Physical Layer Security for Keyhole-based NOMA Downlink Systems with a Multi-antenna Eavesdropper

Sang-Quang Nguyen[1] and Chi-Bao Le[2]

[1]*Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam,*
[2]*Transcosmos Vietnam, Ho Chi Minh City, Vietnam*

https://doi.org/10.26636/jtit.2025.3.2116

Abstract — This paper investigates the physical layer security of downlink nonorthogonal multiple access (NOMA) systems operating over a degenerate keyhole channel in the presence of a multi-antenna eavesdropper. We propose a joint antenna selection framework with transmit antenna selection at the source and receive antenna selection at both legitimate users and eavesdroppers, thus striving to reduce hardware complexity while maximizing secrecy performance. In this framework, the efficacy of confidentiality is assessed for a specific user allocation methodology by deriving the closed-form approximate expression of secrecy outage probability (SOP). Extensive Monte Carlo simulations validate analytical results and reveal that increasing the number of antennas at the source and legitimate users dramatically lowers SOP, whereas a more capable eavesdropper raises the risk of secrecy. Our findings demonstrate that strategic antenna deployment and non-orthogonal access can effectively safeguard communications even through severely scattering environments.

Keywords — keyhole, multi-antenna, NOMA, physical layer security, secrecy outage probability

1. Introduction

Wireless systems are based on spatial diversity to boost capacity and reliability through utilization of multi-antenna techniques. In richly scattered environments, multiple transmit and receive antennas allow high spectral efficiency by creating uncorrelated transmission paths [1], [2]. However, when propagation is restricted, such as through a hallway, tunnel or narrow aperture, the so-called keyhole effect occurs and collapses the channel rank to one, degrading the benefits of using MIMO and reducing link capacity to SISO level [3]–[6].

Meanwhile, physical layer security (PLS) has emerged as a promising low-complexity approach allowing to protect wireless communications against eavesdropping, exploiting the randomness of fading channels to achieve secrecy without upper layer encryption [7], [8]. The authors of [9]–[11] studied PLS in keyhole-aided MIMO and cascaded fading scenarios. They also derived secrecy capacity and outage metrics under various relay and scheduling schemes. As a rule, these studies assume that orthogonal multiple access is relied upon and often neglect the impact of multiantenna eavesdroppers. By superimposing users signals with different power levels and employing successive interference cancelation (SIC), non-orthogonal multiple access (NOMA) can dramatically increase spectral efficiency and user connectivity in 5G and beyond networks [12], [13]. However, the security of NOMA under degenerate keyhole channels remains largely unexplored, especially when legitimate receivers and adversaries employ antenna selection to reduce hardware cost.

To address this gap, we investigate a downlink NOMA system where a multi-antenna source communicates through a single keyhole with two users and a multi-antenna eavesdropper. By combining transmit antenna selection (TAS) at the source with receive antenna selection (RAS) at the users and the eavesdropper, we derive tractable expressions for secrecy-outage probability (SOP) of both near and far users. To handle the resulting multidimensional integrals, we develop a Gauss-Chebyshev quadrature that converts them into finite sums with a negligible loss of accuracy.

The main contributions of this work are as follows:

1) We propose a method with joint TAS at the source and RAS at both legitimate users and the eavesdropper, balancing hardware simplicity against secrecy performance.
2) Using the Gauss-Chebyshev quadrature, we obtain the closed-form approximate expression of SOP expressions for both near and far NOMA users under a keyhole channel.
3) We benchmark the proposed NOMA design against a conventional orthogonal multiple access (OMA) baseline, demonstrating that NOMA superposition coding and SIC decoding yield substantially lower SOP for both users under identical antenna and power allocation settings.
4) Through extensive Monte Carlo simulations, we show how the number of antennas at the source, users, and the eavesdropper, as well as the keyhole's scattering cross section and the NOMA power split, interact to shape the SOP, offering practical guidelines for low complexity and secure deployments.

The remainder of this paper is organized as follows. Section 2 describes the system and channel models. Section 3 presents the secrecy-outage analysis and the quadrature approximation. Section 4 states the numerical results. Finally, Section 5 concludes the article.

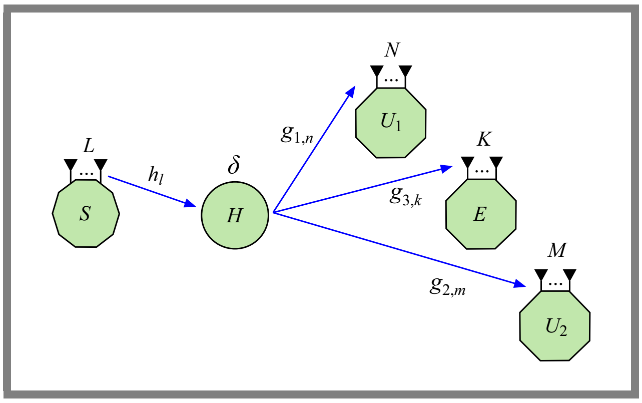

Fig. 1. Model of a keyhole-based NOMA system for downlink with a multi-antenna eavesdropper.

2. System Model

Consider a downlink NOMA communication system consisting of a source node S equipped with L antennas, a keyhole H with scattering cross-section δ, two legitimate users U_1 and U_2, and a potential eavesdropper E, as shown in Fig. 1.

Communication takes place through a keyhole with a scattering cross-section δ, separating the regions containing the users and the source. This keyhole models a propagation environment with limited scattering, such as a narrow passage or tunnel through which all signals must pass. Specifically, source S transmits information to users U_1 (near user) and U_2 (far user) via keyhole H.

Due to severe shadowing and scattering effects, direct transmission paths between the source and the users, as well as between S and E, are neglected. Therefore, all communications occur through the keyhole link.

User U_1 is equipped with N antennas, user U_2 with M antennas, and E with K antennas. Channels from H to U_1, U_2 and E are denoted by $g_{1,n}$, $g_{2,m}$, and $g_{3,k}$, respectively, while the channel from S to H is denoted by h_l. All wireless links in the network are assumed to be independent, non-selective block Rayleigh fading.

Furthermore, following common assumptions made in the literature, it is considered that the eavesdropper has complete knowledge of the relay transmission protocol and the user decoding strategies, enabling a worst-case security analysis.

The probability density function (PDF) and the cumulative distribution function (CDF) associated with random variables Z that follow an exponential distribution characterized by parameter Ω_Z can be written, respectively, as:

$$f_Z(x) = \Omega_Z^{-1} e^{-\frac{x}{\Omega_A}} , \tag{1}$$

$$F_Z(x) = 1 - e^{-\frac{x}{\Omega_A}} . \tag{2}$$

Following the NOMA principle, source S simultaneously transmits messages to both users U_1 and U_2 over the same time frequency resource by superimposing their signals with different power levels.

Specifically, the transmitted signal consists of a linear combination of two unit-power signals x_1 and x_2, U_1 and U_2, respectively. The resulting superimposed signal sent from the source can be expressed as [14]:

$$x = \sqrt{a_1}\, x_1 + \sqrt{a_2}\, x_2 , \tag{3}$$

where a_1 and a_2 are the power allocation coefficients such that $a_1 + a_2 = 1$, and typically $a_1 < a_2$ to ensure that the far user U_2 (with weaker channel conditions) receives a stronger signal.

We employ the antenna selection (AS) technique on both the transmitter and receiver sides, including the eavesdropper, to reduce system complexity while preserving its performance. At source S, which is equipped with L antennas, transmit antenna selection (TAS) is applied to choose the antenna with the strongest channel to the keyhole. Specifically, the selected transmit antenna index is given by:

$$l^* = \arg \max_{l \in \{1,\ldots,L\}} |h_l|^2 , \tag{4}$$

where h_l denotes the channel coefficient between the l-th antenna and the keyhole.

Similarly, both users and E apply the receive antenna selection technique. For user U_i, $i \in \{1,2\}$, the antenna with the strongest gain is selected as:

$$n^* = \arg \max_{n \in \{1,\ldots,N\}} |g_{1,n}|^2 , \tag{5}$$

$$m^* = \arg \max_{m \in \{1,\ldots,M\}} |g_{2,m}|^2 . \tag{6}$$

Similarly, the eavesdropper, equipped with K antennas, selects the best antenna via:

$$k^* = \arg \max_{k \in \{1,\ldots,K\}} |g_{3,k}|^2 . \tag{7}$$

The effective signal received at user U_i, $i \in \{1,2\}$ through the keyhole with antenna selection applied at both ends is given by:

$$\begin{aligned} y_1 &= \delta\, h_{l^*} g_{1,n^*} \sqrt{P_S}\, x + n_1 \\ &= \delta\, h_{l^*} g_{1,n^*} \sqrt{P_S} \left(\sqrt{a_1}\, x_1 + \sqrt{a_2}\, x_2\right) + n_1 \end{aligned} , \tag{8}$$

$$\begin{aligned} y_2 &= \delta\, h_{l^*} g_{2,m^*} \sqrt{P_S}\, x + n_2 \\ &= \delta\, h_{l^*} g_{2,m^*} \sqrt{P_S} \left(\sqrt{a_1}\, x_1 + \sqrt{a_2}\, x_2\right) + n_2 \end{aligned} , \tag{9}$$

where P_S is the total transmit power at S, x_1 and x_2 are the normalized NOMA signal with unit average power, i.e.

$$\mathbb{E}\left\{|x_1|^2\right\} = \mathbb{E}\left\{|x_2|^2\right\} = 1 ,$$

$$n_i \sim \mathcal{CN}\left(0, \sigma_i^2\right)$$

is the additive white Gaussian noise at user i in which $\mathbb{E}\{.\}$ denotes the expectation operation and $\mathcal{CN}(., .)$ denotes the complex Gaussian distribution.

Similarly, the signal received at E is:

$$y_e = \delta\, h_{l^*} g_{3,k^*} \sqrt{P_S} \left(\sqrt{a_1}\, x_1 + \sqrt{a_2}\, x_2\right) + n_e . \tag{10}$$

where $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ is the noise at E.

In this case, the instantaneous signal-to-interference-plus-noise ratio (SINR) at U_1 to detect x_2 for the keyhole link is given by:

$$\begin{aligned}\gamma_{1,x_2} &= \frac{\delta^2 P_S\, a_2\, |h_{l^*}|^2\, |g_{1,n^*}|^2}{\delta^2 P_S\, a_1\, |h_{l^*}|^2\, |g_{1,n^*}|^2 + \sigma_1^2} \\ &= \frac{\delta^2 \rho_S\, a_2\, |h_{l^*}|^2\, |g_{1,n^*}|^2}{\delta^2 \rho_S\, a_1\, |h_{l^*}|^2\, |g_{1,n^*}|^2 + 1} \ ,\end{aligned} \tag{11}$$

where $\rho_S = P_S/\sigma_i^2$ is the transmit signal-to-noise radio (SNR).

Suppose that U_1 can correctly cancel x_2, then, by performing SIC at U_1 to cancel signal x_2, the received SNR at U_1 to detect x_1 can be expressed by:

$$\gamma_{1,x_1} = \delta^2 \rho_S\, a_1 |h_{l^*}|^2\, |g_{1,n^*}|^2 + 1 \ . \tag{12}$$

Similarly, SIC is required at U_2 to eliminate signal x_1, and SINR at U_2 can be computed to consider decoding x_2 as:

$$\gamma_{2,x_2} = \frac{\delta^2 \rho_S\, a_2\, |h_{l^*}|^2\, |g_{2,m^*}|^2}{\delta^2 \rho_S\, a_1\, |h_{l^*}|^2\, |g_{2,m^*}|^2 + 1} \ . \tag{13}$$

It is worth noting that SNR at E can be achieved by employing SIC as [15]:

$$\gamma_{E,x_2} = \delta^2\, a_2\, \rho_E\, |h_{l^*}|^2\, |g_{3,k^*}|^2 \ , \tag{14}$$

$$\gamma_{E,x_1} = \delta^2\, a_1\, \rho_E\, |h_{l^*}|^2\, |g_{3,k^*}|^2 \ , \tag{15}$$

where $\rho_E = P_S/\sigma_e^2$.

The normalized capacity per Hertz of bandwidth for both the user channel and the eavesdropper channel can be formulated as follows:

$$\mathcal{C}_{U_1}^{NOMA} = \log_2\left(1 + \gamma_{1,x_1}\right) \ , \tag{16}$$

$$\mathcal{C}_{U_2}^{NOMA} = \log_2\left(1 + \gamma_{2,x_2}\right) \ , \tag{17}$$

$$\mathcal{C}_{E,x_1}^{NOMA} = \log_2\left(1 + \gamma_{E,x_1}\right) \ , \tag{18}$$

$$\mathcal{C}_{E,x_2}^{NOMA} = \log_2\left(1 + \gamma_{E,x_2}\right) \ . \tag{19}$$

The secrecy capacity of keyhole-based NOMA systems for individual users U_i, $(i = 1, 2)$ can be defined as:

$$\mathcal{C}_i^{NOMA} = \left[\mathcal{C}_{U_i}^{NOMA} - \mathcal{C}_{E,x_i}^{NOMA}\right]^+ \ , \tag{20}$$

where $[x]^+ = \max\{x, 0\}$.

Utilizing the order statistics, the CDF of $|h_{l^*}|^2$, $|g_{1,n^*}|^2$, $|g_{2,m^*}|^2$ and $|g_{3,k^*}|^2$ can be written as:

$$F_{|h_{l^*}|^2}(x) = 1 + \sum_{l=1}^{L} \binom{L}{l} (-1)^l\, e^{-\frac{lx}{\Omega_{h_l}}} \ , \tag{21}$$

$$F_{|g_{1,n^*}|^2}(x) = 1 + \sum_{n=1}^{N} \binom{N}{n} (-1)^n\, e^{-\frac{nx}{\Omega_{g_1}}} \ , \tag{22}$$

$$F_{|g_{2,m^*}|^2}(x) = 1 + \sum_{m=1}^{M} \binom{M}{m} (-1)^m\, e^{-\frac{mx}{\Omega_{g_2}}} \ , \tag{23}$$

$$F_{|g_{3,k^*}|^2}(x) = 1 + \sum_{k=1}^{K} \binom{K}{k} (-1)^k\, e^{-\frac{kx}{\Omega_{g_3}}} \ . \tag{24}$$

Differentiation Eqs. (21)–(24) yield the appropriate PDF as:

$$f_{|h_{l^*}|^2}(x) = \sum_{l=1}^{L} \binom{L}{l} \frac{l(-1)^{l+1}}{\Omega_{h_l}}\, e^{-\frac{lx}{\Omega_{h_l}}} \ , \tag{25}$$

$$f_{|g_{1,n^*}|^2}(x) = \sum_{n=1}^{N} \binom{N}{n} \frac{n(-1)^{n+1}}{\Omega_{g_1}}\, e^{-\frac{nx}{\Omega_{g_1}}} \ , \tag{26}$$

$$f_{|g_{2,m^*}|^2}(x) = \sum_{m=1}^{M} \binom{M}{m} \frac{m(-1)^{m+1}}{\Omega_{g_2}}\, e^{-\frac{mx}{\Omega_{g_2}}} \ , \tag{27}$$

$$f_{|g_{3,k^*}|^2}(x) = \sum_{k=1}^{K} \binom{K}{k} \frac{k(-1)^{k+1}}{\Omega_{g_3}}\, e^{-\frac{kx}{\Omega_{g_3}}} \ . \tag{28}$$

To demonstrate the dependability of such a system, we assess confidentiality performance based on SOP metrics. In the following sections, we derive the analytical formulations for the probabilities associated with SOP.

3. Secure Outage Probability

3.1. Probability of U_2

A secrecy outage occurs whenever the instantaneous secrecy rate of the far user U_2 falls below its target rate R_2. Equivalently, denoting $\theta_2 = 2^{R_2}$, we have:

$$\begin{aligned}\mathcal{S}_{U_2} &= \Pr\left(\mathcal{C}_2^{NOMA} < R_2\right) \\ &= \Pr\left(\log_2 \frac{1 + \gamma_{2,x_2}}{1 + \gamma_{E,x_2}} < R_2\right) \ .\end{aligned} \tag{29}$$

Substituting SINR expressions from Eqs. (13) and (14) yields the following:

$$\mathcal{S}_{U_2} = \Pr\left(\frac{\delta^2\, a_2\, \rho_S\, Z\, X}{\delta^2\, a_1\, \rho_S\, Z\, X + 1} < \theta_2\, \delta^2\, a_2\, \rho_E\, Z\, Y + \varsigma_2\right) \ , \tag{30}$$

where

$$X = |g_{2,m^*}|^2, \ \ Y = |g_{3,k^*}|^2, \ \ Z = |h_{l^*}|^2,$$

and

$$\varsigma_2 = \theta_2 - 1.$$

3.2. Integral Form Expression

By defining:

$$\mathcal{G}(z, y) = \frac{\theta_2\, \delta^2\, a_2\, \rho_E\, z\, y + \varsigma_2}{\delta^2\, \rho_S\, z\left[a_2 - a_1\left(\theta_2\, \delta^2\, a_2\, \rho_E\, z\, y + \varsigma_2\right)\right]} \ , \tag{31}$$

one shows by means of standard order statistics arguments that one must confront Eqs. (23) and (24) – that:

$$\begin{aligned}\mathcal{S}_{U_2} = &\sum_{m=1}^{M} \sum_{k=1}^{K} \sum_{l=1}^{L} (-1)^{m+k+l} \binom{M}{m} \binom{K}{k} \binom{L}{l} \\ &\times \int_0^\infty \int_0^\infty e^{-\frac{ky}{\Omega_{g_3}}}\, e^{-\frac{lz}{\Omega_h}}\, F_X\big(\mathcal{G}(z, y)\big) dz\, dy,\end{aligned} \tag{32}$$

where:

$$F_X(x) = 1 + \sum_{j=1}^{M} (-1)^j \begin{pmatrix} M \\ j \end{pmatrix} e^{-\frac{jx}{\Omega_{g2}}} . \tag{33}$$

3.3. Gaussian-Chebyshev Quadrature Approximation

Each inner integral

$$\mathcal{I}_{k,l} = \int_0^\infty \int_0^\infty e^{-\frac{ky}{\Omega_{g3}}} e^{-\frac{lz}{\Omega_h}} F_X\big(\mathcal{G}(z,y)\big)\, dz\, dy$$

is over $[0, \infty)$.

We map y, z to $[-1, 1]$ via:

$$y = \frac{\Omega_{g3}(1+t)}{k(1-t)}, \; z = \frac{\Omega_h(1+u)}{l(1-u)}, \\ t, u \in [-1, 1] \;, \tag{34}$$

so that

$$dy = \frac{2(\Omega_{g3}/k)}{(1-t)^2} dt \;, \; dy = \frac{2(\Omega_h/l)}{(1-t)^2} du \;, \tag{35}$$

and

$$e^{-ky/\Omega_{g3}} = e^{-\frac{1+t}{1-t}}, \\ e^{-lz/\Omega_h} = e^{-\frac{1+u}{1-u}} .$$

Hence

$$\mathcal{I}_{k,l} = \int_{-1}^{1} \int_{-1}^{1} \mathcal{H}_{k,l}(t,u)\, dt\, du \;, \tag{36}$$

in which

$$\mathcal{H}_{k,l}(t,u) = \\ = 4F_X\left[\mathcal{G}\big(z(u), y(t)\big)\right] \frac{\Omega_{g3}\,\Omega_h\, e^{-\frac{1+t}{1-t}} e^{-\frac{1+u}{1-u}}}{k\,l\,(1-t)^2(1-u)^2}, \tag{37}$$

Applying a Gauss-Chebyshev quadrature of the second kind [16], we have:

$$t_q = \cos\left(\frac{2q-1}{2Q}\pi\right), \quad \omega'_q = \frac{\pi}{Q}\sqrt{1-t_q^2} , \\ q = 1, \ldots, Q \tag{38}$$

and similarly $\{u_r, {\omega'}_r\}$. The double integral is approximated by the following formula:

$$\mathcal{I}_{k,l} \approx \sum_{q=1}^{Q}\sum_{r=1}^{Q} {\omega'}_q\, {\omega'}_r\, \mathcal{H}_{k,l}(t_q, u_r) \;, \tag{39}$$

where Q is a trade-off parameter between complexity and accuracy.

Putting everything together, the approximate closed-form expression of SOP for U_2 is given by:

$$\mathcal{S}_{U_2} \approx \sum_{m=1}^{M}\sum_{k=1}^{K}\sum_{l=1}^{L} (-1)^{m+k+l} \begin{pmatrix} M \\ m \end{pmatrix} \begin{pmatrix} K \\ k \end{pmatrix} \begin{pmatrix} L \\ l \end{pmatrix} \\ \times \sum_{q=1}^{Q}\sum_{r=1}^{Q} {\omega'}_q\, {\omega'}_r\, \mathcal{H}_{k,l}(t_q, u_r) . \tag{40}$$

3.4. Secure Outage Probability of U_1

By direct analogy with the far-user case, one may formulate expressions for the near-user:

$$\mathcal{S}_{U_1} = \Pr\left(\mathcal{C}_1^{NOMA} < R_1\right) = \Pr\left(\frac{1+\gamma_{1,x_1}}{1+\gamma_{E,x_1}} < \theta_1\right) \\ = \sum_{n=1}^{N}\sum_{k=1}^{K}\sum_{l=1}^{L} (-1)^{n+k+l} \begin{pmatrix} N \\ n \end{pmatrix} \begin{pmatrix} K \\ k \end{pmatrix} \begin{pmatrix} L \\ l \end{pmatrix} , \\ \times \int_0^\infty \int_0^\infty e^{-\frac{ky}{\Omega_{g3}}} e^{-\frac{lz}{\Omega_h}} F_{X_1}(\Lambda(z,y))\, dz\, dy \tag{41}$$

where $\theta_1 = 2^{R_1}$ and:

$$\Lambda(z,y) = \frac{\theta_1\, \delta^2\, a_1\, \rho_E\, z\, y + \varsigma_1}{\delta^2\, a_1\, \rho_S\, z}, \tag{42}$$

$$F_{X_1}(x) = 1 + \sum_{j=1}^{N} (-1)^j \begin{pmatrix} N \\ j \end{pmatrix} e^{-\frac{jx}{\Omega_{g1}}} . \tag{43}$$

In the above equations, $\varsigma_1 = \theta_1 - 1$.

We directly apply the Gauss-Chebyshev quadrature to avoid a separate derivation, as in Subsection 3.3, and define the same change of variables by:

$$y = \frac{\Omega_{g3}(1+t)}{k(1-t)}, \quad z = \frac{\Omega_h(1+u)}{l(1-u)}, \\ t, u \in [-1, 1] , \tag{44}$$

and set

$$\mathcal{V}_{k,l}(t,u) = \\ = 4F_{X_1}\left[\Lambda\big(z(u), y(t)\big)\right] \frac{\Omega_{g3}\,\Omega_h\, e^{-\frac{1+t}{1-t}} e^{-\frac{1+u}{1-u}}}{k\,l(1-t)^2(1-u)^2} . \tag{45}$$

Using Q Chebyshev-II nodes $\{t_q, {\omega'}_q\}$ and $\{u_r, {\omega'}_r\}$, the double integral is approximated by the following:

$$\int_{-1}^{1} \int_{-1}^{1} \mathcal{V}_{k,l}(t,u)\, dt\, du \approx \sum_{q=1}^{Q}\sum_{r=1}^{Q} {\omega'}_q\, {\omega'}_r\, \mathcal{V}_{k,l}(t_q, u_r) \;. \tag{46}$$

Submitting Eq. (46) into Eq. (41), the approximate closed-form expression of SOP for U_1 is given as:

$$\mathcal{S}_{U_1} \approx \sum_{n=1}^{N}\sum_{k=1}^{K}\sum_{l=1}^{L} (-1)^{n+k+l} \begin{pmatrix} N \\ n \end{pmatrix} \begin{pmatrix} K \\ k \end{pmatrix} \begin{pmatrix} L \\ l \end{pmatrix} \\ \times \sum_{q=1}^{Q}\sum_{r=1}^{Q} {\omega'}_q\, {\omega'}_r\, \mathcal{V}_{k,l}(t_q, u_r) . \tag{47}$$

4. Numerical Results

In this section, we numerically evaluate our theoretical results concerning SOP performance. We now validate analytical formulas via Monte Carlo simulations with 10^7 independent trials and illustrate how key system parameters shape the secrecy-outage performance.

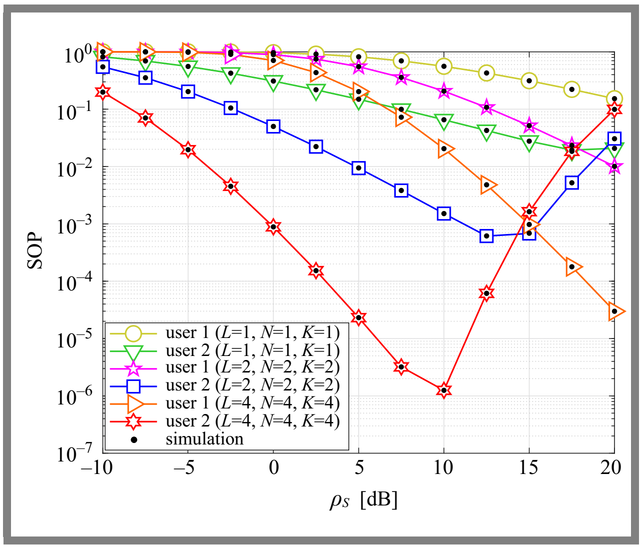

Fig. 2. SOP versus ρ_S for different L, N, M, and K values.

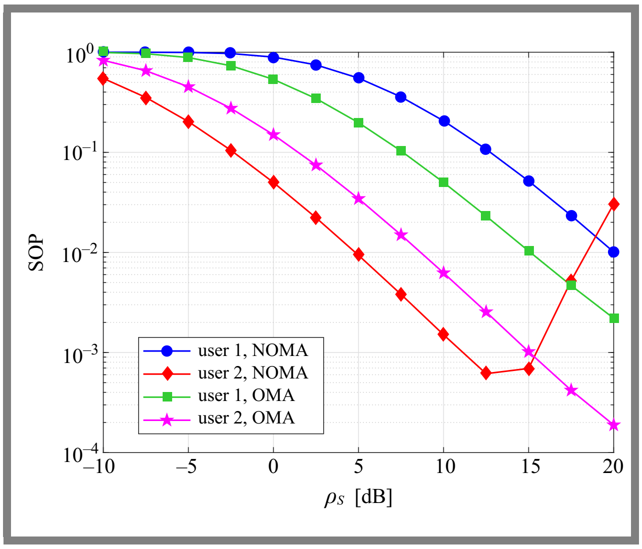

Fig. 3. Comparison between NOMA and OMA for SOP versus ρ_S with $L = N = M = K = 2$.

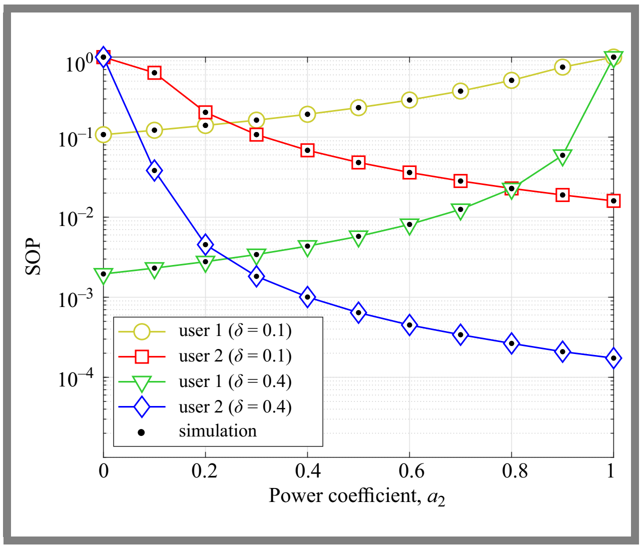

Fig. 4. SOP versus power coefficient a_2 with $L = N = M = K = 2$, $R_1 = R_2 = 0.1$ and $\rho_S = 5$ dB.

Unless otherwise noted, we set the power split $a_2 = 0.9$, $a_1 = 0.1$, target rates $R_1 = R_2 = 1$ bits per channel use (bpcu), scattering cross-section $\delta = 0.5$, and mean link gains $\Omega_h = 3$ dB, $\Omega_{g_1} = 6$ dB, $\Omega_{g_2} = 12$ dB, $\Omega_{g_3} = -20$ dB. For the Gauss-Chebyshev quadrature, we use $Q = 100$ nodes [17], which we found offers a near-perfect match to the simulation.

In Fig. 2, SOP is plotted against ρ_S in decibels for the different combinations of $L \in \{1, 2, 3\}$, $N \in \{1, 2, 3\}$, $M \in \{1, 2, 3\}$ and $K \in \{1, 2, 3\}$. As the number of source antennas L increases, both U_1 and U_2 experience a considerable reduction in SOP, showing better keyhole link diversity due to TAS.

Similarly, equipping the near-user with more antennas N achieves significant SOP gains through enhanced receive-side selection. The performance of far user M also rises noticeably with more antennas, though less steeply than for U_1, which manifests the NOMA power-split trade-off.

On the contrary, more antennas for eavesdropper K shift the SOP curves upward, which represents a more powerful adversary. All SOP curves drop off sharply in the low-to-mid-SNR range before saturating at some non-zero floor in the high-SNR regime. The nearer user U_1 always outperforms U_2 in the high SNR regime, as anticipated with SIC. Overall, Fig. 2 emphasizes that careful placement of antennas at legitimate nodes can greatly boost secrecy, even in the scenario in which a degenerate keyhole channel is exploited.

Figure 3 compares SOP performance of NOMA and OMA under identical antenna settings $L = N = M = K = 2$. As one may see, NOMA (blue and red curves) consistently outperforms OMA (pink and green curves) throughout the entire SNR range. For a given transmit power, the far user in NOMA achieves a lower SOP than its OMA counterpart, thanks to the superposition coding and SIC gains.

In the low-SNR regime ($\rho_S < 5$ dB), both access schemes suffer high outages, but the early slope is noticeably steeper in NOMA, indicating a faster improvement in secrecy as the power increases. Beyond the 10 dB level, NOMA's SOP declines to its asymptotic floor, whereas OMA lags by approximately one order of magnitude in outage. This gap persists even at high SNR, highlighting the enduring benefit of non-orthogonal resource sharing under keyhole fading.

The near-user under NOMA further narrows the outage gap compared to the near-user curve, illustrating how power allocation favors the weaker link. Overall, Fig. 3 confirms that, when operating through a degenerate keyhole channel, NOMA not only boosts spectral efficiency, but also enhances physical-layer security relative to traditional OMA designs.

Figure 4 illustrates the impact of the NOMA power allocation coefficient a_2 on the SOP for both users when $L = N = M = K = 2$, $R_1 = R_2 = 0.1$ bpcu, and $\rho_S = 5$ dB. As a_2 increases from 0.1 to 0.9, the probability of outage of the far user initially decreases sharply, reflecting the stronger average power allocated to its signal, before flattening as a_2 approaches unity.

The simulation markers and Gauss-Chebyshev analytical curves once again overlap almost exactly, confirming the

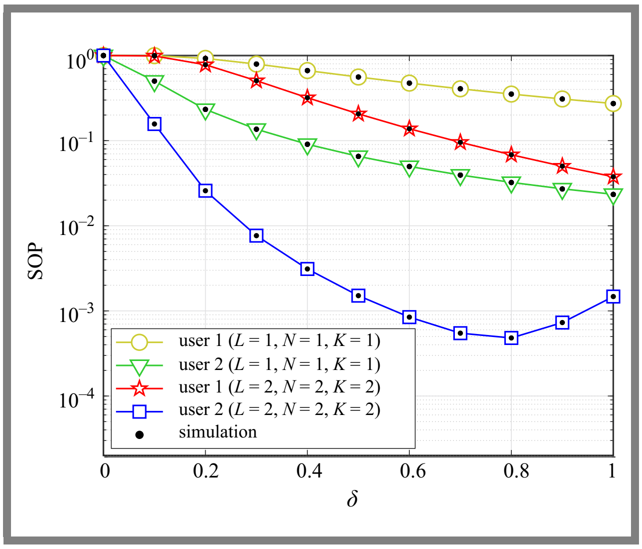

Fig. 5. SOP versus keyhole parameter δ, with $\rho_S = 10$ dB.

robustness of our approximation. Meanwhile, near-user U_1 exhibits a U-shaped SOP trend: too little power for U_2 (small a_2) forces U_1 to suffer large interference, while excessive a_2 starves U_1 of transmit power, also raising its outage.

Overall, Fig. 4 highlights that careful tuning of the NOMA power split can yield substantial secrecy gains in keyhole channels and that our quadrature-based analysis captures this behavior with a high degree of fidelity.

Finally, Fig. 5 examines how keyhole scattering cross-section δ influences SOP at a fixed SNR level of 10 dB with $L = N = M = K = 2$. As δ grows from 0.1 to 1.0, both U_1 and U_2 see their SOP curves drop steeply, reflecting the alleviation of multipath blockage through a "wider" keyhole. In particular, far user U_2 benefits more dramatically from increases in δ, while U_1 enjoys lower overall SOP due to its SIC advantage. Beyond $\delta \approx 0.7$, SOP reduction levels off, approaching the asymptotic floor predicted by the high-SNR analysis. This plateau confirms that additional scattering offers diminishing secrecy gains once the keyhole ceases to be a severe bottleneck. Meanwhile, SOP mirrors the legitimate curves in reverse, improving as δ shrinks and worsening as it expands. Overall, Fig. 4 highlights that enhancing the effective aperture of the keyhole is a potent lever for bolstering physical layer security in NOMA systems.

5. Conclusions

We have presented a comprehensive study of keyhole-based NOMA downlink systems operating under the threat of a multi-antenna eavesdropper. By combining transmit and receive antenna selection with NOMA power splitting, we derived the closed-form approximate expression of SOP for both far and near users.

The proposed Gauss-Chebyshev quadrature method delivers fast and accurate approximations of these expressions, circumventing burdensome infinite integrals. Numerical results confirm that increases in source, near-user, or far-user antenna counts yield steep reductions in SOP, while a stronger eavesdropper degrades secrecy.

Additionally, the keyhole scattering cross-section and the NOMA power allocation balance play pivotal roles in determining outage floors. Overall, this work shows that even in highly constrained propagation scenarios, carefully designed antenna selections and non-orthogonal resource sharing are capable of significantly strengthening physical-layer security, paving the way for robust, low-complexity, secure communications in future IoT and 6G networks.

References

[1] A. Lozano and A.M. Tulino, "Capacity of Multiple-transmit Multiple-receive Antenna Architectures", *IEEE Transactions on Information Theory*, vol. 48, pp. 3117–3128, 2002 (https://doi.org/10.1109/TIT.2002.805084).

[2] W. Gao, X. Lu, C. Han, and Z. Chen, "On Multiple-antenna Techniques for Physical-layer Range Security in the Terahertz Band", *arXiv*, 2022 (https://doi.org/10.48550/arXiv.2201.06253).

[3] D. Chizhik, G.J. Foschini, M.J. Gans, and R.A. Valenzuela, "Keyholes, Correlations, and Capacities of Multielement Transmit and Receive Antennas", *IEEE Transactions on Wireless Communications*, vol. 1, pp. 361–368, 2002 (https://doi.org/10.1109/7693.994830).

[4] D. Chizhik, G.J. Foschini, and R.A. Valenzuela, "Capacities of Multielement Transmit and Receive Antennas: Correlations and Keyholes", *Electronics Letters*, vol. 36, pp. 1099–1100, 2000 (https://doi.org/10.1049/el:20000828).

[5] D. Gesbert, H. Bolcskei, D.A. Gore, and A.J. Paulraj, "Outdoor MIMO Wireless Channels: Models and Performance Prediction", *IEEE Transactions on Communications*, vol. 50, pp. 1926–1934, 2002 (https://doi.org/10.1109/TCOMM.2002.806555).

[6] S. Loyka and A. Kouki, "On MIMO Channel Capacity, Correlations, and Keyholes: Analysis of Degenerate Channels", *IEEE Transactions on Communications*, vol. 50, pp. 1886–1888, 2002 (https://doi.org/10.1109/TCOMM.2002.806543).

[7] H. Rahbari and M. Krunz, "Secrecy Beyond Encryption: Obfuscating Transmission Signatures in Wireless Communications", *IEEE Communications Magazine*, vol. 53, pp. 54–60, 2015 (https://doi.org/10.1109/MCOM.2015.7355566).

[8] M. Mitev, A. Chorti, H.V. Poor and G.P. Fettweis, "What Physical Layer Security Can Do for 6G Security", *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2023 (https://doi.org/10.1109/OJVT.2023.3245071).

[9] P. Almers, F. Tufvensson, and A.F. Molisch, "Keyhole Effect in MIMO Wireless Channels: Measurements and Theory", *IEEE Transactions on Wireless Communications*, vol. 5, pp. 359–3604, 2006 (https://doi.org/10.1109/TWC.2006.256982).

[10] H. Zhang *et al.*, "Performance Analysis of MIMO-HARQ Assisted V2V Communications with Keyhole Effect", *IEEE Transactions on Communications*, vol. 70, pp. 3034–3046, 2022 (https://doi.org/10.1109/TCOMM.2022.3163779).

[11] X. Zang, H. Xu, C. Ouyang, and H. Yang, "PHY Security in MIMOME Keyhole Channels", *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Beijing, China, 2023 (https://doi.org/10.1109/BMSB58369.2023.10211340).

[12] S.Q. Nguyen *et al.*, "Performance Evaluation of Downlink Multiple Users NOMA-able UAV-aided Communication Systems over Nakagami-m Fading Environments", *IEEE Access*, vol. 9, pp. 151641–151653, 2021 (https://doi.org/10.1109/ACCESS.2021.3124017).

[13] B.V. Minh *et al.*, "Performance Prediction in UAV-terrestrial Networks with Hardware Noise", *IEEE Access*, vol. 11, pp. 117562–117575, 2023 (https://doi.org/10.1109/ACCESS.2023.3325478).

[14] C.B. Le *et al.*, “Joint Design of Improved Spectrum and Energy Efficiency with Backscatter NOMA for IoT”, *IEEE Access*, vol. 10, pp. 7504–7519, 2021 (https://doi.org/10.1109/ACCESS.2021.3139118).

[15] J. Chen, L. Yang, and M.-S. Alouini, “Physical Layer Security for Cooperative NOMA Systems”, *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 4645–4649, 2018 (https://doi.org/10.1109/TVT.2017.2789223).

[16] M. Abramowitz and I.A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, New York, USA: Dover, 1072 p., 1972 (ISBN: 9780486612720).

[17] Y. Cheng *et al.*, “Downlink and Uplink Intelligent Reflecting Surface Aided Networks: NOMA and OMA”, *IEEE Transactions on Wireless Communications*, vol. 20, pp. 3988–4000, 2021 (https://doi.org/10.1109/TWC.2021.3054841).

Sang-Quang Nguyen, Ph.D.
https://orcid.org/0000-0002-1798-2296
E-mail: sangnq@ptit.edu.vn
Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam
https://english.ptit.edu.vn

Chi-Bao Le, Student
https://orcid.org/0000-0002-3175-5698
E-mail: lechibao0411@gmail.com
Transcosmos Vietnam, Ho Chi Minh City, Vietnam
https://www.trans-cosmos.com.vn