Average Secrecy Capacity Analysis of NOMA System with Multiple Eavesdroppers Under Hardware Impairments

HE Ansu[1], *YU Xiangbin*[1,2*], *ZHOU Yue*[1]

1. College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, P. R. China;
2. Key Laboratory of Wireless Sensor Network and Communication, Chinese Academy of Sciences, Shanghai 200050, P. R. China

(Received 23 October 2023; revised 16 March 2024; accepted 20 March 2024)

Abstract: This paper studies the physical layer security performance of non-orthogonal-multiple-access (NOMA) communication system. When the base station incorporates the down-link NOMA scheme to send information, due to the openness of the channel, the information is easy to be eavesdropped, and when there are multiple randomly distributed eavesdroppers, the security performance will be further reduced. In order to enhance physical layer security performance of the system with hardware impairments, we take the method named Protected Zone into account. Based on the characteristics of the direct link between ground users and base station, we apply the Rician fading to model small-scale fading. We also assume the locations of multiple eavesdroppers follow homogeneous Poisson point process (HPPP). The closed-form expressions of average secrecy capacity are derived with the help of Gaussian-Chebyshev quadrature, and the asymptotic expressions are also provided for obtaining the insight under high signal-to-noise-ratio cases. The simulation results verify the effectiveness of the protected zone method for enhancing the security performance, and also illustrate the impact of different parameters on the secrecy performance of the system.

Key words: average secrecy capacity; non-orthogonal-multiple-access (NOMA); hardware impairments; Rician fading; physical layer security

CLC number: TN929.5 **Document code:** A **Article ID:** 1005-1120(2024)02-0244-09

0 Introduction

With the advancement of wireless communication technology, a large number of communication devices have been employed, resulting in increasingly scarce frequency resources[1]. As a novel multiple access technology, the non-orthogonal-multiple-access (NOMA) can improved spectral efficiency by increasing the complexity of digital signal processing technology, and has been widely studied in next-generation communication systems[2-3]. However, owing to the broadcast nature of wireless communication, the security of NOMA communication systems is also confronted with grave threats[4].

There have been many studies on the physical layer security (PLS) of wireless NOMA communication systems. The "Protected Zone" concept was introduced to enhance the security performance of the system by excluding malicious recipients from specific areas[1]. Another technology to improve the PLS performance is the use of friendly jammers[5]. Ref.[6] took hardware impairments into account to investigate the PLS performance of the system with single legitimate user. Ref.[7] studied the security performance of NOMA systems based on full duplex relay in the Internet of Things (IoTs) under instantaneous channel state information (CSI) and an analytical expression for average secrecy capacity

*Corresponding author, E-mail address: yxbxwy@nuaa.edu.cn.

How to cite this article: HE Ansu, YU Xiangbin, ZHOU Yue. Average secrecy capacity analysis of NOMA system with multiple eavesdroppers under hardware impairments[J]. Transactions of Nanjing University of Aeronautics and Astronautics, 2024, 41(2): 244-252.

http://dx.doi.org/10.16356/j.1005-1120.2024.02.009

(ASC) was given. Refs.[8-9] studied the security performance of one eavesdropper and multiple eavesdroppers in the NOMA system, respectively. Ref.[10] firstly addressed the PLS issue of communication systems with multiple antennas at both the sending and receiving ends, and proved that the correct use of space-time diversity at the sending end can enhance information security. Ref.[11] investigated the ergodic secrecy sum rate of a two-ray relay NOMA system under Rayleigh system with single eavesdropper and derived a tight closed-form ergodic secrecy sum rate. Ref.[12] investigated the secrecy outage probability for a full-duplex NOMA system aided by artificial noise, where legitimate users are randomly distributed according to homogeneous Poisson point processes (HPPP) whereas a passive eavesdropper is certainly located. Ref.[13] investigated multiple NOMA users and single eavesdropper with imperfect successive interference cancellation at both legitimate users and eavesdropper and derived the closed-form expressions for secrecy outage probability and effective secrecy throughput.

However, the following problems in the current research on the security performance of wireless NOMA communication systems still exist: In the research on the PLS of communication networks, ideal transceiver hardware is assumed. In practical, hardware impairments cannot be avoided due to IQ imbalance, nonlinear amplification, phase noise, and other effects. When analyzing the PLS performance of NOMA communication systems, it is of practical significance to consider hardware impairments. Secondly, most studies assume that the channel is subject to Rayleigh fading. While it is more reasonable to set the channel as a Rician channel, because the base station is often set above a building, which will increase the direct component of the propagation channel. Most recent literature dealing with a physical layer security characterization of NOMA is focused on single eavesdropper with certain location[11-13]. Hence, its use on multiple randomly distributed eavesdroppers' setup is one of the novel contributions of this paper. The work dealing with this scenario does not research on the ASC and does not considered the transceivers' hardware impairments[4].

The main technical differences and challenges on analyzing the ASC in NOMA system with multiple eavesdroppers under hardware impairments from the existing studies with single certain distributed eavesdropper are the following:

(1) We consider both large-scale fading and Rician fading to model the channels between base station and the receivers, which is more suitable than using Rayleigh fading to model the channels when line-of-sight exists in the real communication.

(2) Most researches on the physical layer security in NOMA system only consider single eavesdropper with certain location, while we consider multiple randomly distributed eavesdroppers existing in NOMA system, which makes the analysis of the system performance more complicated.

The main contributions of this paper can be concluded as follows.

(1) We investigate the PLS performance of wireless NOMA communication networks, where the eavesdroppers obey HPPP and transceivers exist hardware impairments. To enhance security performance, we use the Protected Zone scheme.

(2) We consider both large-scale fading and Rician fading, and derive the cumulative distribution function (CDF) and probability distribution function (PDF) of channel gain with random distribution. Further, we analyze the ASC of system, and derive the exact closed-form expressions of ASC by using Gaussian-Chebyshev quadrature. We also analyze the asymptotic performance of ASC to gain deeper insights of ASC.

(3) Through Monte Carlo simulations, we verify the correctness of the derived analytical expressions and indicate the impact of hardware impairments and power allocation coefficient on the system's PLS performance.

1 System Model

We consider a downlink NOMA communica-

tion system, where the base station sends signals to the near user D_1 and the far user D_2. There are several illegal eavesdroppers E on the ground. As shown in Fig.1, legal users, eavesdroppers and base station are assumed to be on the same horizontal plane, and the base station is set at the origin O. In order to enhance the security of signal transmission, a protected zone approach is adopted, where only legal users are allowed to exist in a circular area P with the origin as the center and a radius r_p, while eavesdroppers can only be outside this area. D_1 follows a uniform distribution in a circular area S_1 with an outer radius R_1, and D_2 follows a uniform distribution in a circular area with an inner radius R_1 and an outer radius R. The number of eavesdroppers follows an exponential distribution with a parameter of λ_e, and the positions of these eavesdroppers follow independent and uniform distributions within a circle (S/P) with an inner radius r_p and an outer radius R.

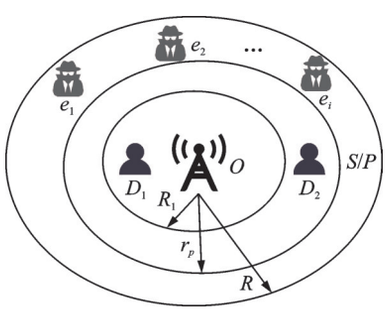

Fig.1 Model diagram of wireless NOMA communication system using Protected Zone

Path loss L_t and small-scale fading h_t are both considered to model the channel between the base station and ground users, where $t\in\{1, 2, e_i\}$, $e_i\in\Phi_e$. The path loss is denoted as

$$L_t = d_t^{-\alpha_t} \tag{1}$$

where α_t denotes the path loss exponent and d_t the distance from O. Here we define $a_1=a_2=a_d$.

We use Rician fading channel to model the small-scale fading. Thus, the channel is denoted as

$$G_t = L_t h_t \tag{2}$$

The CDF of Rician channel gain is

$$F_{|h_t|^2}(x) = 1 - Q_1\left(\sqrt{2K_t}, \sqrt{2\mu_t x}\right) \tag{3}$$

where $\mu_t=(K_t+1)/\Omega_t$, Ω_t denotes the average power gain of h_t, K_t is the Rician factor defined as the ratio of the power of the Los component to the power of the multipath component, and we define $\mu_1=\mu_2=\mu_d$. $Q_1(a, b)$ is the Marcum-Q function[14], here $Q_1(a, b)=\int_b^\infty x\,\mathrm{e}^{-\frac{x^2+a^2}{2}} I_0(ax)\,\mathrm{d}x$ and $I_0(\cdot)$ is the first type of zero-order modified Bessel function.

Due to the difficulty of writing out the closed-form integral expression of Marcum Q-function, the finite series representation for Bessel function can be adopted to express the CDF of $|h_t|^2$[14] as

$$F_{|h_t|^2}(x) = 1 - \mathrm{e}^{-\mu_t x}\sum_{l=0}^{M}\sum_{n=0}^{l} B_t x^n \tag{4}$$

where $B_t=\dfrac{K_t^l \mu_t^n}{\mathrm{e}^{K_t} l!\ n!}$, M is the number of the finite summation terms in the finite series representation for Bessel function[15-16], and l and n are integers between 0 and M. Besides we define $B_1=B_2=B_d$.

The CDF of channel gain considering both random distribution and small-scale fading can be derived as follows

$$F_{|G_t|^2}(x) = Pr\left\{|G_t|^2 < x\right\} = Pr\left\{|h_t|^2 < d_t^{2\alpha_t} x\right\} = \int_{Y_d}^{Y_u} F_{|h_t|^2}(y^{\alpha_t} x)\, f_{d_t^2}(y)\,\mathrm{d}y \tag{5}$$

where $Pr(\cdot)$ denotes the probability, and Y_u and Y_d denote the upper bound and lower bound of the integral of $f_{d_t^2}(y)$, respectively. For D_1, $Y_u=0$, $Y_d=R_1$; for D_2, $Y_u=R_1$, $Y_d=R$. The random distribution of the position between legal users and eavesdroppers are different.

D_1 is uniformly distributed in the disk S_1 around O with the radius R_1. The CDF and PDF of d_1^2 is derived as

$$f_{d_1^2}(x) = \frac{1}{R_1^2} \qquad 0 < x < R_1^2 \tag{6}$$

Substituting Eqs.(4) and (6) into Eq.(5), the CDF of the power gain of channel G_1 can be obtained as

$$F_{|G_1|^2}(x) = 1 - \frac{1}{R_1^2}\sum_{l=0}^{M}\sum_{n=0}^{l} \frac{B_d}{\alpha_d \mu_d^{\,n+\frac{1}{\alpha_d}}} x^{-\frac{1}{\alpha_d}} \gamma\left(n+\frac{1}{\alpha_d}, \mu_d x (R_1^2)^{\alpha_d}\right) \tag{7}$$

where $\gamma(s,x)$ is a lower incomplete Gamma function[17], defined as $\gamma(s,x)=\int_0^x \mathrm{e}^{-t}t^{s-1}\mathrm{d}t(\mathrm{Re}\,s>0)$.

Similar to D_1, D_2 is uniformly distributed in a circular area with an inner radius R_1 and an outer radius R. The PDF of d_2^2 is derived as follows

$$f_{d_2^2}(x)=\frac{1}{R^2-R_1^2} \qquad R_1^2<x<R^2 \tag{8}$$

Substituting Eqs.(4) and (8) into Eq.(5), the CDF of the power gain of channel G_2 can be obtained as

$$F_{|G_2|^2}(x)=1-\frac{1}{R^2-R_1^2}\sum_{l=0}^{M}\sum_{n=0}^{l}\frac{B_d}{\alpha_d\mu_d^{n+\frac{1}{\alpha_d}}}\cdot x^{-\frac{1}{\alpha_d}}\phi\left(n+\frac{1}{\alpha_d},\mu_d x(R^2)^{\alpha_d},\mu_d x(R_1^2)^{\alpha_d}\right) \tag{9}$$

where $\phi(x,y,z)=\gamma(x,y)-\gamma(x,z)$.

Because multiple eavesdroppers exist, it is necessary to consider the ASC in the worst case: The capacity of the eavesdropper with the best channel gain represents the overall wiretapping capacity, so we can obtain $|G_e|^2=\max\limits_{e_i\in\Phi_e}\left\{|G_{e_i}|^2\right\}$, where $|G_e|^2$ is the eavesdropper with the best channel gain.

The CDF of $|G_e|^2$ can be expressed as

$$\begin{aligned}F_{|G_e|^2}(x)&=Pr\left(|G_e|^2<x\right)=\\&Pr\left(\max_{e_i\in\Phi_e}\left\{|G_{e_i}|^2\right\}<x\right)=\\&\prod_{e_i\in\Phi_e}Pr\left(|G_{e_i}|^2<x\right)=\prod_{e_i\in\Phi_e}F_{|G_{e_i}|^2}(x)\end{aligned} \tag{10}$$

Applying the probability generating function lemma, the CDF of $|G_e|^2$ is given by

$$\begin{aligned}F_{|G_e|^2}(x)&=E_{\Phi_e}\left[\prod_{e_i\in\Phi_e}F_{G_{e_i}}(x,y)\right]=\\&\exp\left(-\int_{S/P}\left[1-F_{|G_{e_i}|^2}(x,y)\right]\lambda_e\mathrm{d}y\right)=\\&\exp\left(\frac{-\lambda_e\pi}{\alpha_e}\sum_{l=0}^{M}\sum_{n=0}^{l}B_e x^n\int_{r_p^2}^{R^2}\exp(-\mu_e xy^{\alpha_e})y^{\alpha_e n+1}\mathrm{d}y\right)=\\&\exp\left(-\lambda_e\sum_{l=0}^{M}\sum_{n=0}^{l}\frac{\pi B_e\mu_e^{-n-\frac{1}{\alpha_e}}}{\alpha_e}x^{-\frac{1}{\alpha_e}}\cdot\right.\\&\left.\phi\left(n+\frac{1}{\alpha_e},\mu_e xR^{2\alpha_e},\mu_e xr_p^{2\alpha_e}\right)\right)\end{aligned} \tag{11}$$

where $E[\cdot]$ denotes the expectation.

In the considered system, we take the hardware impairments in the transceivers into account[18]. The distortion noises η_u and η_t, generated by hardware impairments at transceivers, are characterized by the transmitted and received aggregate levels of impairments k_u and k_t. These have zero mean and variance of $k_u^2P_u$ and $k_t^2|G_t|^2P_u$, which can be measured in practice based on the error vector magnitude[19].

Thus, the received signal at the user can be given as

$$y_t=G_t\left(\left(\sqrt{\beta P_u}\,x_1+\sqrt{(1-\beta)P_u}\,x_2\right)+\eta_u\right)+\eta_t+n_t \tag{12}$$

where P_u denotes the transmit power of the base station, β the power allocation coefficient, and n_t the noise at the receiver.

For convenience, the levels of eavesdroppers' impairments are assumed to be equal, so $k_{e_i}=k_e$, $\forall e_i\in\Phi_e$. So are the legal users', and $k_{d_1}=k_{d_2}=k_d$. n_t is the received noise, subject to $CN(0,\sigma_0^2)$, and σ_0^2 the power of noise.

As in NOMA system, the user with better channel gain can decode the signal sent to the user with worse channel gain. According to Eq.(12), signal to interference noise ratios (SINRs) of legal users are given as

$$\gamma_1=\frac{|G_1|^2\beta\gamma_0}{|G_1|^2a\gamma_0+1} \tag{13}$$

$$\gamma_2=\frac{|G_2|^2(1-\beta)\gamma_0}{|G_2|^2\gamma_0(\beta+a)+1} \tag{14}$$

where $\gamma_0=P_u/\sigma_0^2$ is the average signal to noise ratio (SNR). We set $a=k_u^2+k_d^2$ and $b=k_u^2+k_e^2$ for simplicity.

The SINRs of e_i wiretapping D_1 and D_2 are expressed as

$$\gamma_{e_i\to1}=\frac{|G_{e_i}|^2\beta\gamma_0}{|G_{e_i}|^2\gamma_0(1-\beta+b)+1} \tag{15}$$

$$\gamma_{e_i\to2}=\frac{|G_{e_i}|^2(1-\beta)\gamma_0}{|G_{e_i}|^2\gamma_0(\beta+b)+1} \tag{16}$$

The channel capacity of the legal users is expressed as

$$C_t=\log_2(1+\gamma_t)\qquad t\in\{1,2\} \tag{17}$$

Considering the worst condition, the channel capacity of the eavesdropper is

$$C_e = \max_{e_i \in \Phi_e} \{C_{e_i}\} \tag{18}$$

2 ASC Analysis

Secrecy capacity is the difference between the capacity of legal links and that of wiretapping links and secrecy capacity in non-negative. The instantaneous secrecy capacity is expressed as

$$C_s = \max\{C_d - C_e, 0\} \tag{19}$$

where C_d is the channel capacity of the legal user.

2.1 Close-form expressions of ASC of NOMA users

The ASC can be expressed as

$$\bar{C}_s = \int_0^\infty \int_{\gamma_e}^\infty (C_d - C_e) f_{\gamma_d}(\gamma_d) f_{\gamma_e}(\gamma_e) \mathrm{d}\gamma_d \mathrm{d}\gamma_e = \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_e}(\gamma_d)}{1+\gamma_d} \left(1 - F_{\gamma_d}(\gamma_d)\right) \mathrm{d}\gamma_d \tag{20}$$

where γ_d is the signal to interference plus noise ratio (SINR) of the legal user and γ_e the SINR of eavesdropper with the largest channel capacity; f_{γ_d} and f_{γ_e} are the PDF of γ_d and γ_e, and F_{γ_d} and F_{γ_e} the CDF of γ_d and γ_e. For legal user D_1, the CDF of γ_1 is derived as

$$F_{\gamma_1}(x) = Pr\left\{\frac{|G_1|^2 \gamma_0 \beta}{|G_1|^2 \gamma_0 a + 1} < x\right\} = \begin{cases} F_{|G_1|^2}\left(\dfrac{x\gamma_0^{-1}}{\beta - xa}\right) & x \leqslant \dfrac{\beta}{a} \\ 1 & x > \dfrac{\beta}{a} \end{cases} \tag{21}$$

Similarity, the CDF of the SINR for the eavesdroppers wiretapping the signal sent to D_1 is derived as

$$F_{\gamma_{e_i \to 1}}(x) = \begin{cases} F_{|G_{e_i}|^2}\left(\dfrac{x}{\gamma_0\left(\beta - x\left(1-\beta+b\right)\right)}\right) & x \leqslant \dfrac{\beta}{1-\beta+b} \\ 1 & x > \dfrac{\beta}{1-\beta+b} \end{cases} \tag{22}$$

Because it involves piecewise functions, we need to discuss the two situations:

(1) When $\dfrac{\beta}{a} \leqslant \dfrac{\beta}{1-\beta+b}$, $1-\beta \leqslant a-b$, Eq.(20) can be written as

$$\bar{C}_s^1 = \int_0^{\frac{\beta}{a}} \frac{1}{\ln 2(1+x)} F_{|G_e|^2}(X_1(x)) \left(1 - F_{|G_1|^2}(X_2(x))\right) \mathrm{d}x \tag{23}$$

where $X_1(x) = \dfrac{x\gamma_0^{-1}}{\beta - x\left(1-\beta+b\right)}$, $X_2(x) = \dfrac{x\gamma_0^{-1}}{\beta - xa}$.

Substituting Eqs.(7) and (11) into Eq.(23) and using the Gaussian-Chebyshev quadrature[20], the exact closed form of $\bar{C}_s^1$ can be written as

$$\bar{C}_s^1 \approx \frac{1}{R_1^2 \ln 2} \sum_{l=0}^{M} \sum_{n=0}^{l} \frac{B_d}{\alpha_d \mu_d^{n+\frac{1}{\alpha_d}}} \Xi_1 \tag{24}$$

where $\Xi_1 = \dfrac{\pi}{U} \sum_{u=1}^{U} \sqrt{\vartheta_{1u}\left(\dfrac{\beta}{a} - \vartheta_{1u}\right)}\, g_1(\vartheta_{1u})$, here U is the summation item, which reflects accuracy vs. complexity, $g_1(x) = \dfrac{\gamma\left(n + \dfrac{1}{\alpha_d}, \mu_d R_1^{2\alpha_d} X_2(x)\right) F_{|G_e|^2}\left(X_1(x)\right)}{(1+x)\, x^{\frac{1}{\alpha_d}}}$, $\vartheta_{1u} = \dfrac{\beta}{2a}(1+\tau_u)$, and $\tau_u = \cos\dfrac{(2u-1)\pi}{2U}$.

(2) When $1-\beta > a-b$, Eq.(20) can be written as

$$\bar{C}_s^1 = \frac{1}{\ln 2} \int_0^{\frac{\beta}{1-\beta+b}} \frac{F_{\gamma_{e\to 1}}(\gamma_d)}{1+\gamma_d} \left(1 - F_{\gamma_1}(\gamma_d)\right) \mathrm{d}\gamma_d + \frac{1}{\ln 2} \int_{\frac{\beta}{1-\beta+b}}^{\frac{\beta}{a}} \frac{\left(1 - F_{\gamma_1}(\gamma_d)\right)}{1+\gamma_d} \mathrm{d}\gamma_d \tag{25}$$

Similar to the derivation of Eq.(24), Eq.(25) can be presented as

$$\bar{C}_s^1 \approx \frac{1}{R_1^2 \ln 2} \sum_{l=0}^{M} \sum_{n=0}^{l} \frac{B_d}{\alpha_d \mu_d^{n+\frac{1}{\alpha_d}}} (\Xi_2 + \Xi_3) \tag{26}$$

where $\Xi_2 = \dfrac{\pi}{U} \sum_{u=1}^{U} \sqrt{\vartheta_{2u}\left(\dfrac{\beta}{1-\beta+b} - \vartheta_{2u}\right)}\, g_1(\vartheta_{2u})$, $\vartheta_{2u} = \dfrac{\beta(1+\tau_u)}{2(1-\beta+b)}$, $\tau_u = \cos\dfrac{(2u-1)\pi}{2U}$; $\Xi_3 = \dfrac{\pi}{U} \sum_{u=1}^{U} \dfrac{1}{2}\left(\dfrac{\beta}{a} - \dfrac{\beta}{1-\beta+b}\right) \sqrt{1-\tau_u}\, g_2(\vartheta_{3u})$,

$$g_2(x)=\frac{\gamma\left(n+\frac{1}{\alpha_d},\mu_d(R^2+H^2)^{\alpha_d}X_2(x)\right)}{x^{\frac{1}{\alpha_d}}(1+x)},\quad \vartheta_{3u}=\left(\frac{\beta}{2a}-\frac{\beta}{2(1-\beta+b)}\right)(\tau_u+1).$$

Similar to the derivations above, the ASC expression of D_2 can be expressed as:

(1) When $a\geqslant b$, we have

$$\bar{C}_s^2\approx\frac{1}{(R^2-R_1^2)\ln 2}\sum_{l=0}^{M}\sum_{n=0}^{l}\frac{B_d}{\alpha_d\mu_d^{n+\frac{1}{\alpha_d}}}\Xi_4 \quad (27)$$

where $\Xi_4=\frac{\pi}{U}\sum_{u=1}^{U}\sqrt{\vartheta_{4u}\left(\frac{1-\beta}{a+\beta}-\vartheta_{4u}\right)}\,g_3(\vartheta_{4u})$,

$g_3(x)=x^{-\frac{1}{\alpha_d}}(1+x)^{-1}\gamma\left(n+\frac{1}{\alpha_d},\mu_d R_1^{2\alpha_d}X_3(x)\right)\cdot F_{|G_e|^2}\left(X_3(x)\right)$, $\vartheta_{4u}=\frac{1-\beta}{2(a+\beta)}(1+\tau_u)$, $X_3(x)=\frac{x}{\gamma_0\left(1-\beta-x(\beta+b)\right)}$.

(2) When $a<b$, we have

$$\bar{C}_s^2\approx\frac{1}{(R^2-R_1^2)\ln 2}\sum_{l=0}^{M}\sum_{n=0}^{l}\frac{B_d}{\alpha_d\mu_d^{n+\frac{1}{\alpha_d}}}(\Xi_5+\Xi_6) \quad (28)$$

where $\Xi_5=\frac{\pi}{U}\sum_{u=1}^{U}\sqrt{\vartheta_{5u}\left(\frac{1-\beta}{\beta+b}-\vartheta_{2u}\right)}\,g_3(\vartheta_{5u})$,

$\vartheta_{5u}=\frac{1-\beta}{2(\beta+b)}(1+\tau_u)$, $\tau_u=\cos\frac{(2u-1)\pi}{2U}$;

$\Xi_6=\frac{\pi}{2U}\left(\frac{1-\beta}{a+\beta}-\frac{1-\beta}{\beta+b}\right)\sum_{u=1}^{U}\sqrt{1-\tau_u}\,g_4(\vartheta_{6u})$,

$g_4(x)=x^{-\frac{1}{\alpha_d}}(1+x)^{-1}\gamma\left(n+\frac{1}{\alpha_d},\mu_d R^{2\alpha_d}X_3(x)\right)$,

$\vartheta_{6u}=\frac{(\tau_u+1)}{2}\left(\frac{1-\beta}{a+\beta}-\frac{1-\beta}{\beta+b}\right)$.

When $a=b$, the total ASC of the system can be expressed as

$$\bar{C}_s=\bar{C}_s^1+\bar{C}_s^2 \quad (29)$$

Substituting Eqs.(26) and (27) into Eq.(29), the total ASC of the system can be obtained.

2.2 Asymptotic expressions of ASC of NOMA users

Through simulation, we find that when the average SNR tends to infinity, the ASC of D_1 tends to a fixed value. For $\gamma_0\to\infty$, the average capacity of D_1 tend to be: $C_1^{\infty}\approx\log_2(1+\beta/a)$. As to the eavesdroppers, of which the positions are subject to HPPP, the probability that no eavesdropper exists is not zero. When the number of eavesdroppers is not zero, the average wiretapping capacity at high γ_0 is closed to

$$C_{e\to 1}^{\infty}\approx\log_2\left(1+\frac{\beta}{(1-\beta)+b}\right) \quad (30)$$

As to the definition of HPPP model, the probability that no eavesdropper exists is $p_0=e^{-\lambda_e S_{S/P}}$, where $S_{S/P}=\pi(R^2-r_p^2)$ denotes the area of the eavesdroppers' presence. In this scenario, the average wiretapping capacity is equal to zero.

We also need to discuss the size relation of $1-\beta$ and $a-b$, when analyzing the asymptotic ASC at high γ_0.

(1) When $1-\beta>a-b$, the average capacity of D_1 and the average wiretapping capacity at high γ_0 tends to $\log_2(1+\beta/a)$ and $(1-p_0)\log_2\left(1+\frac{\beta}{1-\beta+b}\right)$.

(2) When $1-\beta\leqslant a-b$, considering the non-negativity of ASC, ASC is 0. Only when the number of eavesdroppers is zero, the average wiretapping capacity is zero. In this condition, the ASC of the system is equal to the average capacity of D_1, that is $p_0\log_2(1+\beta/a)$.

To sum up, the asymptotic expression of ASC of D_1 at high SNR can be expressed as

$$\lim_{\gamma_0\to\infty}\bar{C}_s^1=\begin{cases}\log_2\left(1+\frac{\beta}{a}\right)-p_1\log_2\left(1+\frac{\beta}{1-\beta+b}\right) & H_0\\ p_0\log_2\left(1+\frac{\beta}{a}\right) & H_1\end{cases} \quad (31)$$

where H_1: $a-b<1-\beta$; H_0: $a-b\geqslant 1-\beta$; and $p_1=1-p_0$.

Remark 1 The asymptotic expression of

ASC of D_1 is related to power allocation coefficient of NOMA and hardware impairments.

The asymptotic ASC expression of D_2 can be expressed as

$$\lim_{\gamma_0\to\infty}\bar{C}_s^2=\begin{cases}\log_2\left(1+\dfrac{1-\beta}{\beta+a}\right)-p_1\log_2\left(1+\dfrac{1-\beta}{\beta+b}\right) & a<b\\ p_0\log_2\left(1+\dfrac{1-\beta}{\beta+a}\right) & a\geqslant b\end{cases} \tag{32}$$

Remark 2 The asymptotic expression of ASC of D_2 is related to power allocation coefficient of NOMA and hardware impairments. And when the power allocation coefficient β increases, the asymptotic expression of ASC of D_2 increases.

Besides, the asymptotic expression of $\bar{C}_s$ is given by

$$\lim_{\gamma_0\to\infty}\bar{C}_s=\lim_{\gamma_0\to\infty}\bar{C}_s^1+\lim_{\gamma_0\to\infty}\bar{C}_s^2 \tag{33}$$

By substituting Eqs.(31) and (32) into Eq.(33), we can get the total asymptotic ASC of the system.

3 Numerical Results and Discussion

This section verifies the correctness of the formulas derived above through computer simulation, and discusses the impact of power allocation coefficient, transmit power and hardware impairments on PLS performance. The main parameters are set as $\alpha_d=\alpha_e=2$, $\lambda_e=1\times10^{-4}\,\mathrm{m}^2$, $R_1=100\,\mathrm{m}$, $R=500\,\mathrm{m}$, $r_p=200\,\mathrm{m}$, $\beta=0.3$, $k_u=k_d=k_e=0.1$.

Fig.2 shows the analytical and simulation values of ASC for D_1 and D_2 at different power allocation coefficients. It can be seen that simulation and theory are very consistent, indicating that the formula derived above is accurate. The dotted line represents the progressive value of ASC, indicating that the ASC of legitimate users does tend to a fixed value under high average SNRs. In addition, it demonstrates that as the power allocation coefficient decreases, the gap between the ASCs of D_1 and D_2 gradually decreases, reflecting the fairness of NOMA technology. That is, by allocating lower power to users with better channels, the gap between the capacity of the two is minimized.

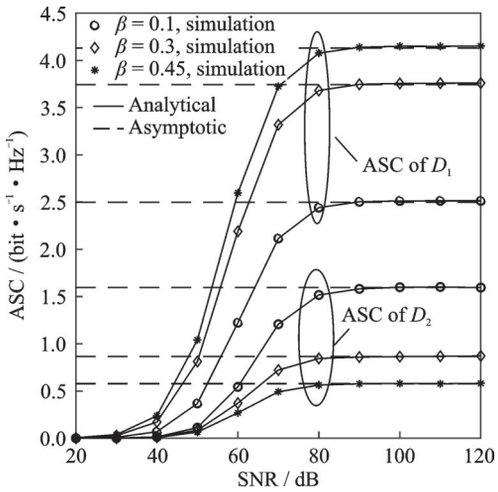

Fig.2 ASC of D_1 and D_2 versus average SNR for varying power allocation coefficients

Fig.3 shows the analytical and simulation values of ASC for the system at different power coefficients. It demonstrates that, as the power allocation coefficient β decreases, the total secrecy capacity of the system also decreases. Referring to Fig.2, it can be seen that, as β decreases, the secrecy capacity of user with poor channels increases, and the secrecy capacity of user with better channels decreases, which increases fairness, but loses the total secrecy capacity of the system. Therefore, a compromise between secrecy capacity and user fairness can be considered.

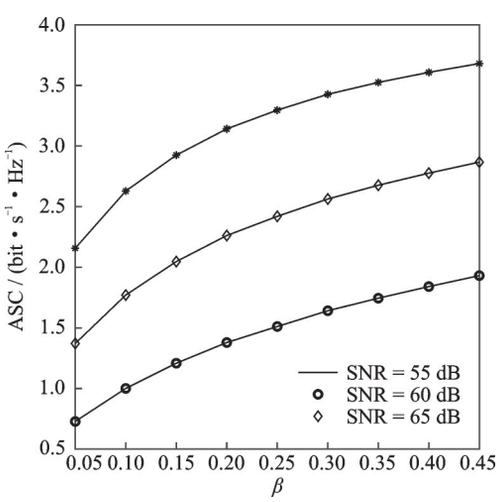

Fig.3 ASC versus average SNR for varying power allocation coefficients

Fig.4 compares the curves of ASC of the system under different hardware impairment levels. It demonstrates that, as the average SNR increases, the ASC of the system approaches a fixed value, which is only related to the hardware impairments. Obviously, the higher the level of hardware impairments, the lower the ASC of the system.

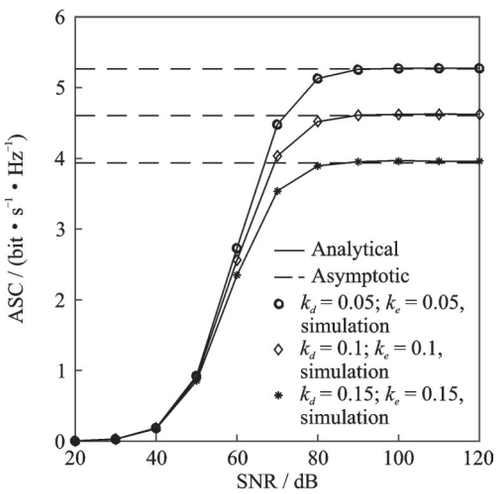

Fig.4 ASR versus transmission power under different hardware impairments levels

4 Conclusions

The paper investigated the PLS issue and the Protected Zone technology in NOMA system. We derived the CDF and PDF of the power gain for the legitimate and eavesdropping channels, and gave an approximate closed-form expression of ASC of the system. The simulation results proved the accuracy of the theory and the effectiveness of Protected Zone technology in improving the physical layer security of communication systems. Besides, we indicated the impact of hardware impairments and power allocation coefficient on the system's PLS performance.

References

[1] WANG H, YU X B, LIU F Y, et al. Performance analysis of uplink distributed massive MIMO system with cross-layer design over rayleigh fading channel[J]. Transactions of Nanjing University of Aeronautics and Astronautics, 2021, 38(6): 1028-1036.

[2] ROMERO-ZURITA N, MCLERNON D, GHOGHO M, et al. PHY layer security based on protected zone and artificial noise[J]. IEEE Signal Processing Letters, 2013, 20(5): 487-490.

[3] CAI J L, YU X B, XU F C, et al. Joint energy-efficient power allocation and beamforming design for mmWave-NOMA system with imperfect CSI[J]. Transactions of Nanjing University of Aeronautics and Astronautics, 2021, 38(S1): 115-121.

[4] LEI H J, ZHU C, PARK K H, et al. On secure NOMA-based terrestrial and aerial IoT systems[J]. IEEE Internet of Things Journal, 2022, 9(7): 5329-5343.

[5] KIM M, KIM S, LEE J. Securing communications with friendly unmanned aerial vehicle jammers[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1972-1977.

[6] LI M L, YU X B, HE A S, et al. On the secrecy performance of UAV-assisted wireless communication system with hardware impairments and protected zone[C]//Proceedings of 2022 IEEE International Conference on Communications Workshops (ICC Workshops). [S.l.]: IEEE, 2022: 993-998.

[7] WEI L, CHEN Y Y, ZHENG D S, et al. Secure performance analysis and optimization for FD-NOMA vehicular communications[J]. China Communications, 2020, 17(11): 29-41.

[8] LU W D, DING Y, GAO Y, et al. Secure NOMA-based UAV-MEC network towards a flying eavesdropper[J]. IEEE Transactions on Communications, 2022, 70(5): 3364-3376.

[9] ABUSHATTAL A, ALTHUNIBAT S, QARAGE M, et al. A secure downlink NOMA scheme against unknown internal eavesdroppers[J]. IEEE Wireless Communications Letters, 2021, 10(6): 1281-1285.

[10] HERO A O. Secure space-time communication[J]. IEEE Transactions on Information Theory, 2003, 49(12): 3235-3249.

[11] SHUKLA M K, NGUYEN H H. Ergodic secrecy sum rate analysis of a two-way relay NOMA system[J]. IEEE Systems Journal, 2021, 15(2): 2222-2225.

[12] GONG C, YUE X, ZHANG Z, et al. Enhancing physical layer security with artificial noise in large-scale NOMA networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(3): 2349-2361.

[13] XIANG Z, TONG X, CAI Y. Secure transmission for NOMA systems with imperfect SIC[J]. China Communications, 2020, 17(11): 67-78.

[14] SIMON M K, ALOUINI M S. Digital communication over fading channels[M]. 2nd ed. New York, NY, USA: Wiley-Interscience, 2005: 93-94.

[15] TRINH P V, THANG T C, PHAM A T. Mixed

mmWave RF/FSO relaying systems over generalized fading channels with pointing errors[J]. IEEE Photonics Journal, 2017, 9(1): 1-14.

[16] LEI H, WANG D, PARK K, et al. Safeguarding UAV IoT communication systems against randomly located eavesdroppers[J]. IEEE Internet of Things Journal, 2020, 7(2): 1230-1244.

[17] GRADSHTEYN I S, RYZHIK I M. Table of Integrals, Series and Products[M]. 7th ed. San Diego, CA, USA: [s.n.], 2007: 899-900.

[18] LI X, WANG Q, LIU Y, et al. UAV-aided multi-way NOMA networks with residual hardware impairments[J]. IEEE Wireless Communication Letters, 2020, 9(9): 1538-1542.

[19] LI X, ZHAO M, ZENG M, et al. Hardware impaired ambient backscatter NOMA systems: Reliability and security[J]. IEEE Transactions on Communications, 2021, 69(4): 2723-2736.

[20] ABRAMOWITZ M, STEGUN I. Handbook of mathematical functions with formulas, graphs, and mathematical tables[M]. 9th ed. New York, NY, USA: Discover, 1972: 889-890.

Acknowledgements This work was supported in part by the National Natrual Science Foundation of China (Nos. 61971220, 61971221), and the Open Research Fund Key Laboratory of Wireless Sensor Network and Communication of Chinese Academy of Science (No.2017006).

Authors Ms. **HE Ansu** received the B.S. degree in communication engineering from Nanjing Normal University, Nanjing, China, in 2021. She is currently pursuing the M.Sc. degree in Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China. Her research interests include the terahertz communication and physical layer security.

Prof. **YU Xiangbin** received his Ph.D. degree in communication and information systems from Southeast University, Nanjing, China, in 2004. From 2010 to 2011, he was a research fellow in Department of Electronic Engineering, City University of Hong Kong. From 2014 to 2015, he was a visiting scholar in electrical and computer engineering, University of Delaware. Now he is a professor of NUAA. His research interests include distributed MIMO, adaptive modulation, precoding design, and green communication.

Author contributions Ms. **HE Ansu** designed the study, complied the models and wrote the manuscript. Prof. **YU Xiangbin** conducted the analysis and contributed to the discussion and background of the study. Ms. **ZHOU Yue** provided the simulation results and interpreted the results. All authors commented on the manuscript draft and approved the submission.

Competing interests The authors declare on competing interest.

(Production Editor: ZHANG Huangqun)

硬件损伤下多窃听器NOMA系统平均保密容量分析

何安苏[1], 虞湘宾[1,2], 周 玥[1]

(1.南京航空航天大学电子信息工程学院,南京 211106,中国;
2.中国科学院无线传感器网络与通信重点实验室,上海 200050,中国)

摘要:研究了非正交多址(Non-orthogonal-multiple-access, NOMA)接入通信系统的物理层安全性能。当基站采用下行NOMA方案发送信息时,由于信道的开放性,信息容易被窃听,而当存在多个随机分布的窃听者时,安全性能会进一步降低。为了增强存在硬件损伤系统的物理层安全性能,本文考虑保护区的方法,针对地面用户与基站之间存在直连链路的情况,采用莱斯衰落来建模小尺度衰落。本文还假设多个窃听者的位置遵循齐次泊松点过程(Homogeneous Poisson point process, HPPP),借助高斯切比雪夫积分公式,推导了平均保密容量的闭式表达式,并给出了在高信噪比情况下的渐近表达式来获得进一步见解。仿真结果验证了保护区方法在增强安全性能方面的有效性,并说明了不同参数对系统保密性能的影响。

关键词:平均保密容量;非正交多址;硬件损伤;硬件损伤;莱斯衰落;物理层安全