-x^2}}dx.\end{aligned} \tag{39}$$

By plugging (39) into (38) and making use the fact that [14, eq.(25.4.38)], $\int_a^b g(x)dx$ can be further expressed as:

$$\int_a^b g(x)dx = \frac{b-a}{2}\sum_{i=1}^{N} w_i\sqrt{1-x_i^2}\,g\left(\frac{b-a}{2}x_i+\frac{b+a}{2}\right)+R_N. \tag{40}$$

This completes the proof of Lemma 3. □

By invoking Lemma 3, the $P_{\mathsf{SOP},x_\mathsf{F}}$ can be approximated as:

$$\begin{aligned}P_{\mathsf{SOP},x_\mathsf{F}} = 1-\beta_1\sum_{n=1}^{N}\frac{\pi}{N}\sqrt{1-x_i^2}\,\Lambda\left(\frac{K}{\lambda_\mathsf{SE}},\beta_1 x_i+\beta_1\right) \\ \times\,\Omega\left(\lambda_\mathsf{SF},\gamma_{\mathsf{th},x_\mathsf{F}}(\beta_1 x_i+\beta_1)+\gamma_{\mathsf{th},x_\mathsf{F}}-1\right)+R_N.\end{aligned} \tag{41}$$

where $\beta_1 = \frac{\frac{1}{p_\mathsf{N}\gamma_{\mathsf{th},x_\mathsf{F}}}-1}{2}$. (41) is the approximated closed-form expression for the SOP of the far user in the considered system.

IV. Numerical Results

In this section, we present representative numerical results to demonstrate the achievable security capability improvement of the proposed TAS scheme. Monte-Carlo simulation results are generated to validate the developed analysis. In simulation setting, we assume that positions of the base station (S), User N, User F, and the eavesdropper (E) are randomly deployed satisfying some given distance constraints. Specifically, we set that the distance between S and User N is $d_{\mathsf{SN}} = 10$ m, the distance between S and User F is $d_{\mathsf{SF}} = 30$ m, and that the distance between S and eavesdropper is $d_{\mathsf{SE}} = 30$ m, respectively. Additional, the reference distance d_0 = 1 m, and power degradation at d_0 is $L = 30$ (dB), the path-loss exponent $\beta = 2.7$.

In order to demonstrate the performance improvement achieved by the proposed TAS scheme, we also consider some existing TAS schemes. For the sake of notational convenience, let Scheme I, Scheme II, Scheme III, and Scheme IV denote the proposed schemes, the random antenna selection scheme, and the two scheme proposed in [6], respectively, which can be detailed as follows. Schemes III and IV select an antenna that maximizes the capacity of the main channel associated with User N and User F, respectively, which can be mathematically expressed as:

$$i^*_{\text{schemeIII}} = \arg\max_{i=1,\ldots,K}\log_2(1+\gamma_{i\mathsf{N}}),$$
$$i^*_{\text{schemeIV}} = \arg\max_{i=1,\ldots,K}\log_2(1+\gamma_{i\mathsf{F}}).$$

In this section, we evaluate the performance of the considered TAS schemes in terms of total secrecy outage probability, which can be is mathematically defined as [3]:

$$P_{\mathsf{SOP,Total}} = 1-(1-P_{\mathsf{SOP},x_\mathsf{N}})(1-P_{\mathsf{SOP},x_\mathsf{F}}).$$

Fig. 2 illustrates the performance comparison between the four schemes, where the total SOP is plotted as a function of the transmit SNR (dBm). As can be seen, Scheme I gives the best performance at the middle and high range of the transmit SNR.

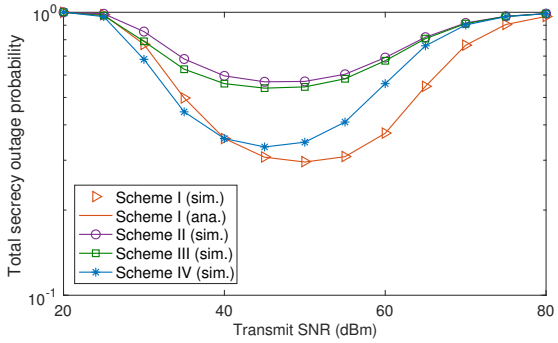

Fig. 2. Performance comparison illustration where the total secrecy outage probability is plotted as a function of the transmit SNR (dBm), where $K = 3$, $\gamma_{\mathsf{th},x_\mathsf{N}} = \gamma_{\mathsf{th},x_\mathsf{F}} = 0.1$ bps/Hz.

In Fig. 3, we investigate the impact of the number of antennas at the BS on the performance of the considered

schemes. As can be observed, the SOP of Scheme I significantly decreases as the number of antennas increases, which is in contrast to that of the others. It means that the proposed scheme is able to achieve higher diversity gain than the other considered schemes.

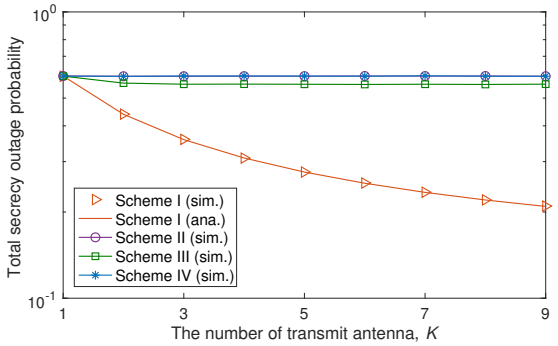

Fig. 3. Performance comparison illustration where the total secrecy outage probability is plotted as a function of the number of antenna, K, where $\gamma_{\mathrm{th},x_{\mathsf{N}}} = \gamma_{\mathrm{th},x_{\mathsf{F}}} = 0.1$ bps/Hz.

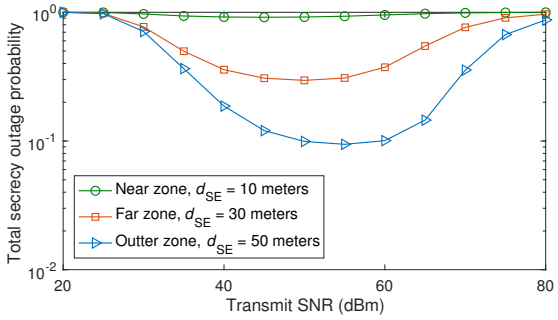

Fig. 4. Illustration for the impact of the location of the eavesdropper on the total secrecy outage probability where the total secrecy outage probability is plotted as a function of the transmit SNR (dBm) , where $K = 3$, $\gamma_{\mathrm{th},x_{\mathsf{N}}} = \gamma_{\mathrm{th},x_{\mathsf{F}}} = 0.1$ bps/Hz.

Next, we investigate the impact of the location of the eavesdropper on the the vulnerability of the system. Specifically, we consider three scenarios of the eavesdropper that is in a near zone, $d_{\mathsf{SE}} \leq d_{\mathsf{SN}}$, a far zone, $d_{\mathsf{SN}} \leq d_{\mathsf{SE}} \leq d_{\mathsf{SF}}$, and an outer zone, $d_{\mathsf{SE}} \geq d_{\mathsf{SF}}$, respectively. As shown in Fig. 4, the system is most vulnerable when the eavesdropper is located in the near zone while the system suffers the least influence when the eavesdropper is located in the outer zone.

V. Conclusions

In this paper, we have proposed the PHY-security-based TAS scheme, which selected the most robust antenna against the attack of the eavesdropper to the two-user NOMA system. We have derived the exact closed-form expression for the SOP of the near user and the tight approximated closed-form expression for the SOP of the far user. Our results have showed that the proposed TAS scheme supports higher security capability for the NOMA system in comparison to some existing TAS schemes. Additionally, the proposed TAS scheme takes more advantages than the others as the number of antenna at the BS increases. We also have pointed out that the secrecy performance of the proposed scheme becomes more vulnerable when the eavesdropper located closer to BS.

Acknowledgments

The work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2016R1D1A1B03934898) and by the Leading Human Resource Training Program of Regional Neo industry Through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future planning (Grant No. 2016H1D5A1910577).

References

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C. L. I, and H. V. Poor, "Application of non-orthogonal multiple access in lte and 5g networks," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, February 2017.

[2] N. T. Do, D. B. D. Costa, T. Q. Duong, and B. An, "A BNBF user selection scheme for NOMA-based cooperative relaying systems with SWIPT," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 664–667, March 2017.

[3] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, March 2017.

[4] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[5] Y. Feng, Z. Yang, and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in fd relay networks," in *2017 IEEE Globecom Workshops (GC Wkshps)*, December 2017, pp. 1–6.

[6] H. Lei, J. Zhang, K. H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17 450–17 464, August 2017.

[7] 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 Transactions on Communications*, vol. PP, no. 99, pp. 1–1, 2018.

[8] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, Dresden, Germany, June 2013, pp. 1–5.

[9] K. Shim, T. N. Do, and B. An, "Performance analysis of physical layer security of opportunistic scheduling in multiuser multirelay cooperative networks," *Sensors*, vol. 17, no. 2, 2017.

[10] N. T. Do, D. B. da Costa, T. Q. Duong, V. N. Q. Bao, and B. An, "Exploiting direct links in multiuser multirelay SWIPT cooperative networks with opportunistic scheduling," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5410–5427, August 2017.

[11] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

[12] N. T. Do and B. An, "Secure transmission using decode-and-forward protocol for underlay cognitive radio networks," in *2015 Seventh International Conference on Ubiquitous and Future Networks*, Sapporo, Japan, July 2015, pp. 914–918.

[13] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products (7th edition)*. Academic Press is an imprint of Elsevier, 2007.

[14] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Courier Corporation, 1964.