Ghavami and Akhbari
J Wireless Com Network (2023) 2023:57
https://doi.org/10.1186/s13638-023-02266-z

EURASIP Journal on Wireless
Communications and Networking

RESEARCH Open Access

Secrecy performance analysis of IRS-NOMA systems

Hossein Ghavami[1] and Bahareh Akhbari[1*]

*Correspondence:
akhbari@kntu.ac.ir

[1] Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran

Abstract

In this paper, we propose to utilize an intelligent reflecting surface (IRS) as a promising technology to enhance the coverage and physical layer security of non-orthogonal multiple access (NOMA) system. In particular, an IRS-assisted NOMA system is considered with the aid of careful channel ordering of the NOMA users, in which the transmitter sends superposed signals to multiple legitimate users by virtue of the IRS in the presence of multiple eavesdroppers. Meanwhile, the secrecy performance of the IRS-assisted NOMA system is investigated under two wiretapping cases: non-colluding and colluding external eavesdroppers. In the non-colluding case, eavesdroppers operate independently, while in the colluding case, every eavesdroppers can combine their observations to decode the messages. To this end, we derive the approximate closed-form expressions for the secrecy outage probability (SOP) and the asymptotic SOP for each wiretapping case. Also, we assume that the phase of the IRS elements is set by using the ON–OFF control method. Based on analytical results, we show that the secrecy diversity order of the IRS-NOMA at legitimate users is in connection with the number of reflecting elements. From the numerical results, it can be seen that the IRS-NOMA can achieve superior secrecy performance with increasing the number of reflecting elements of the IRS. However, we also find out that using the finite ON state reflective elements can improve the secrecy performance. Actually, increasing the number of ON state reflective elements above five has a negative effect on the system's secrecy performance.

Keywords: Intelligent reflecting surface, Secrecy outage probability, Physical layer security, Non-orthogonal multiple access

1 Introduction

An intelligent reflecting surface (IRS), also known as a reconfigurable intelligent surface (RIS), is a green technique that passively reflects the incident signal with low-power consumption. IRS does not amplify or reflect noise when reflecting signals and provides the full-duplex transmission [1]. Moreover, an essential application of IRS is to combine it with wireless communication techniques such as non-orthogonal multiple access (NOMA) in order to improve performance. For example, in [2], the closed-form expressions for the outage probability and the ergodic rate have been derived for the downlink and uplink IRS-NOMA and orthogonal multiple access (OMA) systems. Considering hardware limitations in practice, the ON–OFF control strategy, which is also known as a

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

1-bit coding scheme, has been applied in [3, 4] to establish the IRS-NOMA network. For the first time in [5], the concept of digital metamaterials, which manipulates the electromagnetic waves by a 1-bit coding scheme, has been proposed. In [3], a simple design of IRS-NOMA transmission has been proposed. Also, the outage probability has been expressed by considering the complex Gaussian distribution for the IRS channels. In [4], the exact and asymptotic expressions of outage probability and ergodic rate for the m-th user with imperfect successive interference cancellation (ipSIC) and perfect successive interference cancellation (pSIC) in IRS-NOMA networks have been derived. Since the integral of outage probability with ipSIC is non-analytic, the Gauss–Laguerre integration has been used to achieve the closed-form expression for outage probability with ipSIC. Also, simulation results have shown that the outage behaviors of IRS-NOMA are superior to those of IRS-OMA, amplify-and-forward (AF) relay, and decode-and-forward (DF) relay. Further, the authors in [6] have analyzed the required power and outage performance by introducing continuous and discrete phase shifting in IRS-NOMA with multiple antennas.

Furthermore, physical layer security has been extensively studied for various wireless networks. The secrecy performance of systems using the IRS has been recently considered in [7–12]. In [7, 8], the beamforming at the transmitter and reflecting coefficients at the IRS have been optimized. The differences between [7, 8] are in the objective functions and the constraints of the optimization problem. Nevertheless, the authors in [9–15] have focused on obtaining the closed-form expression for the secrecy outage probability (SOP). The SOP is a common performance metric for evaluating the secrecy of wireless communication. The authors in [9] have shown that utilizing the IRS enhances the secrecy performance in wireless systems. However, the authors in [10] have shown that increasing the number of intelligent elements on the IRS has a negative impact on the secrecy performance of the IRS-NOMA system. Moreover, in [10], it has been assumed that only one eavesdropper exists, and the independent Rayleigh fading channels have been considered. Also, the SOP has been approximated by using the central limit theorem (CLT) for the high number of intelligent elements on the IRS. So, the derived closed-form expression in [10] cannot be used for the low number of intelligent elements. In [12], closed-form analytical expressions for the average secrecy rate and the SOP have been derived. In particular, the upper incomplete gamma function has been substituted by the power series, which would considerably reduce the complexity of the integration of SOP. Then, a genetic algorithm (GA) has been utilized to find an optimal allocation and phase shift adjustment strategy for the IRS. Based on the eavesdropper behavior, in [11, 13, 14], the secrecy performance in wireless communication has been evaluated by considering the non-colluding and colluding scenarios. Actually, different eavesdropping models have been investigated there, namely, the cooperative and independent eavesdropper cases. In detail, in [11], the secrecy performance of an IRS-aided unmanned aerial vehicle (UAV) communication system has been studied by modeling the distribution of eavesdroppers with stochastic geometry theory. For achieving the closed-form expressions of the SOP for both cases, the gamma approximation and the CLT have been used. In [13], the analytical and asymptotic expressions for the SOP of the NOMA system over Nakagami fading have been evaluated. In [14], by using techniques of Laplace transforms and Cauchy integral theorem, the closed-form expressions of the SOP for the internet of things (IoT) networks have been derived. In [15], the closed-form expressions for the SOP and the ergodic secrecy capacity in device-to-device (D2D) communications underlaying cellular networks have been determined. In [16], the closed-form expressions for the SOP and the asymptotic SOP at an IRS-assisted D2D communication underlaying cellular networks in the presence of multiple eavesdroppers have been derived. The authors in [17] have investigated the effective secrecy throughput and SOP of IRS-NOMA networks by considering only single external or internal eavesdropper. In [18], a secure robust design of IRS-NOMA networks has been proposed with the impractical assumption of continuous phase shift.

The theoretical literature previously mentioned provides a strong foundation for understanding IRS-NOMA networks. Inspired by [5], in this paper, we specifically aim to investigate the secrecy performance of an IRS-NOMA network by invoking a 1-bit coding scheme, in which the signals are transmitted from the source to multiple non-orthogonal legitimate users via the assistance of IRS while accounting for the presence of multiple eavesdroppers. In this regard, both non-colluding and colluding eavesdroppers are taken into consideration with the aid of careful channel ordering of the NOMA users. To overcome impractical continuous phase shifting caused by excessive signaling overhead and finite resolution of phase shifters at the IRS, we assume the ON–OFF control as a feasible scheme to redesign the phase shifts of IRS for the secure transmission of IRS-NOMA networks similar to [3–5, 17]. More specifically, we derive approximate and asymptotic closed-form expressions of SOP based on the Gauss–Laguerre quadrature rule under both non-colluding and colluding wiretapping cases. To glean more insights, the secrecy diversity orders at high SNRs are obtained. We confirm that the SOP value converges to the asymptotic SOP value in the high SNR region. The remainder of the paper is organized as follows. In Sect. 2, Methods/Experimental are presented. Results and Discussion are explained in Sect. 3. Finally, Sect. 4 concludes the paper.

2 Methods/experimental

In this section, the formulation of the work is described. Primarily, the system model is presented by considering the multiple eavesdroppers and multiple legitimate users. Actually, external eavesdroppers are considered for non-colluding and colluding cases. In the non-colluding case, eavesdroppers operate independently, while in the colluding case, every eavesdroppers can combine their observations to decode the messages. In the continue, we derive the approximate closed-form expressions for the SOP and the asymptotic SOP of the IRS-NOMA system under two wiretapping cases. More specifically, non-analytic integrals of the SOP are solved by the Gauss–Laguerre quadrature rule.

2.1 System model

According to Fig. 1, we consider an IRS-NOMA system including a source equipped with M antennas, W legitimate users, S eavesdroppers, and one IRS which has R reflection elements controlled by the communication-oriented software. All the nodes except the source are equipped with a single antenna. The baseband equivalent channels from the source to IRS, from IRS to the w^{th} legitimate user, and from IRS to the s^{th} eavesdropper are denoted

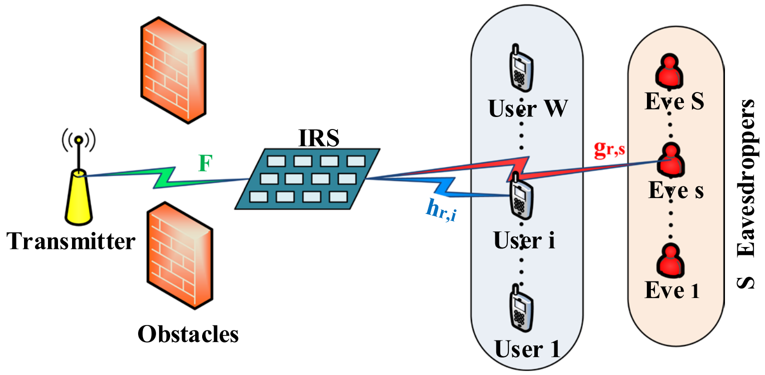

Fig. 1 The system diagram for IRS-NOMA with *S* eavesdroppers and *W* legitimate users

by $\mathbf{F} \in \mathbb{C}^{R\times M}$, $\mathbf{h}_{r,w}^{\mathrm{H}} \in \mathbb{C}^{1\times R}$, and $\mathbf{g}_{r,s}^{\mathrm{H}} \in \mathbb{C}^{1\times R}$, respectively. We assume that there is no direct link between the source and the legitimate users or eavesdroppers. Therefore, all channels such as $\mathbf{F}$, $\mathbf{h}$, and $\mathbf{g}$ are subject to complex Gaussian random variables (RVs) with zero mean and unit variance. By applying the channel estimation method based on the maximum-margin matrix factorization (MMMF) [19], we assume that the perfect channel state information (CSI) of $\mathbf{F}$ and $\mathbf{h}$ links can be obtained. Also, according to a generic assumption on the physical layer security, the channel distribution information of the eavesdropping links ($\mathbf{g}$) is available. Similar to [3, 4], in IRS-NOMA networks, we assume that the source sends the superposed signals to W legitimate users by the virtue of an IRS by using the superposition coding scheme. Hence, the received signal y_i reflected by IRS at the i-th legitimate user is shown as:

$$y_i = \mathbf{h}_{r,i}^{\mathrm{H}}\mathbf{QFw}\sum_{j=1}^{W}\alpha_j P_S x_i + n_i \tag{1}$$

where x_i is assumed to be normalized unity power signal for the i-th legitimate user, i.e., $\mathbb{E}\left(x_i^2\right) = 1$. n_i denotes the noise, P_S is the transmit power at the source (transmitter), and $\mathbf{w}$ denotes the beamforming vector. $\mathbf{Q} \triangleq$ diag $\left(r_k \exp(j\theta_k)\right)$ is a $R \times R$ diagonal matrix, where $r_k \in (0, 1]$ and $\theta_k \in [0, 2\pi)$ are the amplitude reflection coefficient and reflection phase change applied by the k^{th} element of the IRS. The source using power allocation factors α_i sends the transmitted symbols as x_i for $i = 1, \ldots, W$. It is considered that D_1 (the poorest user) and D_W (the strongest user) are paired to perform NOMA. Without loss of generality, we assume $0 < \alpha_W < \cdots < \alpha_2 < \alpha_1 < 1$ and $\sum_{i=1}^{W}\alpha_i = 1$. According to the successive interference cancellation (SIC) principle, x_i is decoded by considering the interference caused by x_j $(i < j \leq W)$ while x_j is decoded after removing the interference caused by x_i $(1 \leq i < j)$. So, the received SINR of x_i at D_i $(1 \leq i \leq W)$ can be expressed as follows:

$$\gamma_{\mathrm{B}}^{i} = \frac{\alpha_i\rho_{\mathrm{B}}\left\|\mathbf{h}_{r,i}^{\mathrm{H}}\mathbf{QFw}\right\|^2}{\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\left\|\mathbf{h}_{r,i}^{\mathrm{H}}\mathbf{QFw}\right\|^2 + 1} = \frac{\alpha_i\rho_{\mathrm{B}}\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2}{\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2 + 1} \tag{2}$$

where $\mathbf{f} = \mathbf{Fw}$ and $\boldsymbol{\varphi}$ are an $R \times 1$ vector containing the elements on the main diagonal of $\mathbf{Q}^{\mathrm{H}}$. $\mathbf{H}_{r,i}$ is the diagonal matrix with its diagonal elements obtained from $\mathbf{h}_{r,i}^{\mathrm{H}}$. We denote

$\rho_{\mathrm{B}} = P_S/\delta_B^2$ as the transmit SNR for the legitimate users' channels, where δ_B^2 is the variance of additive white Gaussian noise (AWGN) at legitimate users. Similar to [4], without loss of generality, the effective cascade channel gains from the BS to IRS and then to legitimate users are ordered as $\left\|\varphi^{\mathrm{H}}\mathbf{H}_{r,1}\mathbf{f}\right\|^2 < \left\|\varphi^{\mathrm{H}}\mathbf{H}_{r,2}\mathbf{f}\right\|^2 < \cdots < \left\|\varphi^{\mathrm{H}}\mathbf{H}_{r,W}\mathbf{f}\right\|^2$. Like [20], we assume that each of the eavesdroppers can detect x_i $(1 \leq i \leq W)$ without being interfered with x_j $(i < j \leq W)$. Under this assumption, the achievable secrecy rate in the worst-case scenario can be used as a lower bound for other scenarios because eavesdroppers have strong detection abilities. Regarding the eavesdropper behavior, we focus on two wiretapping scenarios such as the non-colluding and colluding cases.

For non-colluding case, we assume that eavesdroppers can be modeled as a set of independent and identical uniformly distributed points without cooperation with each other. Under this assumption, the one that can obtain the greatest SNR is the most detrimental eavesdropper [11]. Forasmuch as the received SNR at eavesdroppers is limited to the most detrimental eavesdropper, the received SNR of x_i $(1 \leq i \leq W)$ at eavesdroppers can be given by:

$$\gamma_{\mathrm{E}}^i = \max_{s\in\{1,2,\ldots,S\}} \left(\alpha_i\rho_{\mathrm{E}}\left\|\mathbf{g}_{r,s}^{\mathrm{H}}\mathbf{QFw}\right\|^2\right) = \max_s \left(\alpha_i\rho_{\mathrm{E}}\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{G}_{r,s}\mathbf{f}\right\|^2\right) \tag{3}$$

where $\mathbf{G}_{r,s}$ is the diagonal matrix with its diagonal elements obtained from $\mathbf{g}_{r,s}^{\mathrm{H}}$. $\rho_{\mathrm{E}} = P_S/\delta_E^2$ is the transmit SNR for the eavesdroppers' channels, and δ_E^2 is the variance of AWGN at the eavesdroppers.

For colluding case, we assume that all eavesdroppers' received signals are combined at a central node. So, the received SNR of x_i $(1 \leq i \leq W)$ at eavesdroppers can be given by:

$$\gamma_{\mathrm{E}}^i = \sum_{s=1}^{S}\alpha_i\rho_{\mathrm{E}}\left\|\mathbf{g}_{r,s}^{\mathrm{H}}\mathbf{QFw}\right\|^2 = \sum_{s=1}^{S}\alpha_i\rho_{\mathrm{E}}\left\|\varphi^{\mathrm{H}}\mathbf{G}_{r,s}\mathbf{f}\right\|^2 \tag{4}$$

As such, the secrecy capacity of the i^{th} legitimate user in the IRS-NOMA system can be written as follows:

$$C_S^i = [\log_2(1+\gamma_B^i) - \log_2(1+\gamma_E^i)]^+ \tag{5}$$

where $[x]^+ = \max\{x; 0\}$. Since the use of ON–OFF control which is a typical type of discrete phase shift design leads to better performance than the DFT-based design [3], we consider the ON–OFF control in the design of IRS. So, each element of $\boldsymbol{\varphi}$ is either 0 (OFF) or 1 (ON). Like [3, 4, 17], without loss of generality, we assume $R = PL$, where P and L are integers. Define $\mathbf{V} \triangleq \frac{1}{\sqrt{L}}\mathbf{I}_P \otimes \mathbf{1}_L$, where $\mathbf{I}_P$ is a $P \times P$ identity matrix, $\mathbf{1}_L$ is a $L \times 1$ all-ones vector, and ⊗ denotes the Kronecker product. By denoting $\mathbf{v}_p$ as the p^{th} column of $\mathbf{V}$, it is easy to show that $\mathbf{v}_p^{\mathrm{H}}\mathbf{v}_l = 0$ for $p \neq l$ and $\mathbf{v}_p^{\mathrm{H}}\mathbf{v}_p = 1$. According to [3, 4, 17], the reason for this particular configuration is that defining $\mathbf{V}$ satisfies two important properties for the ON–OFF control. First, each element of $\boldsymbol{\varphi}$ in the ON–OFF control is either 0 (OFF) or 1 (ON), which implies that only a subset of reflective elements are active at any given time. Second, the matrix $\mathbf{V}$ is designed to have orthogonal columns, which ensures that the reflected signals from different active elements do not interfere with each other. For non-colluding and colluding cases, the optimal $\boldsymbol{\varphi}$ to maximize the secrecy capacity is selected based on the following criterion, denoted as (6) and (7), respectively.

$$\max_{\mathbf{v}_p}\ \min_{i=\{1,\ldots,W\}}\ \log_2\left(\frac{1+\frac{\alpha_i\rho_{\mathrm{B}}\left\|\sqrt{L}\mathbf{v}_p^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2}{\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\left\|\sqrt{L}\mathbf{v}_p^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2+1}}{1+\max\limits_{s\in\{1,2,\ldots,S\}}\left(\alpha_i\rho_{\mathrm{E}}\left\|\sqrt{L}\mathbf{v}_p^{\mathrm{H}}\mathbf{G}_{r,s}\mathbf{f}\right\|^2\right)}\right) \tag{6}$$

$$\max_{\mathbf{v}_p}\ \min_{i=\{1,\ldots,W\}}\ \log_2\left(\frac{1+\frac{\alpha_i\rho_{\mathrm{B}}\left\|\sqrt{L}\mathbf{v}_p^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2}{\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\left\|\sqrt{L}\mathbf{v}_p^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2+1}}{1+\sum_{s=1}^{S}\alpha_i\rho_{\mathrm{E}}\left\|\sqrt{L}\mathbf{v}_p^{\mathrm{H}}\mathbf{G}_{r,s}\mathbf{f}\right\|^2}\right) \tag{7}$$

Due to the structure of $\mathbf{v}_p$, $\boldsymbol{\varphi}=\sqrt{L}\mathbf{v}_p^{opt}$ indicates which IRS elements are ON or which of them are OFF. Accordingly, $\boldsymbol{\varphi}$ can be obtained by using Algorithm 1. Algorithm 1 starts by calculating P and $\mathbf{V}$ based on inputs such as R and L. Then, x is initialized to 0, and for each column vector in $\mathbf{V}$, an iterative loop begins. Within this loop, y is initialized to infinity, and for each value from 1 to W, the objective function referred to as (6) or (7) is calculated per i and the current column vector. If this value is less than the current value of y, then y is updated to that value. After completing the inner loop, if $y>x$, then x is updated to y, and $\boldsymbol{\varphi}$ is set to a value based on the current column vector. This algorithm proceeds to the next column vector in $\mathbf{V}$ until all column vectors have been considered. Finally, the optimal value for $\boldsymbol{\varphi}$ is returned by this algorithm. The main symbols related to this scenario are summarized in Table 1.

2.2 Secrecy outage probability analysis

In this section, we derive the approximate closed-form expression for SOP. According to [15], the SOP is derived as "the probability that the secrecy capacity is less than the target secrecy rate." In this regard, based on (5), the SOP for the i^{th} legitimate user $(1\leq i\leq W)$ can be expressed as follows:

$$\mathrm{P}_i(\eta)=\Pr\left(C_S^i\leq\eta\right)=\Pr\left(\frac{1+\gamma_B^i}{1+\gamma_E^i}\leq 2^{\eta}\right) \tag{8}$$

where η is the target secrecy rate. To obtain the SOP for the non-colluding and colluding cases, the required channel statistics are calculated below.

Lemma 1 *Let us define* $\mathbf{u}$ *and* $\mathbf{v}$ *as* $L\times 1$ *complex Gaussian RVs. The cumulative distribution function* (*CDF*) *of* $\left\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\right\|^2$ *can be expressed as follows*:

$$\mathrm{F}_{\left\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\right\|^2}(x)=1-\frac{2}{\Gamma(L)}\sqrt{x^L}\,\mathrm{K}_L(2\sqrt{x}) \tag{9}$$

1 *Proof*

If $\mathbf{u}$ *and* $\mathbf{v}$ *are* $L \times 1$ *complex Gaussian RVs, the cross product of two independent RVs (*$\mathbf{u}^{\mathrm{T}}\mathbf{v}$*) based on Appendix 1 has a statistical distribution with the following probability density function (PDF):*

$$f_{\mathbf{u}^{\mathrm{T}}\mathbf{v}}(x) = \frac{4x^{L}}{\Gamma(L)}\mathrm{K}_{L-1}(2x) \tag{10}$$

where $\mathrm{K}(.)$ and $\Gamma(.)$ denote the modified Bessel function of the second kind and the gamma function, respectively. The PDF of $\left\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\right\|^{2}$ is as follows:

$$f_{\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\|^{2}}(x) = \frac{f_{\mathbf{u}^{\mathrm{T}}\mathbf{v}}\left(\sqrt{x}\right)}{2\sqrt{x}} = \frac{2}{\Gamma(L)}\sqrt{x^{L-1}}\mathrm{K}_{L-1}\left(2\sqrt{x}\right) \tag{11}$$

The CDF of $\left\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\right\|^{2}$ can be expressed as follows:

$$F_{\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\|^{2}}(x) = \int_{0}^{x} \frac{2}{\Gamma(L)}\sqrt{\xi^{L-1}}\mathrm{K}_{L-1}\left(2\sqrt{\xi}\right)\mathrm{d}\xi \tag{12}$$

By applying the change of variable $w = \sqrt{\xi/x}$, we have:

$$F_{\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\|^{2}}(x) = \frac{4}{\Gamma(L)}\int_{0}^{1}\sqrt{(xw)^{L+1}}\mathrm{K}_{L-1}\left(2w\sqrt{x}\right)\mathrm{d}w \tag{13}$$

According to Eq. (6.561.8) in [21], we have:

$$\int_{0}^{1} w^{n+1}\mathrm{K}_{n}(aw)\mathrm{d}w = 2^{n}\alpha^{-n-2}\Gamma(n+1) - \alpha^{-1}\mathrm{K}_{n+1}(a) \tag{14}$$

By substituting (14) into (13), the CDF of $\left\|\mathbf{u}^{\mathrm{T}}\mathbf{v}\right\|^{2}$can be expressed as (9).

□

We define the random variables X_i as $X_i \triangleq \boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}$ $(1 \le i \le W)$. Since the effective cascade channel gains from the BS to IRS and then to legitimate users are ordered as $\left\|\varphi^{\mathrm{H}}\mathbf{H}_{r,1}\mathbf{f}\right\|^{2} < \left\|\varphi^{\mathrm{H}}\mathbf{H}_{r,2}\mathbf{f}\right\|^{2} < \cdots < \left\|\varphi^{\mathrm{H}}\mathbf{H}_{r,W}\mathbf{f}\right\|^{2}$, according to [22], the CDF of the sorted variable X_i is given by:

$$F_{\|X_i\|^{2}}(x) = \frac{W!}{(W-i)!(i-1)!}\sum_{k=0}^{W-i}\frac{(-1)^{k}}{(i+k)}\binom{W-i}{k}\left[\overline{F}_{\|X_i\|^{2}}(x)\right]^{i+k} \tag{15}$$

where $\overline{F}_{\|X_i\|^{2}}(x)$ denotes the CDF of unsorted cascade channel gain. Since the elements of vector $\boldsymbol{\varphi}$ are either 0 (OFF) or 1 (ON) for the IRS with the ON–OFF control, the elements of vector $\mathbf{H}_{r,i}\mathbf{f}$ are obtained from $[\mathbf{h}_{r,i}^{\mathrm{H}}\mathbf{f}]$. So, X_i is derived by the cross product of two complex Gaussian RVs, and also, X_i for $1 \le i \le W$ has the same statistical distributions. Therefore, the CDF of unordered random variables $\|X_i\|^{2}$ $(\overline{F}_{\|X_i\|^{2}})$ for $1 \le i \le W$ can be expressed as (9). Since $\gamma_{\mathrm{B}}^{i} = \frac{\alpha_i\rho_{\mathrm{B}}\|X_i\|^{2}}{\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\|X_i\|^{2}+1}$ $(1 \le i < W)$ and $\gamma_{\mathrm{B}}^{W} = \alpha_W\rho_{\mathrm{B}}\left\|X_W\right\|^{2}$, the CDF of γ_{B}^{i} $(1 \le i < W$ for $\alpha_i - \xi\sum_{j>i}^{W}\alpha_j > 0)$ and γ_{B}^{W} is as follows:

$$
\begin{aligned}
F_{\gamma_{\mathrm{B}}^{i}}(\xi) &= \Pr\left(\frac{\alpha_i\rho_{\mathrm{B}}\|X_i\|^2}{\sum\limits_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\|X_i\|^2+1}<\xi\right) = F_{\|X_i\|^2}\left(\frac{\xi}{\rho_{\mathrm{B}}\left(\alpha_i-\xi\sum\limits_{j>i}^{W}\alpha_j\right)}\right)\\
&= \frac{W!}{(W-i)!(i-1)!}\sum_{k=0}^{W-i}\frac{(-1)^k}{(i+k)}\binom{W-i}{k}\\
&\quad\times\left[1-\frac{2}{\Gamma(L)}\left(\frac{\xi}{\rho_B\left(\alpha_i-\xi\sum\limits_{j>i}^{W}\alpha_j\right)}\right)^{L/2}\mathrm{K}_L\left(2\sqrt{\frac{\xi}{\rho_B\left(\alpha_i-\xi\sum\limits_{j>i}^{W}\alpha_j\right)}}\right)\right]^{i+k}
\end{aligned}
\tag{16}
$$

$$
\begin{aligned}
F_{\gamma_{\mathrm{B}}^{W}}(\xi) &= \Pr\left(\alpha_W\rho_{\mathrm{B}}\|X_W\|^2<\xi\right) = F_{\|X_W\|^2}\left(\frac{\xi}{\alpha_W\rho_{\mathrm{B}}}\right)\\
&= \frac{W!}{(W-i)!(i-1)!}\sum_{k=0}^{W-i}\frac{(-1)^k}{(i+k)}\binom{W-i}{k}\left[1-\frac{2}{\Gamma(L)}\left(\frac{\xi}{\alpha_W\rho_{\mathrm{B}}}\right)^{\frac{L}{2}}\mathrm{K}_L\left(2\sqrt{\frac{\xi}{\alpha_W\rho_{\mathrm{B}}}}\right)\right]^{i+k}
\end{aligned}
\tag{17}
$$

In (16) for $\alpha_i-\xi\sum\limits_{j>i}^{W}\alpha_j\leq 0$ and $F_{\gamma_{\mathrm{B}}^{i}}(\xi)=1$, the argument for (16) is also given in Appendix 2.

On the other hand, we define the random variable Y_s as $Y_s\triangleq\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{G}_{r,s}\mathbf{f}$. Since $\mathbf{G}_{r,s}$ and $\mathbf{f}$ have the complex Gaussian distributions, and the elements of vector $\boldsymbol{\varphi}$ are either 0 (OFF) or 1 (ON) for the IRS with the ON–OFF control, and the elements of vector $\mathbf{G}_{r,i}\mathbf{f}$ are obtained from $[\mathbf{g}_{r,s}^{\mathrm{H}}\mathbf{f}]$, Y_s is derived by the cross product of two complex Gaussian RVs, and also the CDF of $\|Y_s\|^2$ can be expressed as (9). In continues, the CDF of $\gamma_{E_{i,s}}=\alpha_i\rho_{\mathrm{E}}\|Y_s\|^2$ is as follows:

$$
\begin{aligned}
F_{\gamma_{E_{i,s}}}(\xi) &= \Pr\left(\alpha_i\rho_{\mathrm{E}}\|Y_s\|^2<\xi\right) = F_{\|Y_s\|^2}\left(\frac{\xi}{\alpha_i\rho_{\mathrm{E}}}\right)\\
&= 1-\frac{2}{\Gamma(L)}\sqrt{\left(\frac{x}{\alpha_i\rho_{\mathrm{E}}}\right)^{L}}\mathrm{K}_L\left(2\sqrt{\frac{x}{\alpha_i\rho_{\mathrm{E}}}}\right)
\end{aligned}
\tag{18}
$$

In (18), i denotes the i^{th} legitimate user ($1\leq i\leq W$), and s denotes the s^{th} eavesdropper.

Theorem 1 *For the non-colluding case, the PDF of* γ_{E}^{i} *can be found as follows*:

$$
f_{\gamma_{\mathrm{E}}^{i}}(\xi)=\tfrac{2S}{\alpha_i\rho_{\mathrm{E}}\Gamma(L)}\left(\tfrac{\xi}{\alpha_i\rho_{\mathrm{E}}}\right)^{\frac{L-1}{2}}\mathrm{K}_{L-1}\left(2\sqrt{\tfrac{\xi}{\alpha_i\rho_{\mathrm{E}}}}\right)\left(1-\tfrac{2}{\Gamma(L)}\left(\tfrac{\xi}{\alpha_i\rho_{\mathrm{E}}}\right)^{\frac{L}{2}}\mathrm{K}_L\left(2\sqrt{\tfrac{\xi}{\alpha_i\rho_{\mathrm{E}}}}\right)\right)^{S-1}
\tag{19}
$$

1 *Proof*

Based on (3), we have $\gamma_{\mathrm{E}}^{i}=\max\limits_{s\in\{1,2,\ldots,S\}}\left(\gamma_{E_{i,s}}\right)$*. So, the CDF of* γ_{E}^{i} *can be expressed as follows:*

$$F_{\gamma_{\mathrm{E}}^{i}}(\xi) = \Pr\left(\max_{\mathrm{s}\in\{1,2,\ldots,\mathrm{S}\}}\left(\gamma_{E_{i,s}}\right) \le \xi\right) = \prod_{\mathrm{s}=1}^{\mathrm{S}} F_{\gamma_{E_{i,s}}}(\xi) \tag{20}$$

By applying (18) and (20), the CDF of γ_{E}^{i} can be written as follows:

$$F_{\gamma_{\mathrm{E}}^{i}}(\xi) = \left(1 - \frac{2}{\Gamma(L)}\left(\frac{\xi}{\alpha_i\rho_{\mathrm{E}}}\right)^{\frac{L}{2}}\mathrm{K}_L\left(2\sqrt{\frac{\xi}{\alpha_i\rho_{\mathrm{E}}}}\right)\right)^{S} \tag{21}$$

Based on $f_{\gamma_{\mathrm{E}}^{i}}(x) = dF_{\gamma_{\mathrm{E}}^{i}}(x)/\mathrm{d}x$, the PDF of γ_{E}^{i} can be found as (19). □

Theorem 2 *For the colluding case, the PDF of γ_{E}^{i} can be found as follows*:

$$f_{\gamma_{\mathrm{E}}^{i}}(\xi) = \frac{1}{\alpha_i\rho_{\mathrm{E}}(L+2)\Gamma\left(\frac{SL}{L+2}\right)}\left(\frac{\xi}{\alpha_i\rho_{\mathrm{E}}(L+2)}\right)^{\frac{SL}{L+2}-1}\exp\left(-\frac{\xi}{\alpha_i\rho_{\mathrm{E}}(L+2)}\right) \tag{22}$$

1 *Proof*

See Appendix 3. □

As shown in Fig. 1, the baseband equivalent channel from the source to IRS (**F**) is common between the legitimate user and eavesdropper. Since **F** is subject to complex Gaussian RVs with zero mean, we can easily show that the SINRs of the legitimate user and eavesdropper are uncorrelated. Nevertheless, in [11, 12], it is assumed that the SINRs of the legitimate user and eavesdropper are independent. So, according to (8), the SOP for the i^{th} legitimate user $(1 \le i \le W)$ can be given by:

$$\mathrm{P}_i(\eta) = \int_0^\infty F_{\gamma_{\mathrm{B}}^{i}}\left(2^{\eta}(1+\xi)-1\right)f_{\gamma_{\mathrm{E}}^{i}}(\xi)\mathrm{d}\xi \tag{23}$$

By using (16), (17), (19), and (22), the SOP for the i^{th} legitimate user can be simplified as follows:

$$\mathrm{P}_i(\eta) = \int_0^\infty \mathrm{g}_i(\xi,\eta)\mathrm{d}\xi\ , \quad 1 \le i \le W \tag{24}$$

where $\mathrm{g}_i(\xi,\eta)$ for $1 \le i < W$ and $\mathrm{g}_W(\xi,\eta)$ can be written as (25) and (26), respectively. In these equations, $\psi_i(\xi)$ and $\mathrm{h}_2(\xi,y,\eta)$ are mentioned in (27) and (28), respectively. Since the PDF of γ_{E}^{i} is different for the non-colluding and colluding cases, $\mathrm{h}_1(\xi,x)$ is shown as (29) and (30). For the non-colluding case, $\mathrm{h}_1(\xi,x)$ can be written as (29). Also, $\mathrm{h}_1(\xi,x)$ can be written as (30) for the colluding case.

$$\mathrm{g}_i(\xi,\eta) = \begin{cases} \mathrm{h}_1(\xi,\alpha_i\rho_{\mathrm{E}})\mathrm{h}_2\left(\xi,\rho_{\mathrm{B}}\psi_i(\xi),i\right) & \text{for } \psi_i(\xi) > 0 \\ \mathrm{h}_1(\xi,\alpha_i\rho_{\mathrm{E}}) & \text{for } \psi_i(\xi) \le 0 \end{cases} \tag{25}$$

$$\mathrm{g}_W(\xi,\eta) = \mathrm{h}_1(\xi,\alpha_W\rho_\mathrm{E})\mathrm{h}_2\big(\xi,\alpha_W\rho_\mathrm{B},W\big) \tag{26}$$

$$\psi_i(\xi) = \alpha_i - (2^\eta(1+\xi)-1)\sum_{j=i+1}^{W}\alpha_j \tag{27}$$

$$\begin{aligned}\mathrm{h}_2(\xi,y,i) = {}& \frac{W!}{(W-i)!(i-1)!}\sum_{k=0}^{W-i}\frac{(-1)^k}{(i+k)}\binom{W-i}{k} \\ & \times\left[1-\frac{2}{\Gamma(L)}\left(\frac{2^\eta(1+\xi)-1}{y}\right)^{\frac{L}{2}}\mathrm{K}_L\left(2\sqrt{\frac{2^\eta(1+\xi)-1}{y}}\right)\right]^{i+k}\end{aligned} \tag{28}$$

$$\mathrm{h}_1(\xi,x)\tfrac{2S}{x\Gamma(L)}(\xi/x)^{\frac{L-1}{2}}\mathrm{K}_{L-1}\big(2\sqrt{\xi/x}\big)\Big(1-\tfrac{2}{\Gamma(L)}(\xi/x)^{\frac{L}{2}}\mathrm{K}_L\big(2\sqrt{\xi/x}\big)\Big)^{S-1} \tag{29}$$

$$\mathrm{h}_1(\xi,x) = \tfrac{1}{x(L+2)\Gamma(SL/(L+2))}\left(\tfrac{\xi}{x(L+2)}\right)^{SL/(L+2)-1}\exp\left(-\tfrac{\xi}{x(L+2)}\right) \tag{30}$$

Since the integral of Eq. (24) is non-analytic, this integral can be approximated by the Gauss–Laguerre quadrature rule. So, we first convert the above-mentioned integrals to the standard form of this rule. Since the integral is defined over an unbounded interval $[0,\infty)$, we can use (31) for obtaining the approximate closed-form of the SOP of the i^{th} legitimate user.

$$\mathrm{P}_i(\eta) = \int_0^\infty \exp(\lambda)\mathrm{g}_i(\lambda,\eta)\exp(-\lambda)\mathrm{d}\lambda = \sum_{n=1}^{N}\beta_n\exp(\lambda_n)\mathrm{g}_i(\lambda_n,\eta) \tag{31}$$

$$\beta_n = \frac{\lambda_n}{(N+1)^2(\mathrm{L}_{N+1}(\lambda_n))^2} \tag{32}$$

$$\mathrm{L}_N(x) = \sum_{m=0}^{N}\binom{N}{m}\frac{(-1)^m}{m!}x^m \tag{33}$$

where N is the number of points, and λ_n is one of the roots of the N^{th} order Laguerre polynomial, which is given in (33). The β_ns in (32) denote the weights of the Gauss–Laguerre quadrature rule [23]. On the other hand, one can easily verify that $\mathbf{v}_p^\mathrm{H}\mathbf{H}_{r,i}\mathbf{f}$, $\mathbf{v}_p^\mathrm{H}\mathbf{G}_{r,i}\mathbf{f}$, $\mathbf{v}_l^\mathrm{H}\mathbf{H}_{r,i}\mathbf{f}$, and $\mathbf{v}_l^\mathrm{H}\mathbf{G}_{r,i}\mathbf{f}$ are independent and identically distributed (i.i.d.) for $p \neq l$. In this paper, based on the perfect SIC and the strong detection of eavesdroppers, $\big(1+\gamma_\mathrm{B}^i\big)/\big(1+\gamma_\mathrm{E}^i\big)$ isindependent of $\Big(1+\gamma_\mathrm{B}^j\Big)/\Big(1+\gamma_\mathrm{E}^j\Big)$ for $i \neq j$. As a result, the use of the mentioned selection criterion ensures that the SOP of the selected legitimate user can be given by:

$$\begin{aligned}\mathrm{SOP}(\eta) &= \Pr\left(\max_{\mathbf{v}_p}\min_{i}\left\{\frac{1+\gamma_{\mathrm{B}}^{i}}{1+\gamma_{\mathrm{E}}^{i}}\right\}<2^{\eta}\right)=\prod_{p=1}^{P}\Pr\left(\min_{i}\left\{\frac{1+\gamma_{\mathrm{B}}^{i}}{1+\gamma_{\mathrm{E}}^{i}}\right\}<2^{\eta}\right)\\ &=\left(\Pr\left(\min_{i}\left\{\frac{1+\gamma_{\mathrm{B}}^{i}}{1+\gamma_{\mathrm{E}}^{i}}\right\}<2^{\eta}\right)\right)^{P}=\left(1-\prod_{i=1}^{W}\left(1-\mathrm{P}_i(\eta)\right)\right)^{P}\end{aligned} \tag{34}$$

By substituting (31) into (34), the SOP of the selected legitimate user can be simplified as follows:

$$\mathrm{SOP}(\eta)=\left(1-\prod_{i=1}^{W}\left(1-\sum_{n=1}^{N}\beta_n\exp(\lambda_n)\mathrm{g}_i(\lambda_n,\eta)\right)\right)^{P} \tag{35}$$

where $\mathrm{g}_i(\xi,\eta)$ for $1\le i<W$ and $\mathrm{g}_W(\xi,\eta)$ are derived in (25) and (26).

2.3 Asymptotic behavior of the SOP

According to [24] for achieving the asymptotic behavior of the SOP, we can consider $\rho_{\mathrm{B}}\to\infty$, which means that $\frac{1}{\rho_{\mathrm{B}}}\to 0$. According to [3] for $x\to 0$, $\mathrm{K}_L(x)$ can be approximated as follows:

$$\mathrm{K}_L(x)\approx\begin{cases}\frac{1}{x}+\frac{x}{2}\ln\left(\frac{x}{2}\right) & \text{for } \; L=1\\ \frac{1}{2}\left(\frac{(L-1)!}{\left(\frac{x}{L}\right)^{L}}-\frac{(L-2)!}{\left(\frac{x}{L}\right)^{L-2}}\right) & \text{for } \; L\ge 2\end{cases} \tag{36}$$

When $\rho_{\mathrm{B}}\to\infty$, we can approximate (28) as follows:

$$\mathrm{h}_2^{\mathrm{Asy}}(\xi,y,i)\overset{y\to\infty}{\approx}\begin{cases}\binom{W}{i}\left(\frac{1-2^{\eta}(1+\xi)}{y}\ln\left(\frac{2^{\eta}(1+\xi)-1}{y}\right)\right)^{i} & \text{for } \; L=1\\ \binom{W}{i}\left(\frac{2^{\eta}(1+\xi)-1}{y(L-1)}\right)^{i} & \text{for } \; L\ge 2\end{cases} \tag{37}$$

For the non-colluding and colluding cases according to (26)–(29), $\mathrm{h}_1(\xi,\alpha_i\rho_{\mathrm{E}})$ and $\psi_i(\xi)$ are independent of ρ_{B} for $1\le i\le W$. So, when $\rho_{\mathrm{B}}\to\infty$, $\mathrm{g}_i(\xi,\eta)$ for $1\le i\le W$ can be approximated as follows:

$$\mathrm{g}_i^{\mathrm{Asy}}(\xi,\eta)\overset{\rho_{\mathrm{B}}\to\infty}{=}\begin{cases}\mathrm{h}_1(\xi,\alpha_i\rho_{\mathrm{E}})\mathrm{h}_2^{\mathrm{Asy}}(\xi,\rho_{\mathrm{B}}\psi_i(\xi),i) & \text{for } \; \psi_i(\xi)>0\\ \mathrm{h}_1(\xi,\alpha_i\rho_{\mathrm{E}}) & \text{for } \; \psi_i(\xi)\le 0\end{cases} \tag{38}$$

$$\mathrm{g}_W^{\mathrm{Asy}}(\xi,\eta)\overset{\rho_{\mathrm{B}}\to\infty}{=}\mathrm{h}_1(\xi,\alpha_W\rho_{\mathrm{E}})\mathrm{h}_2^{\mathrm{Asy}}(\xi,\alpha_W\rho_{\mathrm{B}},W) \tag{39}$$

By substituting (38) and (39) into (35), the asymptotic SOP of the selected legitimate user can be obtained as follows:

$$\mathrm{SOP}^{\mathrm{Asy}}(\eta)=\left(1-\prod_{i=1}^{W}\left(1-\sum_{n=1}^{N}\beta_n\exp(\lambda_n)\mathrm{g}_i^{\mathrm{Asy}}(\lambda_n,\eta)\right)\right)^{P} \tag{40}$$

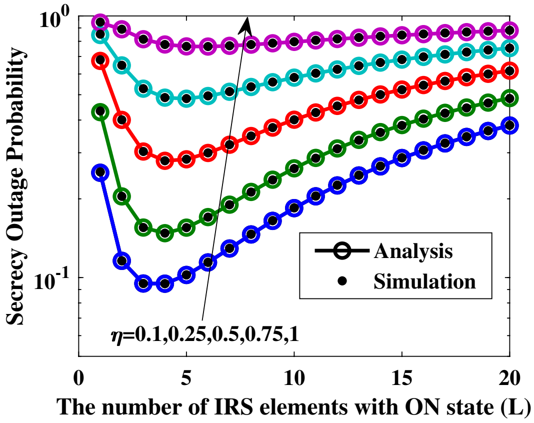

Fig. 2 The SOP versus the number of IRS elements with ON state (L) for different η with $P = 1$and $S = 1$

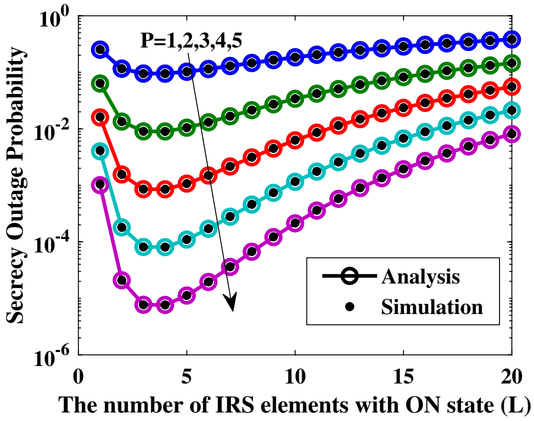

Fig. 3 The SOP versus the number of IRS elements with ON state (L) for different P with $S = 1$and $\eta = 0.1$

According to [24], the secrecy diversity order for legitimate users is defined as follows:

$$D_{\text{sec}} = -\lim_{\rho_{\text{B}}\to\infty} \frac{\log\left(\text{SOP}^{\text{Asy}}(\eta)\right)}{\log\left(\rho_{\text{B}}\right)} \tag{41}$$

By substituting (40) into (41), the secrecy diversity order of IRS-NOMA at legitimate users for $L = 1$ and $L \geq 2$ in the non-colluding and colluding cases is $D_{\text{sec}} = P$.

3 Results and discussion

In this section, Monte Carlo simulation results are presented to verify analytical results. We consider $W = 3$, $\alpha_1 = 0.6$, $\alpha_2 = 0.3$, $\alpha_3 = 0.1$, and $\rho_{\text{E}} = -10$ dB. Similar to [3, 4, 17], these parameters are chosen for a behavioral validation of the system.

In Figs. 2, 3, and 4, we plot the SOP of the selected legitimate user by using (34) versus the number of IRS elements with ON state (L) by assuming $\rho_{\text{B}} = 10$ dB. In Fig. 2, when the target secrecy rate (η) increases for $P = 1$ and $S = 1$, the SOP becomes higher. Figure 3 for $\eta = 0.1$ bits per channel use (BPCU) and $S = 1$ shows that increasing P leads

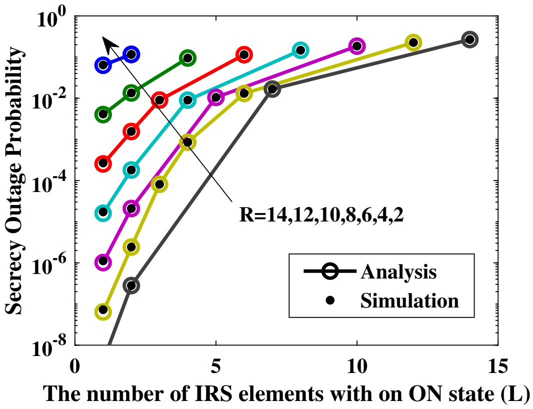

Fig. 4 The SOP versus the number of IRS elements with ON state (L) for different R with $S = 1$and $\eta = 0.1$

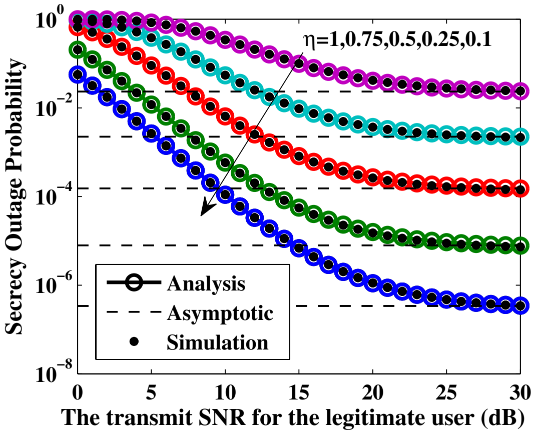

Fig. 5 The SOP versus the transmit SNR for the legitimate user (ρ_B) for different η with $R = 20, L = 5$, and $P = 4$

to increasing the number of choices for which the IRS elements to be ON or OFF. So, according to (6), the optimal vector of $\mathbf{v}_p$ can be found such that the SOP has less value. In Figs. 2 and 3, for $L <= 5$, we observe that increasing the number of IRS elements (L) leads to decreasing the SOP because the transmitter information, that is blocked by obstacles, can be more reflected by using more IRS elements. Also, the signal reflection does not amplify or reflect noise due to the nature of the IRS. Moreover, the IRS instead of amplifying the signal sends L copies of the signal. For $L >= 5$, increasing the number of IRS elements (L) leads to increasing the SOP since increasing L allows eavesdroppers to extract more information. Actually, eavesdroppers receive L copies of the signals from the IRS. Figure 4 shows that increasing the number of IRS elements (R) reduces the SOP. In Fig. 4, unlike the previous figures, it is assumed that each of the curves has the fixed R. Since $R = PL$, increasing L leads to decreasing P for fixed R. As a result, the SOP is reduced. So, the case for which only one of the IRS elements is ON ($L = 1$) has better secrecy performance in comparison with the case wherein all the IRS elements are ON ($L = R$).

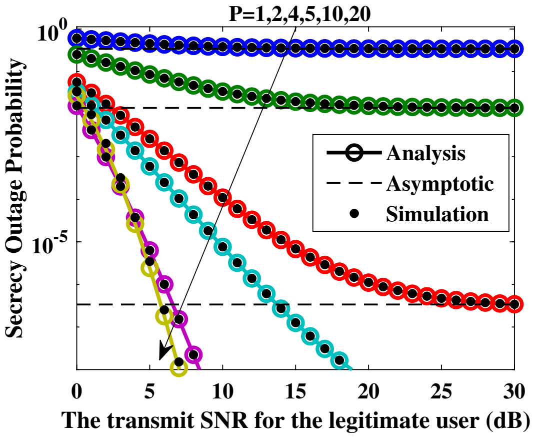

Fig. 6 The SOP versus the transmit SNR for the legitimate user (ρ_B) for different P with $R = 20$ and $S = 1$

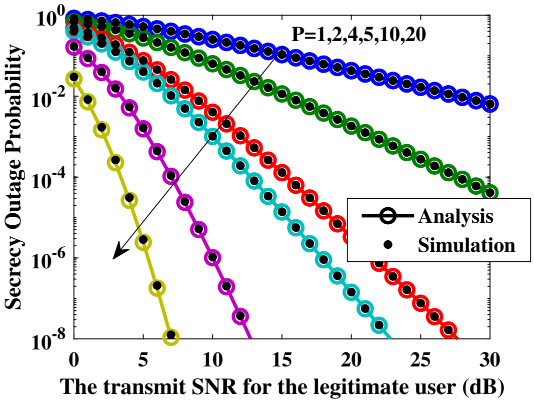

Fig. 7 The SOP versus the transmit SNR for the legitimate user (ρ_B) for different P with $L = 1$and $S = 1$

In Figs. 5, 6, and 7, we plot the SOP of the selected legitimate user versus the transmit SNR for the legitimate user (ρ_B) at different η and P. We can see that our theoretical analysis and simulation results are closely matched. At the higher transmit SNR, the exact SOP curves converge to the asymptotic SOP curves. Figure 5 shows that the SOP becomes higher for different transmit SNRs when η increases for $R = 20$, $L = 5$, $P = 4$, and $S = 1$. In Figs. 6 and 7 for $S = 1$ and $\eta = 0.1$ BPCU, it can be found that increasing P can effectively reduce the SOP for the different transmit SNRs. The difference between Figs. 6 and 7 is that in Fig. 6, the value of R is fixed as $R = 20$ and with increasing P, L decreases; but in Fig. 7, the value of L is fixed as $L = 1$ and with increasing P, R also increases. In addition, Fig. 6 confirms the optimality of the choice of $L = 1$ in the multiuser scenario.

In Figs. 8, 9, 10, and 11, the behavior of eavesdroppers, which can be non-colluding and colluding, has been compared by increasing the number of eavesdroppers (S). In Figs. 8 and 9, we plot the SOP of the selected legitimate user versus the number of IRS elements with ON state (L) for the different number of eavesdroppers (S) by assuming $P = 1$ and $\eta = 0.1$ BPCU. Figures 8 and 9 show that the SOP becomes higher in the non-colluding and colluding cases when S increases. Also, due to the fact that

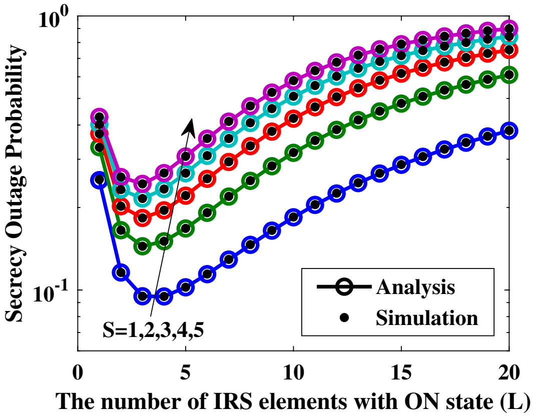

Fig. 8 The SOP versus the number of IRS elements with ON state (L) for the non-colluding case with $P = 1$ and $\eta = 0.1$

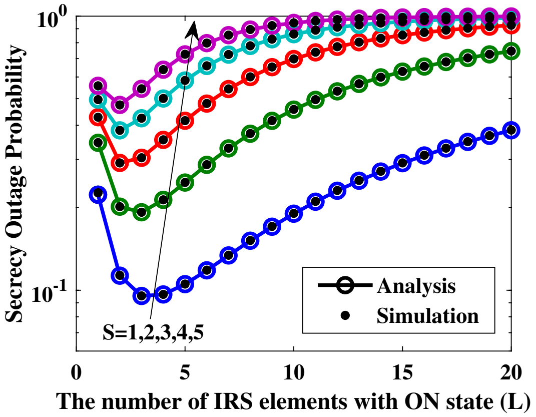

Fig. 9 The SOP versus the number of IRS elements with ON state (L) for the colluding case with $P = 1$and $\eta = 0.1$

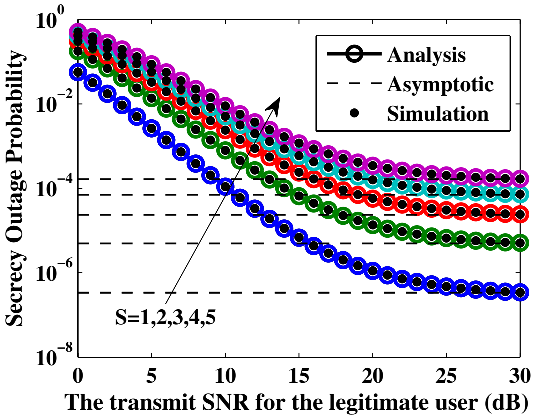

Fig. 10 The SOP versus the transmit SNR for the legitimate user (ρ_B) for the non-colluding case with $R = 20$, $L = 5$, and $P = 4$

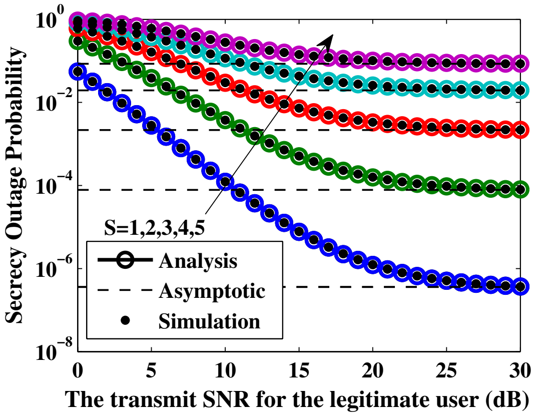

Fig. 11 The SOP versus the transmit SNR for the legitimate user (ρ_{B}) for the colluding case with $R = 20$, $L = 5$, and $P = 4$

Table 1 List of the main symbols

Symbol	Description
L	The number of reflective elements with the ON state
P	The number of activity vectors ($\mathbf{v}_p$)
R	The number of reflective elements
S	The number of eavesdroppers
W	The number of legitimate users
α_i	The power allocation factor of the i^{th} legitimate user at the source
ρ_{B}	The transmit SNR for the legitimate user
ρ_{E}	The transmit SNR for the eavesdropper

eavesdroppers argue with each other to extract information in the colluding case, this case has less SOP values compared to the non-colluding case at high values of S. But, both cases necessarily lead to the same curve in $S = 1$.

In Figs. 10 and 11, we plot the SOP of the selected legitimate user versus the transmit SNR for the legitimate user (ρ_{B}) at the different number of eavesdroppers (S) by considering $R = 20$, $L = 5$, $P = 4$, and $\eta = 0.1$ BPCU. Figures 10 and 11 show that increasing S leads to increasing the SOP in the non-colluding and colluding cases. Also, the colluding case has less SOP values compared to the non-colluding case at high values of S. At the higher transmit SNR, the exact SOP curves converge to the asymptotic SOP curves.

4 Conclusions

In this paper, we have investigated the secrecy performance of an IRS-assisted NOMA system by considering the channel ordering of the NOMA users. Meanwhile, we have derived expressions for the SOP and the asymptotic SOP of IRS-assisted NOMA systems in the presence of multiple legitimate users and multiple non-colluding and colluding eavesdroppers. More specifically, the approximate closed-form expressions for the SOP and the asymptotic SOP have been validated through simulations. Based on the approximated analyses, the secrecy diversity order of the IRS-NOMA at legitimate users has been related to the number of reflecting elements. Also, numerical results have shown that applying the IRS can improve the secrecy performance when we use the ON–OFF control. Actually, increasing the number of reflecting elements (R) can be achieved superior secrecy performance. However, we also find out that using the finite ON state reflective elements (L) can improve the secrecy performance. Actually, increasing the number of reflective elements with the ON state above five has a negative effect on the system secrecy performance, and $L = 1$ is the optimal choice of L when we use the ON–OFF control.

Algorithm 1 The ON-OFF control

```
calculate $P = \frac{R}{L}$
calculate $\mathbf{V} = \frac{1}{\sqrt{L}}\mathbf{I}_P \otimes \mathbf{1}_L$
initialize $x = 0$
for $p = 1$ to $P$ step $1$ do
    consider $\mathbf{v}_p$ as the $p^{th}$ column of $\mathbf{V}$
    initialize $y = \infty$
    for $i = 1$ to $W$ step $1$ do
        consider $t^*$ as the value of objective function shown in (6) or (7) per $i$ and $\mathbf{v}_p$
        if $y > t^*$ then
            $y \Leftarrow t^*$
        end if
    end for
    if $y > x$ then
        $x \Leftarrow y$
        $\varphi \Leftarrow \sqrt{L}\mathbf{v}_p$
    end if
end for
```

Appendix 1

If $\mathbf{u}$ and $\mathbf{v}$ are $L \times 1$ complex Gaussian RVs with zero mean and unit variance, the cross product of two independent RVs ($\mathbf{a} = \mathbf{u}^{\mathrm{T}}\mathbf{v}$) has the real ($\mathbf{a}_{\mathrm{R}}$) and imaginary ($\mathbf{a}_{\mathrm{L}}$) parts, and their conditional distribution $\mathbf{a}_{\mathrm{R}}$ and $\mathbf{a}_{\mathrm{L}}$ are independent of each other with a complex Gaussian distribution.

$$\mathbf{a}_{\mathrm{R}}\|\mathbf{u} \sim \mathbb{CN}\Big(0, \|\mathbf{u}\|^2/2\Big) \tag{42}$$

$$\mathbf{a}_{\mathrm{L}}\|\mathbf{u} \sim \mathbb{CN}\Big(0, \|\mathbf{u}\|^2/2\Big) \tag{43}$$

Hence, the joint conditional characteristic function of $\mathbf{a}_{\mathrm{R}}$ and $\mathbf{a}_{\mathrm{L}}$ is obtained as follows:

$$\Psi_{\mathbf{a}_{\mathrm{R}},\mathbf{a}_{\mathrm{L}}\|\mathbf{u}}(jw_1\|\mathbf{u}, jw_2\|\mathbf{u}) = \mathbb{E}\big(\exp\big(j(w_1\mathbf{a}_{\mathrm{R}} + w_2\mathbf{a}_{\mathrm{L}})\|\mathbf{u}\big)\big) = \exp\left(-\frac{(w_1^2 + w_2^2)\|\mathbf{u}\|^2}{4}\right) \tag{44}$$

The joint characteristic function of $\mathbf{a}_{\mathrm{R}}$ and $\mathbf{a}_{\mathrm{L}}$ is also obtained as follows:

$$\begin{aligned}\Psi_{\mathbf{a}_{\mathrm{R}},\mathbf{a}_{\mathrm{L}}}(jw_1,jw_2) &= \int \Psi_{\mathbf{a}_{\mathrm{R}},\mathbf{a}_{\mathrm{L}}\|\mathbf{u}}(jw_1\|\mathbf{u},jw_2\|\mathbf{u})f_{\mathbf{u}}(\mathbf{u})\mathrm{d}\mathbf{u} \\ &= \frac{1}{\pi^L}\int \exp\left(-\left(1+\frac{(w_1^2+w_2^2)}{4}\right)\|\mathbf{u}\|^2\right)\mathrm{d}\mathbf{u}\end{aligned} \tag{45}$$

According to [25], we know that

$$\frac{1}{\pi^L}\int \exp\left(-a\|\mathbf{u}\|^2+2R\left(\mathbf{u}^T\mathbf{b}\right)+2jR\left(\mathbf{u}^T\mathbf{c}\right)\right)\mathrm{d}\mathbf{u} = \frac{1}{\alpha^L}\exp\left(\frac{\|\mathbf{b}\|^2-\|\mathbf{c}\|^2-j2R\left(\mathbf{b}^T\mathbf{c}\right)}{\alpha}\right) \tag{46}$$

So, the joint characteristic function can be simplified as follows:

$$\Psi_{\mathbf{a}_{\mathrm{R}},\mathbf{a}_{\mathrm{L}}}(jw_1,jw_2) = \left(1+\frac{(w_1^2+w_2^2)}{4}\right)^{-L} \tag{47}$$

After transforming the Cartesian coordinates to the polar coordinates, we can obtain the $P_{\mathbf{a}}(r)$ as:

$$P_{\mathbf{a}}(r) = \int_0^{2\pi} r \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \Psi_{\mathbf{a}_{\mathrm{R}},\mathbf{a}_{\mathrm{L}}}(jw_1,jw_2)\exp(-jr(w_1\cos(\theta)+w_1\sin(\theta)))\mathrm{d}w_1\mathrm{d}w_2\mathrm{d}\theta \tag{48}$$

By using change of variables $w_1 = t\cos(\phi)$ and $w_2 = t\sin(\phi)$, we have

$$P_{\mathbf{a}}(r) = \int_0^{\infty} t\left(1+\frac{t^2}{4}\right)^{-L}\int_0^{2\pi}\int_0^{2\pi}\exp(-jrt\cos(\theta-\phi))\mathrm{d}\theta\mathrm{d}\phi\mathrm{d}t = \frac{4r^L}{\Gamma(L)}\mathrm{K}_{L-1}(2r) \tag{49}$$

Appendix 2

The CDF of γ_{B}^i ($1 \le i < W$ for $\alpha_i - \xi\sum_{j>i}^{W}\alpha_j > 0$) is as follows:

$$\begin{aligned}F_{\gamma_{\mathrm{B}}^i}(\xi) &= \Pr\left(\frac{\alpha_i\rho_{\mathrm{B}}\left\|\boldsymbol{\varphi}^H\mathbf{H}_{r,i}\mathbf{f}\right\|^2}{\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2+1}<\xi\right) \\ &= \Pr\left(\alpha_i\rho_{\mathrm{B}}\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2<\xi\left(\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2+1\right)\right) \\ &= \Pr\left(\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2\left(\alpha_i\rho_{\mathrm{B}}-\xi\sum_{j=i+1}^{W}\alpha_j\rho_{\mathrm{B}}\right)<\xi\right) \\ &= \Pr\left(\left\|\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}\right\|^2<\frac{\xi}{\rho_{\mathrm{B}}\left(\alpha_i-\xi\sum_{j=i+1}^{W}\alpha_j\right)}\right)\end{aligned} \tag{50}$$

In the above equation for $\alpha_i - \xi\sum_{j>i}^{W}\alpha_j \le 0$ and $F_{\gamma_{\mathrm{B}}^i}(\xi) = 1$, as shown in (51), the expression of $\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}\mathbf{f}$ is expressed as the cross product of two independent RVs ($\mathbf{u}^{\mathrm{T}}\mathbf{v}$).

$$
\begin{aligned}
\boldsymbol{\varphi}^{\mathrm{H}}\mathbf{Hf} &= \begin{bmatrix} q_1 & q_2 & .. & q_L \end{bmatrix} \begin{bmatrix} h_1^{\mathrm{H}} & 0 & .. & 0 \\ 0 & h_2^{\mathrm{H}} & & \vdots \\ \vdots & & & 0 \\ 0 & .. & 0 & h_L^{\mathrm{H}} \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_L \end{bmatrix} \\
&= \begin{bmatrix} q_1 h_1^{\mathrm{H}} & \ldots & q_L h_L^{\mathrm{H}} \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_L \end{bmatrix} = \sum_{i=1}^{L} \overbrace{h_i^{\mathrm{H}}}^{u_i} \overbrace{q_i f_i}^{v_i} = \mathbf{u}^{\mathrm{T}} \mathbf{v}
\end{aligned}
\tag{51}
$$

Since we have defined the random variables X_i as $X_i = \boldsymbol{\varphi}^{\mathrm{H}}\mathbf{H}_{r,i}\mathbf{f}$ $(1 \leq i \leq W)$, the CDF of unordered random variables $\|X_i\|^2$ $(\overline{F}_{\|X_i\|^2})$ for $1 \leq i \leq W$ can be expressed as (9).

Appendix 3

Based on (18) and $f_{\gamma_{E_{i,s}}}(x) = dF_{\gamma_{E_{i,s}}}(x)/\mathrm{d}x$, the PDF of $\gamma_{E_{i,s}}$ is shown in (52). The mean and variance values of $\gamma_{E_{i,s}}$ are given by (53) and (54), respectively.

$$
f_{\gamma_{E_{i,s}}}(x) = \frac{2}{\alpha_i \rho_{\mathrm{E}} \Gamma(L)} \left(\frac{x}{\alpha_i \rho_{\mathrm{E}}} \right)^{\frac{L-1}{2}} \mathrm{K}_{L-1}\left(2\sqrt{\frac{x}{\alpha_i \rho_{\mathrm{E}}}} \right) \quad x \geq 0 \tag{52}
$$

$$
\mu = \mathbb{E}\left(\gamma_{E_{i,s}}\right) = \alpha_i \rho_{\mathrm{E}} L \tag{53}
$$

$$
\begin{aligned}
\sigma^2 &= \mathbb{V}\left(\gamma_{E_{i,s}}\right) = \mathbb{E}\left(\gamma_{E_{i,s}}^2\right) - \mathbb{E}^2\left(\gamma_{E_{i,s}}\right) = 2L(L+1)\left(\alpha_i \rho_{\mathrm{E}}\right)^2 - \left(\alpha_i \rho_{\mathrm{E}} L\right)^2 \\
&= L(L+2)\left(\alpha_i \rho_{\mathrm{E}}\right)^2
\end{aligned}
\tag{54}
$$

As the PDF of $\gamma_{E_{i,s}}$ is zero for $x < 0$ and $\lim_{x \to +\infty} f_{\gamma_{E_{i,s}}}(x) \to 0$, the Laguerre series can be used for approximating the PDF of $\gamma_{E_{i,s}}$ [26]. According to [27], the first term of the Laguerre series, which is the gamma distribution, provides a good approximation. So, we have:

$$
f_{\gamma_{E_{i,s}}}(x) \approx \frac{1}{B\Gamma(A+1)} \left(\frac{x}{B} \right)^{A} \exp\left(-\frac{x}{B} \right) x \geq 0 \tag{55}
$$

$$
A = \frac{\mu^2}{\sigma^2} - 1 = \frac{L}{L+2} - 1 \tag{56}
$$

$$
B = \frac{\sigma^2}{\mu} = \alpha_i \rho_{\mathrm{E}} (L+2) \tag{57}
$$

In (55), A and B are written as (56) and (57), respectively, where μ and σ^2 are mentioned in (53) and (54), respectively. Hence, the characteristic function of $\gamma_{E_{i,s}}$ is obtained as follows:

$$
\Psi_{\gamma_{E_{i,s}}}(jw) = \mathbb{E}\left(\exp\left(jw\gamma_{E_{i,s}}\right)\right) = \int_{-\infty}^{\infty} f_{\gamma_{E_{i,s}}}(x) \exp\left(jwx\right) \mathrm{d}x = \left(1 - jwB\right)^{-(A+1)} \tag{58}
$$

Based on (4) in the colluding case, we have $\gamma_{\mathrm{E}}^{i} = \sum_{s=1}^{S} \gamma_{E_{i,s}}$. So, the characteristic function of γ_{E}^{i} is obtained as follows:

$$\Psi_{\gamma_{\mathrm{E}}^{i}}(jw) = \Psi_{\sum\limits_{s=1}^{S} \gamma_{E_{i,s}}}(jw) = \prod_{s=1}^{S} \Psi_{\gamma_{E_{i,s}}}(jw) = \left(1 - jwB\right)^{-S(A+1)} \tag{59}$$

The PDF of γ_{E}^{i} can be found as follows:

$$f_{\gamma_{\mathrm{E}}^{i}}(\xi) = \frac{1}{2\pi} \int\limits_{-\infty}^{\infty} \Psi_{\gamma_{\mathrm{E}}^{i}}(jw) \exp\left(-jwx\right) \mathrm{d}w = \frac{1}{B\Gamma(S(A+1))} \left(\frac{x}{B}\right)^{S(A+1)-1} \exp\left(-\frac{x}{B}\right) \tag{60}$$

where A and B are mentioned in (56) and (57), respectively.

Abbreviations

AF	Amplify-and-forward
AWGN	Additive white Gaussian noise
BPCU	Bits per channel use
CLT	Central limit theorem
CSI	Channel state information
D2D	Device to device
DF	Decode-and-forward
IoT	Internet of Things
ipSIC	Imperfect successive interference cancellation
IRS	Intelligent reflecting surface
GA	Genetic algorithm
MMMF	Maximum-margin matrix factorization
NOMA	Non-orthogonal multiple access
OMA	Orthogonal multiple access
pSIC	Perfect successive interference cancellation
RIS	Reconfigurable intelligent surface
RVs	Random variables
SOP	Secrecy outage probability
UAV	Unmanned aerial vehicle

Acknowledgements

Not applicable.

Author contributions

This work is part of HG's Ph.D. thesis. All authors equally contributed to the formulation, development, numerical simulations, and writing of the manuscript. All authors read and approved the final manuscript.

Funding

This work is not funded by any organization.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 9 February 2023 Accepted: 20 June 2023
Published online: 03 July 2023

References

1. E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, R. Zhang, Wireless communications through reconfigurable intelligent surfaces. IEEE Access **7**, 116753–116773 (2019)
2. Y. Cheng, K.H. Li, Y. Liu, K.C. Teh, H.V. Poor, Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA. IEEE Trans. Wirel. Commun. **20**(6), 3988–4000 (2021)
3. Z. Ding, H.V. Poor, A simple design of IRS-NOMA transmission. IEEE Commun. Lett. **24**(5), 1119–1123 (2020)

4. X. Yue, Y. Liu, Performance analysis of intelligent reflecting surface assisted NOMA networks. IEEE Trans. Wirel. Commun. **21**(4), 2623–2636 (2021)
5. T.J. Cui, M.Q. Qi, X. Wan, J. Zhao, Q. Cheng, Coding metamaterials, digital metamaterials and programmable metamaterials. Light: Sci. Appl. **3**(10), 218–218 (2014)
6. Z. Sun, Y. Jing, On the performance of multi-antenna irs-assisted noma networks with continuous and discrete irs phase shifting. IEEE Trans. Wirel. Commun. **21**(5), 3012–3023 (2021)
7. H. Shen, W. Xu, S. Gong, Z. He, C. Zhao, Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. IEEE Commun. Lett. **23**(9), 1488–1492 (2019)
8. M. Cui, G. Zhang, R. Zhang, Secure wireless communication via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **8**(5), 1410–1414 (2019)
9. L. Yang, J. Yang, W. Xie, M.O. Hasna, T. Tsiftsis, M. Di Renzo, Secrecy performance analysis of RIS-aided wireless communication systems. IEEE Trans. Veh. Technol. **69**(10), 12296–12300 (2020)
10. L. Yang, Y. Yuan, Secrecy outage probability analysis for RIS-assisted NOMA systems. Electron. Lett. **56**(23), 1254–1256 (2020)
11. W. Wang, H. Tian, W. Ni, Secrecy performance analysis of IRS-aided UAV relay system. IEEE Wirel. Commun. Lett. **10**(12), 2693–2697 (2021)
12. I.P. Hong, Secrecy performance analysis and optimization of intelligent reflecting surface-aided indoor wireless communications. IEEE Access **8**, 109440–109452 (2020)
13. C. Yu, H.-L. Ko, X. Peng, W. Xie, Secrecy outage performance analysis for cooperative NOMA over nakagami-*m* channel. IEEE Access **7**, 79866–79876 (2019)
14. Y. Zhang, Y. Shen, H. Wang, J. Yong, X. Jiang, On secure wireless communications for IoT under eavesdropper collusion. IEEE Trans. Autom. Sci. Eng. **13**(3), 1281–1293 (2015)
15. H. Ghavami, B. Akhbari, Secure resource allocation in device-to-device communications underlaying cellular networks. China Commun. **19**(8), 149–167 (2022)
16. H. Ghavami, B. Akhbari, Secrecy performance analysis of IRS-assisted D2D communication underlaying cellular network. Phys. Commun. **55**, 101924 (2022)
17. C. Gong, X. Yue, X. Wang, X. Dai, R. Zou, M. Essaaidi, Intelligent reflecting surface aided secure communications for noma networks. IEEE Trans. Veh. Technol. **71**(3), 2761–2773 (2021)
18. Z. Zhang, L. Lv, Q. Wu, H. Deng, J. Chen, Robust and secure communications in intelligent reflecting surface assisted noma networks. IEEE Commun. Lett. **25**(3), 739–743 (2020)
19. E. Shtaiwi, H. Zhang, S. Vishwanath, M. Youssef, A. Abdelhadi, Z. Han, Channel estimation approach for RIS assisted MIMO systems. IEEE Trans. Cognit. Commun. Netw. **7**(2), 452–465 (2021)
20. Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, L. Hanzo, Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. IEEE Trans. Wirel. Commun. **16**(3), 1656–1672 (2017)
21. I.S. Gradshteyn, I.M. Ryzhik, *Table of Integrals, Series, and Products* (Academic press, New York, 2014)
22. J. Men, J. Ge, Non-orthogonal multiple access for multiple-antenna relaying networks. IEEE Commun. Lett. **19**(10), 1686–1689 (2015)
23. V. Elvira, L. Martino, P. Closas, Importance gaussian quadrature. IEEE Trans. Signal Process. **69**, 474–488 (2020)
24. L. Kong, G. Kaddoum, Z. Rezki, Highly accurate and asymptotic analysis on the SOP over SIMO $\alpha-\mu$ fading channels. IEEE Commun. Lett. **22**(10), 2088–2091 (2018)
25. H. Liu, H. Ding, L. Xiang, J. Yuan, L. Zheng, Outage and BER performance analysis of cascade channel in relay networks. Procedia Comput. Sci. **34**, 23–30 (2014)
26. S. Atapattu, C. Tellambura, H. Jiang, A mixture gamma distribution to model the SNR of wireless channels. IEEE Trans. Wirel. Commun. **10**(12), 4193–4203 (2011)
27. S. Primak, V. Kontorovich, V. Lyandres, *Stochastic Methods and Their Applications to Communications: Stochastic Differential Equations Approach* (Wiley, West Sussex, 2005)

Publisher's Note

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

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com