SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

September 2022, Vol. 65 192304:1–192304:13
https://doi.org/10.1007/s11432-021-3353-5

Secret key generation over a Nakagami-m fading channel with correlated eavesdropping channel

Shixun GONG[1,2], Xiaofeng TAO[1*], Na LI[1,2], Haowei WANG[1] & Jin XU[1]

[1]*National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[2]*Beijing University of Posts and Telecommunications Research Institute, Shenzhen* 518000*, China*

Received 13 July 2021/Revised 29 August 2021/Accepted 26 October 2021/Published online 29 August 2022

Abstract The analysis of secret key capacity is an important investigation on the design of secret key agreement protocol. In this paper, we characterize the secret key capacity based on received signal envelopes obeying Nakagami-m distribution between two legitimate users, in the presence of a passive eavesdropper, when the eavesdropping channel is correlated with the legitimate channel. The expression of secret key capacity is derived based on mutual information and applies to both integer and non-integer m. Simulation results indicate that the secret key capacity is proportional to m-fading parameter and average signal-to-noise ratio (SNR) and inversely proportional to the number of paths. In addition, some behaviors of secret key capacity over a high mobility fading channel, and microcell and macrocell environments are provided. These results cover the performance of secret key capacity when the received signal envelope follows Rayleigh, Rician, and Gaussian distributions.

Keywords physical layer security, physical layer secret key generation, Nakagami-m fading, correlated eavesdropping channel, secret key capacity

Citation Gong S X, Tao X F, Li N, et al. Secret key generation over a Nakagami-m fading channel with correlated eavesdropping channel. Sci China Inf Sci, 2022, 65(9): 192304, https://doi.org/10.1007/s11432-021-3353-5

1 Introduction

Information security has become one of the top priorities in the fifth generation (5G) mobile communications and beyond [1–7]. Physical layer secret key generation (PLSKG) is one of the effective technologies to achieve secure communications. The secret key can be extracted from wireless channels based on inherent characteristics such as randomness and unpredictability, regardless of the correlation of common randomness observed by legitimate users [8–11]. This kind of technology makes the security of generated secret key less dependent on hardware conditions and computing capability, and it does not require third-party infrastructure like traditional cryptography technology in the process of key distribution [12, 13].

Most of the previous studies on PLSKG over wireless networks consider the independence of eavesdropping channel and legitimate channel when the eavesdropper is more than a half of wavelength far away from legitimate users [14–16]. However, as pointed out in [17], this assumption of spatial decorrelation with distance is not accurate enough in a real wireless system, and the eavesdroppers might obtain useful information of secret keys using their own observations when channel variations come from the motion in the environment. Because of this, the security performance in the presence of eavesdroppers should be fully considered during the design and realization of secret key agreement protocols.

In the literature on correlated channel models for PLSKG, Ref. [18] investigated the impact of channel sparsity on PLSKG. Ref. [19] studied a more practical model and derived the expression of secret key capacity between channel gains by taking into account the parameters including sampling period, eavesdroppers' location, qualities of legitimate and eavesdropping channels, Doppler spread, and length of pilot. Based on the aforementioned model, Ref. [20] further derived the expression of secret key capacity when users regarded the received signal phase as the common randomness. These studies all

* Corresponding author (email: taoxf@bupt.edu.cn)

considered the correlated multipath Rayleigh fading channel model, where the in-phase and quadrature components of channel gain approximately follow Gaussian distribution. The expression of secret key capacity between Gaussian sources is already derived in [21], and it can be approximated as a function of the correlation coefficient. In addition to the Rayleigh fading channel, the Nakagami-m fading channel is also widely studied in wireless communications, where the Nakagami-m distribution suits well for many scenarios and covers several different distributions, including one-sided Gaussian, Rayleigh, Rician, and Gaussian distributions, by changing the value of the m-fading parameter. To the best of our knowledge, the secret key capacity for Nakagami-m fading channel with correlated eavesdropping channel model has not been characterized so far, possibly because of the high complexity of numerical calculating the mutual information of Nakagami-m fading process.

Motivated by the above observations, in this paper, we consider a more general correlated channel model under the Nakagami-m fading channel for PLSKG. In the considered model, two legitimate users (Alice and Bob) wish to generate a secret key when an eavesdropper (Eve) is curious about the secret key and tries to guess it using his/her channel observations.

The main contributions of this paper are summarized as follows.

• We derive the expression of secret key capacity, measured by mutual information, based on the sampling of the received signal envelopes. The expression shows that the secret key capacity is determined by the m-fading parameter, the average power, and the power correlation coefficient.

• The expression applies to both integer and non-integer m. To verify the theoretical results, we build two simulation models. For integer m, the Nakagami-m fading channel is modeled by the Rayleigh fading channel model proposed in [22], and the corresponding autocorrelation and cross-correlation coefficients in power terms are further derived. For non-integer m, the method in [23] based on the generalized Rician distribution is used to generate two correlated Nakagami-m variables.

• The secret key capacity versus m-fading parameter, number of paths, and average signal-to-noise ratio (SNR) are analyzed using simulations, which indicate that the secret key capacity increases with m-fading parameter and SNR, and reduces with the number of paths.

• The secret key capacity is also analyzed in realistic scenarios including high-speed railway and cellular networks. Simulation results show that the secret key capacity is inversely proportional to the speed of the high-speed railway and the distance in cellular networks.

Compared with the previous studies [19, 20], the results of this paper cover multiple types of fading distributions, and we also can obtain some conclusions different from that in [19, 20]. The results of this paper can provide guidelines on the design of more practical secret key agreement protocols.

The rest of this paper is organized as follows. Section 2 describes the system model. In Section 3, the expression of secret key capacity is derived. The simulation models of correlated Nakagami-m fading channels for integer and non-integer m are shown in Sections 4 and 5, respectively. The numerical results are shown in Section 6. Section 7 concludes this paper.

Notations. $\mathrm{E}(\cdot)$, $\mathrm{Cov}(\cdot,\cdot)$, and $\mathrm{Var}(\cdot)$ denote the expectation, covariance, and variance operations, respectively; $(\cdot)^{\mathrm{H}}$ denotes the conjugate transpose; $I(\cdot,\cdot)$ denotes the mutual information of two parties; $\|\cdot\|$ is the norm of matrix; $J_0(\cdot)$ is a zeroth-order Bessel function of the first kind; $[\cdot]^+$ is $a=\max\{x,0\}$; $\lfloor\cdot\rfloor$ denotes the integer part of the random variable; $I_\nu(\cdot)$ is the modified Bessel function of the first kind of order ν.

2 System model

In this section, the considered system model for PLSKG is introduced, including correlated Nakagami-m fading channel model and channel estimation.

2.1 Correlated Nakagami-m fading channel model

As shown in Figure 1, two legitimate users (Alice and Bob) aim to generate a secret key when an eavesdropper (Eve) listens to their communication. Without loss of generality, a common correlated channel model is considered, where Eve is d away from Bob, and Eve and Bob are both stationary. Under this assumption, the channel between Eve and Bob is not random enough and the corresponding channel observations do not influence the secret key bits [24]. Thus, Eve only receives the transmissions from Alice. The involved channels from Alice to Bob, Bob to Alice, and Alice to Eve are denoted as h_{ab}, h_{ba}, and h_{ae}, respectively. The legitimate and eavesdropping channels are correlated and the received signal

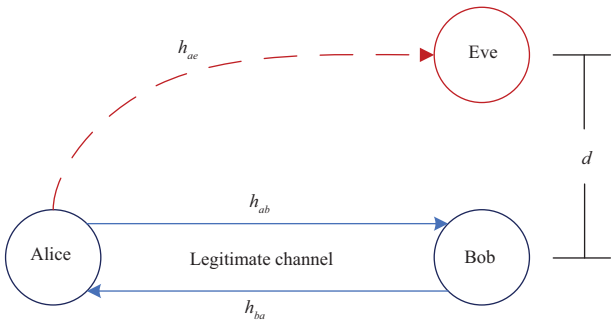

Figure 1 (Color online) System model for PLSKG.

envelope at each terminal follows Nakagami-m fading distribution. The marginal probability density function (pdf) of Nakagami-m distribution is proposed and defined in [25] as follows:

$$f_{R_i}(r_i) = \frac{2m_i^{m_i} r_i^{2m_i-1}}{\Gamma(m_i)\Omega_i^{m_i}} \exp\left[-\frac{m_i}{\Omega_i} r_i^2\right], \quad r_i \geqslant 0, \quad \text{for } i = a, b, e, \tag{1}$$

where $m_i = \frac{\mathrm{E}^2[r_i^2]}{\mathrm{E}[(r_i^2 - \mathrm{E}[r_i^2])^2]} \geqslant \frac{1}{2}$ denotes the Nakagami fading parameter, which characterizes the fading severity of channel [25], and the fading severity decreases with the increase of m_i; $\Gamma(m_i) = \int_0^\infty x^{m_i-1}\mathrm{e}^{-x}\mathrm{d}x$ represents the Gamma function [26]; $\Omega_i = \mathrm{E}[r_i^2]$ is the average power.

In this paper, identical fading parameters are considered, i.e., $m_a = m_b = m_e = m$ holds. In addition, Nakagami-m distribution is a generic model for encompassing various distributions for different values of m (one-sided Gaussian distribution for $m = 1/2$; Rayleigh distribution for $m = 1$, i.e., $r \sim \text{Rayleigh}(\sqrt{\frac{\Omega}{2}})$; Rician distribution for $m > 1$, and the relationship between Rician factor k and m is $k = \frac{\sqrt{m^2-m}}{m-\sqrt{m^2-m}}$; Gaussian distribution for $m \to \infty$) [25].

2.2 Channel estimation

In this subsection, the common process of channel estimation for PLSKG is described.

Assume that the PLSKG works in time-division duplex (TDD) mode, and the reciprocity holds for the uplink and downlink wireless channels. Denote T_{Sam} and τ as the sampling period and time delay, respectively. Suppose that at time $t_a = iT_{\text{Sam}}$ with $i = 0, 1, \ldots, L-1$, where L is the sampling times, Alice transmits a pilot sequence $s(t_a)$ to Bob (Eve also can receive the signal). Then, at time $t_b = t_a + \tau$, Bob transmits a pilot sequence $s(t_b)$ to Alice. Alice, Bob, and Eve receive

$$y_a(t_b) = h_{ba}(t_b)s(t_b) + n_a(t_b), \tag{2}$$
$$y_b(t_a) = h_{ab}(t_a)s(t_a) + n_b(t_a), \tag{3}$$
$$y_e(t_a) = h_{ae}(t_a)s(t_a) + n_e(t_a), \tag{4}$$

where n_a, n_b, and n_e are independent and identically distributed (i.i.d.) additive white Gaussian noises (AWGN) with variances $\sigma_{n_a}^2$, $\sigma_{n_b}^2$, and $\sigma_{n_e}^2$, respectively. For case of notation, in this paper, the time index t_a and t_b are removed from above formulas with the assumptions $s(t_a) = s(t_b) = s$. Denote R_a, R_b, and R_e as the Nakagami-m random variables and the received signal envelopes at Alice, Bob, and Eve, respectively. Denote ϕ_a, ϕ_b, and ϕ_e as the received signal phases at Alice, Bob, and Eve, respectively. The channel gains can be written as $h_{ab} = R_b\mathrm{e}^{\mathrm{j}\phi_b}$, $h_{ba} = R_a\mathrm{e}^{\mathrm{j}\phi_a}$, and $h_{ae} = R_e\mathrm{e}^{\mathrm{j}\phi_e}$, and the envelope and phase are statistically independent.

After receiving signals, Alice, Bob, and Eve all can observe a noisy version of channel gain by [19, 20]

$$\hat{h}_{ba} = y_a \frac{s^{\mathrm{H}}}{||s||^2} = h_{ba} + n_a \frac{s^{\mathrm{H}}}{||s||^2}, \tag{5}$$
$$\hat{h}_{ab} = y_b \frac{s^{\mathrm{H}}}{||s||^2} = h_{ab} + n_b \frac{s^{\mathrm{H}}}{||s||^2}, \tag{6}$$
$$\hat{h}_{ae} = y_e \frac{s^{\mathrm{H}}}{||s||^2} = h_{ae} + n_e \frac{s^{\mathrm{H}}}{||s||^2}, \tag{7}$$

$$\text{s.t.} \quad ||s||^2 = P_s l_s,$$

where l_s represents the length of s, and P_s denotes the transmission power. The average SNR of channel is expressed as $\gamma_i = \frac{P_s \Omega_i}{\sigma^2}$, for $i = a, b, e$. The corresponding average power with estimate error is $\hat{\Omega}_i = \Omega_i + \frac{\sigma^2}{P_s l_s}$, for $i = a, b, e$.

After channel estimation, Alice and Bob make the Nakagami-m fading envelopes extracted from estimated channel state information as the common randomness to generate a secret key. In the meanwhile, Eve also can estimate the secret key using his/her channel observations. The rest processes of PLSKG contain quantization, information reconciliation, and privacy amplification, which are omitted since they are not the focus of this paper.

3 Secret key capacity

In this section, the expression of secret key capacity for the considered PLSKG model is derived.

According to [27], the secret key capacity can be calculated through mutual information between channel characteristics (received signal envelope in this paper).

Theorem 1. The secret key capacity C_{key} based on the sampling of the received signal envelope for the considered PLSKG model is defined as

$$\begin{aligned} &C_{\text{key}} = [I(\hat{R}_a; \hat{R}_b) - I(\hat{R}_a; \hat{R}_e)]^+, \\ &\text{s.t.} \;\; \hat{R}_a = |\hat{h}_{ba}|, \;\; \hat{R}_b = |\hat{h}_{ab}|, \;\; \hat{R}_e = |\hat{h}_{ae}|, \end{aligned} \tag{8}$$

where $I(\hat{R}_a; \hat{R}_b)$ denotes the maximum achievable secret key rate when the eavesdropping channel is independent with the legitimate channel; $I(\hat{R}_a; \hat{R}_e)$ denotes the information leaked to the eavesdropper.

To calculate the terms in (8), Theorem 2 is utilized.

Theorem 2 (Subsection 2.3 of [28])**.** Let $(X, Y) \sim f(x, y)$ be a pair of continuous random variables. The mutual information (in bits) between X and Y is defined as

$$I(X; Y) = \iint_{x,y} f(x, y) \log_2 \frac{f(x, y)}{f(x) f(y)} \mathrm{d}x \mathrm{d}y, \tag{9}$$

where $f(x)$ and $f(y)$ are the marginal pdf of X and Y, respectively; $f(x, y)$ denotes the joint pdf of (X, Y).

The marginal pdf of Nakagami-m distribution is defined in (1), and the joint pdf of Nakagami-m distribution with identical m-fading parameter is as follows [25]:

$$\begin{aligned} &f_{R_i, R_j}(r_i, r_j) = \frac{4 (r_i r_j)^m}{\Gamma(m) \Theta_i \Theta_j (1 - \rho_2) (\Theta_i \Theta_j \rho_2)^{(m-1)/2}} \exp\left[-\frac{\Theta_j r_i^2 + \Theta_i r_j^2}{\Theta_i \Theta_j (1 - \rho_2)} \right] I_{m-1}\left\{ \frac{2\sqrt{\rho_2} r_i r_j}{\sqrt{\Theta_i \Theta_j}(1 - \rho_2)} \right\}, \\ &\text{for } i = a, \;\; j = b, e; \;\; r_i \geqslant 0, \;\; r_j \geqslant 0; \;\; m \geqslant \frac{1}{2}, \end{aligned} \tag{10}$$

where $\rho_2 = \frac{\mathrm{Cov}(r_i^2, r_j^2)}{\sqrt{\mathrm{Var}(r_i^2)\mathrm{Var}(r_j^2)}}$ denotes the correlation coefficient in power terms between two Nakagami-m fading envelopes; $\Theta_i = \frac{\Omega_i}{m}$ and $\Theta_j = \frac{\Omega_j}{m}$.

Remark 1. The expression of joint pdf in (10) is derived when the Nakagami-m fading process is modeled as the square root of a summation of m squared i.i.d. Rayleigh fading process [25], where ρ_2, Θ_i, and Θ_j are the correlation coefficient in power terms and the average power of the Rayleigh fading process, respectively. The power autocorrelation coefficient describes the correlation between legitimate channel observations, and the power cross-correlation coefficient describes the correlation between legitimate and eavesdropping channel observations.

Remark 2. Even though the joint pdf of Nakagami-m distribution defined in (10) is derived when m is subject to a positive integer, the expression (10) is also suitable for the scenarios with any positive number which is not less than $\frac{1}{2}$. Please refer to Section 6 of [25] for more information.

Substituting (1) and (10) into (9), the expression of mutual information can be obtained.

Theorem 3. For $(X,Y)\sim$ Nakagami$(m,\Omega_1;m,\Omega_2|\rho_2)$, the expression of mutual information for (X,Y) can be expressed as

$$
\begin{aligned}
I_{\text{nak}} =& \frac{2m^{m+1}}{\ln 2\Gamma(m)(\Omega_1\Omega_2)^{(m+1)/2}} \\
&\times\left\{\begin{array}{l}
\ln\dfrac{\Gamma(m)\Omega_1^{(m-1)/2}\Omega_2^{(m-1)/2}}{(1-\rho_2)\rho_2^{(m-1)/2}m^{m-1}}\displaystyle\sum_{k_1=0}^{\infty}b_{k_1}\gamma\left(m+k_1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\gamma\left(m+k_1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right) \\
+\displaystyle\sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}c_{k_1,k_2}\left[\frac{\ell_x^{2m+2k_1+2k_2}\ln\ell_x}{2m+2k_1+2k_2}-\frac{\ell_x^{2m+2k_1+2k_2}}{(2m+2k_1+2k_2)^2}\right]\gamma\left(m+k_1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right) \\
+\displaystyle\sum_{k_1=0}^{\infty}\sum_{k_3=0}^{\infty}c_{k_1,k_3}\left[\frac{\ell_y^{2m+2k_1+2k_3}\ln\ell_y}{2m+2k_1+2k_3}-\frac{\ell_y^{2m+2k_1+2k_3}}{(2m+2k_1+2k_3)^2}\right]\gamma\left(m+k_1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right) \\
-\displaystyle\sum_{k_1=0}^{\infty}b_{k_1}\rho_2\gamma\left(m+k_1+1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\gamma\left(m+k_1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right) \\
-\displaystyle\sum_{k_1=0}^{\infty}b_{k_1}\rho_2\gamma\left(m+k_1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\gamma\left(m+k_1+1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right) \\
+\displaystyle\sum_{k_1=0}^{\infty}\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\frac{a_{k_1}(-1)^{n_1+n_2}m^{n_1+n_2}}{n_1!n_2!\Omega_1^{n_1}\Omega_2^{n_2}(1-\rho_2)^{n_1+n_2}}\left[\frac{\ell_x^{2m+2k_1+2n_1}\ell_y^{2m+2k_1+2n_2}}{4\left(m+k_1+n_1\right)\left(m+k_1+n_2\right)}\right. \\
\times\ln I_{m-1}\left\{\dfrac{2m\sqrt{\rho_2}\ell_x\ell_y}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}\right\}-\dfrac{2m\sqrt{\rho_2}\ell_y^{2m+2k_1+2n_2+1}\Xi\left(\ell_x\right)}{4\sqrt{\Omega_1\Omega_2}(1-\rho_2)\left(m+k_1+n_1\right)\left(m+k_1+n_2\right)} \\
+\dfrac{(m-1)\ell_x^{2m+2k_1+2n_1}\ell_y^{2m+2k_1+2n_2}}{8(m+k_1+n_1)^2\left(m+k_1+n_2\right)}-\dfrac{2m\sqrt{\rho_2}\Xi\left(\ell_x,\ell_y\right)}{2\sqrt{\Omega_1\Omega_2}(1-\rho_2)\left(m+k_1+n_2\right)} \\
\left.+\dfrac{(m-1)\ell_x^{2m+2k_1+2n_1}\ell_y^{2m+2k_1+2n_2}}{8\left(m+k_1+n_1\right)\left(m+k_1+n_2\right)^2}\right]
\end{array}\right\},
\end{aligned}
$$

$$
\begin{aligned}
\text{s.t.}\quad & a_{k_1}\triangleq\frac{2m^{m+2k_1-1}\rho_2^{k_1}}{k_1!\Gamma\left(m+k_1\right)(\Omega_1\Omega_2)^{m/2+k_1-1/2}(1-\rho_2)^{m+2k_1}}, \\
& b_{k_1}\triangleq\frac{\rho_2^{k_1}(1-\rho_2)^m(\Omega_1\Omega_2)^{m/2+1/2}}{2k_1!\Gamma\left(m+k_1\right)m^{m+1}}, \\
& c_{k_1,k_2}\triangleq\frac{(-1)^{k_2}(1-m)m^{k_1+k_2-1}\Omega_2^{m/2+1/2}\rho_2^{k_1}}{k_1!k_2!\Gamma\left(m+k_1\right)\Omega_1^{m/2+k_1+k_2-1/2}(1-\rho_2)^{k_1+k_2}}, \\
& c_{k_1,k_3}\triangleq\frac{(-1)^{k_3}(1-m)m^{k_1+k_3-1}\Omega_1^{m/2+1/2}\rho_2^{k_1}}{k_1!k_3!\Gamma\left(m+k_1\right)\Omega_2^{m/2+k_1+k_3-1/2}(1-\rho_2)^{k_1+k_3}}, \\
& \Xi\left(\ell_x\right)\triangleq\int_0^{\ell_x}x^{2m+2k_1+2n_1}\frac{I_{m-2}\left\{B\right\}}{I_{m-1}\left\{B\right\}}\mathrm{d}x, \\
& \Xi\left(\ell_x,\ell_y\right)\triangleq\int_0^{\ell_x}\int_0^{\ell_y}x^{2m+2k_1+2n_1}y^{2m+2k_1+2n_2}\frac{I_{m-2}\left\{A\right\}}{I_{m-1}\left\{A\right\}}\mathrm{d}y\mathrm{d}x, \\
& A\triangleq\frac{2m\sqrt{\rho_2}xy}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}, \\
& B\triangleq\frac{2m\sqrt{\rho_2}\ell_y x}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)},
\end{aligned}
\tag{11}
$$

where $\gamma(a,b)=\int_0^b\mathrm{e}^{-t}t^{a-1}\mathrm{d}t$ is the incomplete gamma function; ℓ_x and ℓ_y are the preset integration range according to pdf; Ω_1 and Ω_2 are the average powers of X and Y, respectively. In particular, Eq. (11) is not a closed-form expression, and $\Xi(\ell_x)$ and $\Xi(\ell_x,\ell_y)$ can be calculated by numerical integration or Monte Carlo integration method.

Proof. See Appendix A.

In Sections 4 and 5, two types of simulation models are introduced for integer and non-integer m, respectively, and they will be used to generate the received signal envelope in Section 6.

4 Simulation model for Nakagami-m fading channels with integer m

In this section, the Nakagami-m fading channel simulation model for integer m is described, and the expressions of power correlation coefficients are derived.

According to [25], for integer m, the envelope of Nakagami-m fading can be modeled as

$$R_{i,\mathrm{nak}}(t) = \sqrt{\sum_{k=1}^{m} |Z_k(t)|^2},\ i = a, b, e, \tag{12}$$

where $Z_k(t)$ is the k-th Rayleigh fader, and $Z_k(t)$ and $Z_l(t)$ are uncorrelated for all $k \neq l$.

For this modeling method, according to (127) of [25], the power correlation coefficient ρ_2 in (10) is equal to the correlation coefficient between each correlated pair of $|Z_k(t)|^2$.

In this paper, an improved model for the generation of multiple uncorrelated Rayleigh fading waveforms proposed in [22] is utilized as follows:

$$Z_k(t) = Z_{c,k}(t) + \mathrm{j}Z_{s,k}(t), \tag{13}$$

$$Z_{c,k}(t) = \sqrt{\frac{2}{M}} \sum_{n=1}^{M} \cos\left[\omega_d t \cos\alpha_n + \varphi_{n,k}\right], \tag{14}$$

$$Z_{s,k}(t) = \sqrt{\frac{2}{M}} \sum_{n=1}^{M} \cos\left[\omega_d t \sin\alpha_n + \psi_{n,k}\right], \tag{15}$$

$$\text{s.t. } M = \frac{N}{4}, \quad \alpha_n = \frac{2\pi n - \pi + \theta_k}{4M},$$

where M is the number of sinusoids; N is the number of paths; $\omega_d = 2\pi f_d$ is the maximum angular Doppler shift; θ_k, $\varphi_{n,k}$, and $\psi_{n,k}$ are mutually independent and uniformly distributed on $[-\pi, \pi)$ for all n and k. The meaning of "improved" is that the statistical properties of this model hold for small M values when the statistical properties of most other models cannot match the results as expected.

The marginal pdf of Nakagami-m distribution with $m = 1$, $m = 4$, and $m = 10$ are illustrated in Figure 2(a), which shows that the simulation curves match the theoretical curves.

Let $R_{ZZ}(\tau) = \mathrm{E}(Z_k(t)Z_k(t+\tau))$ and $R_{|Z|^2|Z|^2}(\tau) = \mathrm{E}(|Z_k(t)|^2|Z_k(t+\tau)|^2)$ be the correlation function with τ. The statistical properties of $Z_k(t)$ are as follows [22]:

$$R_{ZZ}(\tau) = 2J_0(2\pi f_d \tau), \tag{16}$$

$$R_{|Z|^2|Z|^2}(\tau) = 4 + 4J_0^2(2\pi f_d \tau) + \frac{2 + J_0(4\pi f_d \tau)}{M}. \tag{17}$$

According to (12) and (16), $\Theta_i = \mathrm{E}[|Z_k(t)|^2] = 2$ with $i = a, b, e$ holds for the considered Rayleigh fading channel model, which are used in this paper.

Furthermore, define $\rho_{2,\mathrm{au}}(\tau)$ and $\rho_{2,\mathrm{cross}}(d/\lambda)$ as the autocorrelation coefficient and cross-correlation coefficient between $|Z_k(t)|^2$ and $|Z_l(t)|^2$ for $k = l$.

Theorem 4. The autocorrelation coefficient between $|Z_k(t)|^2$ and $|Z_l(t)|^2$ for $k = l$ can be expressed as

$$\rho_{2,\mathrm{au}}(\tau) = \frac{4MJ_0^2(2\pi f_d \tau) + J_0(4\pi f_d \tau) + 2}{4M + 3}. \tag{18}$$

Proof. Based on (16) and (17),

$$\rho_{2,\mathrm{au}}(\tau) = \frac{\mathrm{E}[Z_k^2(t)Z_k^2(t+\tau)] - \mathrm{E}[Z_k^2(t)]\mathrm{E}[Z_k^2(t+\tau)]}{\sqrt{\mathrm{Var}[Z_k^2(t)]\mathrm{Var}[Z_k^2(t+\tau)]}}, \tag{19}$$

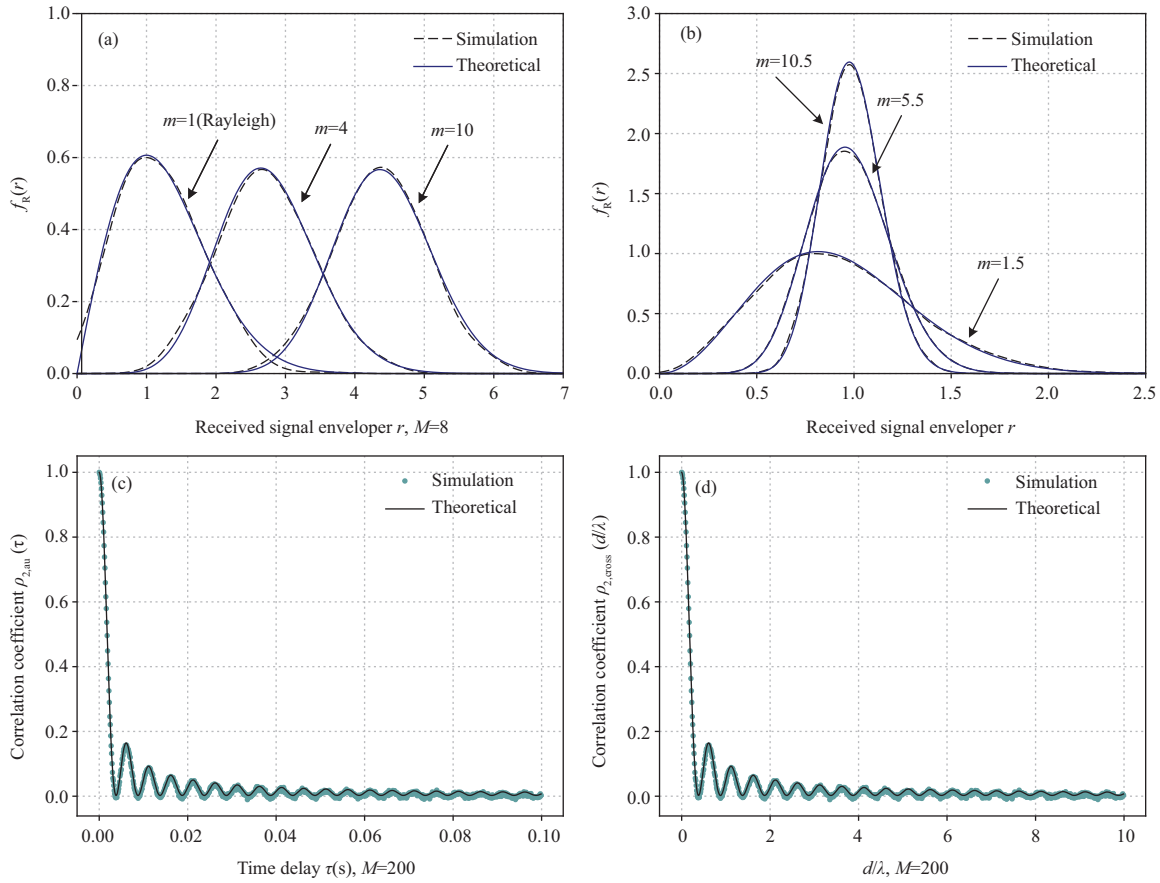

Figure 2 (Color online) The pdf and power correlation coefficients of Nakagami-m distribution with $f_d = 100$ Hz. (a) The pdfs for $m = 1$, $m = 4$, and $m = 10$ with $M = 8$; (b) the pdfs for $m = 1.5$, $m = 5.5$, and $m = 10.5$ with $M = 200$; (c) simulation of $\rho_{2,\mathrm{au}}(\tau)$ for $m = 1$ and $M = 200$; (d) simulation of $\rho_{2,\mathrm{cross}}(\tau)$ for $m = 1$ and $M = 200$.

with

$$\mathrm{E}[Z_k^2(t)Z_k^2(t+\tau)] = 4 + 4J_0^2(2\pi f_d\tau) + \frac{2 + J_0(4\pi f_d\tau)}{M}, \tag{20}$$

$$\mathrm{E}[Z_k^2(t)]\mathrm{E}[Z_k^2(t+\tau)] = R_{ZZ}(0)R_{ZZ}(0) = 4, \tag{21}$$

and

$$\mathrm{Var}[Z_k^2(t)] = \mathrm{E}[|Z_k^2(t) - 2|^2] = \mathrm{E}[Z_k^4(t)] - 4 = R_{|Z|^2|Z|^2}(0) - 4 = \frac{4M+3}{M}. \tag{22}$$

Substituting (20)–(22) into (19),

$$\rho_{2,\mathrm{au}}(\tau) = \frac{4MJ_0^2(2\pi f_d\tau) + J_0(4\pi f_d\tau) + 2}{4M+3}.$$

The proof of Theorem 4 has been completed.

Theorem 5. The cross-correlation coefficient between $|Z_k(t)|^2$ and $|Z_l(t)|^2$ for $k = l$ can be expressed as follows:

$$\rho_{2,\mathrm{cross}}(d/\lambda) = \frac{4MJ_0^2(2\pi d/\lambda) + J_0(4\pi d/\lambda) + 2}{4M+3}. \tag{23}$$

Proof. The cross-correlation coefficient can be obtained based on (18) by setting $f_d\tau = d/\lambda$, where λ denotes the wavelength.

Remark 3. According to [22], the correlation functions of the squared Rayleigh random variable modeled by (13) have good approximation when M is not less than 8 and are close to the theoretical values when M approaches infinity. In particular, for (18) and (23), $\lim_{M\to\infty}\rho_{2,\mathrm{au}}(\tau) = J_0^2(2\pi f_d\tau)$ and

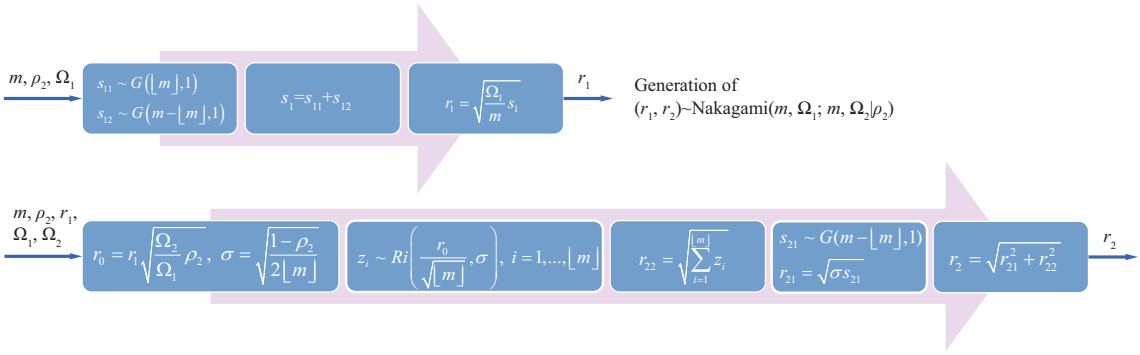

Figure 3 (Color online) Block diagram of generating two correlated Nakagami-m variables with non-integer m for $m > 1$ values.

$\lim_{M\to\infty} \rho_{2,\text{cross}}(d/\lambda) = J_0^2(2\pi d/\lambda)$ hold. Figures 2(c) and (d) show that the simulation curves of $\rho_{2,\text{au}}(\tau)$ and $\rho_{2,\text{cross}}(d/\lambda)$ match the theoretical curves with $M = 200$. For convenience, $\rho_{2,\text{au}}(\tau)$ is replaced by $\rho_{2,\text{au}}$, and $\rho_{2,\text{cross}}(d/\lambda)$ is replaced by $\rho_{2,\text{cross}}$ in the rest of this paper.

5 Simulation model for Nakagami-m fading channels with non-integer m

In this section, the Nakagami-m fading channel simulation model with non-integer m is introduced, and the main stages are shown in Figure 3.

First of all, to generate the bivariate Nakagami-m envelopes $(r_1, r_2) \sim \text{Nakagami}(m, \Omega_1; m, \Omega_2|\rho_2)$, some useful pdfs are defined as follows.

• Define $Ri(\zeta, \sigma)$ as the Rician distribution whose pdf is given by

$$f(x) = \frac{x}{\sigma^2} \mathrm{e}^{-\left(\frac{x^2+\zeta^2}{2\sigma^2}\right)} I_0\left(\frac{\zeta x}{\sigma^2}\right), \quad x \geqslant 0. \tag{24}$$

• Define $Ri(m, r_0, \sigma)$ as the generalized Rician distribution whose pdf is given by [25]

$$\begin{aligned} f(r_2/r_1) &= \frac{r_2^m}{\sigma^2 r_0^{m-1}} \mathrm{e}^{-\left(\frac{r_2^2+r_0^2}{2\sigma^2}\right)} I_{m-1}\left(\frac{r_2 r_0}{\sigma^2}\right), \\ \text{s.t.} \quad \sigma &= \sqrt{\frac{1-\rho_2}{2m}}, \ r_0 = r_1\sqrt{\frac{\Omega_2}{\Omega_1}\rho_2}. \end{aligned} \tag{25}$$

• Define $G(\alpha, \beta)$ as the gamma distribution, and the corresponding pdf is

$$f(x) = \frac{1}{\Gamma(\alpha)\beta^\alpha} x^{\alpha-1} \mathrm{e}^{-\frac{x}{\beta}}, \quad x \geqslant 0. \tag{26}$$

As shown in Figure 3, the bivariate Nakagami-m fading envelopes with non-integer m can be generated using Gamma and Rician variables. The main stages are as follows [23].

• Generate $s_1 \sim G(m, 1)$ and $r_1 \sim \text{Nakagami}(m, \Omega_1)$. For $m < 1$ values, s_1 can be expressed as a product of beta and complex Gaussian processes [29]. For $m > 1$ values, given m, ρ_2, and Ω_1, the Nakagami-m variable r_1 can be generated by Gamma variables s_{11} and s_{12}, which are integer part ($\lfloor m \rfloor$) and decimal part ($m - \lfloor m \rfloor$) of m.

• Generate $r_2 \sim Ri(m, r_0, \sigma)$, where $\sigma = \sqrt{\frac{1-\rho_2}{2\lfloor m \rfloor}}$ and $r_0 = \sqrt{\frac{\Omega_2}{\Omega_1}\rho_2}$. In particular, variable r_2 can be generated as $r_2 = \sqrt{r_{21}^2 + r_{22}^2}$, where r_{22} is the integer part of m and generated by $\lfloor m \rfloor$ Rician variables, and r_{21} denotes the decimal part of m and generated by Gamma variables. See [23] for the details of bivariate Nakagami-m fading envelopes generation and Figure 2(b) shows the simulation of the pdfs with $m = 1.5$, $m = 5.5$, and $m = 10.5$.

Remark 4. The simulation method in Figure 3 also applies to integer m ($m = \lfloor m \rfloor$) by setting $s_{12} = 0$ and $r_{21} = 0$ during the process of generation of s_1 and r_2, respectively. The reason we built different models for integer and non-integer m in this paper is that the method in Section 4 can obtain the expression of ρ_2, which is a function of τ, M, f_d, l_s, and d/λ, while the method in Figure 3 cannot achieve this goal. It is obvious that τ, M, f_d, l_s, and d/λ are the important factors during the design of the practical secret key generation protocols.

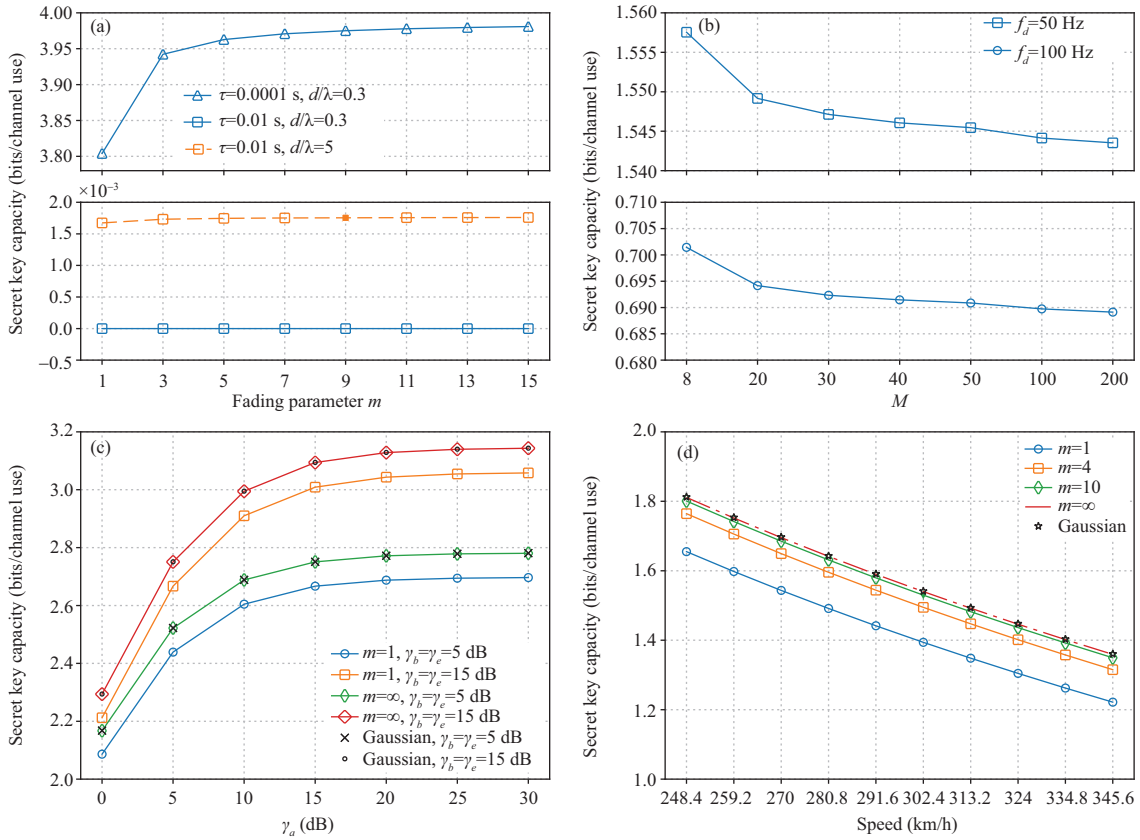

Figure 4 (Color online) The simulations for integer m. (a) The secret key capacity change versus m-fading parameter, $\gamma = 10$ dB; (b) the secret key capacity change versus M, $\tau = 0.001$ s, $m = 1$, $\gamma = 10$ dB; (c) the secret key capacity change versus different SNR at Alice and Bob, $\tau = 0.0001$ s, $d/\lambda = 0.1$; (d) the secret key capacity change versus the speed of high-speed railway, $\tau = 0.0001$ s, $d/\lambda = 0.3$, $\gamma = 10$ dB.

6 Numerical results and discussion

In this section, numerical results are provided to evaluate the effects of parameters on secret key capacity over correlated Nakagami-m fading channels.

The expression of secret key capacity is defined in (8) and can be calculated using (11). It is assumed that $m_a = m_b = m_e = m$, $\Theta_a = \Theta_b = \Theta_e = 2$ for integer m, $\Omega_a = \Omega_b = \Omega_e = 1$ for non-integer m, and $l_s = 100$ hold for simulations. The power correlation coefficient ρ_2 is determined by (18) to calculate $I(\hat{R}_a; \hat{R}_b)$ and determined by (23) to calculate $I(\hat{R}_a; \hat{R}_e)$. Unless otherwise specified, $\gamma_a = \gamma_b = \gamma_e = \gamma$, $\sigma^2_{n_a} = \sigma^2_{n_b} = \sigma^2_{n_e} = \sigma^2$, $f_d = 100$ Hz, and $M = 200$ are used in all simulations, where $f_d = 100$ Hz is the typical Doppler spread in vehicular communications [17], and $M = 200$ is to ensure the accuracy of ρ_2. Take into consideration that the effects of τ, f_d and l_s on secret key capacity over correlated Rayleigh fading model are already evaluated in [19], which also apply to the considered model of this paper, we will provide some different results in the rest of this section. To verify the correctness of the analysis results, we perform $L = 10^5$ received signal envelopes to directly calculate the secret key capacity in (8) using MATLAB information theoretical estimator (ITE) toolbox [30]. The Nakagami-m fading envelopes for integer and non-integer m are generated using the methods in Sections 4 and 5, respectively.

The secret key capacity measured by mutual information is a function of the m-fading parameter. Figure 4(a) plots the secret key capacity change versus m. The m-fading parameter under study is from 1 to 15, which is the typical range in practical wireless applications [31]. It is observed that the secret key capacity increases as m increases. This is because an increase on m reduces the severity of fading. Then, the growth rate of the secret key capacity decreases with the increase of m. It can be also seen that the secret key capacity between Rician fading envelopes ($m > 1$) is larger than that for Rayleigh fading envelopes ($m = 1$). In addition, to obtain a positive secret key rate, $\rho_{2,\text{au}} > \rho_{2,\text{cross}}$ is required, which means $d/\lambda > f_d\tau$ is needed. For $\tau = 0.0001$ s ($\rho_{2,\text{au}} \approx 0.9980$), the values of secret key capacity are all positive with $d/\lambda = 0.3$ ($\rho_{2,\text{cross}} \approx 0.0861$) and $d/\lambda = 5$ ($\rho_{2,\text{cross}} \approx 0.0126$) due to $d/\lambda > f_d\tau = 0.01$

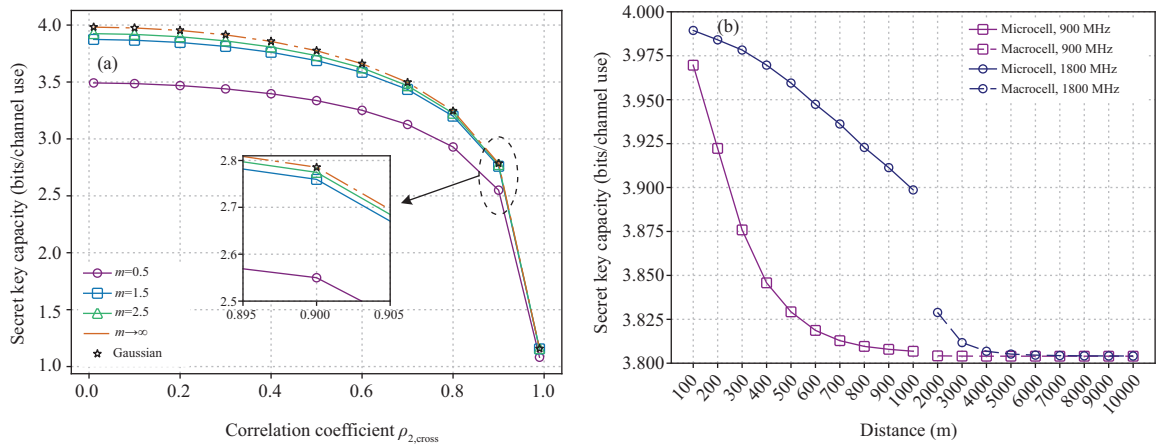

Figure 5 (Color online) The simulations for non-integer m. $\gamma = 10$ dB. (a) The secret key capacity change versus $\rho_{2,\text{cross}}$, $\tau = 0.0001$ s; (b) the secret key capacity change versus distance for Microcell and Macrocell, $\rho_{2,\text{au}} = 0.9980$, $\rho_{2,\text{cross}} = 0.008$.

holds for all m. However, the secret key capacity is positive when $\tau = 0.01$ s ($\rho_2 \approx 0.0510$) with $d/\lambda = 5$, while the secret key capacity is equal to zero when $d/\lambda = 0.3$ because $d/\lambda < f_d\tau = 1$.

According to (18) and (23), the power correlation coefficient ρ_2 is a function of the number of sinusoids M. Figure 4(b) shows that the secret key capacity reduces with the increase of M due to that the correlation between randomness sources decreases as M increases. Furthermore, the rate of reduction slows down as M grows. These results also apply to the number of paths N when $N = 4M$.

In Figure 4(c), the influence of different average SNR at Alice and Bob on the secret key capacity is studied. Assume that $\gamma_b = \gamma_e$, the results indicate that the secret key capacity increases as γ_a increases for fixed γ_b and γ_e. As γ_a grows large, the secret key capacity tends to be saturated. The main cause of this result is the secret key capacity is limited by the fixed γ_b and γ_e. On the other hand, for the same γ_a, the secret key capacity increases with the increase of γ_b and γ_e, which yields the lower channel estimation error and the higher correlation coefficient. In particular, the Nakagami-m distribution approximates Gaussian distribution when $m \to \infty$, and the expression of mutual information (in bits) for Gaussian variables has been derived, i.e., $I_{\text{gaussian}} = -\frac{1}{2}\log_2(1-\rho^2)$, where ρ is the correlation coefficient between Gaussian variables [32]. According to (139) of [25], the relationship $\rho \approx \rho_2$ holds for Gaussian variables. Figure 4(c) also shows the curves with $m \to \infty$ match that of Gaussian variables perfectly.

The high-speed mobile wireless channels can be modeled as the Nakagami-m fading model. For vehicle communications, the maximum Doppler shift can be viewed as a function of the relative velocity between users, i.e., $f_d = \frac{\Delta v}{\lambda} = \frac{\Delta v f_0}{\text{c}}$, where Δv is the relative velocity, c is the light speed (3×10^8 m/s), and f_0 is the communication frequency [33]. Then, the coherence time can be computed as $T_c \approx \frac{0.423}{f_d}$ [33]. Figure 4(d) plots the secret key capacity change versus the speed of the high-speed railway. It can be observed that the secret key capacity decreases as the speed increases due to that T_c decreases with the speed grows, which means that fewer bits can be extracted from each sample. Furthermore, the performance with $m \to \infty$ is also performed in Figure 4(d). It also can be seen that when the value of m becomes larger, the impact on the secret key capacity becomes smaller. This result is consistent with the overall trend of the curves in Figure 4(a).

For non-integer m, Figure 5(a) plots the secret key capacity change versus $\rho_{2,\text{cross}}$ with $m = 0.5$, $m = 1.5$, $m = 2.5$, and $m \to \infty$, which show that the secret key capacity reduces as $\rho_{2,\text{cross}}$ grows. As in Figure 5(a), the curve of the secret key capacity for Nakagami-m variables with $m \to \infty$ matches that of Gaussian variables perfectly. It also can be seen that as $\rho_{2,\text{cross}}$ grows, the decrease rate of the secret key capacity becomes larger.

In the realistic environment, the transceiver antenna heights, and the distance between the mobile station and the scatterers affect the value of m [34]. The simulation parameters and the estimated m-parameters are listed in Tables 1 and 2, respectively. Figure 5(b) provides a comparison on the secret key capacity versus distance for Micro and Macrocells at 900 MHz ($\lambda \approx 0.33$ m) and 1800 MHz ($\lambda \approx 0.17$ m). It is found that the higher the frequency, the larger the secret key capacity. Furthermore, for the 900 MHz system, the decay rate decreases for smaller distances (Microcell) and remains nearly constant for longer distances (Macrocell). Unlike the 900 MHz system, the decay rate for Microcell at 1800 MHz is basically

Table 1 Simulation parameters

Parameter	Value
Distribution of reflection co-efficient	Uniform
Carrier frequency	900 and 1800 MHz
Path loss exponent	2
Additional path loss exponent	4
Tranmitter antenna height	50 m
Receiver antenna height	3 m
Average distance between mobile station and scatterers	12 m

Table 2 Nakagami-m parameters

Distance (m)	Microcell=900 MHz m (dB)	Microcell=1800 MHz m (dB)	Distance (m)	Microcell=900 MHz m (dB)	Microcell=1800 MHz m (dB)
100	8.19	19.76	2000	3.57E−03	4.73E−01
200	3.47	13.80	3000	6.99E−04	1.39E−01
300	1.63	10.59	4000	2.51E−04	4.95E−02
400	0.84	8.20	5000	9.43E−05	2.13E−02
500	0.48	6.53	6000	4.60E−05	1.08E−02
600	0.27	5.21	7000	2.54E−05	6.00E−03
700	0.16	4.32	8000	1.47E−05	3.48E−03
800	0.10	3.50	9000	9.05E−06	2.24E−03
900	0.07	2.93	10000	6.01E−06	1.46E−03
1000	0.05	2.40			

unchanged. Then, it is almost keeping the same for 900 and 1800 MHz systems when the distance is longer than 6000 m. These behaviors of secret key capacity are similar to the variations of the Nakagami-m parameter. Moreover, there are many other scenarios in [34] with the different height settings or the distribution of reflection co-efficient. For more information, please refer to Section 4 of [34].

7 Conclusion

This paper characterized the secret key capacity over correlated Nakagami-m fading channel, in the presence of a passive eavesdropper. The expression of secret key capacity applies to both integer and non-integer m and is determined by the m-fading parameter, the average power, and the power correlation coefficients. The numerical results can provide theoretical guidance on the practical secret key generation protocol design. The model in this paper considered identical Nakagami-m parameter, while it might be different in a realistic environment. For future work, it is interesting to analyze the performance of secret key capacity for non-identical m-fading parameters using the joint pdf of Nakagami-m distribution derived in [35] to calculate the mutual information.

Acknowledgements This work was supported in part by National Key R&D Program of China (Grant No. 2019YFE0114000), in part by National Natural Science Foundation of China (Grant Nos. 61932005, 62071066), in part by Shenzhen Science and Technology Innovation Commission Free Exploring Basic Research Project (Grant Nos. 2021Szvup008, JCYJ20170307172830043), in part by National High-tech R&D Program of China (Grant No. 2014AA01A701), in part by 111 Project of China (Grant No. B16006), and in part by Fundamental Research Funds for the Central Universities (Grant No. 2020RC39).

References

1 Khan R, Kumar P, Jayakody D N K, et al. A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. IEEE Commun Surv Tut, 2020, 22: 196–248
2 Cao J, Ma M D, Li H, et al. A survey on security aspects for 3GPP 5G networks. IEEE Commun Surv Tut, 2020, 22: 170–195
3 Wang N, Wang P, Alipour-Fanid A, et al. Physical-layer security of 5G wireless networks for IoT: challenges and opportunities. IEEE Internet Things J, 2019, 6: 8169–8181
4 Li N, Xia S D, Tao X F, et al. An area based physical layer authentication framework to detect spoofing attacks. Sci China Inf Sci, 2020, 63: 222302
5 Chen H, Tao X F, Li N, et al. A data analysis of political polarization using random matrix theory. Sci China Inf Sci, 2020, 63: 129303
6 Zhong B, Zhang Z S. Secure full-duplex two-way relaying networks with optimal relay selection. IEEE Commun Lett, 2017, 21: 1123–1126
7 Zhong B, Chen L, Tang Z J. Ergodic rate analysis for full-duplex NOMA networks with energy harvesting. Sci China Inf Sci, 2021, 64: 189303

8 Jiao L, Wang N, Wang P, et al. Physical layer key generation in 5G wireless networks. IEEE Wirel Commun, 2019, 26: 48–54
9 Qin D R, Ding Z. Exploiting multi-antenna non-reciprocal channels for shared secret key generation. IEEE Trans Inform Forensic Secur, 2016, 11: 2693–2705
10 Xu P, Cumanan K, Ding Z G, et al. Group secret key generation in wireless networks: algorithms and rate optimization. IEEE Trans Inform Forensic Secur, 2016, 11: 1831–1846
11 Gong S X, Tao X F, Li N, et al. Secure secret key and private key generation in source-type model with a trusted helper. IEEE Access, 2020, 8: 34611–34628
12 Tavangaran N, Boche H, Schaefer R. Secret-key generation using compound sources and one-way public communication. IEEE Trans Inform Forensic Secur, 2017, 12: 227–241
13 Tavangaran N, Schaefer R F, Poor H V, et al. Secret-key generation and convexity of the rate region using infinite compound sources. IEEE Trans Inform Forensic Secur, 2018, 13: 2075–2086
14 Lai L F, Liang Y B, Du W L. Cooperative key generation in wireless networks. IEEE J Sel Areas Commun, 2012, 30: 1578–1588
15 Zeng K. Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun Mag, 2015, 53: 33–39
16 Aldaghri N, Mahdavifar H. Physical layer secret key generation in static environments. IEEE Trans Inform Forensic Secur, 2020, 15: 2692–2705
17 Pierrot A J, Chou R A, Bloch M R. The effect of eavesdropper's statistics in experimental wireless secret-key generation. 2013. ArXiv:1312.3304
18 Chou T H, Draper S C, Sayeed A M. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In: Proceedings of IEEE International Symposium on Information Theory, Austin, 2010. 2518–2522
19 Zhang J Q, He B, Duong T Q, et al. On the key generation from correlated wireless channels. IEEE Commun Lett, 2017, 21: 961–964
20 Jin H L, Huang K Z, Xiao S F, et al. A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel. IEEE Access, 2019, 7: 26480–26487
21 Lai L F, Liang Y B, Poor H V. A unified framework for key agreement over wireless fading channels. IEEE Trans Inform Forensic Secur, 2012, 7: 480–490
22 Zheng Y R, Xiao C S. Improved models for the generation of multiple uncorrelated Rayleigh fading waveforms. IEEE Commun Lett, 2002, 6: 256–258
23 Reig J, Martinez-Amoraga M A, Rubio L. Generation of bivariate Nakagami-m fading envelopes with arbitrary not necessary identical fading parameters. Wirel Commun Mob Comput, 2007, 7: 531–537
24 Wal J W, Sharma R K. Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis. IEEE Trans Inform Forensic Secur, 2010, 5: 381–392
25 Nakagami M. The m-distribution — a general formula of intensity distribution of rapid fading. In: Statistical Methods in Radio Wave Propagation. Elmsford: Pergamon Press, 1960
26 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products. 6th ed. Orlando: Academic Press, 2000
27 Bloch M, Barros J. Physical-Layer Security: from Information Theory to Security Engineering. Cambridge: Cambridge University Press, 2011
28 Gamal A E, Kim Y H. Network Information Theory. Cambridge: Cambridge University Press, 2011
29 Yip K W, Ng T S. A simulation model for Nakagami-m fading channels, $m < 1$. IEEE Trans Commun, 2000, 48: 214–221
30 Szabo Z. Information theoretical estimators toolbox. J Mach Learn Res, 2014, 15: 283–287
31 Braun W R, Dersch U. A physical mobile radio channel model. IEEE Trans Veh Technol, 1991, 40: 472–482
32 Cover T M, Thomas J A. Elements of Information Theory. 2nd ed. Hoboken: Wiley, 2006
33 Ribouh S, Malawade A V, Elhillali Y, et al. Channel state information-based cryptographic key generation for intelligent transportation systems. IEEE Trans Int Trans Syst, 2021, 22: 7496–7507
34 Azam M I. Impact of variability of Nakagami-m parameter on the performance of digital communication systems. 2006. http://eprints.kfupm.edu.sa/9763/1/9763.pdf
35 Reig J, Rubio L, Cardona N. Bivariate Nakagami-m distribution with arbitrary fading parameters. Electron Lett, 2002, 38: 1715–1717

Appendix A Proof of Theorem 3

For the convenience of understanding, let $x \triangleq r_i$ and $y \triangleq r_j$ for the rest of the Appendix. Through transforming the bottom of the logarithm, the double integral in (9) can be calculated as

$$\iint_{x,y} f(x,y)\log_2\frac{f(x,y)}{f(x)f(y)}\mathrm{d}x\mathrm{d}y = \frac{1}{\ln 2}\underbrace{\iint_{x,y} f(x,y)\ln\frac{f(x,y)}{f(x)f(y)}\mathrm{d}x\mathrm{d}y}_{I_1}. \tag{A1}$$

By using the series representation $I_v(z) = \sum_{k=0}^{\infty}\frac{1}{k!\Gamma(v+k+1)}\left(\frac{z}{2}\right)^{v+2k}$ [26], I_1 can be computed as

$$\begin{aligned} I_1 &= \frac{4m^{m+1}}{\Gamma(m)(1-\rho_2)\rho_2^{(m-1)/2}(\Omega_1\Omega_2)^{(m+1)/2}}\iint_{x,y} x^m y^m \mathrm{e}^{-\frac{m\Omega_2 x^2+m\Omega_1 y^2}{\Omega_1\Omega_2(1-\rho_2)}} I_{m-1}\left\{\frac{2m\sqrt{\rho_2}xy}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}\right\} \\ &\quad\times\ln\frac{\Gamma(m)\Omega_1^{(m-1)/2}\Omega_2^{(m-1)/2}}{(1-\rho_2)\rho_2^{(m-1)/2}m^{m-1}}x^{1-m}y^{1-m}\mathrm{e}^{-\frac{m\Omega_2\rho_2 x^2+m\Omega_1\rho_2 y^2}{\Omega_1\Omega_2(1-\rho_2)}} I_{m-1}\left\{\frac{2m\sqrt{\rho_2}xy}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}\right\}\mathrm{d}x\mathrm{d}y \\ &= \frac{4m^{m+1}}{\Gamma(m)(1-\rho_2)\rho_2^{(m-1)/2}(\Omega_1\Omega_2)^{(m+1)/2}} \end{aligned}$$

$$\times\left\{\begin{array}{l}\ln\dfrac{\Gamma(m)\Omega_1^{(m-1)/2}\Omega_2^{(m-1)/2}}{(1-\rho_2)\rho_2^{(m-1)/2}m^{m-1}}\displaystyle\sum_{k_1=0}^{\infty}a_{k_1}\underbrace{\iint_{x,y}x^{2m+2k_1-1}y^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\mathrm{d}x\mathrm{d}y}_{I_2}\\ +\displaystyle\sum_{k_1=0}^{\infty}a_{k_1}\underbrace{\iint_{x,y}x^{2m+2k_1-1}y^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\ln x^{1-m}y^{1-m}\mathrm{e}^{-\frac{m\Omega_2\rho_2x^2+m\Omega_1\rho_2y^2}{\Omega_1\Omega_2(1-\rho_2)}}\mathrm{d}x\mathrm{d}y}_{I_3}\\ +\displaystyle\sum_{k_1=0}^{\infty}a_{k_1}\underbrace{\iint_{x,y}x^{2m+2k_1-1}y^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\ln I_{m-1}\left\{\dfrac{2m\sqrt{\rho_2}xy}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}\right\}\mathrm{d}x\mathrm{d}y}_{I_4}\end{array}\right\},\tag{A2}$$

where a_{k_1} is defined as

$$a_{k_1}\triangleq\frac{2m^{m+2k_1-1}\rho_2^{k_1}}{k_1!\Gamma(m+k_1)(\Omega_1\Omega_2)^{m/2+k_1-1/2}(1-\rho_2)^{m+2k_1}}.$$

Define the integral areas of x and y are $[0,\ell_x]$ and $[0,\ell_y]$, respectively, I_2 in (A2) can be computed as

$$\begin{aligned}I_2=&\int_0^{\ell_x}x^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{d}x\int_0^{\ell_y}y^{2m+2k_1-1}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\mathrm{d}y\\ =&\frac{\Omega_1^{m+k_1}\Omega_2^{m+k_1}(1-\rho_2)^{2m+2k_1}}{4m^{2m+2k_1}}\gamma\left(m+k_1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\gamma\left(m+k_1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right),\end{aligned}\tag{A3}$$

where (3.381.8) of [26] is used and $\gamma(a,b)=\int_0^b\mathrm{e}^{-t}t^{a-1}\mathrm{d}t$ is the incomplete gamma function.

Based on (2.723.1) of [26], the following integral representation is derived and used later,

$$\int_0^u x^a\mathrm{e}^{-bx^n}\ln x\mathrm{d}x=\sum_{k=0}^{\infty}\frac{(-b)^k}{k!}\left[\frac{u^{nk+a+1}\ln u}{nk+a+1}-\frac{u^{nk+a+1}}{(nk+a+1)^2}\right],\ \text{for}\ a\geqslant 0,\ b>0,\ n>0.\tag{A4}$$

Then, I_3 can be calculated as

$$\begin{aligned}I_3=&(1-m)\int_0^{\ell_x}x^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\ln x\mathrm{d}x\int_0^{\ell_y}y^{2m+2k_1-1}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\mathrm{d}y\\ &+(1-m)\int_0^{\ell_x}x^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{d}x\int_0^{\ell_y}y^{2m+2k_1-1}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\ln y\mathrm{d}y\\ &-\frac{m\rho_2}{\Omega_1(1-\rho_2)}\int_0^{\ell_x}x^{2m+2k_1+1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{d}x\int_0^{\ell_y}y^{2m+2k_1-1}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\mathrm{d}y\\ &-\frac{m\rho_2}{\Omega_2(1-\rho_2)}\int_0^{\ell_x}x^{2m+2k_1-1}\mathrm{e}^{-\frac{mx^2}{\Omega_1(1-\rho_2)}}\mathrm{d}x\int_0^{\ell_y}y^{2m+2k_1+1}\mathrm{e}^{-\frac{my^2}{\Omega_2(1-\rho_2)}}\mathrm{d}y\\ =&\sum_{k_2=0}^{\infty}\frac{(-1)^{k_2}(1-m)\Omega_2^{m+k_1}(1-\rho_2)^{m+k_1-k_2}}{2m^{m+k_1-k_2}k_2!\Omega_1^{k_2}}\left[\frac{\ell_x^{2m+2k_1+2k_2}\ln\ell_x}{2m+2k_1+2k_2}-\frac{\ell_x^{2m+2k_1+2k_2}}{(2m+2k_1+2k_2)^2}\right]\gamma\left(m+k_1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right)\\ &+\sum_{k_3=0}^{\infty}\frac{(-1)^{k_3}(1-m)\Omega_1^{m+k_1}(1-\rho_2)^{m+k_1-k_3}}{2m^{m+k_1-k_3}k_3!\Omega_2^{k_3}}\left[\frac{\ell_y^{2m+2k_1+2k_3}\ln\ell_y}{2m+2k_1+2k_3}-\frac{\ell_y^{2m+2k_1+2k_3}}{(2m+2k_1+2k_3)^2}\right]\gamma\left(m+k_1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\\ &-\frac{(\Omega_1\Omega_2)^{m+k_1}(1-\rho_2)^{2m+2k_1}\rho_2}{4m^{2m+2k_1}}\gamma\left(m+k_1+1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\gamma\left(m+k_1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right)\\ &-\frac{(\Omega_1\Omega_2)^{m+k_1}(1-\rho_2)^{2m+2k_1}\rho_2}{4m^{2m+2k_1}}\gamma\left(m+k_1,\frac{m\ell_x^2}{\Omega_1(1-\rho_2)}\right)\gamma\left(m+k_1+1,\frac{m\ell_y^2}{\Omega_2(1-\rho_2)}\right).\end{aligned}\tag{A5}$$

Finally, I_4 can be computed as

$$\begin{aligned}I_4=&\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\frac{(-1)^{n_1+n_2}m^{n_1+n_2}}{n_1!n_2!\Omega_1^{n_1}\Omega_2^{n_2}(1-\rho_2)^{n_1+n_2}}\left[\frac{\ell_x^{2m+2k_1+2n_1}\ell_y^{2m+2k_1+2n_2}}{4(m+k_1+n_1)(m+k_1+n_2)}\ln I_{m-1}\left\{\frac{2m\sqrt{\rho_2}\ell_x\ell_y}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}\right\}\right.\\ &-\frac{2m\sqrt{\rho_2}\ell_y^{2m+2k_1+2n_2+1}\Xi(\ell_x)}{4\sqrt{\Omega_1\Omega_2}(1-\rho_2)(m+k_1+n_1)(m+k_1+n_2)}+\frac{(m-1)\ell_x^{2m+2k_1+2n_1}\ell_y^{2m+2k_1+2n_2}}{8(m+k_1+n_1)^2(m+k_1+n_2)}\\ &\left.-\frac{2m\sqrt{\rho_2}\Xi(\ell_x,\ell_y)}{2\sqrt{\Omega_1\Omega_2}(1-\rho_2)(m+k_1+n_2)}+\frac{(m-1)\ell_x^{2m+2k_1+2n_1}\ell_y^{2m+2k_1+2n_2}}{8(m+k_1+n_1)(m+k_1+n_2)^2}\right],\end{aligned}\tag{A6}$$

$$\begin{aligned}\text{s.t.}\quad&\Xi(\ell_x)\triangleq\int_0^{\ell_x}x^{2m+2k_1+2n_1}\frac{I_{m-2}\{B\}}{I_{m-1}\{B\}}\mathrm{d}x,\\ &\Xi(\ell_x,\ell_y)\triangleq\int_0^{\ell_x}\int_0^{\ell_y}x^{2m+2k_1+2n_1}y^{2m+2k_1+2n_2}\frac{I_{m-2}\{A\}}{I_{m-1}\{A\}}\mathrm{d}y\mathrm{d}x,\\ &A\triangleq\frac{2m\sqrt{\rho_2}xy}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)},\ B\triangleq\frac{2m\sqrt{\rho_2}\ell_yx}{\sqrt{\Omega_1\Omega_2}(1-\rho_2)}.\end{aligned}$$

The proof of Theorem 3 has been completed.