IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

ESR analysis over ST-MRC multi-input multi-output Nakagami fading channels

ISSN 1751-8709
Received on 10th January 2018
Revised 20th December 2018
Accepted on 4th March 2019
E-First on 25th March 2019
doi: 10.1049/iet-ifs.2018.5185
www.ietdl.org

Jin-Yuan Wang[1,2] ✉, Sheng-Hong Lin[1], Wei Cai[1], Jianxin Dai[3]

[1]*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, People's Republic of China*

[2]*Key Laboratory (Research Base) of Signal and Information Processing, Xihua University, Chengdu 610039, People's Republic of China*

[3]*College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, People's Republic of China*

✉ *E-mail: jywang@njupt.edu.cn*

Abstract: Different from conventional key-based cryptography schemes, physical-layer security (PLS) techniques have drawn much attention recently to realise unconditional security from the information theory perspective. As an important performance metric in PLS, the ergodic secrecy rate (ESR) for a multi-input multi-output wireless communication network over a Nakagami fading channel is analysed. The network is consisted of a multi-antenna transmitter (Alice), a multi-antenna legitimate receiver (Bob), and a multi-antenna eavesdropper (Eve). By using the selective transmission (ST) at Alice and the maximum ratio combining (MRC) at Bob and Eve, an exact expression of the ESR is derived. However, due to the infinite summation, it is very hard to evaluate the ESR performance. To reduce computational complexity and obtain more insights, a lower bound of the ESR is then obtained, which is in a closed form. As special cases, the lower bounds of the ESR for the signal-antenna scenario and Rayleigh fading channel are also obtained, respectively. Numerical results show that the derived expressions of the ESR and its lower bound are very accurate to evaluate system performance.

Nomenclature

N_{A}	antennas numbers of Alice
N_{B}	antennas numbers of Bob
N_{E}	antennas numbers of Eve
m_a	fading parameter for the Alice−Bob channel
m_b	fading parameter for the Alice−Bob channel
Ω_a	parameter controlling spread for the Alice−Bob channel
Ω_b	parameter controlling spread for the Alice−Eve channel
X	transmit signal
$\boldsymbol{Z}_{\mathrm{B}}$	Gaussian noise vector at Bob
$\boldsymbol{Z}_{\mathrm{E}}$	Gaussian noise vector at Eve
$\boldsymbol{H}_{\alpha^*,\mathrm{B}}$	channel gain vector for the Alice−Bob channel
$\boldsymbol{H}_{\alpha^*,\mathrm{E}}$	channel gain vector for the Alice−Eve channel
E_s	energy per symbol
σ_{B}^2	noise variance at Bob
σ_{E}^2	noise variance at Eve

1 Introduction

With the unprecedented increase of traffic volumes in wireless communication networks, data privacy and security are becoming key issues for mobile users. In the last decade, the physical-layer security (PLS) in wireless communications has drawn much attention, which utilises the wireless channel characteristics to hide information from illegal users and does not rely on the upper-layer encryption techniques [1, 2].

The framework of PLS was pioneered by Shannon, who first proposed the concept of *perfect secrecy* over noiseless channels [3]. However, the random noise is an intrinsic element of wireless communication channels. Under noisy channels, Wyner proposed the concept of *secrecy capacity* [4]. Wyner proved that the secure communication can be realised as long as the main channel outperforms the eavesdropping channel regardless of the decoding technology or the eavesdropper's computational ability. Considering the stochasticity of wireless channels, the results in [3, 4] were extended to many other fading scenarios. In [5], the secrecy capacity over complex Gaussian fading channels was discussed. For multi-input multi-output (MIMO) Rayleigh fading channels, the secrecy capacity of wireless communication systems was studied in [6]. As is known, Nakagami fading is a generalised model, which is suitable for many fading scenarios. In [7], it was shown that Nakagami fading has higher accuracy in matching actual data than the lognormal, Rayleigh or Rice fading. Moreover, many well-known fadings, such as Rayleigh fading, one-side Gaussian fading, *et al.*, are special cases of Nakagami fading. In [8], the probability of nonzero secrecy capacity (PNSC) and the secrecy outage probability (SOP) over Nakagami fading channels were analysed. For relay-assisted wireless networks over Nakagami fading channels, the instantaneous secrecy capacity was derived in [9]. Considering a system with a transmitter, a legitimate receiver and an eavesdropper, the ergodic secrecy capacity (ESC) over Nakagami fading channels was analysed in [10]. In [11], the ESC over Nakagami fading channels with multiple eavesdroppers was analysed. In [12], the ESC over $\alpha-\mu$ fading channels was discussed. However, Tang *et al.* [8], Zhao *et al*. [9], Nguyen *et al.* [10], Sarkar *et al.* [11], and Lei *et al.* [12] focus on single-antenna scenarios. For multi-antenna scenarios, less work has been done for the PLS over Nakagami channels. In [13], the SOP, PNSC, and ϵ-outage secrecy rate were analysed over MIMO Nakagami channels.

To the best of our knowledge, when the transmitter has perfect channel state information (CSI) of the main channel and no CSI of the eavesdropping channel, the secrecy capacity over Nakagami channels, even over Rayleigh fading channels, is still unknown [14]. For the MIMO system, the CSI of the main channel is needed to feed back to the transmitter. Moreover, the front-end architecture and radio frequency selection of multi-antenna nodes are highly complex and expensive. An efficient method is to employ the selective transmission (ST) and maximal ratio combining (MRC) scheme, which provides a good trade-off between system performance and computational complexity. In [15], the SOP was analysed over Rayleigh fading channels with the ST-MRC scheme. By using the ST-MRC scheme, the SOP, PNSC, and asymptotic outage probability over Rayleigh fading channels were analysed in [16]. It should be emphasised that the secrecy capacity is the supremum of all achievable secrecy rates. When employing the ST-

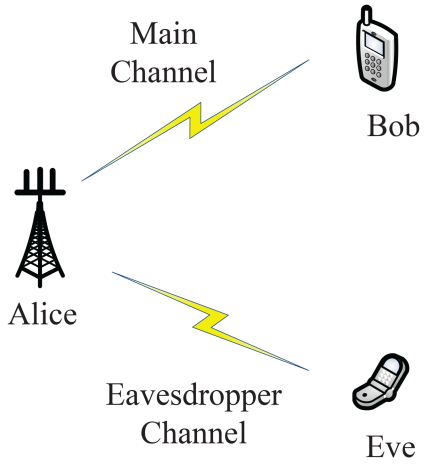

Fig. 1 *Wireless communication network including three multi-antenna entities (i.e. Alice, Bob, and Eve)*

Table 1 Some special cases of the Nakagami distribution

Distributions	m
Rayleigh	1
one-side Gaussian	1/2
AWGN	$\to \infty$

MRC scheme, the secrecy capacity reduces to the secrecy rate. Up to now, the ergodic secrecy rate (ESR) over the MIMO Nakagami fading channel with the ST-MRC scheme has not been investigated in the open literature.

Motivated by the above-mentioned work, the ESR for a wireless communication network over MIMO Nakagami fading channels is further investigated in this paper. The network includes three entities, i.e. a transmitter with N_A antennas (i.e. Alice), a legitimate receiver with N_B antennas (i.e. Bob), and an eavesdropper with N_E antennas (i.e. Eve). By employing the ST scheme at Alice and the MRC scheme at Bob and Eve, the ESR and its lower bound are analysed. The main contributions of this paper are listed as follows:

- Under Nakagami fading channels, an exact theoretical expression of the ESR is derived. At Alice, the ST is employed, while the MRC is employed at Bob and Eve. By using the ST-MRC scheme, the theoretical expression of the ESR is derived, which is with infinite summation and continued product terms.
- Under Nakagami fading channels, a lower bound of the ESR is derived. Due to the infinite summations and continued products, the exact theoretical expression of the ESR is not tractable to evaluate the system performance. To reduce the computational complexity and obtain more insights, the lower bound of the ESR is obtained, which is in a closed form.
- As special cases, the lower bounds of the ESR for signal-antenna scenario and Rayleigh fading channel are also derived, respectively. All derived theoretical expressions are verified by using the Monte-Carlo simulations.

The rest of the paper is organised as follows. At first, the system model is provided in Section 2. Then, Section 3 focuses on the secrecy performance analysis, and derives the exact expression of the ESR and its lower bound. Section 4 presents some numerical results before Section 5 concludes the paper.

2 System model

As shown in Fig. 1, a wireless communication system is established, which includes three multi-antenna entities. The transmitter, legitimate receiver, and eavesdropping receiver are denoted as Alice, Bob, and Eve, respectively. At Alice, Bob, and Eve, the numbers of antennas are denoted as N_A, N_B, and N_E, respectively. In the system, Alice transmits visible-light signal to Bob. Due to the broadcast feature of the visible-light signal, Eve can also receive the signal.

At Alice, the ST scheme is employed to maximise the received signal-to-noise ratio (SNR) at Bob. Therefore, the best antenna at Alice is selected by using the following criterion:

$$\alpha^* = \arg\max_{1 \le \alpha \le N_A} \| \boldsymbol{H}_{\alpha,B} \| \tag{1}$$

where $\| \cdot \|$ represents the Euclidean norm. $\boldsymbol{H}_{\alpha,B} = [h_{\alpha,1}, \ldots, h_{\alpha,N_B}]^T$ denotes the channel gain vector between the αth antenna at Alice and all antennas at Bob. The element $h_{\alpha,n}$ in $\boldsymbol{H}_{\alpha,B}$ denotes the channel gain between the αth antenna at Alice and nth antenna at Bob, which follows a Nakagami distribution, i.e. [17]

$$f_{h_{\alpha,n}}(h) = \frac{2m^m}{\Gamma(m)\Omega^m} h^{2m-1} \exp\left(-\frac{mh^2}{\Omega}\right), \quad h > 0, \tag{2}$$

where $m \ge 0.5$ denotes the fading parameter, $\Omega \ge 0$ is a parameter controlling spread, $\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\,dx$ denotes the Gamma function. The Nakagami distribution can be adjusted by the controlling parameter m. Moreover, the Nakagami distribution covers several commonly used fading distributions, as shown in Table 1.

After using the ST scheme, the received signal vector $\boldsymbol{Y}_B \in \mathbb{C}^{N_B \times 1}$ at Bob is expressed as

$$\boldsymbol{Y}_B = \boldsymbol{H}_{\alpha^*,B} X + \boldsymbol{Z}_B \tag{3}$$

where X is the transmit signal. $\boldsymbol{Z}_B \sim N(0, \sigma_B^2)$ is the additive white Gaussian noise (AWGN) vector at Bob, where σ_B^2 is the noise variance at Bob. Then, by using the MRC scheme at Bob, the received signal is given by

$$y_B = \boldsymbol{H}_{\alpha^*,B}^H \boldsymbol{H}_{\alpha^*,B} X + \boldsymbol{H}_{\alpha^*,B}^H \boldsymbol{Z}_B \tag{4}$$

Therefore, the instantaneous SNR U at Bob is expressed as

$$U = \frac{E_s \| \boldsymbol{H}_{\alpha^*,B} \|^2}{\sigma_B^2} \tag{5}$$

where E_s is the energy per symbol. $\bar{r}_a$ is the average SNR per symbol, which is given by $\bar{r}_a = \Omega_a E_s / \sigma_B^2$.

By analyzing the system model, the probability density function (PDF) and the cumulative distribution function (CDF) of the instantaneous SNR U are given in the following lemma.

Lemma 1: Under the Nakagami fading channels, the PDF and CDF of the instantaneous SNR U can be written, respectively, as

$$f_U(u) = \frac{N_A}{\Gamma(N_B m_a)} \sum_{p=0}^{N_A - 1} \binom{N_A - 1}{p} (-1)^p e^{-(((p+1)m_a u)/\bar{r}_a)} \times \prod_{i=1}^{N_B m_a - 1} \left[\sum_{n_i = 0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(i+1)} \right)^{n_i - n_{i+1}} \right] \left(\frac{m_a}{\bar{r}_a} \right)^{\mu} u^{\mu - 1}, \; u \ge 0 \tag{6}$$

and (see (7)) , where $m_a \in \mathbb{N}^+$, $\mu = N_B m_a + \sum_{k=1}^{N_B m_a - 1} n_k$, $n_0 = p$, $n_{N_B m_a} = 0$. $\binom{a}{b}$ denotes the binomial coefficient, and $\gamma(s,x) = \int_0^x t^{s-1} e^{-t}\,dt$ denotes the lower incomplete Gamma function.

Proof: See [13]. □

By using the ST scheme, a best transmit antenna is chosen for Bob. However, the chosen antenna using the ST scheme is just a

$$F_U(u) = \frac{N_A}{\Gamma(N_B m_a)} \sum_{p=0}^{N_A-1} \binom{N_A-1}{p} (-1)^p \times \prod_{i=1}^{N_B m_a - 1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(i+1)} \right)^{n_i - n_{i+1}} \right] \frac{\gamma(\mu, ((p+1)m_a u/\bar{r}_a))}{(p+1)^\mu} \tag{7}$$

randomly selected antenna for Eve. At Eve, the MRC scheme is also employed. Therefore, the received signal y_E at Eve is obtained as

$$y_E = \boldsymbol{H}_{\alpha^*,E}^H \boldsymbol{H}_{\alpha^*,E} X + \boldsymbol{H}_{\alpha^*,E}^H \boldsymbol{Z}_E \tag{8}$$

where $\boldsymbol{H}_{\alpha^*,E} = [h_{\alpha^*,1}, \ldots, h_{\alpha^*,N_E}]^T$ denotes the channel gain vector between the α^*th antenna at Alice and all antennas at Eve, and the element $h_{\alpha^*,n}$ denotes the channel gain between the α^*th antenna at Alice and the nth antenna at Eve. $\boldsymbol{Z}_E$ is AWGN vector, and σ_E^2 is the noise variance at Eve. Consequently, the instantaneous SNR W at Eve is expressed as

$$W = \frac{E_s \| \boldsymbol{H}_{\alpha^*,E} \|^2}{\sigma_E^2} \tag{9}$$

and the average SNR is $\bar{r}_b = \Omega_b E_s/\sigma_E^2$.

In this section, suppose that the channel components of Bob and Eve are independent but not necessarily identically distributed (INID) random variables with parameters $(m_a, \bar{r}_a)$ and $(m_b, \bar{r}_b)$, respectively. In this case, the PDF and CDF of the instantaneous SNR W are obtained in the following lemma.

Lemma 2: Under the Nakagami fading channel, the PDF and the CDF of the instantaneous SNR W are given, respectively, by

$$f_W(w) = \frac{(m_b)^{N_E m_b} w^{N_E m_b - 1} e^{-(m_b/\bar{r}_b)w}}{\Gamma(N_E m_b)(\bar{r}_b)^{N_E m_b}}, \quad w \geq 0 \tag{10}$$

and

$$F_W(w) = \frac{\gamma(N_E m_b, (m_b w/\bar{r}_b))}{\Gamma(N_E m_b)} \tag{11}$$

where $m_b \in \mathbb{N}^+$.

Proof: See [13, 18]. □

3 Secrecy performance analysis

Here, the secrecy performance will be analysed. Firstly, the exact expression of ESR over the Nakagami−Nakagami fading channels is derived. To reduce computational complexity and achieve more insights, the lower bound of ESR is then obtained.

3.1 Exact ESR

According to the information theory, the instantaneous achievable secrecy rate $R(u, w)$ is given by

$$R(u, w) = \{\ln(1+u) - \ln(1+w)\}^+ \tag{12}$$

where $\{x\}^+ = \max\{x, 0\}$, and $\ln(\cdot)$ denotes the natural logarithm.

Assume that U and W are independent of each other, the ESR can be written as

$$\begin{aligned} R_{Erg} &= \mathbb{E}[R(u,w)] \\ &= \int_0^\infty \int_0^\infty R(u,w) f_{UW}(u,w)\, dw\, du \\ &= \int_0^\infty \int_0^\infty R(u,w) f_U(u) f_W(w)\, dw\, du \end{aligned} \tag{13}$$

where $\mathbb{E}[\cdot]$ represents the expectation operator, and $f_{UW}(u, w)$ denotes the joint PDF of U and W. By calculating (13), the following theorem is derived.

Theorem 1: For the MIMO Nakagami fading channels with the ST-MRC scheme, the exact expression of ESR is given by

$$R_{Erg} = R_1 + R_2 - R_3 \tag{14}$$

where R_1, R_2, and R_3 can be written, respectively, as

$$\begin{aligned} R_1 = {} & \frac{N_A}{\Gamma(N_B m_a)\Gamma(N_E m_b)} \sum_{p=0}^{N_A-1} \binom{N_A-1}{p} (-1)^p \\ & \times \prod_{i=1}^{N_B m_a - 1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(i+1)} \right)^{n_i - n_{i+1}} \right] \left(\frac{m_a}{\bar{r}_a} \right)^\mu \\ & \times \sum_{l=0}^{+\infty} \frac{(-1)^l \Gamma(N_E m_b + l + \mu)}{\Gamma(l+1)(N_E m_b + l)} \left(\frac{m_b}{\bar{r}_b} \right)^{N_E m_b + l} e^{((p+1)m_a)/\bar{r}_a} \\ & \times \sum_{k=1}^{N_E m_b + l + \mu} \frac{\Gamma(k - N_E m_b - l - \mu, (((p+1)m_a)/\bar{r}_a))}{(((p+1)m_a)/\bar{r}_a)^k} \end{aligned} \tag{15}$$

$$\begin{aligned} R_2 = {} & \frac{N_A}{\Gamma(N_E m_b)\Gamma(N_B m_a)} \left(\frac{m_b}{\bar{r}_b} \right)^{N_E m_b} e^{(m_b/\bar{r}_b)} \sum_{p=0}^{N_A-1} \binom{N_A-1}{p} (-1)^p \\ & \times \prod_{i=1}^{N_B m_a - 1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{n-1}}{n_i} \left(\frac{1}{\Gamma(i+1)} \right)^{n_i - n_{i+1}} \right] \frac{1}{(p+1)^\mu} \\ & \times \sum_{l=0}^{+\infty} \frac{(-1)^l \Gamma(\mu + l + N_E m_b)}{\Gamma(l+1)(\mu+l)} \left(\frac{(p+1)m_a}{\bar{r}_a} \right)^{\mu+l} \\ & \times \sum_{k=1}^{\mu + l + N_E m_b} \frac{\Gamma(k - \mu - l - N_E m_b, (m_b/\bar{r}_b))}{(m_b/\bar{r}_b)^k} \end{aligned} \tag{16}$$

and

$$R_3 = \left(\frac{m_b}{\bar{r}_b} \right)^{N_E m_b} e^{(m_b/\bar{r}_b)} \sum_{k=1}^{N_E m_b} \frac{\Gamma(k - N_E m_b, (m_b/\bar{r}_b))}{(m_b/\bar{r}_b)^k} \tag{17}$$

where $\Gamma(s, x) = \int_x^\infty t^{s-1} e^{-t}\, dt$ denotes the upper incomplete Gamma function, $m_a, m_b \in \mathbb{N}^+$, and $\mu = N_B m_a + \sum_{k=1}^{N_B m_a - 1} n_k$, $n_0 = p$, $n_{N_B m_a} = 0$.

Proof: From (13), the ESR is further written as

$$R_{\mathrm{Erg}} = \int_0^{\infty} \ln(1+u) f_U(u) F_W(u)\,\mathrm{d}u + \int_0^{\infty} \ln(1+w) f_W(w) F_U(w)\,\mathrm{d}w - \int_0^{\infty} \ln(1+w) f_W(w)\,\mathrm{d}w \tag{18}$$

where the first integral is denoted as R_1, and it is given by

$$R_1 = \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}}m_a)\Gamma(N_{\mathrm{E}}m_b)} \sum_{p=0}^{N_{\mathrm{A}}-1} \binom{N_{\mathrm{A}}-1}{p} (-1)^p \times \prod_{i=1}^{N_{\mathrm{B}}m_a-1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(\mathrm{i}+1)} \right)^{n_i-n_{i+1}} \right] \left(\frac{m_a}{\bar{r}_a} \right)^{\mu} \times \underbrace{\int_0^{\infty} \ln(1+u) \mathrm{e}^{-(((p+1)m_a u)/\bar{r}_a)} u^{\mu-1} \gamma\left(N_{\mathrm{E}}m_b, \frac{m_b u}{\bar{r}_b} \right) \mathrm{d}u}_{D_1} \tag{19}$$

Referring to (8.354) in [19] and (78) in [20], D_1 is given by

$$D_1 = \sum_{l=0}^{+\infty} \frac{(-1)^l \Gamma(N_{\mathrm{E}}m_b + l + \mu)}{\Gamma(l+1)(N_{\mathrm{E}}m_b + l)} \left(\frac{m_b}{\bar{r}_b} \right)^{N_{\mathrm{E}}m_b + l} \mathrm{e}^{(((p+1)m_a)/\bar{r}_a)} \times \sum_{k=1}^{N_{\mathrm{E}}m_b + l + \mu} \frac{\Gamma(k - N_{\mathrm{E}}m_b - l - \mu, (((p+1)m_a)/\bar{r}_a))}{(((p+1)m_a)/\bar{r}_a)^k} \tag{20}$$

Substituting (20) into (19), R_1 can be derived as (15).

The second integral in (18) is denoted as R_2, and it is given by

$$R_2 = \frac{(m_b)^{N_{\mathrm{E}}m_b}}{\Gamma(N_{\mathrm{E}}m_b)(\bar{r}_b)^{N_{\mathrm{E}}m_b}} \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}}m_a)} \sum_{p=0}^{N_{\mathrm{A}}-1} \binom{N_{\mathrm{A}}-1}{p} (-1)^p \times \prod_{i=1}^{N_{\mathrm{B}}m_a-1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(i+1)} \right)^{n_i-n_{i+1}} \right] \frac{1}{(p+1)^{\mu}} \times \underbrace{\int_0^{\infty} \ln(1+w) w^{N_{\mathrm{E}}m_b-1} \mathrm{e}^{-(m_b/\bar{r}_b)w} \gamma\left(\mu, \frac{(p+1)m_a w}{\bar{r}_a} \right) \mathrm{d}w}_{D_2} \tag{21}$$

Referring to (8.354) in [19] and (78) in [20], D_2 is given by

$$D_2 = \sum_{l=0}^{+\infty} \frac{(-1)^l \Gamma(\mu + l + N_{\mathrm{E}}m_b)}{\Gamma(l+1)(\mu + l)} \left(\frac{(p+1)m_a}{\bar{r}_a} \right)^{\mu+l} \mathrm{e}^{m_b/\bar{r}_b} \times \sum_{k=1}^{\mu+l+N_{\mathrm{E}}m_b} \frac{\Gamma(k - \mu - l - N_{\mathrm{E}}m_b, (m_b/\bar{r}_b))}{(m_b/\bar{r}_b)^k} \tag{22}$$

Submitting (22) into (21), (16) can be derived.

Finally, the third integral in (18) is denoted as R_3, which is expressed as

$$R_3 = \frac{(m_b)^{N_{\mathrm{E}}m_b}}{\Gamma(N_{\mathrm{E}}m_b)(\bar{r}_b)^{N_{\mathrm{E}}m_b}} \int_0^{\infty} \ln(1+w) w^{N_{\mathrm{E}}m_b-1} \mathrm{e}^{-(m_b/\bar{r}_b)w} \mathrm{d}w \tag{23}$$

According to (78) in [20], (23) can be written as (17). □

3.2 Lower bound of ESR

Although an exact expression is obtained in (14), it is very difficult to evaluate the ESR. This is because infinite summations and continued products exist in the exact expression (14). In this subsection, to reduce the computational complexity, a tight lower bound of ESR will be analysed. Mathematically, the lower bound of the ESR is given by

$$R_{\mathrm{Erg}}^{\mathrm{Low}} = \{R_{1,\mathrm{Erg}} - R_{2,\mathrm{Erg}}\}^+ \tag{24}$$

where $R_{1,\mathrm{Erg}}$ and $R_{2,\mathrm{Erg}}$ denote the ESRs for the Alice−Bob link and Alice−Eve link, respectively. By calculating (24), the following theorem is derived.

Theorem 2: For the MIMO Nakagami fading channels with the ST-MRC scheme, a closed-form expression for the lower bound of ESR is given by

$$R_{\mathrm{Erg}}^{\mathrm{Low}} = \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}}m_a)} \sum_{p=0}^{N_{\mathrm{A}}-1} \binom{N_{\mathrm{A}}-1}{p} (-1)^p \times \prod_{i=1}^{N_{\mathrm{B}}m_a-1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(\mathrm{i}+1)} \right)^{n_i-n_{i+1}} \right] \left(\frac{m_a}{\bar{r}_a} \right)^{\mu} \times \Gamma(\mu) \mathrm{e}^{(((p+1)m_a)/\bar{r}_a)} \sum_{k=1}^{\mu} \frac{\Gamma(k-\mu, (((p+1)m_a)/\bar{r}_a))}{(((p+1)m_a)/\bar{r}_a)^k} - \left(\frac{m_b}{\bar{r}_b} \right)^{N_{\mathrm{E}}m_b} \mathrm{e}^{m_b/\bar{r}_b} \sum_{k=1}^{N_{\mathrm{E}}m_b} \frac{\Gamma(k - N_{\mathrm{E}}m_b, (m_b/\bar{r}_b))}{(m_b/\bar{r}_b)^k} \tag{25}$$

Proof: Referring to (78) in [20], $R_{1,\mathrm{Erg}}$ is given by

$$R_{1,\mathrm{Erg}} = \mathbb{E}_U[\ln(1+U)] = \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}}m_a)} \sum_{p=0}^{N_{\mathrm{A}}-1} \binom{N_{\mathrm{A}}-1}{p} (-1)^p \times \prod_{i=1}^{N_{\mathrm{B}}m_a-1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(\mathrm{i}+1)} \right)^{n_i-n_{i+1}} \right] \left(\frac{m_a}{\bar{r}_a} \right)^{\mu} \times \int_0^{\infty} \mathrm{e}^{-(((p+1)m_a u)/\bar{r}_a)} u^{\mu-1} \ln(1+u)\,\mathrm{d}u \tag{26}$$

Furthermore, (26) can be written as

$$R_{1,\mathrm{Erg}} = \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}}m_a)} \sum_{p=0}^{N_{\mathrm{A}}-1} \binom{N_{\mathrm{A}}-1}{p} (-1)^p \times \prod_{i=1}^{N_{\mathrm{B}}m_a-1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(\mathrm{i}+1)} \right)^{n_i-n_{i+1}} \right] \left(\frac{m_a}{\bar{r}_a} \right)^{\mu} \times \Gamma(\mu) \mathrm{e}^{(((p+1)m_a)/\bar{r}_a)} \sum_{k=1}^{\mu} \frac{\Gamma(k-\mu, (((p+1)m_a)/\bar{r}_a))}{(((p+1)m_a)/\bar{r}_a)^k} \tag{27}$$

Similarly, $R_{2,\mathrm{Erg}}$ can be written as

$$R_{2,\mathrm{Erg}} = \mathbb{E}_W[\ln(1+W)] = R_3 \tag{28}$$

Substituting (27) and (28) into (24), (25) is obtained. □

Remark 1: The lower bound of ESR increases with the increase of N_{A}, and thus large N_{A} can improve the secrecy performance of the system.

Corollary 1: For single-antenna scenario (i.e. $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 1$), the lower bound of ESR (25) reduces to

$$R_{\mathrm{Erg}}^{\mathrm{Low}} = \left\{ \left(\frac{m_a}{\bar{r}_a} \right)^{m_a} \mathrm{e}^{m_a/\bar{r}_a} \sum_{k=1}^{m_a} \frac{\Gamma(k-m_a, (m_a/\bar{r}_a))}{(m_a/\bar{r}_a)^k} - \left(\frac{m_b}{\bar{r}_b} \right)^{m_b} \mathrm{e}^{m_b/\bar{r}_b} \sum_{k=1}^{m_b} \frac{\Gamma(k-m_b, (m_b/\bar{r}_b))}{(m_b/\bar{r}_b)^k} \right\}^+ \tag{29}$$

Corollary 2: Under Rayleigh fading channels (i.e. $m_a = m_b = 1$), the lower bound of ESR (25) becomes

$$
\begin{aligned}
R_{\mathrm{Erg}}^{\mathrm{Low}} = & \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}})} \sum_{p=0}^{N_{\mathrm{A}}-1} \binom{N_{\mathrm{A}}-1}{p} (-1)^p \\
& \times \prod_{i=1}^{N_{\mathrm{B}}-1} \left[\sum_{n_i=0}^{n_{i-1}} \binom{n_{i-1}}{n_i} \left(\frac{1}{\Gamma(i+1)} \right)^{n_i - n_{i+1}} \right] \left(\frac{1}{\bar{r}_a} \right)^{\mu} \\
& \times \Gamma(\mu) \mathrm{e}^{(p+1)/\bar{r}_a} \sum_{k=1}^{\mu} \frac{\Gamma(k-\mu, ((p+1)/\bar{r}_a))}{((p+1)/\bar{r}_a)^k} \\
& - \left(\frac{1}{\bar{r}_b} \right)^{N_{\mathrm{E}}} \mathrm{e}^{1/\bar{r}_b} \sum_{k=1}^{N_{\mathrm{E}}} \frac{\Gamma(k-N_{\mathrm{E}}, (1/\bar{r}_b))}{(1/\bar{r}_b)^k}
\end{aligned} \tag{30}
$$

Corollary 3: For single-antenna scenario (i.e. $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 1$) over Rayleigh fading channels (i.e. $m_a = m_b = 1$), the lower bound of ESR (25) becomes

$$
R_{\mathrm{Erg}}^{\mathrm{Low}} = \left\{ \mathrm{e}^{1/\bar{r}_a} \Gamma\left(0, \frac{1}{\bar{r}_a}\right) - \mathrm{e}^{1/\bar{r}_a} \Gamma\left(0, \frac{1}{\bar{r}_b}\right) \right\}^+ \tag{31}
$$

4 Numerical results

In the simulation, a wireless communication network consisting of Alice, Bob, and Eve is considered. Under the system model, some typical results will be presented. To show the accuracy of the derived theoretical expression of the ESR, all theoretical results are confirmed by the Monte Carlo simulations over $Snap = 10^4$ independent snapshots. Specifically, the simulation processes for the exact ESR and the lower bound of the ESR are given in Figs. 2 and 3, respectively.

Fig. 4 depicts the ESR versus $\bar{r}_a$ with different $\bar{r}_b$ when $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 4$ and $m_a = m_b = 1$. As can be seen, when $\bar{r}_a$ is small, the ESR is always zero. This indicates that the main channel is worse than the eavesdropping channel in this case. When $\bar{r}_a$ is large, the ESR becomes larger than zero. Moreover, with the increase of $\bar{r}_a$, the ESR also increases. Therefore, we can conclude that the large average SNR of Bob can improve the system performance. Furthermore, the ESR decreases with the increase of $\bar{r}_b$, which indicates that the large average SNR of Eve will degrade the system performance.

Fig. 5 presents the ESR versus $\bar{r}_a$ with different m_b when $N_{\mathrm{A}} = 4$, $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$, $m_a = 2$ and $\bar{r}_b = 6$. As can be observed, the ESR increases with the increase of $\bar{r}_a$, which is consistent with the observed conclusion in Fig. 4. Moreover, the ESR increases with the decrease of m_b, which indicates that large m_b will degrade the system performance.

Fig. 6 shows the ESR versus $\bar{r}_a$ with different N_{A} when $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$, $m_a = m_b = 2$, and $\bar{r}_b = 6$. With the increase of N_{A}, the ESR increases accordingly, which coincides with Remark 1. Therefore, the large number of antennas at Alice can enhance the security for wireless transmissions.

In Figs. 4–6, all theoretical results of the exact ESR and its lower bound match the simulation results very well. Moreover, the gaps between the exact ESR and the lower bounds are also very small. Therefore, as a low complexity expression, the derived lower bound of ESR can be used to evaluate the ESR without time-intensive simulations.

The ESC with the single-antenna setting over the Nakagami channel has been investigated in [10]. To compare our work with [10], Fig. 7 shows the ESR comparison between (29) in Corollary 1 and (5) in [10]. In the simulation, $m_a = m_b = 2$ and $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 1$. It can be found that the results of (29) in Corollary 1 are the same as that of (5) in [10], which verifies the correctness of the derived theoretical expression in this paper. Moreover, the expression (5) in [10] is only suitable for the case $m_a = m_b$, while the expression (29) in this paper has no such constraint, which is suitable for any m_a and m_b.

The Rayleigh fading channel is a special case of Nakagami fading channel. Fig. 8 compares the ESR results over Rayleigh channel (i.e. $m_a = m_b = 1$) with that over Nakagami channel (i.e. $m_a = m_b = 2$) when $\bar{r}_b = 6$, $N_{\mathrm{A}} = 4$, and $N_{\mathrm{B}} = N_{\mathrm{E}} = 2$. Similar to Figs. 4–6, the ESR in this figure also increases with $\bar{r}_a$. Moreover, it can be observed that the curve over Rayleigh channel outperforms that over Nakagami channel with $m_a = m_b = 2$.

Step 1): According to the PDF in (6), randomly generate a realization of U, i.e., u.
Step 2): According to the PDF in (10), randomly generate a realization of W, i.e., w.
Step 3): Compute the instantaneous secrecy rate $R_i(u, w)$ by using (12).
Step 4): Perform **Steps 1)-3)** for $\mathrm{Snap} = 10^4$ times, the ESR is given by $R_{\mathrm{Erg}} = \sum_{i=1}^{\mathrm{Snap}} R_i(u, w)/\mathrm{Snap}$.

Fig. 2 *Simulation processes for the exact ESR*

Step 1): According to the PDF in (6), randomly generate a realization of U, i.e., u.
Step 2): Compute the instantaneous secrecy rate of Bob $R_{1,i} = \ln(1+u)$.
Step 3): According to the PDF in (10), randomly generate a realization of W, i.e., w.
Step 4): Compute the instantaneous secrecy rate of Eve $R_{2,i} = \ln(1+w)$.
Step 5): Perform **Steps 1)-4)** for $\mathrm{Snap} = 10^4$ times, the ESRs of Bob and Eve are given by $R_{1,\mathrm{Erg}} = \sum_{i=1}^{\mathrm{Snap}} R_{1,i}/\mathrm{Snap}$ and $R_{2,\mathrm{Erg}} = \sum_{i=1}^{\mathrm{Snap}} R_{2,i}/\mathrm{Snap}$, respectively.
Step 6): Compute the lower bound of the ESR $R_{\mathrm{Erg}}^{\mathrm{Low}}$ by using (24).

Fig. 3 *Simulation processes for the lower bound of ESR*

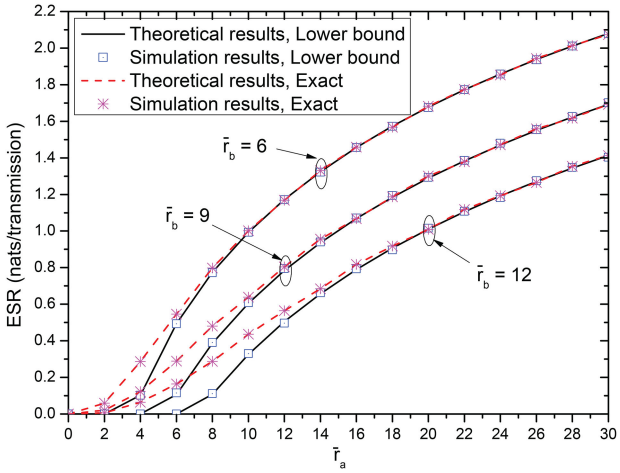

Fig. 4 *ESR versus $\bar{r}_a$ with different $\bar{r}_b$ when $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 4$ and $m_a = m_b = 1$*

5 Conclusion

Recently, PLS is an increasing concern for wireless communication, where the secure transmissions may be affected by channel fading. Focusing on the MIMO Nakagami fading model, this paper investigates the performance of ESR. By using the ST scheme at Alice and the MRC scheme at Bob and Eve, closed-form expressions of the ESR and its lower bound are derived, respectively. Numerical results show that the derived expressions are very accurate to evaluate the ESR performance. The availability of the closed-form expressions will expedite the analysis and help gain deeper insights.

6 Acknowledgments

The work is supported by National Natural Science Foundation of China (61701254), Natural Science Foundation of Jiangsu Province (BK20170901), the Funds for International Cooperation and Exchange of the National Natural Science Foundation of China

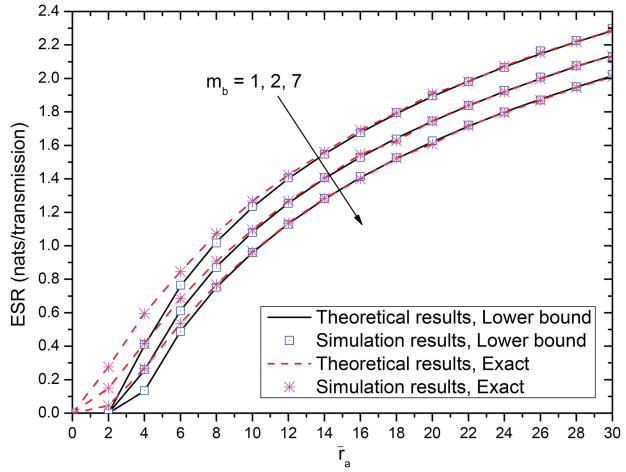

Fig. 5 *ESR versus $\bar{r}_a$ with different m_b when $N_A = 4$, $N_B = N_E = 1$, $m_a = 2$ and $\bar{r}_b = 6$*

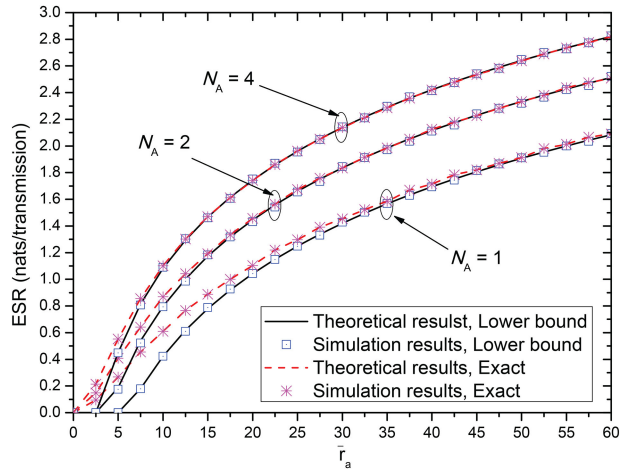

Fig. 6 *ESR versus $\bar{r}_a$ with different N_A when $N_B = N_E = 1$, $m_a = m_b = 2$, and $\bar{r}_b = 6$*

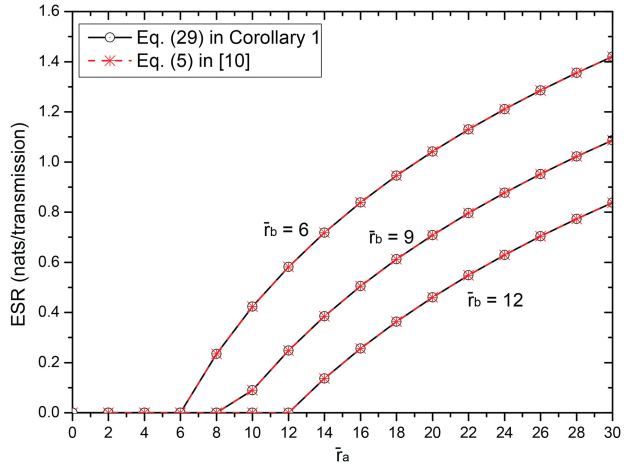

Fig. 7 *ESR comparison between (29) in Corollary 1 and (5) in [10] when $m_a = m_b = 2$ and $N_A = N_B = N_E = 1$*

(61720106003), the open research fund of National Mobile Communications Research Laboratory, Southeast University (2017D06), the open fund for Jiangsu key laboratory of traffic and transportation security, Huaiyin Institute of Technology (TTS2017-03), the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry

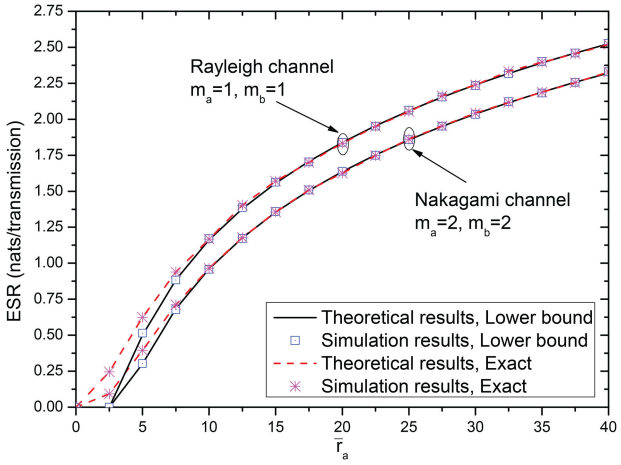

Fig. 8 *ESR comparison between Rayleigh channel and Nakagami channel when $\bar{r}_b = 6$, $N_A = 4$, and $N_B = N_E = 2$*

of Education (JZNY201706), the Open Research Subject of Key Laboratory (Research Base) of Signal and Information Processing, Xihua University (szjj2017-047), and NUPTSF (NY216009).

7 References

[1] Chen, X., Ng, D.W.K., Gerstacker, W.H., *et al.*: 'A survey on multiple-antenna techniques for physical layer security', *IEEE Commun. Surv. Tutorials*, 2017, **19**, (2), pp. 1027–1053

[2] Shiu, Y.-S., Chang, S.Y., Wu, H.-C., *et al.*: 'Physical layer security in wireless networks: a tutorial', *IEEE Wirel. Commun.*, 2011, **18**, (2), pp. 66–74

[3] Shannon, C.E.: 'Communication theory of secrecy systems', *Bell Syst. Tech. J.*, 1949, **28**, (4), pp. 656–715

[4] Wyner, A.D.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387

[5] Nguyen, V.-D., Hoang, T.M., Shin, O.-S.: 'Secrecy capacity of the primary system in a cognitive radio network', *IEEE Trans. Veh. Technol.*, 2015, **64**, (8), pp. 3834–3843

[6] Lin, S.-C., Lin, C.-L.: 'On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT', *IEEE Trans. Wirel. Commun.*, 2014, **13**, (6), pp. 3293–3306

[7] Mishra, M.K., Sood, N., Sharma, A.K.: 'Efficient BER analysis of OFDM system over Nakagami-m fading channel', *Int. J. Ad. Sci. Technol.*, 2011, **37**, pp. 37–46

[8] Tang, C., Pan, G., Li, T.: 'Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels', *IEEE Wirel. Commun. Lett.*, 2014, **3**, (6), pp. 609–612

[9] Zhao, R., Yuan, Y., Fan, L., *et al.*: 'Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels', *IEEE Trans. Commun.*, 2017, **65**, (2), pp. 549–562

[10] Nguyen, T.V., Ngo, H.Q., Shin, H.: 'Secrecy capacity of Nakagami-m fading channels'. Proc. Int. Techn. Conf. Circuits Syst., Comput., Commun., Jeju Island, Korea, July 2009, pp. 1262–1265

[11] Sarkar, M.Z.I., Ratnarajah, T., Sellathurai, M.: 'Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppres'. Proc. 43th Asilomar Conf. Sig., Syst., Comput., Pacific Grove, California, USA, November 2009, pp. 829–833

[12] Lei, H., Ansari, I.S., Pan, G., *et al.*: 'Secrecy capacity analysis over α-μ fading channels', *IEEE Commun. Lett.*, 2017, **21**, (6), pp. 1445–1448

[13] Yang, N., Yeoh, P.L., Elkashlan, M., *et al.*: 'Transmit antenna selection for security enhancement in MIMO wiretap channels', *IEEE Trans. Commun.*, 2013, **61**, (1), pp. 144–154

[14] Khisti, A., Wornell, G.W.: 'Secure transmission with multiple antennas I: The MISOME wiretap channel', *IEEE Trans. Inf. Theory*, 2010, **56**, (7), pp. 3088–3104

[15] Yang, N., Yeoh, P.L., Elkashlan, M., *et al.*: 'MIMO wiretap channels: secure transmission using transmit antenna selection and receive generalized selection combining', *IEEE Commun. Lett.*, 2013, **17**, (9), pp. 1754–1757

[16] Xiong, J., Tang, Y., Ma, D., *et al.*: 'Secrecy performance analysis for TAS-MRC system with imperfect feedback', *IEEE Trans. Inf. Forensics Secur.*, 2015, **10**, (8), pp. 1617–1629

[17] Simon, M.K., Alouini, M.-S.: '*Digital communication over fading channels*' (John Wiley and Sons, Hoboken, 2000, 2nd edn. 2005)

[18] Chen, Z., Chi, Z., Li, Y., *et al.*: 'Error performance of maximal-ratio combining with transmit antenna selection in flat Nakagami-m fading channels', *IEEE Trans. Wirel. Commun.*, 2009, **8**, (1), pp. 424–431

[19] Gradshteyn, I.S., Ryzhik, I.M.: '*Table of integrals, series, and products*' (Elsevier, Boston, 1980, 7th edn. 2007)

[20] Alouini, M.-S., Goldsmith, A. J.: 'Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques', *IEEE Trans. Veh. Technol.*, 1999, **48**, (4), pp. 1165–1181