Mobile Networks and Applications (2023) 28:1206–1219
https://doi.org/10.1007/s11036-023-02125-7

Secrecy Performance of Multi-RIS-Assisted Wireless Systems

Ba Cao Nguyen[1] · Quyet-Nguyen Van[2] · Le The Dung[3] · Tran Manh Hoang[1] · Nguyen Van Vinh[4] · Gia Thien Luu[5]

Accepted: 13 January 2023 / Published online: 10 June 2023

Abstract
This paper presents a theoretical framework using multiple reconfigurable intelligent surfaces (RISs) for enhancing the secrecy performance of wireless systems. In particular, multiple RISs are exploited to support transmitter-legitimate user communication under the existence of an eavesdropper. Two practical scenarios are investigated, i.e., there are only transmitter-eavesdropper links (case 1) and there are both transmitter-eavesdropper and transmitter-RIS-eavesdropper links (case 2). We mathematically obtain the closed-form expressions of the average secrecy capacity (ASC) of the considered system in these two investigated cases over Nakagami-*m* fading channels. The impacts of the system parameters, such as the locations of the RISs, the number of REs, and the Nakagami-*m* channels, are deeply evaluated. Computer simulations are used to validate our mathematical analysis. Numerical results clarify the benefits of using multiple RISs for improving the secrecy performance of wireless systems. Specifically, the ASCs in cases 1 and 2 are significantly higher than that in the case without RISs. Importantly, when the locations of the RISs are fixed, we can arrange the larger RSIs near either the transmitter or legitimate user to achieve higher ASCs. In addition, when the numbers of reflecting elements (REs) in the RISs increase, the ASCs in cases 1 and 2 are greatly enhanced.

Keywords Reconfigurable intelligent surfaces · Physical-layer security · Secrecy performance · Eavesdropper · 6G wireless communications

1 Introduction

In the age of the Internet of Things, besides coverage and capacity improvements, security and reliability enhancements of wireless communication systems are the key requirements, especially in the fifth and beyond generations (5G and B5G) of wireless systems [1, 2]. For the security requirements of the 5G and B5G wireless systems, physical layer security (PLS) has been proposed [3]. Unlike classical cryptographic algorithms, PLS utilizes the random nature of wireless channels for information security. Consequently, the PLS can provide secrecy performance without depending on the computation resources of wireless devices [3, 4]. As a result, the PLS is now widely considered and applied to enhance information security in 5G and B5G wireless systems [5–7].

On the other hand, the emergence of reconfigurable intelligent surfaces (RISs) used for assisting wireless systems has greatly attracted the attention of wireless researchers and designers [8, 9]. In particular, the RISs are equipped with many reflecting elements (REs) that can reflect signals transmitted from transmitter to receiver without signal processing [10, 11]. In addition, the RISs can work without power supply, decoding, encoding, and amplifying signals [12]. Consequently, the usage of RISs is much more effective than the usage of classical relays in wireless systems [13, 14]. Therefore, the RISs are promising candidates that can be deployed in B5G wireless systems. Nowadays, the RISs are widely used not only for improving capacity and reducing outage probability but also enhancing information security of the wireless systems [15, 16].

1.1 Related Works

In the literature, the secrecy performance of the RIS-assisted wireless systems has been analyzed in different scenarios such as in vehicular communications [5, 17], cognitive systems [18], and non-orthogonal multiple access networks [19]. Specifically, the key performance metrics such as secrecy

✉ Gia Thien Luu
lg.thien@hutech.edu.vn

Extended author information available on the last page of the article

outage probability (SOP) and secrecy ergodic capacity (SEC) have been derived for evaluating the security performance of the RIS-assisted wireless systems [4, 5, 16–24]. In [5, 20, 21], the authors investigated the case that the reflected signals generated by RIS were not arrived at an eavesdropper. Consequently, the eavesdropper only receives signals transmitted from the transmitter. Their numerical results observed the potential of the RIS for improving the secrecy performance of wireless systems.

In practice, besides receiving signals directly from the transmitter, the eavesdropper can receive signals reflected by the RIS. Thus, the works in [4, 16–19, 22–24] investigated the case that the reflected signals generated by RIS also arrive at the eavesdropper. The SOP expression was derived for the system performance analysis. It was shown that the SOP performance of the wireless systems is greatly improved when the number of REs increases [4, 16, 23]. In addition, the RIS-assisted wireless systems outperform the multiple-input multiple-output systems in terms of PLS [23]. However, the case of utilizing multi-RIS-assisted wireless systems for further enhancing the secrecy performance has not been analyzed yet.

1.2 Motivations and Contributions

As aforementioned, the secrecy performance of one-RIS-assisted wireless systems has been analyzed for both with and without reflected paths generated by RIS [4, 16, 18, 19, 21, 25–27]. Unfortunately, these works used only one RIS. The case of multiple RISs was not considered due to the computational complexity. Meanwhile, in practical scenarios, multiple RISs are often deployed in wireless systems [28]. In particular, multiple RISs are arranged in different areas; thus, either all RISs or some RISs can be used to assist the wireless systems depending on the specific goals [28, 29]. Generally, when multiple RISs are exploited, the performance of wireless systems is significantly improved compared with the case of only one RIS. However, the usage of multiple RISs to improve the secrecy performance of wireless systems was not studied. Furthermore, previous works only considered either the direct link or reflected RIS links at the legitimate users and/or eavesdroppers. The case that signals traveled on both direct link and reflected RIS links are combined at the legitimate users and/or eavesdropper was not considered. These issues motivate us to consider the secrecy performance of the wireless systems under the support of multiple RISs. Specifically, two practical scenarios where the eavesdropper receives signals either via only the transmitter-eavesdropper link or via transmitter-eavesdropper and transmitter-RISs-eavesdropper links are investigated. Also, the considered system is evaluated over Nakagami-m fading channels where the channel parameters are proposed for the 5G standard such as 3rd Generation Partnership Project [28, 30]. The main contributions of this paper can be summarized as follows:

- We consider a multi-RIS-assisted wireless system under the existence of an eavesdropper. Specifically, the eavesdropper receives signals via either direct transmitter-eavesdropper links (case 1) or both direct transmitter-eavesdropper and transmitter-RIS-eavesdropper links (case 2). Additionally, multiple RISs are arranged in different areas to enhance the secrecy performance of the considered system.
- We exploit the benefits of the traditional wireless channel and advanced RISs by combining the direct transmitter-receiver and reflect transmitter-RISs-receiver links to achieve higher signal-to-noise ratio (SNR) power at the receiver. We successfully obtain the closed-form expressions of the average secrecy capacity (ASC) of the considered system in cases 1 and 2 over Nakagami-m fading channels. We validate all derived expressions via computer simulations.
- We evaluate the ASCs of the considered system with the channel model proposed for the 5G standard[1] Numerical results show that the ASCs of the considered system in cases 1 and 2 are significantly higher than that in the case without RISs (case 3). This observation confirms the benefits of using RISs for improving the secrecy performance of wireless systems. Another important observation is that the RISs located near either transmitter or receiver can reflect signals better than the RISs located far from either transmitter or receiver. In addition, the impacts of the number of REs, the total number of REs, the locations of the RISs, and other system parameters are also studied.

The rest of this paper is organized as follows. Section 2 describes the system and signal models, where the formulas of the received signals at the legitimate user and eavesdropper in two cases are provided in detail. Section 3 analyzes the secrecy performance of the considered system by mathematically deriving the ASC expressions in two cases. Section 4 presents the numerical results and discussions to get insights into the system behaviors. Finally, Section 5 concludes this paper.

Notations The cumulative distribution function (CDF) and probability density function (PDF) are, respectively, denoted by $F(.)$ and $f(.)$; the gamma, lower, upper incomplete

[1] We should note that previous works, such as [4, 16], often normalized the system parameters. Thus, their results may not be suitable in 5G and B5G networks. Meanwhile, our results fully reflect the behaviors of 5G and B5G networks because the system and channel parameters are set based on practical measurements.

gamma, and Meijer functions are, respectively, denoted by $\gamma(.,.)$, $\Gamma(.)$, $\Gamma(.,.)$, and $G^{:,:}_{:,:}(.)$; the probability of an event and the expectation operator are, respectively, denoted by $\Pr\{.\}$ and $\mathbb{E}\{.\}$; the Gaussian noise variable with zero mean and variance of σ^2 is denoted by $\mathcal{CN}(0, \sigma^2)$.

2 System Model

Figure 1 illustrates the multi-RIS-assisted wireless system with eavesdropper links. In particular, a base station (S) transmits signals to a legitimate user (D) via S-D direct link and S-RIS-D reflected links. Meanwhile, an eavesdropper (E) attempts to receive and decode the signals transmitted from S via S-E direct link and S-RIS-E reflected links. In the considered system, K RISs are used to assist S-D communication, where each RIS is equipped with L REs. In addition, all transceivers (S, D, and E) are equipped with a single antenna for transmitting/receiving.

Since multiple RISs are deployed to support S—D communication, the channels from RISs to E may or may not be available. As a result, we consider two scenarios: i) E only receives signals via the S-E link. The reflected links via RISs are not available at E due to blocking objects (similar to the works in [5, 20, 21]); ii) E receives signals via both S-E link and RIS reflected links.

The received signal at the legitimate user D is expressed as

$$y_d = \left(\hat{h}_{sd} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} \hat{g}_{kl}\hat{h}_{kl}e^{j\varphi_{kl}}\right)x_s + z_d, \tag{1}$$

where $\hat{h}_{sd}$, $\hat{g}_{kl}$ and $\hat{h}_{kl}$ are, respectively, the channels from S to D, from S to the lth RE of the kth RIS, and from the lth RE of the kth RIS to D; φ_{kl} is the phase shift of the lth RE of the kth RIS; x_s is the transmitted signal at S; $z_d \sim \mathcal{CN}(0, \sigma_d^2)$ is the Gaussian noise at the D.

Using the magnitudes and phases of the complex numbers, we can represent $\hat{h}_{sd}$, $\hat{g}_{kl}$, and $\hat{h}_{kl}$ as $\hat{h}_{sd} = h_{sd}e^{-j\phi_{sd}}$, $\hat{g}_{kl} = g_{kl}e^{-j\theta_{kl}}$, and $\hat{h}_{kl} = h_{kl}e^{-j\psi_{kl}}$, where h_{sd}, g_{kl}, and h_{kl} are the magnitudes and ϕ_{sd}, θ_{kl}, and ψ_{kl} are the phases of $\hat{h}_{sd}$, $\hat{g}_{kl}$, and $\hat{h}_{kl}$, respectively.

Now, the received signal at D becomes

$$\begin{aligned} y_d =& \left(h_{sd}e^{-j\phi_{sd}} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}h_{kl}e^{j(\varphi_{kl}-\theta_{kl}-\psi_{kl})}\right)x_s + z_d \\ =& e^{-j\phi_{sd}}\left(h_{sd} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}h_{kl}e^{j\zeta_{kl}}\right)x_s + z_d. \end{aligned} \tag{2}$$

where $\zeta_{kl} = \varphi_{kl} - \theta_{kl} - \psi_{kl} + \phi_{sd}$ is the phase error induced by the lth RE of the kth RIS [28].

As demonstrated in previous works on one-RIS or multi-RIS-assisted wireless systems, the phase of the RIS φ_{kl} can be adjusted to achieve maximum received signal power [8, 13, 28, 31]. Specifically, φ_{kl} can be chosen from a set of discrete phases so that $\zeta_{kl} = 0$ [28]. This value of φ_{kl} is the optimal phase of the RIS, which is computed as

$$\varphi_{kl}^{*} = \theta_{kl} + \psi_{kl} - \phi_{sd}. \tag{3}$$

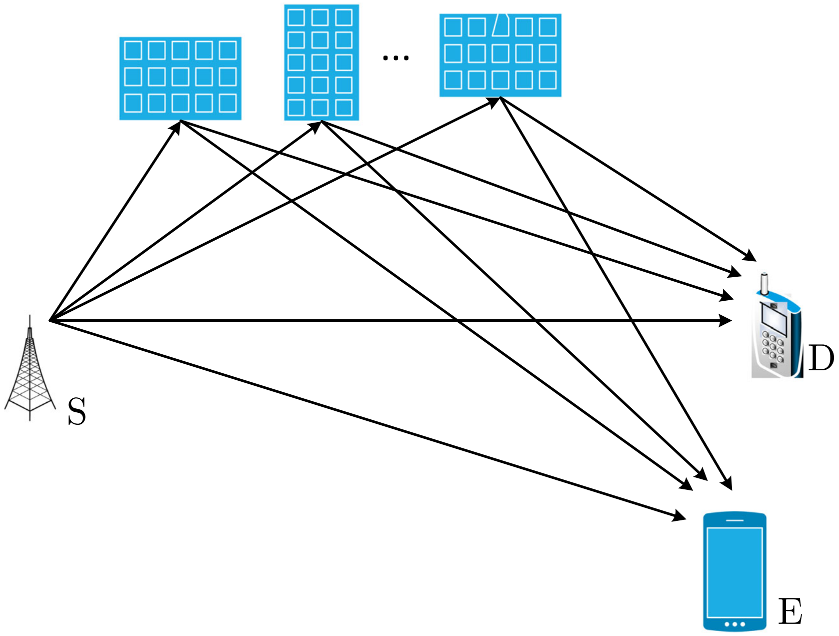

Fig. 1 The system model of the considered multi-RIS-assisted wireless system with eavesdropping link

With φ_{kl}^{*} of the RISs, the received signal at D now is

$$y_d = e^{-j\phi_{sd}}\Big(h_{sd} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}h_{kl}\Big)x_s + z_d. \qquad (4)$$

Since $|e^{-j\phi_{sd}}|^2 = 1$, the instantaneous signal-to-noise ratio (SNR) at D is

$$\begin{aligned}\beta_d &= \frac{\Big(h_{sd} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}h_{kl}\Big)^2 P_s}{\sigma_d^2}\\ &= \Big(h_{sd} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}h_{kl}\Big)^2 \rho_d,\end{aligned} \qquad (5)$$

where $\rho_d = P_s/\sigma_d^2$ is the average SNR at D.

At the eavesdropper E, the received signal is computed as

$$y_e = \Big(\hat{h}_{se} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} \hat{g}_{kl}\hat{r}_{kl}e^{j\varphi_{kl}}\Big)x_s + z_e, \qquad (6)$$

where $\hat{h}_{se}$ and $\hat{r}_{kl}$ are, respectively, the channels from S to E and from the lth RE of the kth RIS to E; $z_e \sim \mathcal{CN}(0, \sigma_e^2)$ is the Gaussian noise at the E.

In the literature on RIS-assisted multi-user systems, when RISs configure their phases to maximize the SNR at one user, the SNRs at other users may not be maximized [32]. However, the case that maximum SNRs at all users is often assumed [33]. This assumption has been widely used not only for legitimate users but also for eavesdroppers [4, 16, 18, 19, 21]. Similar to these works, in this paper, we assume that the received signal at E can be maximal. In other words, we consider the worst case of the secrecy performance, where maximum SNR at the E is achieved. As a result, the received signal at E can be presented as

$$y_e = e^{-j\phi_{se}}\Big(h_{se} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}r_{kl}\Big)x_s + z_e, \qquad (7)$$

where h_{se} and ϕ_{se} are, respectively, the amplitude and phase of $\hat{h}_{se}$; r_{kl} is the amplitude of $\hat{r}_{kl}$.

In case 1, due to the blocking objects, the reflected paths from the RISs are not available at E. In other words, we have $r_{kl} = 0$. Thus, the instantaneous SNR at E is expressed as

$$\beta_e^{c1} = \frac{h_{se}^2 P_s}{\sigma_e^2} = h_{se}^2\rho_e, \qquad (8)$$

where $\rho_e = P_s/\sigma_e^2$ is the average SNR at E.

In case 2, the reflected paths from the RISs are available at E. Thus, the instantaneous SNR at E is

$$\begin{aligned}\beta_e^{c2} &= \frac{\Big(h_{se} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}r_{kl}\Big)^2 P_s}{\sigma_e^2}\\ &= \Big(h_{se} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}r_{kl}\Big)^2 \rho_e.\end{aligned} \qquad (9)$$

On the other hand, the CDF and PDF of the channel amplitudes (h_{sd}, h_{se}, g_{kl}, h_{kl}, and r_{kl}) which follow the Nakagami-m distributions are, respectively, given by

$$\begin{aligned}F_X(x) &= \frac{1}{\Gamma(m_X)}\gamma\Big(m_X, \frac{m_X}{\Omega_X}x^2\Big)\\ &= 1 - \frac{1}{\Gamma(m_X)}\Gamma\Big(m_X, \frac{m_X}{\Omega_X}x^2\Big),\ x \geq 0,\end{aligned} \qquad (10)$$

$$f_X(x) = \frac{2m_X^{m_X}}{\Gamma(m_X)\Omega_X^{m_X}}x^{2m_X-1}\exp\Big(-\frac{m_X}{\Omega_X}x^2\Big),\ x \geq 0, \qquad (11)$$

where $X \in \{sd, se, g_k, h_k, r_k\}$; m_X and Ω_X are, respectively, the shape and spread parameters. The spread parameter calculated by the path loss model applied in the 5G standard is given as [13, 28, 30]

$$\Omega_X = G_{\rm tx} + G_{\rm rx} - 22.7 - 26\log(f_c) - 36.7\log(d/d_0), \qquad (12)$$

where $G_{\rm tx}$ (tx $\in \{s, ris\}$) and $G_{\rm rx}$ (rx $\in \{ris, d, e\}$) are, respectively, the antenna gains of the transmitter and receiver; f_c is the carrier frequency; d and d_0 are, respectively, the transmitter-receiver and reference distances.

Furthermore, the variance of the Gaussian noise is given as [28]

$$\sigma^2 = N_0 + 10\log(\mathrm{BW}) + \mathrm{NF}, \qquad (13)$$

where N_0, BW, and NF are, respectively, the thermal noise power density, bandwidth, and noise figure.

3 Secrecy Performance Analysis

In this section, we will derive the average secrecy capacity expression of the considered system over Nakagami-m fading channels. In particular, the ASC of the considered system is defined as the difference between the capacities of the legitimate channel and the wiretap channel. Mathematically, it is computed as [21]

$$\mathcal{C} = [\mathbb{E}\left\{\log_2(1+\beta_d) - \log_2(1+\beta_e)\right\}]^+, \tag{14}$$

where β_d is given in Eq. 5; β_e is given in Eq. 8 for case 1 and Eq. 9 for case 2; $[x]^+ = \max\{x, 0\}$.
From the properties of expectation [34], Eq. 14 can be rewritten as

$$\mathcal{C} = [\mathbb{E}\left\{\log_2(1+\beta_d)\right\} - \mathbb{E}\left\{\log_2(1+\beta_e)\right\}]^+. \tag{15}$$

We should note that in case 2, β_d and β_e are not independent because of g_{kl}; however, Eq. 15 is still correct due to the expectation properties. As a result, Eq. 15 has been widely utilized when calculating the ASC of RIS-assisted wireless systems [4, 19–23].

Consequently, the ASC of the considered system in these two cases can be, respectively, expressed as

$$\mathcal{C}^{c1} = \mathcal{C}_d - \mathcal{C}_e^{c1}, \tag{16}$$

$$\mathcal{C}^{c2} = \mathcal{C}_d - \mathcal{C}_e^{c2}, \tag{17}$$

where $\mathcal{C}_d = \mathbb{E}\left\{\log_2(1+\beta_d)\right\}$, $\mathcal{C}_e^{c1} = \mathbb{E}\left\{\log_2(1+\beta_e^{c1})\right\}$, and $\mathcal{C}_e^{c2} = \mathbb{E}\left\{\log_2(1+\beta_e^{c2})\right\}$. Notice that if $\mathcal{C}_d < \mathcal{C}_e^{c1}$, we have $\mathcal{C}^{c1} = 0$. It is similar for $\mathcal{C}^{c2}$.

Based on Eqs. 16 and 17, we obtain the ASCs of the considered system in the following Theorem.

Theorem *The ASCs of the considered system in cases 1 and 2 over Nakagami-m fading channels are, respectively, given by*

$$\begin{aligned}\mathcal{C}^{c1} =& \frac{2^{\Xi_d - 1}}{\sqrt{\pi}\Gamma(\Xi_d)\ln 2} G_{3,5}^{5,3}\left(\frac{\Psi_d^2}{4\rho_d}\middle|_{\frac{\Xi_d}{2},\frac{\Xi_d+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right) \\ &- \frac{1}{\Gamma(m_{se})\ln 2} G_{2,3}^{3,1}\left(\frac{m_{se}}{\Omega_{se}\rho_e}\middle|_{0,m_{se},0}^{0,1}\right),\end{aligned} \tag{18}$$

$$\begin{aligned}\mathcal{C}^{c2} =& \frac{2^{\Xi_d - 1}}{\sqrt{\pi}\Gamma\left(\Xi_d\right)\ln 2} G_{3,5}^{5,3}\left(\frac{\Psi_d^2}{4\rho_d}\middle|_{\frac{\Xi_d}{2},\frac{\Xi_d+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right) \\ &- \frac{2^{\Xi_e - 1}}{\sqrt{\pi}\Gamma\left(\Xi_e\right)\ln 2} G_{3,5}^{5,3}\left(\frac{\Psi_e^2}{4\rho_e}\middle|_{\frac{\Xi_e}{2},\frac{\Xi_e+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right),\end{aligned} \tag{19}$$

where Ξ_d, Ψ_d, Ξ_e, and Ψ_e are, respectively, given in Eqs. 61,62,63 and 64.

Proof : To derive the ASCs in Eqs. 18 and 19, we must firstly derive $\mathcal{C}_d$, $\mathcal{C}_e^{c1}$, and $\mathcal{C}_e^{c2}$, then replace them into Eqs. 16 and 17.

First, $\mathcal{C}_d$, $\mathcal{C}_e^{c1}$, and $\mathcal{C}_e^{c2}$ can be calculated as

$$\mathcal{C}_d = \mathbb{E}\left\{\log_2(1+\beta_d)\right\} = \frac{1}{\ln 2}\int_0^\infty \frac{1 - F_{\beta_d}(x)}{1+x}dx, \tag{20}$$

$$\mathcal{C}_e^{c1} = \mathbb{E}\left\{\log_2(1+\beta_e^{c1})\right\} = \frac{1}{\ln 2}\int_0^\infty \frac{1 - F_{\beta_e^{c1}}(x)}{1+x}dx, \tag{21}$$

$$\mathcal{C}_e^{c2} = \mathbb{E}\left\{\log_2(1+\beta_e^{c2})\right\} = \frac{1}{\ln 2}\int_0^\infty \frac{1 - F_{\beta_e^{c2}}(x)}{1+x}dx. \tag{22}$$

Next, we have to obtain the CDFs of β_d, β_e^{c1}, and β_e^{c2} and then replace them into Eqs. 20,21 and 22. Mathematically, $F_{\beta_d}(x)$, $F_{\beta_e^{c1}}(x)$, and $F_{\beta_e^{c2}}(x)$ are, respectively, computed as

$$\begin{aligned}F_{\beta_d}(x) &= \Pr\left\{\beta_d < x\right\} \\ &= \Pr\left\{\left(h_{sd} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}h_{kl}\right)^2 \rho_d < x\right\},\end{aligned} \tag{23}$$

$$F_{\beta_e^{c1}}(x) = \Pr\left\{\beta_e^{c1} < x\right\} = \Pr\left\{h_{se}^2\rho_e < x\right\}, \tag{24}$$

$$\begin{aligned}F_{\beta_e^{c2}}(x) &= \Pr\left\{\beta_e^{c2} < x\right\} \\ &= \Pr\left\{\left(h_{se} + \sum_{k=1}^{K}\sum_{l=1}^{L_k} g_{kl}r_{kl}\right)^2 \rho_e < x\right\}.\end{aligned} \tag{25}$$

From these above expressions, we can obtain $F_{\beta_d}(x)$, $F_{\beta_e^{c1}}(x)$, and $F_{\beta_e^{c2}}(x)$ as (the detailed calculations are presented in Appendix)

$$F_{\beta_d}(x) = 1 - \frac{1}{\Gamma(\Xi_d)}\Gamma\left(\Xi_d, \Psi_d\sqrt{\frac{x}{\rho_d}}\right), \tag{26}$$

$$F_{\beta_e^{c1}}(x) = 1 - \frac{1}{\Gamma(m_{se})}\Gamma\left(m_{se}, \frac{m_{se}x}{\Omega_{se}\rho_e}\right), \tag{27}$$

$$F_{\beta_e^{c2}}(x) = 1 - \frac{1}{\Gamma(\Xi_e)}\Gamma\left(\Xi_e, \Psi_e\sqrt{\frac{x}{\rho_e}}\right). \tag{28}$$

On the other hand, using [35, Eq. (8.4.2.5)] and [35, Eq. (8.4.16.2)], we have

$$(1+x)^{-1} = G_{1,1}^{1,1}\left(x\middle|_{0}^{0}\right), \tag{29}$$

$$\Gamma(a,x) = G_{1,2}^{2,0}\left(x\middle|_{a,0}^{1}\right). \tag{30}$$

Now, $\mathcal{C}_d$, $\mathcal{C}_e^{c1}$, and $\mathcal{C}_e^{c2}$ are, respectively, calculated as

$$\begin{aligned}\mathcal{C}_d &= \frac{1}{\Gamma(\Xi_d)\ln 2}\int_0^\infty \frac{1}{1+x}\Gamma\left(\Xi_d, \Psi_d\sqrt{\frac{x}{\rho_d}}\right)dx\\ &= \frac{1}{\Gamma(\Xi_d)\ln 2}\int_0^\infty G_{1,1}^{1,1}\left(x\middle|_{0}^{0}\right)G_{1,2}^{2,0}\left(\Psi_d\sqrt{\frac{x}{\rho_d}}\middle|_{\Xi_d,0}^{1}\right)dx,\end{aligned} \tag{31}$$

$$\begin{aligned}\mathcal{C}_e^{c1} &= \frac{1}{\Gamma(m_{se})\ln 2}\int_0^\infty \frac{1}{1+x}\Gamma\left(m_{se}, \frac{m_{se}x}{\Omega_{se}\rho_e}\right)dx\\ &= \frac{1}{\Gamma(m_{se})\ln 2}\int_0^\infty \frac{1}{1+x}G_{1,2}^{2,0}\left(\frac{m_{se}x}{\Omega_{se}\rho_e}\middle|_{m_{se},0}^{1}\right)dx,\end{aligned} \tag{32}$$

$$\begin{aligned}\mathcal{C}_e^{c2} &= \frac{1}{\Gamma(\Xi_e)\ln 2}\int_0^\infty \frac{1}{1+x}\Gamma\left(\Xi_e, \Psi_e\sqrt{\frac{x}{\rho_e}}\right)dx\\ &= \frac{1}{\Gamma(\Xi_e)\ln 2}\int_0^\infty G_{1,1}^{1,1}\left(x\middle|_{0}^{0}\right)G_{1,2}^{2,0}\left(\Psi_e\sqrt{\frac{x}{\rho_e}}\middle|_{\Xi_e,0}^{1}\right)dx.\end{aligned} \tag{33}$$

Applying [35, Eq. (2.24.1.1)], Eqs. 31 and 33 respectively become

$$\mathcal{C}_d = \frac{2^{\Xi_d-1}}{\sqrt{\pi}\Gamma(\Xi_d)\ln 2}G_{3,5}^{5,3}\left(\frac{\Psi_d^2}{4\rho_d}\middle|_{\frac{\Xi_d}{2},\frac{\Xi_d+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right), \tag{34}$$

$$\mathcal{C}_e^{c2} = \frac{2^{\Xi_e-1}}{\sqrt{\pi}\Gamma(\Xi_e)\ln 2}G_{3,5}^{5,3}\left(\frac{\Psi_e^2}{4\rho_e}\middle|_{\frac{\Xi_e}{2},\frac{\Xi_e+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right). \tag{35}$$

Using [36, Eq. (7.811.5)], Eq. 32 becomes

$$\mathcal{C}_e^{c1} = \frac{1}{\Gamma(m_{se})\ln 2}G_{2,3}^{3,1}\left(\frac{m_{se}}{\Omega_{se}\rho_e}\middle|_{0,m_{se},0}^{0,1}\right). \tag{36}$$

Finally, replacing Eqs. 34, 36 and 35 into Eqs. 16 and 17, we obtain the ASCs of the considered system as in Eqs. 18 and 19. The proof is thus complete.

4 Numerical Results and Discussions

In this section, the secrecy performance of the considered system is examined by using the analysis expressions. Computer simulations are used to verify our numerical expressions. Besides investigating the ASCs in cases 1 and 2, the ASC in the case without RISs (denoted by “Case 3" in all below figures) is also provided to show the benefits of using RISs. Unless otherwise specified, in all scenarios, we set $K = 5$ RISs and $m_{sd} = m_{se} = m_{g_k} = m_{h_k} = m_{r_k} = m$. To obtain the spread parameter and noise power given in Eqs. 12 and 13, respectively, we set $G_s = G_d = G_{ris} = 5$ dB, $G_e = 0$ dB, $f_c = 3$ GHz, $d_0 = 1$ m, $d_{sd} = 100$ m, $d_{se} = 150$ m, BW $= 10$ MHz, $N_0 = -174$ dBm/Hz, and NF $= 10$ dBm. The number of REs in each RIS is determined via vector $\mathbf{L}$, i.e., $\mathbf{L} = [L_1\ L_2\ L_3\ L_4\ L_5]$, where L_k $(k \in \{1, 2, .., 5\})$ denotes the number of REs in the kth RIS. Additionally, we use the coordinate axis (x_k, y_k) to indicate the location of the kth RIS, with $(0, 0)$ is the location of S.

Figure 2 illustrates the ASCs of the considered system in cases 1 and 2 in comparison with the ASC in the case without RISs (case 3) for $m = 2$, $\mathbf{L} = [40\ 40\ 40\ 40\ 40]$, and $(x, y) = (30, 10), (40, 10), (50, 10), (60, 10)$, and $(70, 10)$. We use Eqs. 18 and 19 to obtain the analysis curves in cases 1 and 2, respectively. Notice that with the investigated parameters, the numbers of REs in all RISs are equal. However, they are located in different locations, where the 1st RIS is located

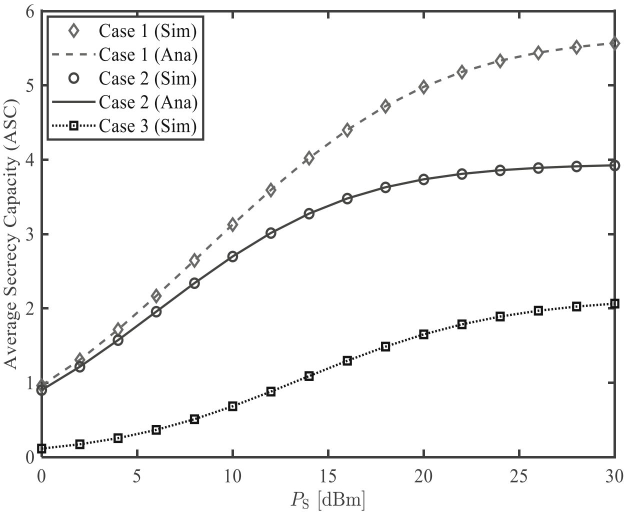

Fig. 2 The ASCs of the considered system in the cases 1 and case 2 in comparison with the ASC in the case without RISs for $m = 2$, $\mathbf{L} = [40\ 40\ 40\ 40\ 40]$, and $(x, y) = (30, 10), (40, 10), (50, 10), (60, 10)$, and $(70, 10)$

nearest to the S and the 5th RIS is located furthest from the S. It is easy to see in Fig. 2 that the ASC in case 1 is the best while the ASC in case 3 is the worst. This result demonstrates the benefits of using RISs for improving the ASC of wireless systems. For example, when $P_s = 16$ dBm, the ASCs in the cases 1, 2, and 3 are, respectively, 4.4, 3.5, and 1.3 bit/s/Hz. That means cases 1 and 2 can achieve 3.1 and 2.2 bit/s/Hz higher ASC in comparison with case 3. As P_s increases, the ASCs of three cases increase. However, the increasing rates of the ASCs in cases 2 and 3 are slow in the high transmit power regime ($P_s > 25$ dBm). Also, all ASCs gradually reach the capacity ceiling when $P_s > 30$ dBm.

Figure 3 investigates the effects of the distance between S and E (d_{se}) on the ASCs of the considered system. As shown in Fig. 3, even $d_{se} = 100$ m, the ASCs in cases 1 and 2 are still high, especially in case 1. Meanwhile, the ASC in case 3 equals zero. In other words, even though the distances between transmitter and legitimate user and between transmitter and eavesdropper are identical ($d_{sd} = d_{se} = 100$ m), the usage of RISs still significantly enhances the ASC of wireless systems. Another observation is that when $d_{se} = 100$ m, the ASCs with $P_s = 15$ and $P_s = 30$ dBm are similar for cases 2 and 3. Meanwhile, they are different for case 1. As d_{se} increases, the ASCs in three cases increase for both $P_s = 15$ and $P_s = 30$ dBm. In particular, when $d_{se} = 200$ m, the ASCs in cases 1 and 2 are greatly higher than that in case 3 for both $P_s = 15$ and $P_s = 30$ dBm. Specifically, the ASCs in cases 1 and 2 with $P_s = 15$ dBm are higher than the ASC in case 3 with $P_s = 30$ dBm. Thus, besides enhancing the secrecy performance, the RISs help to reduce the power consumption of the transmitter. As a result, the usage of RISs can significantly improve the secrecy performance and energy efficiency of wireless systems.

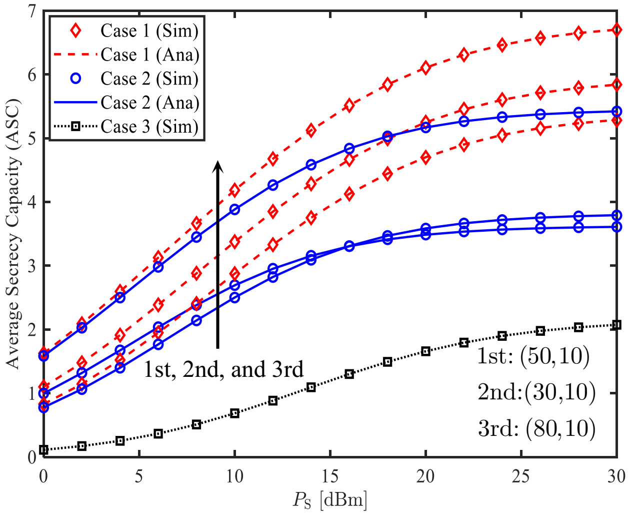

Fig. 4 The impacts of the locations of the RISs on the ASCs of the considered system for $m = 2$ and $\mathbf{L} = [40\ 40\ 40\ 40\ 40]$.

In Fig. 4, the impacts of the locations of the RISs on the ASCs of the considered system are investigated. Unlike Figs. 2 and 3, the locations of all RISs in Fig. 4 are similar for each investigated scenario. For example, the 1st: (50, 10) in Fig. 4 indicates that $(x, y) = (50, 10), (50, 10), (50, 10), (50, 10)$, and (50, 10). In other words, all RISs in the 1st scenario are

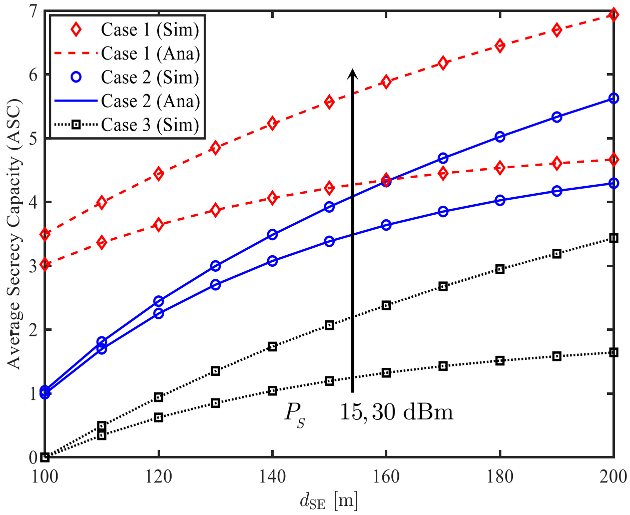

Fig. 3 The ASCs of the considered system versus the distance between S and E for $P_s = 15$ and 30 dBm, $m = 2$, $\mathbf{L} = [40\ 40\ 40\ 40\ 40]$, and $(x, y) = (30, 10), (40, 10), (50, 10), (60, 10)$, and (70, 10)

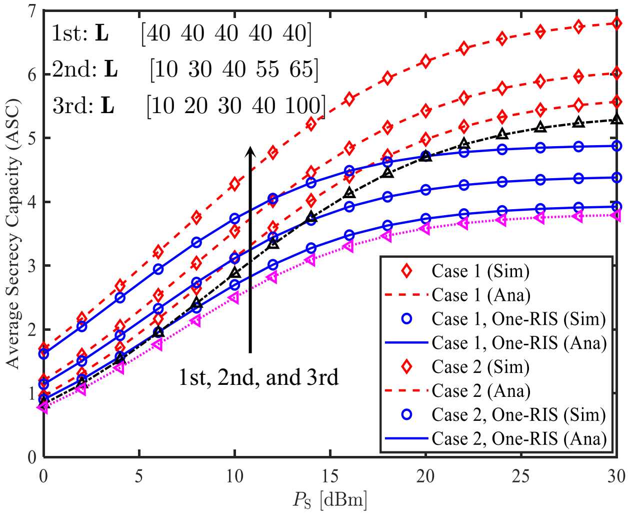

Fig. 5 The ASCs of the considered system for different numbers of REs in each RIS, $m = 2$, $(x, y) = (30, 10), (40, 10), (50, 10), (60, 10)$, and (70, 10)

located right in the middle between S and D. Meanwhile, all RISs in the 2nd and 3rd scenarios are located near to S and far from S, respectively. As observed in Fig. 4, the ASCs in the 3rd scenario are the best, and the ASCs in the 1st scenario are the worst among the three scenarios. On the other hand, the ASCs of the 1st and 2nd scenarios of case 2 are nearly similar. Meanwhile, they are significantly different in case 1. Hence, the locations of the RISs greatly affect the ASCs of the considered system. Additionally, we can locate RISs near either transmitter or receiver in practice to achieve higher ASCs.

In Fig. 5, three investigated scenarios such as $\mathbf{L} = [40\ 40\ 40\ 40\ 40]$, $\mathbf{L} = [10\ 30\ 40\ 55\ 65]$, and $\mathbf{L} = [10\ 20\ 30\ 40\ 100]$ are evaluated, where the number of REs in each RIS is varied. We should note that the total number of REs in all RISs is identical, i.e., equal to 200, in three scenarios. We also provide the ASCs in cases 1 and 2 with only one RIS (denoted by "One-RIS" in Fig. 5). Note that the ASCs with only one RIS are obtained by setting $K = 1$ RIS, $L = 200$ REs, and $(x, y) = (50, 10)$. Figure 5 confirms the great benefits of the considered multi-RIS-assisted wireless system in comparison with one-RIS-assisted wireless systems presented in the previous works [4, 19, 20]. It is obvious from Fig. 5 that with these parameter settings, the ASCs in the 3rd scenario are the best while the ASCs in the 1st scenario are the worst. As a result, when the locations of the RISs are different, the ASCs can be higher with different numbers of REs in the RISs. In particular, when $P_s = 30$ dBm, the ASCs are 5.6, 6, and 6.8 in case 1 and 3.9, 4.4, and 4.9 bit/s/Hz in case 2 corresponding to the 1st, 2nd, and 3rd scenarios. Furthermore, when the numbers of REs in the RISs vary from the 1st to the 3rd scenarios, the ASCs increase 1.2 and 1 bit/s/Hz for cases 1 and 2, respectively. Therefore, besides locating the RISs in suitable areas, we should choose an appropriate number of REs in each RIS to improve the ASC of the wireless systems.

Unlike Fig. 5, where the total number of REs in all RISs is constant, the total number of REs in all RISs in Fig. 6 is varied, i.e., $\mathbf{L} = [10\ 10\ 10\ 10\ 10]$, $\mathbf{L} = [20\ 20\ 20\ 20\ 20]$, ..., and $\mathbf{L} = [50\ 50\ 50\ 50\ 50]$. As shown in Fig. 6, an increase of the number of REs in the RISs significantly enhances the ASCs of the considered system. Specifically, even when the number of REs in the RISs is small (i.e., $L = 10$), the ASCs in cases 1 and 2 are still higher than that in case 3. When L increases, i.e., $L = 20, 30, 40$, and 50, the ASCs in cases 1 and 2 greatly increase, especially in case 1. Another observation is that the ASCs in cases 1 and 2 are almost linearly proportional to L. Thus, we can use larger L to achieve higher ASCs of the considered system.

In Fig. 7, the severity of Nakagami-m fading is varied, i.e., $m = 1, 3$, and 5. Other system parameters are similar to those in Fig. 2. Notice that in the case $m = 1$, the Nakagami-m fading channels become the Rayleigh fading channels. Obviously, the ASCs in the three cases remarkably increase when m increases from 1 to 3. However, when m increases from 3 to 5, these ASCs are nearly unchanged. Specifically, with high transmission power, i.e., $P_s = 30$ dBm, the ASCs are similar for different m. As a result, higher values of m cannot improve the ASCs of the considered system in cases 1 and 2, even with high transmission power. Therefore, when the considered system operates in environments with higher

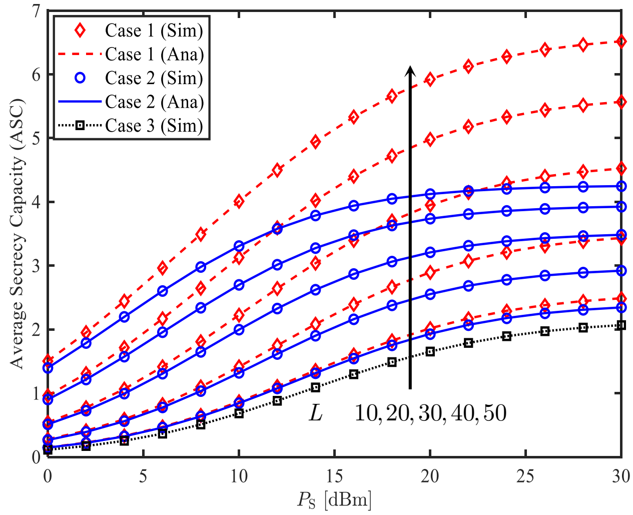

Fig. 6 The ASCs of the considered system when the total number of REs in all RISs varies for $m = 2$, $(x, y) = (30, 10)$, $(40, 10)$, $(50, 10)$, $(60, 10)$, and $(70, 10)$

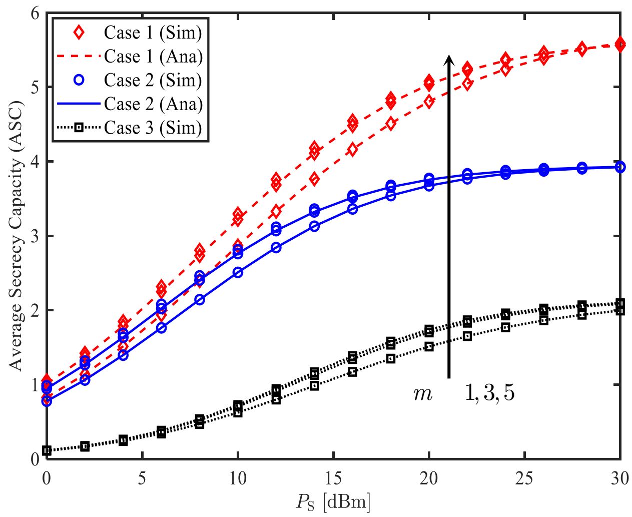

Fig. 7 The ASCs of the considered system for different values of Nakagami-m parameter

m, we should use a suitable transmission power to exploit the benefit of these environments and avoid the ASC ceilings. On the other hand, since we set $\rho_d = \rho_e$, the ASCs of the considered system are saturated in the high transmit power regime. This feature is reasonable because β_d and β_e are nearly parallel when P_s increases. As a result, the subtraction of $\log_2(1+\beta_d) - \log_2(1+\beta_e)$ becomes a constant in the high transmit power regime[2]

5 Conclusion

This paper exploits multiple RISs to enhance the secrecy performance of a wireless system with an eavesdropper. We successfully derived the closed-form expressions of the average secrecy capacity of the considered system over Nakagami-m fading channels in two cases, where the eavesdropper receives signals from either transmitter-eavesdropper link or both transmitter-eavesdropper and transmitter-RIS-eavesdropper links. Numerical results showed that using multiple RISs significantly increases the ASCs of the considered system compared to the case without RISs. Specifically, when the number of REs in each RIS is constant, by choosing suitable locations of the RISs, the ASCs of the considered system are significantly enhanced. When the locations of the RISs are fixed, the locations near either the base station or legitimate receiver should be used for RISs with a larger number of REs to achieve higher secrecy performance. On the other hand, using RISs with larger sizes is also a suitable method for improving the secrecy performance of the considered system.

Funding The authors did not receive support from any organization for the submitted work.

Data Availability Data will be made available on reasonable request.

Declarations

Competing Interests The authors have no competing interests to declare that are relevant to the content of this article.

Appendix

This appendix detailedly provides the step-by-step derivations of the CDFs of β_d, β_e^{c1}, and β_e^{c2}.

Firstly, $F_{\beta_e^{c1}}(x)$ can be derived directly by using the CDF of the channel gain following Nakagami-m fading channels [37], i.e.,

$$\begin{aligned}F_{\beta_e^{c1}}(x) &= \Pr\left\{h_{se}^2\rho_e < x\right\} = \Pr\left\{h_{se}^2 < \frac{x}{\rho_e}\right\}\\ &= \frac{1}{\Gamma(m_{se})}\gamma\left(m_{se}, \frac{m_{se}x}{\Omega_{se}\rho_e}\right)\\ &= 1 - \frac{1}{\Gamma(m_{se})}\Gamma\left(m_{se}, \frac{m_{se}x}{\Omega_{se}\rho_e}\right).\end{aligned} \tag{37}$$

Secondly, $F_{\beta_d}(x)$ and $F_{\beta_e^{c2}}(x)$ are calculated as follows. Let $\mathcal{X}_{dkl} = g_{kl}h_{kl}$, $\mathcal{Y}_{dk} = \sum_{l=1}^{L_k}\mathcal{X}_{dkl}$, $\mathcal{Z}_d = \sum_{k=1}^{K}\mathcal{Y}_{dk}$, $\mathcal{T}_d = h_{sd} + \mathcal{Z}_d$, $\mathcal{X}_{ekl} = g_{kl}r_{kl}$, $\mathcal{Y}_{ek} = \sum_{l=1}^{L_k}\mathcal{X}_{ekl}$, $\mathcal{Z}_e = \sum_{k=1}^{K}\mathcal{Y}_{ek}$, and $\mathcal{T}_e = h_{se} + \mathcal{Z}_e$ be new variables, Eqs. 23 and 25 respectively become

$$F_{\beta_d}(x) = \Pr\left\{\mathcal{T}_d^2\rho_d < x\right\}, \tag{38}$$

$$F_{\beta_e^{c2}}(x) = \Pr\left\{\mathcal{T}_e^2\rho_e < x\right\}. \tag{39}$$

It is obvious that $F_{\beta_d}(x)$ and $F_{\beta_e^{c2}}(x)$ have similar types. Thus, in the following parts, we focus on deriving $F_{\beta_d}(x)$, $F_{\beta_e^{c2}}(x)$ can be derived similarly as $F_{\beta_d}(x)$.

Since the Nakagami-m fading channels are considered, the nth moment of h_{sd} is given by [28]

$$\mu_{h_{sd}}(n) \triangleq \mathbb{E}\{h_{sd}^n\} = \frac{\Gamma(m_{sd}+n/2)}{\Gamma(m_{sd})}\left(\frac{m_{sd}}{\Omega_{sd}}\right)^{-n/2}. \tag{40}$$

From Eq. 40, we obtain the first and second moments of h_{sd} as

$$\mu_{h_{sd}}(1) = \frac{\Gamma(m_{sd}+1/2)}{\Gamma(m_{sd})}\sqrt{\frac{\Omega_{sd}}{m_{sd}}}, \tag{41}$$

$$\mu_{h_{sd}}(2) = \frac{\Gamma(m_{sd}+1)\Omega_{sd}}{\Gamma(m_{sd})m_{sd}} = \Omega_{sd}. \tag{42}$$

Since $\mathcal{X}_{dkl} = g_{kl}h_{kl}$, the PDF of $\mathcal{X}_{dkl}$ is calculated as

$$f_{\mathcal{X}_{dkl}}(y) = \int_0^\infty \frac{1}{x} f_{h_{kl}}\left(\frac{y}{x}\right) f_{g_{kl}}(x)dx. \tag{43}$$

[2] In the previous works, since ρ_e is fixed while ρ_d is increased when P_s increases, the ASC avoids the saturation ceilings in the high transmit power regime [4].

Replacing the PDF given in Eq. 11 into Eq. 43, we have

$$f_{\mathcal{X}_{dkl}}(y) = \frac{4}{\Gamma(m_{g_k})\Gamma(m_{h_k})}\left(\frac{m_{g_k}}{\Omega_{g_k}}\right)^{m_{g_k}}\left(\frac{m_{h_k}}{\Omega_{h_k}}\right)^{m_{h_k}} \times y^{2m_{h_k}-1}\int_0^\infty x^{2m_{g_k}-2m_{h_k}-1} \times \exp\left(-\frac{m_{g_k}x^2}{\Omega_{g_k}}-\frac{y^2 m_{h_k}}{\Omega_{h_k}x^2}\right)dx. \quad (44)$$

Applying [36, Eq. (3.478.4)], Eq. 44 becomes

$$f_{\mathcal{X}_{dkl}}(y) = \frac{4\alpha_{kl}^{m_{g_k}+m_{h_k}}}{\Gamma(m_{g_k})\Gamma(m_{h_k})} y^{m_{g_k}+m_{h_k}-1}\mathcal{K}_{m_{g_k}-m_{h_k}}(2\alpha_{kl}y), \quad (45)$$

where $\alpha_{kl} = \sqrt{\frac{m_{g_k}m_{h_k}}{\Omega_{g_k}\Omega_{h_k}}}$.

Now, the nth moment of $\mathcal{X}_{dkl}$ is computed as

$$\mu_{\mathcal{X}_{dkl}}(n) \triangleq \mathbb{E}\{\mathcal{X}_{dkl}^n\} = \int_0^\infty y^n f_{\mathcal{X}_{dkl}}(y)dy. \quad (46)$$

Using [36, Eq. (6.561.16)], Eq. 46 becomes

$$\mu_{\mathcal{X}_{dkl}}(n) = \alpha_{kl}^{-n}\frac{\Gamma(m_{g_k}+n/2)\Gamma(m_{h_k}+n/2)}{\Gamma(m_{g_k})\Gamma(m_{h_k})}. \quad (47)$$

Then, the CDF of $\mathcal{X}_{dkl}$ is given by

$$F_{\mathcal{X}_{dkl}}(x) \approx \frac{1}{\Gamma\left(\frac{[\mu_{\mathcal{X}_{dkl}}(1)]^2}{\mu_{\mathcal{X}_{dkl}}(2)-[\mu_{\mathcal{X}_{dkl}}(1)]^2}\right)} \times \gamma\left(\frac{[\mu_{\mathcal{X}_{dkl}}(1)]^2}{\mu_{\mathcal{X}_{dkl}}(2)-[\mu_{\mathcal{X}_{dkl}}(1)]^2}, \frac{\mu_{\mathcal{X}_{dkl}}(1)x}{\mu_{\mathcal{X}_{dkl}}(2)-[\mu_{\mathcal{X}_{dkl}}(1)]^2}\right). \quad (48)$$

Now, we can derive the CDF of $\mathcal{Y}_{dk} = \sum_{l=1}^{L_k}\mathcal{X}_{dkl}$ as

$$F_{\mathcal{Y}_{dk}}(x) \approx \frac{1}{\Gamma\left(\frac{L_k[\mu_{\mathcal{X}_{dkl}}(1)]^2}{\mu_{\mathcal{X}_{dkl}}(2)-[\mu_{\mathcal{X}_{dkl}}(1)]^2}\right)} \times \gamma\left(\frac{L_k[\mu_{\mathcal{X}_{dkl}}(1)]^2}{\mu_{\mathcal{X}_{dkl}}(2)-[\mu_{\mathcal{X}_{dkl}}(1)]^2}, \frac{\mu_{\mathcal{X}_{dkl}}(1)x}{\mu_{\mathcal{X}_{dkl}}(2)-[\mu_{\mathcal{X}_{dkl}}(1)]^2}\right). \quad (49)$$

Based on [38], we obtain the nth moment of $\mathcal{Y}_{dk}$ as

$$\mu_{\mathcal{Y}_{dk}}(n) \triangleq \mathbb{E}\{\mathcal{Y}_{dk}^n\} = \sum_{n_1=0}^{n}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{L_k-1}=0}^{n_{L_k-2}}\binom{n}{n_1}\binom{n_1}{n_2}\cdots\binom{n_{L_k-2}}{n_{L_k-1}} \times \mu_{\mathcal{X}_{dk1}}(n-n_1)\mu_{\mathcal{X}_{dk2}}(n_1-n_2)\cdots\mu_{\mathcal{X}_{dkL_k}}(n_{L_k-1}), \quad (50)$$

where $\binom{a}{b} = \frac{a!}{b!(a-b)!}$, and the nth moment of $\mathcal{Z}_d = \sum_{k=1}^K \mathcal{Y}_{dk}$ is

$$\mu_{\mathcal{Z}_d}(n) \triangleq \mathbb{E}\{\mathcal{Z}_d^n\} = \sum_{n_1=0}^{n}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{K-1}=0}^{n_{K-2}}\binom{n}{n_1}\binom{n_1}{n_2}\cdots\binom{n_{K-2}}{n_{K-1}} \times \mu_{\mathcal{Y}_{d1}}(n-n_1)\mu_{\mathcal{Y}_{d2}}(n_1-n_2)\cdots\mu_{\mathcal{Y}_{dK}}(n_{K-1}). \quad (51)$$

From Eqs. 47,50 and 51, we compute the first and second moments of $\mathcal{Z}_d$ as

$$\mu_{\mathcal{Z}_d}(1) = \sum_{k=1}^{K}\sum_{l=1}^{L_k}\mu_{\mathcal{X}_{dkl}}(1), \quad (52)$$

$$\mu_{\mathcal{Z}_d}(2) = \sum_{k=1}^{K}\left[\sum_{l=1}^{L_k}\mu_{\mathcal{X}_{dkl}}(2) + 2\sum_{l=1}^{L_k}\mu_{\mathcal{X}_{dkl}}(1)\sum_{l'=l+1}^{L_k}\mu_{\mathcal{X}_{dkl'}}(1)\right] + 2\sum_{k=1}^{K}\left[\sum_{l=1}^{L_k}\mu_{\mathcal{X}_{dkl}}(1)\right]\sum_{k'=k+1}^{K}\left[\sum_{l=1}^{L_{k'}}\mu_{\mathcal{X}_{dk'l}}(1)\right]. \quad (53)$$

Then, the nth moment of $\mathcal{T}_d = h_{sd} + \mathcal{Z}_d$ is calculated as

$$\mu_{\mathcal{T}_d}(n) \triangleq \mathbb{E}\{(h_{sd}+\mathcal{Z}_d)^n\} = \mathbb{E}\left\{\sum_{i=0}^{n}\binom{n}{i}h_{sd}^i\mathcal{Z}_d^{n-i}\right\} = \sum_{i=0}^{n}\binom{n}{i}\mu_{h_{sd}}(i)\mu_{\mathcal{Z}_d}(n-i). \quad (54)$$

Consequently, the first and second moments of $\mathcal{T}_d$ calculated from Eq. 54 are

$$\mu_{\mathcal{T}_d}(1) = \mu_{h_{sd}}(1) + \mu_{\mathcal{Z}_d}(1), \quad (55)$$

$$\mu_{\mathcal{T}_d}(2) = \mu_{h_{sd}}(2) + \mu_{\mathcal{Z}_d}(2) + 2\mu_{h_{sd}}(1)\mu_{\mathcal{Z}_d}(1). \quad (56)$$

Similarly, the first and second moments of $\mathcal{T}_e$ are expressed as

$$\mu_{\mathcal{T}_e}(1) = \mu_{h_{se}}(1) + \mu_{\mathcal{Z}_e}(1), \quad (57)$$

$$\mu_{\mathcal{T}_e}(2) = \mu_{h_{se}}(2) + \mu_{\mathcal{Z}_e}(2) + 2\mu_{h_{se}}(1)\mu_{\mathcal{Z}_e}(1). \quad (58)$$

Therefore, the CDFs of $\mathcal{T}_d$ and $\mathcal{T}_e$ are, respectively, given by

$$
\begin{aligned}
F_{\mathcal{T}_d}(x) =& \frac{1}{\Gamma\left(\frac{[\mu_{\mathcal{T}_d}(1)]^2}{\mu_{\mathcal{T}_d}(2)-[\mu_{\mathcal{T}_d}(1)]^2}\right)} \\
& \times \gamma\left(\frac{[\mu_{\mathcal{T}_d}(1)]^2}{\mu_{\mathcal{T}_d}(2)-[\mu_{\mathcal{T}_d}(1)]^2}, \frac{\mu_{\mathcal{T}_d}(1)x}{\mu_{\mathcal{T}_d}(2)-[\mu_{\mathcal{T}_d}(1)]^2}\right) \\
=& \frac{1}{\Gamma(\Xi_d)}\gamma(\Xi_d, \Psi_d x) \\
=& 1 - \frac{1}{\Gamma(\Xi_d)}\Gamma(\Xi_d, \Psi_d x),
\end{aligned} \tag{59}
$$

$$
F_{\mathcal{T}_e}(x) = 1 - \frac{1}{\Gamma(\Xi_e)}\Gamma(\Xi_e, \Psi_e x), \tag{60}
$$

where

$$
\Xi_d = \frac{[\mu_{\mathcal{T}_d}(1)]^2}{\mu_{\mathcal{T}_d}(2) - [\mu_{\mathcal{T}_d}(1)]^2}, \tag{61}
$$

$$
\Psi_d = \frac{\mu_{\mathcal{T}_d}(1)}{\mu_{\mathcal{T}_d}(2) - [\mu_{\mathcal{T}_d}(1)]^2}, \tag{62}
$$

$$
\Xi_e = \frac{[\mu_{\mathcal{T}_e}(1)]^2}{\mu_{\mathcal{T}_e}(2) - [\mu_{\mathcal{T}_e}(1)]^2}, \tag{63}
$$

$$
\Psi_e = \frac{\mu_{\mathcal{T}_e}(1)}{\mu_{\mathcal{T}_e}(2) - [\mu_{\mathcal{T}_e}(1)]^2}. \tag{64}
$$

Next, we can calculate the CDFs of β_d and β_e^{c2} from Eqs. 38 and 39 as

$$
F_{\beta_d}(x) = \Pr\left\{\mathcal{T}_d^2 < \frac{x}{\rho_d}\right\} = \Pr\left\{\mathcal{T}_d < \sqrt{\frac{x}{\rho_d}}\right\} = F_{\mathcal{T}_d}\left(\sqrt{\frac{x}{\rho_d}}\right), \tag{65}
$$

$$
F_{\beta_e^{c2}}(x) = \Pr\left\{\mathcal{T}_e^2 < \frac{x}{\rho_e}\right\} = \Pr\left\{\mathcal{T}_e < \sqrt{\frac{x}{\rho_e}}\right\} = F_{\mathcal{T}_e}\left(\sqrt{\frac{x}{\rho_e}}\right). \tag{66}
$$

Applying Eqs. 59 and 60,65, and 66 become Eqs. 26 and 28, respectively. The proof is thus complete.

References

1. Lu W, Ding Y, Gao Y, Hu S, Wu Y, Zhao N, Gong Y (2022) Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems. IEEE Trans. Ind. Informatics 18(4):2704–2713
2. Hoang TM, Dung LT, Nguyen BC, Tran XN, Kim T (2021) Secrecy outage performance of FD-NOMA relay system with multiple non-colluding eavesdroppers. IEEE Trans. Veh. Technol. 70(12):12 985–12 997
3. Hoang TM, Duong TQ, Tuan HD, Lambotharan S, Hanzo L (2021) Physical layer security: Detection of active eavesdropping attacks by support vector machines. IEEE Access 9:31 595–31 607
4. Do D, Le A, Ha NX, Dao N (2022) Physical layer security for internet of things via reconfigurable intelligent surface. Future Gener. Comput. Syst. 126:330–339
5. Ai Y, de Figueiredo FAP, Kong L, Cheffena M, Chatzinotas S, Ottersten BE (2021) Secure vehicular communications through reconfigurable intelligent surfaces. IEEE Trans. Veh. Technol. 70(7):7272–7276
6. Ha D, Duy TT, Son PN, Le-Tien T, Voznák M (2021) Security-reliability trade-off analysis for rateless codes-based relaying protocols using NOMA, cooperative jamming and partial relay selection. IEEE Access 9:131 087–131 108
7. Thai CDT, Bao V-NQ, Vo N-S (2022) Secure communication using interference cancellation against multiple jammers. IEEE Trans. Veh, Technol
8. Atapattu S, Fan R, Dharmawansa P, Wang G, Evans JS, Tsiftsis TA (2020) Reconfigurable intelligent surface assisted two-way communications: Performance analysis and optimization. IEEE Trans. Commun. 68(10):6552–6567
9. Yu H, Tuan HD, Nasir AA, Duong TQ, Poor HV (2020) Joint design of reconfigurable intelligent surfaces and transmit beamforming under proper and improper gaussian signaling. IEEE J. Sel. Areas Commun. 38(11):2589–2603
10. Basar E, Renzo MD, de Rosny J, Debbah M, Alouini M, Zhang R (2019) Wireless communications through reconfigurable intelligent surfaces. IEEE Access 7:116 753–116 773
11. Björnson E, Sanguinetti L (2020) Power scaling laws and near-field behaviors of massive MIMO and intelligent reflecting surfaces. IEEE Open J. Commun. Soc. 1:1306–1324
12. Chen Y, Ai B, Zhang H, Niu Y, Song L, Han Z, Poor HV (2021) Reconfigurable intelligent surface assisted device-to-device communications. IEEE Trans. Wirel. Commun. 20(5):2792–2804
13. Björnson E, Özdogan Ö, Larsson EG (2020) Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying? IEEE Wirel. Commun. Lett. 9(2):244–248
14. Boulogeorgos AA, Alexiou A (2020) Performance analysis of reconfigurable intelligent surface-assisted wireless systems and comparison with relaying. IEEE Access 8:94 463–94 483
15. ElMossallamy MA, Zhang H, Song L, Seddik KG, Han Z, Li GY (2020) Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities. IEEE Trans. Cogn. Commun. Netw. 6(3):990–1002
16. Yang L, Yang J, Xie W, Hasna MO, Tsiftsis T, Renzo MD (2020) Secrecy performance analysis of RIS-aided wireless communication systems. IEEE Trans. Veh. Technol. 69(10):12 296–12 300
17. Makarfi AU, Rabie KM, Kaiwartya O, Li X, Kharel R (2020) Physical layer security in vehicular networks with reconfigurable intelligent surfaces. In 91st IEEE Vehicular Technology Conference, VTC Spring 2020, Antwerp, Belgium, May 25-28, 2020. IEEE, pp. 1–6
18. Nguyen ND, Le A, Munochiveyi M (2021) Secrecy outage probability of reconfigurable intelligent surface-aided cooperative underlay cognitive radio network communications. In 22nd Asia-Pacific Network Operations and Management Symposium, APNOMS 2021, Tainan, Taiwan, September 8-10, 2021. IEEE, pp. 73–77
19. Tang Z, Hou T, Liu Y, Zhang J (2021) Secrecy performance analysis for reconfigurable intelligent surface aided NOMA network. In IEEE International Conference on Communications Workshops,

ICC Workshops 2021, Montreal, QC, Canada, June 14-23, 2021. IEEE, pp. 1–6
20. Ferreira RC, Facina MSP, de Figueiredo FAP, Fraidenraich G, de Lima ER (2021) Secrecy analysis and error probability of LIS-aided communication systems under Nakagami-m fading. Entropy 23(10):1284
21. Khoshafa MH, Nkouatchah TMN, Ahmed MH (2021) Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications. IEEE Commun. Lett. 25(5):1443–1447
22. Trigui I, Ajib W, Zhu W (2021) Secrecy outage probability and average rate of RIS-aided communications using quantized phases. IEEE Commun. Lett. 25(6):1820–1824
23. Zhang J, Du H, Sun Q, Ai B, Ng DWK (2021) Physical layer security enhancement with reconfigurable intelligent surface-aided networks. IEEE Trans. Inf. Forensics Secur. 16:3480–3495
24. Youn J, Son W, Jung BC (2021) Physical-layer security improvement with reconfigurable intelligent surfaces for 6g wireless communication systems. Sensors 21(4):1439
25. Tuan PV, Son PN, Duy TT, Nga TTK, Koo I et al (2022) Information security in intelligent reflecting surface-aided two-way network. In 2022 IEEE Ninth International Conference on Communications and Electronics (ICCE). IEEE, pp. 155–159
26. Gong C, Yue X, Wang X, Dai X, Zou R, Essaaidi M (2022) Intelligent reflecting surface aided secure communications for NOMA networks. IEEE Trans. Veh. Technol. 71(3):2761–2773
27. Cao K, Ding H, Li W, Lv L, Gao M, Gong F, Wang B (2022) On the ergodic secrecy capacity of intelligent reflecting surface aided wireless powered communication systems. IEEE Wirel. Commun. Lett. 11(11):2275–2279
28. Tran PT, Nguyen BC, Hoang TM, Le XH, Nguyen VD (2022) Exploiting multiple RISs and direct link for performance enhancement of wireless systems with hardware impairments. IEEE Trans. Commun. 70(8):5599–5611
29. Yang L, Yang Y, da Costa DB, Trigui I (2021) Outage probability and capacity scaling law of multiple RIS-aided networks. IEEE Wirel. Commun. Lett. 10(2):256–260
30. Yildirim I, Uyrus A, Basar E (2021) Modeling and analysis of reconfigurable intelligent surfaces for indoor and outdoor applications in future wireless networks. IEEE Trans. Commun. 69(2):1290–1301
31. Hou T, Liu Y, Song Z, Sun X, Chen Y, Hanzo L (2020) Reconfigurable intelligent surface aided NOMA networks. IEEE J. Sel. Areas Commun. 38(11):2575–2588
32. Tahir B, Schwarz S, Rupp M (2021) Analysis of uplink IRS-assisted NOMA under nakagami-m fading via moments matching. IEEE Wirel. Commun. Lett. 10(3):624–628
33. Alnwaimi G, Boujemaa H (2021) Non orthogonal multiple access using reconfigurable intelligent surfaces. Wirel. Pers. Commun. 121(3):1607–1625
34. Leon-Garcia A, Leon-Garcia A (2008) Probability, statistics, and random processes for electrical engineering. Pearson/Prentice Hall, 3rd ed. Upper Saddle River, NJ
35. Prudnikov AP (1998) Integrals and series. vol 3, More special functions; Prudnikov AP, Brychkov Yu A, Marichev OI; translated from the Russian by Gould GG. Gordon and Breach
36. Jeffrey A, Zwillinger D (2007) Table of integrals, series, and products. Academic press
37. Nguyen BC, Dung LT, Hoang TM, Tran XN, Kim T (2021) Impacts of imperfect CSI and transceiver hardware noise on the performance of full-duplex DF relay system with multi-antenna terminals over nakagami-m fading channels. IEEE Trans. Commun. 69(10):7094–7107
38. da Costa DB, Ding H, Ge J (2011) Interference-limited relaying transmissions in dual-hop cooperative networks over nakagami-m fading. IEEE Commun. Lett. 15(5):503–505

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

Ba Cao Nguyen received the B.S. degree in electrical engineering from Telecommunication University, Khanh Hoa, Vietnam, in 2006 and the M.S. degree in electrical engineering from the Posts and Telecommunications Institute of Technology (VNPT), Ho Chi Minh City, Vietnam, in 2011. He received the Ph.D. degree in electrical engineering from Le Quy Don Technical University, Hanoi, Vietnam, in 2020. From November 2019 to April 2021, he works as a Lecturer with Telecommunications University, Khanh Hoa, Vietnam. He has been with Chungbuk National University, Cheongju, South Korea as a Postdoctoral Research Fellow from May 2021 to July 2022 and also with Telecommunications University as a Lecturer. He currently works as a Lecturer with Telecommunications University, Khanh Hoa, Vietnam. His research interests include energy harvesting, full-duplex, spatial modulation, NOMA, MIMO, RIS, UAV, and cooperative communication.

Quyet-Nguyen Van received the B.E. degree in information technology from the University of Information Technology, Vietnam National University, Ho Chi Minh City, Vietnam, in 2009, and the M.S. degree in information technology from Lac Hong University, Bien Hoa, Dong Nai, in 2015. His major research interests include computer science, networking, cloud computing, the IoT, and image processing.

Le The Dung (S'14–M'16) received the B.S. degree in electronics and telecommunication engineering from Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, in 2008, and both the M.S. and Ph.D. degrees in electronics and computer engineering from Hongik University, Seoul, South Korea, in 2012 and 2016, respectively. From 2007 to 2010, he joined Signet Design Solutions Vietnam as a Hardware Design Engineer. He was with Chungbuk National University as a postdoctoral research fellow from May 2016 to December 2022. Since September 2022, I have been with FPT University, HCMC Campus, as a Lecturer and Researcher. At the same time, he also has been with RMIT University Vietnam as a Teaching Assistant. He has more than 80 papers in referred international journals and conferences. His major research interests include routing protocols, network coding, network stability analysis and optimization in mobile ad-hoc networks, cognitive radio ad-hoc networks, and visible light communication networks. He was a recipient of the IEEE IS3C2016 Best Paper Award.

Tran Manh Hoang received the B.S. degree in communication command from Telecommunications University, Ministry of Defense, Nha Trang, Khanh Hoa, Vietnam, in 2002, the B.Eng. degree in electrical engineering from Le Quy Don Technical University, Hanoi, Vietnam, in 2006, the M.Eng. degree in electronics engineering from the Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam, in 2013, and the Ph.D. degree in electrical engineering from Le Quy Don Technical University, in 2020. He has been with Chungbuk National University, as a Visiting Professor and also with Telecommunications University, as a Lecturer. His research interests include energy harvesting, nonorthogonal multiple access, and signal processing for wireless cooperative communications.

Nguyen Van Vinh was born in Binh Dinh, Viet Nam, in 1984. He received the B.E. degree in Computer Science from Nha Trang University, Vietnam, in 2008. In 2015, he received a Master's degree in Computer Science from University of Transport and Communications, Vietnam. He is currently a lecturer at the Department of Information Assurance (IA), FPT University, Ho Chi Minh City, Vietnam. His research interests are wireless communication in 5G, networking, cybersecurity, physical layer security and NOMA.

Gia Thien Luu graduated in Physics from Ho Chi Minh City University of Pedagogy, Viet Nam in 2003. In 2007, he obtained his MSc degree in Laser technology from Ho Chi Minh City University of Technology. He obtained Ph.D degree from Orleans University, France in 2013 with the thesis on the development of methods for time delay estimation of the electromyography signals. He is currently an Assistant Professor at Biomedical Engineering Department, Institute of Engineering of HUTECH University. His main interests concern the development of methods in signal processing and their applications to the biomedical engineering and telecommunications.

Authors and Affiliations

Ba Cao Nguyen[1] · Quyet-Nguyen Van[2] · Le The Dung[3] · Tran Manh Hoang[1] · Nguyen Van Vinh[4] · Gia Thien Luu[5]

Ba Cao Nguyen
nguyenbacao@tcu.edu.vn

Quyet-Nguyen Van
nguyenvanquyet@dntu.edu.vn

Le The Dung
dunglt96@fe.edu.vn

Tran Manh Hoang
tranmanhhoang@tcu.edu.vn

Nguyen Van Vinh
vinhnv27@fe.edu.vn

[1] Faculty of Basic Techniques, Telecommunications University, 650000 Khanh Hoa, Vietnam

[2] Faculty of Technology, Dong Nai Technology University, 76000 Dong Nai, Vietnam

[3] Department of Computing Fundamentals, FPT University, 729000 Ho Chi Minh, Vietnam

[4] FPT University, 100000 Hanoi, Vietnam

[5] Hutech Institute of Engineering, HUTECH University, Ho Chi Minh, Vietnam