Enhancing Physical Layer Security of Cooperative NOMA Systems Using User Selection

Menghuan Ma, Yucheng He, Yan Zhang, Yu Zhang, and Lin Zhou

Abstract In this paper, we study a physical layer security improvement method for a multi-user cooperative non-orthogonal multiple access (NOMA) system in the presence of an adaptive eavesdropper. In the system, the eavesdropper adaptively switches the eavesdropping mode and interference mode. In order to resist the eavesdropping attack of the eavesdropper, a number of device-to-device (D2D) relay users are available for cooperating to forward legitimate signals, and one of them can be selected for assistance through a user selection strategy based on the channel side information (CSI) of the eavesdropping channel. The selected relay uses the NOMA technology to superimpose ordinary signals that only require data services with the received sensitive signals, and then forwards the superimposed signals. The ergodic secrecy sum capacity lower bound of the system is derived. Theoretical analysis and Monte Carlo simulation show that the performance of the proposed multi-user cooperative NOMA system is better than that of the single-relay user cooperative system.

1 Introduction

Since the available frequency band of mobile communication is mainly below 3 GHz, 5G networks need to meet the requirements of low latency and massive connections under limited spectrum resources. Non-orthogonal multiple access (NOAM) is a important technology to solve the shortage of spectrum resources. Its basic principle is that the transmitter adopts power domain superposition coding, actively

M. Ma · Y. He (✉) · Y. Zhang · Y. Zhang · L. Zhou
Xiamen Key Laboratory of Mobile Multimedia Communications, National Huaqiao University, Xiamen 361021, Fujian, China
e-mail: yucheng.he@hqu.edu.cn

Y. He · L. Zhou
State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, Shaanxi, China

L. C. Jain et al. (eds.), *Advances in Wireless Communications and Applications*,
Smart Innovation, Systems and Technologies 299,
https://doi.org/10.1007/978-981-19-2255-8_3

introducing interference information, and the receiver adopts successive interference cancellation (SIC) to realize correct demodulation [1].

Due to shadow fading and path loss, the communication reliability of users far from the transmitter is poor. Relay cooperative NOMA network can improve the communication quality of far users. According to the NOMA superposition coding principle, strong user know the signal information of weak users and act as a Decode-and-Forward (DF) relay to assist in forwarding the signal information of weak users [2]. Under the statistical channel state information (CSI), the authors analyzed a communication system in which a single relay forwards the signals of multiple edge users over Nakagami-m fading channels, and the differences between DF relay and amplify-and-forward (AF) relay in improving communication performance was compared in [3]. In addition, device-to-device (D2D) technology allows two adjacent user equipment to communicate directly by reusing the spectrum resources of the cellular network, thereby reducing communication delay and improve spectrum utilization. So D2D relay cooperative communication based on NOMA has attracted extensive research scholars' attention. For D2D cooperative NOMA network, a power allocation strategy based on signal-to-noise ratio (SNR) was proposed in [4] to achieve the maximum capacity. Moreover, two different SIC decoding schemes were proposed in [5], namely the single signal decoding scheme and the maximum ratio combining (MRC) decoding scheme, respectively, and the authors compared and analyzed the influence of different decoding schemes on communication performance. In order to avoid the loss of communication performance caused by SIC error decoding, according to the decoding of D2D relay, three different relay forwarding strategies were studied in [6].

Due to the openness of RF signals, sensitive information with high security requirements is easily attacked by eavesdroppers during transmission. Therefore, the security of NOMA network must be considered. Relay cooperation can not only improve the communication reliability of cell-edge users, but also help legitimate nodes improve the physical layer security of the system. Physical layer security technology is based on Shannon theory. Its main idea is to protect the physical layer by using the inherent random characteristics of wireless channel [7]. At present, many researches on physical layer security are relay selection, cooperative beamforming, cooperative interference and so on. According to the different understanding of the eavesdropping channel, the corresponding relay selection strategy was proposed to combat the malicious eavesdropping of adaptive eavesdroppers in [8]. Considering the problem of energy limitation in communication, a AF relay collected energy from part of artificial interference signals, and forwarded the remaining artificial interference signals to eavesdroppers, so as to protect the legitimate signals [9]. In [10], the multi-antenna relay beamforming technology was used to design artificial interference signals to interfere with eavesdroppers without affecting the communication of legitimate users.

At present, there is little research on D2D cooperative NOMA scheme in the intelligent eavesdropping scenario. Furthermore, each user has different requirements for information security service experience. For example, sensitive information such as bank information and personal privacy information has high security requirements,

but ordinary data information has low security requirements. So this paper proposes a multi-user cooperative NOMA scheme by using the differences of users' security service requirements, in order to further improve physical layer security, a user selection strategy was studied. We derive the expression on the ergodic secrecy sum capacity lower bound of the proposed scheme, and compare the performance differences between the scheme and single user cooperative NOMA scheme.

2 System Model

Figure 1 shows the system model of the proposed scheme, where a source node denoted S, a number N of DF relay user nodes denoted $\mathrm{R}_k (k = 1, 2, \ldots, N)$, two destination nodes denoted D_1 and D_2, and a eavesdropping node denoted E are considered. All nodes work in half-duplex mode, equipped with a single antenna. Moreover, E is equipped with a directional antenna. We assume that all channels are independent quasi-static Rayleigh fading channels. Denote h_{S1}, h_{SR_k}, $h_{\mathrm{R}_k\mathrm{E}}$, $h_{\mathrm{R}_k 2}$, h_{E1}, h_{ER_k} as the channel coefficients of links S - D_1, S - R_k, R_k - E, R_k - D_2, E - D_1, E - R_k respectively. According to [11], $h_{\mathrm{R}_k\mathrm{E}} = h_{\mathrm{ER}_k}$. Due to path loss and shadow fading, the links S - D_2 and S - E are not available. $h_{\mathrm{S1}}, h_{\mathrm{SR}_k}, h_{\mathrm{R}_k\mathrm{E}}, h_{\mathrm{R}_k 2}, h_{\mathrm{E1}}, h_{\mathrm{ER}_k}$ are independent complex Gaussian random variables with mean denoted as λ_{S1}, λ_{SR_k}, $\lambda_{\mathrm{R}_k\mathrm{E}}$, $\lambda_{\mathrm{R}_k 2}$, λ_{E1}, $\lambda_{\mathrm{R}_k\mathrm{E}}$. Each node knows the CSI between itself and other nodes, and the CSI of the eavesdropping channel can be obtained by the method mentioned in [12]. Here E is an intelligent eavesdropper, which means that if E detects the signal transmitted by R_k, E will work in eavesdropping mode and directed eavesdropping R_k, otherwise it will switch to interference mode.

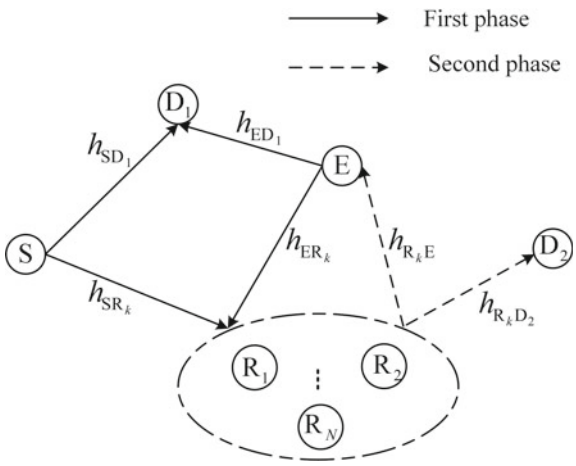

Fig.1 System model

2.1 Design of Transmission Scheme

The entire transmission process comprises two phases. In the first phase, the source node S broadcasts the superimposed signal $\sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2$, where P_S is the transmit power of S, x_i represents the intended message for $D_i, i \in \{1, 2\}$. According to NOMA principles, the power allocation coefficient $a_1 < a_2$ and $a_1 + a_2 = 1$. At the same time, the eavesdropper E executes interference mode and transmits interference signals $\sqrt{P_J} x_J$ to legitimate nodes. The signal received at D_1 and R are given by

$$y_1 = h_{S1}\left(\sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2\right) + h_{E1}\sqrt{P_J} x_J + n_1 \tag{1}$$

$$y_{R_k} = h_{SR_k}\left(\sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2\right) + h_{ER_k}\sqrt{P_J} x_J + n_{R_k} \tag{2}$$

where $n_1 \sim CN(0, \sigma_1)$ and $n_{R_k} \sim CN\left(0, \sigma_{R_k}\right)$ represent the additive white Gaussian noise AWGN at D_1 and R_k respectively. To abide with the principle of SIC, D_1 first decodes and removes the symbol x_2 by treating the symbol x_1 as noise, and then will decode symbol x_1. The received signal-to-interference-plus-noise ratio (SINR) for x_1 and x_2 at D_1 are given by

$$\gamma_{1 \to x_2} = \frac{|h_{S1}|^2 a_2 P_S}{|h_{S1}|^2 a_1 P_S + |h_{E1}|^2 P_J + \sigma_1^2} \tag{3}$$

$$\gamma_{1 \to x_1} = \frac{|h_{S1}|^2 a_1 P_S}{|h_{E1}|^2 P_J + \sigma_1^2} \tag{4}$$

Similarly, the received SINR for x_2 at R_k is expressed as

$$\gamma_{R_k \to x_2} = \frac{\left|h_{SR_k}\right|^2 a_2 P_S}{\left|h_{SR_k}\right|^2 a_1 P_S + \left|h_{ER_k}\right|^2 P_J + \sigma_{R_k}^2} \tag{5}$$

In the second phase, in order to alleviate the communication congestion and reduce the SINR of the eavesdropper, R_k forwards the new superimposed signal $\sqrt{a_1 P_R} x_R + \sqrt{a_2 P_R} x_2$ with the transmit power P_R. x_R is the normal data signal intended for D_2. Assuming that in the entire time slot, E can detect the signal forwarded by R, so it works in eavesdropping mode. The signal received at D_2 and E are given by

$$y_2 = h_{R_k 2}\left(\sqrt{a_1 P_R} x_R + \sqrt{a_2 P_R} x_2\right) + n_2 \tag{6}$$

$$y_E = h_{R_k E}\left(\sqrt{a_1 P_R} x_R + \sqrt{a_2 P_R} x_2\right) + n_E \tag{7}$$

where $n_2 \sim CN(0, \sigma_2)$ and $n_{\mathrm{E}} \sim CN(0, \sigma_{\mathrm{E}})$ represent the AWGN at D_2 and E respectively. The received SINR for x_2 and x_{R} can be obtained as

$$\gamma_{2\to x_2} = \frac{\left|h_{\mathrm{R}_k 2}\right|^2 a_2 P_{\mathrm{R}}}{\left|h_{\mathrm{R}_k 2}\right|^2 a_1 P_{\mathrm{R}} + \sigma_2^2} \tag{8}$$

$$\gamma_{2\to x_{\mathrm{R}}} = \frac{\left|h_{\mathrm{R}_k 2}\right|^2 a_1 P_{\mathrm{R}}}{\sigma_2^2} \tag{9}$$

Since E only decodes sensitive signals x_2 that have eavesdropping value, the received SINR at E is given by

$$\gamma_{\mathrm{E}\to x_2} = \frac{\left|h_{\mathrm{R}_k \mathrm{E}}\right|^2 a_2 P_{\mathrm{R}}}{\left|h_{\mathrm{R}_k \mathrm{E}}\right|^2 a_1 P_{\mathrm{R}} + \sigma_{\mathrm{E}}^2} \tag{10}$$

In order to reduce the eavesdropping quality of E, we propose a relay selection strategy that minimizes the channel gain of eavesdropping, and the mathematical expression is as follows

$$\mathrm{R}_b = \arg \min_{k=1,2,\ldots,N} \left|h_{\mathrm{R}_k \mathrm{E}}\right|^2 \tag{11}$$

3 Analysis of Ergodic Secrecy Sum Capacity

Here we use ergodic secrecy sum capacity (ESSC) as the performance indicator to evaluate the effectiveness of the proposed scheme. For the convenience of writing, let $\sigma_i^2 = \sigma^2$, for $i \in \{1, 2, \mathrm{R}_b, \mathrm{E}\}$, $\gamma_{\mathrm{S}} = \frac{P_{\mathrm{S}}}{\sigma^2}$, $\gamma_{\mathrm{J}} = \frac{P_{\mathrm{J}}}{\sigma^2}$, $\gamma_{\mathrm{R}} = \frac{P_{\mathrm{R}}}{\sigma^2}$, $\beta_\varphi \triangleq \left|h_\varphi\right|^2$, for $\varphi \in \{\mathrm{S1}, \mathrm{SR}_b, \mathrm{R}_b\mathrm{E}, \mathrm{R}_b 2, \mathrm{E1}, \mathrm{ER}_b\}$.

3.1 Ergodic Secrecy Capacity of x_1

Ergodic secrecy capacity (ESC) of x_1 is defined as $\overline{C}_{\mathrm{ESC}}^{x_1} \triangleq \mathbb{E}\left[\left\{C_1^{x_1} - C_{\mathrm{E}}^{x_1}\right\}^+\right]$, where $C_1^{x_1}$ and $C_{\mathrm{E}}^{x_1}$ is the achievable maximum instantaneous rate of x_1 at D_1 and E respectively. According to Jensen's inequality, the definition of the ESC lower bound of x_1 can be expressed as

$$\overline{C}_{\mathrm{ESC,lb}}^{x_1} \triangleq \left\{\mathbb{E}\left[C_1^{x_1}\right] - \mathbb{E}\left[C_{\mathrm{E}}^{x_1}\right]\right\}^+ = \left\{\overline{C}_1^{x_1} - \overline{C}_{\mathrm{E}}^{x_1}\right\}^+ \tag{12}$$

Let $Q_1 = \gamma_{1\to x_1}$, the complementary cumulative distribution function (CCDF) of Q_1 is written as

$$\overline{F}_{Q_1}(q_1) = \Pr\left(\frac{\beta_{\mathrm{S}1} a_1 P_{\mathrm{S}}}{\beta_{\mathrm{E}1} P_{\mathrm{J}} + \sigma^2} > q_1\right) = \frac{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}}}{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}} + \lambda_{\mathrm{E}1} \gamma_{\mathrm{J}} q_1} \mathrm{e}^{-\frac{q_1}{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}}}} \tag{13}$$

Using the equation in [5]

$$\int_0^\infty \log(1+x) f_X(x) dx = \frac{1}{\ln 2} \int_0^\infty \frac{1 - F(x)}{1+x} dx \tag{14}$$

and [13, Eq. (25.4)], we can finally obtain

$$\approx \frac{\pi^2}{8L_1 \ln 2} \sum_{i=1}^{L_1} \frac{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}} \sqrt{1-\alpha_i} \sec^2 \theta_i}{(\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}} + \lambda_{\mathrm{E}1} \gamma_{\mathrm{J}} \tan\theta_i)(1+\tan\theta_i)} \mathrm{e}^{-\frac{\tan\theta_i}{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}}}} \tag{15}$$

where $\alpha_i = \cos\frac{(2i-1)\pi}{2L_1}$, $\theta_i = \frac{\pi}{4}\alpha_i + \frac{\pi}{4}$, L_1 denotes the number of the Gauss–Chebyshev quadrature approximation. Due to path loss and shadows, the eavesdropper E cannot eavesdrop on the superimposed signal broadcasted by S, thus $\overline{C}_{\mathrm{E}}^{x_1} = 0$ ◦Substituting $\overline{C}_{\mathrm{E}}^{x_1} = 0$ and (15) into (12), the expression of the ESC lower bound of x_1 can be obtained as

$$\overline{C}_{\mathrm{ESC,lb}}^{x_1} \approx \left\{ \frac{\pi^2}{8L_1 \ln 2} \sum_{i=1}^{L_1} \frac{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}} \sqrt{1-\theta_i} \sec^2 \theta_i}{(\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}} + \lambda_{\mathrm{E}1} \gamma_{\mathrm{J}} \tan\theta_i)(1+\tan\theta_i)} \mathrm{e}^{-\frac{\tan\theta_i}{\lambda_{\mathrm{S}1} a_1 \gamma_{\mathrm{S}}}} \right\}^+ \tag{16}$$

3.2 Ergodic Secrecy Capacity of x_2

Similar to x_1, using Jensen's inequality, the definition of the ESC lower bound of x_2 can be expressed as

$$\overline{C}_{\mathrm{ESC,lb}}^{x_2} \triangleq \left\{\mathbb{E}\left[C_2^{x_2}\right] - \mathbb{E}\left[C_{\mathrm{E}}^{x_2}\right]\right\}^+ = \left\{\overline{C}_2^{x_2} - \overline{C}_{\mathrm{E}}^{x_2}\right\}^+ \tag{17}$$

where $C_2^{x_2}$ and $C_{\mathrm{E}}^{x_2}$ is the achievable maximum instantaneous rate of x_2 at D_1 and E. Let $T_1 = \min\left\{\gamma_{1\to x_2}, \gamma_{\mathrm{R}_k\to x_2}, \gamma_{2\to x_2}\right\}$, $T_2 = \gamma_{\mathrm{E}\to x_2}$, $V_1 = \beta_{\mathrm{R}_b\mathrm{E}}$, where T_1 is the effective received SNR for x_2. Due to $\left|h_{\mathrm{R}_1\mathrm{E}}\right|^2, \left|h_{\mathrm{R}_2\mathrm{E}}\right|^2, \ldots, \left|h_{\mathrm{R}_N\mathrm{E}}\right|^2$ are an independent and identically distributed random variable, the probability density function (PDF) of V_1 is $f_{V_1}(v_1) = \frac{N}{\lambda_{\mathrm{RE}}} \mathrm{e}^{-\frac{N}{\lambda_{\mathrm{RE}}} v_1}$. The achievable ESC of x_2 at D_2 and E can be written

as

$$\overline{C}_2^{x_2} = \frac{1}{2}\int_0^{\infty} \log(1+t_1) f_{T_1}(t_1) dt_1 = \frac{1}{2\ln 2}\int_0^{\infty} \frac{1-F_{T_1}(t_1)}{1+t_1} dt_1 \tag{18}$$

$$\overline{C}_{\mathrm{E}}^{x_2} = \frac{1}{2}\int_0^{\infty} \log(1+t_2) f_{T_2}(t_2) dt_2 = \frac{1}{2\ln 2}\int_0^{\infty} \frac{1-F_{T_2}(t_2)}{1+t_2} dt_2 \tag{19}$$

In order to obtain the expression of $C_2^{x_2}$ and $C_{\mathrm{E}}^{x_2}$, we derive the CCDF of T_1 and T_2 as follows:

$$\begin{aligned}
\overline{F}_{T_1}(t_1) &= \Pr\left(\min\left\{\gamma_{1\to x_2}, \gamma_{\mathrm{R}_k\to x_2}, \gamma_{2\to x_2}\right\} > t_1\right) \\
&= \frac{N}{\lambda_{\mathrm{E}1}\lambda_{\mathrm{ER}_b}} \mathrm{e}^{-\left(\frac{1}{\lambda_{\mathrm{S}1}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{R}2}\gamma_{\mathrm{R}}}\right)\frac{t_1}{(a_2-a_1t_1)}} \\
&\quad \int_0^{\infty} \mathrm{e}^{-u\left(\frac{\gamma_{\mathrm{J}}t_1}{\lambda_{\mathrm{S}1}(a_2-a_1t_1)\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{E}1}}+\frac{\gamma_{\mathrm{J}}t_1}{\lambda_{\mathrm{SR}}(a_2-a_1t_1)\gamma_{\mathrm{S}}}+\frac{N}{\lambda_{\mathrm{ER}_b}}\right)} \mathrm{d}u \\
&= \frac{\lambda_{\mathrm{S}1}\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}^2 N(a_2-a_1t_1)^2 \mathrm{e}^{-\left(\frac{1}{\lambda_{\mathrm{S}1}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{R}2}\gamma_{\mathrm{R}}}\right)\frac{t_1}{(a_2-a_1t_1)}}}{\left[\lambda_{\mathrm{S}1}\gamma_{\mathrm{S}}(a_2-a_1t_1)+\lambda_{\mathrm{E}1}\gamma_{\mathrm{J}}t_1\right]\left[\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}N(a_2-a_1t_1)+\lambda_{\mathrm{ER}}\gamma_{\mathrm{J}}t_1\right]}
\end{aligned} \tag{20}$$

$$\overline{F}_{T_2}(t_2) = \Pr\left(\gamma_{\mathrm{E}\to x_2} > t_2\right) = \Pr\left(\frac{\beta_{\mathrm{R}_k\mathrm{E}}a_2P_{\mathrm{R}}}{\beta_{\mathrm{R}_k\mathrm{E}}a_1P_{\mathrm{R}}+\sigma_{\mathrm{E}}^2} > t_2\right) = \mathrm{e}^{-\frac{Nt_2}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}(a_2-a_1t_2)}} \tag{21}$$

Substituting (20) into (18), the achievable ESC of x_2 at D_2 is given by

$$\overline{C}_2^{x_2} = \frac{\pi}{2L_2\ln 2}\sum_{i=1}^{L_2} \frac{\lambda_{\mathrm{S}1}\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}^2 a_1^2 a_2 N(1-x_i)^2\sqrt{1-y_i^2}\times \mathrm{e}^{-\left(\frac{1}{\lambda_{\mathrm{S}1}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{R}2}\gamma_{\mathrm{R}}}\right)\frac{(1+x_i)}{a_1(1-x_i)}}}{A(x_i)} \tag{22}$$

where L_2 denotes the number of the Gauss–Chebyshev quadrature approximation, $y_i = \cos\frac{(2i-1)\pi}{2L_2}$, $x_i = y_i$, and

$$\begin{aligned}
A(x_i) &= (2a_1 + a_2(1+x_i))(\lambda_{\mathrm{S}1}\gamma_{\mathrm{S}}a_1(1-x_i) + \lambda_{\mathrm{E}1}\gamma_{\mathrm{J}}(1+x_i)) \\
&\quad \times (\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}Na_1(1-x_i) + \lambda_{\mathrm{ER}}\gamma_{\mathrm{J}}(1+x_i))
\end{aligned} \tag{23}$$

Using (19), (21) and [14, Eq. (3.352.2)], the achievable ESC of x_2 at E is given by

$$\overline{C}_{\mathrm{E}}^{x_2} = \frac{1}{2\ln 2}\left[\mathrm{e}^{\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}a_1}}\mathrm{Ei}\left(-\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}a_1}\right) - \mathrm{e}^{\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}}}\mathrm{Ei}\left(-\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}}\right)\right] \tag{24}$$

where Ei(·) is exponential integral function. Therefore, the expression of the ESC lower bound of x_2 can be finally obtained as

$$\overline{C}_{\mathrm{ESC,lb}}^{x_2} \approx \frac{1}{2\ln 2}\left\{\begin{array}{l}\dfrac{\pi}{L_2}\displaystyle\sum_{i=1}^{L_2}\frac{\lambda_{\mathrm{S1}}\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}^2 a_1^2 a_2 N(1-x_i)^2\sqrt{1-y_i^2}\times \mathrm{e}^{-\left(\frac{1}{\lambda_{\mathrm{S1}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}}\right)\frac{(1+x_i)}{a_1(1-x_i)}}}{A(x_i)} \\ -\left[\mathrm{e}^{\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}a_1}}\mathrm{Ei}\left(-\dfrac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}a_1}\right)-\mathrm{e}^{\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}}}\mathrm{Ei}\left(-\dfrac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}}\right)\right]\end{array}\right\}^+ \tag{25}$$

3.3 Ergodic Secrecy Capacity of x_{R} and ESSC of System

Since x_{R} is a ordinary data signal, and E only intercepts valuable and sensitive signals, the ergodic secrecy capacity of x_{R} is its ergodic capacity. Let $V_2 = \gamma_{2\to x_{\mathrm{R}}}$, CCDF of V_2 is as follows

$$\overline{F}_{V_2}(v_2) = \Pr\left(\frac{\left|h_{\mathrm{R}_k 2}\right|^2 a_1 P_{\mathrm{R}}}{\sigma_2^2} > v_2\right) = \mathrm{e}^{-\frac{v_2}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}a_1}} \tag{26}$$

According to [14, Eq. (3.352.4)], the ergodic secrecy capacity of x_{R} can be written as

$$\begin{aligned}\overline{C}_{\mathrm{ESC}}^{x_{\mathrm{R}}} &= \frac{1}{2}\int_0^\infty \log(1+v_1) f_{V_1}(v_1)dv_1 = \frac{1}{2\ln 2}\int_0^\infty \frac{1-F_{v_1}(v_1)}{1+v_1}dv_1 \\ &= -\frac{1}{2\ln 2}\mathrm{e}^{\frac{1}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}a_1}}\mathrm{Ei}\left(-\frac{1}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}a_1}\right)\end{aligned} \tag{27}$$

So the ESSC of system is approximated as

$$\begin{aligned}\overline{C}_{\mathrm{ESSC,lb}} = \overline{C}_{\mathrm{ESC,lb}}^{x_{\mathrm{R}}} + \overline{C}_{\mathrm{ESC,lb}}^{x_1} + \overline{C}_{\mathrm{ESC,lb}}^{x_2} &\approx -\frac{1}{2\ln 2}\mathrm{e}^{\frac{1}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}a_1}}\mathrm{Ei}\left(-\frac{1}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}a_1}\right) \\ &+\left\{\frac{\pi^2}{8L_1\ln 2}\sum_{i=1}^{L_1}\frac{\lambda_{\mathrm{S1}}a_1\gamma_{\mathrm{S}}\sqrt{1-\theta_i}\sec^2\theta_i}{(\lambda_{\mathrm{S1}}a_1\gamma_{\mathrm{S}}+\lambda_{\mathrm{E1}}\gamma_{\mathrm{J}}\tan\theta_i)(1+\tan\theta_i)}\mathrm{e}^{-\frac{\tan\theta_i}{\lambda_{\mathrm{S1}}a_1\gamma_{\mathrm{S}}}}\right\}^+ \\ &+\frac{1}{2\ln 2}\left\{\begin{array}{l}\dfrac{\pi}{L_2}\displaystyle\sum_{i=1}^{L_2}\frac{\lambda_{\mathrm{S1}}\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}^2 a_1^2 a_2 N(1-x_i)^2\sqrt{1-y_i^2}\times \mathrm{e}^{-\left(\frac{1}{\lambda_{\mathrm{S1}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{SR}}\gamma_{\mathrm{S}}}+\frac{1}{\lambda_{\mathrm{R2}}\gamma_{\mathrm{R}}}\right)\frac{(1+x_i)}{a_1(1-x_i)}}}{A(x_i)} \\ -\left[\mathrm{e}^{\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}a_1}}\mathrm{Ei}\left(-\dfrac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}a_1}\right)-\mathrm{e}^{\frac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}}}\mathrm{Ei}\left(-\dfrac{N}{\lambda_{\mathrm{RE}}\gamma_{\mathrm{R}}}\right)\right]\end{array}\right\}^+\end{aligned} \tag{28}$$

4 Numerical Analysis

In this section, we will evaluate the performance of our proposed D2D-NOMA system in terms of ESSC under the user selection scheme through simulation. The relevant parameter settings in the simulation are as follows: $L_1 = L_2 = 100$, legal channel parameters $\lambda_{S1} = \lambda_{SR} = 1$, $\lambda_{R2} = 2$, in order to avoid being discovered, the eavesdropper is far away from the legal nodes, so $\lambda_{RE} = \lambda_{E1} = 0.1$. If there is no special instructions, we set $\gamma_S = \gamma_R = 30\,\text{dB}$, $a_1 = 0.2$, $a_2 = 0.8$ and $N = 10$. Similarly, due to the need for concealment, $\gamma_J = 5\,\text{dB}$. The number of Monte Carlo simulations is 1,000,000.

For comparison, we consider the following benchmark schemes in the simulation.

(1) Benchmark scheme 1 is a multi-relay user cooperative NOMA scheme, in which the number of relay users is $N = 10$. In the first time slot, S broadcast superimposed signal $\sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2$, at the same time the eavesdropper transmits interference signals $\sqrt{P_J} x_J$. In the second time slot, the selected relay forward the signal x_2 with the transmit power P_R, and E switches to eavesdropping mode.

(2) Benchmark scheme 2 is a single-relay user cooperative NOMA scheme, in which the number of relay users is $N = 1$. In first time slot, S broadcast superimposed signal $\sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2$, and the eavesdropper transmits interference signals $\sqrt{P_J} x_J$. In the second time slot, relay user forwards signal $\sqrt{a_1 P_R} x_R + \sqrt{a_2 P_J} x_2$, and E switches to eavesdropping mode.

Figure 2 shows the relationship between the number of relay users and the system ESSC under different power allocation factors. As shown in Fig. 1, as the number of

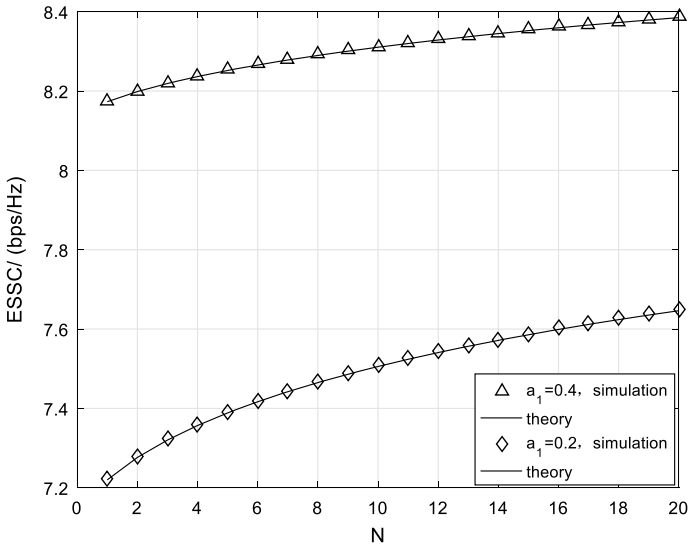

Fig. 2 The effect of N on system ESSC with different power allocation factors

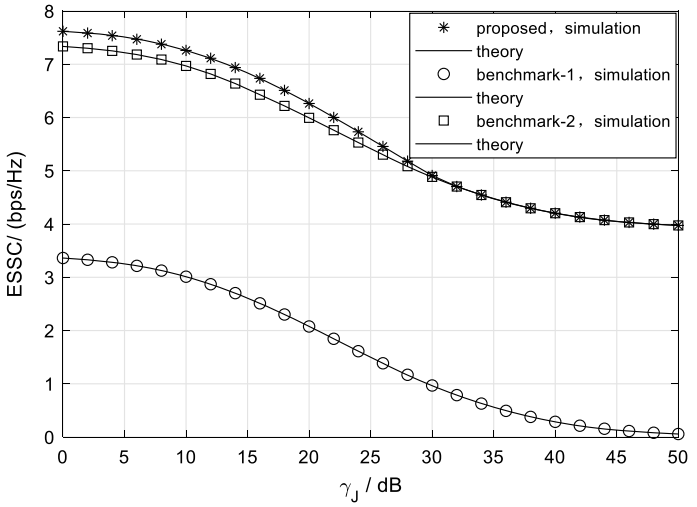

Fig. 3 The effect of γ_J on system ESSC with different transmission schemes

relay users increases, the ESSC of the system increases monotonically, and compared to $a_1 = 0.4$, the number of relay users has a greater impact on the system ESSC when $a_1 = 0.2$. It can also be observed from the figure, secrecy performance of the system when $a_1 = 0.4$ is better than that of the system when $a_1 = 0.2$. This is because there is more power allocated to x_1 and x_R when $a_1 = 0.4$, which is beneficial for D_1 to resist the interference attack of E, furthermore the eavesdropper does not eavesdrop on the ordinary data signals x_R.

Figure 3 simulates the influence of the eavesdropper's transmitted SINR on the system ESSC. The simulation shows that the security performance of the proposed scheme is better than that of Benchmark scheme 1 and Benchmark scheme 2, and the performance gap between the proposed scheme and Benchmark scheme 1 is more obvious. It implies that it is of great significance to design a secure communication scheme based on the differences in user experience requirements for information security services. In addition, it can also be observed that the ESSC of the proposed scheme and Benchmark scheme 2 tend to a positive definite value in the high SIR, this is because the transmission of x_R occurs in the second time slot, so it will not be affected by the interference of E. By comparing the curves of Monte Carlo simulation and theoretical analysis, it can be found that the two basically overlap, reflecting the accuracy of the numerical calculation.

5 Conclusions

This paper combines user selection technology with D2D technology to design a NOMA communication scheme against intelligent eavesdropping, and derives the expression of the ESSC lower bound of the proposed scheme. Theoretical derivation and simulation show that the proposed scheme is better than the two Benchmark schemes. The communication system can take advantage of the differences in information security service experience requirements of each user to alleviate communication congestion and improve the overall security performance. In addition, by increasing the number of relay users, the security of information transmission can be further ensured.

References

1. Wang, G., Xu, X., Zhou, R., Zhang, R.: Power domain non-orthogonal multiple access technology for wireless communication. Radio Commun. Technol. **45**(4), 329–336 (2019)
2. Ding, Z., Peng, M., Poor, H.: Cooperative non-orthogonal multiple access in 5G systems. IEEE Commun. Lett. **19**(8), 1462–1465 (2015)
3. Wan, D., Wen, M., Ji, F., Liu, Y., Huang, Y.: Cooperative NOMA systems with partial channel state information over Nakagami-m fading channels. IEEE Trans. Commun. **66**(3), 947–958 (2018)
4. Kim, J., Lee, I., Lee, J.: Capacity scaling for D2D aided cooperative relaying systems using NOMA. IEEE Commun. Lett. **7**(1), 42–45 (2018)
5. Ji, Y., Wen, M., Padidar, P., Duan, W., Li, J., Cheng, N., Ho, P.: Spectral efficiency enhanced cooperative device-to-device systems with NOMA. IEEE Trans. Intell. Transp. Syst. **22**(7), 4040–4050 (2021)
6. Duan, W., Ji, Y., Hou, J., Zhuo, B., Wen, M., Zhang, G.: Partial-DF full-duplex D2D-NOMA systems for IoT with/without an eavesdropper. IEEE Internet Things J. **8**(8), 6154–6166 (2021)
7. Zou, Y., Zhu, J., Wang, X., Hanzo, L.: A survey on wireless security: technical challenges, recent advances, and future trends. Proc. IEEE **104**(9), 1727–1756 (2016)
8. Yang, L., Chen, J., Jiang, H., Vorobyov, S., Zhang, H.: Optimal relay selection for secure cooperative communications with an adaptive eavesdropper. IEEE Trans. Wireless Commun. **16**(1), 26–42 (2017)
9. Lee, K., Hong, J., Choi, H., Levorato, M.: Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication. IEEE Internet Things J. **5**(4), 2793–2803 (2018)
10. Cao, Y., Zhao, N., Pan, G., Chen, Y., Fan, L., Jin, M., Alouini, M.: Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay. IEEE Trans. Commun. **67**(8), 5574–5587 (2019)
11. Bletsas, A., Shin, H., Win, M.: Cooperative communications with outage-optimal opportunistic relaying. IEEE Trans. Wireless Commun. **6**(9), 3450–3460 (2007)
12. Shim, K., Do, T., Nguyen, T., Costa, D., An, B.: Enhancing PHY-security of FD-enabled NOMA systems using Jamming and user selection: performance analysis and DNN evaluation. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2021.3080425
13. Abramowitz, M., Stegun, I.: Handbook Mathematical Functions with Formulas, Graphs, Mathematical Tables. New York, NY , USA, Dover (1972)
14. Gradshteyn, I., Ryzhik, I.: Table of Integrals, Series and Products, 7th edn. NY, USA, Academic, New York (2007)