Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1498918, 15 pages
https://doi.org/10.1155/2022/1498918

Research Article

Empowering Reconfigurable Intelligent Surfaces for Security of Downlink NOMA

Nhan Duc Nguyen,[1] **Minh-Sang Van Nguyen**,[2] **and Munyaradzi Munochiveyi**[3]

[1]*Faculty of Mechanical-Electrical and Computer Engineering, School of Engineering and Technology, Van Lang University, 69/ 68 Dang Thuy, Tram Street, Ward 13, Binh Thanh District, 70000 Ho Chi Minh City, Vietnam*
[2]*Faculty of Electronics Technology, Industrial University of ho chi Minh City (IUH), Ho Chi Minh City, Vietnam*
[3]*Electrical and Electronics Engineering Department, University of Zimbabwe, Mount Pleasant, Harare, Zimbabwe*

Correspondence should be addressed to Munyaradzi Munochiveyi; mmunochiveyi@eng.uz.ac.zw

Received 3 March 2022; Revised 25 April 2022; Accepted 6 May 2022; Published 25 May 2022

Academic Editor: Han Wang

Reconfigurable intelligent surfaces (RIS) and non-orthogonal multiple access (NOMA) are promising techniques to develop next-generation wireless systems. While RIS has huge potential to create massive device connectivity, NOMA exhibits its spectrum efficient communication among multiple access approaches. RIS is a passive device made up of low-cost meta-surfaces which can control the propagation of radio waves, and it is easily deployable in lots of applications in the Internet of Things. The full-duplex nature of RIS has also been a major reason for its consideration of major emerging and trending technologies. In this paper, we aim to investigate the secrecy performance of the RIS-NOMA-assisted Internet of Things (IoT) systems in the presence of two legitimate users who belong to a cluster, and those devices are associated with the existence of an eavesdropper situated close to such a cluster. This paper considers the devices in the presence of RIS and an eavesdropper. As main performance metrics, the closed-form expressions for secrecy outage probability (SOP) and strictly positive secrecy capacity (SPSC) are derived to evaluate the performance of legitimate users. Simulations are performed in support of the Monte-Carlo method, and the obtained results show that in most of the cases, the number of meta-surfaces in RIS and signal-to-noise ratio (SNR) levels at the source also plays a pivotal role in influencing the secure performance of the system.

1. Introduction

RIS is a passive device that is made of low-cost meta-surfaces which can control the propagation of radio waves impinging on it, according to the position of the receiver [1]. Also, RIS is a passive device that does not rely on any external energy sources and performs the signal transmission using soft programming. Also, RIS can work in full-duplex mode communication, which makes it a perfect choice for enabling massive device connectivity. Even though the idea of RIS devices came into existence a couple of years back, there is currently immense research work and publications available in various journals on this topic. Primarily, the researchers have focused on integrating this technology with various trending and emerging technologies such as NOMA, cognitive radio (CR) systems, visible light communications (VLC), and physical layer security (PLS) [2–4]. Consequently, increased research work is being performed in enhancing secrecy efficiency and PLS, as the day-to-day privacy concerns of the users' increase. Therefore, in the following subsection, we introduce in detail various works related to our research.

1.1. Related Works. The integration of RIS with underlay CR network has been considered in [5], and the SOP performance is investigated in the presence of interference from the secondary network to the primary network. In [6], the authors have an intelligent reflecting surface– (IRS–) assisted mmWave system operating in the presence of CR networks to perform robust secure transmission under imperfect channel state information (CSI) conditions. The performance was analyzed in terms of achievable secrecy rate, and the proposed algorithm indicated that it had a better performance compared to traditional

systems. In [7], the authors considered a multiple-input-multiple-output– (MIMO–) aided RIS system with secure wireless information and power transfer (SWIPT) technique. The authors also considered multiple antennas at the sender, receiver, and energy receiver (ER), where ER is assumed to be the potential eavesdropper in the network. Moreover, the authors proposed various techniques to improve the efficiency of the secrecy performance of the system. A similar system in an orthogonal frequency division multiple access– (OFDM) aided systems was considered in [8], where passive beamforming and joint optimization with alternating optimization were proposed techniques to enhance the secrecy performance of the system. In [9], the authors considered a deep learning-based approach for RIS systems in the PLS perspective to maximize the secrecy rate performance of the legitimate user in real time, based on the reflecting elements in the system. The results showed that the proposed method achieved better performance, as well as reduced computational complexity. In [10], the authors investigated the performance of beamforming and RIS design to analyze and enhance the security of multiple-input single-output– (MISO–) assisted RIS system. Two designs were proposed, which are as follows: low-computational complexity successive design and high-security performance joint design. Both designs achieved better secrecy performance compared to the traditional existing systems.

In [11], the authors considered RIS-enabled IoT network when the Fisher-Snedecor $\mathcal{F}$ model is utilized to analyze the generalized composite fading and shadowing model effect. The authors performed the analysis in terms of average capacity, bit error rate, and outage probability. The results demonstrated that employing the proposed model is beneficial in the considered system and achieves efficient performance over the other fading models. Furthermore, RIS-assisted satellite for IoT network is proposed in [12]. The installation of reflecting surfaces on satellites is proposed to enhance the broadcasting and beamforming of the signal with significant gains. The study showed that up to 10^5 times increase in the uplink and downlink achievable rates of IoT networks can be obtained. In [13], the authors considered a RIS system with multiple antennas at the base station (BS) serving multiple users with single antennas on the ground. The authors also proposed a joint optimization at the BS and RIS to minimize the system sum mean squared error. The numerical results demonstrated that the proposed technique and algorithm outperformed traditional systems, whereas in [14], the authors considered RIS to enhance the performance of wireless power transfer (WPT) in the presence of mobile edge computing (MEC) IoT network. Various optimizations techniques were performed at the RIS, MEC, and WPT; subsequently, a reinforcement learning method is adopted to effectively overcome the nonconvex problems. The numerical results showed the effective and beneficial performance of the proposed system and method. Similarly in [15], resource allocation was studied for RIS-assisted wireless powered frequency division multiple access (FDMA) IoT networks. With the aid of passive beamforming reflectors at the RIS, the wireless energy transfer (WET) and wireless information transfer (WIT) have also been efficiently improved by applying various optimization algorithms. The performance of the system was analyzed in terms of system throughput, transmission time scheduling, and energy harvesting, and the demonstrated results proved to be effective compared to the traditional systems.

However, the aforementioned works have not considered secure RIS-NOMA systems; hence, this has motivated us to derive main equations of secure performance along with detailed evaluations of these equations.

1.2. Our Contributions and Organization. In this paper, we aim to analyze the secrecy performance of the RIS-NOMA system in the presence of two legitimate users located in a cluster and an eavesdropper, both possessing single antennas. Two cases were considered in the research, i.e., with and without a direct link between devices in the presence of a RIS device. The primary contributions of the papers are as follows:

(i) To characterize secure performance, we rely on the SNR at each intended NOMA device which is likely to experience degraded performance under the impact of eavesdropping. In addition, we intend to compute the SNR expressions and secrecy rate expressions for scenarios where users lack a direct link with the BS. Importantly, we want to answer the question of the impact of RIS-aided link transmission on secure performance. Our results provide important guidelines to design RIS for future IoT systems

(ii) Furthermore, the main contributions are deriving the asymptotic and closed-form expressions for SOP and SPSC based on the initial expressions obtained in related works. The main coefficients are determined in order to recommend future design of reliable transmissions from the source (BS or access point (AP)) to intended devices

(iii) We provide main parameters affecting secure performance in numerical simulations. We then simulate and compare the performance of the proposed model with the aid of simulations performed based on the obtained expressions between RIS and non-line of sight users

Meanwhile, the paper is structured as follows. Section 2 will introduce and describe the system model and its characteristics. In Section 4, the numerical results and simulations are presented and discussed to understand the performance of the proposed system in both cases. Finally, in Section 5, the paper will be concluded. After the conclusion, the appendix is provided for explaining the computations related to Sections 2.

2. System Model

Figure 1 shows the system model for the normal case when direct link transmission does not exist due to blockage, while both RIS-link work together to serve destinations. In this paper, we consider a RIS-assisted wireless communication

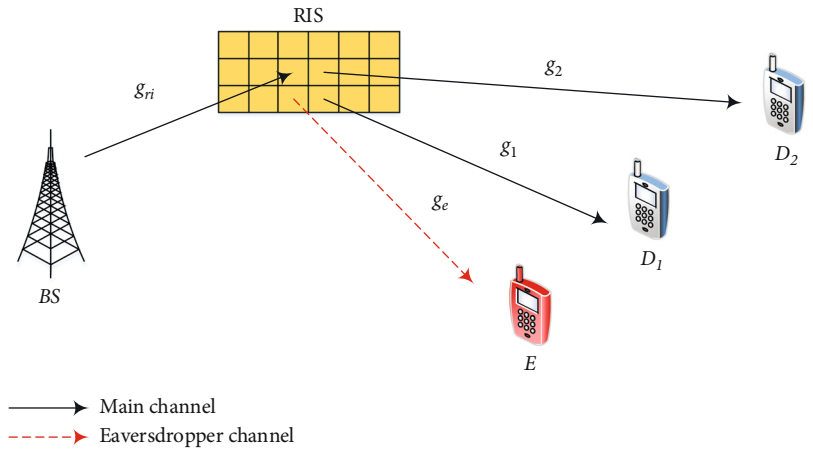

Figure 1: A sketch of IoT secure transmission relying on NOMA and RIS.

Table 1: Main notations.

Symbol	Description
$\Pr(.)$	Probability
$F_Y(.)$	The cumulative distribution function (CDF) of a random variable Y
$f_Y(.)$	The probability density function (PDF) of a random variable Y
P	The BS normalized transmission powers
x_i	The signal for D_i, $(i = 1, 2)$
τ_i	The corresponding power allocation coefficients
∂_i	The additive white Gaussian noise (AWGN) at D_i that is modeled as a zero-mean complex Gaussian distribution with variance N_0
σ	The amplitude reflection coefficient with $\sigma \in (0, 1]$
φ_n	The RIS adjustable phase applied by the n-th reflecting element
ε	The path loss exponent
R_i	The target rate at the user D_i
g_{ri}	The complex channel coefficient for the link $BS \longrightarrow$ RIS
g_1	The complex channel coefficient for the link RIS $\longrightarrow D_1$
g_2	The complex channel coefficient for the link RIS $\longrightarrow D_2$
g_e	The complex channel coefficient for the link RIS $\longrightarrow E$

network in the presence of a BS or AP, two legitimate users (D_1) and (D_2) (it can be extended to multiple users which belong to a group to implement NOMA. As reported in the literature, the performance of two NOMA users often satisfies the high requirement of services at IoT devices rather than multiple users scenarios [16]. Therefore, this paper wants to retain relevant performance by focusing on two users case), and an eavesdropper (E). The RIS is assumed to be installed with N reflecting or meta-surfaces. All the nodes are equipped with a single antenna and experience Rayleigh fading among the channels. The basic signal propagation in this model is assumed as follows: The legitimate user receives a signal from the source via RIS, in which the RIS is expected to improve the quality of the signal. The eavesdropper attempts to obtain the signal from the RIS. The CSI of the legitimate users is assumed to be known, and the RIS utilizes the CSI to maximize the received SNR at the legitimate user. The RIS will not have the CSI of the eavesdropper link. In this scenario, the signals are transmitted from the source at a rate of R_i, and secure transmission is not ensured if the secrecy rate is less than R_i. To determine the performance, we utilize the SOP and SPSC as performance metrics of interest. It is noted that the other main parameters are shown in Table 1.

In this article, the channels are assumed to be slow varying and flat fading channels. Then, the received signals reflected by the RIS at D_1 are given as follows [17–19]:

$$y_{D_1}^{no} = \sigma \sum_{n=1}^{N} \frac{g_{ri} g_1}{\sqrt{d_{ri}^{\varepsilon} d_1^{\varepsilon}}} e^{j\varphi_n} \left(\sqrt{P\tau_1} x_1 + \sqrt{P\tau_2} x_2 \right) + \partial_1, \quad (1)$$

where to ensure better fairness between the users, we assume that $\tau_2 > \tau_1$ with $\tau_1 + \tau_2 = 1$ [20]. Further, g_{ri} and g_i

Table 2: Main parameters for our simulations.

Parameters	Notation	Values
Power coefficients	$\{\tau_1, \tau_2\}$	{0.4,0.6}
Target rates	$R_1 = R_2$; R_1^o=R_2^o	0.2 (bps/Hz); 1.5 (bps/Hz)
Amplitude reflection coefficient [18]	σ	0.8
Path loss exponent	ε	3
Reflecting elements	N	200
Normalized distances [20]	d_{ri}; $d_1 = d_2$; d_e	0.7; 1; 0.6
Average powers [18]	λ_{W_e}; λ_{Φ_e}	0.02; 0.07
Transmit SNR [24]	α_e	17 (dB)

represent complex Gaussian random variables (RV) with zero mean and unit variance and d_{ri} and d_i are the distances for the BS-RIS and RIS-D_i links, respectively. The small-scale fading channel coefficients are modeled as independent and identically distributed $CN(0,1)$ variables [21]. With large N, via the central limit theorem, we find that $\sum_{n=1}^{N} g_{ri}g_i \sim CN(0,N)$ [17]. When the radio frequency (RF) source transmits its signal x_i to the receiver, the RIS will also receive the same signal and then adjust the phase $\varphi_n \in [0, 2\pi)$ of reflector $n \in \{n, \cdots, N\}$ based upon CSI [17].

The resulting SNR at the legitimate user D_1 to decode x_2 can be formulated as

$$\gamma_{D_1}^{no,x_{21}} = \frac{\sigma^2 d_{ri}^{-\varepsilon} d_1^{-\varepsilon} \sum_{n=1}^{N} |g_{ri}|^2 |g_1|^2 P\tau_2}{\sigma^2 d_{ri}^{-\varepsilon} d_1^{-\varepsilon} \sum_{n=1}^{N} |g_{ri}|^2 |g_1|^2 P\tau_1 + N_0} = \frac{\chi_{W_1} \alpha \tau_2 W_1^2}{\chi_{W_1} \alpha \tau_1 W_1^2 + 1}, \tag{2}$$

where $\chi_{W_1} = \sigma^2 d_{ri}^{-\varepsilon} d_1^{-\varepsilon}$, $\alpha = P/N_0$, due to $W_1 = |\sum_{n=1}^{N} g_{ri} g_1 e^{j\varphi_n}| = \sum_{n=1}^{N} |g_{ri}||g_1|$ in the case of perfect CSI [17].

After successive interference cancellation (SIC), the resulting SNR at the legitimate user D_1 to decode x_1 can be formulated as

$$\gamma_{D_1}^{no,x_1} = \chi_{W_1} \alpha \tau_1 W_1^2, \tag{3}$$

where it assumes a slow varying and flat fading model for all the channels. The received signal reflected by the RIS at D_2 can be written as follows [17, 18]:

$$y_{D_2}^{no} = \sigma \sum_{n=1}^{N} \frac{g_{ri} g_2}{\sqrt{d_{ri}^{\varepsilon} d_2^{\varepsilon}}} e^{j\varphi_n} \left(\sqrt{P\tau_1} x_1 + \sqrt{P\tau_2} x_2 \right) + \partial_2. \tag{4}$$

The resulting SNR at the legitimate user D_2 to decode x_2 can be formulated as

$$\gamma_{D_2}^{no,x_2} = \frac{\chi_{W_2} \alpha \tau_2 W_2^2}{\chi_{W_2} \alpha \tau_1 W_2^2 + 1}, \tag{5}$$

where $\chi_{W_2} = \sigma^2 d_{ri}^{-\varepsilon} d_2^{-\varepsilon}$, $W_2 = \sum_{n=1}^{N} |g_{ri}||g_2|$ [17].

The received RIS reflected signal at E can be written as [18, 22, 23]

$$y_E^{no} = \sigma \sum_{n=1}^{N} \frac{g_{ri} g_e}{\sqrt{d_{ri}^{\varepsilon} d_e^{\varepsilon}}} e^{j\varphi_n} \left(\sqrt{P\tau_1} x_1 + \sqrt{P\tau_2} x_2 \right) + \partial_e, \tag{6}$$

where g_e is a complex Gaussian RV with zero mean and unit variance and d_e is the distances for the RIS-E links. $\partial_e \sim CN(0, N_e)$ is the AWGN at E modeled as a zero-mean complex Gaussian distribution with variance N_e.

Particularly, parallel interference cancellation (PIC) is utilized at E to differentiate the superimposed signals. The resulting SNR at E to decode x_i can be formulated as [24]:

$$\gamma_E^{no,x_i} = \chi_{W_e} \alpha_e \tau_i W_e^2, \tag{7}$$

where $\chi_{W_e} = \sigma^2 d_{ri}^{-\varepsilon} d_e^{-\varepsilon}$, $\alpha_e = P/N_e$, $W_e = \sum_{n=1}^{N} |g_{ri}||g_e|$. W_e can be approximated by an exponential random variable parameter λ_{W_e} [18].

The instantaneous secrecy rate at D_1 is written as follows [18, 24, 25]:

$$C_{D_1}^{no} = \max \left\{ \frac{1}{2} \log_2 \left(1 + \min \left(\gamma_{D_1}^{no,x_{21}}, \gamma_{D_1}^{no,x_1} \right) \right) - \frac{1}{2} \log_2 \left(1 + \gamma_E^{no,x_1} \right), 0 \right\}. \tag{8}$$

The instantaneous secrecy rate at D_2 can be expressed as

$$C_{D_2}^{no} = \max \left\{ \frac{1}{2} \log_2 \left(1 + \gamma_{D_2}^{no,x_2} \right) - \frac{1}{2} \log_2 \left(1 + \gamma_E^{no,x_2} \right), 0 \right\}. \tag{9}$$

2.1. Secure Performance Analysis. In this section, the secrecy performance in terms of SOP and SPSC metrics is determined. To gain more insights, we also provide asymptotic SOP analyses.

2.1.1. SOP Analysis. In NOMA-aided systems, signals are transmitted from the source to D_1 and D_2 with the help of a RIS, respectively. Hence, outage happens when either $C_{D_1}^{no}$ or $C_{D_2}^{no}$ falls below their own target rates. With this

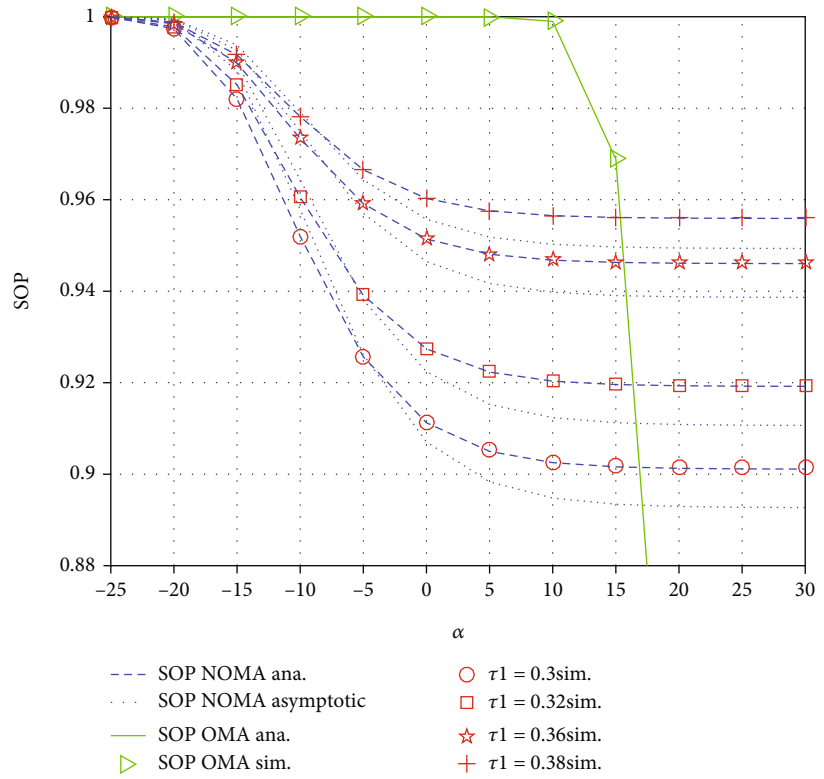

Figure 2: SOP versus α for different τ_1.

understanding, the SOP can be given as follows [24]:

$$SOP_{no} = \Pr\left(C_{D_1}^{no} < R_1 \text{ or } C_{D_2}^{no} < R_2\right) = 1 - \underbrace{\Pr\left(\frac{1+\gamma_{D_1}^{no,x_{21}}}{1+\gamma_E^{no,x_1}} \geq C_{th_1}, \frac{1+\gamma_{D_1}^{no,x_1}}{1+\gamma_E^{no,x_1}} \geq C_{th_1}\right)}_{\theta_1^{no}} \times \underbrace{\Pr\left(\frac{1+\gamma_{D_2}^{no,x_2}}{1+\gamma_E^{no,x_2}} \geq C_{th_2}\right)}_{\theta_2^{no}}, \tag{10}$$

where $C_{th_i} = 2^{2R_i}$.

Proposition 1. *The exact expression for SOP_{no} is given by*

$$SOP_{no} = 1 - \frac{\chi_{W_1}\alpha N\zeta_1\zeta_2}{\left(C_{th_1}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N\right)\lambda_{W_e}\lambda_{W_e}} \times \exp\left(-\frac{\mu_1}{\chi_{W_1}\alpha\tau_1 N}\right) \times \int_0^1 \exp\left(-\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t + \mu_1\right)\right)\chi_{W_1}\alpha N} - \frac{\zeta_1 t}{\lambda_{W_e}}\right) dt \times \int_0^1 \exp\left(-\frac{C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 q + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 q + \mu_2\right)\right)\chi_{W_2}\alpha N} - \frac{\zeta_2 q}{\lambda_{W_e}}\right) dq, \tag{11}$$

where $\zeta_1 = \tau_2 - \tau_1\mu_1/\tau_1\tau_1 C_{th_1}\chi_{W_e}\alpha_e$, $\zeta_2 = \tau_2 - \tau_1\mu_2/\tau_1\tau_2 C_{th_2}\chi_{W_e}\alpha_e$, $\mu_i = C_{th_i} - 1$.

Proof. The details are given in Appendix A. □

Remark 2. The results of (11) illustrate the SOP performance of the proposed system with no direct link between the users albeit assisted by a RIS device. The secure outage threshold is the main factor vital to SOP performance. It is intuitively seen that power allocation coefficients for the two NOMA devices are crucial factors which make a difference in evaluating the system performance for the two considered devices.

2.1.2. SOP Asymptotic. From (6), by using Gauss-Chebyshev integral [26, 27], θ_1^{no} can be computed by the following integral approximation:

$$\theta_1^{no} \approx \frac{\chi_{W_1}\alpha N}{C_{th_1}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N}\frac{\pi\zeta_1}{2G\lambda_{W_e}} \exp\left(-\frac{\mu_1}{\chi_{W_1}\alpha\tau_1 N}\right) \times \sum_{j=1}^{G} \Xi \exp\left(-\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t_j + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t_j + \mu_1\right)\right)\chi_{W_1}\alpha N} - \frac{\zeta_1 t_j}{\lambda_{W_e}}\right), \tag{12}$$

where $t_j = 1/2(1 + \cos(2j - 1/G))$, $\Xi = |\sin(2j - 1/G)|$ and G

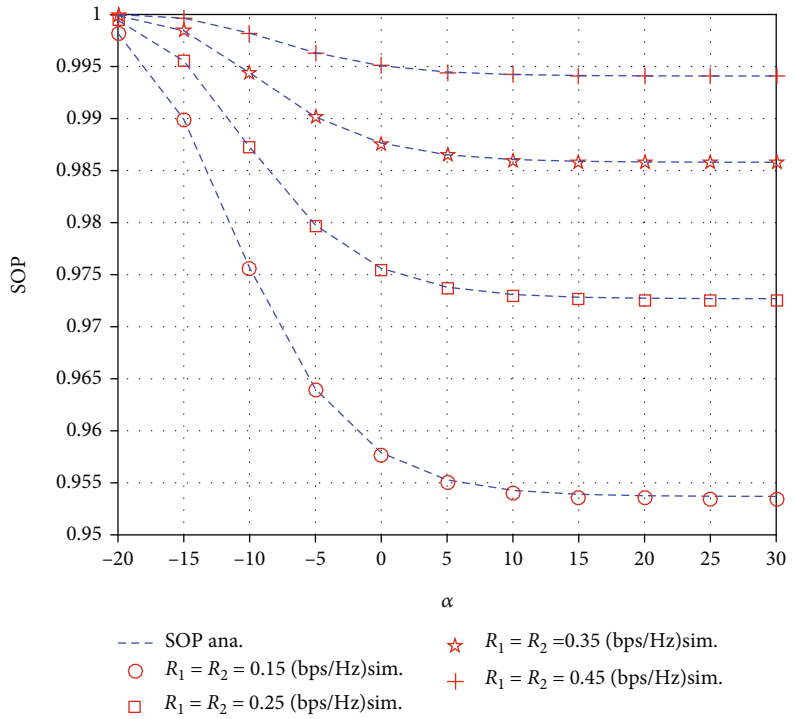

FIGURE 3: SOP versus α for different $R_1 = R_2$.

is the Gauss-Chebyshev integral approximated sum term [26].

From (9), by using Gauss-Chebyshev integral [26, 27], θ_2^{no} can be obtained using the following integral approximation:

$$\theta_2^{no} \approx \frac{\pi\zeta_2}{2G\lambda_{W_e}} \sum_{j=1}^{G} \Xi \exp\left(\begin{array}{c} -\dfrac{C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 t_j + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 t_j + \mu_2\right)\right)\chi_{W_2}\alpha N} \\ -\dfrac{\zeta_2 t_j}{\lambda_{W_e}} \end{array} \right). \tag{13}$$

Based on (12) and (13), the final approximate closed-form expression for SOP_{no} is given by

$$\begin{aligned} SOP_{no}^{asym} \approx 1 &- \frac{\chi_{W_1}\alpha N\pi\pi\zeta_1\zeta_2}{\left(C_{th_1}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N\right)4GG\lambda_{W_e}\lambda_{W_e}} \\ &\times \exp\left(-\frac{\mu_1}{\chi_{W_1}\alpha\tau_1 N}\right) \\ &\times \sum_{j=1}^{G} \Xi \exp\left(\begin{array}{c} -\dfrac{C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t_j + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t_j + \mu_1\right)\right)\chi_{W_1}\alpha N} \\ -\dfrac{\zeta_1 t_j}{\lambda_{W_e}} \end{array} \right) \\ &\times \sum_{j=1}^{G} \boxtimes\Xi \exp\left(\begin{array}{c} -\dfrac{C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 t_j + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 t_j + \mu_2\right)\right)\chi_{W_2}\alpha N} \\ -\dfrac{\zeta_2 t_j}{\lambda_{W_e}} \end{array} \right). \end{aligned} \tag{14}$$

2.1.3. SPSC Analysis. SPSC is one of the fundamental benchmarks for secrecy performance, and it denotes the probability of existence of secrecy capacity [24, 28]. Thus, the SPSC for a NOMA system can be written as

$$\begin{aligned} SPSC_{no} &= \Pr\left(C_{D_1}^{no} > 0, C_{D_2}^{no} > 0\right) \\ &= \underbrace{\Pr\left(\min\left(\gamma_{D_1}^{no,x_{21}}, \gamma_{D_1}^{no,x_1}\right) > \gamma_E^{no,x_1}\right)}_{\Omega_1^{no}} \\ &\quad \times \underbrace{\Pr\left(\gamma_{D_2}^{no,x_2} > \gamma_E^{no,x_2}\right)}_{\Omega_2^{no}}. \end{aligned} \tag{15}$$

Proposition 3. *The exact expression for $SPSC_{no}$ is given by*

$$\begin{aligned} SPSC_{no} = &\frac{\chi_{W_1}\alpha N\zeta_3\zeta_4}{\left(\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N\right)\lambda_{W_e}\lambda_{W_e}} \\ &\times \int_0^1 \exp\left(\begin{array}{c} -\dfrac{\chi_{W_e}\alpha_e\tau_1\zeta_3 t}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1\zeta_3 t\right)\chi_{W_1}\alpha N} \\ -\dfrac{\zeta_3 t}{\lambda_{W_e}} \end{array} \right) dt \\ &\times \int_0^1 \exp\left(\begin{array}{c} -\dfrac{\chi_{W_e}\alpha_e\tau_2\zeta_4 q}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_2\zeta_4 q\right)\chi_{W_2}\alpha N} \\ -\dfrac{\zeta_4 q}{\lambda_{W_e}} \end{array} \right) dq, \end{aligned} \tag{16}$$

where $\zeta_3 = \tau_2/\tau_1\tau_1\chi_{W_e}\alpha_e$, $\zeta_4 = 1/\tau_1\chi_{W_e}\alpha_e$.

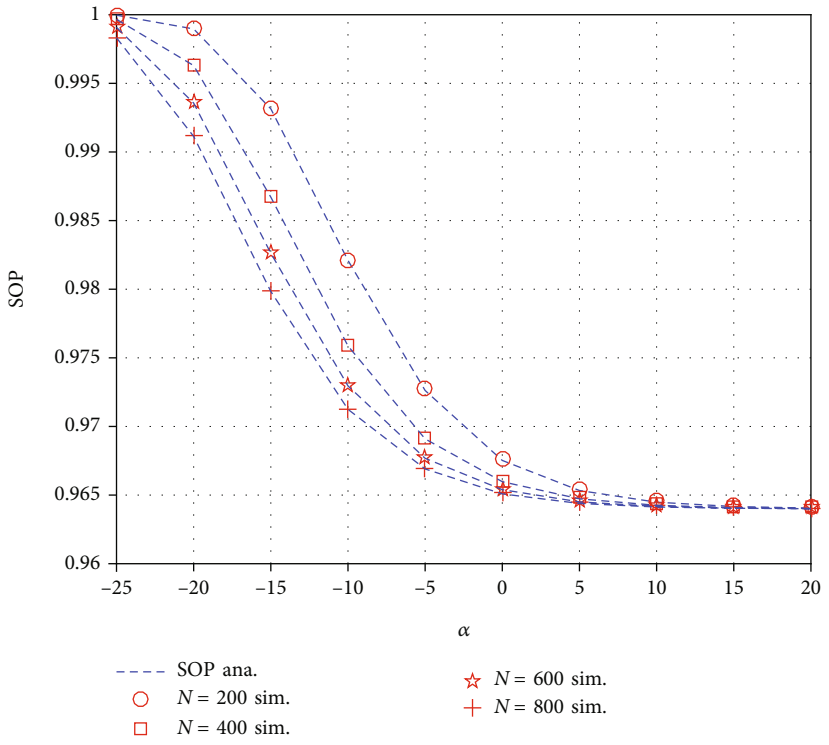

FIGURE 4: SOP versus α for different N.

Proof. The details are given in Appendix B. □

Remark 4. (16) illustrates the SPSC performance of the proposed system with no direct link between the users in the presence of RIS. The structure of RIS influences the SPSC performance. Therefore, by tailoring RIS, the traditional IoT gets more benefits against eavesdroppers.

2.1.4. SPSC Asymptotic. From (6), by using the Gauss-Chebyshev integral [26, 27], Ω_1^{no} can be obtained via the following integral approximation:

$$\Omega_1^{no} \approx \frac{\chi_{W_1}\alpha N\pi\zeta_3}{\left(\chi_{W_e}\alpha_e\lambda_{W_e}+\chi_{W_1}\alpha N\right)2G\lambda_{W_e}} \times \sum_{j=1}^{G}\Xi \exp\left(-\frac{\chi_{W_e}\alpha_e\tau_1\zeta_3 t_j}{\left(\tau_2-\chi_{W_e}\alpha_e\tau_1\tau_1\zeta_3 t_j\right)\chi_{W_1}\alpha N}-\frac{\zeta_3 t_j}{\lambda_{W_e}}\right). \tag{17}$$

From (9), by using the Gauss-Chebyshev integral [26, 27], Ω_2^{no} can be formulated using the following integral approximation:

$$\Omega_2^{no} \approx \frac{\pi\zeta_4}{2G\lambda_{W_e}}\sum_{j=1}^{G}\Xi \exp\left(-\frac{\chi_{W_e}\alpha_e\tau_2\zeta_4 t_j}{\left(\tau_2-\chi_{W_e}\alpha_e\tau_1\tau_2\zeta_4 t_j\right)\chi_{W_2}\alpha N}-\frac{\zeta_4 t_j}{\lambda_{W_e}}\right). \tag{18}$$

Based on (17) and (18), the final approximate closed-form expression for $SPSC_{no}$ is given by

$$SPSC_{no}^{asym} \approx \frac{\chi_{W_1}\alpha N\pi\pi\zeta_3\zeta_4}{\left(\chi_{W_e}\alpha_e\lambda_{W_e}+\chi_{W_1}\alpha N\right)4GG\lambda_{W_e}\lambda_{W_e}} \times \sum_{j=1}^{G}\Xi \exp\left(\begin{array}{c}-\dfrac{\chi_{W_e}\alpha_e\tau_1\zeta_3 t_j}{\left(\tau_2-\chi_{W_e}\alpha_e\tau_1\tau_1\zeta_3 t_j\right)\chi_{W_1}\alpha N} \\ -\dfrac{\zeta_3 t_j}{\lambda_{W_e}}\end{array}\right) \times \sum_{j=1}^{G}\Xi \exp\left(\begin{array}{c}-\dfrac{\chi_{W_e}\alpha_e\tau_2\zeta_4 t_j}{\left(\tau_2-\chi_{W_e}\alpha_e\tau_1\tau_2\zeta_4 t_j\right)\chi_{W_2}\alpha N} \\ -\dfrac{\zeta_4 t_j}{\lambda_{W_e}}\end{array}\right). \tag{19}$$

3. RIS-OMA Scheme

It would be better to compare with the counterpart, i.e., RIS-OMA. Similarly, the received signal reflected by the RIS at D_i are given as

$$y_{D_i}^{o} = \sigma\sum_{n=1}^{N}\frac{g_{ri}g_i}{\sqrt{d_{ri}^{\varepsilon}d_i^{\varepsilon}}}e^{j\varphi_n}\sqrt{P}x_i+\partial_i. \tag{20}$$

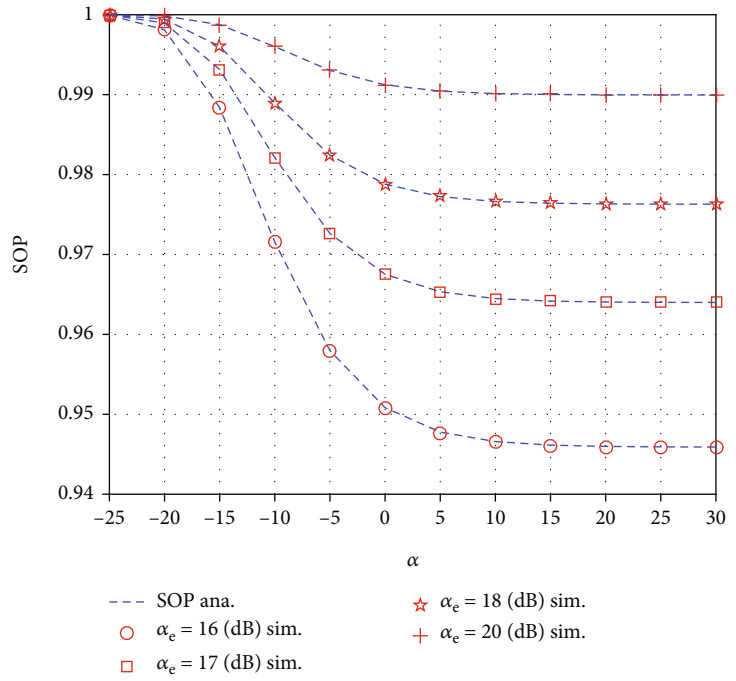

Figure 5: SOP versus α for different α_e.

We then compute SNR at the user D_i to decode x_i as

$$\gamma_{D_i}^{o,x_i} = \chi_{W_i} \alpha W_i^2, \tag{21}$$

where $\chi_{W_i} = \sigma^2 d_{ri}^{-\varepsilon} d_i^{-\varepsilon}$, $W_i = |\sum_{n=1}^{N} g_{ri} g_i e^{j\varphi_n}| = \sum_{n=1}^{N} |g_{ri}||g_i|$.

The RIS is also able to reflect signals to E and the received signal at E can be written as

$$y_E^o = \sigma \sum_{n=1}^{N} \frac{g_{ri} g_e}{\sqrt{d_{ri}^{\varepsilon} d_e^{\varepsilon}}} e^{j\varphi_n} \sqrt{P} x_i + \partial_e. \tag{22}$$

Based on the received signal at E, we then calculate SNR at E to decode x_i as

$$\gamma_E^{o,x_i} = \chi_{W_e} \alpha_e W_e^2. \tag{23}$$

The instantaneous secrecy rate at D_i in this RIS-OMA scenario is computed by

$$C_{D_i}^o = \max\left\{\frac{1}{4}\log_2\left(1+\gamma_{D_i}^{o,x_i}\right) - \frac{1}{4}\log_2\left(1+\gamma_E^{o,x_i}\right), 0\right\}. \tag{24}$$

3.1. SOP Analysis. Similarly from (10), the SOP can be given as

$$\begin{aligned} SOP_o &= \Pr\left(C_{D_1}^o < R_1^o \text{ or } C_{D_2}^o < R_2^o\right) \\ &= 1 - \underbrace{\Pr\left(\frac{1+\gamma_{D_1}^{o,x_1}}{1+\gamma_E^{o,x_1}} \geq C_{th_1}^o\right)}_{\theta_1^o} \times \underbrace{\Pr\left(\frac{1+\gamma_{D_2}^{o,x_2}}{1+\gamma_E^{o,x_2}} \geq C_{th_2}^o\right)}_{\theta_2^o}, \end{aligned} \tag{25}$$

where $C_{th_i}^o = 2^{8R_i^o}$ and R_i^o is the target rate at the user D_i for RIS-OMA case.

Firstly, θ_1^o can given by

$$\begin{aligned} \theta_1^o &= \Pr\left(\frac{1+\gamma_{D_1}^{o,x_1}}{1+\gamma_E^{o,x_1}} \geq C_{th_1}^o\right) \\ &= \Pr\left(W_1^2 \geq \frac{C_{th_1}^o \chi_{W_e} \alpha_e W_e^2 + \mu_1^o}{\chi_{W_1} \alpha}\right) \\ &= \int_0^{\infty} \left(1 - F_{W_1^2}\left(\frac{C_{th_1}^o \chi_{W_e} \alpha_e x + \mu_1^o}{\chi_{W_1} \alpha}\right)\right) f_{W_e^2}(x) dx \\ &= \frac{1}{\lambda_{W_e}} \exp\left(-\frac{\mu_1^o}{\chi_{W_1} \alpha N}\right) \\ &\quad \times \int_0^{\infty} \boxtimes \exp\left(-\left(\frac{C_{th_1}^o \chi_{W_e} \alpha_e}{\chi_{W_1} \alpha N} + \frac{1}{\lambda_{W_e}}\right) x\right) dx \\ &= \frac{\chi_{W_1} \alpha N}{C_{th_1}^o \chi_{W_e} \alpha_e \lambda_{W_e} + \chi_{W_1} \alpha N} \exp\left(-\frac{\mu_1^o}{\chi_{W_1} \alpha N}\right), \end{aligned} \tag{26}$$

where $\mu_i^o = C_{th_i}^o - 1$.

Next, θ_2^o is calculated similarly to θ_1^o. In particular, θ_2^o can expressed by

$$\theta_2^o = \frac{\chi_{W_2} \alpha N}{C_{th_2}^o \chi_{W_e} \alpha_e \lambda_{W_e} + \chi_{W_2} \alpha N} \exp\left(-\frac{\mu_2^o}{\chi_{W_2} \alpha N}\right). \tag{27}$$

From (26) and (27) into (25), the closed-form expression

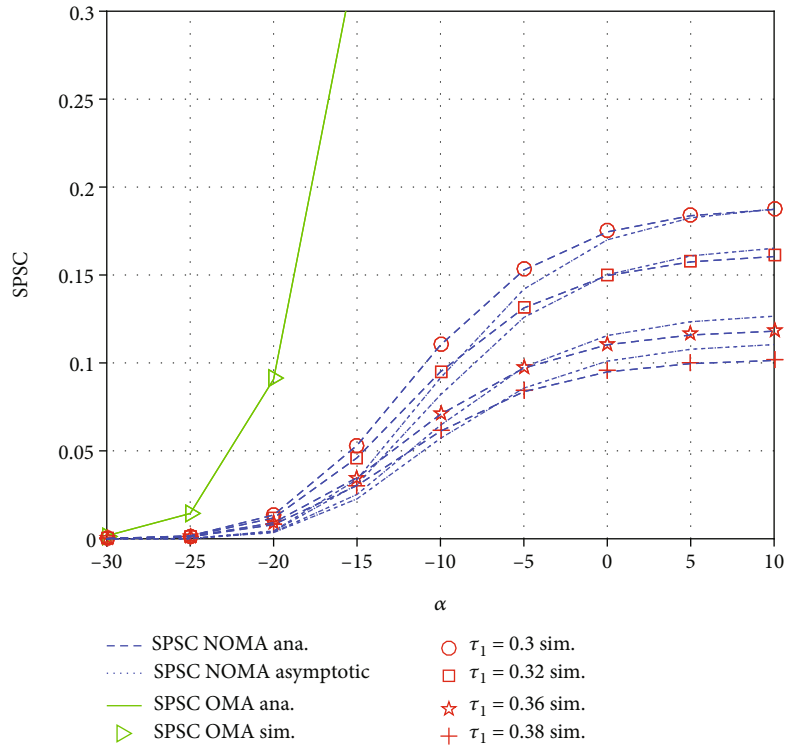

Figure 6: SPSC versus α for different τ_1.

SOP_o is given by

$$SOP_o = 1 - \frac{\chi_{W_1}\alpha N}{C^o_{th_1}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N} \times \frac{\chi_{W_2}\alpha N}{C^o_{th_2}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_2}\alpha N} \times \exp\left(-\frac{\mu^o_1}{\chi_{W_1}\alpha N} - \frac{\mu^o_2}{\chi_{W_2}\alpha N}\right). \tag{28}$$

3.2. SPSC Analysis. The SPSC for a OMA system can be written as

$$SPSC_o = \Pr\left(C^o_{D_1} > 0, C^o_{D_2} > 0\right) = \underbrace{\Pr\left(\gamma^{o,x_1}_{D_1} > \gamma^{o,x_1}_E\right)}_{\Omega^o_1} \underbrace{\Pr\left(\gamma^{o,x_2}_{D_2} > \gamma^{o,x_2}_E\right)}_{\Omega^o_2}. \tag{29}$$

From (29), Ω^o_1 is written by

$$\begin{aligned}\Omega^o_1 &= \Pr\left(\gamma^{o,x_1}_{D_1} > \gamma^{o,x_1}_E\right) = \Pr\left(W^2_1 \geq \frac{\chi_{W_e}\alpha_e W^2_e}{\chi_{W_1}\alpha}\right) \\ &= \int_0^\infty \left(1 - F_{W^2_1}\left(\frac{\chi_{W_e}\alpha_e x}{\chi_{W_1}\alpha}\right)\right) f_{W^2_e}(x)dx \\ &= \frac{1}{\lambda_{W_e}}\int_0^\infty \exp\left(-\left(\frac{\chi_{W_e}\alpha_e}{\chi_{W_1}\alpha N} + \frac{1}{\lambda_{W_e}}\right)x\right)dx \\ &= \frac{\chi_{W_1}\alpha N}{\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N}.\end{aligned} \tag{30}$$

Then, Ω^o_2 is calculated similarly to Ω^o_1. Ω^o_2 can given by

$$\Omega^o_2 = \frac{\chi_{W_2}\alpha N}{\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_2}\alpha N}. \tag{31}$$

From (30) and (31) into (29), the closed-form expression $SPSC_o$ is given by

$$SPSC_o = \frac{\chi_{W_1}\alpha N}{\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N} \times \frac{\chi_{W_2}\alpha N}{\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_2}\alpha N}. \tag{32}$$

4. Numerical Results

In this section, numerical examples are presented to verify our analytical results. In the simulation results, the Rayleigh fading is assumed for all the channels [18]. The SOP and SPSC are obtained with Monte Carlo simulations. The main parameters can be considered in Table 2 except for specific cases.

Figure 2 shows the simulation of SOP versus transmit SNR for different power allocation levels. It can be determined from (10), (11) that the transmit SNR α contributes significantly to SOP performance and this can be verified in this figure. It can also be observed from the simulation that even a minute level of change in power allocation can create a noticeable difference in the performance of the system. As the transmit SNR increases beyond 15 (dB), the performance of the system goes constant. This phenomenon can be explained by the fact that SOP depends on many parameters rather than α, for example, channel gain, and data rates C_{th_i}. SOP performance is important to indicate

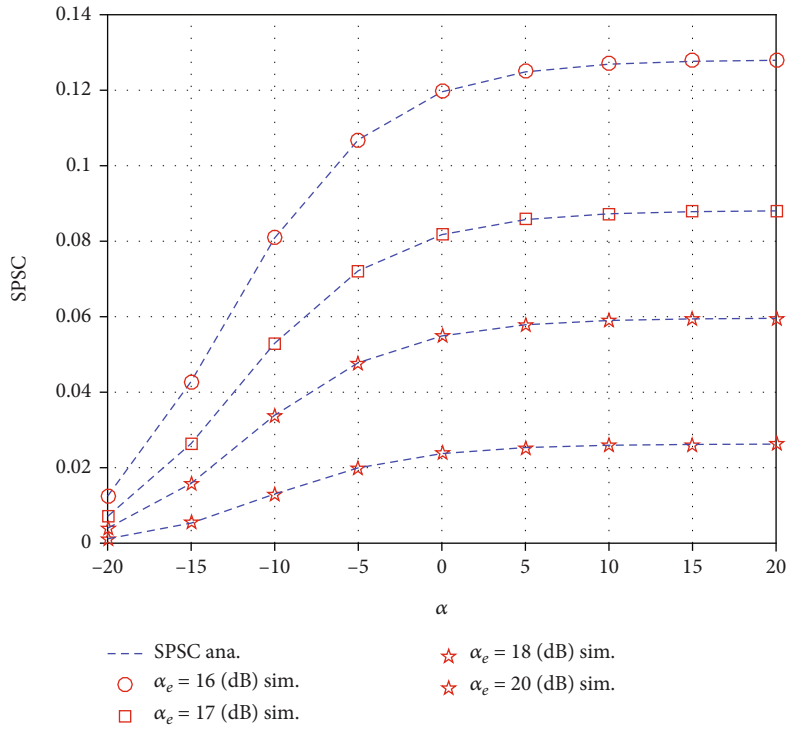

Figure 7: SPSC versus α for different α_e.

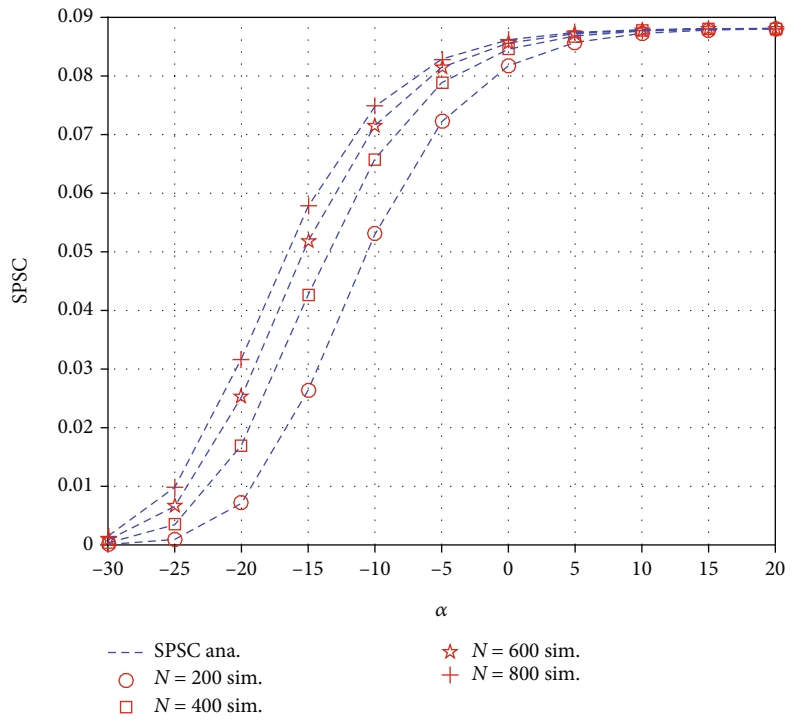

Figure 8: SPSC versus α for different N.

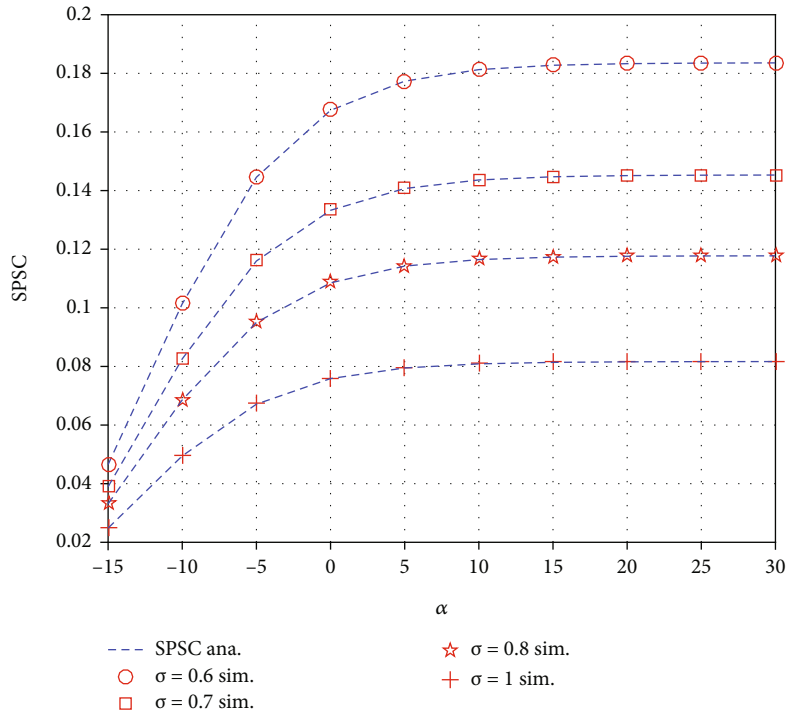

Figure 9: SPSC versus α for different σ.

how system works under particular conditions of channels. We can deal with SOP improvement if α and data rates C_{th_i} are adjusted properly. Further, we can confirm that RIS-NOMA outperforms than RIS-OMA if α is less than 17 (dB). The main reason is that RIS-NOMA provides higher spectrum efficiency.

Figure 3 shows the simulation for SOP versus transmit SNR for different levels of target rates R_1, R_2 assigned to the users. To perform a fair comparison, in each case, the target rates are assigned equally for all the users in the system. As we can observe, as the target rates increase, the performance of the system also becomes worse. The reason is that SOP performance derived in (10) and (11) are logically limited by such target rates C_{th_i}.

Figure 4 demonstrates the simulation of SOP versus transmit SNR for a different number of meta-surfaces installed at RIS. As we can see, as the number of meta-surfaces increases, the secrecy performance of the system increases. The noticeable point in this study is, even though the number of meta-surfaces is sufficiently large enough, as, with the increase in the transmit SNR, the performance of the system goes into constant mode after a certain level of α. The major reason for this situation is because, at high SNR levels, the interference between the users in the cluster becomes dominant which affects the performance of the system. SOP performance corresponds to how we design RIS with respect to the number of meta-surface. It can be explained that more meta-surface elements at RIS contributes to improve quality of received signal and the corresponding SOP can be enhanced.

Figure 5 shows the simulation of SOP versus transmit SNR for different levels of SNR at the eavesdropper. Since PIC is considered in the system, the effect of SNR at eavesdropper can be seen clearly. As the value of α_e increases, the performance of the system is decreasing rapidly. Even for the small difference between each case, the secrecy performance of the system is being affected or decreased with a huge gap between the curves.

Figure 6 shows the simulation of SPSC versus transmit SNR for different levels of power allocation at D_1. This simulation is performed similar to Figure 2 but with a different method of analysis, i.e., SPSC. As we can observe, the change in power allocation levels has shown significant change in the performance of the system. Further, it can be seen the gap between RIS-OMA and RIS-NOMA cases if we refer to SPSC case. In this case, RIS-NOMA deals with a fixed allocation scheme to assign power to two NOMA users, and hence its SPSC performance looks worse compared with RIS-OMA case.

Similarly, Figure 7 is simulated identically to Figure 5, and it shows SPSC versus transmit SNR with different levels of SNR at the eavesdropper. As mentioned, since PIC is considered, as the α_e value increases, the SPSC performance of the system decreases rapidly.

Figure 8 is simulated similarly to Figure 4. It shows that the simulation between SPSC versus transmits SNR for different numbers of meta-surfaces installed at RIS. As the number of meta-surfaces increases, the performance of the system increases comparatively.

Figure 9 shows the simulation between SPSC versus transmit SNR for different levels of amplitude reflection coefficients. We can observe that the changes in the level of

σ do not show much effect on the direct link and it shows a huge effect on the no direct link since the RIS is the only possible way of communication between the devices. As the σ value decreases, the performance of the system decreases.

5. Conclusion

In this paper, we have considered a RIS system with two legitimate users, being served in a cluster, and an eavesdropper. All users are equipped with a single antenna. The proposed model was considered no direct link between the devices in the presence of RIS. The performance of the system is analyzed from the perspective of secrecy efficiency. Asymptotic and closed-form expressions are derived for SOP and SPSC. The simulations were performed based on these expressions, and the results are verified using the Monte-Carlo method. The study provides that in most of the cases, the secrecy performance of the system was efficient in the direct link between the devices in the presence of RIS. As we previously mentioned, the number of meta-surfaces and SNR levels at the users also play a pivotal role in influencing the performance of the system.

Appendix

A. Proof of Proposition 1

From (10), θ_1^{no} is given by

$$\theta_1^{no} = \underbrace{\Pr\left(\frac{1+\gamma_{D_1}^{no,x_{21}}}{1+\gamma_E^{no,x_1}} \geq C_{th_1}\right)}_{\theta_{1a}^{no}} \times \underbrace{\Pr\left(\frac{1+\gamma_{D_1}^{no,x_1}}{1+\gamma_E^{no,x_1}} \geq C_{th_1}\right)}_{\theta_{1b}^{no}}. \tag{A.1}$$

Then, an upper bound of θ_{1a}^{no} can be obtained as

$$\begin{aligned}\theta_{1a}^{no} &= \Pr\left(\frac{\chi_{W_1}\alpha\tau_2 W_1^2}{\chi_{W_1}\alpha\tau_1 W_1^2 + 1} \geq C_{th_1}\chi_{W_e}\alpha_e\tau_1 W_e^2 + \mu_1\right) \\ &= \Pr\left(W_1^2 \geq \frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1 W_e^2 + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1 W_e^2 + \mu_1\right)\right)\chi_{W_1}\alpha}\right),\end{aligned} \tag{A.2}$$

where $\mu_i = C_{th_i} - 1$ and θ_{1a}^{no} is calculated with the condition $W_e^2 < \tau_2 - \tau_1\mu_1/\tau_1\tau_1 C_{th_1}\chi_{W_e}\alpha_e$, we let $\zeta_1 = \tau_2 - \tau_1\mu_1/\tau_1\tau_1 C_{th_1}\chi_{W_e}\alpha_e$. It is noted that all channels follow the Rayleigh distribution with PDF and CDF $f_{|X|^2}(x) = (1/\varphi_X)\exp(-x/\varphi_X)$, $F_{|X|^2}(x) = 1 - \exp(-x/\varphi_X)$, respectively [18]. Then, θ_{1a}^{no} can be calculated as

$$\begin{aligned}\theta_{1a}^{no} &= \int_0^{\zeta_1}\left(1 - F_{W_1^2}\left(\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1\right)\right)\chi_{W_1}\alpha}\right)\right) \\ &\quad \times f_{W_e^2}(x)dx = \int_0^{\zeta_1}\exp\left(-\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1\right)\right)\chi_{W_1}\alpha N}\right) \\ &\quad \times \frac{1}{\lambda_{W_e}}\exp\left(-\frac{x}{\lambda_{W_e}}\right)dx \\ &= \frac{1}{\lambda_{W_e}}\int_0^{\zeta_1}\exp\left(-\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1\right)\right)\chi_{W_1}\alpha N} - \frac{x}{\lambda_{W_e}}\right)dx.\end{aligned} \tag{A.3}$$

From (A.3), $t = x/\zeta_1$. θ_{1a}^{no} can written by

$$\theta_{1a}^{no} = \frac{\zeta_1}{\lambda_{W_e}}\int_0^1\exp\left(-\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t + \mu_1\right)\right)\chi_{W_1}\alpha N} - \frac{\zeta_1 t}{\lambda_{W_e}}\right)dt. \tag{A.4}$$

From (A.1), θ_{1b}^{no} can be expressed as follows:

$$\begin{aligned}\theta_{1b}^{no} &= \Pr\left(W_1^2 \geq \frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1 W_e^2 + \mu_1}{\chi_{W_1}\alpha\tau_1}\right) \\ &= \int_0^{\infty}\left(1 - F_{W_1^2}\left(\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1 x + \mu_1}{\chi_{W_1}\alpha\tau_1}\right)\right)f_{W_e^2}(x)dx \\ &= \frac{1}{\lambda_{W_e}}\exp\left(-\frac{\mu_1}{\chi_{W_1}\alpha\tau_1 N}\right) \times \int_0^{\infty}\exp\left(-\left(\frac{C_{th_1}\chi_{W_e}\alpha_e}{\chi_{W_1}\alpha N} + \frac{1}{\lambda_{W_e}}\right)x\right)dx \\ &= \frac{\chi_{W_1}\alpha N}{C_{th_1}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N}\exp\left(-\frac{\mu_1}{\chi_{W_1}\alpha\tau_1 N}\right).\end{aligned} \tag{A.5}$$

From (A.4) and (A.5) into (A.1), θ_1^{no} can be written as

$$\begin{aligned}\theta_1^{no} &= \frac{\chi_{W_1}\alpha N}{C_{th_1}\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N}\frac{\zeta_1}{\lambda_{W_e}}\exp\left(-\frac{\mu_1}{\chi_{W_1}\alpha\tau_1 N}\right) \\ &\quad \times \int_0^1\exp\left(-\frac{C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t + \mu_1}{\left(\tau_2 - \tau_1\left(C_{th_1}\chi_{W_e}\alpha_e\tau_1\zeta_1 t + \mu_1\right)\right)\chi_{W_1}\alpha N} - \frac{\zeta_1 t}{\lambda_{W_e}}\right)dt.\end{aligned} \tag{A.6}$$

Further, θ_2^{no} can be written as

$$\theta_2^{no} = \Pr\left(\frac{\chi_{W_2}\alpha\tau_2 W_2^2}{\chi_{W_2}\alpha\tau_1 W_2^2 + 1} \geq C_{th_2}\chi_{W_e}\alpha_e\tau_2 W_e^2 + \mu_2\right) = \Pr\left(W_2^2 \geq \frac{C_{th_2}\chi_{W_e}\alpha_e\tau_2 W_e^2 + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2 W_e^2 + \mu_2\right)\right)\chi_{W_2}\alpha}\right). \tag{A.7}$$

We let $\zeta_2 = \tau_2 - \tau_1\mu_2/\tau_1\tau_2 C_{th_2}\chi_{W_e}\alpha_e$, θ_2^{no} be calculated with the condition $W_e^2 < \zeta_2$. θ_2^{no} can be expressed as follows:

$$\begin{aligned}\theta_2^{no} &= \int_0^{\zeta_2}\left(1 - F_{W_2^2}\left(\frac{C_{th_2}\chi_{W_e}\alpha_e\tau_2 x + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2 x + \mu_2\right)\right)\chi_{W_2}\alpha}\right)\right) \times f_{W_e^2}(x)dx \\ &= \int_0^{\zeta_2}\exp\left(-\frac{C_{th_2}\chi_{W_e}\alpha_e\tau_2 x + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2 x + \mu_2\right)\right)\chi_{W_2}\alpha N}\right) \\ &\quad \times \frac{1}{\lambda_{W_e}}\exp\left(-\frac{x}{\lambda_{W_e}}\right)dx \\ &= \frac{1}{\lambda_{W_e}}\int_0^{\zeta_2}\exp\left(-\frac{C_{th_2}\chi_{W_e}\alpha_e\tau_2 x + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2 x + \mu_2\right)\right)\chi_{W_2}\alpha N} - \frac{x}{\lambda_{W_e}}\right)dx.\end{aligned} \tag{A.8}$$

From (A.8), we let $q = x/\zeta_2$. θ_2^{no} be written as

$$\theta_2^{no} = \frac{\zeta_2}{\lambda_{W_e}}\int_0^1\exp\left(-\frac{C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 q + \mu_2}{\left(\tau_2 - \tau_1\left(C_{th_2}\chi_{W_e}\alpha_e\tau_2\zeta_2 q + \mu_2\right)\right)\chi_{W_2}\alpha N} - \frac{\zeta_2 q}{\lambda_{W_e}}\right)dq. \tag{A.9}$$

Substituting (A.6) and (A.9) into (10), we can obtain (11).

The proof is completed.

B. Proof of Proposition 3

From (15), Ω_1^{no} can be written as

$$\Omega_1^{no} = \underbrace{\Pr\left(\min\left(\gamma_{D_1}^{no,x_{21}}, \gamma_{D_1}^{no,x_1}\right) > \gamma_E^{no,x_1}\right)}_{\Omega_{1a}^{no}} \underbrace{\Pr\left(\gamma_{D_1}^{no,x_{21}} > \gamma_E^{no,x_1}\right)\Pr\left(\gamma_{D_1}^{no,x_1} > \gamma_E^{no,x_1}\right)}_{\Omega_{1b}^{no}}. \tag{B.1}$$

From (B.1), Ω_{1a}^{no} can be obtained as

$$\Omega_{1a}^{no} = \Pr\left(\gamma_{D_1}^{no,x_{21}} > \gamma_E^{no,x_1}\right) = \Pr\left(\frac{\chi_{W_1}\alpha\tau_2 W_1^2}{\chi_{W_1}\alpha\tau_1 W_1^2 + 1} \geq \chi_{W_e}\alpha_e\tau_1 W_e^2\right) = \Pr\left(W_1^2 \geq \frac{\chi_{W_e}\alpha_e\tau_1 W_e^2}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1 W_e^2\right)\chi_{W_1}\alpha}\right). \tag{B.2}$$

Next, we let $\zeta_3 = \tau_2/\tau_1\tau_1\chi_{W_e}\alpha_e$ and Ω_{1a}^{no} be calculated with the condition $W_e^2 < \zeta_3$. Ω_{1a}^{no} can be rewritten as

$$\begin{aligned}\Omega_{1a}^{no} &= \int_0^{\zeta_3}\left(1 - F_{W_1^2}\left(\frac{\chi_{W_e}\alpha_e\tau_1 x}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1 x\right)\chi_{W_1}\alpha}\right)\right) \times f_{W_e^2}(x)dx \\ &= \int_0^{\zeta_3}\exp\left(-\frac{\chi_{W_e}\alpha_e\tau_1 x}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1 x\right)\chi_{W_1}\alpha N}\right) \\ &\quad \times \frac{1}{\lambda_{W_e}}\exp\left(-\frac{x}{\lambda_{W_e}}\right)dx \\ &= \frac{1}{\lambda_{W_e}}\int_0^{\zeta_3}\exp\left(-\frac{\chi_{W_e}\alpha_e\tau_1 x}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1 x\right)\chi_{W_1}\alpha N} - \frac{x}{\lambda_{W_e}}\right)dx.\end{aligned} \tag{B.3}$$

From (B.3), we let $t = x/\zeta_3$. Ω_{1a}^{no} be given by

$$\Omega_{1a}^{no} = \frac{\zeta_3}{\lambda_{W_e}}\int_0^1\exp\left(-\frac{\chi_{W_e}\alpha_e\tau_1\zeta_3 t}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1\zeta_3 t\right)\chi_{W_1}\alpha N} - \frac{\zeta_3 t}{\lambda_{W_e}}\right)dt. \tag{B.4}$$

From (B.1), Ω_{1b}^{no} can be obtained as

$$\begin{aligned}\Omega_{1b}^{no} &= \Pr\left(\gamma_{D_1}^{no,x_1} \geq \gamma_E^{no,x_1}\right) = \Pr\left(W_1^2 \geq \frac{\chi_{W_e}\alpha_e W_e^2}{\chi_{W_1}\alpha}\right) \\ &= \int_0^{\infty}\left(1 - F_{W_1^2}\left(\frac{\chi_{W_e}\alpha_e x}{\chi_{W_1}\alpha}\right)\right)f_{W_e^2}(x)dx \\ &= \frac{1}{\lambda_{W_e}}\int_0^{\infty}\exp\left(-\left(\frac{\chi_{W_e}\alpha_e}{\chi_{W_1}\alpha N} + \frac{1}{\lambda_{W_e}}\right)x\right)dx \\ &= \frac{\chi_{W_1}\alpha N}{\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N}.\end{aligned} \tag{B.5}$$

From (B.4) and (B.5) into (B.1), Ω_1^{no} can be written as

$$\Omega_1^{no} = \frac{\chi_{W_1}\alpha N\zeta_3}{\left(\chi_{W_e}\alpha_e\lambda_{W_e} + \chi_{W_1}\alpha N\right)\lambda_{W_e}} \times \int_0^1 \exp\left(\begin{array}{c} -\dfrac{\chi_{W_e}\alpha_e\tau_1\zeta_3 t}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_1\zeta_3 t\right)\chi_{W_1}\alpha N} \\ -\dfrac{\zeta_3 t}{\lambda_{W_e}} \end{array}\right) dt. \tag{B.6}$$

From (15), Ω_2^{no} can be obtained as

$$\Omega_2^{no} = \Pr\left(\gamma_{D_2}^{no,x_2} > \gamma_E^{no,x_2}\right) = \Pr\left(W_2^2 \geq \frac{\chi_{W_e}\alpha_e\tau_2 W_e^2}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_2 W_e^2\right)\chi_{W_2}\alpha}\right). \tag{B.7}$$

Next, we let $\zeta_4 = 1/\tau_1\chi_{W_e}\alpha_e$ and Ω_2^{no} be calculated with the condition $W_e^2 < \zeta_4$. Ω_2^{no} can be rewritten as

$$\begin{aligned}\Omega_2^{no} &= \int_0^{\zeta_4}\left(1 - F_{W_2^2}\left(\frac{\chi_{W_e}\alpha_e\tau_2 x}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_2 x\right)\chi_{W_2}\alpha}\right)\right) f_{W_e^2}(x)dx \\ &= \int_0^{\zeta_4}\exp\left(-\frac{\chi_{W_e}\alpha_e\tau_2 x}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_2 x\right)\chi_{W_2}\alpha N}\right) \times \frac{1}{\lambda_{W_e}}\exp\left(-\frac{x}{\lambda_{W_e}}\right)dx \\ &= \frac{1}{\lambda_{W_e}}\int_0^{\zeta_4}\exp\left(\begin{array}{c} -\dfrac{\chi_{W_e}\alpha_e\tau_2 x}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_2 x\right)\chi_{W_2}\alpha N} \\ -\dfrac{x}{\lambda_{W_e}} \end{array}\right) dx.\end{aligned} \tag{B.8}$$

From (B.8), we let $q = x/\zeta_4$. Ω_2^{no} be given by

$$\Omega_2^{no} = \frac{\zeta_4}{\lambda_{W_e}}\int_0^1 \exp\left(-\frac{\chi_{W_e}\alpha_e\tau_2\zeta_4 q}{\left(\tau_2 - \chi_{W_e}\alpha_e\tau_1\tau_2\zeta_4 q\right)\chi_{W_2}\alpha N} - \frac{\zeta_4 q}{\lambda_{W_e}}\right) dq. \tag{B.9}$$

Substituting (B.6) and (B.9) into (15), we can obtain (16).

The proof is completed.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

We are greatly thankful to Van Lang University, Vietnam, for providing the budget for this study.

References

[1] M. Munochiveyi, A. C. Pogaku, D. T. Do, A. T. le, M. Voznak, and N. D. Nguyen, "Reconfigurable intelligent surface aided multi-user communications: state-of-the-art techniques and open issues," *IEEE Access*, vol. 9, pp. 118584–118605, 2021.

[2] M. S. Van Nguyen, D. T. Do, S. Al-Rubaye, S. Mumtaz, A. Al-Dulaimi, and O. A. Dobre, "Exploiting impacts of antenna selection and energy harvesting for massive network connectivity," *IEEE Transactions on Communications*, vol. 69, no. 11, pp. 7587–7602, 2021.

[3] D.-T. Do, A.-T. Le, N.-D. Xuan Ha, and N.-N. Dao, "Physical layer security for internet of things via reconfigurable intelligent surface," *Future Generation Computer Systems*, vol. 126, pp. 330–339, 2022.

[4] M. Jain, S. Soni, N. Sharma, and D. Rawal, "Performance analysis at far and near user in NOMA based system in presence of SIC error," *AEU-International Journal of Electronics and Communications*, vol. 114, article 152993, 2020.

[5] N. D. Nguyen, A. -T. Le, and M. Munochiveyi, "Secrecy outage probability of reconfigurable intelligent surface-aided cooperative underlay cognitive radio network communications," in *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 73–77, Tainan, Taiwan, 2021.

[6] X. Wu, J. Ma, C. Gu, X. Xue, and X. Zeng, "Robust Secure Transmission Design for IRS-Assisted mmWave Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, p. 1, 2022.

[7] N. Hehao and L. Ni, "Intelligent reflect surface aided secure transmission in MIMO channel with SWIPT," *IEEE Access*, vol. 8, pp. 192132–192140, 2020.

[8] W. Jiang, B. Chen, J. Zhao, Z. Xiong, and Z. Ding, "Joint active and passive beamforming design for the IRS-assisted MIMOME-OFDM secure communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 10369–10381, 2021.

[9] Y. Song, M. R. A. Khandaker, F. Tariq, K. -K. Wong, and A. Toding, "Truly intelligent reflecting surface-aided secure communication using deep learning," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pp. 1–6, Helsinki, Finland, 2021.

[10] B. Ning, Z. Chen, W. Chen, and L. Li, "Improving security of THz communication with intelligent reflecting surface," in *2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Waikoloa, HI, USA, 2019.

[11] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, O. S. Badarneh, X. Li, and R. Kharel, "Reconfigurable intelligent surface enabled IoT networks in generalized fading channels," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[12] K. Tekbıyık, G. K. Kurt, and H. Yanikomeroglu, "Energy-Efficient RIS-Assisted Satellites for IoT Networks," *IEEE Internet of Things Journal*, 2021.

[13] P. Mursia, V. Sciancalepore, A. Garcia-Saavedra, L. Cottatellucci, X. C. Perez, and D. Gesbert, "RISMA: reconfigurable intelligent surfaces enabling beamforming for IoT massive access," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 4, pp. 1072–1085, 2021.

[14] A. Li, Y. Liu, M. Li, Q. Wu, and J. Zhao, "Joint scheduling design in wireless powered MEC IoT networks aided by reconfigurable intelligent surface," in *2021 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 159–164, Xiamen, China, 2021.

[15] Z. Chu, Z. Zhu, X. Li, F. Zhou, L. Zhen, and N. Al-Dhahir, "Resource Allocation for IRS Assisted Wireless Powered FDMA IoT Networks," *IEEE Internet of Things Journal*, 2021.

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

[17] W. Zhao, G. Wang, S. Atapattu, T. A. Tsiftsis, and C. Tellambura, "Is backscatter link stronger than direct link in reconfigurable intelligent surface-assisted system?," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1342–1346, 2020.

[18] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12296–12300, 2020.

[19] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, "Residual transceiver hardware impairments on cooperative NOMA networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 680–695, 2020.

[20] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Z. Ding, "Exploiting full/half-duplex user relaying in NOMA systems," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 560–575, 2018.

[21] F. Benkhelifa, A. Tall, Z. Rezki, and M. Alouini, "On the low SNR capacity of MIMO fading channels with imperfect channel state information," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 1921–1930, 2014.

[22] X. Li, M. Zhao, M. Zeng et al., "Hardware impaired ambient backscatter NOMA systems: reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, 2021.

[23] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12286–12290, 2020.

[24] J. Chen, L. Yang, and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.

[25] C. Yu, H. Ko, X. Peng, W. Xie, and P. Zhu, "Jammer-aided secure communications for cooperative NOMA systems," *IEEE Communications Letters*, vol. 23, no. 11, pp. 1935–1939, 2019.

[26] Z. Yang, Z. Ding, Y. Wu, and P. Fan, "Novel relay selection strategies for cooperative NOMA," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10114–10123, 2017.

[27] E. Hildebrand, *Introduction to Numerical Analysis*, Dover, New York, USA, 1987.

[28] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician Fading Channel," *IEEE Wireless Communications Letters*, vol. 2, no. 1, pp. 50–53, 2013.