Physical Layer Security of Intelligent Reflective Surface Aided NOMA Networks

Zhiqing Tang, *Graduate Student Member, IEEE,* Tianwei Hou, *Member, IEEE,* Yuanwei Liu, *Senior Member, IEEE,* Jiankang Zhang, *Senior Member, IEEE,* and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—Intelligent reflective surface (IRS) technology is emerging as a promising performance enhancement technique for next-generation wireless networks. Hence, we investigate the physical layer security of the downlink in IRS-aided non-orthogonal multiple access networks in the presence of an eavesdropper, where an IRS is deployed for enhancing the quality by assisting the cell-edge user to communicate with the base station. To characterize the network's performance, the expected value of the new channel statistics is derived for the reflected links in the case of Nakagami-m fading. Furthermore, the performance of the proposed network is evaluated both in terms of the secrecy outage probability (SOP) and the average secrecy capacity (ASC). The closed-form expressions of the SOP and the ASC are derived. We also study the impact of various network parameters on the overall performance of the network considered. To obtain further insights, the secrecy diversity orders and the high signal-to-noise-ratio (SNR) slopes are obtained. We finally show that: 1) the expectation of the channel gain in the reflected links is determined both by the number of IRS elements and by the Nakagami-m fading parameters; 2) If the Nakagami-m parameter is no less than 2, the SOP of both User 1 and User 2 becomes unity, when the number of IRS elements tends to infinity; 3) The secrecy diversity orders are affected both by the number of IRS elements and by the Nakagami-m fading parameters, whereas the high-SNR slopes are not affected by these parameters. Our Monte-Carlo simulations perfectly demonstrate the analytical results.**

Keywords: Intelligent reflective surface, non-orthogonal multiple access, physical layer security.

I. Introduction

In recent years, intelligent reflective surface (IRS[1]) has been proposed for beneficially influencing wireless signal propagation [2]–[4]. They can be installed on (or removed from) walls, ceilings, building facades and other infrastructure elements. Second, because they may be readily integrated into the existing wireless networks, hence they constitute a promising cost-effective spectral efficiency (SE) and/or energy efficiency (EE) improvement technique capable of controlling the scattering, reflection and refraction characteristics of the radio waves [5], [6]. However, the design and optimization of IRS-aided networks demand further study. By appropriately adjusting the amplitude-reflection and phase coefficients, the signals reflected by the IRS can be superimposed on the direct link for enhancing the received signals [7], [8]. As another benefit, IRS also has the ability to eliminate the undesired signals, such as co-channel interference [9]. It was revealed that the IRS is capable of reducing the outage probability (OP) of optical communication networks [10]. In [11], the authors jointly optimized the active beamforming at the access point (AP) and the passive beamforming at the IRS of a specific case for maximizing the harvested power of an energy harvesting receiver. In [12], the authors studied the weighted sum-power maximization problem of the IRS-aided wireless information and power transfer (SWIPT) network. In [13], the authors proposed beam index modulation for millimeter wave (mmWave) communication exploiting the benefits of IRS.

To a parallel development, power domain non-orthogonal multiple access (NOMA[2]) has the ability of providing services for multiple users within the same physical time and/or frequency resource block at the same time, thereby significantly improving the SE and connection density [14]–[16]. In [17], the authors studied the OP of the single cell multi-carrier NOMA downlink, where the transmitter side only has statistical the channel state information (CSI) knowledge. In [18], the authors pointed out that the secrecy diversity order and the asymptotic secrecy outage probability (SOP) of a pair of NOMA users are determined by the user having poorer channel gains. As demonstrated in [19], to unleash the full potential of NOMA is important to ensure that an appropriate power difference exists between the users. The IRS has the ability to change the channel gains for enhancing the performance of NOMA, hence their intrinsic amalgam has substantial benefits.

Motivated by the potential joint benefits of IRS and NOMA, IRS-aided NOMA networks have been proposed in [20] for enhancing the network's SE and EE. Furthermore, both the

Manuscript received June 2, 2021; revised November 14, 2021 and February 25, 2022; accepted April 12, 2022. Date of publication ; date of current version .

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/P034284/1 and EP/P003990/1 (COALESCE) as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028). This paper is also supported by the National Science Foundation of China under Grant 61571401 and Grant 61901416. This paper was presented in part at the IEEE International Conference on Communications Workshops (ICC Workshops) 2021 [1].(Corresponding authors: Jiankang Zhang and Lajos Hanzo.)

Z. Tang is with Zhengzhou University, Zhengzhou, China (email:iezqtang@zzu.edu.cn).

T. Hou is with Beijing Jiaotong University, Beijing, China (email:twhou@bjtu.edu.cn).

Y. Liu is with Queen Mary University of London, London, U.K. (email:yuanwei.liu@qmul.ac.uk).

J. Zhang is with Bournemouth University, Bournemouth, U.K. (e-mail: jzhang3@bournemouth.ac.uk).

L. Hanzo is with University of Southampton, Southampton, U.K. (email:lh@ecs.soton.ac.uk).

[1]Also known as Reconfigurable Intelligent Surface (RIS).

[2]Throughout this paper, we focus our attention on the family of power-domain NOMA schemes. We simply use "NOMA" to refer to "power-domain NOMA" in the following.

downlink (DL) and uplink IRS-aided NOMA networks were studied [21]. Additionally, IRS-aided NOMA transmission was contrasted to the spatial division multiple access (SDMA) in [22]. The performance of IRS-aided NOMA networks relying on both imperfect and perfect successive interference cancellation were investigated in [23]. In [24], the authors considered both the ideal and non-ideal IRS assumptions by jointly optimizing the active beamforming at the base station (BS) and the passive beamforming at the IRS of a link to maximize the sum rate. Furthermore, in [25], the authors jointly optimized the active beamforming at the BS and the passive beamforming at the IRS of a link for minimizing the total transmit power. In [26], the authors derived the closed-form expression of the coverage probability of paired NOMA users and proved that the performance of the IRS-aided NOMA network is better than that of the traditional NOMA network. A new type of multi-cell IRS-aided NOMA resource allocation framework was proposed in [27], while an IRS-aided mmWave NOMA network was considered in [28]. In [29], machine learning techniques were adopted in an IRS-aided NOMA network for maximizing the EE.

Since the broadcast nature of wireless transmission, the issue of physical layer security (PLS) attracted widespread interests [30], [31]. In [32], the authors discussed the rich opportunities and the challenges of PLS in heterogeneous networks, massive multiple-input multiple-output schemes and of mmWave systems. Although rigorous efforts have been dedicated to the PLS of wireless communications, the overall progress is relatively slow [33]. However, the emergence of IRS technology provides a new horizon for PLS problems. In [34], the authors studied the secrecy performance of an IRS-aided wireless communication network in the presence of an eavesdropper (Eve). Similarly, in [35], the authors investigated an IRS-aided secure wireless communication network, where the eavesdropping channels are stronger than the legitimate communication channels. In [36], the authors studied the SOP of IRS-aided NOMA network in a multi-user scenario. In [37], the authors investigated whether the use of artificial noise is helpful in terms of enhancing the secrecy rate of IRS-aided networks. Additionally, a motile wiretap network was investigated [38], in which an unmanned aerial vehicle equipped with IRS was considered. The PLS of an IRS-aided vehicular network was studied in [39]. Furthermore, in [40], [41], the authors investigated the robust design of an IRS-aided secure communication system by considering realistic imperfect CSI.

A. Motivation and Contribution

Because the knowledge of the channel statistics of the reflected links is essential for the performance evaluation, many researchers investigated the channel statistics of the reflected links. We can divide the results on the CSI of the reflected links into the following two categories: 1) Central limit theorem (CLT) based CSI of the reflected links [34]–[36], [42]. Since these papers rely on the CLT, the result is inaccurate when the number of IRS elements is small or in the low signal-to-noise-ratio (SNR) region [21], which will make the analysis of PLS inaccurate. 2) accurate CSI of the reflected links [43]–[45], which relies on Meijer's G-function. However, because of Meijer's G-function, the accurate CSI cannot provide explicit insights; Most of the existing contribution on PLS in IRS-aided networks studied the problem of maximizing the secrecy rate. An IRS-aided multiple-input multiple-output network has been studied in [46]. Furthermore, in [47], [48], IRS-aided multiple input single output networks have been studied.

As mentioned above, PLS has been studied in diverse scenarios, but rarely been studied in IRS-aided NOMA, which motivates this contribution. It is worth mentioning that although the authors of [36] studied the PLS of IRS-aided NOMA networks, they only considered Rayleigh fading. However, due to the CLT-based CSI of the reflected links, the analysis results and the simulation results do not match well when the number of IRS elements is small. Furthermore, the secrecy diversity order and the secrecy capacity are not given. However, the BS-IRS and IRS-User 2/Eve links may obey Rayleigh fading [34], [36] or Rician fading [49], [50]. Hence, for the BS-IRS and IRS-User 2/Eve links we analysed the more general Nakagami-m fading scenario, which conveniently subsumes the Gaussian, Rayleigh, Ricean and single-sided Gaussian scenarios [51], [52][3] Table I provides a summary of current works of literature, and compares our proposed scheme with them. In this paper, we specifically consider the scenario of an IRS-aided NOMA network, where a BS supports a typical user as well as a cell-edge user, and NOMA is invoked. Additionally, an Eve is close to the cell-edge user. Specifically, we consider a NOMA network in which the cell-edge user cannot directly communicate with the BS, hence relies on the IRS to communicate with the BS. Although the authors of [21] revealed the CSI of the reflected links, which is divided into a high-SNR region (the number of IRS elements is small) and low-SNR region (the number of IRS elements is large), the global CSI of the reflected links is not given. This results in difficulties for the analysis of PLS problems. Our new contributions can be summarized as follows:

- We investigate the secrecy performance of IRS-aided NOMA networks, where the BS communicates with a pair of NOMA users in the presence of an Eve. In particular, we investigate the SOP and the average secrecy capacity (ASC).
- We adopt the Nakagami-m fading model for the reflected links so that it can be either Line-of-sight (LoS) or non-line-of-sight (NLoS). Correspondingly, we derive new channel statistics for the reflected links based on the associated Laplace transforms and moments. We demonstrate that the expectation of the channel gain for the reflected links is determined by the number of IRS elements and the Nakagami-m fading parameters.
- We derive closed-form expressions of the SOP and the

[3]It is worth noting that the fading parameter of Nakagami-m fading, namely $m = \frac{(K+1)^2}{2K+1}$ may be approximately converted to the Rician fading parameter K. Moreover, when the fading parameter of Nakagami-m fading is $m = 1$, the Nakagami-m distribution approximates Rayleigh fading.

TABLE I: Contrasting our novelty to the state-of-the-art.

	[6]	[21]	[23]	[24]	[34]	[36]	[39]	[46]	Proposed scheme
IRS-aided network	✓	✓	✓	✓	✓	✓	✓	✓	✓
OMA scheme	✓	✓	✓	✓	✓		✓		✓
NOMA scheme		✓	✓	✓		✓		✓	✓
Imperfect CSI			✓	✓					✓
Approximated distribution		✓			✓	✓			✓
SOP analysis					✓	✓	✓		✓
High-SNR slope		✓	✓						✓

ASC for the proposed network. To glean further insights, we derive asymptotic approximations of the SOP and the ASC in the high-SNR regime to derive both the secrecy diversity order and the high-SNR slope. We demonstrate that the number of IRS elements and Nakagami-m fading parameters directly affect the secrecy diversity order, but have no effect on the high-SNR slope.

B. Organization

The rest of the paper is organized as follows. In Section II, the model of the IRS-aided NOMA network is discussed. In Section III, the new channel statistics of the reflected links are derived, and then the performance analysis of IRS-aided NOMA networks is conducted. Furthermore, our numerical and simulation results are presented in Section IV. Finally, our conclusions are offered in Section V.

In this paper, scalars are denoted by italic letters. For a scalar s, $s!$ denotes the factorial of s. Vectors and matrices are denoted by boldface letters. For a vector $\mathbf{v}$, $\mathbf{v}^T$ denotes the transpose of $\mathbf{v}$, and diag($\mathbf{v}$) denotes a diagonal matrix in which each diagonal element is the corresponding element in $\mathbf{v}$, respectively. $\mathbb{P}(\cdot)$ denotes the probability, and $\mathbb{E}(\cdot)$ represents the expectation.

II. System Model

As shown in Fig. 1, we consider the secure DL of an IRS-aided NOMA network, where a BS communicates with two legitimate users in the presence of an Eve. The pair of legitimate users share an orthogonal resource block in power-domain NOMA. It is assumed that the BS, the paired NOMA users and Eve are equipped with a single antenna. We have an IRS, who has N elements, at the appropriate location. More specifically, User 1 is a typical user, who can communicate with the BS without the IRS. By contrast, User 2 is the cell-edge user, who needs help from the IRS to communicate with the BS. At the same time, the IRS also provides an opportunity for the Eve, who cannot overhear the messages from the BS without the IRS. Furthermore, the links between the IRS and User 1, as well as between the BS supporting User 2 and the Eve are blocked, given their distance and the presence of blocking objects.

The small-scale fading vector between the BS and IRS is denoted by

$$\mathbf{h} = [h_1, h_2, \cdots, h_N]^T. \tag{1}$$

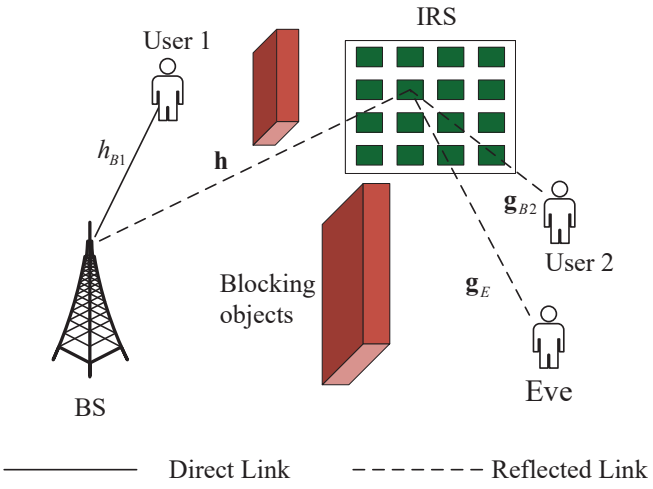


Fig. 1: An IRS-aided NOMA secure communication.

The small-scale fading vectors between the IRS and User 2 and that between the IRS and the Eve are given by

$$\mathbf{g}_{B2} = [g_{2,1}, g_{2,2}, \cdots, g_{2,N}], \tag{2}$$

and

$$\mathbf{g}_E = [g_{E,1}, g_{E,2}, \cdots, g_{E,N}], \tag{3}$$

respectively. The elements in $\mathbf{h}$, $\mathbf{g}_{B2}$ and $\mathbf{g}_E$ obey the Nakagami-m distribution having fading parameters of m_1, m_2, and m_3, respectively. Moreover, the direct link between the BS and User 1 is modelled by Rayleigh fading, which is denoted by h_{B1}.

The BS sends the following signal to the paired NOMA users

$$s = \sqrt{a_1}s_1 + \sqrt{a_2}s_2, \tag{4}$$

where s_1 and s_2 are the signals intended for User 1 and User 2, respectively, while $\sqrt{a_1}$ and $\sqrt{a_2}$ are the power allocation factors of User 1 and User 2, respectively. Based on the NOMA protocol, the power allocation coefficients satisfy the condition that $a_1 + a_2 = 1$.

The signals received by User 1 and User 2 are given by

$$y_1 = h_{B1}\sqrt{d_{B1}^{-\alpha_{B1}}}Ps + n_1, \tag{5}$$

and

$$y_2 = \mathbf{g}_{B2}\mathbf{\Phi}\mathbf{h}\sqrt{d_1^{-\alpha_1}d_{B2}^{-\alpha_{B2}}}Ps + n_2, \tag{6}$$

respectively, where d_{B1} and d_1 denote the distances from the BS to User 1 and the IRS, respectively. Furthermore, d_{B2} denotes the distance from the IRS to User 2, α_{B1}, α_1 and α_{B2} represent the path-loss exponents of the BS-User 1 link, BS-IRS links and IRS-User 2 links, respectively. Still referring to P denotes the transmit power of the BS, n_1 and n_2 represent additive white Gaussian noise (AWGN) at User 1 and User 2, respectively, which is modelled as a realization of a zero-mean complex circularly symmetric Gaussian variable with variance σ^2. Additionally, $\mathbf{\Phi} \triangleq \text{diag}[\beta_1\phi_1, \beta_2\phi_2, \ldots, \beta_N\phi_N]$ is a diagonal matrix, which represents the effective phase shift applied by all IRS elements, where $\beta_n \in (0, 1]$ is the amplitude reflection coefficient of the IRS, while $\phi_n = \exp(j\theta_n)$, $j = \sqrt{-1}$, $\forall n = 1, 2, \ldots, N$ and $\theta_n \in [0, 2\pi)$, represents the phase shift caused by the n-th IRS element. The signal received by the Eve is given by

$$y_E = \mathbf{g}_E \mathbf{\Phi} \mathbf{h} \sqrt{d_1^{-\alpha_1} d_E^{-\alpha_E}} P s + n_E, \tag{7}$$

where d_E is the distance between the IRS and Eve, α_E denotes the path-loss exponent of the IRS-Eve link and n_E represents the AWGN at Eve.

III. Performance and analysis

In this section, we consider the IRS is designed to maximize the rate of User 2. In order to simultaneously control multiple IRS elements, we assume that $\beta_1 = \beta_2 = \cdots = \beta_N = 1$. The CSI of the paired NOMA users channels is assumed to be perfectly known, since the accurate CSI of the IRS-aided system can be obtained using for example the techniques proposed in [53], [54]. In the following subsections, we first derive new channel statistics for both the direct link and reflected links. Then the SOP is studied when the CSI of Eve is not available. Furthermore, the ASC is illustrated when the CSI of Eve is known.

A. New Channel Statistics

According to the previous assumptions, and to the further assumption that the channel gain of the BS-User 1 link is better than that of the concatenated BS-IRS-User 2 link, successive interference cancellation (SIC) can be performed at User 1 to defeat the signal of User 2. The instantaneous SNR of User 1 and the instantaneous signal-to-interference-plus-noise-ratio (SINR) of User 2 can be expressed as

$$\gamma_{B1} = \rho a_1 |h_{B1}|^2 d_{B1}^{-\alpha_{B1}}, \tag{8}$$

and

$$\gamma_{B2} = \frac{a_2 |\hat{h}_{B2}|^2 d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}}}{a_1 |\hat{h}_{B2}|^2 d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}} + \frac{1}{\rho}}, \tag{9}$$

respectively, where $\rho = \frac{P}{\delta_b^2}$ denotes the transmit SNR, δ_b^2 is the variance of the AWGN at the users and $\hat{h}_{B2} = \sum_{n=1}^{N} |g_{2,n}||h_n|$ represents the equivalent channel of the concatenated BS-IRS-User 2 link.

In this paper, we consider the worst-case scenario of an IRS-aided NOMA network, in which the Eve is located within the beam cone, and all the BS-IRS-Eve signals are co-phased.[4] Moreover, we also assume that Eve has powerful detection capability, which is capable of detecting the messages of the paired NOMA users. By stipulating this assumption, our results tend to represent the lower bound of secrecy performance for the IRS-aided NOMA network. Therefore, the equivalent channel of the Eve is similar to that of User 2, which can be expressed as

$$\hat{h}_E = \sum_{n=1}^{N} |g_{E,n}||h_n|. \tag{10}$$

Therefore, the instantaneous SNR of detecting the information of User 1 and User 2 can be expressed as:

$$\gamma_{E_i} = \rho_e a_i |\hat{h}_E|^2 d_1^{-\alpha_1} d_E^{-\alpha_E}, \tag{11}$$

where $i \in \{1, 2\}$, $\rho_e = \frac{P}{\delta_e^2}$ and δ_e^2 is the variance of the AWGN at the Eve.

Lemma 1. *The cumulative distribution function (CDF) of γ_{B1} is*

$$F_{\gamma_{B1}}(x) = 1 - e^{-\frac{x}{a_1 \rho d_{B_1}^{-\alpha_{B1}}}}, \tag{12}$$

Proof. The CDF of $|h_{B1}|^2$ is $F_{|h_{B1}|^2}(x) = 1 - e^{-x}$. Then, $F_{\gamma_{B1}}$ can be derived as

$$\begin{aligned} F_{\gamma_{B1}}(x) &= \mathbb{P}\left(\gamma_{B1} < x\right) \\ &= F_{|h_{B1}|^2}\left(\frac{x}{a_1 \rho d_{B_1}^{-\alpha_{B1}}}\right) \\ &= 1 - e^{-\frac{x}{a_1 \rho d_{B_1}^{-\alpha_{B1}}}}. \end{aligned} \tag{13}$$

This completes the proof. □

Lemma 2. *Recall that the fading parameters of the elements in $\mathbf{h}$ and $\mathbf{g}_{B2}$ are m_1 and m_2, respectively. The CDF of γ_{B2} in the low-SNR regimes and the high-SNR regimes (when $m_1 \neq m_2$) are given by*

$$F_{\gamma_{B2}}(x) = 1 - Q_{\frac{1}{2}}\left(\sqrt{\lambda}, \sqrt{\frac{x}{N(1-\epsilon)\rho(a_2 - a_1 x) d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}}}}\right), \tag{14}$$

and

$$F_{\gamma_{B2}}^{0_+}(x) = \Xi\gamma\left(2m_s N, \frac{2\sqrt{m_s m_l x}}{\sqrt{\rho(a_2 - a_1 x) d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}}}}\right), \tag{15}$$

respectively, where $x < \frac{a_2}{a_1}$, $\Xi = \frac{m^N (4 m_s m_l)^{-m_s N}}{\Gamma(2 m_s N)}$, $Q_\alpha(\cdot, \cdot)$ is the Marcum Q-function, $\epsilon = \frac{1}{m_1 m_2}\left(\frac{\Gamma(m_1 + \frac{1}{2})}{\Gamma(m_1)}\right)^2 \left(\frac{\Gamma(m_2 + \frac{1}{2})}{\Gamma(m_2)}\right)^2$, $\lambda = \frac{N\epsilon}{1-\epsilon}$, $m =$

[4]For the far-field scenario, the large radius of the spherical wavefront results in approximately parallel wave propagation paths. Therefore, first of all, the practical scenario considered represents the situation, when the Eve and User 2, as well as the IRS, are located in a line. The IRS is designed for ensuring that the signals received at User 2 are co-phased, which means that User 2 is in the beam cone. In this situation, the signals received at the Eve are also co-phased. This may be encountered in IoT networks of smart wearable devices, where the users are close to each other. When the distance between the Eve and User 2 is less than $\frac{\ell}{2}$, where ℓ is the beam width of passive beamforming, we may consider the signals received at both User 2 and the Eve to be co-phased.

$\frac{\sqrt{\pi}4^{m_s-m_l+1}(m_s m_l)_s^m \Gamma(2m_s)\Gamma(2m_l-2m_s)}{\Gamma(m_s)\Gamma(m_l)\Gamma(m_l-m_s+\frac{1}{2})}$, $m_l = \max(m_1, m_2)$, $m_s = \min(m_1, m_2)$, $\Gamma(\cdot)$ *denotes the Gamma function and* $\gamma(\cdot,\cdot)$ *is the lower incomplete Gamma function.*

Proof. Please refer to Appendix A. □

Lemma 3. *Upon introducing* $Z = \sum_{n=1}^{N} |g_{q,n}||h_n|$, *where* $q \in \{2, E\}$, *the expectation of* Z^2 *is given by*

$$\mathbb{E}(Z^2) = aN\omega^N d^{-aN} k_1^N \mho, \tag{16}$$

where $a = 2m_c$, $b = m_c - m_d + \frac{1}{2}$, $c = m_c + m_d + \frac{1}{2}$, $d = 2\sqrt{m_c m_d}$, $\omega = \frac{\sqrt{\pi}4^{m_c-m_d+1}(m_c m_d)^{m_c}\Gamma(2m_c)\Gamma(2m_d)}{\Gamma(m_c)\Gamma(m_d)\Gamma\left(m_c+m_d+\frac{1}{2}\right)}$ *and* $\mho = \mho_1+\mho_2-\mho_3+\mho_4$ *with* $\mho_1 = \frac{aN+1}{d^2}$, $\mho_2 = \frac{4ab^2k_2^2}{c^2d^2k_1^2}(N-1)$, $\mho_3 = \frac{4abNk_2}{cd^2k_1}$ *and* $\mho_4 = \frac{4(a+1)(b^2+b)}{(c^2+c)d^2}k_3 - \frac{4b}{cd^2}k_2$. *Furthermore,* $k_1 = {}_2F_1(a, b; c; -1)$, $k_2 = {}_2F_1(a+1, b+1; c+1; -1)$ *and* $k_3 = {}_2F_1(a+2, b+2; c+2; -1)$ *are the Gauss hypergeometric function [55, eq. (9.100)]. In the case of* $q = 2$, *we have* $m_c = \min(m_1, m_2)$, $m_d = \max(m_1, m_2)$ *and* $\mathbb{E}(Z^2)$ *denotes the average channel gain of the BS-IRS-User 2 links, otherwise, we have* $m_c = \min(m_1, m_3)$, $m_d = \max(m_1, m_3)$ *and* $\mathbb{E}(Z^2)$ *denotes the average channel gain of the BS-IRS-Eve links.*

Proof. Please refer to Appendix B. □

Remark 1. *The second moment* $\mathbb{E}(Z^2)$ *is accurate for the global CSIs. Hence, we observe from* (16) *that the expectation of the channel gain for the reflected links is determined by the number of IRS elements and the Nakagami-*m *fading parameters.*

B. Secrecy Outage Probability

In the proposed network, the capacity of the main channel for the i-th user is given by $C_{B_i} = \log(1+\gamma_{B_i})$, while the capacity of Eve's channel for the i-th user is quantified by $C_{E_i} = \log(1+\gamma_{E_i})$. As such, the secrecy rate of the i-th user can be expressed as

$$C_i = [C_{B_i} - C_{E_i}]^+, \tag{17}$$

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

1) SOP analysis:

Next, we focus our attention on the SOP of User 1 and User 2. For the i-th user, we note that, if $C_i < R_i$, information transmission at a rate of R_i is compromised. The SOP of the i-th user can be expressed as

$$P_i(R_i) = \mathbb{P}(C_i < R_i) \tag{18}$$

Then we derive the SOP of User 1 and User 2 in the following theorems.

Theorem 1. *In the IRS-aided NOMA network considered, the SOP of User 1 is given by*

$$P_1(R_1) \approx 1 - e^{\frac{-y_1}{a_1\rho_d d_{B_1}^{-\alpha_{B_1}}}}, \tag{19}$$

where $y_1 = 2^{R_1}\left(1 + a_1\rho_e\mu d_1^{-\alpha_1} d_E^{-\alpha_E}\right) - 1$, *and* $\mu = \mathbb{E}\left(|\hat{h}_E|^2\right)$ *which can be obtained from* ***Lemma 3*** *in the case of* $m_c = \min(m_1, m_3)$ *and* $m_d = \max(m_1, m_3)$.

Proof. Based on (11) and (18), we have

$$P_1(R_1) \approx F_{\gamma_{B1}}\left(2^{R_1}\left(1 + \rho_e a_1 \mathbb{E}\left(|\hat{h}_E|^2\right) d_1^{-\alpha_1} d_E^{-\alpha_E}\right) - 1\right). \tag{20}$$

Then, by substituting (12) and (16) into (20), in the case of $m_c = \min(m_1, m_3)$ and $m_d = \max(m_1, m_3)$, we arrive at (19) after some further manipulations. This completes the proof. □

Theorem 2. *The SOP of User 2 in the low-SNR and high-SNR regimes (when* $m_1 \neq m_2$*) are given by*

$$P_2^l(R_2) \approx e^{-\frac{\lambda}{2}} \sum_{k=0}^{\infty} \frac{\lambda^k \gamma\left(k+\frac{1}{2}, \frac{y_l}{2}\right)}{k! 2^k \Gamma\left(k+\frac{1}{2}\right)}, \tag{21}$$

and

$$P_2^h(R_2) \approx \Xi\gamma\left(2m_s N, 2\sqrt{m_s m_l} y_h\right), \tag{22}$$

respectively, where we have

$$y_l = \frac{y_2}{N(1-\epsilon)\rho(a_2 - a_1 y_2) d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}}}, \tag{23}$$

$$y_h = \frac{\sqrt{y_2}}{\sqrt{\rho(a_2 - a_1 y_2) d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}}}}, \tag{24}$$

and

$$y_2 = 2^{R_2}\left(1 + a_2\mu\rho_e d_1^{-\alpha_1} d_E^{-\alpha_E}\right) - 1. \tag{25}$$

Proof. Based on (11), (18) and **Lemma 2**, the SOP of User 2 in the low-SNR regime can be expressed as

$$P_2^l(R_2) \approx F_{\gamma_{B2}}\left(2^{R_2}\left(1 + a_2\rho_e \mathbb{E}\left(|\hat{h}_E|^2\right) d_1^{-\alpha_1} d_E^{-\alpha_E}\right) - 1\right). \tag{26}$$

Then, by substituting (14) and (16) into (26), in the case of $m_c = \min(m_1, m_3)$ and $m_d = \max(m_1, m_3)$, (21) can be obtained after some further mathematical manipulations.

The SOP of User 2 in the high-SNR regime can be expressed as

$$P_2^h(R_2) \approx F_{\gamma_{B2}}^{0_+}\left(2^{R_2}\left(1 + a_2\rho_e \mathbb{E}\left(|\hat{h}_E|^2\right) d_1^{-\alpha_1} d_E^{-\alpha_E}\right) - 1\right). \tag{27}$$

Then, by substituting (15) and (16) into (27), in the case of $m_c = \min(m_1, m_3)$ and $m_d = \max(m_1, m_3)$, (22) can be obtained after some further mathematical manipulations. This completes the proof. □

Proposition 1. *In the case of* $m_d \geq 2$, *both the SOP of User 1 and of User 2 becomes* 1, *when the number of IRS elements tends to infinity.*

Proof. By substituting $N \to \infty$ into (16), we have

$$\mu \approx a^2 N^2 \left(\frac{\omega k_1}{d}\right)^N \left(1 - \frac{2bk_2}{ck_1}\right)^2. \tag{28}$$

Since we have $c = 1 + a - b$, k_1 can be rewritten as $k_1 = \frac{\Gamma(m_c+m_d+\frac{1}{2})\Gamma(1+m_c)}{\Gamma(1+2m_c)\Gamma(m_d+\frac{1}{2})}$. Let $\mu_1 = \frac{\omega k_1}{d}$, then upon substituting k_1 into μ_1, we arrive at:

$$\mu_1 = \frac{\sqrt{\pi}4^{m_c-m_d+1}(m_c m_d)^{m_c}\Gamma(2m_c)\Gamma(2m_d)\Gamma(1+m_c)}{\Gamma(m_c)2\sqrt{m_c m_d}\Gamma(1+2m_c)\Gamma(m_d+\frac{1}{2})}. \tag{29}$$

Given that $\Gamma(1+x) = x\Gamma(x)$ and $\Gamma(x)\Gamma(x+\frac{1}{2}) = 2^{1-2x}\sqrt{\pi}\Gamma(2x)$, (29) can be rewritten as

$$\mu_1 = 2^{2m_c-1}(m_c m_d)^{m_c-\frac{1}{2}} m_c \Gamma(m_d). \tag{30}$$

Since $m_d \geq 2$ and $m_d > m_c \geq \frac{1}{2}$, we have $\mu_1 \geq 1$. Then, upon substituting μ_1 into (28), we have $\mu \to \infty$ when $N \to \infty$. By substituting μ into **Theorem 1** and **Theorem 2**, in the case of $N \to \infty$, we have $P_1(R_1) = 1$ and $P_2(R_2) = 1$. This completes the proof. □

2) Asymptotic SOP and Secrecy Diversity Order Analysis:

In order to derive the secrecy diversity order to gain further insights into the network's operation in the high-SNR regime, the asymptotic behaviour is analysed. Again, as the worst-case scenario, we assume that Eve has a powerful detection capability, hence all of the reflected signals are co-phased. Without loss of generality, it is assumed that the transmit SNR for the paired NOMA users is sufficiently high (i.e., $\rho \to \infty$), and the SNR of the BS-IRS-Eve links is set to arbitrary values. Please note that the SOP tends to 1, when Eve's transmit SNR $\rho_e \to \infty$. The secrecy diversity order can be defined as follows:

$$d_s = -\lim_{\rho\to\infty} \frac{\log P^{\infty}}{\log \rho}, \tag{31}$$

where P^{∞} is the asymptotic SOP.

Corollary 1. *The asymptotic SOP of User 1 is given by*

$$P_1^{\infty}(R_1) = \frac{y_1}{a_1 \rho d_{B_1}^{-\alpha_{B_1}}}. \tag{32}$$

Proof. By expanding the exponential function in (19) and extracting the leading-order term, (32) is obtained. This completes the proof. □

Remark 2. *Upon substituting* (32) *into* (31)*, the secrecy diversity order of User 1 is* 1.

Proposition 2. *The floor of $P_1(R_1)$ in the case of $\rho_e = \rho$ is given by*

$$P_{1,\infty}^{\infty}(R_1) = \frac{2^{R_1}\mu d_1^{-\alpha_1} d_E^{-\alpha_E}}{d_{B_1}^{-\alpha_{B_1}}}. \tag{33}$$

Proof. By Substituting $\rho_e = \rho$ into (32), after some mathematical manipulations, (33) can be obtained. This completes the proof. □

Corollary 2. *The asymptotic SOP of User 2 is given by*

$$P_2^{\infty}(R_2) = \frac{m^N y_h^{2m_s N}}{\Gamma(2m_s N + 1)}. \tag{34}$$

Proof. Based on **Theorem 2**, we have the SOP of User 2 in the high-SNR regime. Then, by using the expansions of the lower incomplete Gamma function [55, eq. (8.354.1)], (22) can be represented as

$$P_2^{\infty}(R_2) = \Xi \sum_{k=0}^{\infty} \frac{(-1)^k \left(2\sqrt{m_s m_l} y_h\right)^{2m_s N+k}}{k!\,(2m_s N + k)}. \tag{35}$$

By extracting the leading-order term in (35), (34) can be obtained. This completes the proof. □

Remark 3. *Upon substituting* (34) *into* (31)*, the secrecy diversity order of User 2 is $m_s N$.*

Remark 4. *The secrecy diversity order of User 1 is not affected by the number of IRS elements and by the Nakagami-m fading parameters. By contrast, the secrecy diversity order of User 2 is affected by the number of IRS elements and by the Nakagami-m fading parameters.*

In this paper, based on the assumptions of using perfect SIC for the paired NOMA users and strong detection capability of Eve, the secrecy outage occurrences of User 1 and User 2 are independent. As a consequence, we define the SOP for the network as that of either the outage of User 1 or of User 2.

$$P_{1,2} = 1 - (1 - P_1)(1 - P_2), \tag{36}$$

where P_1 and P_2 are given by **Theorem 1** and **Theorem 2**, respectively.

Proposition 3. *The secrecy diversity order of the network can be expressed as*

$$d_s = \min(1, m_s N). \tag{37}$$

Proof. Based on **Corollary 1** as well as **Corollary 2**, and upon substituting (32) and (34) into (36), the asymptotic SOP for the network can be expressed as

$$P_{1,2}^{\infty} = P_1^{\infty} + P_2^{\infty} - P_1^{\infty} P_2^{\infty} \approx \begin{cases} \frac{m^N}{\Gamma(2m_s N+1)} \left(\frac{y_2}{\rho(a_2 - a_1 y_2) d_1^{-\alpha_1} d_{B2}^{-\alpha_{B2}}} \right)^{m_s N}, & 1 > m_s N \\ \frac{y_1}{a_1 \rho d_{B_1}^{-\alpha_{B_1}}}, & 1 < m_s N \end{cases}. \tag{38}$$

By substituting (38) into (31), we arrive at (37). The proof is completed. □

Remark 5. *The secrecy diversity order of the network is determined by the smallest one between* 1 *and $m_s N$.*

Remark 5 provides insightful guidelines for improving the SOP of the network considered by invoking IRS-aided NOMA. The SOP of the network is determined by User 1 in the case of $N \geq 2$, because the Nakagami-m fading parameters obey $m \geq \frac{1}{2}$. Specifically, the SOP of the network is determined by User 1, when the links between the BS and IRS as well as that between the IRS and User 2 is Rayleigh or Rician fading.

C. Average Secrecy Capacity Analysis

1) Approximate ASC:

In this subsection, we derive analytical expressions for the ASC of the network. The secrecy capacity in (17) can be rewritten as

$$C_i = \begin{cases} \log_2(1+\gamma_{B_i}) - \log_2(1+\gamma_{E_i}), & \gamma_{B_i} > \gamma_{E_i} \\ 0, & \gamma_{B_i} \leq \gamma_{E_i} \end{cases}. \tag{39}$$

The approximate ASC can be expressed as

$$C_i^{app} = R_{B_i} - R_{E_i} \approx C_i, \tag{40}$$

where R_{B_i} and R_{E_i} are the ergodic rates of the paired NOMA users and Eve, respectively, which can be expressed as

$$R_{B_i} = \mathbb{E}\big[\log_2(1+\gamma_{B_i})\big], \tag{41}$$

and

$$R_{E_i} = \mathbb{E}\big[\log_2(1+\gamma_{E_i})\big], \tag{42}$$

respectively.

The ergodic rates of the paired NONA users have been studied in [21], and that of Eve is necessary for obtaining the ASC. Hence, the ergodic rate of Eve and the approximate ASC are presented in the following theorems.

Theorem 3. *In the IRS-aided NOMA network considered, the ergodic rate of Eve is given by*

$$R_{E_i} = \frac{1}{\ln(2)} e^{-\frac{\lambda_e}{2}} \sum_{k=0}^{\infty} \frac{\lambda_e^k}{k! 2^k \Gamma\left(k+\frac{1}{2}\right)} \sum_{l=0}^{u_1} \omega_{1,l} \mathcal{J}_{1,i}(x_l), \tag{43}$$

where x_l is the l-th root of the Laguerre polynomial $L_n(x)$, and the weight $\omega_{1,l}$ is given by

$$w_{1,l} = \frac{x_l}{(n+1)^2 \left[L_{n+1}(x_l)\right]^2}, \tag{44}$$

and

$$\mathcal{J}_{1,i}(x) = \frac{\Gamma\left(l+\frac{1}{2}\right) - \gamma\left(l+\frac{1}{2}, \frac{t}{a_i}\right)}{1+x} e^x, \tag{45}$$

with $t = \frac{x}{2\rho_e N(1-\epsilon_e) d_1^{-\alpha_1} d_E^{-\alpha_E}}$.

Proof. Please refer to Appendix C. □

a) **Approach 1:**

Theorem 4. *In the IRS-aided NOMA network considered, the approximate ASC of User 1 can be represented as*

$$\begin{aligned} C_1^{app} \approx & -\frac{1}{\ln(2)} e^{\frac{1}{a_1 \rho d_{B_1}^{-\alpha_{B_1}}}} E_i\left(-\frac{1}{a_1 \rho d_{B_1}^{-\alpha_{B_1}}}\right) - \\ & \frac{1}{\ln(2)} e^{-\frac{\lambda_e}{2}} \sum_{k=0}^{\infty} \frac{\lambda_e^k}{k! 2^k \Gamma\left(k+\frac{1}{2}\right)} \sum_{l=0}^{u_1} \omega_{1,l} \mathcal{J}_{1,1}(x_l), \end{aligned} \tag{46}$$

where $E_i(\cdot)$ is the exponential integral.

Proof. Based on [21], the ergodic rate of User 1 is

$$R_{B_1} = -\frac{1}{\ln(2)} e^{\frac{1}{a_1 \rho d_{B_1}^{-\alpha_{B_1}}}} E_i\left(-\frac{1}{a_1 \rho d_{B_1}^{-\alpha_{B_1}}}\right). \tag{47}$$

By Substituting (43) and (47) into (40), (46) can be obtained. This completes the proof. □

Theorem 5. *In the IRS-aided NOMA network considered, the approximate ASC of User 2 can be represented as*

$$\begin{aligned} C_2^{app} \approx & \log_2\left(\frac{1}{a_1}\right) - \frac{1}{\ln(2)} e^{-\frac{\lambda}{2}} \sum_{i=0}^{\infty} \frac{\lambda^i}{i! 2^i \Gamma\left(i+\frac{1}{2}\right)} \sum_{p=0}^{u_2} \omega_p \mathcal{J}_2(t_p) \\ & - \frac{1}{\ln(2)} e^{-\frac{\lambda_e}{2}} \sum_{k=0}^{\infty} \frac{\lambda_e^k}{k! 2^k \Gamma\left(k+\frac{1}{2}\right)} \sum_{l=0}^{u_1} \omega_{1,l} \mathcal{J}_{1,2}(x_l), \end{aligned} \tag{48}$$

where $\omega_p = \frac{\pi}{u_2}$, $t_p = \cos\left(\frac{2p-1}{2u_2}\pi\right)$ *and*

$$\mathcal{J}_2(t) = \frac{\gamma\left(p+\frac{1}{2}, \frac{t+1}{N(1-\epsilon)\rho a_1 (1-t) d_1^{-\alpha_1} d_{B_2}^{-\alpha_{B_2}}}\right)}{1+t+\frac{2a_1}{a_2}} \sqrt{1-t^2}. \tag{49}$$

Proof. Based on [21], the ergodic rate of User 2 is

$$R_{B_2} \approx \log_2\left(\frac{1}{a_1}\right) - \frac{1}{\ln(2)} e^{-\frac{\lambda}{2}} \sum_{i=0}^{\infty} \frac{\lambda^i}{i! 2^i \Gamma\left(i+\frac{1}{2}\right)} \sum_{p=0}^{u_2} \omega_p \mathcal{J}_2(t_p). \tag{50}$$

By substituting (43) and (50) into (40), (48) can be obtained. This completes the proof. □

b) **Approach 2:**

For the approximate ASC of User 2, we provide a more convenient approach. It is worth noting that (51) also produces highly accurate results, despite the computational complexity reduction compared to (48), as it will be demonstrated in Section IV.

Theorem 6. *In the IRS-aided NOMA network considered, the approximate ASC of User 2 can be represented as*

$$C_2^b \approx \log_2\left(\frac{\mu_2 \rho d_1^{-\alpha_1} d_{B_1}^{-\alpha_{B_1}} + 1}{(a_1 \mu_2 \rho d_1^{-\alpha_1} d_{B_1}^{-\alpha_{B_1}} + 1)(1 + a_2 \mu d_1^{-\alpha_1} d_E^{-\alpha_E} \rho_e)}\right), \tag{51}$$

where μ_2 is the expectation of $|\hat{h}_{B_2}|^2$, which can be obtained from ***Lemma 3*** *in the case of $m_c = \min(m_1, m_2)$ and $m_d = \max(m_1, m_2)$.*

Proof. It can be seen from (40) that the approximate ASC is defined as a difference function of the ergodic rate, while the ergodic rate is defined as a logarithmic function. Thus, we can define an approximate bound to the solution in (41) and (42) by invoking Jensen's inequality [55, eq. (12.411)]. Therefore, the ergodic rate of User 2 and Eve are

$$\begin{aligned} \mathbb{E}\big[\log_2(1+\gamma_{B_2})\big] &\le \log_2\left[1+\mathbb{E}(\gamma_{B_2})\right] \\ &= \log_2\left(1 + \frac{a_2 \mu_2 d_1^{-\alpha_1} d_{B_1}^{-\alpha_{B_1}}}{a_1 \mu_2 d_1^{-\alpha_1} d_{B_1}^{-\alpha_{B_1}} + \frac{1}{\rho}}\right), \end{aligned} \tag{52}$$

and

$$\begin{aligned} \mathbb{E}\big[\log_2(1+\gamma_{E_2})\big] &\le \log_2\left[1+\mathbb{E}(\gamma_{E_2})\right] \\ &= \log_2\left(1 + a_2 \mu d_1^{-\alpha_1} d_E^{-\alpha_E} \rho_e\right), \end{aligned} \tag{53}$$

respectively.

In this way, the approximate ASC can be expressed as a difference function of two approximate bounds. Then, upon substituting (52) and (53) into (40), (51) can be obtained. This completes the proof. □

2) Asymptotic ASC:

Again we consider $\rho \to \infty$. Based on this assumption, the asymptotic expression of the ASC is given by [56]

$$C_i^{\infty} \approx R_{B_i}^{\infty} - R_{E_i}. \tag{54}$$

To obtain it, the asymptotic expressions of User 1's ASC and the ceiling of User 2's ASC are derived in the following corollaries.

Corollary 3. *The asymptotic ASC of User 1 is given by*

$$C_1^{\infty} \approx \log_2\left(\frac{1}{a_1\rho d_{B_1}^{-\alpha_{B_1}}}\right) - \frac{E_c}{\ln(2)} - \frac{1}{\ln(2)} e^{-\frac{\lambda_e}{2}} \sum_{k=0}^{\infty} \frac{\lambda_e^k}{k! 2^k \Gamma\left(k+\frac{1}{2}\right)} \sum_{l=0}^{u_1} \omega_{1,l} \mathcal{J}_{1,1}(x_l), \tag{55}$$

where E_c denotes the Euler constant.

Proof. Based on [21], the asymptotic ergodic rate of User 1 is given by

$$R_{B_1}^{\infty} = \log_2\left(\frac{1}{a_1\rho d_{B_1}^{-\alpha_{B_1}}}\right) - \frac{E_c}{\ln(2)}. \tag{56}$$

Then, by substituting (56) into (54), (55) can be obtained. This completes the proof. □

Corollary 4. *The ceiling of C_2 in the high-SNR regime is given by*

$$C_2^{\infty} \approx \log_2(\frac{1}{a_1}) - \frac{1}{\ln(2)} e^{-\frac{\lambda_e}{2}} \sum_{k=0}^{\infty} \frac{\lambda_e^k}{k! 2^k \Gamma\left(k+\frac{1}{2}\right)} \sum_{l=0}^{u_1} \omega_{1,l} \mathcal{J}_{1,2}(x_l), \tag{57}$$

or

$$C_2^{b,\infty} \approx \log_2\left(\frac{1}{a_1\left(1+a_2\mu\rho_e d_1^{-\alpha_1} d_E^{-\alpha_E}\right)}\right). \tag{58}$$

Proof. Based on [21], the asymptotic ergodic rate of User 1 is given by

$$R_{B_2}^{\infty} = \log_2\left(1+\frac{a_2}{a_1}\right). \tag{59}$$

Then, by substituting (59) into (54), (57) can be obtained. Finally, by substituting $\rho \to \infty$ into (51), (58) can be obtained. This completes the proof. □

Remark 6. *Both the ASCs of User 1 and User 2 are affected by the number of IRS elements and by the Nakagami-m fading parameters.*

To gain deep insights into the network's performance, the high-SNR slope is worth estimating. Therefore, we first express the high-SNR slope as

$$S = \lim_{\rho\to\infty} \frac{C(\rho)}{\log_2(\rho)}. \tag{60}$$

In this analysis, we also consider $\rho \to \infty$, and maintain the consideration of arbitrary values of the average SNR of Eve's channel.

Proposition 4. *By substituting* (55) *into* (60)*, the high-SNR slope of User 1 can be illustrated as*

$$S_1 = 1. \tag{61}$$

Then upon substituting (57) *or* (58) *into* (60)*, the high-SNR slope of User 2 can be illustrated as*

$$S_2 = 0. \tag{62}$$

Remark 7. *Both the high-SNR slopes of User 1 and User 2 remain unaffected by the number of IRS elements and by the Nakagami-m fading parameters.*

Having completed the analyses of the IRS-aided network, all results related to both the secrecy diversity order and to the high-SNR slope are summarized in Table II. The orthogonal multiple access (OMA) benchmark schemes are described in [21].

TABLE II: Secrecy diversity order and high-SNR slope for the IRS-aided network

Multiple-access scheme	user	d	S
NOMA	Bob1	1	1
	Bob2	$m_s N$	0
OMA	Bob1	1	$\frac{1}{2}$
	Bob2	$m_s N$	$\frac{1}{2}$

IV. Numerical Results

In this section, our numerical results are presented for characterizing the performance of the network considered, complemented by our Monte-Carlo simulations to verify the accuracy attained. It is assumed that the power allocation coefficients of NOMA are $a_1 = 0.2$, $a_2 = 0.8$, respectively. The bandwidth of the DL is set to $BW = 1$ MHz, and the power of the AWGN is set to $\sigma^2 = -174 + 10\log_{10}(BW)$ dBm. In addition, the amplitude reflection coefficients of all the IRS elements are set to 1. The fading parameters are set to $m_1 = 3$, $m_2 = m_3 = 1$, while the distance between the BS and IRS is set to $d_1 = 100$m. The distances from IRS to User 2 and Eve are set to $d_{B2} = 10$m and $d_E = 50$m, and that of the BS to User 1 is set to $d_{B1} = 20$m. The path-loss exponents of the reflected links (i.e., BS-IRS, IRS-User 2 and IRS-Eve) and the direct link are set to $\alpha_1 = \alpha_{B2} = \alpha_E = 2.5$ and $\alpha_{B1} = 3.5$, respectively, unless otherwise stated.

As a benchmark, we consider the imperfect CSI scenario. Because of the passive nature of the IRS, the CSI of the reflected links is much more challenging to obtain than that of the direct link. Therefore, we assume that the CSI of the direct link is perfect, while the CSI of the reflected links is imperfect. The estimated reflected links can be represented as $\bar{\mathbf{h}}_{B2} = \bar{\mathbf{g}}_{B2}\bar{\Phi}\bar{\mathbf{h}}$, where the elements of $\bar{\mathbf{g}}_{B2}$, $\bar{\mathbf{h}}$ and $\bar{\Phi}$ can be represented as $\bar{g}_{2,n} = g_{2,n} - \Delta g_{2,n}$, $\bar{h}_n = h_n - \Delta h_n$ and $\bar{\Phi}_n = \beta_n\phi_n e^{j(-\text{angle}(\Delta g_{2,n})-\text{angle}(\Delta h_n))}$, respectively. Specifically, $\Delta g_{2,n}$ and Δh_n are zero-mean complex-valued circularly symmetric Gaussian variables with a variance of 1. Furthermore, in order to illustrate the rationality of our assumption, we also compare the secrecy performance when the signals received by the Eve are co-phase and random phase.

A. Secrecy outage probability

For comparisons, we regard the IRS-aided OMA network as the benchmark. Specifically, an IRS is employed for providing legitimate access service to User 2 as well as for the

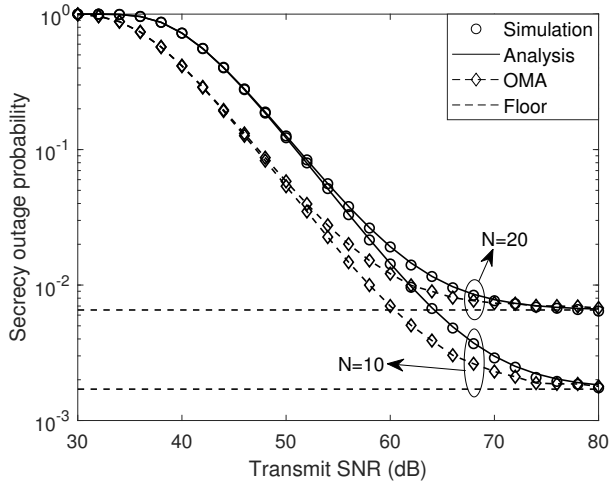


Fig. 2: The SOP of User 1 versus the transmit SNR. The analytical results and the floor are calculated from (19) and (33).

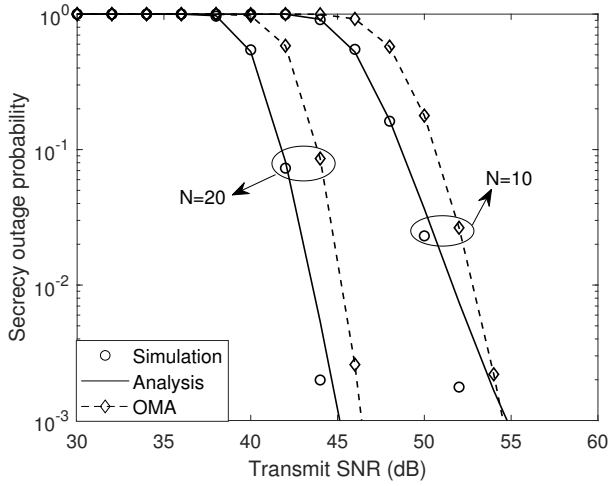


Fig. 3: The SOP of User 2 versus the transmit SNR. The analytical results are calculated from (21).

illegitimate access of Eve to the BS. In Fig. 2 to Fig. 5, we investigate the SOP, when the targeted secrecy capacity of the paired NOMA users is assumed to be $R_1 = R_2 = 100$Kbps, which corresponds to the scenario considered in Section III-B.

Fig. 2 plots the SOP of User 1 versus the transmit SNR for different number of IRS elements. It confirms the close agreement between the simulation and analytical results. A specific observation is that the SOP of User 1 reduces upon reducing the number of IRS elements, because the number of IRS elements has no effect on the channel gain of User 1. By contrast, the channel gain of Eve increases, as the number of IRS elements increases. As a benchmark, the SOP curves of the IRS-aided OMA network are plotted for comparison. We observe that for User 1 in the IRS-aided OMA network has a better performance than that in the IRS-aided NOMA network in the high-SNR regime. This is because the transmit power allocated to User 1 in the NOMA network is lower than that in the OMA network due to the influence of the power allocation factor. As the transmit SNR increases, we find that the SOP of User 1 tends to a constant, which is consistent with **Proposition 2**.

Fig. 3 plots the SOP of User 2 versus the transmit SNR. We observe that, owing to the CLT of the channel statistics of User 2, the analytical results are accurate in the low-SNR regime, but inaccurate in the high-SNR regime. As a benchmark, the SOP curves of the IRS-aided OMA network are also plotted for comparison. We observe that the performance of User 2 in the IRS-aided NOMA network is better than that of the IRS-aided OMA network. This is because the transmit power allocated to User 2 in the NOMA network is higher than that in the OMA network due to the influence of the power allocation factor.

Since the SOP of User 2 in the high-SNR regime is not accurate in Fig. 3, we further plot the high-SNR asymptotic curves in the cases of $N = 1$ and $N = 3$ in Fig. 4. We observe that the SOPs of User 1 and User 2 gradually approach their

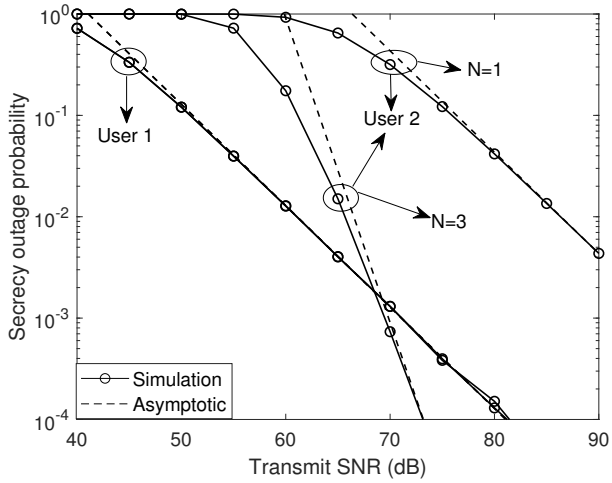


Fig. 4: Asymptotic SOP versus the transmit power results in the case of $\rho_e = 10$ dB. The asymptotic results are calculated from (32) and (34).

respective asymptotic curves, which validates our analysis. Furthermore, we also observe that in the cases of $N = 1$ and $N = 3$, the secrecy diversity orders of User 1 are both 1 and the secrecy diversity orders of User 2 are 1 and 3, respectively, which is consistent with **Remark 2** and **Remark 3**.

In Fig. 5, the SOP curves versus the number of IRS elements are depicted. We observe that, since we have global CSI for User 1, the SOP of User 1 is accurate. On the other hand, the SOP of User 2 is accurate in the low-SNR regime. However, the SOP of User 2 is inaccurate in the high-SNR regime, owing to using the CLT-based channel statistics of User 2. We also observe that the SOP of User 1 increases as the number of IRS elements increases since the ergodic rate of User 1 is not affected by the number of IRS elements. By contrast, the SOP of User 2 decreases as the number of IRS elements increases, when the number of IRS elements is small, since the IRS-aided transmissions to Eve experience more severe path-loss

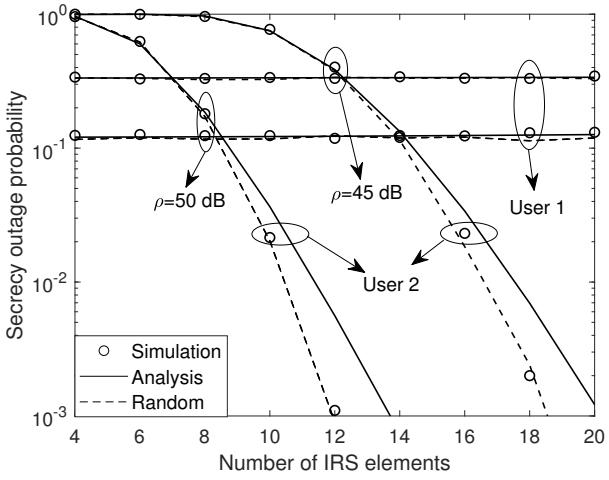


Fig. 5: The SOP versus the number of IRS elements. The analytical results are calculated from (19) and (21).

then that destined for User 2. We also find that the SOPs of the RIS-aided NOMA network are equal when the signals received by the Eve are co-phase and random phase, which shows that our assumption, the signals received by the Eve are co-phase, is reasonable.

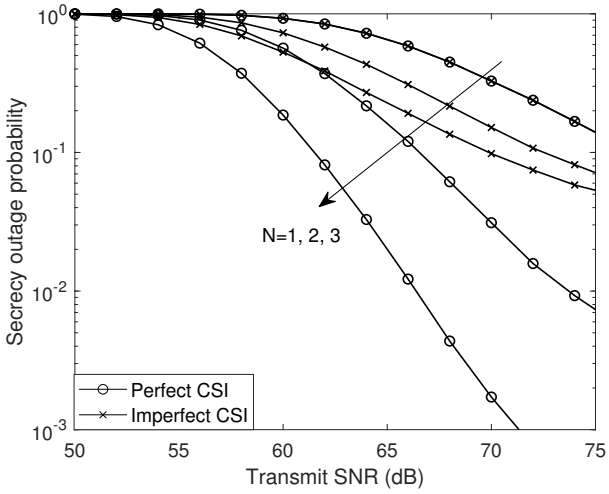


Fig. 6: The SOP of User 2 in both the perfect and imperfect CSI scenarios versus the transmit SNR.

In Fig. 6, the SOP of User 2 encountered in both the perfect and imperfect CSI scenarios versus the transmit SNR are depicted. We observe that, with $N = 1$, the SOP of perfect CSI is equal to the SOP of imperfect CSI. This is because, when $N = 1$, we do not have to consider whether the signals received at User 2 are co-phase or not. However, when $N = 2$ and $N = 3$, we observe that the SOP of imperfect CSI is worse than that of perfect CSI. We can also observe that as the transmit SNR and N increase, the gap between the SOP of perfect CSI and imperfect CSI increases. This is because the IRS design process treats the estimated CSI as perfect CSI, which results in energy leakage to User 2.

B. Average Secrecy Capacity

In this subsection, the number of points for the Chebyshev-Gauss and Gauss-Laguerre quadratures are set to $u_1 = u_2 = 100$. In Fig. 7 and Fig. 8, we investigate the ASC of the IRS-aided NOMA network, which corresponds to the scenario considered in Section III-C.

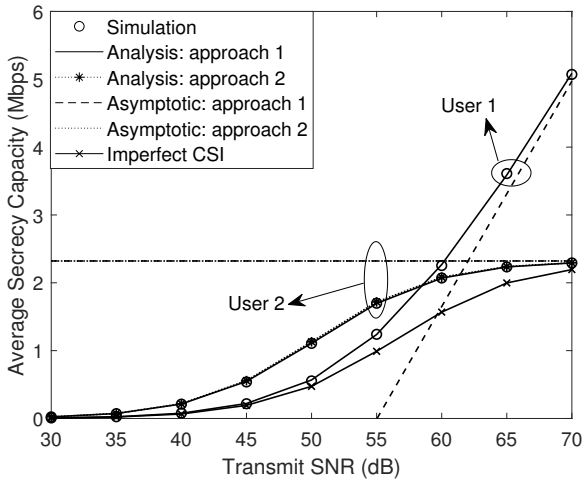


Fig. 7: The ASC versus the transmit SNR in the case of N=30 and $\rho_e = 30$ dB. The analytical results are calculated from (46), (48) and (51), respectively. The asymptotic curves are calculated from (55), (57) and (58), respectively.

In Fig. 7, the ASC curves for the IRS-aided NOMA network are depicted. On the one hand, for User 1, we observe that the simulation results match well with the analytical results, and the asymptotic results derived are accurate. On the other hand, for User 2, we observe that the analytical results both of approaches are highly accurate. Furthermore, the asymptotic results derived both from (57) and (58) are also accurate. Additionally, we observe that the high-SNR slope of User 1 is 1, which coincides with **Proposition 4**. While the ASC of User 2 approaches a ceiling in the high-SNR regime, which coincides with **Corollary 4**. We also assume having imperfect CSI for the reflected links. It can be observed that the imperfect CSI increases the secrecy outage probability of User 2 in the low-SNR regime, and that does not affect the performance in the high-SNR regime due to the properties of downlink NOMA.

Fig. 8 plots the ASC of an IRS-aided NOMA network versus the number of IRS elements and the transmit SNR, in the case of $\rho_e = \rho$. We assume that the transmit SNR of the paired NOMA users and Eve are identical. For User 1, we can observe that the ASC increases as the transmit SNR increases, since the BS-IRS-Eve links experience more severe path-loss then the BS-User 1 link. We can also observe the ASC of User 1 decreases upon increasing the number of IRS elements, since the ergodic rate of User 1 is not affected by the number of IRS elements, while the ergodic rate of Eve increases upon increasing the number of IRS elements. For User 2, we observe that the ASC increases as the number of IRS elements as well as the transmit SNR increase, up to

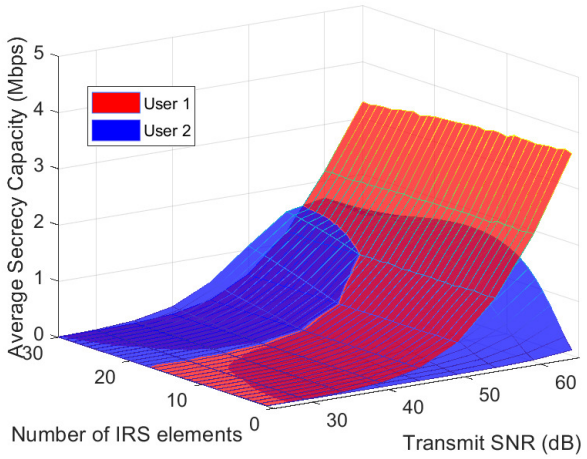


Fig. 8: The ASC versus the numbers of IRS elements and the transmit SNR, in the case of $\rho_e = \rho$.

the ceiling given by **Corollary 4** and then decreases as the number of IRS elements or the transmit SNR increase. This is because Eve has strong eavesdropping capability, which leads to an ergodic rate increase of Eve as increase the transmit SNR and the number of IRS elements is.

V. Conclusions

In this paper, the secrecy performance of IRS-aided NOMA networks was studied. Specifically, we first derived new channel gain expressions for the reflected links. Then, based on the new channel statistics, the closed-form SOP and ASC expressions were derived. Numerical results were presented for validating our results. Furthermore, the secrecy diversity orders and the high-SNR slopes have also been determined. The presence of the direct link between the BS and the cell-edge user as well as Eve deserves further investigation in our future research.

Appendix A: Proof of Lemma 2

Firstly, according to [21], the CDF of $X = \frac{\left(\sum_{n=1}^{N}|g_{2,n}||h_n|\right)^2}{N(1-\epsilon)}$ in the low-SNR regime is given by

$$F_X(x) = 1 - Q_{\frac{1}{2}}\left(\sqrt{\lambda}, \sqrt{x}\right) \tag{A.1}$$

Hence, the CDF of γ_{B2} in the low-SNR regime can be derived as

$$\begin{aligned} F_{\gamma_{B2}}(x) &= \mathbb{P}\left(\gamma_{B2} < x\right) \\ &= F_X\left(\frac{x}{N(1-\epsilon)\rho(a_2 - a_1 x)d_1^{-\alpha_1}d_{B2}^{-\alpha_{B2}}}\right) \\ &= 1 - Q_{\frac{1}{2}}\left(\sqrt{\lambda}, \sqrt{\frac{x}{N(1-\epsilon)\rho(a_2 - a_1 x)d_1^{-\alpha_1}d_{B2}^{-\alpha_{B2}}}}\right). \end{aligned} \tag{A.2}$$

Then, according to [21], the CDF of $Y = \sum_{n=1}^{N}|g_{2,n}||h_n|$ in the high-SNR regime is given by

$$F_Y(y) = \Xi\gamma\left(2m_s N, 2\sqrt{m_s m_l}y\right). \tag{A.3}$$

Therefore, the CDF of γ_{B2} in the high-SNR regime can be formulated as

$$\begin{aligned} F_{\gamma_{B2}}^{0_+}(x) &= \mathbb{P}\left(\gamma_{B2} < x\right) \\ &= F_Y\left(\sqrt{\frac{x}{\rho(a_2 - a_1 x)d_1^{-\alpha_1}d_{B2}^{-\alpha_{B2}}}}\right) \\ &= \Xi\gamma\left(2m_s N, \frac{2\sqrt{m_s m_l x}}{\sqrt{\rho(a_2 - a_1 x)d_1^{-\alpha_1}d_{B2}^{-\alpha_{B2}}}}\right). \end{aligned} \tag{A.4}$$

This completes the proof.

Appendix B: Proof of Lemma 3

By stipulating that $z_n = |g_{q,n}||h_n|$, and that f_{z_n} is the probability density function (PDF) of z_n, according to [21], the Laplace transform of f_{z_n} is given in (B.1) shown at the top of next page.

Assuming that f_Z is the PDF of Z, the Laplace transform of f_Z is given by

$$\mathcal{L}_{f_Z}(s) = \underbrace{\omega^N(s+d)^{-aN}}_{f(s)}\underbrace{\left({}_2F_1\left(a, b; c; \frac{s-d}{s+d}\right)\right)^N}_{g(s)}. \tag{B.2}$$

According to the relationship between the Laplace transform and moments, we have

$$\mathbb{E}(Z^2) = \mathcal{L}_{f_Z}^{''}(0). \tag{B.3}$$

From (B.2), we have

$$\mathcal{L}_{f_Z}^{'}(s) = J_1(s) + J_2(s)J_4(s), \tag{B.4}$$

where

$$J_1(s) = -aN\omega^N(s+d)^{-aN-1}g(s), \tag{B.5}$$

$$J_2(s) = f(s)\underbrace{N\left({}_2F_1\left(a, b; c; \frac{s-d}{s+d}\right)\right)^{N-1}}_{J_3(s)}, \tag{B.6}$$

and

$$J_4(s) = \frac{ab}{c}{}_2F_1\left(a+1, b+1; c+1; \frac{s-d}{s+d}\right)\frac{2d}{(s+d)^2}. \tag{B.7}$$

Furthermore, we have

$$\mathcal{L}_{f_Z}^{''}(s) = J_1^{'}(s) + J_2^{'}(s)J_4(s) + J_2(s)J_4^{'}(s), \tag{B.8}$$

where $J_1^{'}(s)$, $J_2^{'}(s)$ and $J_4^{'}(s)$ are given in (B.9), (B.10) and (B.11) at the top of next page.

By substituting $s = 0$ into J_2, J_4, (B.9), (B.10) and (B.11), we have

$$J_2(0) = \omega^N d^{-aN} N k_1^N, \tag{B.12}$$

$$J_4(0) = \frac{2ab}{cd}k_2, \tag{B.13}$$

$$J_1^{'}(0) = \frac{aN\omega^N k_1^{N-1}}{d^{aN+2}}\left((aN+1)k_1 - \frac{2abNk_2}{c}\right), \tag{B.14}$$

$$\mathcal{L}_{f_{z_n}}(s) = \omega(s+2\sqrt{m_c m_d})^{-2m_c}{}_2F_1\left(2m_c, m_c-m_d+\frac{1}{2}; m_c+m_d+\frac{1}{2}; \frac{s-2\sqrt{m_c m_d}}{s+2\sqrt{m_c m_d}}\right). \tag{B.1}$$

$$J_1^{'}(s) = aN(aN+1)\omega^N(s+d)^{-aN-2}g(s) - aN\omega^N(s+d)^{-aN-1}J_3(s)J_4(s), \tag{B.9}$$

$$J_2^{'}(s) = -aN\omega^N(s+d)^{-aN-1}J_3(s) + f(s)N(N-1)\left({}_2F_1\left(a,b;c;\frac{s-d}{s+d}\right)\right)^{N-2}J_4(s), \tag{B.10}$$

$$\begin{aligned} J_4^{'}(s) = {} & \frac{2abd}{c}(-2)(s+d)^{-3}{}_2F_1\left(a+1,b+1;c+1;\frac{s-d}{s+d}\right) + \\ & \frac{2abd}{c(s+d)^2}\frac{(a+1)(b+1)}{c+1}{}_2F_1\left(a+2,b+2;c+2;\frac{s-d}{s+d}\right)\frac{2d}{(s+d)^2}. \end{aligned} \tag{B.11}$$

$$J_2^{'}(0) = \frac{\omega^N N k_1^{N-2}}{d^{aN+1}}\left(\frac{2ab}{c}(N-1)k_2 - aNk_1\right), \tag{B.15}$$

$$J_4^{'}(0) = \frac{4a(a+1)b(b+1)}{c(c+1)d^2}k_3 - \frac{4ab}{cd^2}k_2. \tag{B.16}$$

Then, by substituting (B.12)-(B.16) into (B.8), and after some further mathematical manipulations, (16) can be obtained. This completes the proof.

Appendix C: Proof of **Theorem 3**

Based on the above assumptions, the CDF of γ_{E_i} in the low-SNR regime can be expressed as

$$\begin{aligned} F_{\gamma_{E_i}}(x) &= F_X\left(\frac{x}{a_i\rho_e N(1-\epsilon_e)d_1^{-\alpha_1}d_E^{-\alpha_E}}\right) \\ &= 1 - Q_{\frac{1}{2}}\left(\sqrt{\lambda_e}, \sqrt{\frac{x}{a_i\rho_e N(1-\epsilon_e)d_1^{-\alpha_1}d_E^{-\alpha_E}}}\right) \\ &= e^{-\frac{\lambda_e}{2}}\sum_{k=0}^{\infty}\frac{\lambda_e^k\gamma\left(k+\frac{1}{2}, \frac{x}{2a_i\rho_e N(1-\epsilon_e)d_1^{-\alpha_1}d_E^{-\alpha_E}}\right)}{k!2^k\Gamma\left(k+\frac{1}{2}\right)}, \end{aligned} \tag{C.1}$$

where we have $\epsilon_e = \frac{1}{m_1 m_3}\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\right)^2\left(\frac{\Gamma(m_3+\frac{1}{2})}{\Gamma(m_3)}\right)^2$ and $\lambda_e = \frac{N\epsilon_e}{1-\epsilon_e}$.

Therefore, the ergodic rate of Eve can be expressed as

$$\begin{aligned} R_{E_i} &= \mathbb{E}\left(\log_2(1+\gamma_{E_i})\right) \\ &= \int_0^{\infty}\log_2(1+x)df_{\gamma_{E_i}}(x) \\ &= \int_0^{\infty}(1-F_{\gamma_{E_i}}(x))d\log_2(1+x) \\ &= \frac{1}{\ln(2)}e^{-\frac{\lambda_e}{2}}\sum_{k=0}^{\infty}\frac{\lambda_e^k}{k!2^k\Gamma\left(k+\frac{1}{2}\right)}J_{5,i}, \end{aligned} \tag{C.2}$$

where

$$J_{5,i} = \int_0^{\infty}\frac{\Gamma\left(k+\frac{1}{2}\right) - \gamma\left(k+\frac{1}{2}, \frac{x}{2a_i\rho_e N(1-\epsilon_e)d_1^{-\alpha_1}d_E^{-\alpha_E}}\right)}{1+x}dx. \tag{C.3}$$

Next, by using the Gauss-Laguerre quadrature, (C.3) can be rewritten as

$$J_{5,i} \approx \sum_{l=0}^{n}\omega_{5,l}\mathcal{J}_5(x_{5,l}), \tag{C.4}$$

where $x_{5,l}$ is the l-th root of the Laguerre polynomial $L_n(x)$, the weight $\omega_{5,l}$ is given by

$$w_{5,l} = \frac{x_l}{(n+1)^2\left[L_{n+1}(x_l)\right]^2}, \tag{C.5}$$

and

$$\mathcal{J}_{5,i}(x) = \frac{\Gamma\left(l+\frac{1}{2}\right) - \gamma\left(l+\frac{1}{2}, \frac{t}{a_i}\right)}{1+x}e^x, \tag{C.6}$$

with $t = \frac{x}{2\rho_e N(1-\epsilon_e)d_1^{-\alpha_1}d_E^{-\alpha_E}}$. This completes the proof.

References

[1] Z. Tang, T. Hou, Y. Liu, and J. Zhang, "Secrecy performance analysis for reconfigurable intelligent surface aided NOMA network," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada*, Jun. 2021, pp. 1–6.

[2] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Aug. 2019.

[3] Ö. Özdogan, E. Björnson, and E. G. Larsson, "Intelligent reflecting surfaces: Physics, propagation, and pathloss modeling," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 581–585, Dec. 2019.

[4] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Nov. 2019.

[5] R. Alghamdi, R. Alhadrami, D. Alhothali, H. Almorad, A. Faisal, S. Helal, R. Shalabi, R. Asfour, N. Hammad, A. Shams *et al.*, "Intelligent surfaces for 6G wireless networks: A survey of optimization and performance analysis techniques," *IEEE Access*, vol. 8, pp. 202 795 – 202 818, Oct. 2020.

[6] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Jun. 2019.

[7] M. Di Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. C. Alexandropoulos, J. Hoydis, H. Gacanin *et al.*, "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, May 2019.

[8] M. Di Renzo and J. Song, "Reflection probability in wireless networks with metasurface-coated environmental objects: An approach based on random spatial processes," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 99, Apr. 2019.

[9] T. Hou, Y. Liu, Z. Song, X. Sun, and Y. Chen, "MIMO-NOMA networks relying on reconfigurable intelligent surface: A signal cancellation-based design," *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 6932–6944, Nov. 2020.

[10] H. Wang, Z. Zhang, B. Zhu, J. Dang, L. Wu, L. Wang, K. Zhang, and Y. Zhang, "Performance of wireless optical communication with reconfigurable intelligent surfaces and random obstacles," *arXiv preprint arXiv:2001.05715*, Jan. 2020.

[11] W. Shi, X. Zhou, L. Jia, Y. Wu, F. Shu, and J. Wang, "Enhanced secure wireless information and power transfer via intelligent reflecting surface," *IEEE Commun. Lett.*, vol. 25, no. 4, pp. 1084–1088, Apr. 2020.

[12] Q. Wu and R. Zhang, "Weighted sum power maximization for intelligent reflecting surface aided SWIPT," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 586–590, Dec. 2019.

[13] S. Gopi, S. Kalyani, and L. Hanzo, "Intelligent reflecting surface assisted beam index-modulation for millimeter wave communication," *IEEE Trans. Wireless Commun.*, vol. 20, no. 2, pp. 983–996, Feb. 2021.

[14] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Non-orthogonal multiple access for 5G and beyond," *IEEE Proc.*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[15] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[16] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[17] S. Li, M. Derakhshani, S. Lambotharan, and L. Hanzo, "Outage probability analysis for the multi-carrier NOMA downlink relying on statistical CSI," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3572–3587, Jun. 2020.

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

[19] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Sep. 2015.

[20] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen, and L. Hanzo, "Reconfigurable intelligent surface aided NOMA networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2575–2588, Nov. 2020.

[21] Y. Cheng, K. H. Li, Y. Liu, K. C. Teh, and H. V. Poor, "Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, pp. 3988–4000, Jun. 2021.

[22] Z. Ding and H. V. Poor, "A simple design of IRS-NOMA transmission," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1119–1123, May 2020.

[23] X. Yue and Y. Liu, "Performance analysis of intelligent reflecting surface assisted NOMA networks," *arXiv preprint arXiv:2002.09907*, Jun. 2020.

[24] X. Mu, Y. Liu, L. Guo, J. Lin, and N. Al-Dhahir, "Exploiting intelligent reflecting surfaces in multi-antenna aided NOMA systems," *arXiv preprint arXiv:1910.13636*, Jun. 2019.

[25] M. Fu, Y. Zhou, and Y. Shi, "Reconfigurable intelligent surface empowered downlink non-orthogonal multiple access," *IEEE Transactions on Communications*, Early Access, 2021.

[26] C. Zhang, W. Yi, Y. Liu, Z. Qin, and K. K. Chai, "Downlink analysis for reconfigurable intelligent surfaces aided NOMA networks," in *2020 IEEE Global Communications Conference (GLOBECOM 2020)*, Taipei, China, Jun. 2020, pp. 1–6.

[27] W. Ni, X. Liu, Y. Liu, H. Tian, and Y. Chen, "Resource allocation for multi-cell IRS-aided NOMA networks," *IEEE Trans. Wireless Commun.*, Early Access, 2021.

[28] J. Zuo, Y. Liu, E. Basar, and O. A. Dobre, "Intelligent reflecting surface enhanced millimeter-wave NOMA systems," *IEEE Commun. Lett.*, vol. 24, no. 11, pp. 2632–2636, Nov. 2020.

[29] X. Liu, Y. Liu, Y. Chen, and H. V. Poor, "RIS enhanced massive non-orthogonal multiple access networks: Deployment and passive beamforming design," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 4, pp. 1057–1071, Apr. 2021.

[30] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[31] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[32] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[33] A. Almohamad, A. M. Tahir, A. Al-Kababji, H. M. Furqan, T. Khattab, M. O. Hasna, and H. Arslan, "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1442–1456, Sep. 2020.

[34] L. Yang, Y. Jinxia, W. Xie, M. Hasna, T. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 296–12 300, Oct. 2020.

[35] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, May 2019.

[36] L. Yang and Y. Yuan, "Secrecy outage probability analysis for RIS-assisted NOMA systems," *Electronics Letters*, vol. 56, no. 23, pp. 1254–1256, Nov. 2020.

[37] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jan. 2020.

[38] H. Long, M. Chen, Z. Yang, B. Wang, Z. Li, X. Yun, and M. Shikh-Bahaei, "Reflections in the sky: Joint trajectory and passive beamforming design for secure UAV networks with reconfigurable intelligent surface," *arXiv preprint arXiv:2005.10559*, Jun. 2020.

[39] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, X. Li, M. Quiroz-Castellanos, and R. Kharel, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," *arXiv preprint arXiv:2004.11288*, Apr. 2020.

[40] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[41] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in RIS-aided MISO systems with hardware impairments," *IEEE Wireless Commun. Lett.*, Early Access, 2021.

[42] P. K. Sharma and P. Garg, "Intelligent reflecting surfaces to achieve the full-duplex wireless communication," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 622–626, Feb. 2021.

[43] S. Atapattu, R. Fan, P. Dharmawansa, G. Wang, and J. Evans, "Two–way communications via reconfigurable intelligent surface," in *2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea (South)*, Jun. 2020, pp. 1–6.

[44] L. Yang, F. Meng, Q. Wu, D. B. da Costa, and M. S. Alouini, "Accurate closed-form approximations to channel distributions of RIS-aided wireless systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 1985–1989, Nov. 2020.

[45] H. Ibrahim, H. Tabassum, and U. T. Nguyen, "Exact coverage analysis of intelligent reflecting surfaces with Nakagami-m channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1072–1076, Jan. 2021.

[46] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[47] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Sep. 2020.

[48] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Jun. 2019.

[49] S. Li, B. Duo, M. D. Renzo, M. Tao, and X. Yuan, "Robust secure UAV communications with the aid of reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6402–6417, Oct. 2021.

[50] S. Zhang, H. Zhang, B. Di, Y. Tan, M. Di Renzo, Z. Han, H. Vincent Poor, and L. Song, "Intelligent omni-surfaces: Ubiquitous wireless transmission by reflective-refractive metasurfaces," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 219–233, Jan. 2022.

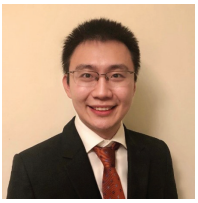
[51] Y. Ni, Y. Liu, J. Wang, Q. Wang, H. Zhao, and H. Zhu, "Performance analysis for RIS-assisted D2D communication under Nakagami-m fading," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5865–5879, Jun. 2021.

[52] D. Selimis, K. P. Peppas, G. C. Alexandropoulos, and F. I. Lazarakis, "On the performance analysis of RIS-empowered communications over Nakagami-m fading," *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2191–2195, Jul. 2021.

[53] Z.-Q. He and X. Yuan, "Cascaded channel estimation for large intelligent metasurface assisted massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 210–214, Feb. 2020.
[54] H. Liu, X. Yuan, and Y.-J. A. Zhang, "Matrix-calibration-based cascaded channel estimation for reconfigurable intelligent surface assisted multiuser MIMO," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2621–2636, Nov. 2020.
[55] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam, The Netherlands: Elsevier, 2007.
[56] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. Nkouatchah, and U. S. Dias, "Transmit antenna selection in secure MIMO systems over $\alpha - \mu$ fading channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, Jun. 2019.

Zhiqing Tang received the M.Sc. degree in information and communication engineering from Zhengzhou University, where he is currently pursuing the Ph.D. degree in information and communication engineering with the School of Information Engineering. His research interests include 5G/6G networks, wireless communications theory, non-orthogonal multiple access, Reconfigurable intelligent surface, relay communications, and physical layer security.

Tianwei Hou received the M.Sc. and Ph.D. degrees from Beijing Jiaotong University in 2016 and 2021, respectively, all in Information and Communication Engineering. He has been an associate professor with the School of Electronic and Information Engineering at Beijing Jiaotong University since 2021. His research interests include 5G/6G networks, wireless communications theory, non-orthogonal multiple access, UAV communications, Reconfigurable intelligent surface, Integrated sensing and communication (ISaC) and Internet of Things.



Yuanwei Liu (S13M16SM19, http://www.eecs.qmul.ac.uk/ yuanwei) received the B.S. and M.S. degrees from the Beijing University of Posts and Telecommunications in 2011 and 2014, respectively, and the PhD degree in electrical engineering from the Queen Mary University of London, U.K., in 2016. He was with the Department of Informatics, Kings College London, from 2016 to 2017, where he was a Post-Doctoral Research Fellow. He has been a Senior Lecturer (Associate Professor) with the School of Electronic Engineering and Computer Science, Queen Mary University of London, since Aug. 2021, where he was a Lecturer (Assistant Professor) from 2017 to 2021. His research interests include non-orthogonal multiple access, 5G/6G networks, RIS, integrated sensing and communications, and machine learning.

Yuanwei Liu is a Web of Science Highly Cited Researcher 2021. He is currently a Senior Editor of IEEE Communications Letters, an Editor of the IEEE Transactions on Wireless Communications and the IEEE Transactions on Communications. He serves as the leading Guest Editor for IEEE JSAC special issue on Next Generation Multiple Access, a Guest Editor for IEEE JSTSP special issue on Signal Processing Advances for Non-Orthogonal Multiple Access in Next Generation Wireless Networks. He received IEEE ComSoc Outstanding Young Researcher Award for EMEA in 2020. He received the 2020 IEEE Signal Processing and Computing for Communications (SPCC) Technical Early Achievement Award, IEEE Communication Theory Technical Committee (CTTC) 2021 Early Achievement Award. He received IEEE ComSoc Young Professional Outstanding Nominee Award in 2021. He has served as the Publicity Co-Chair for VTC 2019-Fall. He is the leading contributor for Best Readings for Non-Orthogonal Multiple Access (NOMA) and the primary contributor for Best Readings for Reconfigurable Intelligent Surfaces (RIS). He serves as the chair of Special Interest Group (SIG) in SPCC Technical Committee on the topic of signal processing Techniques for next generation multiple access (NGMA), the vice-chair of SIG Wireless Communications Technical Committee (WTC) on the topic of Reconfigurable Intelligent Surfaces for Smart Radio Environments (RISE), and the Tutorials and Invited Presentations Officer for Reconfigurable Intelligent Surfaces Emerging Technology Initiative.

Jiankang Zhang (Senior Member, IEEE) is currently a Senior Lecturer with Bournemouth University, U.K. Prior to joining in Bournemouth University, he was a Senior Research Fellow with the University of Southampton, Southampton, U.K. He was a Lecturer from 2012 to 2013 and then an Associate Professor from 2013 to 2014 with Zhengzhou University, Zhengzhou, China. His research interests include the areas of aeronautical communications, aeronautical networks, evolutionary algorithms, and edge computing. He is an Associate Editor for the IEEE Access.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) (FIEEE'04, Fellow of the Royal Academy of Engineering F(REng), of the IET and of EURASIP), received his Master degree and Doctorate in 1976 and 1983, respectively from the Technical University (TU) of Budapest. He was also awarded the Doctor of Sciences (DSc) degree by the University of Southampton (2004) and Honorary Doctorates by the TU of Budapest (2009) and by the University of Edinburgh (2015). He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He has served several terms as Governor of both IEEE ComSoc and of VTS. He has published 2000+ contributions at IEEE Xplore, 19 Wiley-IEEE Press books and has helped the fast-track career of 123 PhD students. Over 40 of them are Professors at various stages of their careers in academia and many of them are leading scientists in the wireless industry.