

RESEARCH

Open Access



On secrecy outage probability for downlink NOMA systems with relay–antenna selection

Shu Xu¹, Chen Liu^{1*} , Hong Wang¹, Mujun Qian¹ and Wenfeng Sun^{1,2}

*Correspondence:
liuch@njupt.edu.cn

¹ National and Local Joint Engineering Laboratory of RF Integration and Micro-Assembly Technology, Nanjing University of Posts and Telecommunications, No.9 Wenyuan Road, Qixia District, Nanjing 210003, People's Republic of China

² School of Science and Information, Qingdao Agricultural University, Qingdao 266109, People's Republic of China

Abstract

Secure transmission is essential for future non-orthogonal multiple access (NOMA) system. This paper investigates relay–antenna selection to enhance physical-layer security of cooperative NOMA system in the presence of an eavesdropper, where multiple antennas are deployed at the relays, the users, and the eavesdropper. In order to reduce expense on radio frequency chains, selection combining (SC) is employed at both the relays and the users, whilst the eavesdropper employs either maximal-ratio combining or SC to process the received signals. Under the condition that the channel state information of the eavesdropping channel is available or unavailable, two effective relay–antenna selection schemes are proposed. Additionally, the closed-form expressions of secrecy outage probability (SOP) are derived for the proposed relay–antenna selection schemes. In order to gain more deep insights on the derived results, the asymptotic performance of the derived SOP is analyzed. In simulations, it is demonstrated that the theoretical results match well with the simulation results and the SOP of the proposed schemes is less than that of the conventional orthogonal multiple access scheme obviously.

Keywords: Wireless communication, Non-orthogonal multiple access, Relay–antenna selection, Physical-layer security, Secrecy outage probability

1 Introduction

Compared with 5G, 6G has the advantages of wider wireless coverage, faster transmission speed, and more intelligence, which has attracted substantial attention from academic community [1–3]. Non-orthogonal multiple access (NOMA) has been recognized as a promising technique for 6G communication networks, due to its benefits of enhancing spectrum efficiency and accommodating massive connectivity [4–6]. NOMA mainly includes two categories: code-domain NOMA and power-domain NOMA. Code domain NOMA allows controllable interference at the destinations on the same time-frequency resources by leveraging different but partially overlapping codes [7]. Differently, power-domain NOMA separates the user messages by leveraging different received power levels. In this paper, we focus on power-domain NOMA, in which multiple user signals are superposed linearly by well-designed weights at the transmitter to share the same time/frequency/code resource. In order to distinguish multiple desired signals, successive interference cancellation (SIC) is employed at the receiver [8]. More

specifically, the SIC performed in NOMA systems enables the users with better channel conditions to decode not only their own information but also the messages of the users with small channel gains.

Recently, significant research efforts have been shifted toward the combination of NOMA with cooperative communication due to its superiority in improving system performance. Ding et al. [9] proposed a novel cooperative NOMA transmission scheme, in which users with strong channels act as relays to forward other users' messages by following NOMA principle in the cooperation stage. It was shown that the strength of the signal received by weak users is improved substantially. Compared to pure NOMA method, cooperative NOMA has the capability of yielding a lower outage probability [9]. To further exploit spectral efficiency and space diversity, relay selection scheme in cooperative NOMA systems has been widely investigated, such as [10, 11]. In a decode-and-forward (DF) cooperative NOMA systems, the authors devised a two-stage relay selection algorithm and derived closed-form expressions of outage probability in [10]. It was shown that the two-stage relay selection scheme is capable of achieving the maximal diversity order and the minimal outage probability. Yu et al. [11] derived the expressions of system throughput for cooperative NOMA network with relay selection. It was verified that system throughput of cooperative NOMA with relay selection outperforms those of the conventional orthogonal multiple access (OMA) and the non-cooperative NOMA. Furthermore, the authors in [12] studied energy efficiency and outage probability of cooperative NOMA in both full-duplex and half-duplex relay assisted heterogeneous networks. In addition, the authors proposed a two-stage relay selection strategy for NOMA networks based on user-specific quality of services (QoS) in [13], where the closed-form expressions of outage probabilities were derived with the DF and amplify-and-forward (AF) relaying protocols, respectively.

Moreover, in [14], an antenna selection (AS) problem was considered for multiple-input multiple-output (MIMO) NOMA systems, in which two efficient AS algorithms were developed, i.e., NOMA with fixed power allocation (F-NOMA) and NOMA with cognitive radio-inspired power allocation (CR-NOMA). Furthermore, the asymptotic closed-form expressions of average sum-rate were derived. The authors investigated a multi-antenna two-way relay assisted NOMA system in [15], in which two cooperative strategies, namely multiple-access broadcast NOMA and time division broadcast NOMA, were proposed. For each of the two cooperative strategies, a joint antenna-and-relay selection scheme was devised to enhance the transmission reliability. Besides, the closed-form expressions of both outage probability and diversity order were derived to evaluate the system performance. However, if eavesdropping nodes are within the coverage of the relays, there may have a chance to wiretap legitimate users' messages. Thus, physical layer security (PLS) is an important issue in cooperative NOMA systems [16, 17], but it was not considered in the above literature.

Currently, the relay selection schemes for improving PLS in cooperative NOMA system have been investigated in some prior works, e.g., [18–20]. In [18], a relay selection method was proposed to minimize the secrecy outage probability for cooperative NOMA system with multiple DF relays, in which the transmission rate of the source should be adjusted according to the channel gains in two hops. Moreover, considering two users with different QoS requirements, three relay selection schemes with fixed

power allocation and dynamic power allocation were studied in [19] aiming at enhancing secrecy outage probability. Furthermore, the authors in [20] proposed a two-stage relay selection scheme and derived the outage probability in DF cooperative NOMA system. However, the impact of multiple relays and multiple antennas was not analyzed for cooperative NOMA networks.

In this paper, we intend to study the PLS of a cooperative NOMA system with multiple relays and multiple antennas. To the best of our knowledge, the secrecy performance of cooperative NOMA systems with joint relay and antenna selection has not been reported by the existing works. Motivated by these observations, we will focus on deriving the secrecy outage probabilities (SOP) of cooperative NOMA networks with AF relays (DF relays will be investigated in future) and the optimal antenna selection strategy in the presence of a multi-antenna eavesdropper, in which both selection combining (SC) and maximum ratio combining (MRC) are taken into account. The contributions of this work can be summarized as follows:

First, an analytical framework of a multi-AF relay multi-antenna NOMA system with joint relay and antenna selection is developed. Besides, the impacts of various eavesdropping scenarios are modelled and investigated thoroughly. Specifically, in the considered model, four transmission scenarios are included, i.e., SC adopted at the eavesdropper with/without the channel state information (CSI) of the eavesdropper links, MRC employed at the eavesdropper with/without the CSI of the eavesdropper links.

Second, in order to improve secrecy performance in a cost-effective way, a two-stage joint relay and antenna selection scheme is proposed. The benefit of the proposed scheme is that diversity gains stemming from both relay selection and antenna selection can be achieved. Based on the statistics of the channel gains, the SOPs are derived in closed-forms for the proposed relay–antenna selection scheme in four different circumstances. To gain more useful insights on the derived results, the secrecy diversity orders of the proposed scheme are derived.

The rest of this paper is organized as follows. In Section II, the secure cooperative NOMA system model and relay–antenna selection scheme are presented. The closed-form of SOP for AF-based cooperative NOMA in four eavesdropping scenarios are derived in Section III. In Section IV, the asymptotic SOPs for AF-based cooperative NOMA in four eavesdropping scenarios are derived. Moreover, in Section V, we derive the secrecy diversity order for different eavesdropping environments. Numerical results are presented in Section VI to reveal valuable insights on the secrecy performance of the proposed schemes. Finally, this paper is concluded in Section VII.

The aim of this paper is to analyze the secrecy performance of NOMA based on multi-relay and multi-antenna assistance, specifically, analyzing the secrecy outage probability and secrecy diversity order of this system. For multi-relay and multi-antenna systems, we propose an optimal single relay and single antenna selection scheme, which minimizes the secrecy outage probability. The main link adopts SC mode to save radio frequency (RF) chains. The eavesdropping link adopts SC or MRC in order to compare the two receiving merging methods. Brief introduction to the design idea: When the CSI of the eavesdropping link is known; Firstly, a relay is specified and an antenna set is selected from the antennas equipped with the relay. The antennas in the antenna set meet the requirements of transmitting signals with this antenna, so that the cell-edge user can

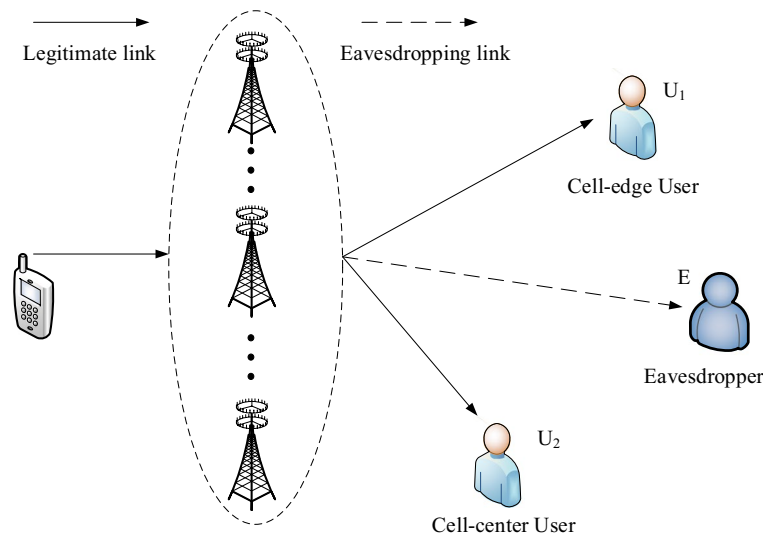


Fig. 1 System model. A illustration of system architecture of cooperative NOMA system with a single source and multiple AF relays

safely decode his own signal. Secondly, in the antenna set mentioned above, the antenna that enables the cell-center user to obtain the maximum secure decoding rate (decoding rate minus eavesdropping rate) is selected as the best antenna for this relay. Thirdly, in all the remaining relays, adopt similar steps to find the best antenna corresponding to the relay. Finally, the maximum rate obtained by the cell-center user from all relays and all antennas is found. Accordingly, the corresponding relay and antenna is the best single relay and single antenna in the system. When the CSI of the eavesdropping link is not known; The process of optimal relay antenna is similar to the above, with some differences: First, specify a relay and select an antenna set from the antennas equipped with the relay. Among them, the antennas in the antenna set meet the requirements of transmitting signals with this antenna, so that the cell-edge user can decode his own signal. Secondly, in the antenna set mentioned above, the antenna that enables the cell-center user to obtain the maximum decoding rate is selected as the best antenna for this relay; Thirdly, in all the remaining relays, adopt similar steps to find the best antenna corresponding to the relay; Finally, the maximum rate obtained by the cell-center user from all relays and antennas is found. At this time, the corresponding relay and antenna is the best single relay and single antenna in the system.

2 System model and relay–antenna selection

2.1 System model

2.1.1 Network description

Consider a downlink secure cooperative NOMA system including a single source S , N AF relays¹ $\{R_1, \dots, R_N\}$, two legitimate users, i.e., the cell-edge user U_1 and the cell-center user U_2 , and an eavesdropper E , as shown in Fig. 1. The relays operate in half-duplex

¹ AF relay is widely used because AF has advantages in power consumption compared with DF relay, which is the reason why AF is adopted in this paper.

mode. It is assumed that there is no direct link between the source and the legitimate users due to long propagation distance and severe obstacle blocking. We also assume that the eavesdropper is located in the vicinity of the users but far from the source. In such case, the eavesdropper can only overhear the messages coming from the relays. The source is equipped with a single antenna². The numbers of antennas equipped at each relay, the user U_i and the eavesdropper are M , L_i and K , respectively. Let $h_{SR_{n,m}}$ and $h_{R_{n,m}U_i}$ denote the channel from the source to the m -th antenna of the n -th relay ($S \rightarrow R_{n,m}$) and from the m -th antenna of the n -th relay to the user U_i ($R_{n,m} \rightarrow U_i$), respectively. It is assumed that both $h_{SR_{n,m}}$ and $h_{R_{n,m}U_i}$ are available at the legitimate nodes [21]. Besides, let $h_{R_{n,m}E_k}$ denote the channel coefficient between the m -th antenna of the n -th relay and the k -th antenna of the eavesdropper, i.e., $R_{n,m} \rightarrow E_k$. We assume that all the CSI is perfect³. All the channels in the system follow the block Rayleigh fading, in which the channel coefficients remain unchanged within one block, but vary independently from one block to another, i.e., $h_{SR_{n,m}} \sim \mathcal{CN}(0, \Omega_{SR_{n,m}})$, $h_{R_{n,m}U_i} \sim \mathcal{CN}(0, \Omega_{R_{n,m}U_i})$, and $h_{R_{n,m}E_k} \sim \mathcal{CN}(0, \Omega_{R_{n,m}E_k})$.

In the considered model, the data transmission is divided into two phases. In the first phase, the source S broadcasts the superposed signal, $\sqrt{P_S}x$, to the relays, where P_S denotes the transmit power of the source S , the transmit data $x = \sqrt{\alpha}s_1 + \sqrt{(1-\alpha)}s_2$, s_1 and s_2 are the signals for U_1 and U_2 with unit power, respectively. The power allocation coefficient of s_1 is α with $0.5 < \alpha < 1$, and the rest transmit power is allocated to the signal s_2 [9]. It is known that the power allocation coefficients affect the relay-source selection scheme in cooperative NOMA system. In order to facilitate the development of the relay-source selection scheme, the power allocation coefficients at the source are chosen to maximize the secrecy capacity of an arbitrary source-relay-users link. Therefore, the received signal at the m -th antenna of the relay R_n is given by

$$y_{R_{n,m}} = h_{SR_{n,m}}\sqrt{P_S}x + n_{R_{n,m}}, \tag{1}$$

where $n_{R_{n,m}} \sim \mathcal{CN}(0, \sigma_{R_{n,m}}^2)$ represents the additive white Gaussian noise (AWGN) at $R_{n,m}$ with zero mean and variance $\sigma_{R_{n,m}}^2$.

In the second phase, the selected relay transmits the received signal to the users U_1 and U_2 following the NOMA principle. More details about the transmission in the second phase will be presented in the remaining of this section. Hereafter, the AF protocol is considered at the relays.

2.1.2 Secrecy capacity

In order to reduce the cost of circuit caused by expensive RF chains, the antenna selection technique is used at the relays and the users. In the considered model, only one antenna is

² This paper provides an performance analysis for the model that the signal source (S) is equipped with a single antenna. In fact, the source is equipped with a single antenna in NOMA networks is an active research topic of the existing works. The design scheme proposed in this work can be extended to the multiple-antenna and beamforming scenario with multiple relays straightforwardly. In addition, the multiple relays can also be used in a cooperative way, which can effectively improve the security performance. However, this will increase the computational complexity of the system. In this article, the focus of our consideration is to save the radio frequency (RF) chains and reduce the computational complexity, which is also the focus of many existing works.

³ It is quite difficult to achieve the perfect CSI of the nodes (legitimate users and eavesdropper) in practice. Thus, it is interesting to investigate SOP for the case with imperfect CSI. However, it also brings a big challenge to analyze the security performance of the system. In future, we will study the more general case with the imperfect CSI.

selected for reception or transmission at each relay. It is worth mentioning that the selected receiving antenna and transmission antenna may be different because the channel conditions in two hops are independent. Suppose the relay R_n employing the m -th antenna amplifies and forwards its received signals to the two legitimate users in the second phase. In order to satisfy the power budget at the selected relay in the AF mode, the power amplification factor is expressed as $G_{n,m} = \sqrt{\frac{P_{R_n}}{|h_{SR_{n,m}}|^2 P_S + \sigma_{R_{n,m}}^2}}$, where P_{R_n} is the transmit power of the relay R_n . As a result, the received signals at $U_i, i \in (1, 2)$, and the eavesdropper E are respectively given by

$$y_{U_i}^{n,m} = h_{R_{n,m}U_i} G_{n,m} y_{R_{n,m}} + n_{U_i}, \tag{2}$$

$$y_E^{n,m} = h_{R_{n,m}E} G_{n,m} y_{R_{n,m}} + n_E, \tag{3}$$

where $n_{U_i} \sim \mathcal{CN}(0, \sigma_{U_i}^2)$ and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ are the AWGNs at the user U_i and the eavesdropper E , respectively. For mathematical tractability, we assume that $P_S = P_{R_n} = P, \sigma_{R_n}^2 = \sigma_{U_i}^2 = \sigma_E^2 = \sigma_0^2$ in the following. According to the decoding order in the NOMA system, the cell-edge user's signal s_1 is first decoded at both the user U_i and the eavesdropper E . When decoding signal s_1 , the signal s_2 is treated as the interference. Then, the received signal-to-interference-plus-noise ratio (SINR) of s_1 at U_i and E can be respectively expressed as

$$\gamma_{U_i \leftarrow s_1}^{n,m} = \frac{\alpha \rho^2 X_{n,m} Y_{U_i,n,m}}{(1 - \alpha) \rho^2 X_{n,m} Y_{U_i,n,m} + \rho X_{n,m} + \rho Y_{U_i,n,m} + 1}, \tag{4}$$

$$\gamma_{E \leftarrow s_1}^{n,m} = \frac{\alpha \rho^2 X_{n,m} Z_{n,m}}{(1 - \alpha) \rho^2 X_{n,m} Z_{n,m} + \rho Z_{n,m} + \rho X_{n,m} + 1}, \tag{5}$$

where $X_{n,m} = |h_{SR_{n,m}}|^2, Y_{U_i,n,m} = |h_{R_{n,m}U_i}|^2, Z_{n,m} = |h_{R_{n,m}E}|^2$, and $\rho = \frac{P}{\sigma^2}$ denotes the transmit signal-to-noise ratio (SNR).

After the signal s_1 is decoded, it is subtracted from the received signal at the user U_2 and the eavesdropper E with the aid of SIC. In such case, the user U_2 and the eavesdropper E detect s_2 without the inter-user interference. Then, the SINR of s_2 at U_2 and E can be, respectively, given by

$$\gamma_{U_2 \leftarrow s_2}^{n,m} = \frac{(1 - \alpha) \rho^2 X_{n,m} Y_{U_2,n,m}}{\rho Y_{U_2,n,m} + \rho X_{n,m} + 1}, \tag{6}$$

$$\gamma_{E \leftarrow s_2}^{n,m} = \frac{(1 - \alpha) \rho^2 X_{n,m} Z_{n,m}}{\rho Z_{n,m} + \rho X_{n,m} + 1}. \tag{7}$$

Based on the SINR derived above, the capacity of the user U_i to decode its own signal s_i is expressed as

$$C_{U_i}^{n,m} = \frac{1}{2} \log_2 \left(1 + \gamma_{U_i \leftarrow s_i}^{n,m} \right). \tag{8}$$

Similarly, the capacity of the cell-center user U_2 to detect s_1 is given by

$$C_{U_2 \leftarrow s_1}^{n,m} = \frac{1}{2} \log_2 \left(1 + \gamma_{U_2 \leftarrow s_1}^{n,m} \right). \tag{9}$$

Besides, the channel capacity of the $R_n \rightarrow E$ link can be expressed as

$$C_{E \leftarrow s_i}^{n,m} = \frac{1}{2} \log_2 \left(1 + \gamma_{E \leftarrow s_i}^{n,m} \right). \tag{10}$$

Accordingly, the secrecy capacities obtained at U_i are respectively given by

$$C_{sec,U_i}^{n,m} = \left[C_{U_i}^{n,m} - C_{E \leftarrow s_i}^{n,m} \right]^+, \tag{11}$$

$$C_{sec,U_2 \leftarrow s_1}^{n,m} = \left[C_{U_2 \leftarrow s_1}^{n,m} - C_{E \leftarrow s_1}^{n,m} \right]^+, \tag{12}$$

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

2.2 Relay-antenna selection schemes

In order to improve system performance in a cost-effective way, the optimal single-relay and single-antenna is selected to assist the data transmission in both the reception and the transmission⁴. The proposed joint relay and antenna selection schemes are respectively presented when the CSI of the eavesdropper is available and unavailable.

2.2.1 Relay-antenna selection scheme with the CSI of the eavesdropper

The optimal relay-antenna selection (ORAS) algorithm is implemented by three steps:

Firstly, for a given relay R_n , the candidate transmit antenna subset $\Phi_{n,m}^{w/}$ ($w/$ means with the CSI of the eavesdropper) is selected, in which the antenna can transmit s_1 to both users successfully, i.e., the secrecy capacity of s_1 is larger than the rate requirement at both users. Thus, $\Phi_{n,m}^{w/}$ can be expressed as

$$\Phi_{n,m}^{w/} = \left\{ m : C_{sec,U_1}^{n,m} \geq R_1^s, C_{sec,U_2 \leftarrow s_1}^{n,m} \geq R_1^s, m \in [1, 2, \dots, M] \right\}, \tag{13}$$

where R_1^s denotes the required secrecy rate of s_1 .

Secondly, from the candidate transmit antenna subset $\Phi_{n,m}^{w/}$, the best transmit antenna is selected to achieve the maximum secrecy rate of s_2 at the cell-center user U_2 . Then, in the subset $\Phi_{n,m}^{w/}$, the index of the best transmit antenna is given by

$$m_{n,*}^{w/} = \operatorname{argmax}_{m \in \Phi_{n,m}^{w/}} \left\{ C_{sec,U_2}^{n,m} \right\}, \tag{14}$$

where R_2^s denotes the required secrecy rate for s_2 .

⁴ When the beamforming scheme is considered, the PDF and CDF for SINR/SNR of received signals should be thoroughly reshaped based on the new statistical distribution properties. Besides, compared to the proposed scheme, the beamforming scheme requires higher hardware requirement and higher computational complexity. However, the full security diversity order can be achieved by our proposed scheme, which is same as that of the beamforming scheme. In future, we will pursue the study of robust design by considering beamforming in multiple-relay and multiple-antenna of NOMA networks.

Finally, the optimal relay is selected to achieve the maximum secrecy rate of U_2 among all the relays. Thus, the index of the optimal relay is obtained by

$$n_*^{w/o} = \operatorname{argmax}_{n \in [1, N]} \left\{ C_{sec, U_2}^{n, m_{n,*}^{w/o}} \right\}. \tag{15}$$

Accordingly, the index of the optimal transmit antenna for the optimal relay $R_{n_*^{w/o}}$ can be obtained by $m_{n,*}^{w/o}$ shown in (14).

2.2.2 Relay–antenna selection scheme without the CSI of the eavesdropper

In this scenario, the achieved SOP is less than that of the case with the CSI. Thus, the optimal relay–antenna selection scheme hereafter. Since the CSI of the eavesdropper is unavailable, the wiretap capacity is not considered in this scheme. The detailed algorithm is described as follows:

Firstly, for a given relay R_n , the candidate transmit antenna subset $\Phi_{n,m}^{w/o}$ (w/o means without the CSI of the eavesdropper) is selected, in which the antenna can transmit the signal s_1 to the both users successfully without considering the CSI of the eavesdropper, i.e., the capacity of s_1 is larger than the rate requirement at both users. Thus, $\Phi_{n,m}^{w/o}$ is expressed as

$$\Phi_{n,m}^{w/o} = \left\{ m : C_{U_1}^{n,m} \geq R_1^{th}, C_{U_2 \leftarrow s_1}^{n,m} \geq R_1^{th}, m \in [1, 2, \dots, M] \right\}, \tag{16}$$

where R_1^{th} denotes the rate requirement of signal s_1 .

Secondly, from the candidate transmit antenna subset $\Phi_{n,m}^{w/o}$, the best transmit antenna is selected to achieve the maximum required rate of s_2 at the cell-center user U_2 . Then, the index of the best transmit antenna is given by

$$m_{n,*}^{w/o} = \operatorname{argmax}_{m \in \Phi_{n,m}^{w/o}} \left\{ C_{U_2}^{n,m} \right\}, \tag{17}$$

where R_2^{th} denotes the rate requirement of signal s_2 .

Finally, the optimal relay is selected to achieve the maximum rate of U_2 among all the relays. Thus, the index of the optimal relay is obtained by

$$n_*^{w/o} = \operatorname{argmax}_{n \in [1, N]} \left\{ C_{U_2}^{n, m_{n,*}^{w/o}} \right\}. \tag{18}$$

Accordingly, the index of the optimal transmit antenna for the optimal relay $R_{n_*^{w/o}}$ can be obtained by $m_{n,*}^{w/o}$ given in (17).

3 Secrecy outage performance analysis

In this section, the SOPs of U_i to detect s_i are respectively derived for the proposed relay–antenna selection schemes. For each relay, each user, and the eavesdropper, two practical signal processing techniques, i.e., SC and MRC, are considered. As such, the proposed relay–antenna selection schemes should be designed in four cases⁵: (1)

⁵ the main links employ SC to save RF chain, and the eavesdropper employ SC or MRC for comparison.

SC-SC w/ CSI: SC at the legitimate nodes (relays and users), and SC at the eavesdropper with the CSI of the eavesdropping channel; (2) SC-MRC w/ CSI: SC at the legitimate nodes, and MRC at the eavesdropper with the CSI of the eavesdropping channel; (3) SC-SC w/o CSI: SC at the legitimate nodes, and SC at the eavesdropper without the CSI of the eavesdropping channel; (4) SC-MRC w/o CSI: SC at the legitimate nodes, and MRC at the eavesdropper without the CSI of the eavesdropping channel.

3.1 The SOP derivation for ORAS w/ CSI

3.1.1 SC at the eavesdropper

In the case of SC at the eavesdropper, each antenna wiretaps the transmission date independently. Hence, the individual secrecy performance is limited by the antenna with the best channel condition. In such case, the probability density function (PDF) of the equivalent eavesdropping channel gain is given by [22]

$$f_Z(z) = \sum_{k=1}^K \binom{K}{k} (-1)^{k+1} \frac{k}{\Omega_Z} e^{-\frac{kz}{\Omega_Z}}, \tag{19}$$

where Z stands for eavesdropping channel gain, Ω_Z represents the reciprocal of the expected gain of the eavesdropping channel.

As a result, the SOP of U_1 can be expressed as

$$P_{U_1,w/}^{SC-SC} = \prod_{n=1}^N \underbrace{\Pr \{ |\Phi_{U_1,w/}| = 0 \}}_{\Psi_{1,w/}^{SC-SC}}, \tag{20}$$

and the SOP of U_2 can be expressed as

$$P_{U_2,w/}^{SC-SC} = \prod_{n=1}^N \left[\underbrace{\Pr (|\Phi_{U_2,w/}| = 0)}_{\Psi_{2,w/}^{SC-SC}} + \sum_{m=1}^M \underbrace{\Pr (|\Phi_{U_2,w/}| = m)}_{\Psi_{3,w/}^{SC-SC}} \right] \times \underbrace{\Pr (C_{sec,U_2} < R_2^s | |\Phi_{U_2,w/}| = m)}_{\Psi_{4,w/}^{SC-SC}}, \tag{21}$$

To further derive the expression of the SOPs in (20) and (21), Lemma 1 is developed in the following.

Lemma 1 *By using the statistics of channel gains, the analytical expressions of $\Psi_{1,w/}^{SC-SC}$, $\Psi_{2,w/}^{SC-SC}$, $\Psi_{3,w/}^{SC-SC}$ and $\Psi_{4,w/}^{SC-SC}$ can be derived as*

$$\begin{cases} \Psi_{i,w/}^{SC-SC} = \prod_{m=1}^M (1 - \Delta_{i,w/}^{SC-SC}), i \in (1, 2), \\ \Psi_{3,w/}^{SC-SC} = \binom{M}{m} (\Delta_{2,w/}^{SC-SC})^m (1 - \Delta_{2,w/}^{SC-SC})^{M-m}, \\ \Psi_{4,w/}^{SC-SC} = (1 - \Delta_{3,w/}^{SC-SC} / \Delta_{2,w/}^{SC-SC})^m, \end{cases} \tag{22}$$

where

$$\begin{cases} \Delta_{1,w/}^{SC-SC} = Q_1 Q_2 J_1 \exp(-W_1), \\ \Delta_{2,w/}^{SC-SC} = Q_1 Q_3 J_1 \exp(-W_2), \\ \Delta_{3,w/}^{SC-SC} = Q_1 Q_3 G_1 O_1 \mu_1^{-1}, \end{cases}$$

and

$$\begin{cases} Q_1 = \sum_{k=1}^K \binom{K}{k} (-1)^{k+1}, \\ Q_2 = \sum_{l_1=1}^{L_1} \binom{L_1}{l_1} (-1)^{l_1+1}, \\ Q_3 = \sum_{l_2=1}^{L_2} \binom{L_2}{l_2} (-1)^{l_2+1}, \\ \mu_1 = \frac{B_1}{\Omega_{SR_{n,m}}} + \frac{l_2 B_1}{\Omega_{R_{n,m} U_2}} + \frac{k}{\Omega_{R_{n,m} E}}, \\ G_1 = \frac{k}{\Omega_{R_{n,m} E}} \exp\left(-\frac{A_1}{\Omega_{SR_{n,m}}} - \frac{l_2 A_1}{\Omega_{R_{n,m} U_2}}\right), \\ W_1 = \frac{kE(t+1)}{2\Omega_{R_{n,m} E}} + \left(\frac{1}{\Omega_{SR_{n,m}}} + \frac{l_1}{\Omega_{R_{n,m} U_1}}\right) F(t), \\ W_2 = \frac{kE(t+1)}{2\Omega_{R_{n,m} E}} + \left(\frac{1}{\Omega_{SR_{n,m}}} + \frac{l_2}{\Omega_{R_{n,m} U_2}}\right) F(t), \\ J_1 = \sum_{l_0=1}^{N_0} \frac{k\pi E \sqrt{1-t^2}}{2N_0 \Omega_{R_{n,m} E}}, O_1 = 1 - \exp(-\mu_1 E), \end{cases}$$

$t = \cos\left(\frac{2l_0-1}{2N_0}\pi\right)$, $A_0 = 2^{2R_1^s} - 1$, $B_0 = \rho(A_0 + \alpha)$, $C_0 = \rho(\alpha + \alpha A_0 - A_0)$, $D_0 = \rho^2 A_0(1 - \alpha)$, $E = \frac{C_0}{D_0}$, $A_1 = \frac{2^{2R_2^s}-1}{\rho(1-\alpha)}$, $B_1 = 2^{2R_2^s}$, $F(t) = \frac{2A_0+B_0E(t+1)}{2C_0-D_0E(t+1)}$, and N_0 denotes the number of terms for the quadrature approximation.

Proof The proof of Lemma 1 is shown in Appendix 1.

By substituting (22) into (20) and (21), we can get the closed-form expressions of the SOPs for $P_{U_1,w/}^{SC-SC}$ and $P_{U_2,w/}^{SC-SC}$. Thus, in the presence of SC at the eavesdropper, the total SOP can be expressed as

$$P_{out,w/}^{SC-SC} = \frac{\left(P_{U_1,w/}^{SC-SC} + P_{U_2,w/}^{SC-SC}\right)}{2}. \tag{23}$$

Accordingly, the SOP for NOMA system with SC at the eavesdropper in ORAS scheme w/ CSI can be approximated as

$$P_{out,w/}^{SC-SC} = \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M \left(1 - \Delta_{1,w/}^{SC-SC}\right) + \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M \left(1 - \Delta_{3,w/}^{SC-SC}\right). \tag{24}$$

3.1.2 MRC at the eavesdropper

In the case of MRC at the eavesdropper, the antenna cooperates with each other to wiretap the transmission date. Hence, the PDF of the equivalent eavesdropping channel gain is given by [22]

$$f_Z(z) = \frac{Z^{K-1}}{\Omega_Z^K (K-1)!} e^{-\frac{z}{\Omega_Z}}. \tag{25}$$

In this scheme, the SOPs of U_1 and U_2 can be gotten by changing the superscript “SC-SC” in (20) and (21) to “SC-MRC”. However, the derivation of each term is different. Similar to Lemma 1, Lemma 2 is given as follows.

Lemma 2 *The analytical expressions of $\Psi_{1,w/}^{SC-MRC}$, $\Psi_{2,w/}^{SC-MRC}$, $\Psi_{3,w/}^{SC-MRC}$ and $\Psi_{4,w/}^{SC-MRC}$ can be expressed as*

$$\begin{cases} \Psi_{i,w/}^{SC-MRC} = \prod_{m=1}^M (1 - \Delta_{i,w/}^{SC-MRC}), i \in (1, 2), \\ \Psi_{3,w/}^{SC-MRC} = \binom{M}{m} (\Delta_{2,w/}^{SC-MRC})^m (1 - \Delta_{2,w/}^{SC-MRC})^{M-m}, \\ \Psi_{4,w/}^{SC-MRC} = (1 - \Delta_{3,w/}^{SC-MRC} / \Delta_{2,w/}^{SC-MRC})^m, \end{cases} \tag{26}$$

where

$$\begin{cases} \Delta_{1,w/}^{SC-MRC} = Q_2 J_2 \exp(-W_3), \\ \Delta_{2,w/}^{SC-MRC} = Q_3 J_2 \exp(-W_4), \\ \Delta_{3,w/}^{SC-MRC} = Q_3 G_2 O_2, \end{cases}$$

and

$$\begin{cases} G_2 = \frac{\exp\left(-\frac{A_1}{\Omega_{SRn,m}} - \frac{l_2 A_1}{\Omega_{Rn,m} U_2}\right)}{(\Omega_{Rn,m} E)^K (K-1)!}, \\ \mu_2 = \frac{B_1}{\Omega_{SRn,m}} + \frac{l_2 B_1}{\Omega_{Rn,m} U_2} + \frac{1}{\Omega_{Rn,m} E}, \\ O_2 = (\mu_2)^{-K} (\Gamma(K) - \Gamma(K, \mu_2 E)), \\ W_3 = \frac{E(t+1)}{2\Omega_{Rn,m} E} + \left(\frac{1}{\Omega_{SRn,m}} + \frac{l_1}{\Omega_{Rn,m} U_1}\right) F(t), \\ W_4 = \frac{E(t+1)}{2\Omega_{Rn,m} E} + \left(\frac{1}{\Omega_{SRn,m}} + \frac{l_2}{\Omega_{Rn,m} U_2}\right) F(t), \\ J_2 = \sum_{l_0=1}^{N_0} \frac{\pi E \sqrt{1-t^2}}{2N_o (\Omega_{Rn,m} E)^K (K-1)!} \left[\frac{E(t+1)}{2}\right]^{K-1}, \end{cases}$$

where $\Gamma(x)$ is the Gamma function, and $\Gamma(x, y)$ is the upper incomplete Gamma function [23].

Similar to that of the “SC-SC” case in the ORAS scheme w/ CSI, the total SOP of the “SC-MRC” case can be computed by (23). The detailed proof is omitted here to avoid redundancy.

By substituting (26) into (20) and (21), the closed-form expression of the SOP with MRC at the eavesdropper can be obtained accordingly. Thus, for the ORAS scheme w/ CSI, the SOP with MRC at the eavesdropper can be approximated as

$$P_{out,w/}^{SC-MRC} = \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M (1 - \Delta_{1,w/}^{SC-MRC}) + \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M (1 - \Delta_{3,w/}^{SC-MRC}). \tag{27}$$

3.2 The SOP derivation for ORAS w/o CSI

3.2.1 SC at the eavesdropper

In this scenario, the SOPs of the users U_1 and U_2 can be expressed as (28) and (29), respectively,

$$P_{U_1,w/o}^{SC-SC} = \underbrace{\Pr(|\Phi_{U_1,sub.}| = (0,0))}_{\Psi_{1,w/o}^{SC-SC}} + \sum_{n=1}^N \underbrace{\Pr(|\Phi_{U_1,w/o}| = (n,m))}_{\Psi_{2,w/o}^{SC-SC}} \times \underbrace{\Pr(C_{sec,U_1 \leftarrow s_1} < R_1^s \mid |\Phi_{U_1,w/o}| = (n,m))}_{\Psi_{3,w/o}^{SC-SC}}, \tag{28}$$

and

$$P_{U_2,w/o}^{SC-SC} = \underbrace{\Pr(|\Phi_{U_2,w/o}| = (0,0))}_{\Psi_{4,w/o}^{SC-SC}} + \sum_{n_+=1}^N \underbrace{\Pr(|\Phi_{U_2,w/o}| = (n_+,m_+))}_{\Psi_{5,w/o}^{SC-SC}} \times \underbrace{\Pr(C_{sec,U_2} < R_2^s \mid |\Phi_{U_2,w/o}| = (n_+,m_+))}_{\Psi_{6,w/o}^{SC-SC}}, \tag{29}$$

To further derive the expressions of the above SOPs, Lemma 3 is developed in the following.

Lemma 3 *The analytical expressions of $\Psi_{1,w/o}^{SC-SC}$, $\Psi_{2,w/o}^{SC-SC}$, $\Psi_{3,w/o}^{SC-SC}$, $\Psi_{4,w/o}^{SC-SC}$, $\Psi_{5,w/o}^{SC-SC}$ and $\Psi_{6,w/o}^{SC-SC}$ can be expressed as*

$$\begin{cases} \Psi_{1,w/o}^{SC-SC} = \prod_{m=1}^M \prod_{n=1}^N (1 - \Delta_{1,w/o}^{SC-SC}), \\ \Psi_{2,w/o}^{SC-SC} = \beta_1 (\Delta_{1,w/o}^{SC-SC})^{\zeta_1} (1 - \Delta_{1,w/o}^{SC-SC})^{MN - \zeta_1}, \\ \Psi_{3,w/o}^{SC-SC} = 1 - \Delta_{2,w/o}^{SC-SC} / (\Delta_{1,w/o}^{SC-SC})^{\zeta_1}, \\ \Psi_{4,w/o}^{SC-SC} = \prod_{m=1}^M \prod_{n=1}^N (1 - \Delta_{3,w/o}^{SC-SC}), \\ \Psi_{5,w/o}^{SC-SC} = \beta_2 (\Delta_{3,w/o}^{SC-SC})^{\zeta_2} (1 - \Delta_{3,w/o}^{SC-SC})^{MN - \zeta_2}, \\ \Psi_{6,w/o}^{SC-SC} = 1 - \Delta_{4,w/o}^{SC-SC} / (\Delta_{3,w/o}^{SC-SC})^{\zeta_2}, \end{cases} \tag{30}$$

where

$$\begin{cases} \Delta_{1,w/o}^{SC-SC} = Q_2 \exp\left(-\frac{C_1}{\Omega_{SR_n,m}} - \frac{l_1 C_1}{\Omega_{R_n,m} U_1}\right), \\ \zeta_1 = m_1 + \dots + m_n, \zeta_2 = m_+^1 + \dots + m_+^{n_+}, \\ \beta_1 = \binom{N}{n} \sum_{m_1=1}^M \dots \sum_{m_n=1}^M \binom{M}{m_1} \dots \binom{M}{m_n}, \\ \Delta_{2,w/o}^{SC-SC} = Q_1 Q_4 G_3 J_1 \exp(-W_5), \\ \Delta_{3,w/o}^{SC-SC} = Q_3 \exp\left(-\frac{D_1}{\Omega_{SR_n,m}} - \frac{l_2 D_1}{\Omega_{R_n,m} U_2}\right), \\ \beta_2 = \binom{N}{n_+} \sum_{m_+^1=1}^M \dots \sum_{m_+^{n_+}=1}^M \binom{M}{m_+^1} \dots \binom{M}{m_+^{n_+}}, \\ \Delta_{4,w/o}^{SC-SC} = Q_1 Q_5 G_4 \mu_3^{-1} k / \Omega_{R_n,m} E, \end{cases}$$

and

$$\left\{ \begin{array}{l} Q_4 = \sum_{j=0}^{\zeta_1} \binom{\zeta_1}{j} (-1)^j (Q_2)^j, \\ Q_5 = \sum_{j=0}^{\zeta_2} \binom{\zeta_2}{j} (-1)^j (Q_3)^j, \\ \mu_3 = \left(\frac{jB_1}{\Omega_{SR_{n,m}}} + \frac{j_2 B_1}{\Omega_{R_{n,m}U_2}} + \frac{k}{\Omega_{R_{n,m}E}} \right), \\ G_3 = \exp \left(-\frac{C_1(\zeta_1-j)}{\Omega_{SR_{n,m}}} - \frac{l_1 C_1(\zeta_1-j)}{\Omega_{R_{n,m}U_1}} \right), \\ C_1 = \frac{2^{2R_1^{th}} - 1}{\rho(1 - (1-\alpha)2^{2R_1^{th}})}, D_1 = \frac{2^{2R_2^{th}} - 1}{(1-\alpha)\rho}, \\ W_5 = \frac{kE(t+1)}{2\Omega_{R_{n,m}E}} + \left(\frac{j}{\Omega_{SR_{n,m}}} + \frac{j_1 l_1}{\Omega_{R_{n,m}U_1}} \right) F(t), \\ G_4 = \exp \left(-\frac{D_1(\zeta_2-ii)+jA_1}{\Omega_{SR_{n,m}}} - \frac{l_2 D_1(\zeta_2-j)+j_2 A_1}{\Omega_{R_{n,m}U_2}} \right). \end{array} \right.$$

Proof The proof of Lemma 3 is shown in Appendix 2.

By substituting (30) into (28) and (29), the closed-form expression of the SOP can be obtained by

$$P_{out,w/o}^{SC-SC} = \frac{1}{2} \left(1 - Q_1 Q_6 G_5 J_1 \exp(-W_6) \right) + \frac{1}{2} \left(1 - Q_1 Q_7 G_6 \mu_4^{-1} k / \Omega_{R_{n,m}E} \right), \quad (31)$$

where

$$\left\{ \begin{array}{l} Q_6 = \sum_{i_o=0}^{MN} \binom{MN}{i_o} (-1)^{i_o} (Q_2)^{i_o}, \\ Q_7 = \sum_{i_{oo}=0}^{MN} \binom{MN}{i_{oo}} (-1)^{i_{oo}} (Q_3)^{i_{oo}}, \\ \mu_4 = \left(\frac{i_{oo} B_1}{\Omega_{SR_{n,m}}} + \frac{i_{oo} l_2 B_1}{\Omega_{R_{n,m}U_2}} + \frac{k}{\Omega_{R_{n,m}E}} \right), \\ G_5 = \exp \left(-\frac{C_1(MN-i_o)}{\Omega_{SR_{n,m}}} - \frac{l_1 C_1(MN-i_o)}{\Omega_{R_{n,m}U_1}} \right), \\ W_6 = \frac{kE(t+1)}{2\Omega_{R_{n,m}E}} + \left(\frac{i_o}{\Omega_{SR_{n,m}}} + \frac{i_o l_1}{\Omega_{R_{n,m}U_1}} \right) F(t), \\ G_6 = \exp \left(-\frac{D_1(MN-i_{oo})+i_{oo} A_1}{\Omega_{SR_{n,m}}} - \frac{l_2 D_1(MN-i_{oo})+i_{oo} l_2 A_1}{\Omega_{R_{n,m}U_2}} \right). \end{array} \right.$$

3.2.2 MRC at the eavesdropper

In this case, the SOPs of U_1, U_2 have the similar forms with (28) and (29). Following Lemma 3, Lemma 4 is given as follows.

Lemma 4 The analytical expressions of $\Psi_{1,w/o}^{SC-MRC}, \Psi_{2,w/o}^{SC-MRC}, \Psi_{3,w/o}^{SC-MRC}, \Psi_{4,w/o}^{SC-MRC}, \Psi_{5,w/o}^{SC-MRC}$ and $\Psi_{6,w/o}^{SC-MRC}$ can be expressed as

$$\begin{cases} \Psi_{1,w/o}^{SC-MRC} = \Psi_{1,w/o}^{SC-SC}, \\ \Psi_{2,w/o}^{SC-MRC} = \Psi_{2,w/o}^{SC-SC}, \\ \Psi_{3,w/o}^{SC-MRC} = 1 - \Delta_{2,w/o}^{SC-MRC} / \left(\Delta_{1,w/o}^{SC-SC} \right)^{\zeta_1}, \\ \Psi_{4,w/o}^{SC-MRC} = \Psi_{4,w/o}^{SC-SC}, \\ \Psi_{5,w/o}^{SC-MRC} = \Psi_{5,w/o}^{SC-SC}, \\ \Psi_{6,w/o}^{SC-MRC} = 1 - \Delta_{4,w/o}^{SC-MRC} / \left(\Delta_{3,w/o}^{SC-SC} \right)^{\zeta_2}, \end{cases} \quad (32)$$

where

$$\begin{cases} \Delta_{2,w/o}^{SC-MRC} = Q_4 G_3 J_2 \exp(-W_7), \\ \Delta_{4,w/o}^{SC-MRC} = Q_5 G_7 (\mu_5)^{-K} \Gamma(K), \end{cases}$$

and

$$\begin{cases} \mu_5 = \frac{jB_1}{\Omega_{SR_{n,m}}} + \frac{jI_2 B_1}{\Omega_{R_{n,m}U_2}} + \frac{1}{\Omega_{R_{n,m}E}}, \\ G_7 = \frac{\exp\left(-\frac{(\zeta_2-j)A_1}{\Omega_{SR_{n,m}}} - \frac{(\zeta_2-j)I_2 A_1}{\Omega_{R_{n,m}U_2}}\right)}{(\Omega_{R_{n,m}E})^K (K-1)!}, \\ W_7 = \frac{E(t+1)}{2\Omega_{R_{n,m}E}} + \left(\frac{j}{\Omega_{SR_{n,m}}} + \frac{jI_1}{\Omega_{R_{n,m}U_1}}\right) F(t). \end{cases}$$

The derivation is similar to that for the “SC-SC” case in the ORAS scheme w/o CSI. The detailed proof is omitted here to avoid redundancy.

By substituting (32) into (28) and (29), the closed-form of the SOP can be expressed as

$$P_{out,w/o}^{SC-MRC} = \frac{1}{2} \left(1 - Q_6 G_5 J_2 \exp(-W_8) \right) + \frac{1}{2} (1 - Q_7 G_6 O_3), \quad (33)$$

where

$$\begin{cases} \mu_6 = \left(\frac{i_{00} B_1}{\Omega_{SR_{n,m}}} + \frac{i_{00} I_2 B_1}{\Omega_{R_{n,m}U_2}} + \frac{1}{\Omega_{R_{n,m}E}} \right), \\ W_8 = \frac{E(t+1)}{2\Omega_{R_{n,m}E}} + \left(\frac{i_0}{\Omega_{SR_{n,m}}} + \frac{i_0 I_1}{\Omega_{R_{n,m}U_1}} \right) F(t), \\ O_3 = (\mu_6)^{-K} \Gamma(K) / \left((\Omega_{R_{n,m}E})^K (K-1)! \right). \end{cases}$$

4 Asymptotic secrecy outage performance analysis for ORAS

The closed-form expressions of the SOPs have been derived for four cases in the last section. However, the expressions are quite complicated. In order to get more useful insights on the derived results, we derive a closed-form expression for the asymptotic SOP in the high transmit power region, where $P_S = P_R \rightarrow \infty$. The asymptotic SOPs are presented in the following four subsections.

4.1 SC at the eavesdropper for ORAS w/ CSI

When $P_S = P_R \rightarrow \infty$, one can easily obtain $\gamma_{U_i \leftarrow s_1} \approx \frac{\alpha}{1-\alpha}$. Recalling (24), the asymptotic SOP of the “SC-SC” case in the ORAS scheme w/ CSI is derived as

$$P_{out,w/\infty}^{SC-SC} = \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M \left(1 - Q_1 Q_2 G_8 \mu_7^{-1}\right) + \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M \left(1 - Q_1 Q_3 G_1 \mu_1^{-1}\right), \quad (34)$$

where

$$\begin{cases} A_2 = \frac{A_0}{C_0}, B_2 = \frac{B_0}{C_0}, \\ \mu_7 = \frac{B_2}{\Omega_{SRn,m}} + \frac{l_1 B_2}{\Omega_{Rn,m} U_1} + \frac{k}{\Omega_{Rn,m} E}, \\ G_8 = \frac{k}{\Omega_{Rn,m} E} \exp\left(-\frac{A_2}{\Omega_{SRn,m}} - \frac{l_1 A_2}{\Omega_{Rn,m} U_1}\right). \end{cases}$$

Remark 1 A factor of $\frac{1}{2}$ is used to determine the rate requirement and the eavesdroppers' channel capacity for the RAS-NOMA schemes. Although, the capacity of the $S - R_i - U_1$ links in the RAS-NOMA scheme is limited by the ratio of the power allocation coefficients (i.e., $\alpha/(1 - \alpha)$), the eavesdroppers' channel capacity is not interference-limited. Therefore, when the transmit power at the source is in the low and medium regimes, the capacity of the $S - R_i - U_1$ links in the RAS-NOMA schemes is larger than that in the RAS-OMA schemes. This indicates that the RAS-NOMA schemes outperform the RAS-OMA schemes when the transmit power is in the low and medium regimes. In addition, when the transmit power is in the high regime, by optimizing the power allocation coefficient, the capacity of the $S - R_i - U_1$ links in the RAS-NOMA schemes is also larger than that in the RAS-OMA schemes.

4.2 MRC at the eavesdropper for ORAS w/ CSI

Referring to the asymptotic expression of the "SC-SC" case in the ORAS scheme w/ CSI, the asymptotic SOP of (27) is expressed as

$$P_{out,w/\infty}^{SC-MRC} = \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M \left(1 - Q_2 G_9 \mu_8^{-K} \Gamma(K)\right) + \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M \left(1 - Q_3 G_2 \mu_2^{-K} \Gamma(K)\right), \quad (35)$$

where

$$\begin{cases} G_9 = \frac{\exp\left(-\frac{A_2}{\Omega_{SRn,m}} - \frac{l_1 A_2}{\Omega_{Rn,m} U_1}\right)}{(\Omega_{Rn,m} E)^K (K-1)!}, \\ \mu_8 = \frac{B_2}{\Omega_{SRn,m}} + \frac{l_1 B_2}{\Omega_{Rn,m} U_1} + \frac{1}{\Omega_{Rn,m} E}. \end{cases}$$

The derivation is similar to that of the "SC-MRC" case in the ORAS scheme w/ CSI. The detailed proof is omitted here to avoid redundancy.

Remark 2 Focusing on the $S - R_i - U_2$ links in the second phase, our proposed schemes always achieve a larger capacity than the RAS-OMA schemes. This is due to the fact that the capacity of the $S - R_i - U_2$ links for the RAS-NOMA schemes is not interference-limited. Due to the use of SIC, a half loss in the capacity of the $S - R_i - U_2$ links

exists for the RAS-OMA schemes. This indicates that the advantage of the RAS-NOMA schemes over the RAS-OMA schemes increases as R_2^{th} increases.

Remark 3 From (34) and (35), it is known that the asymptotic SOPs of the “SC-SC” and the “SC-MRC” cases in the ORAS scheme w/ CSI are constant values. Moreover, the asymptotic SOP of the former case is less than that of the latter.

4.3 SC at the eavesdropper for ORAS w/o CSI

Recalling (31), the asymptotic SOP of the “SC-SC” case in the ORAS scheme w/o CSI is expressed as

$$P_{out,w/o,\infty}^{SC-SC} = \frac{1}{2} \left(1 - Q_1 Q_4 G_{10} \mu_9^{-1} \right) + \frac{1}{2} \left(1 - Q_1 Q_5 G_{11} \mu_3^{-1} \right), \tag{36}$$

where

$$\begin{cases} \mu_9 = \frac{B_2}{\Omega_{SR_{n,m}}} + \frac{l_1 B_2}{\Omega_{R_{n,m}} U_1} + \frac{k}{\Omega_{R_{n,m}} E}, \\ G_{10} = \frac{k}{\Omega_{R_{n,m}} E} \exp \left(-\frac{jA_2}{\Omega_{SR_{n,m}}} - \frac{j l_1 A_2}{\Omega_{R_{n,m}} U_1} \right), \\ G_{11} = \frac{k}{\Omega_{R_{n,m}} E} \exp \left(-\frac{jA_1}{\Omega_{SR_{n,m}}} - \frac{j l_2 A_1}{\Omega_{R_{n,m}} U_2} \right). \end{cases}$$

The derivation is similar to the proof of Lemma 3. The detailed proof is omitted here to avoid redundancy.

4.4 MRC at the eavesdropper for ORAS w/o CSI

Referring to (33), we can obtain the asymptotic SOP of the “SC-MRC” case in the ORAS scheme w/o CSI, which can be expressed as

$$P_{out,w/o,\infty}^{SC-MRC} = \frac{1}{2} \left(1 - Q_4 G_{12} \mu_{10}^{-K} \Gamma(K) \right) + \frac{1}{2} \left(1 - Q_5 G_{13} \mu_4^{-K} \Gamma(K) \right), \tag{37}$$

where

$$\begin{cases} G_{12} = \frac{\exp \left(-\frac{jA_2}{\Omega_{SR_{n,m}}} - \frac{j l_1 A_2}{\Omega_{R_{n,m}} U_1} \right)}{(\Omega_{R_{n,m}} E)^K (K-1)!}, \\ G_{13} = \frac{\exp \left(-\frac{jA_1}{\Omega_{SR_{n,m}}} - \frac{j l_2 A_1}{\Omega_{R_{n,m}} U_2} \right)}{(\Omega_{R_{n,m}} E)^K (K-1)!}, \\ \mu_{10} = \frac{jB_2}{\Omega_{SR_{n,m}}} + \frac{j l_1 B_2}{\Omega_{R_{n,m}} U_1} + \frac{1}{\Omega_{R_{n,m}} E}. \end{cases}$$

The derivation is similar to that for the “SC-MRC” case in the ORAS scheme w/o CSI. The detailed proof is omitted here to avoid redundancy.

Remark 4 Referring to Remark 1 and Remark 2, we can get the asymptotic secrecy outage probability of the RAS-NOMA schemes is prior to that of the RAS-OMA schemes. Moreover, from (36) and (37), it can be obtained that the asymptotic SOPs of the “SC-SC” and the “SC-MRC” cases in the ORAS scheme w/o CSI are constant values. Besides, the constant value of the former is less than that of the latter. In addition, the asymptotic

SOP of the “SC-SC” case in the ORAS scheme w/ CSI is less than that of the “SC-MRC” case in the ORAS scheme w/o CSI.

Remark 5 The complexity of equation (34) is $O(MN)$, since equation (34) is M times N . In the same way, the complexity of equations (35), (36) and (37) can be obtained as $O(MN)$. The detailed proof is omitted here to avoid redundancy.

5 Secrecy diversity order in ORAS

Although the SOP expressions shown in (24), (27), (31), and (33) can be used to evaluate the secrecy performance of the proposed relay–antenna selection schemes, they fail to provide intuitive insights. To gain more deep insights, we further analyze the secrecy diversity order of the proposed schemes. As indicated by [24–26], the secrecy diversity order is achieved when both the transmit power and main-to-eavesdropper ratio (MER) are sufficiently high, i.e., $P_S = P_R \rightarrow \infty$ and $MER = \frac{\Omega_{main}}{\Omega_{RE}} \rightarrow \infty$, where Ω_{main} is related to the average channel gain of the main links, Ω_{RE} is related to the average channel gain of the eavesdropping link. Specifically, we rewrite $\Omega_{RU_1} = MER \cdot \Omega_{RE}$, $\Omega_{SR} = \lambda_1 MER \cdot \Omega_{RE}$ and $\Omega_{RU_2} = \lambda_2 MER \cdot \Omega_{RE}$, where λ_1 and λ_2 are positive constants. Hence, the secrecy diversity order is defined as

$$d_u = - \lim_{MER \rightarrow \infty} \frac{\log P_{out}^\infty}{\log MER}, \tag{38}$$

where $u \in (U_1, U_2)$ and P_{out}^∞ denotes the asymptotic SOP.

5.1 SC at the eavesdropper for ORAS w/ CSI

Recalling (34), we rewrite the asymptotic SOP in this case as

$$P_{out,w/\infty}^{SC-SC} = \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M (1 - Q_1 Q_2 T_1) + \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M (1 - Q_1 Q_3 T_2), \tag{39}$$

where

$$\begin{cases} T_1 = \exp\left(\frac{-\eta_1}{MER}\right) \frac{MER}{MER+v_1}, \\ T_2 = \exp\left(\frac{-\eta_2}{MER}\right) \frac{MER}{MER+v_2}, \\ v_1 = \frac{B_2}{k\lambda_1} + \frac{l_1 B_2}{k}, v_2 = \frac{B_1}{k\lambda_1} + \frac{l_2 B_1}{k\lambda_2}, \\ \eta_1 = \frac{A_2}{\lambda_1 \Omega_{RE}} + \frac{l_1 A_2}{\Omega_{RE}}, \eta_2 = \frac{A_1}{\lambda_1 \Omega_{RE}} + \frac{l_2 A_1}{\lambda_2 \Omega_{RE}}. \end{cases}$$

By substituting (39) into (38) and using $e^{-x} = 1 - x$ for small x , when $MER \rightarrow \infty$, we obtain the secrecy diversity order of the ORAS scheme w/ CSI, which is given by

$$d_{w/}^{SC-SC} = MN \min(L_1, L_2). \tag{40}$$

The derivation is similar to the asymptotic analysis of the “SC-SC” in the ORAS scheme w/ CSI. The detailed proof is omitted here to avoid redundancy.

5.2 MRC at the eavesdropper for ORAS w/ CSI

Recalling (35), the asymptotic SOP, $P_{out,w/\infty}^{SC-MRC}$, is reexpressed as

$$P_{out,w/\infty}^{SC-MRC} = \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M (1 - Q_2 T_3) + \frac{1}{2} \prod_{n=1}^N \prod_{m=1}^M (1 - Q_3 T_4), \tag{41}$$

where

$$\begin{cases} T_3 = \exp\left(\frac{-\eta_1}{MER}\right) \frac{MER}{MER+v_3}, \\ T_4 = \exp\left(\frac{-\eta_2}{MER}\right) \frac{MER}{MER+v_4}, \\ v_3 = \frac{B_2}{\lambda_1} + l_1 B_2, v_4 = \frac{B_1}{\lambda_1} + l_2 B_1. \end{cases}$$

By substituting (41) into (38), the secrecy diversity order for “SC-MRC” in the ORAS scheme w/ CSI can be written as

$$d_{w/}^{SC-MRC} = MN \min(L_1, L_2). \tag{42}$$

The derivation is similar to the asymptotic analysis in the ORAS scheme w/ CSI. The detailed proof is omitted here to avoid redundancy.

5.3 SC at the eavesdropper for ORAS w/o CSI

Recalling (36), the asymptotic SOP, $P_{out,w/o,\infty}^{SC-SC}$, can be rewritten as

$$\begin{aligned} P_{out,w/o,\infty}^{SC-SC} = & \frac{1}{2} \left(1 - Q_1 Q_{14} \exp\left(\frac{-\eta_3}{MER}\right) \frac{MER}{MER+v_5} \right) \\ & + \frac{1}{2} \left(1 - Q_1 Q_{15} \exp\left(\frac{-\eta_4}{MER}\right) \frac{MER}{MER+v_6} \right), \end{aligned} \tag{43}$$

where

$$\begin{cases} Q_{14} = Q_4/Q_2^j, Q_{15} = Q_5/Q_3^j, \\ v_5 = \frac{jB_2}{k\lambda_1} + \frac{j_1 B_2}{k}, v_6 = \frac{jB_1}{k\lambda_1} + \frac{j_2 B_1}{k\lambda_2}, \\ \eta_3 = \frac{jA_2}{\lambda_1 \Omega_{RE}} + \frac{j_1 A_2}{\Omega_{RE}}, \eta_4 = \frac{jA_1}{\lambda_1 \Omega_{RE}} + \frac{j_2 A_1}{\lambda_2 \Omega_{RE}}. \end{cases}$$

By substituting (43) into (38), the secrecy diversity order for this scenario can be obtained as

$$d_{w/o}^{SC-SC} = MN \min(L_1, L_2). \tag{44}$$

The derivation is similar to the asymptotic analysis of the “SC-SC” case in the ORAS scheme w/o CSI. The detailed proof is omitted here to avoid redundancy.

5.4 MRC at the eavesdropper for ORAS w/o CSI

Similar to SC at the eavesdropper for SRAS, by using (37), we rewrite the asymptotic SOP for this scenario as

Table 1 Simulation Parameters

Parameters	Values
Rates $R_1^{\text{th}} = R_1^s$	0.1BPCU
Rates $R_2^{\text{th}} = R_2^s$	1.0BPCU
Gaussian noise power σ_0^2	- 70 dBm
Transmit power $P_S = P_R$	10 dBm
Path loss exponents ϵ	3
The number of relays N	2
The gain of Eavesdropping channel Ω_{RE}	- 50 dBm
The receive antenna number of each relay M	2
The receive antenna number of cell-edge user L_1	2
The receive antenna number of cell-center user L_2	2
The number of antennas at the eavesdropper K	2
The distance between source and relays d_{SR}	100m
The distance between relays and cell-center user d_{RU_2}	100m
The distance between relays and cell-edge user d_{RU_1}	300m
The distance between relays and eavesdropper d_{RE}	500m

$$\begin{aligned}
 P_{out,w/o,\infty}^{SC-MRC} = & \frac{1}{2} \left(1 - Q_6 \exp \left(\frac{-\eta_3}{MER} \right) \frac{MER}{MER + \nu_7} \right) \\
 & + \frac{1}{2} \left(1 - Q_7 \exp \left(\frac{-\eta_4}{MER} \right) \frac{MER}{MER + \nu_8} \right), \tag{45}
 \end{aligned}$$

where $\nu_7 = \frac{jB_2}{\lambda_1} + jl_1B_2$, $\nu_8 = \frac{jB_1}{\lambda_1} + jl_2B_1$.

By substituting (45) into (38), one can easily obtain the secrecy diversity order for this scheme as

$$d_{w/o}^{SC-MRC} = MN \min(L_1, L_2). \tag{46}$$

The derivation is similar to the asymptotic analysis for ‘‘SC-MRC’’ in the ORAS scheme w/o CSI. The detailed proof is omitted here to avoid redundancy.

Remark 6 From (40), (42), (44), and (46), we can get that the secrecy diversity order of ‘‘SC-SC/MRC’’ for the proposed ORAS schemes is equal to $MN \min(L_1, L_2)$. It indicates that the secrecy diversity order can be improved by increasing the number of the relays or the antennas per legitimate node (relays, a pair of NOMA users).

6 Results and discussion

In this section, simulation results are presented to validate the theoretical expressions. The simulation parameters used in this section are presented in Table 1. All the noise powers are set to σ_0^2 , and the transmit power of the source is equal to that of each relay. The simulation results are averaged over 10^6 channel realizations. In the ORAS scheme w/ CSI, the power allocation coefficient α is computed by minimizing (24) for SC at the eavesdropper and by minimizing (27) for MRC at the eavesdropper with $M = 1$ and $N = 1$; in the ORAS scheme w/o CSI, the power allocation

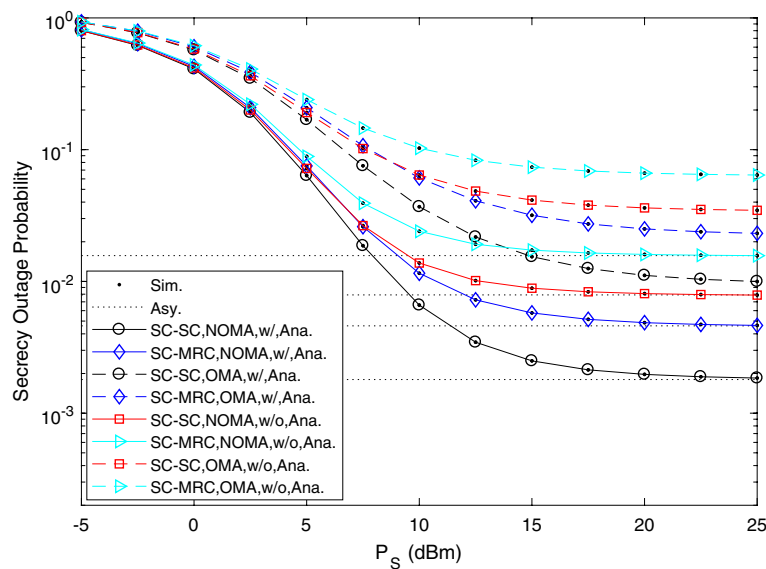


Fig. 2 The theoretical results and simulation results of SOP versus transmit power. The SOP of the four cases for NOMA VS OMA

coefficients α is obtained by minimizing (31) for SC at the eavesdropper and by minimizing (33) for MRC at the eavesdropper with $M = 1$ and $N = 1$.

Figure 2 demonstrates the SOP of relay–antenna selection schemes for cooperative NOMA and conventional OMA systems with SC and MRC at the eavesdropper, respectively. In this figure, it is observed that the analytical results of the SOPs agree with the simulations. It is also shown that the cooperative NOMA system achieves a lower SOP than the OMA system. This is due to the fact that the achievable capacity of cooperative NOMA is larger than that of OMA system. As expected, the secrecy performance of the “SC-SC” case is better than that of the “SC-MRC” case, as discussed in Remark 1 and Remark 2. It is because the wiretapping signals can be enhanced by the joint detection for the MRC scheme at the eavesdropper.

Figure 3 demonstrates the SOP of relay–antenna selection schemes for cooperative NOMA and [20] with SC and MRC at the eavesdropper, respectively. It is also shown that the cooperative NOMA system achieves a lower SOP than [20]. This is due to the fact that the achievable capacity of cooperative NOMA is larger than that of [20]. The power allocation coefficient is optimized to increase the safety rate and obtain a beneficial secrecy outage probability.

Besides, the average SOP of the statistical CSI method in the work [28] and proposed methods are also plotted. Figure 4 depicts the average SOP of cooperative NOMA networks versus under the scenario of imperfect and perfect CSI, where $M = L_1 = L_2 = K = 1$. As seen from the figures, the proposed scheme outperforms the statistical CSI (imperfect CSI) method when the channel estimated error is not small. Clearly, when the channel estimated error is large of the proposed scheme, the achievable secrecy capacity is reduced. Moreover, it is also observed that the two schemes have nearly the same average SOP when the channel estimation error is close to zero.

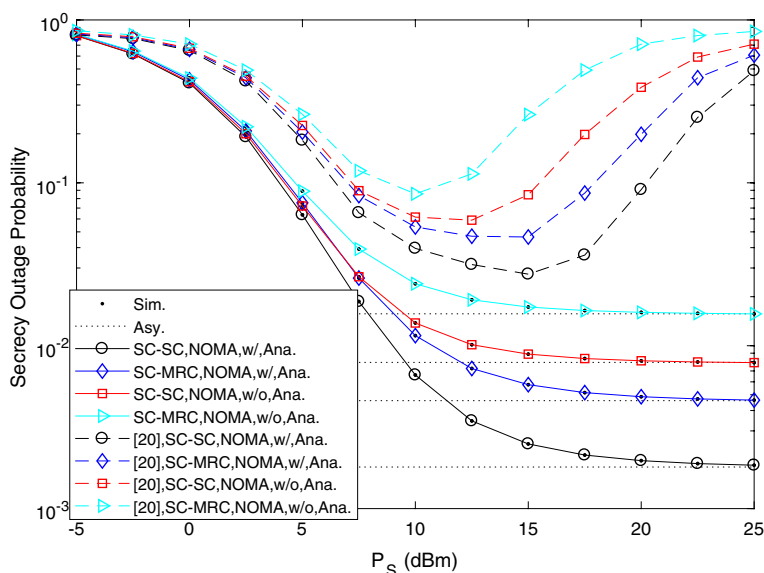


Fig. 3 The theoretical results and simulation results of SOP versus transmit power. The SOP of the four cases for NOMA VS [20]

Figure 5 illustrates the SOP of cooperative NOMA system versus different secrecy rate requirements. From this figure, it can be observed that the SOP of the proposed relay–antenna selection scheme becomes degraded as the secrecy rate increases for both the ORAS scheme w/o and the w/o CSI in cooperative NOMA system. That is because the successful transmission occurs at the case with more stringent channel condition when the requirement of secrecy rate increases. Moreover, the variance of the security rate requirement of the cell-edge user has a greater impact on the SOP than that of the cell-center user. This is due to the fact that a lower security rate requirement of the cell-edge user leads to a higher successful probability of decoding s_1 for the proposed relay–antenna selection schemes.

Figure 6 illustrates the SOP of cooperative NOMA network versus the number of relays. It can be seen in this figure that the SOPs of both the SC and the MRC scenarios at the eavesdropper decrease with the number of relays because the secrecy capacity of cooperative NOMA system is enhanced by transmit diversity gain. Moreover, the ORAS scheme w/ CSI achieves a better secrecy performance than the ORAS scheme w/o CSI. The reason is that the ORAS scheme w/ CSI takes advantage of the CSI of the eavesdropper link over the ORAS scheme w/o CSI. In addition, when the number of relays is large, the decline rate of the SOP becomes slow for the ORAS scheme w/o CSI.

Figure 7(a) examines the SOP of cooperative NOMA system versus the number of antennas at the eavesdropper. The SOP increases with the increasing number of antennas for both ORAS scheme w/ and w/o CSI in cooperative NOMA systems. It is because the capacity of the wiretap link is increased, and thus the secrecy outage probability is increased as a consequence. Moreover, when the number of antennas at the eavesdropper is one, both the SC and the MRC methods at the eavesdropper have the same secrecy outage performance. Figure 7(b) demonstrates the SOP of cooperative NOMA network versus different eavesdropping distances. It is shown that the

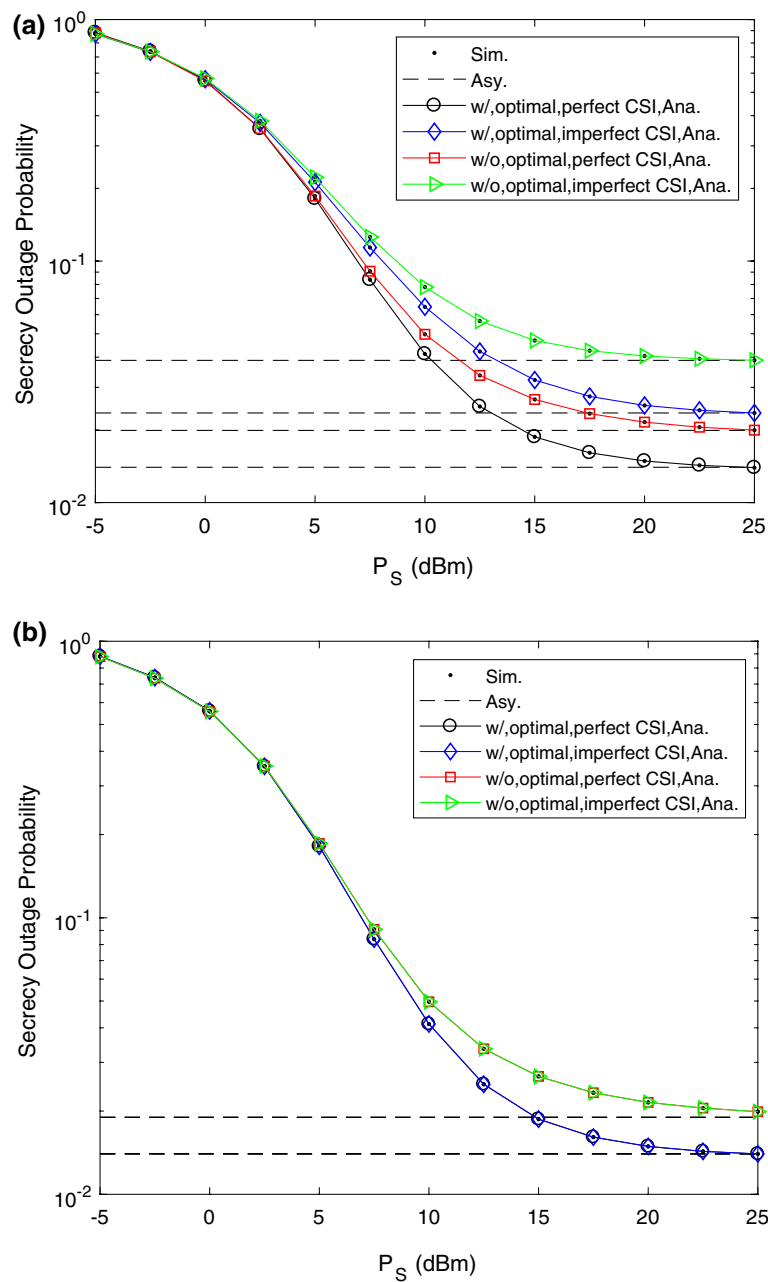


Fig. 4 The theoretical results and simulation results of SOP versus transmit power. (a) The channel estimation error is 0.1; (b) The channel estimation is zero, i.e., perfect CSI. The SOP of the proposed schemes VS [28]

SOPs of both w/ and w/o CSI schemes are decreased when the distance between the relays and the eavesdropper increases. It is obvious that the capacity of the wiretap link is decreased when the propagation distance is increased. It is observed that the closer is the distance between the eavesdropper and the legitimate user, the greater is the system security outage probability. The reason is that as the distance from the

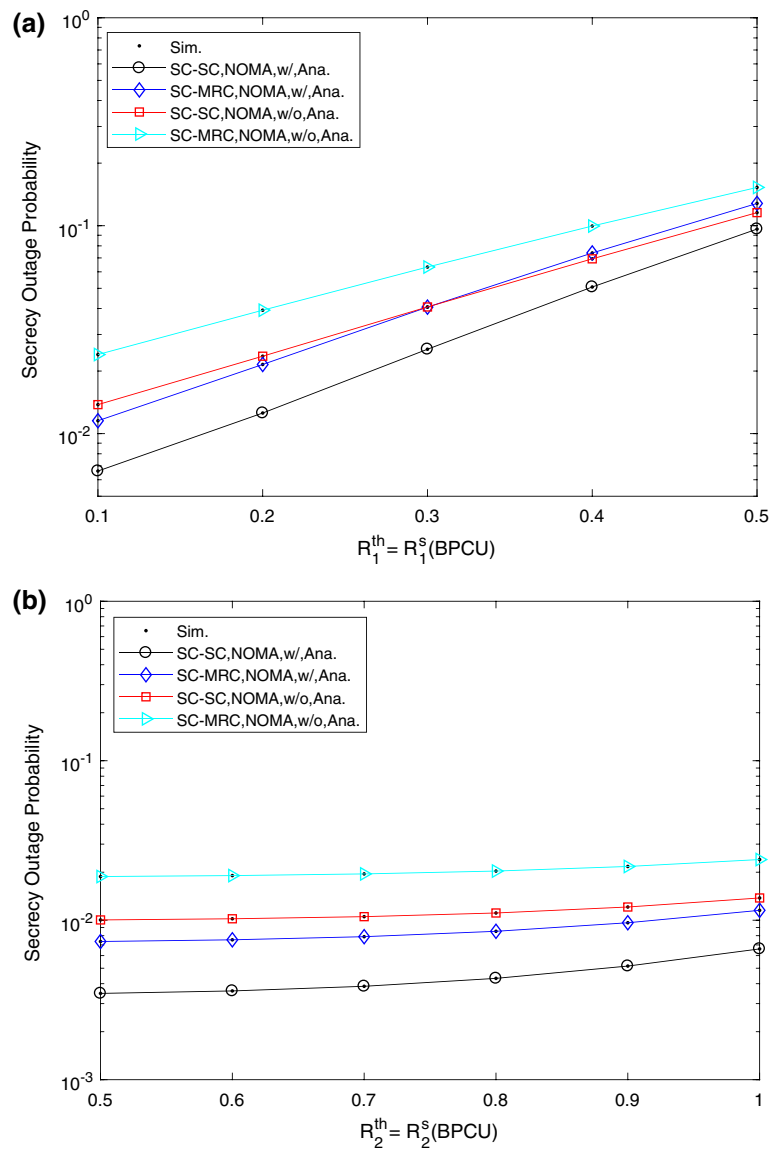


Fig. 5 SOP versus the rate requirement of each user. (a) The rate requirement of cell-edge user; (b) The rate requirement of cell-center user. When the transmission power is constant, the influence of different information transmission rates is on the SOP

legitimate user to the eavesdropper decreases, the capacities achieved by the legitimate user and the eavesdropper are nearly the same.

Figure 8 shows the secrecy outage probability of the proposed scheme versus MER. As seen from this figure, both the ORAS scheme w/ CSI and w/o CSI scheme have a better secrecy performance than the random relay-antenna selection (RRAS) scheme. Interestingly, the secrecy diversity order of the ORAS scheme w/ CSI remains the same as that of the ORAS scheme w/o CSI, when MER is in the medium to high regime, which is consistent with our discussion in Remark 4. Moreover, the

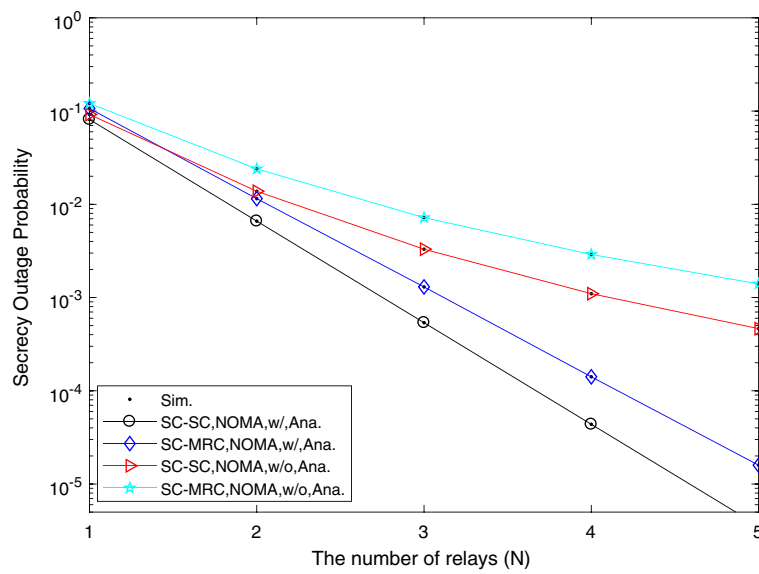


Fig. 6 SOP for the different number of relays. When the transmission power is constant, the influence of different number of relays is on the SOP

secrecy diversity order of the RRAS scheme is one, that is to say, the performance of the RRAS is equivalent to that of single-relay single-antenna scheme.

7 Conclusion

In this paper, we proposed two relay–antenna selection schemes to enhance PLS in cooperative NOMA systems, in which a single source transmitted data to two legitimate users with the aid of multiple relays in the presence of an eavesdropper, where the relays, the users and the eavesdropper were equipped with multiple antennas. The SOP was derived in closed-form for four cooperative NOMA scenarios. A close agreement was observed between the analytical results and simulation results, and the proposed NOMA scheme outperformed the conventional OMA scheme in terms of SOP. In addition, the proposed ORAS schemes had a better secrecy performance than the RRAS scheme. Infuture, we will investigate the secrecy performance of a more complicated scenario with multiple relays and multiple eavesdroppers, in which each of them is equipped with multiple antennas.

8 Appendix

8.1 Appendix

Based on (20), the SOP of the cell-edge user for a given relay can be written by

$$\begin{aligned}
 \Psi_{1,w/}^{SC-SC} &= \Pr \left(\operatorname{argmax}_{m \in \{1,2,\dots,M\}} C_{sec,U_1}^{n,m} < R_1^s \right) \\
 &= \Pr \left\{ \frac{1 + \gamma_{U_1 \leftarrow s_1}^{n,m_{n,*}^{w/}}}{1 + \gamma_{E \leftarrow s_1}^{n,m_{n,*}^{w/}}} < 2^{2R_1^s} \right\}.
 \end{aligned} \tag{47}$$

According to $\frac{ab}{a+b+1} \approx \min(a, b)$, $\gamma_{U_1 \leftarrow s_1}^{m_{n,*}^{w/}}$ and $\gamma_{E \leftarrow s_1}^{m_{n,*}^{w/}}$ can be further expressed as

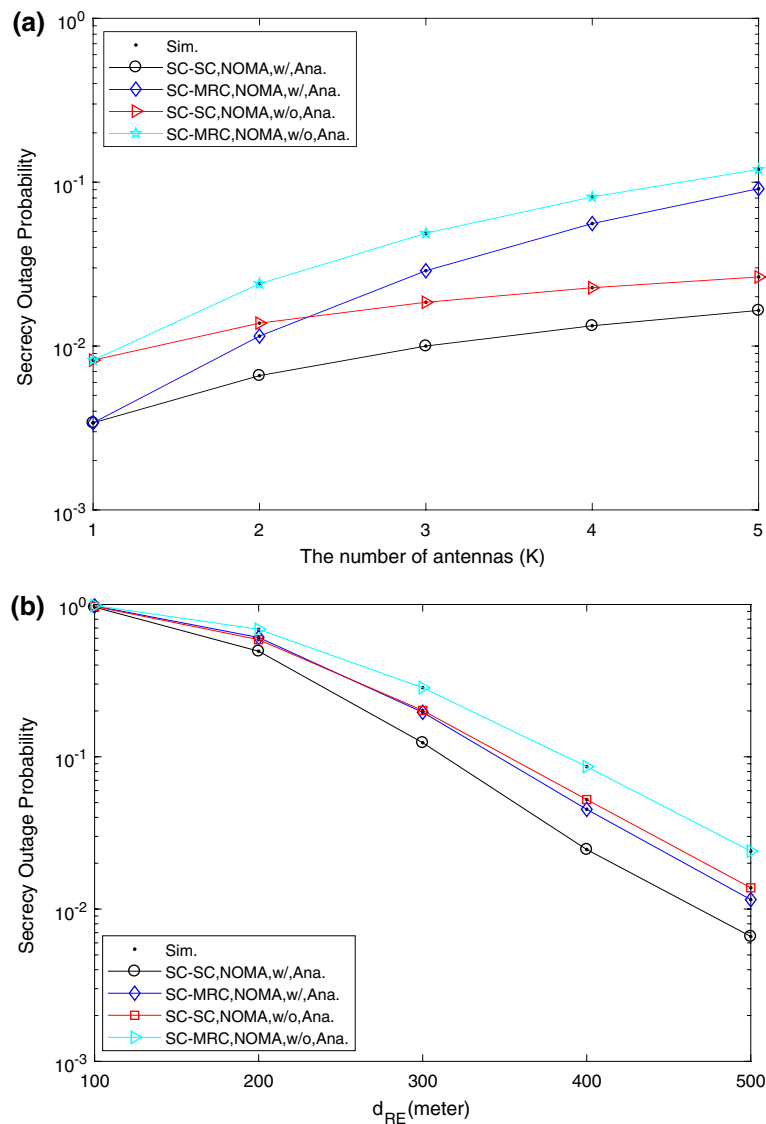


Fig. 7 The effects of the eavesdropper on SOP. (a) The different number of antenna on eavesdropper; (b) The different eavesdropping distance. When the transmission power is constant, the impact of the number of antennas and eavsdropping distances is on the SOP

$$\gamma_{U_1 \leftarrow s_1}^{n,m,w/} \approx \frac{\alpha \rho \min(X, Y_1^*)}{(1 - \alpha) \rho \min(X, Y_1^*) + 1} = \frac{\alpha \omega_1}{(1 - \alpha) \omega_1 + 1}, \tag{48}$$

$$\gamma_{U_1 \leftarrow s_1}^{n,m,w/} \approx \frac{\alpha \rho \min(X, Y_1^*)}{(1 - \alpha) \rho \min(X, Y_1^*) + 1} = \frac{\alpha \omega_1}{(1 - \alpha) \omega_1 + 1}, \tag{49}$$

where $Y_1^* = |h_{R_{n,m^*}U_1}|^2$, $Z^* = |h_{R_{n,m^*}E}|^2$. Furthermore, $\omega_1 = \rho \min(X, Y_1^*)$, $\omega_2 = \rho \min(X, Z^*)$. Then, $\Psi_{1,w/}^{SC-SC}$ in (20) can be written as

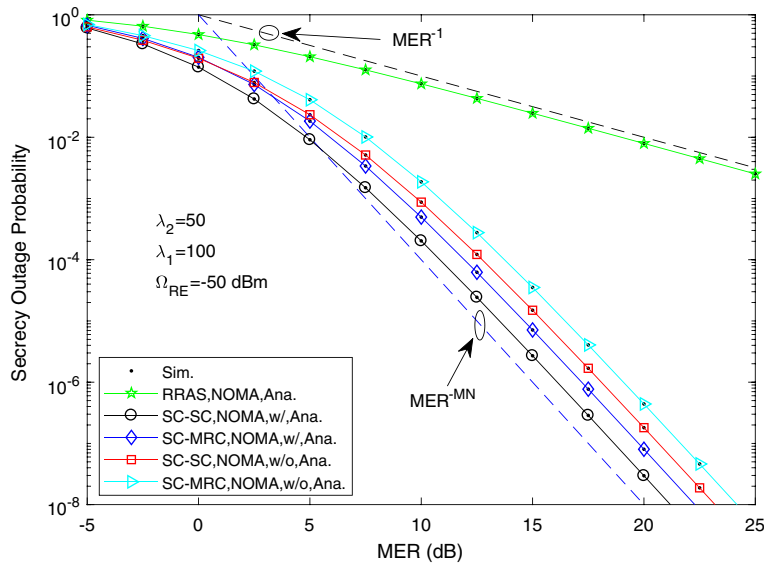


Fig. 8 SOP versus secrecy diversity order. When the transmission power is constant, the impact of the MER is on the SOP

$$\begin{aligned}
 \Psi_{1,w/}^{SC-SC} &= \Pr \left[\frac{(\omega_1 + 1)(\alpha\omega_2 + 1)}{(\omega_2 + 1)(\alpha\omega_1 + 1)} < 2^{2R_1^s} \right] \\
 &\stackrel{(a)}{=} \prod_{m=1}^M \left[\min(X, Y_1) < \frac{A_0 + B_0 Z}{C_0 - D_0 Z} \right] \\
 &= \prod_{m=1}^M \left[1 - \int_0^E f_Z(z) \int_{\frac{A_0+B_0Z}{C_0-D_0Z}}^{+\infty} f_X(x) \right. \\
 &\quad \left. \times \int_{\frac{A_0+B_0Z}{C_0-D_0Z}}^{+\infty} f_{Y_1}(y_1) dy_1 dx dz \right] \\
 &= \prod_{m=1}^M \left[1 - \Delta_{1,w/}^{SC-SC} \right],
 \end{aligned} \tag{50}$$

where equation (a) holds by following $X \geq Z$ [20, 27].

It is challenging to derive the exact closed-form of the integral in (50). By using the Gaussian-Chebyshev quadrature [23], the approximate expression of (50) can be given by $\Delta_{1,w/}^{SC-SC}$, which can be written as

$$\begin{aligned}
 \Delta_{1,w/}^{SC-SC} &= \sum_{k=1}^K \sum_{l_1=1}^{L_1} \binom{K}{k} \binom{L_1}{l_1} (-1)^{k+l_1} \sum_{l_0=1}^{N_0} \frac{k\pi E \sqrt{1-t^2}}{2N_o \Omega_{R_{n,m}} E} \\
 &\quad \times \exp \left[-\frac{kE(t+1)}{2\Omega_{R_{n,m}} E} - \left(\frac{1}{\Omega_{SR_{n,m}}} + \frac{l_1}{\Omega_{R_{n,m}} U_1} \right) F(t) \right].
 \end{aligned} \tag{51}$$

Then, we can derive the SOP for the cell-center user. The expression of $\Psi_{2,w/}^{SC-SC}$ can be expressed as

$$\begin{aligned} \Psi_{2,w/}^{SC-SC} &= \Pr \left[\frac{(\omega_3 + 1)(\alpha\omega_2 + 1)}{(\omega_2 + 1)(\alpha\omega_3 + 1)} < 2^{2R_1^s} \right] \\ &\stackrel{(a)}{=} \prod_{m=1}^M \left[\min(X, Y_2) < \frac{A_0 + B_0 Z}{C_0 - D_0 Z} \right] \\ &= \prod_{m=1}^M \left[1 - \Delta_{2,w/}^{SC-SC} \right], \end{aligned} \tag{52}$$

where $Y_2^* = |h_{R_n, m^*} U_2|^2$, $\omega_3 = \rho \min(X, Y_2^*)$, the approximate expression of (53) can be given by $\Delta_{2,w/}^{SC-SC}$, which can be expressed as

$$\begin{aligned} \Delta_{2,w/}^{SC-SC} &= \sum_{k=1}^K \sum_{l_2=1}^{L_2} \binom{K}{k} \binom{L_2}{l_2} (-1)^{k+l_2} \sum_{l_0=1}^{N_0} \frac{k\pi E \sqrt{1-t^2}}{2N_0 \Omega_{R_n, m} E} \\ &\times \exp \left[-\frac{kE(t+1)}{2\Omega_{R_n, m} E} - \left(\frac{1}{\Omega_{SR_n, m}} + \frac{l_2}{\Omega_{R_n, m} U_2} \right) F(t) \right]. \end{aligned} \tag{53}$$

Next, the expression of $\Psi_{3,w/}^{SC-SC}$ can be calculated as

$$\Psi_{3,w/}^{SC-SC} = \Pr(|\Phi_{U_2, w/}| = m) = \binom{M}{m} (\Delta_{2,w/}^{SC-SC})^m (1 - \Delta_{2,w/}^{SC-SC})^{M-m}. \tag{54}$$

Besides, $\Psi_{4,w/}^{SC-SC}$ can be calculated as

$$\begin{aligned} \Psi_{4,w/}^{SC-SC} &= \Pr \left(C_{sec, U_2}^{n, m} < R_2^s \mid |\Phi_{U_2, w/}| = m \right) \\ &= (1 - \Delta_{3,w/}^{SC-SC} / \Delta_{2,w/}^{SC-SC})^m, \end{aligned} \tag{55}$$

where $\Delta_{3,w/}^{SC-SC}$ can be expressed as

$$\begin{aligned} \Delta_{3,w/}^{SC-SC} &= \sum_{k=1}^K \sum_{l_2=1}^{L_2} \binom{K}{k} \binom{L_2}{l_2} (-1)^{k+l_2} \\ &\times \frac{k \exp \left[-\frac{A_1}{\Omega_{SR_n, m}} - \frac{l_2 A_1}{\Omega_{R_n, m} U_2} - \left(\frac{B_1}{\Omega_{SR_n, m}} + \frac{l_2 B_1}{\Omega_{R_n, m} U_2} + \frac{k}{\Omega_{R_n, m} E} \right) E \right]}{\Omega_{R_n, m} E \left(\frac{B_1}{\Omega_{SR_n, m}} + \frac{l_2 B_1}{\Omega_{R_n, m} U_2} + \frac{k}{\Omega_{R_n, m} E} \right)}. \end{aligned} \tag{56}$$

By substituting (56), (53), (51) into (55), (54), (50) and then into (20), (21), (23), the expression in (24) can be obtained. Here, the proof is completed.

8.2 Appendix

On one hand, based on (28), the SOP of the cell-edge user for a given relay can be expressed as

$$\begin{aligned}
 \Psi_{1,w/o}^{SC-SC} &= \Pr (|\Phi_{U_1,w/o}| = (0, 0)) \\
 &= \left\{ \begin{array}{l} \operatorname{argmax} \quad \min(X_{m,n}, Y_{m,n}^1) < C_1 \\ m \in (1, 2, \dots, M) \\ n \in (1, 2, \dots, N) \end{array} \right\} \\
 &= \prod_{m=1}^M \prod_{n=1}^N [\min(X, Y^1) < C_1] \\
 &= \prod_{m=1}^M \prod_{n=1}^N [1 - \Delta_{1,w/o}^{SC-SC}],
 \end{aligned} \tag{57}$$

where $C_1 = \frac{2^{2R_1^{th}} - 1}{\rho(1 - (1 - \alpha)2^{2R_1^{th}})}$. $\Delta_{1,w/o}^{SC-SC}$ can be expressed as

$$\Delta_{1,w/o}^{SC-SC} = \sum_{l_1=1}^{L_1} \binom{L_1}{l_1} (-1)^{l_1+1} \exp\left(-\frac{C_1}{\Omega_{SR_{n,m}}} - \frac{l_1 C_1}{\Omega_{R_{n,m}U_1}}\right). \tag{58}$$

On the other hand, $\Psi_{2,w/o}$ can also be derived as

$$\begin{aligned}
 \Psi_{2,w/o}^{SC-SC} &= \Pr (|\Phi_{U_1,w/o}| = (m, n)) \\
 &= \binom{N}{n} \sum_{m^1=1}^M \dots \sum_{m^n=1}^M \binom{M}{m^1} \dots \binom{M}{m^n} \\
 &\quad \times (\Delta_{1,w/o}^{SC-SC})^{\zeta_1} (1 - \Delta_{1,w/o}^{SC-SC})^{MN - \zeta_1},
 \end{aligned} \tag{59}$$

where $\zeta_1 = m^1 + \dots + m^n$, and β_1 can be achieved. Then, $\Psi_{3,w/o}^{SC-SC}$ can be given by

$$\begin{aligned}
 \Psi_{3,w/o}^{SC-SC} &= \Pr \left(C_{sec,U_1 \leftarrow s_1}^{n,m} < R_1^s \mid |\Phi_{U_1,w/o}| = (m, n) \right) \\
 &= \frac{\Pr \left(C_{sec,U_1 \leftarrow s_1}^{n,m} < R_1^s \mid |\Phi_{U_1,w/o}| = (m, n) \right)}{\Pr (|\Phi_{U_1,w/o}| = (m, n))} \\
 &= \frac{\Delta_{2,w/o}^{SC-SC}}{(\Delta_{1,w/o}^{SC-SC})^{\zeta_1}},
 \end{aligned} \tag{60}$$

where the expression for $\Delta_{2,w/o}^{SC-SC}$ in (60) can be written as

$$\Delta_{2,w/o}^{SC-SC} = \int_0^{+\infty} \left[\min(X, Y_1) > C_1, \min(X, Y_1) < \frac{A_0 + B_0 Z}{C_0 - D_0 Z} \right]^{\zeta_1} f_Z(z) dz. \tag{61}$$

After a complicated mathematical derivation, $\Delta_{2,w/o}^{SC-SC}$ can be given by

$$\begin{aligned} \Delta_{2,w/o}^{SC-SC} &= \sum_{j=1}^{\zeta_1} \sum_{k=1}^K \binom{\zeta_1}{j} \binom{K}{k} (-1)^{j+k+1} \left(\sum_{l_1=1}^{L_1} \binom{L_1}{l_1} (-1)^{l_1+1} \right)^j \\ &\sum_{l_0=1}^{N_0} \frac{k\pi E \sqrt{1-t^2}}{2N_o \Omega_{R_n, m} E} \exp \left(-\frac{C_1(\zeta_1 - j)}{\Omega_{SR_n, m}} - \frac{l_1 C_1(\zeta_1 - j)}{\Omega_{R_n, m} U_1} \right) \\ &\exp \left[-\frac{kE(t+1)}{2\Omega_{R_n, m} E} - \left(\frac{j}{\Omega_{SR_n, m}} + \frac{j l_1}{\Omega_{R_n, m} U_1} \right) F(t) \right]. \end{aligned} \tag{62}$$

Furthermore, we derive the SOP for the cell-center user. The derivations of $\Psi_{4,w/o}^{SC-SC}$, $\Psi_{5,w/o}^{SC-SC}$ and $\Psi_{6,w/o}^{SC-SC}$ are similar to those of $\Psi_{1,w/o}^{SC-SC}$, $\Psi_{2,w/o}^{SC-SC}$, and $\Psi_{3,w/o}^{SC-SC}$ are similar to those of the $\Psi_{4,w/o}^{SC-SC}$ can be calculated as

$$\begin{aligned} \Psi_{4,w/o}^{SC-SC} &= \Pr (|\Phi_{U_2, w/o}| = (0, 0)) \\ &= \left\{ \begin{array}{l} \operatorname{argmax} \quad \min(X_{m,n}, Y_{m,n}^2) < C_1 \\ m \in (1, 2, \dots, M) \\ n \in (1, 2, \dots, N) \end{array} \right\} \\ &= \prod_{m=1}^M \prod_{n=1}^N [\min(X, Y^2) < C_1] \\ &= \prod_{m=1}^M \prod_{n=1}^N [1 - \Delta_{3,w/o}^{SC-SC}], \end{aligned} \tag{63}$$

where $D_1 = \frac{2^{2R_2^{th}} - 1}{\rho(1-\alpha)}$.

From (63), $\Delta_{3,w/o}^{SC-SC}$ can be expressed as

$$\Delta_{3,w/o}^{SC-SC} = \sum_{l_2=1}^{L_2} \binom{L_2}{l_2} (-1)^{l_2+1} \exp \left(-\frac{D_1}{\Omega_{SR_n, m}} - \frac{l_2 D_1}{\Omega_{R_n} U_2} \right). \tag{64}$$

Besides, $\Psi_{5,w/o}$ can also be computed by

$$\begin{aligned} \Psi_{5,w/o}^{SC-SC} &= \Pr (|\Phi_{U_2, w/o}| = (m_+, n_+)) \\ &= \binom{N}{n_+} \sum_{m_+^1=1}^M \cdots \sum_{m_+^n=1}^M \binom{M}{m_+^1} \cdots \binom{M}{m_+^n} \\ &\times \left(\Delta_{3,w/o}^{SC-SC} \right)^{\zeta_2} \left(1 - \Delta_{3,w/o}^{SC-SC} \right)^{MN - \zeta_2}, \end{aligned} \tag{65}$$

where $\zeta_2 = m_+^1 + \dots + m_+^n$, and β_2 can be achieved. Then, $\Psi_{6,w/o}^{SC-SC}$ can be given by

$$\Psi_{6,w/o}^{SC-SC} = \Pr \left(C_{sec, U_2}^{n, m} < R_2^s \mid |\Phi_{U_2, sub.}| = (m, n) \right) = \frac{\Delta_{4,w/o}^{SC-SC}}{\left(\Delta_{3,w/o}^{SC-SC} \right)^{\zeta_2}}. \tag{66}$$

The expression for $\Delta_{4,w/o}^{SC-SC}$ in (66) can be written as

$$\Delta_{4,w/o}^{SC-SC} = \int_0^{+\infty} \left[\min(X, Y_2) > D_1, \min(X, Y_2) < A_1 + B_1 Z \right]^{\xi_2} f_Z(z) dz. \tag{67}$$

After a complicated mathematical derivation, $\Delta_{4,w/o}^{SC-SC}$ can be given by

$$\Delta_{4,w/o}^{SC-SC} = \sum_{j=1}^{\xi_2} \sum_{k=1}^K \binom{\xi_2}{j} \binom{K}{k} (-1)^{j+k+1} \left(\sum_{l_2=1}^{L_2} \binom{L_2}{l_2} (-1)^{l_2+1} \right)^j \frac{k \exp \left(-\frac{D_1(\xi_2-j)+jA_1}{\Omega_{SR,n,m}} - \frac{l_2 D_1(\xi_2-j)+j l_2 A_1}{\Omega_{R,n,m} u_2} \right)}{\Omega_{R,n,m} E \left(-\frac{kE}{\Omega_{R,n,m} E} - \frac{j B_1 E}{\Omega_{SR,n,m}} - \frac{j l_2 B_1 E}{\Omega_{R,n,m} u_2} \right)}. \tag{68}$$

By substituting (58), (62), (64), (68) into (57), (59), (60), (63), (65), (66) and then into (28), (29), (31) can be obtained. Here, the proof is completed.

Abbreviations

- NOMA: Non-orthogonal multiple access
- RAS: Relay-antenna selection
- PLS: Physical-layer security
- RF: Radio frequency
- SC: Selection combining
- MRC: Maximal-ratio combining
- CSI: Channel state information
- SOP: Secrecy outage probability
- OMA: Orthogonal multiple access
- DF: Decode-and-forward
- QoS: Quality of services
- AF: Amplity-and-forward
- MIMO: Multiple-input multiple-output
- F-NOMA: Non-orthogonal multiple access with fixed power allocation
- CR-NOMA: Non-orthogonal multiple access with cognitive radio-inspired power allocation
- SINR: Signal-to-interference-plus-noise ratio
- SNR: Signal-to-noise ratio
- ORAS: Optimal relay-antenna selection
- PDF: Probability density function
- MER: Main-to-eavesdropper ratio
- RRAS: Random relay-antenna selection

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that helped improve the quality of this manuscript.

Author Contributions

All authors have contributed equally. All authors have read and approved the final manuscript.

Funding

This work was supported by the Natural Science Foundation of China under Grants 62171237, 61901232.

Declarations

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: 10 March 2022 Accepted: 20 June 2022

Published online: 05 July 2022

References

1. C.D. Alwis, A. Kalla, Q.-V. Pham et al., Survey on 6G Frontiers: trends, applications, requirements, technologies and future research. *IEEE Open J. Veh. Technol.* **2**, 836–886 (2021)
2. G. Gui, M. Liu, F. Tang et al., 6G: opening new horizons for integration of comfort, security, and intelligence. *IEEE Wirel. Commun.* **27**(5), 126–132 (2020)
3. C.-X. Wang, J. Huang, H. Wang et al., 6G Wireless channel measurements and models: trends and challenges. *IEEE Trans. Veh. Technol.* **15**(4), 22–32 (2020)
4. Z. Ding, X. Lei, G.K. Karagiannidis et al., A survey on non-orthogonal multiple access for 5G networks: research challenges and future trends. *IEEE J. Sel. Areas Commun.* **35**(10), 2181–2195 (2017)
5. Y. Liu, Z. Qin, M. El-kashlan et al., Nonorthogonal multiple access for 5G and beyond. *Proc. IEEE* **105**(12), 2347–2381 (2017)
6. Z. Zhang, H. Sun, R. Q. Hu, et al., Downlink and uplink non-orthogonal multiple access in a dense wireless network. *IEEE J. Sel. Areas Commun.* **35**(12), 2771–2784(2017)
7. H. Wang, R. Zhang, R. Song et al., A novel power minimization precoding scheme for MIMO-NOMA uplink systems. *IEEE Commun. Lett.* **22**(5), 1106–1109 (2018)
8. M. Wildemeersch, T. Quek, M. Kountouris et al., Successive interference cancellation in heterogeneous networks. *IEEE Trans. Commun.* **62**(12), 4440–4453 (2014)
9. Z. Ding, M. Peng, H.V. Poor et al., Cooperative non-orthogonal multiple access in 5G Systems. *IEEE Commun. Lett.* **19**(8), 1462–1465 (2015)
10. Z. Ding, H. Dai, H.V. Poor et al., Relay selection for cooperative NOMA. *IEEE Commun. Lett.* **5**(4), 416–419 (2016)
11. Z. Yu, C. Zhai, J. Liu et al., Cooperative relaying based non-orthogonal multiple access (NOMA) with relay selection. *IEEE Trans. Veh. Technol.* **67**(12), 11606–11618 (2018)
12. X. Yue, Y. Liu, S. Kang et al., Exploiting full/half-duplex user relaying in NOMA systems. *IEEE Trans. Commun.* **66**(2), 560–575 (2018)
13. Z. Yang, Z. Ding, Y. Wu et al., Novel relay selection strategies for cooperative NOMA. *IEEE Trans. Veh. Technol.* **66**(11), 10114–10123 (2017)
14. Y. Yu, H. Chen, Y. Li et al., Antenna selection for MIMO nonorthogonal multiple access systems. *IEEE Trans. Veh. Technol.* **67**(4), 3158–3171 (2018)
15. L. Lv, Q. Ye, Z. Ding et al., Multi-antenna two-way relay based cooperative NOMA. *IEEE Trans. Commun.* **19**(10), 6486–6503 (2020)
16. M. Zhang, Y. Liu, Energy harvesting for physical layer security in OFDMA networks. *IEEE Trans. Inf. Forensics Secur.* **11**(1), 154–162 (2016)
17. L. Fan, N. Yang, T.Q. Duong et al., Exploiting direct links for physical layer in multiuser multirelay networks. *IEEE Wirel. Commun.* **15**(6), 3856–3867 (2016)
18. Y. Feng, S. Yan, C. Liu et al., Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access. *IEEE Trans. Inf. Forensics Secur.* **14**(6), 1670–1683 (2019)
19. H. Lei, Z. Yang, K.H. Park et al., Secrecy outage analysis for cooperative NOMA system with relay selection schemes. *IEEE Trans. Commun.* **67**(9), 6282–6298 (2019)
20. Z. Wang, Z. Peng, Secrecy performance analysis of relay selection in cooperative NOMA systems. *IEEE Access.* **7**, 86274–86287 (2019)
21. G. Wang, Q. Liu, R. He et al., Acquisition of channel state information in heterogeneous cloud radio access networks: challenges and research directions. *IEEE Wirel. Commun. Lett.* **22**(3), 100–107 (2015)
22. K. Jiang, T. Jing, Y. Huo, et al., Sic-based secrecy performance in uplink NOMA multi-eavesdropper wiretap channels. *IEEE Access.* **6**, 19664–19680(2018)
23. F. B. Hildebrand, *Introduction to Numerical Analysis*(Dover Press, New York, 1987, 2th edn.)
24. L. Lv, Z. Ding, J. Chen et al., Design of secure NOMA against full-duplex proactive eavesdropping. *IEEE Commun. Lett.* **8**(4), 1090–1094 (2019)
25. Y. Zou, X. Wang, W. Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.* **31**(10), 2099–2111 (2013)
26. H. Lei, J. Zhang, K.-H. Park et al., On secure NOMA systems with transmit antenna selection schemes. *IEEE Access.* **5**, 17450–17464 (2017)
27. J. Chen, L. Yang, M.-S. Alouini, Physical layer security for cooperative NOMA systems. *IEEE Trans. Veh. Technol.* **67**(8), 6981–6990 (2018)
28. X. Wang, W. Feng, Y. Chen et al., Energy-efficiency maximization for secure multiuser MIMO SWIPT systems with CSI uncertainty. *IEEE Access.* **6**, 2097–2109 (2017)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.