KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com
ScienceDirect
ICT Express 9 (2023) 452–458
www.elsevier.com/locate/icte

On the secrecy performance of RIS-enabled wireless communications over Nakagami-*m* fading channels

Ashutosh K. Yadav[a], Suneel Yadav[a,*], Anshul Pandey[b], Adão Silva[c]

[a] *Department of Electronics and Communication Engineering, Indian Institute of Information Technology Allahabad, Prayagraj, 211015, India*
[b] *Secure Systems Research Center, Technology Innovation Institute, Abu Dhabi 9639, United Arab Emirates*
[c] *Instituto de Telecomunicações (IT) and Departamento de Eletrónica, Telecomunicações e Informática (DETI), University of Aveiro, 3810-193 Aveiro, Portugal*

Received 17 December 2021; received in revised form 1 April 2022; accepted 5 April 2022
Available online 16 April 2022

Abstract

This paper examines the secrecy performance of reconfigurable intelligent surface aided wireless communication systems. Specifically, we derive the secrecy outage probability (SOP), intercept probability, probability of non-zero secrecy capacity, and ergodic secrecy capacity (ESC) expressions over Nakagami-*m* fading channels. We further evaluate the asymptotic SOP expressions to get some insights into the secrecy diversity order under two scenarios of interest; (1) when the signal-to-noise ratio approaches infinity, and (2) when the main-to-eavesdropper ratio tends to infinity. Also, we analytically show the effect of reflecting element density on the ESC performance. The numerical and simulation studies verify our analytical findings.

Keywords: Reconfigurable intelligent surface; Physical layer security; Secrecy outage probability; Ergodic secrecy capacity; Nakagami-*m* fading channels

1. Introduction

Wireless communications have made realizing the dream of a truly digitally connected world possible, but the random and uncontrollable nature of the wireless channels is the ultimate barrier in achieving the reliable and secure communications. Reconfigurable intelligent surfaces (RISs) can help in achieving these requirements, as they have an ability to alter the propagation of waves impinging on them by adjusting the reflection amplitude, phase shift, and angle of departure [1,2]. However, for pervasive wireless networks and Internet-of-Things (IoT) use-cases, the security concerns (e.g., jamming, spoofing, and eavesdropping) are of paramount importance. To deal with, physical layer security (PHY-security) has emerged as a promising solution which exploits the random channel behavior and device specific irregularities [3,4].

The performance of various wireless communication systems by exploiting the RISs has been examined in recent works (see [5–9] and related references) but without considering PHY-security aspects. Nowadays, the emergence of RIS technology has further provided a new horizon for PHY-security solution deployments. The secrecy performance of wireless networks has been investigated mainly for two use-cases of RIS; viz., i) when RIS acts as a relay between transmitter and receiver, and (ii) when RIS acts as an access point, as proposed in [10]. To this end, PHY-security in wireless systems for first use-case has been widely studied in [11–15]. The authors in [11] have studied the secrecy performance of RIS-assisted systems with direct links. The beamforming schemes for an RIS-assisted wireless system have been analyzed in [12]. The authors in [13] have studied the secrecy rate performance of an RIS-aided downlink system under multi-antenna eavesdropper. PHY-security in RIS-assisted systems with randomly deployed users and a multi-antenna eavesdropper has been studied in [14]. The RIS-assisted jamming technique for wireless systems has been studied in [15].

Of particular interest is the wireless communication systems under the scenario where an access point is configured with RIS. The secrecy performance investigation under this scenario is very scarce [16–18]. The authors in [16] have studied the performance of RIS-based IoT networks over

* Corresponding author.
E-mail addresses: rse2019003@iiita.ac.in (A.K. Yadav), suneel@iiita.ac.in (S. Yadav), anshul@ssrc.tii.ae (A. Pandey), asilva@av.it.pt (A. Silva).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2022.04.003

generalized fading channels but without considering PHY-security. The ergodic secrecy capacity (ESC) performance of RIS-enabled vehicular networks has been analyzed over double-Rayleigh fading in [17]. PHY-security performance of RIS-aided wireless networks has been studied in terms of secrecy outage probability (SOP) and ESC over Fisher-Snedecor composite fading [18]. However, there is a lack of performance evaluation measures, viz., asymptotic SOP, intercept probability (IP), probability of non-zero secrecy capacity (PNZSC), and impact of reflecting element density on the ESC, under such system setup.

With above motivation, we deduce the SOP, IP, PNZSC, and ESC expressions of an RIS-enabled secure communication system under Nakagami-m fading channels. We further perform the asymptotic SOP analysis for two scenarios of interest; (1) when signal-to-noise ratio (SNR) goes to infinity, and (2) when main-to-eavesdropper ratio (MER)[1] approaches infinity. From which, we reveal that the system's secrecy diversity order tends to zero when SNR approaches infinity, and $m_D N_S$ when MER goes to infinity, where m_D is the fading severity parameter of the main channel (between source and destination), and N_S is the number of reflecting elements. We then show that the ergodic capacities for the main link and the wiretap link (between source and eavesdropper) vary logarithmically when N_S grows large and are independent of fading severity parameters.

2. System and channel models

We consider a Wyner's wiretap model, where an access point S (configured with RIS having N_S number of passive reflecting elements) transmits its confidential information to a single-antenna legitimate destination D, in the presence of a passive eavesdropper E. The RIS configuration supports transmission from S via wired connections, without any radio frequency processing [10]. The perfect instantaneous channel state information (CSI) of D is considered at S, but it can only obtain the statistical CSI[2] of E, since E is passive in nature and does not reveal its identity [11], [14], [17–19].

For this system, the received signal at node i, for $i \in \{D, E\}$, can be given as $y_i = \sqrt{P_S}\Big[\sum_{\ell=1}^{N_S} h_{i,\ell}\epsilon_\ell\Big]x_S + n_i$, where P_S is the transmit power at S, x_S is the transmit signal with unit energy, and n_i is the additive white Gaussian noise at node i with zero mean and N_0 variance. $\epsilon_\ell = \varphi_\ell(\phi_\ell)\mathrm{e}^{j\phi_\ell}$ is the reflection coefficient produced by the ℓth reflector element of the RIS, where $\varphi_\ell(\phi_\ell) = 1$, for $\ell = 1, 2, \ldots, N_S$, under ideal phase shifts. We denote the channel gains $h_{D,\ell}$ and $h_{E,\ell}$ as $h_{D,\ell} = g_{D,\ell} d_D^{-\alpha/2}\mathrm{e}^{-j\theta_{D,\ell}}$ and $h_{E,\ell} = g_{E,\ell} d_E^{-\alpha/2}\mathrm{e}^{-j\theta_{E,\ell}}$, where d_D and d_E are the distances between $S-D$ and $S-E$, α is the path-loss exponent, and $g_{D,\ell}$ and $g_{E,\ell}$ are the amplitudes of the channel gains and follow independent and identically distributed (i.i.d.) Nakagami-m fading.

Assuming the optimal phase shifting for RIS,[3] the instantaneous SNR at D and E can be expressed as

$$\gamma_D = \rho d_D^{-\alpha}\sum_{\ell=1}^{N_S}|g_{D,\ell}|^2 \text{ and } \gamma_E = \rho d_E^{-\alpha}\sum_{\ell=1}^{N_S}|g_{E,\ell}|^2, \tag{1}$$

where $\rho \triangleq \frac{P_S}{N_0}$ is the transmit SNR. The capacity for $S \to i$ link, for $i \in \{D, E\}$, is given as $\mathcal{C}_i = \log_2(1+\gamma_i)$, and hence the secrecy capacity $\mathcal{C}_{\text{sec}} = \max\{\mathcal{C}_D - \mathcal{C}_E, 0\}$.

2.1. Preliminaries

Under Nakagami-m fading, the channel gain $|g_{i,\ell}|^2$, for $i \in \{D, E\}$ is Gamma distributed [20], whose cumulative distribution function (CDF) and probability density function (PDF) can be expressed as $F_{|g_{i,\ell}|^2}(x) = \frac{1}{\Gamma(m_i)}\Upsilon\big(m_i, \frac{m_i x}{\Omega_i}\big)$, and $f_{|g_{i,\ell}|^2}(x) = \frac{1}{\Gamma(m_i)}\big(\frac{m_i}{\Omega_i}\big)^{m_i} x^{m_i-1}\mathrm{e}^{-\frac{m_i}{\Omega_i}x}$. Further, the CDF and PDF of sum of N_S i.i.d. Gamma RVs, Λ_i, which can be defined as [20] $\Lambda_i = \sum_{\ell=1}^{N_S}|g_{i,\ell}|^2$, are given as $F_{\Lambda_i}(x) = \frac{1}{\Gamma(N_S m_i)}\Upsilon\big(N_S m_i, \frac{m_i x}{\Omega_i}\big)$, and $f_{\Lambda_i}(x) = \frac{1}{\Gamma(N_S m_i)}\big(\frac{m_i}{\Omega_i}\big)^{N_S m_i} x^{N_S m_i - 1}\mathrm{e}^{-\frac{m_i x}{\Omega_i}}$, for $i \in \{D, E\}$, where $\Gamma(x)$ and $\Upsilon(n, x)$ denote the complete Gamma and lower incomplete Gamma functions [21, eq. (8.350)].

3. Secrecy performance analysis

3.1. Exact SOP analysis

The SOP can be mathematically expressed as $\mathcal{P}_{\text{SOP}} = \Pr\big[\max\{\mathcal{C}_D - \mathcal{C}_E, 0\} < \mathcal{R}_s\big]$, where $\mathcal{R}_s$ (in bps/Hz) is the predefined secrecy target rate. Note that when $\mathcal{C}_D \le \mathcal{C}_E$, $\mathcal{P}_{\text{SOP}} = 1$. Hence, the SOP is evaluated for $\mathcal{C}_D > \mathcal{C}_E$ as

$$\begin{aligned}\mathcal{P}_{\text{SOP}} &= \Pr\big[\mathcal{C}_D - \mathcal{C}_E < \mathcal{R}_s\big] = \Pr\left[\frac{1+\gamma_D}{1+\gamma_E} < \Lambda_{\text{th}}\right] \\ &= \int_0^\infty F_{\gamma_D}((\Lambda_{\text{th}}-1) + \Lambda_{\text{th}} y) f_{\gamma_E}(y) dy,\end{aligned} \tag{2}$$

where $\Lambda_{\text{th}} = 2^{\mathcal{R}_s}$ is the secrecy threshold. $F_{\gamma_D}(x)$ and $f_{\gamma_E}(x)$ are the CDF of γ_D and the PDF of γ_E. Now, the exact SOP expression is presented as per Theorem 1.

Theorem 1. *The exact SOP for the considered system under Nakagami-*m *fading channels can be obtained as*

$$\begin{aligned}\mathcal{P}_{SOP}(\Lambda_{th}) = 1 - \frac{\big(\frac{m_E}{\rho d_E^{-\alpha}}\big)^{m_E N_S} e^{-\frac{m_D}{\rho d_D^{-\alpha}}(\Lambda_{th}-1)}}{\Gamma(m_E N_S)} \sum_{n=0}^{m_D N_S - 1}\sum_{k=0}^{n}\frac{\binom{n}{k}}{n!} \\ \times \frac{\Lambda_{th}^k\big(\frac{m_D}{\rho d_D^{-\alpha}}\big)^n}{(\Lambda_{th}-1)^{k-n}}\left(\frac{\rho}{d_E^\alpha m_E + d_D^\alpha m_D \Lambda_{th}}\right)^{k+m_E N_S}\Gamma(k + m_E N_S).\end{aligned} \tag{3}$$

[1] MER is the ratio of average channel gains from source to destination to that from source to eavesdropper.

[2] The statistical CSI of E's channel can be obtained under the scenario where E is part of a system and becomes an active trusted member in the system during alternate time slots. Accordingly, E feeds back its CSI to S during the serving period. With this information, the statistical knowledge of E's channel during the non-serving period can be obtained. Also, with the known statistical CSI of E at S, one can get the information about the position of E.

[3] In this work, we assume the worst-case scenario by considering the optimal phase shift design for E. The investigation under the assumption of random phase shift for E will be carried out in future.

Proof. The proof is given in the Appendix. ■

Remark 1. The expression in (3) consists of finite summations with elementary functions, and as such, it can readily be computed and makes it practical to use.

3.2. Asymptotic SOP analysis

To obtain some insights about the secrecy diversity order,[4] the asymptotic SOP analysis is presented for two cases of interest; (i) Case 1: when SNR goes to infinity, i.e., $\rho \to \infty$, and (ii) Case 2: when MER tends to infinity, i.e., $\lambda = \frac{\Omega_D}{\Omega_E} \to \infty$, where Ω_D and Ω_E are the average channel gains of $S \to D$ and $S \to E$ links, respectively, and can be equivalently represented as $\Omega_D \triangleq d_D^{-\alpha}$ and $\Omega_E \triangleq d_E^{-\alpha}$ under path-loss channel modeling.

Case 1: For the case when $\rho \to \infty$, we can obtain the asymptotic SOP according to the below proposition.

Proposition 1. *The asymptotic SOP under Case 1 ($\rho \to \infty$) over Nakagami-*m *fading can be obtained as*

$$\mathcal{P}_{SOP}^{asy,\ case\ 1}(\Lambda_{th}) = 1 - \frac{1}{\Gamma(m_E N_S)}\left(\frac{m_E}{d_E^{-\alpha}}\right)^{m_E N_S} \sum_{n=0}^{m_D N_S - 1} \frac{1}{n!} \times \left(\frac{\Lambda_{th} m_D}{d_D^{-\alpha}}\right)^{n} \left(\frac{1}{d_E^{\alpha} m_E + d_D^{\alpha} m_D \Lambda_{th}}\right)^{n + m_E N_S} \Gamma(n + m_E N_S). \quad (4)$$

Proof. When $\rho \to \infty$, we can have $\mathcal{P}_{\text{SOP}}^{\text{asy, case 1}}(\Lambda_{\text{th}}) \approx \Pr\left[\frac{F_D}{F_E} < \Lambda_{\text{th}}\right] = \int_0^{\infty} F_{F_D}(\Lambda_{\text{th}} y) f_{F_E}(y) dy$, where $F_i = d_i^{-\alpha} \sum_{\ell=1}^{N_S} |g_{i,\ell}|^2$, for $i \in \{D, E\}$. Now, invoking the CDF of F_D and the PDF of F_E via relation $\Upsilon(\beta, z) = (\beta - 1)!\left[1 - e^{-z} \sum_{r=0}^{\beta-1} \frac{z^r}{r!}\right]$ [21, eq. (8.352.6)], and then simplifying the resultant integrals by using [21, eq. (3.351.3)], with some involved manipulations, we can get the asymptotic SOP for Case 1, as given in (4). ■

Remark 2. We can infer from (4) that the asymptotic SOP expression is independent of ρ, and thus the secrecy diversity order goes to zero. This is due to the simultaneous improvement in SNR at both D and E.

Case 2: When MER $\lambda = \frac{\Omega_D}{\Omega_E} \to \infty$, the asymptotic SOP expression can be evaluated as per Proposition 2.

Proposition 2. *The asymptotic SOP for the Case 2 ($\lambda \to \infty$) under Nakagami-*m *fading can be given by*

$$\mathcal{P}_{SOP}^{asy,\ case\ 2}(\Lambda_{th}) = \left[\frac{1}{(m_D N_S)!} \frac{\left(\frac{m_D}{\rho d_E^{-\alpha}}\right)^{m_D N_S}}{\Gamma(m_E N_S)} \sum_{n=0}^{m_D N_S} \binom{m_D N_S}{n} \times (\Lambda_{th} - 1)^{m_D N_S - n} \left(\frac{m_E}{\Lambda_{th} \rho d_E^{-\alpha}}\right)^{-n} \Gamma(n + m_E N_S)\right] \frac{1}{\lambda^{m_D N_S}}. \quad (5)$$

[4] It is defined as the asymptotic ratio of the logarithmic SOP to the logarithmic SNR (or MER), and can be mathematically expressed as $\mathcal{D}_{\text{div}} = -\lim_{\chi \to \infty} \frac{\log(\mathcal{P}_{\text{SOP}})}{\log(\chi)}$, where $\chi \in \{\text{SNR}, \text{MER}\}$

Proof. By applying the approximation of $\Upsilon(\beta, x) \simeq \frac{x^{\beta}}{\beta}$ for small value of $|x|$, we can be obtain $F_{\gamma_D}(x) \simeq \frac{1}{\Gamma(m_D N_S + 1)} \left(\frac{m_D x}{\rho d_D^{-\alpha}}\right)^{m_D N_S}$. Invoking this alongwith the PDF of γ_E into (2), and simplifying the resultant integral via binomial expansion and [21, eq. (3.351.3)], the asymptotic SOP can be obtained, as given in (5). ■

Remark 3. From (5), we can infer that the system can achieve the secrecy diversity order of $m_D N_S$.

3.3. IP analysis

The IP estimates the probability that the eavesdropper is able to intercept the information, and can be given as

$$\mathcal{P}_{\text{IP}} = \Pr[\mathcal{C}_D < \mathcal{C}_E] = \Pr[\gamma_D < \gamma_E] = \int_0^{\infty} F_{\gamma_D}(x) f_{\gamma_E}(x) dx. \quad (6)$$

By inserting $F_{\gamma_D}(x)$ and $f_{\gamma_E}(x)$ by using the identity [21, eq. (8.352.6)] into (6), and computing the integral by the aid of [21, eq. (3.351.3)], we can get the IP as

$$\mathcal{P}_{\text{IP}} = 1 - \frac{\left(\frac{m_E}{d_E^{-\alpha}}\right)^{m_E N_S}}{\Gamma(m_E N_S)} \sum_{n=0}^{m_D N_S - 1} \frac{1}{n!} \frac{\left(\frac{m_D}{d_D^{-\alpha}}\right)^{n} \Gamma(n + m_E N_S)}{\left(d_E^{\alpha} m_E + d_D^{\alpha} m_D\right)^{n + m_E N_S}}. \quad (7)$$

Remark 4. From (7), we can infer that when $m_D = m_E = 1$ and $N_S = 1$, the IP is a function of relative locations of the nodes, i.e., $\mathcal{P}_{\text{IP}} = \left[1 + \frac{d_E^{\alpha}}{d_D^{\alpha}}\right]^{-1}$. From which, we can reveal that (a) when $d_D = d_E$, $\mathcal{P}_{\text{IP}} = 0.5$, (b) when $d_D \gg d_E$, $\mathcal{P}_{\text{IP}}$ approaches to 1, which implies that E can perfectly intercept the S's information, and (c) when $d_D \ll d_E$, $\mathcal{P}_{\text{IP}}$ approaches to 0, which indicates that no information is intercepted by E.

3.4. PNZSC analysis

The PNZSC highlights the reliability level of the main channel and measures the existence of positive secrecy capacity with a probability

$$\mathcal{P}_{\text{nzsc}} = \Pr[\mathbb{C}_D > \mathbb{C}_E] = \Pr[\gamma_D > \gamma_E] = 1 - \mathcal{P}_{\text{IP}}. \quad (8)$$

Substituting (7) into (8), the PNZSC is expressed as

$$\mathcal{P}_{\text{nzsc}} = \frac{\left(\frac{m_E}{d_E^{-\alpha}}\right)^{m_E N_S}}{\Gamma(m_E N_S)} \sum_{n=0}^{m_D N_S - 1} \frac{1}{n!} \frac{\left(\frac{m_D}{d_D^{-\alpha}}\right)^{n} \Gamma(n + m_E N_S)}{\left(d_E^{\alpha} m_E + d_D^{\alpha} m_D\right)^{n + m_E N_S}}. \quad (9)$$

Remark 5. The expression in (9) consists of elementary functions, and as such, it can easily be evaluated.

4. ESC analysis

4.1. Conditional ESC analysis

The ESC is given by averaging the secrecy capacity $\mathcal{C}_{\text{sec}} = \mathcal{C}_D - \mathcal{C}_E = \log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)$, if $\gamma_D > \gamma_E$, and 0 if $\gamma_D \le \gamma_E$, over

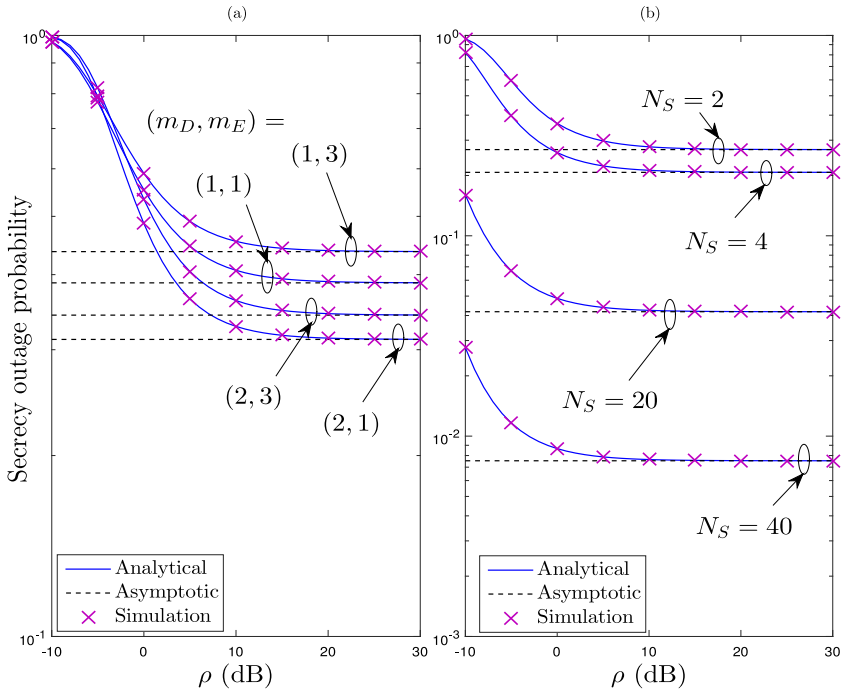

Fig. 1. SOP performance for various values of m_D, m_E, and N_S.

the distributions of γ_D and γ_E as

$$\overline{\mathcal{C}}_{\text{sec}} = \begin{cases} \overline{\mathcal{C}}_D - \overline{\mathcal{C}}_E, & \text{if } \gamma_D > \gamma_E \\ 0, & \text{if } \gamma_D \leq \gamma_E, \end{cases} \tag{10}$$

where $\overline{\mathcal{C}}_D = \mathbb{E}[\log_2(1+\gamma_D)]$ and $\overline{\mathcal{C}}_E = \mathbb{E}[\log_2(1+\gamma_E)]$ are the ergodic capacities of the main and wiretap links.

First, we evaluate the ergodic capacity (EC) at D as

$$\overline{\mathcal{C}}_D = \mathbb{E}[\log_2(1+\gamma_D)] = \frac{\int_0^\infty \ln(1+x) f_{\gamma_D}(x) dx}{\ln(2)}. \tag{11}$$

Now, invoking the PDF $f_{\gamma_D}(x)$ into (11), we can obtain

$$\overline{\mathcal{C}}_D = \frac{1}{\ln(2)} \frac{\left(\frac{m_D}{\rho d_D^{-\alpha}}\right)^{m_D N_S}}{\Gamma(m_D N_S)} \int_0^\infty \ln(1+x) x^{m_D N_S - 1} \mathrm{e}^{-\frac{m_D}{\rho d_D^{-\alpha}} x} dx, \tag{12}$$

which can be then simplified by applying the fact $\int_0^\infty \ln(1+t) t^{n-1} \mathrm{e}^{-\mu t} dt = (n-1)! \mathrm{e}^{\mu} \sum_{k=1}^{n} \frac{\Gamma(-n+k,\mu)}{\mu^k}$, as

$$\overline{\mathcal{C}}_D = \frac{1}{\ln(2)} \mathrm{e}^{\frac{m_D}{\rho d_D^{-\alpha}}} \sum_{k=1}^{m_D N_S} \frac{\Gamma\left(-m_D N_S + k, \frac{m_D}{\rho d_D^{-\alpha}}\right)}{\left(\frac{m_D}{\rho d_D^{-\alpha}}\right)^{k - m_D N_S}}. \tag{13}$$

Likewise, following the same steps as used to obtain (13), we can express the EC at E as

$$\overline{\mathcal{C}}_E = \frac{1}{\ln(2)} \mathrm{e}^{\frac{m_E}{\rho d_E^{-\alpha}}} \sum_{k=1}^{m_E N_S} \frac{\Gamma\left(-m_E N_S + k, \frac{m_E}{\rho d_E^{-\alpha}}\right)}{\left(\frac{m_E}{\rho d_E^{-\alpha}}\right)^{k - m_E N_S}}. \tag{14}$$

Finally, invoking (13) and (14) into (10), we can obtain the ESC under Nakagami-m fading channels.

4.2. Impact of reflecting element density on ESC

Here, we reveal the effect of a large number of reflective elements on the ESC performance. For this, by applying the approximation $\ln(1+x) \underset{x\to\infty}{\approx} \ln(x)$ along with the PDF of γ_D into (11), and simplifying the required integral with the aid of [21, eq. (4.352.1)], we can get

$$\overline{\mathcal{C}}_D = \frac{1}{\ln(2)} \left[\Psi(m_D N_S) - \ln\left(\frac{m_D}{\rho d_D^{-\alpha}}\right) \right], \tag{15}$$

where $\Psi(\cdot)$ is the digamma function [21, eq. (8.365.4)]. Now, considering $\Psi(x) \underset{x\to\infty}{\approx} \ln(x)$ [22, eq. (6.3.18)] for a large number of N_S, the main link's EC is given as

$$\overline{\mathcal{C}}_D = \frac{1}{\ln(2)} \ln(\rho d_D^{-\alpha} N_S). \tag{16}$$

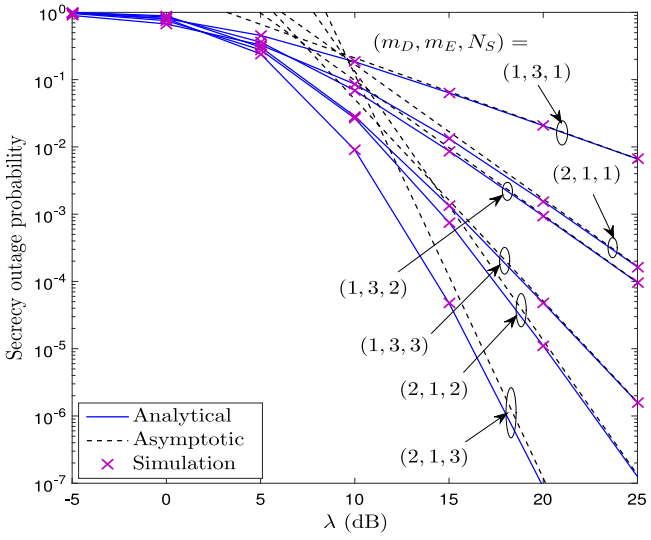

Fig. 2. The SOP vs. MER for various m_D, m_E, and N_S.

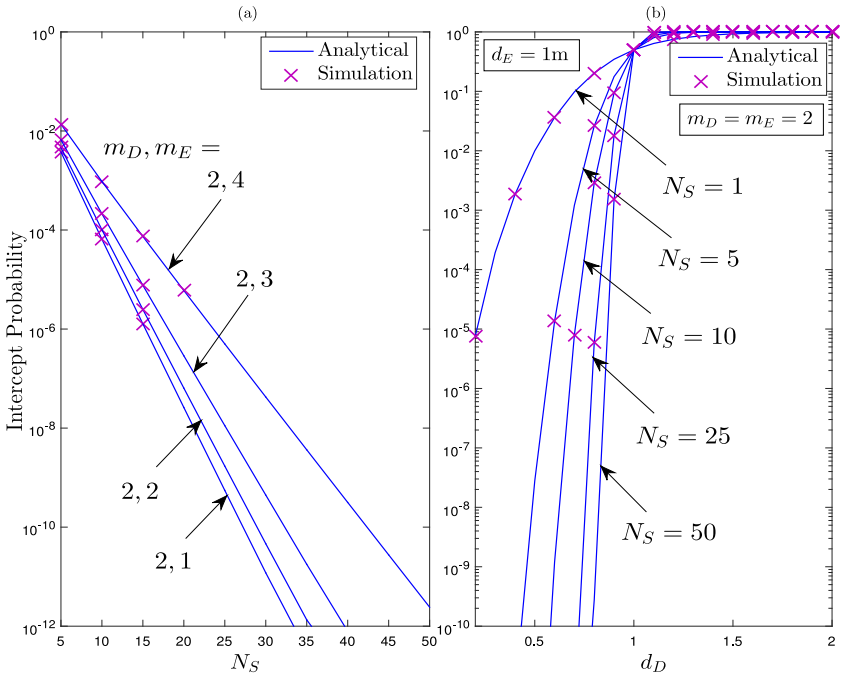

Fig. 3. Impact of N_S, m_D, m_E, and d_D on the IP performance.

Also, we can express the EC of the wiretap link as

$$\overline{\mathcal{C}}_E = \frac{1}{\ln(2)} \ln(\rho d_E^{-\alpha} N_S). \tag{17}$$

Remark 6. Based on (16) and (17), we can observe that i) for sufficiently large N_S, the ECs of the main and wiretap links increase logarithmically with N_S, and are independent of fading severity parameters, and (ii) the ESC follows the scaling law $\Theta\left(\ln\left(\frac{d_E^{\alpha}}{d_D^{\alpha}}\right)\right)$, and therefore depends on the relative locations of the nodes D and E.

5. Numerical results and discussion

We verify our analytical results via numerical and simulation studies. We set $\alpha = 4$, $d_E = 1$ m, $d_D = 0.75 d_E$, and $\mathcal{R}_s = 1$ bps/Hz, unless otherwise stated.

Fig. 1 depicts the SOP versus SNR (ρ) curves for different values of m_D, m_E, and N_S. Fig. 1 reveals that the analytical results in (3) are well matched with the simulation ones over the entire range of SNR, and the asymptotic results in (4) match well with the exact ones for medium-to-high SNR regime. Moreover, it can be seen that the SOP performance improves when $m_D > m_E$, and deteriorates when $m_D < m_E$. Further, the SOP performance improves as N_S increases. However, there exists a secrecy error floor in the high SNR regime, which is due to the improvement in the SNR at both D and E by the same factor, as also shown analytically in (4).

Fig. 2 plots the SOP versus MER (λ) for different values of m_D, m_E, and N_S. The curves reveal that the SOP performance improves when $m_D > m_E$ and *vice versa*, irrespective of N_S. Also, the SOP performance significantly enhances as N_S increases, regardless of m_D and m_E. From the SOP plots, the system's secrecy diversity order, $m_D N_S$, can be verified for various values of m_D and N_S in terms of MER, as proved analytically in (5).

In Fig. 3, we show the effect of N_S, m_D, m_E, and d_D (i.e., distance between S and D) on the IP performance. It is observed that the IP decreases as N_S increases, since more number of N_S strengthen the main channel's quality. Also, when $m_E > m_D$, the IP significantly increases, for all N_S. It is further seen that the IP approaches to 1 as $d_D > d_E$, whereas the IP tends to 0 as $d_D < d_E$. Further, it equals to 0.5 when $d_D = d_E$. We also depicted these analytically in Section 3.3.

Fig. 4 illustrates the PNZSC performance for different numbers of N_S, m_D, m_E, and d_D. Fig. 4(a) depicts that the PNZSC increases as N_S increases, irrespective of m_D and m_E. Further, the PNZSC increases for $m_D > m_E$ and *vice versa*. From Fig. 4(b), it can be observed that the PNZSC decreases as d_D and N_S increase. However, it should be noted that when $d_D < d_E$, the PNZSC is slightly higher for higher values of N_S than the lower values of N_S, and *vice versa*.

Fig. 5 studies the effects of m_D and m_E on the ESC performance. The ESC performance improves when $m_D > m_E$ for all ρ. Moreover, the performance enhances as ρ increases, however, the curves saturate for large ρ, since ρ at both D and E are increased by the same factor.

Fig. 6(a) shows the impact N_S on the ESC performance, for various values of m_D and m_E, when $\rho = 5$ dB. It is revealed that the ESC performance improves with increased N_S, but saturates for higher values of N_S, since ESC vary logarithmically with N_S, irrespective of m_D and m_E. Further, Fig. 6(b) shows the ESC versus the ratio $\frac{d_E}{d_D}$, for $d_D = 1$m, $m_D = 2, m_E = 1$, and $N_S = 5$. We can see that the ESC depends on the relative locations of the nodes. Also, the ESC performance improves as α increases. These are shown analytically in Section 4.2.

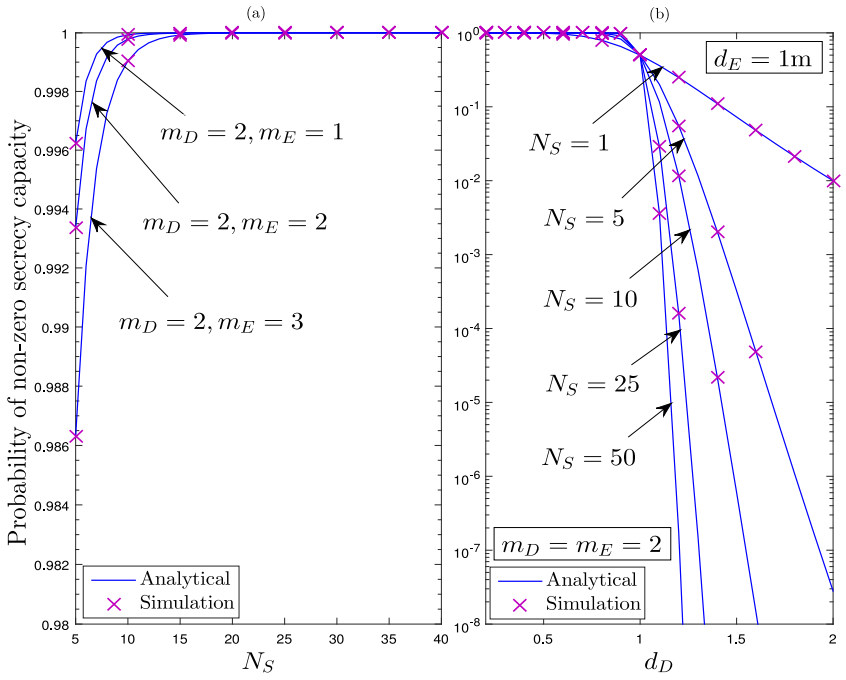

Fig. 4. The PNZSC performance for different N_S, m_D, m_E, and d_D.

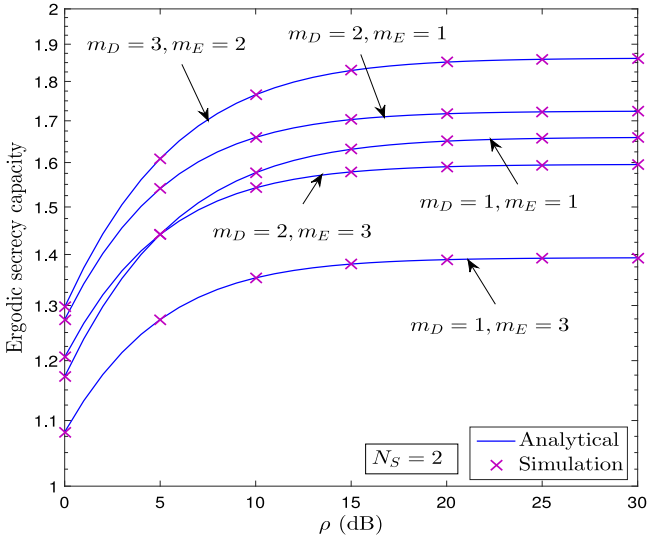

Fig. 5. Impact of fading severity parameters on the ESC.

6. Conclusions

This paper investigated the secrecy performance of a RIS-aided secure communication system. Specifically, we deduced the closed-form expressions for the SOP, IP, PNZSC, and ESC over Nakagami-m fading channels. Moreover, we derived the asymptotic SOP expressions in the high SNR and MER regimes. Based on this, we demonstrated that the system's secrecy diversity order becomes zero under the high SNR, and $m_D N_S$ under high MER regime. Further, under the impact of a large number of N_S, we showed that the ESC (i) varies logarithmically with N_S, and (ii) depends on the relative locations of the nodes. Lastly, we verified our theoretical results with numerical and simulation studies.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/50008/2020-UIDP/50008/2020.

Appendix

By substituting $F_{\gamma_D}(x)$ and $f_{\gamma_E}(x)$ via the identity [21, eq. (8.352.6)] into (2), we can express the exact SOP as

$$\mathcal{P}_{\text{SOP}}(\Lambda_{\text{th}}) = \frac{\left(\frac{m_E}{\rho d_E^{-\alpha}}\right)^{m_E N_S}}{\Gamma(m_E N_S)} \int_0^\infty y^{m_E N_S - 1} \mathrm{e}^{-\frac{m_E}{\rho d_E^{-\alpha}} y} dy$$
$$- \frac{1}{\Gamma(m_E N_S)} \left(\frac{m_E}{\rho d_E^{-\alpha}}\right)^{m_E N_S} \sum_{n=0}^{m_D N_S - 1} \frac{1}{n!} \left(\frac{m_D}{\rho d_D^{-\alpha}}\right)^n \mathrm{e}^{-\frac{m_D}{\rho d_D^{-\alpha}}(\Lambda_{\text{th}} - 1)}$$
$$\times \int_0^\infty \mathrm{e}^{-\left(\frac{m_D \Lambda_{\text{th}}}{\rho d_D^{-\alpha}} + \frac{m_E}{\rho d_E^{-\alpha}}\right) y} ((\Lambda_{\text{th}} - 1) + \Lambda_{\text{th}} y)^n y^{m_E N_S - 1} dy. \quad (18)$$

The first integral (say $\mathcal{I}_1$) in (18) can be computed via [21, eq. (3.351.3)] as $\mathcal{I}_1 = \Gamma(m_E N_S) \left(\frac{m_E}{\rho d_E^{-\alpha}}\right)^{-m_E N_S}$.

The second integral (say $\mathcal{I}_2$) in (18) is simplified by using the binomial expansion and [21, eq. (3.351.3)] as

$$\mathcal{I}_2 = \sum_{k=0}^{n} \binom{n}{k} (\Lambda_{\text{th}} - 1)^{n-k} \Lambda_{\text{th}}^k \left(\frac{m_D \Lambda_{\text{th}}}{\rho d_D^{-\alpha}} + \frac{m_E}{\rho d_E^{-\alpha}}\right)^{-(k + m_E N_S)}$$
$$\times \Gamma(k + m_E N_S). \quad (19)$$

Invoking $\mathcal{I}_1$ and $\mathcal{I}_2$ into (18), and after some manipulations, we can obtain the SOP expression of (3).

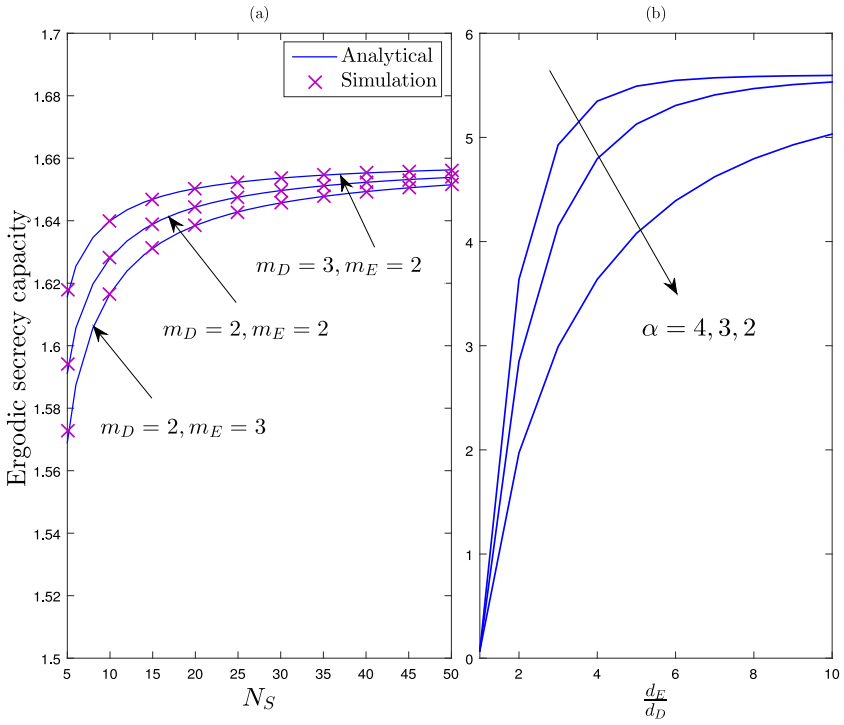

Fig. 6. ESC vs. N_S for various m_D and m_E.

Appendix B. Supplementary data

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.icte.2022.04.003.

References

[1] M.A. Mossallamy, et al., Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities, IEEE Trans. Cogn. Commun. Netw. 6 (3) (2020) 990–1002.
[2] E. Basar, et al., Wireless communications through reconfigurable intelligent surfaces, IEEE Access 7 (2019) 116753-116773.
[3] A. Pandey, S. Yadav, Physical layer security in cooperative AF relay networks over mixed Nakagami-m and double Nakagami-m fading channels: Performance evaluation and optimization, IET Commun. 14 (1) (2020) 95–104.
[4] G. Anjos, et al., Exploiting the reciprocal channel for discrete jamming to secure wireless communications against multiple-antenna eavesdropper, IEEE Access 6 (2018) 33410–33420.
[5] B. Tahir, et al., Analysis of uplink IRS-assisted NOMA under Nakagami-m fading via moments matching, IEEE Wirel. Commun. Lett. 10 (3) (2020) 624–628.
[6] Q. Tao, et al., Intelligent reflecting surface aided multicasting with random passive beamforming, IEEE Wirel. Commun. Lett. 10 (1) (2021) 92–96.
[7] J. Yuan, et al., Intelligent reflecting surface-assisted cognitive radio system, IEEE Trans. Commun. 69 (1) (2021) 675–687.
[8] Anh-T. Le, et al., Enabling user grouping and fixed power allocation scheme for reconfigurable intelligent surfaces-aided wireless systems, IEEE Access 9 (2021) 92263–92275.
[9] D. Gunasinghe, et al., Performance analysis of SWIPT for intelligent reflective surfaces for wireless communication, IEEE Commun. Lett. 25 (7) (2021) 2201–2205.
[10] E. Basar, Transmission through large intelligent surfaces: A new frontier in wireless communications, in: European Conf. Netw. Commun., EuCNC, 2019, pp. 112–117.
[11] L. Yang, et al., Secrecy performance analysis of RIS-aided wireless communication systems, IEEE Trans. Veh. Technol. 69 (10) (2020) 12296–12300.
[12] M. Cui, G. Zhang, R. Zhang, Secure wireless communication via intelligent reflecting surface, IEEE Wirel. Commun. Lett. 8 (5) (2019) 1410–1414.
[13] K. Feng, X. Li, Y. Han, S. Jin, Y. Chen, Physical layer security enhancement exploiting intelligent reflecting surface, IEEE Commun. Lett. 25 (3) (2021) 734–738.
[14] J. Zhang, et al., Physical layer security enhancement with reconfigurable intelligent surface- aided networks, IEEE Trans. Inf. Forensics Secur. 16 (2021) 3480–3495.
[15] X. Yu, et al., Robust and secure wireless communications via intelligent reflecting surfaces, IEEE J. Sel. Areas Commun. 38 (11) (2020) 2637–2652.
[16] A.U. Makarfi, et al., Reconfigurable intelligent surface enabled IoT networks in generalized fading channels, in: IEEE International Conference on Communications, ICC, 2020, pp. 1–6.
[17] A.U. Makarfi, et al., Physical layer security in vehicular networks with reconfigurable intelligent surfaces, in: IEEE 91st Vehicular Technology Conference, 2020, pp. 1–6.
[18] A.U. Makarfi, et al., Physical layer security in RIS-assisted networks in Fisher-Snedecor composite fading, in: 12th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP, 2020, pp. 1–6.
[19] L. Fan, et al., Exploiting direct links for physical layer security in multiuser multirelay networks, IEEE Trans. Wirel. Commun. 15 (6) (2016) 3856–3867.
[20] T.N. Do, et al., Multi-RIS-aided wireless systems: Statistical characterization and performance analysis, IEEE Trans. Commun. 69 (12) (2020) 8641–8658.
[21] I.S. Gradshteyn, I.M. Ryzhik, Tables of Integrals, Series, and Products, 6th ed., Academic Press, New York, 2000.
[22] M. Abromowitz, I.A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, Dover, New York, NY, USA, 1970.