TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214
DOI: 10.26599/TST.2023.9010128

Physical Layer Security for CR-NOMA Network with Cooperative Jamming

Meiling Li*[1],Peng Xue[1],Hu Yuan[2],Yuxing Han[3]

1. Taiyuan University of Science and Technology,Taiyuan 030024, China 2. University of Kingston, KT1 2EE, UK 3. Shenzhen International Graduate Shool, Tsinghua University, Shenzhen 518055, China

Abstract: Cooperative jamming can effectively combat eavesdropping in physical layer security communication without affecting the legal receiver and improve the security performance of the system. This paper introduces cooperative jamming to cognitive radio (CR) networks with non-orthogonal multiple access (NOMA) technology. The secure performance of the considered NOMA and CR (CR-NOMA) network is evaluated using two modes: non-cooperative jamming and cooperative jamming. In particular, the secrecy outage probabilities (SOPs) of the primary user (PU) in the two modes are derived under Rician fading channels, based on which, the influence of the transmission signal-to-noise ratio (SNR) of secondary users (SUs), the number of SUs, the secrecy rate and the power allocation coefficient on the SOPs of PU are analyzed thereafter. Both analysis and simulation results show that cooperative jamming effectively prevents eavesdropping behaviour, which reduces the SOP of PU compared to non-cooperative jamming. We also show that the transmit SNR, the number of SUs, the secrecy rate and the power distribution coefficients greatly influence performance improvement.

Key words: Cognitive radio, non-orthogonal multiple access, physical layer security, cooperative jamming.

1 Introduction

According to the initial deployment stages, fifth generation (5G) wireless networks have achieved a significant data rate enhancement and close-to-boundary spectral efficiency, by enabling massive multiple-input multiple-output (MIMO), network densification, and mmWave communications [1]. Compared to 5G networks, it is envisioned that emerging technologies in the sixth generation (6G) networks will provide enhanced services with reduced cost and improved energy efficiency, intelligence, security, privacy, secrecy, and reconfigurability [2]. In this context, non-orthogonal multiple access (NOMA) and cognitive radio (CR) are considered as key enabling technologies for 5G wireless networks, which are capable of providing enhanced connectivity, data rate, and spectral and energy efficiency. The core idea of NOMA and CR schemes is to achieve an efficient spectrum sharing between multiple users within a resource block [3]. It is worth noting that NOMA and CR networks are strong candidates for future 6G networks.

Spectral and energy efficiency enhancement in NOMA can be achieved by enabling superposition coding, where multiple users are permitted to share the same time and frequency resources simultaneously

Received date: 27-Oct-2023; accepted date: 29-Oct-2023

∗ Supported by NSFC (62001320), the project of National Overseas Study Fund Committee, Central government funds for guiding local scientific and technological development of ShanXi (YDZJSX2021A037), Shanxi Province Science and Technology achievement transformation guidance special project (202204021301055), Project for Patent transformation of Shanxi under Grant (202302003), Research Project Supported by Shanxi Scholarship Council of China (2021-133).

∗ To whom correspondence should be addressed.
E-mail: meilingli@tyust.edu.cn;

[1]. On the other hand, CR networks improve spectrum utilization through dynamic spectrum access under the premise of coexistence of unlicensed and licensed users. Spectrum access of unlicensed users is coordinated based on different protocols, namely, overlay, underlay, and interweave [4]. The integration of NOMA and CR networks has been widely considered in the literature, as a prominent solution to improve the overall network throughput.

1.1 Related Work

Motivated by the advantages brought by NOMA-enabled CR networks, considerable research efforts were devoted to investigate such networks. In particular, the authors in [5] analyzed the performance CR-NOMA networks, where multicast secondary users (SUs) are utilized as relays, in order to improve the outage performance of both primary and secondary networks. In [6], the outage probability of cooperative underlay NOMA-enabled CR networks with imperfect CSI was studied. The obtained results showed that the outage performance of CR-NOMA outperforms CR-orthogonal multiple access (OMA). Furthermore, the authors in [7] proposed primary user (PU) priority decoding mode and SU priority decoding mode in NOMA-enabled CR system, and analyzed the two modes in terms of throughput. Additionally, in [8], the authors investigated the outage performance of NOMA-enabled CR networks under two relaying modes, namely, decode-and forward (DF) and amplify-and-forward (AF). Several other contributions in the open literature have considered investigating the integration of NOMA and CR networks, under different system models and practical scenarios, e.g. [9, 10].

In actual Internet of Things (IoT) communications for example, traditional cryptographic techniques may result in high latency, which cannot satisfy the stringent latency requirement. As a result, it is of great challenge to realise the security by the traditional signalling process, which makes it difficult to satisfy the requirement for such dynamic and complex cognitive environment by traditional cryptography techniques. This motivates the shift towards more secure and robust approaches, which are independent of the computational complexity. Physical layer security (PLS) is a low complexity approach to provide security to the users by utilising the dynamic properties of wireless communication [11–13], which is more suitable to solve the secure transmission for a heterogeneous network.

Recently, there have been a lot of research on PLS-NOMA [14–17]. The authors in [14] investigate the PLS performance by applying NOMA in a large-scale networks. Furthermore, the authors in [15] investigate the impact of PLS on the performance of a unified NOMA framework. The authors in [16, 17] also investigate the PLS performance for NOMA network in different metrics.

Further, there have been considerable research efforts on the application PLS schemes in NOMA-enabled CR networks. The considered CR architectures primarily include underlay, overlay, and interweave based NOMA networks [9]. Concurrent primary and secondary transmissions are permitted in the first scenario, provided that interference on the primary network is kept below a manageable level. In the second scenario, a SU provides relaying services to the primary network while also transmitting its own signal, which also referred as cooperative CR-NOMA. As a reward, the SU can send its own signal simultaneously using the NOMA principle. In the third scenario, a SU can transmit only when no PU occupies the licensed spectrum [18]. To this end, our paper focus on the second scenario, which has been investigated in [19–24]. Specifically, The authors in [19] considered a cooperative cognitive millimeter wave NOMA networks, in which the primary user and the secondary user are served by a base station. They analyzed the connection outage probability (COP), secrecy outage probabilities (SOP), and secrecy throughput. The authors in [20] investigates PLS in an inspired CR-NOMA networks with multiple primary and secondary users, the NOMA transmission strategy was proposed to reduce mutual interference between signals and improve transmission security. The authors in [21] designed a secure transmission scheme in hybrid automatic repeat request assisted cognitive NOMA networks. The authors in [22–24] considered that a cognitive transmitter serves as a relay and assists primary/cognitive transmissions using the NOMA principle. In the context of NOMA-enabled underlay CR networks, the authors in [25] investigated the secrecy performance of a downlink wiretap system, as a way to improve spectrum utilization and connection reliability. Moreover, the authors in [20] assumed that SUs are intercepting the signals of PUs in NOMA-enabled CR networks. Therefore, they studied the outage probability, secrecy outage probability, and effective secrecy throughput of PUs over Nakagami-m channels. In [26], the authors proposed an artificial-noise-aided cooperative jamming scheme to enhance the security of the primary network in multiple-input single-output NOMA-enabled CR network, by utilizing simultaneous wireless information and power transfer. In [27], the authors propose a multi-antenna physical layer security technology that improves confidentiality performance by utilizing spatial degrees of freedom. The secrecy performance of CR-inspired NOMA network over Rayleigh fading channels were studied in [28], where jamming signals are transmitted from the base station to improve PLS. In specific, the authors in [28] considered that jamming signals are transmitted from the BS, and it should be decoded at the SUs. Furthermore, the total transmission power from the BS is divided between the information signals and jamming signals, yielding degraded performance. The power budget allocated to legitimate signals is further divided between secondary and primary users in order to realize NOMA. Also, during the second time slot, one of the SUs is selected to forward a superimposed message comprising the SU message, PU message and jamming signal with power divided between all signals.

To the best of authors' knowledge, there has little research on how to improve the PLS performance for the considered cooperative CR-NOMA networks by friendly jammers. Further, we consider Rician fading channels to evaluate the correlations between the channels, which is more applicable and interesting to describe the actual complex communication scenarios.

1.2 Contributions

Cooperative jamming is a prominent PLS scheme that has been extensively investigated in OMA systems [29, 30]. Motivated by this and the earlier discussion, in this paper, we investigate the PLS performance of the primary user in a cooperative CR-NOMA network with the existence of an eavesdropper and a cooperative jammer, which sends jamming signals to the PU and the eavesdropper. The detailed contributions are concluded as:

- The closed-form expressions of the SOP for the primary user under the two scenarios, i. e. with cooperative jammer and without jammer, are derived respectively over Rician fading channels, where the optimal SU is selected from multiple SUs who work at DF mode.
- We further derive the asymptotic SOP expressions to gain deep insights in the high SNR region for the considered cooperative CR-NOMA networks.
- We verify the analysis by simulations. We also compare the SOP performance with and without channel correlation under different SU number, which is reflected by Rician factor. The results clearly indicate that the better SOP performance can be obtained when the channel correlation is considered, no matter how much SUs exist, which benefits from the LoS link.
- We investigate the influence of the transmit power from SU and the jamming power on the SOP performance under the two scenarios. The results indicate that in these two scenarios, the performance of SOP improves as the SU transmission power increases. Furthermore, as the power of the jammer increases, the SOP performance in scenarios with jammers is significantly superior to that in the other scenario.
- We also investigate the effect of the transmit power from SU and the jamming power on the SOP performance under the power allocation coefficient. The results indicate that the overall system's SOP performance worsens with the power allocation coefficient increases. When the power allocation coefficient remains constant, the SOP is more significantly influenced by the SU transmitter power compared to the friendly jammer power.

2 System Model and Proposed Protocol

We consider a downlink NOMA-enabled CR network, which consists of a single base station (BS), N SUs, denoted by $SU_i = \{SU_1, SU_2, \cdots, SU_N\}$, a single PU and a single eavesdropper (E). Furthermore, we consider the existence of a cooperative jammer (J) in order to realize PLS. Fig. 1 depicts the adopted system model with the cooperative jammer. Among them, the communications between BS and SU are in broadcast mode, i.e. x_1 remains the same value for all SUs, and there is no channel link between BS and E. Furthermore, we assume that the SUs operate as DF relays to assist in data transmission between the BS and the PU. DF relays aims to provide services for both the remaining SU and PU simultaneously. For the sake of clarity, CR-NOMA-NCJ refers to the scenario where we don't have a jammer. On the other hand, CR-NOMA-CJ represents the system with a cooperative jammer, as shown in Fig. 1. Without loss of generality, we assume that the direct link between the BS and the PU is unavailable due to obstacles or shadowing effect.

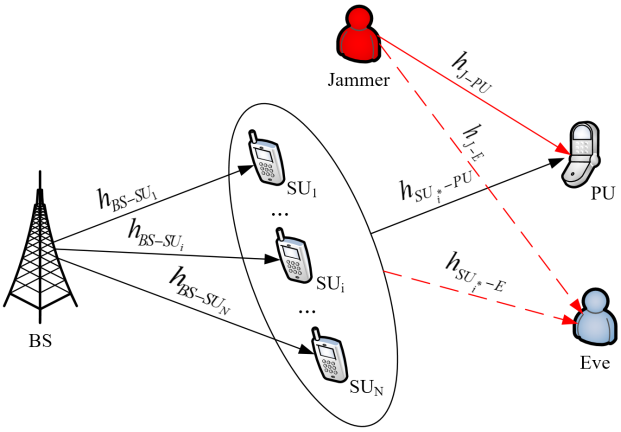


Fig. 1 CR-NOMA-CJ system.

In both scenarios, the BS broadcasts a superimposed signal to all SUs, which are divided into two sets, namely, D and $\bar{D}$. The classification of D and $\bar{D}$ is random and depends on the quality of the channel. SUs in D can successfully decode the superimposed signal, while SUs in $\bar{D}$ fail to successfully decode the superimposed signal. Therefore, SU_{i^*} is selected from D (if $D \neq \varnothing$) to re-encode and forward a new superimposed signal to the PU and SUs in $\bar{D}$ [18]. Simultaneously, in CR-NOMA-CJ scenario, node J broadcasts a jamming signal that is received by the PU and the eavesdropper. Due to the broadcast nature of the wireless channels, the message intended to the PU is intercepted by the eavesdropper. It is assumed that the PU has a prior knowledge of the jamming signal, thus, jamming signals can be canceled at the primary receiver. In this work, we consider that the instantaneous channel state information (CSI) of E and all legitimate users are available at the BS as well as node J. It is noted that this assumption can be used for the scenario that both PU and E are assumed to be beyond the coverage area of the BS as considered in [31]. However, there is further case in which PU and E are within the coverage of the same source node. In such a case, both PU and E will receive signals from SUs. Thus, the enhanced SINR for PU and E will be used for evaluating the SOP.

2.1 Signal Model

In this subsection, we present the signal models of CR-NOMA-NCJ and CR-NOMA-CJ systems.

For the two scenarios, in the first time slot, the BS sends superimposed signal including x_1 of PU and x_2 of SU to all SUs, which can be expressed as

$$x = \sqrt{\alpha_1 P} x_1 + \sqrt{\alpha_2 P} x_2, \tag{1}$$

where, P is the total transmit power at the BS, α_1 and α_2 are the power allocation coefficients of x_1 and x_2, respectively. Moreover, $\alpha_1 + \alpha_2 = 1$, $\alpha_1 > \alpha_2$ and $E\left[|x_1|^2\right] = E\left[|x_2|^2\right] = 1$. We assume that: 1) All nodes are equipped with a half-duplex single antenna; 2) Fading channel between any two nodes follows the Rician distribution; 3) The additive white gaussian noise (AWGN) variance equals to N_0 in all nodes.

Thus, the received signal at SU_i can be expressed as

$$y_{SU_i} = \sqrt{P} h_{BS-SU_i} \left(\sqrt{\alpha_1} x_1 + \sqrt{\alpha_2} x_2\right) + n_S. \tag{2}$$

where h_{BS-SU_i} denotes the channel gain between the BS and SU_i, and $n_S \sim \mathcal{CN}\left(0, N_0\right)$ is the AWGN received at SU_i.

SUs perform successive interference cancellation (SIC) process in order to decode x_1 first, which is intended to the PU, and then decode signal x_2. The signal-to-interference-plus-noise ratios (SINR) at SU_i to decode x_1 and x_2 can be obtained as

$$SINR_{SU}^{x_1} = \frac{\alpha_1 \rho |h_{BS-SU_i}|^2}{\alpha_2 \rho |h_{BS-SU_i}|^2 + 1}, \tag{3}$$

and

$$SINR_{SU}^{x_2} = \alpha_2 \rho |h_{BS-SU_i}|^2. \tag{4}$$

Also, $\rho = \frac{P}{N_0}$ represents the average transmit signal-to-noise ratio (SNR) at the BS.

In the following two subsections, we present the signal models at the second transmission phase for the two scenarios, CR-NOMA-NJC and CR-NOMA-CJ.

2.1.1 CR-NOMA-NCJ System

In the second time slot, SU_{i^*}, is selected from D to re-encode and forward a superimposed signal $\sqrt{\alpha_1 P_i} x_1 + \sqrt{\alpha_2 P_i} x_2$ to the PU and SUs in $\bar{D}$, where P_i is the average transmit power at SU_{i^*}. The received signal at the PU can be formulated as

$$y_{PU} = \sqrt{P_i} h_{SU_{i^*}-PU} \left(\sqrt{\alpha_1} x_1 + \sqrt{\alpha_2} x_2\right) + n_P, \tag{5}$$

where $h_{SU_{i^*}-PU}$ denotes the channel gain between SU_{i^*} and the PU, and $n_P \sim \mathcal{CN}\left(0, N_0\right)$ is the AWGN received at the PU.

During the second transmission, the eavesdropper intercept the transmitted data to the PU. Hence, the received signal at node E is given by

$$y_E = \sqrt{P_i} h_{SU_{i^*}-E} \left(\sqrt{\alpha_1} x_1 + \sqrt{\alpha_2} x_2\right) + n_E. \quad (6)$$

where $h_{SU_{i^*}-E}$ denotes the channel gain between SU_{i^*} and node E, and $n_E \sim \mathcal{CN}(0, N_0)$ is the AWGN received at node E.

The received SINR at the PU in the second time slot can be given as

$$SINR_{PU}^{x_1} = \frac{\alpha_1 \rho_i \left|h_{SU_{i^*}-PU}\right|^2}{\alpha_2 \rho_i \left|h_{SU_{i^*}-PU}\right|^2 + 1}, \quad (7)$$

where $\rho_i = \frac{P_i}{N_0}$ represents the average transmit SNR at SU_{i^*}.

The received SINR at node E in the second time slot can be given as

$$SINR_E^{x_1} = \frac{\alpha_1 \rho_i \left|h_{SU_{i^*}-E}\right|^2}{\alpha_2 \rho_i \left|h_{SU_{i^*}-E}\right|^2 + 1}. \quad (8)$$

Based on the SINR of each link in the second time slot, the mutual information between SU_{i^*} and the PU, SU_{i^*} and node E can be respectively expressed as

$$I_{PU} = \frac{1}{2} \log_2 \left(1 + SINR_{PU}^{x_1}\right), \quad (9)$$

and

$$I_E = \frac{1}{2} \log_2 \left(1 + SINR_E^{x_1}\right). \quad (10)$$

2.1.2 CR-NOMA-CJ System

Considering the presence of a CJ, in the second time slot, both the PU and E receive the superimposed signal $\sqrt{\alpha_1 P_i} x_1 + \sqrt{\alpha_2 P_i} x_2$ sent by SU_{i^*} and x_j sent by J. However, recalling that the PU has a prior knowledge of the jamming signal, the PU is able to cancel the effect of the jamming signal in order to perform reliable signal detection. Assuming that the transmit power P_j of J satisfies $P_j \ll P_i$. Consequently, after eliminating the jamming signal, the received signal of the PU in CR-NOMA-CJ system can be expressed by (5).

On the other hand, the received signal at node E is given by

$$\begin{aligned} y_E^J = &\sqrt{P_i} h_{SU_{i^*}-E} \left(\sqrt{\alpha_1} x_1 + \sqrt{\alpha_2} x_2\right) \\ &+ \sqrt{P_j} h_{J-E} x_j + n_E, \end{aligned} \quad (11)$$

where h_{J-E} denotes the channel gain between node J and node E.

Hence, the received SINR at node E is given by

$$SINR_E^{J,x_1} = \frac{\alpha_1 \rho_i |h_{SU_{i^*}-E}|^2}{\alpha_2 \rho_i |h_{SU_{i^*}-E}|^2 + \rho_j |h_{J-E}|^2 + 1}, \quad (12)$$

where $\rho_j = \frac{P_j}{N_0}$ represents the average transmit SNR at J.

The mutual information between SU_{i^*} and node E can be represented as

$$I_E^J = \frac{1}{2} \log_2 \left(1 + SINR_E^{J,x_1}\right). \quad (13)$$

2.2 Optimal SU Selection Scheme

Based on CR-NOMA-NCJ and CR-NOMA-CJ systems considered in Fig.1 , all SUs that successfully decode the signal of BS will be eligible to forward the signal to the PU. Because the wireless channels are affected by shadow and fading, the performance of the systems are different by choosing different SU. The system model considered in this paper is that cognitive users can exchange their own communication by helping the primary user transmit. The maximization and minimization method is adopted [18]. Specifically, we firstly select the weakest link between SU_i and SU_l, where SU_i belongs to D and SU_l belongs to $\bar{D}$, to form a subset. Then, we select SU_{i^*} from D to let the channel difference between cognitive transmission link and eavesdropping link is the largest. The proposed optimal SU selection scheme can be described as

$$SU_{i^*} = \arg \max_{i \in D} \left\{ \min_{l \in \bar{D}} \left\{ \left|h_{SU_i - SU_l}\right|^2 \right\} - \left|h_{SU_i - E}\right|^2 \right\}. \quad (14)$$

where $h_{SU_i - SU_l}$ is the channel gain between SU_i and SU_l, $h_{SU_i - E}$ is the channel gain between SU_i and E.

3 Secrecy Performance Analysis

In this work, we analyze the SOP in order to investigate the secrecy performance of the two scenarios.

3.1 SOP of CR-NOMA-NCJ System

Utilizing (9) and (10), the secrecy capacity of the PU in CR-NOMA-NCJ scenario can be defined as

$$R_{SEC} = \left[I_{PU} - I_E\right]^+. \quad (15)$$

where $[x]^+ = \max\{x, 0\}$.

Note that, in the first time slot, the outage event occurs at the PU when the selected SU cannot successfully decode the superimposed signal sent by the BS, *i.e.*, D=∅. On the other hand, in the second time slot, the PU will be in an outage if its secrecy capacity falls below a certain threshold value, *i.e.*, $R_{SEC} < R_{th}$, where $R_{th} \geq 0$. Hence, the SOP of the PU in CR-

$$\Pr\left(D=\varnothing\right)=\prod_{i=1}^{N}\left[\Pr\left(\frac{\alpha_1{|h_{BS-SU_i}|}^2}{\alpha_2{|h_{BS-SU_i}|}^2+\frac{1}{\rho}}<\xi_p\right)+\Pr\left(\frac{\alpha_1{|h_{BS-SU_i}|}^2}{\alpha_2{|h_{BS-SU_i}|}^2+\frac{1}{\rho}}>\xi_p,\alpha_2\rho{|h_{BS-SU_i}|}^2<\xi_s\right)\right]. \tag{20}$$

NOMA-NCJ system is given by

$$\begin{aligned} P_{OUT}=&\Pr\left(D=\varnothing\right)\\ &+\sum_{k=1}^{2^N-1}\Pr\left(D=D_k,R_{SEC}<R_{th}\right), \end{aligned} \tag{16}$$

where $D=D_k$ represents the decoding set, and k represents the combination of all SU sets.

Recalling that SUs perform SIC in order to detect x_1 and x_2, the probability that the SUs cannot successfully detect x_1 and the probability that certain SUs can successfully detect x_1 but cannot successfully detect x_2 can be evaluated as shown in (20), where $\xi_p=2^{2R_{PU}}-1$, $\xi_s=2^{2R_{SU}}-1$, R_{SU} and R_{PU} denotes the targeted secrecy rates of the SU and PU, respectively.

Given that, all channels are Rician distributed, then ${|h|}^2$ follows the exponential distribution with probability density function (PDF) given by [32]

$$f_{|h|^2}\left(x\right)=\frac{\left(K+1\right)e^{-\frac{(x-\lambda)K+x}{\lambda}}}{\lambda}I_0\left(2\sqrt{\frac{K\left(K+1\right)x}{\lambda}}\right), \tag{17}$$

where λ is the channel variance. K is the Rician K-factor defifined as the ratio of the power of the line-of-sight component to the separate components and $I_0\left(\cdot\right)$ denotes the zeroth-order modifified Bessel function of the first kind. $(\cdot)!$ is the factorial. Using [33], the PDF of the Rician channels can be rewritten as

$$f_{|h|}\left(x\right)=\sum_{l=0}^{\infty}\frac{\left(K+1\right)x^le^{-\frac{(x-\lambda)K+x}{\lambda}}}{{(l!)}^2\lambda}{\left(\frac{K\left(K+1\right)}{\lambda}\right)}^l, \tag{18}$$

Utilizing (18), (20), [34, eq.(3.381.1)] can be further evaluated as

$$\begin{aligned} \Pr\left(D=\emptyset\right)=&\sum_{a=0}^{\infty}\sum_{b=0}^{a}\prod_{i=1}^{N}\frac{K^{2a+1}{(K+1)}^{2a+2}e^{-K}}{a!\lambda_{BS-SU_i}^{2a+2}}\\ &\times\left(1-\frac{{Q_1}^be^{Q_1}}{b!}\right), \end{aligned} \tag{19}$$

where $\beta=\max\left(\frac{\xi_p}{(\alpha_1-\alpha_2\xi_p)},\frac{\xi_s}{\alpha_2}\right)$ and $Q_1=\frac{(K+1)\beta}{\rho\lambda_{BS-SU_i}^2}$.

As the event that SU_i successfully detects the superimposed signal is independent with the event that the secrecy capacity falls below a certain threshold value. We have $\Pr\left(D=D_k,R_{SEC}<R_{th}\right)=\Pr\left(D=D_k\right)\Pr\left(R_{SEC}<R_{th}\right)$. $\Pr\left(D=D_k\right)$ and can be given by

$$\begin{aligned} \Pr\left(D=D_k\right)=&\sum_{a_1=0}^{\infty}\sum_{b_1=0}^{a_1}\sum_{a_2=0}^{\infty}\sum_{b_2=0}^{a_2}\prod_{i=1}^{N}\prod_{l=1}^{N}\frac{e^{-2K}}{a_2!a_1!}\\ &\times\frac{{(K+1)}^{2(a_1+a_2+2)}K^{2(a_1+a_2+1)}}{\lambda_{BS-SU_l}^{2a_2+2}\lambda_{BS-SU_i}^{2a_1+2}}\\ &\times\left(1-\frac{{Q_1}^be^{Q_1}}{b_1!}\right)\left(1-\frac{{Q_2}^be^{Q_1}}{b_2!}\right), \end{aligned} \tag{21}$$

Letting $X=\frac{\alpha_1\rho_i{\left|h_{SU_i-PU}\right|}^2}{\alpha_2\rho_i{\left|h_{SU_i-PU}\right|}^2+1}$ and $Y=\frac{\alpha_1\rho_i{\left|h_{SU_i-E}\right|}^2}{\alpha_2\rho_i{\left|h_{SU_i-E}\right|}^2+1}$, $\Pr\left(R_{SEC}<R_{th}\right)$ can be given by

$$\begin{aligned} &\Pr\left(R_{SEC}<R_{th}\right)=\Pr\left(I_{PU}-I_E<R_{th}\right)\\ &=\Pr\left(\frac{1+SINR_{PU}^{x_1}}{1+SINR_E^{x_1}}<2^{2R_{th}}\right)\\ &=\sum_{i\in D_k}\Pr\left(i^*=i\right)\Pr\left(\frac{1+SINR_{PU}^{x_1}}{1+SINR_E^{x_1}}<2^{2R_{th}}\left|i^*=i\right.\right)\\ &=\sum_{i\in D_k}\Pr\left(i^*=i\right)\int_0^\infty\int_0^{\delta+\delta y-1}f\left(x\right)f\left(y\right)dxdy, \end{aligned} \tag{22}$$

where $Q_2=\frac{(K+1)\beta}{\rho\lambda_{BS-SU_l}^2}$ and $\delta=2^{2R_{th}}$. In order to solve (22), we first need to present the PDF of X and Y according to (17) as

$$\begin{aligned} f\left(x\right)=&\sum_{c_1=0}^{\infty}\sum_{d_1=0}^{c_1}\frac{K^{d_1}{(K+1)}^{d_1+1}e^{-\frac{K(K+1)x}{(\alpha_1\rho_i-\alpha_1\rho_ix)\lambda_{SU_i-PU}}}}{e^K{\left(\alpha_1\rho_i-\alpha_1\rho_ix\right)}^{d_1+1}\lambda_{SU_i-PU}^{d_1+1}d_1!c_1!}\\ &\times\left(\frac{K\left(K+1\right)x^{d_1}}{\lambda_{SU_i-PU}}-d_1{(\alpha_1\rho_i)}^{d_1}\right), \end{aligned} \tag{23}$$

$$\begin{aligned} f\left(y\right)=&\sum_{c_2=0}^{\infty}\sum_{d_2=0}^{c_2}\frac{K^{d_1}{(K+1)}^{d_1+1}e^{-\frac{K(K+1)y}{(\alpha_1\rho_i-\alpha_2\rho_iy)\lambda_{SU_i-E}}}}{e^K{\left(\alpha_1\rho_i-\alpha_2\rho_iy\right)}^{d_1+1}\lambda_{SU_i-E}^{d_1+1}d_2!c_2!}\\ &\times\left(\frac{K\left(K+1\right)x^{d_2}}{\lambda_{SU_i-E}}-d_1{(\alpha_1\rho_i)}^{d_2}\right). \end{aligned} \tag{24}$$

According to (16), (19), (21) and (25), the SOP of the PU of CR-NOMA-NCJ system can be rewritten as (26) shown at the bottom of this page. As it is difficult to obtain the closed-form expression of $\int_0^\infty A\left(y\right)dy$, Using the Gauss-Laguerre (GL) quadrature, and performing some further mathematical manipulations the result can be approximated as in (25), we resorted to numerical evaluation in order to get the final results. $\int_0^\infty A\left(y\right)e^{-y}dy \approx \sum\limits_{v=1}^{V} e^{y}\omega_v A\left(y_v\right)$. With ω_v and y_v are the weight and the points of GL quadrature, respectively, while V is a complexity-vs-accuracy tradeoff parameter of such a method [35]. Where $A\left(y\right) = \frac{\left(\frac{K(K+1)(\delta+\delta y-1)^{d_1}}{\lambda_{SU_i-PU}} - d_1(\alpha_1\rho_i)^{d_1}\right)}{(\alpha_1\rho_i(2-\delta-\delta y))^{d_1+1}\lambda_{SU_i-PU}^2} e^{-\frac{K(K+1)(\delta+\delta y-1)}{(\alpha_1\rho_i(2-\delta-\delta y))\lambda_{SU_i-PU}}}$.

Further, by substituting (23) and (24) into (22), we obtain $\Pr\left(R_{SEC} < R_{th}\right)$ in (25) shown at the bottom of previous page. Due to the intractability of (26) and (25), we resorted to numerical evaluation in order to get the final results.

Lemma 1 The SOP of CR-NOMA-NCJ system is expressed in (26). Also, for the optimal relay selection scheme discussed in Subsection 2.2, the expression for $\Pr\left(i^* = i\right)$ in (26) is given in Appendix A.

3.2 SOP of CR-NOMA-CJ System

According to (9) and (13), the secrecy capacity of the PU of CR-NOMA-CJ can be defined by

$$R_{SEC}^{J} = \left[I_{PU} - I_{E}^{J}\right]^{+}. \tag{27}$$

The SOP of the PU of CR-NOMA-CJ system is given by

$$\begin{aligned} P_{OUT}^{J} =& \Pr\left(D = \emptyset\right) \\ &+ \sum_{k=1}^{N} C_n^k \Pr\left(D = D_k\right) \Pr\left(R_{SEC}^{J} < R_{th}\right), \end{aligned} \tag{28}$$

Letting $Z = \alpha_1\rho_i{\left|h_{SU_i-E}\right|}^2/(\alpha_2\rho_i{\left|h_{SU_i-E}\right|}^2 + \rho_j {\left|h_{J-E}\right|}^2 + 1)$, $\Pr\left(R_{SEC}^{J} < R_{th}\right)$ can be expressed as

$$\begin{aligned} &\Pr\left(R_{SEC}^{J} < R_{th}\right) = \Pr\left(I_{PU} - I_{E}^{J} < R_{th}\right) \\ &= \sum_{i\in D_k} \Pr\left(i^* = i\right) \Pr\left(\frac{1 + SINR_{PU}^{x_1}}{1 + SINR_{E}^{J,x_1}} < 2^{2R_{th}} \middle| i^* = i\right) \\ &= \sum_{i\in D_k} \Pr\left(i^* = i\right) \int_0^\infty \int_0^{\delta+\delta z-1} f\left(x\right) f\left(z\right) dxdz. \end{aligned} \tag{29}$$

PDF of Z is given by

$$\begin{aligned} f\left(z\right) =& \sum_{c_3=0}^{\infty} \sum_{c_4=0}^{\infty} \sum_{m=0}^{c_3} C_m^{c_3} (K+1)^{c_3+c_4+2} K^{c_3+c_4} \\ &\times \frac{\zeta^{-(a+m+1)}{(\rho_j)}^m e^{-\frac{K(K+1)z}{(\alpha_1\rho_i-\alpha_2\rho_i z)\lambda_{SU_i-E}}} e^{-2K}}{\lambda_{SU_i-E}^{c_3+1}\lambda_{J-E}^{c_4+1}} \\ &\times \gamma\left(c_4 + m + 1, \frac{\zeta\alpha_1}{\alpha_2}\right) \left(\frac{z}{\alpha_1\rho_i - \alpha_2\rho_i z}\right)^{c_3}. \end{aligned} \tag{30}$$

where $\zeta = \frac{K(K+1)\left(\rho_j z\lambda_{J-E} + \lambda_{SU_i-E}\right)}{(\alpha_1\rho_i-\alpha_2\rho_i z)\lambda_{J-E}\lambda_{SU_i-E}}$, $\gamma\left(\cdot\right)$ represents an incomplete lower gamma function.

By substituting (23) and (30) into (29), we obtain $\Pr\left(R_{SEC}^{J} < R_{th}\right)$ in (31) shown at the bottom of next page.

According to (19), (21), (28) and (31), the SOP of

$$\begin{aligned} \Pr\left(R_{SEC} < R_{th}\right) =& \sum_{i\in D_k} \sum_{c_1=0}^{\infty} \sum_{d_1=0}^{c_1} \sum_{v=1}^{V} \frac{K^{d_1}(K+1)^{d_1+1} e^{-(K-y_v)}\omega_v f(y_v)}{\lambda_{SU_i-PU}^2 \lambda_{SU_i-PU}^{d_1-1} d_1! c_1!} \\ &\times \Pr\left(i^* = i\right) \frac{\left(K\left(K+1\right)\left(\delta + \delta y_v - 1\right)^{d_2} - d_1(\alpha_1\rho_i)^{d_2}\lambda_{SU_i-PU}\right) e^{-\frac{K(K+1)(\delta+\delta y_v-1)}{(\alpha_1\rho_i-\alpha_1\rho_i(\delta+\delta y_v-1))\lambda_{SU_i-PU}}}}{\lambda_{SU_i-PU}(\alpha_1\rho_i - \alpha_1\rho_i\left(\delta + \delta y_v - 1\right))^{d_2+1}}, \end{aligned} \tag{25}$$

$$\begin{aligned} P_{OUT} =& \sum_{a=0}^{\infty}\sum_{b=0}^{a}\prod_{i=1}^{N} \frac{K^{2a+1}(K+1)^{2a+2}e^{-K}\left(1 - \frac{{Q_1}^b e^{Q_1}}{b!}\right)}{a!\lambda_{BS-SU_i}^{2a+2}} + \sum_{K=1}^{N} \sum_{a_1=0}^{\infty} \sum_{b_1=0}^{a_1} \sum_{a_2=0}^{\infty} \sum_{b_2=0}^{a_2} \sum_{i\in D_k} \sum_{c_1=0}^{\infty} \sum_{d_1=0}^{c_1} \sum_{v=1}^{V} \prod_{i=1}^{N} \prod_{l=1}^{N} C_n^k \\ &\times \frac{K^{2(a_1+a_2+1)+d_1}(K+1)^{2(a_1+a_2)+d_1+5} e^{-3K}\left(1 - \frac{e^{Q_1}{Q_1}^{b_1}}{b_1!}\right)\left(1 - \frac{e^{Q_1}{Q_2}^{b_2}}{b_2!}\right) e^{y_v}\omega_v f(y_v)}{\lambda_{BS-SU_l}^{2a_2+2}\lambda_{BS-SU_i}^{2a_1+2}\lambda_{SU_i-PU}^{d_1-1} a_2! a_1! d_1! c_1!} \\ &\times \Pr\left(i^* = i\right) \frac{\left(\frac{K(K+1)(\delta+\delta y_v-1)^{d_1}}{\lambda_{SU_i-PU}} - d_1(\alpha_1\rho_i)^{d_1}\right) e^{-\frac{K(K+1)(\delta+\delta y_v-1)}{(\alpha_1\rho_i-\alpha_1\rho_i(\delta+\delta y_v-1))\lambda_{SU_i-PU}}}}{(\alpha_1\rho_i - \alpha_1\rho_i\left(\delta + \delta y_v - 1\right))^{d_1+1}\lambda_{SU_i-PU}^2}. \end{aligned} \tag{26}$$

the PU of CR-NOMA-CJ system becomes (32) shown at the bottom of this page. Due to the intractability of (32), we resorted to numerical evaluation in order to get the final result.

3.3 Asymptotic Analysis

This section aims to investigate the asymptotic performance of secrecy outage probability in the considered system, offering deeper insights into the system's performance in high signal-to-noise ratio (SNR) scenarios. By letting ($\rho_1 = \rho_2 = \rho$), the asymptotic performance is investigated as the SNR is sufficiently high, i.e., ($\rho \to \infty$). When $x \to 0$, $e^{(-x)} \approx 1 - x$ and $\frac{ax+b}{cx+d} \approx \frac{a}{c}$, then in the high SNR range, the asymptotic of the PU can be written as

$$\begin{aligned} P_{OUT}^{J,\infty} \approx & \sum_{K=1}^{N} \sum_{a_1=0}^{\infty} \sum_{a_2=0}^{\infty} \sum_{c_1=0}^{\infty} \sum_{d_1=0}^{c_1} \sum_{c_3=0}^{\infty} \sum_{c_4=0}^{\infty} \sum_{m=0}^{c_3} \sum_{i \in D_k} \prod_{i=1}^{N} \prod_{l=1}^{N} \\ & \times -\frac{C_n^k C_m^{c_3} e^{-4K} d_1 (\alpha_1 \rho_i)^{d_1} (\rho_j)^m}{a_1! a_2! \lambda_{BS-SU_l}^{2(a_2+1)} \lambda_{BS-SU_i}^{2(a_1+1)}} \\ & \times \frac{K^{2(a_1+a_2+1)+c_3+c_4} (K+1)^{2(a_1+a_2+3)+c_3+c_4}}{\lambda_{SU_i-E}^{c_3+1} \lambda_{J-E}^{c_4+1}} \\ & \times \Pr(i^* = i) \gamma(c_4 + m + 1, 0) . \end{aligned} \tag{33}$$

4 Numerical Results

This section provides simulation results by MATLAB to verify the above analysis, thereby it gives a reference to the actual system design. Unless otherwise stated, default values for simulation parameters have the following settings: transmit SNRs are $\rho = \rho_i = \rho_j = 10$ dB; the channel fading parameters are $\lambda_{BS-SU_i} = \lambda_{SU_i-PU} = 1$, $\lambda_{SU_i-E} = 0.01$, $\lambda_{J-E} = 0.5$; the target secrecy rates are $R_{SU} = 0.5$ bps/Hz, $R_{PU} = 0.1$ bps/Hz; the secrecy rate of PU is $R_{th} = 0.1$ bps/Hz; the power allocation coefficients are $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, and when $\alpha_1 \neq 0.8$, $\alpha_2 = 1 - \alpha_1$; Rician factor $K = 0$ or 1;

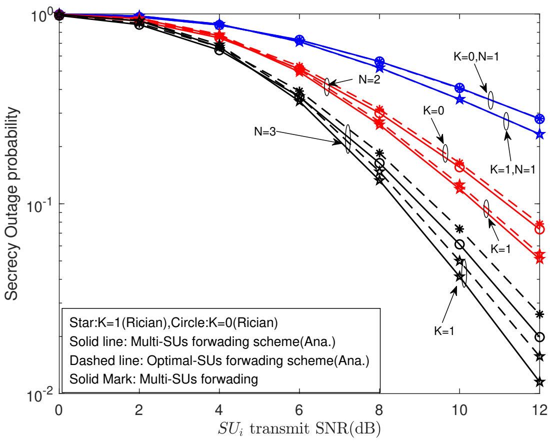
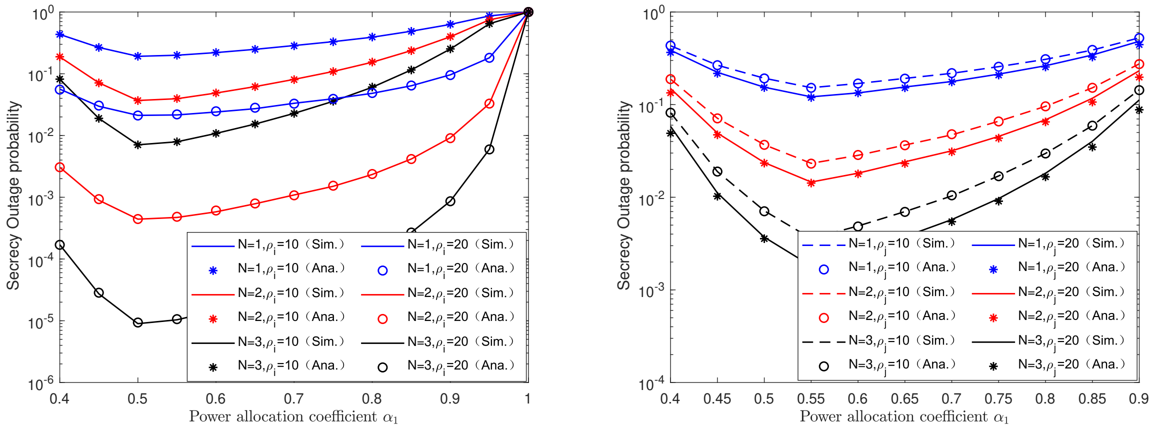


Fig. 2 Secrecy outage probability of PU versus SU_i transmit SNR under different relay forwarding scheme.

Fig.2 plots secrecy outage probability of PU vs. transmit SNR of SU_i for CR-NOMA-CJ system, when the number of SUs is $N = 1, 2, 3$ under different K and SU forwarding schemes. We can see from Fig.2 that secrecy outage probabilities of PU are nearly the same under the proposed optimal SU selection scheme and multi-SUs (that successfully decode the received BS signal) forwarding scheme with number

$$\begin{aligned} \Pr\left(R_{SEC}^J < R_{th}\right) = & \sum_{i \in D_k} \sum_{c_2=0}^{\infty} \sum_{d_2=0}^{c_2} \sum_{v=1}^{V} \frac{K^{d_2} (K+1)^{d_2+1} e^{-(K-z_v)} \omega_v f(z_v)}{\lambda_{SU_i-PU}^2 \lambda_{SU_i-PU}^{d_2-1} d_1! c_1!} \\ & \times \Pr(i^* = i) \frac{\left(K(K+1)(\delta + \delta z_v - 1)^{d_2} - d_1 (\alpha_1 \rho_i)^{d_2} \lambda_{SU_i-PU}\right) e^{-\frac{K(K+1)(\delta+\delta z_v-1)}{(\alpha_1\rho_i - \alpha_1\rho_i(\delta+\delta z_v-1))\lambda_{SU_i-PU}}}}{\lambda_{SU_i-PU} (\alpha_1 \rho_i - \alpha_1 \rho_i (\delta + \delta z_v - 1))^{d_2+1}}, \end{aligned} \tag{31}$$

$$\begin{aligned} P_{OUT}^J = & \sum_{a=0}^{\infty} \sum_{b=0}^{a} \prod_{i=1}^{N} \frac{K^{2a+1} (K+1)^{2a+2} e^{-K} \left(1 - \frac{{Q_1}^b e^{Q_1}}{b!}\right)}{a! \lambda_{BS-SU_i}^{2a+2}} + \sum_{K=1}^{N} \sum_{a_1=0}^{\infty} \sum_{b_1=0}^{a_1} \sum_{a_2=0}^{\infty} \sum_{b_2=0}^{a_2} \sum_{i \in D_k} \sum_{c_1=0}^{\infty} \sum_{d_1=0}^{c_1} \sum_{v=1}^{V} \prod_{i=1}^{N} \prod_{l=1}^{N} C_n^k \\ & \times \frac{K^{2(a_1+a_2+1)+d_1} (K+1)^{2(a_1+a_2)+d_1+5} e^{-3K} \left(1 - \frac{e^{Q_1} {Q_1}^{b_1}}{b_1!}\right) \left(1 - \frac{e^{Q_1} {Q_2}^{b_2}}{b_2!}\right) e^{z_v} \omega_v f(z_v)}{\lambda_{BS-SU_l}^{2a_2+2} \lambda_{BS-SU_i}^{2a_1+2} \lambda_{SU_i-PU}^{d_1-1} a_2! a_1! d_1! c_1!} \\ & \times \Pr(i^* = i) \frac{\left(\frac{K(K+1)(\delta+\delta z_v-1)^{d_1}}{\lambda_{SU_i-PU}} - d_1 (\alpha_1 \rho_i)^{d_1}\right) e^{-\frac{K(K+1)(\delta+\delta z_v-1)}{(\alpha_1\rho_i - \alpha_1\rho_i(\delta+\delta z_v-1))\lambda_{SU_i-PU}}}}{(\alpha_1 \rho_i - \alpha_1 \rho_i (\delta + \delta z_v - 1))^{d_1+1} \lambda_{SU_i-PU}^2}. \end{aligned} \tag{32}$$



(a) Different SU_i transmit SNR ρ_i

(b) Different jammer transmit SNR ρ_j

Fig. 3 Secrecy outage probability of PU versus power allocation coefficient α_1 under different ρ_i and ρ_j.

of SU. Especially, the secrecy outage probabilities of PU under the two schemes are exactly same when $N = 1$. However, utilizing optimal SU forwarding has less energy consumption. Therefore, in the following simulations, we only discuss secrecy outage probability of PU under the optimal SU selection scheme proposed in Subsection 2.2.

Fig.3 (a) and Fig.3 (b) present secrecy outage probability of PU of CR-NOMA-CJ system versus power allocation coefficient α_1 under different ρ_i and ρ_j, respectively. According to the curves in Fig.3 (a), when N is a fixed value, the SOP of PU decreases by increasing ρ_i and the SOP of PU decreases first and then increases by increasing power allocation coefficient α_1. We can also see that the curves of SOP of PU reach the lowest point when $\alpha_1 = 0.9$. We can obtain the system has optimal power allocation. As we can see from Fig.3 (b), ρ_j has a little effect on the SOP of PU of CR-NOMA-CJ system, which is consistent with the analysis results in Fig.7. Similar with Fig.3 (a), the curves of SOP of PU reach the lowest point when $\alpha_1 = 0.9$.

Fig.4 plots secrecy outage probability of PU of CR-NOMA-NCJ and CR-NOMA-CJ systems versus SU_i transmit SNR, when the number of SUs is $N = 1, 2, 3$. The dashed lines represent the SOP of PU of CR-NOMA-NCJ system, and solid lines represent the SOP of PU of CR-NOMA-CJ system. We can see that theoretical results are completely in agreement with simulation results, which verifies the correctness of (25) and (31). This figure indicates that the SOP of PU decreases as SU_i transmit the SNR and the number of SUs increases. The SOP of PU decreases rapidly when the values of SU_i transmit SNR and the number of SUs are changed to a suitable interval, which shows that increasing SU_i transmits SNR and the number of SUs can indeed improve the physical layer security performance of the systems. In addition, the SOP of PU of NOMA-CJ system is always lower than that of the NOMA-NCJ system when the values of SU_i transmit SNR and the number of SUs are fixed, indicating that cooperative jamming can effectively improve physical layer security performance.

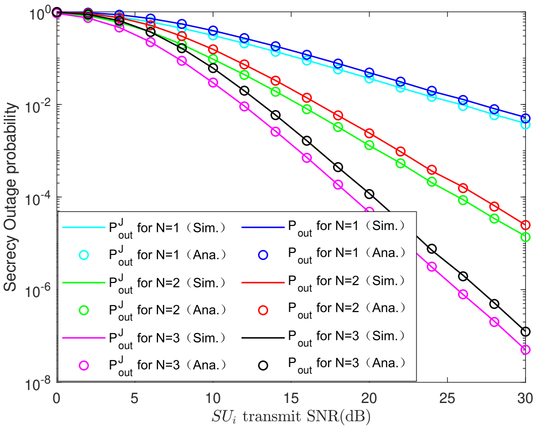


Fig. 4 Secrecy outage probability of PU versus SU_i transmit SNR under different number of SUs.

Fig.5 plots secrecy outage probability of PU of CR-NOMA-CJ systems versus SU_i transmit SNR, when the number of SUs is $N = 1, 2, 3$. It considers three scenarios and analyzes the secrecy outage probability of PU transmission in the CR-NOMA-CJ system. The dashed line represents the asymptotic analysis under high SNR in the CR-NOMA-CJ system. The solid

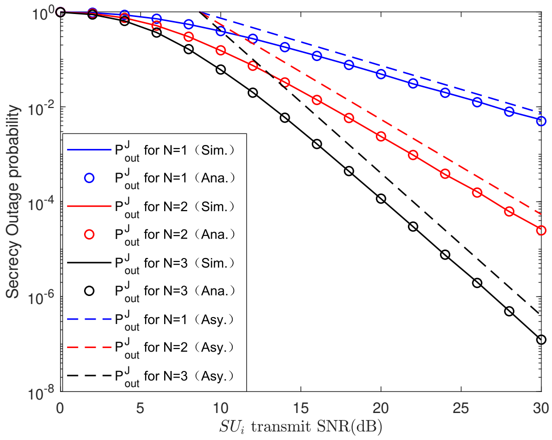


Fig. 5 Secrecy outage probability of PU versus SU_i transmit SNR under different relay forwarding scheme.

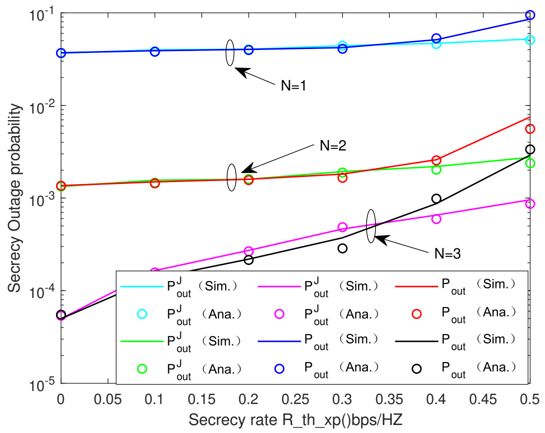


Fig. 6 Secrecy outage probability of PU versus R_{th} under different number of SUs.

line represents the simulation results of secrecy outage probability under the CR-NOMA-CJ system. From the figure, it is evident that the theoretical and simulation results are comparable, suggesting consistency between the analysis and simulation outcomes. It indicates that the SOP of the PU decreases with increasing SNR and SU count, suggesting that enhancing the number of SUs and SNR can improve the physical layer performance. This observation also confirms the validity of system described in Eq. (32) and Eq. (33).

Fig.6 shows secrecy outage probability of PU of CR-NOMA-NCJ and CR-NOMA-CJ systems versus the secrecy rate of PU when the number of SUs is $N = 1, 2, 3$. From these curves, we can observe that the SOP of PU increases with the increase of R_{th} and the high SOP of PU of NOMA-CJ system is always lower than that of the NOMA-NCJ system when N is the same, which shows that the cooperative jamming can effectively improve physical layer security performance. It means that improving the security performance of the system affected by cooperative jamming is limited by R_{th}. Therefore, it is necessary to select appropriate N and R_{th} when improving physical layer security performance of the system.

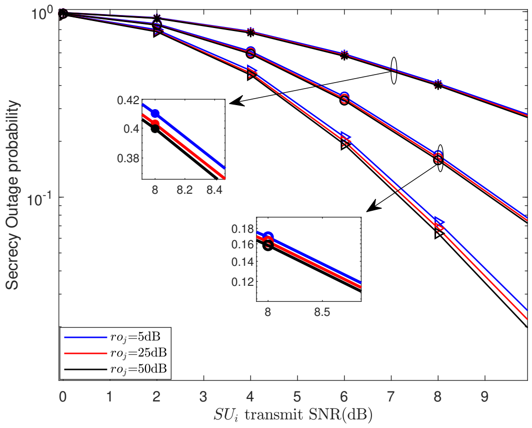


Fig. 7 Secrecy outage probability of PU versus SU_i transmit SNR under different ρ_j.

Fig. 7 shows secrecy outage probability of PU of CR-NOMA-CJ system versus SU_i transmit SNR when the number of SUs is $N = 1, 2, 3$ under different ρ_j. The SOP of PU decreases with the increase of SU_i transmit SNR. The change of SOP of PU is not obvious as ρ_j increases when $N = 1, 2$; the change of SOP of PU is obvious as ρ_j increases when $N = 3$. These results show that the physical layer security performance of NOMA-CJ system is less affected by ρ_j, and ρ_j will have a more significant impact on the physical layer security performance of the NOMA-CJ system, when N reaches a certain amount. The SOP of PU of $\rho_j = 25$ dB is greater than that of $\rho_j = 5$ dB when SU_i transmit SNR is greater than 20 dB and less than 25 dB; the SOP of PU of $\rho_j = 50$ dB is greater than that of $\rho_j = 5$ dB when SU_i transmit SNR is greater than 25 dB. These effects indicate that the influence of ρ_j on the SOP of PU is related to SU_i transmit SNR and the appropriate ρ_j should be selected when SU_i transmit SNRs are different, in order to improve the security performance.

5 Conclusion

In this paper, we investigated the physical layer security performance of CR-NOMA network with eavesdropper based on DF that applies cooperative jamming technology. The physical layer security performance of CR-NOMA system with and without cooperative jamming are compared and analyzed. We derived the expressions for SOP of PU of CR-NOMA-NCJ and CR-NOMA-CJ systems and verified them using Monte Carlo simulations. Simulation results demonstrated that cooperative jamming technology can effectively improve the physical layer security performance of a CR-NOMA system. Furtherly, the results showed how to select the appropriate the number of SUs and the value of security rate of PU to improve the physical layer security performance of CR-NOMA-CJ system. Simulation results also demonstrated that CR-NOMA-CJ system has an optimal power allocation coefficient, so we can further analyze optimal power allocation algorithm of CR-NOMA-CJ system under different conditions later.

6 Appendix A:Proof of Lemma 1

According to the best secondary user selection criteria described in section II, $\Pr\left(i^*=i\right)$ can be given by

$$\begin{aligned}&\Pr\left(i^*=i\right)\\&=\Pr\left(\bigcap_{i'\neq i}^{D_k}\left(\begin{array}{c}\underbrace{\min_{l\in\bar{D}_k}\left\{\left|h_{SU_i-SU_l}\right|^2\right\}-\left|h_{SU_i-E}\right|^2>}_{Q}\\ \underbrace{\min_{l\in\bar{D}_k}\left\{\left|h_{SU_{i'}-SU_l}\right|^2\right\}-\left|h_{SU_{i'}-E}\right|^2}_{R}\end{array}\right)\right),\end{aligned}\tag{A.1}$$

where $i'\in D_k$ and $i'\neq i$.

Using the conditional probability [18], (A.1) can be written as

$$\Pr\left(i^*=i\right)=\int_0^\infty\underbrace{\prod_{i'\in D_k-\{i\}}F_R\left(q\right)}_{\Delta}f_Q\left(q\right)dq. \tag{A.2}$$

Let $X_1=\min\limits_{l\in\bar{D}_k}\left\{\left|h_{SU_i-SU_l}\right|^2\right\}$ and $Y_1=\left|h_{SU_i-E}\right|^2$ in (A.1). Then the cumulative distribution function (CDF) of $Q=X_1-Y_1$ can be expressed as

$$\begin{aligned}&F_Q\left(q\right)=\Pr\left(X_1-Y_1\le q\right)\\&=1-\frac{\exp\left(-\sum\limits_{l\in\bar{D}_k}\frac{q}{\lambda_{SU_i-SU_l}}\right)}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_i-E}}{\lambda_{SU_i-SU_l}}+1}.\end{aligned}\tag{A.3}$$

From (A.3), the PDF of Q can be obtained as

$$f_Q\left(q\right)=\frac{\sum\limits_{l\in\bar{D}_k}\frac{1}{\lambda_{SU_i-SU_l}}}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_i-E}}{\lambda_{SU_i-SU_l}}+1}\exp\left(-\sum_{l\in\bar{D}_k}\frac{q}{\lambda_{SU_i-SU_l}}\right). \tag{A.4}$$

Similarly, let $X_2=\min\limits_{l\in\bar{D}_k}\left\{\left|h_{SU_{i'}-SU_l}\right|^2\right\}$, $Y_2=\left|h_{SU_{i'}-E}\right|^2$. Then the CDF of $R=X_2-Y_2$ can be expressed as

$$\begin{aligned}&F_R\left(r\right)=\Pr\left(X_2-Y_2\le r\right)\\&=1-\frac{1}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_{i'}-E}}{\lambda_{SU_{i'}-SU_l}}+1}\exp\left(-\sum_{l\in\bar{D}_k}\frac{r}{\lambda_{SU_{i'}-SU_l}}\right).\end{aligned}\tag{A.5}$$

Substituting (A.5) into (A.2), then Δ can be expressed as

$$\Delta=\prod_{i'\in D_k-\{i\}}\left(\begin{array}{c}1-\frac{1}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_{i'}-E}}{\lambda_{SU_{i'}-SU_l}}+1}\\ \times\exp\left(-\sum\limits_{l\in\bar{D}_k}\frac{q}{\lambda_{SU_{i'}-SU_l}}\right)\end{array}\right). \tag{A.6}$$

According to the polynomial expansion, (A.6) can be further expressed as

$$\begin{aligned}&\Delta=\\&1+\sum_{r=1}^{2^{|D_k|-1}-1}\left(-1\right)^{\left|\tilde{D}_k(r)\right|}\exp\left(-\sum_{i'\in\tilde{D}_k(r)}\sum_{l\in\bar{D}_k}\frac{q}{\lambda_{SU_{i'}-SU_l}}\right)\\&\times\prod_{i'\in\tilde{D}_k(r)}\frac{1}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_{i'}-E}}{\lambda_{SU_{i'}-SU_l}}+1}.\end{aligned}\tag{A.7}$$

where $|D_k|$ is the cardinality of the set D_k, and $\tilde{D}_k\left(r\right)$ denotes the rth non-empty subset of the set $D_k-\{i\}$.

Substituting (A.4) and (A.7) into (A.2) and performing the required integration, the closed expression of $\Pr\left(i^*=i\right)$ can be obtained and it is shown in (A.8) at the bottom of next page.

References

[1] M. Li et al, ”Error Performance of NOMA System With Outdated, Imperfect CSI, and RHI Over Fading Channels,” in IEEE Transactions on Vehicular Technology, 2023.

[2] L. Bariah, L. Mohjazi, S. Muhaidat, P. C. Sofotasios, G. Karabulut Kurt, H. Yanikomeroglu, and O. A. Dobre, “A prospective look: Key enabling technologies, applications and open research topics in 6G networks,” *IEEE Access*, vol. 8, pp. 174792–174820, Aug. 2020.

[3] X. Li, J. Li, and L. Li, “Performance analysis of impaired SWIPT NOMA relaying networks over imperfect weibull channels,” *IEEE Systems Journal* vol. 14, no. 1, pp. 669–672, Mar. 2020.

[4] M. Li, H. Yuan, C. Maple, Y. Li and O. Alluhaibi, ”Security Outage Probability Analysis of Cognitive Networks With Multiple Eavesdroppers for Industrial Internet of Things,” in IEEE Transactions on Cognitive Communications and Networking, vol. 8, no. 3, pp. 1422-1433, Sep. 2022.

[5] L. Lv, J. Chen, Q. Ni, and Z. Ding, “Design of cooperative non-orthogonal multicast cognitive multiple access for 5G systems: User scheduling and performance analysis,” *IEEE Transactions on Communications*, vol. 65, no. 6, pp. 2641–2656, Jun. 2017.

[6] S. Arzykulov, T. A. Tsiftsis, G. Nauryzbayev, and M. M. Abdallah, “Outage performance of cooperative underlay CR-NOMA with imperfect CSI,” *IEEE Communications Letters*, vol. 23, no. 1, pp. 176–179, Jan. 2019.

[7] X. Liu, Y. Wang, S. Liu, J. Meng, “Spectrum resource optimization for NOMA-based cognitive radio in 5G communications,” *IEEE Access*, vol. 6, pp. 24904–24911, Apr. 2018.

[8] Kumar A, and Kumar K. “Relay sharing with DF and AF techniques in NOMA assisted cognitive radio networks,” *Physical Communication*, vol. 42, pp. 1–10, Jun. 2020.

[9] L. Lv, J. Chen, Q. Ni, Z. Ding, and H. Jiang, “Cognitive non-orthogonal multiple access with cooperative relaying: a new wireless frontier for 5G spectrum sharing,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 188–195, Apr. 2018.

[10] F. Zhou, Y. Wu, Y. Liang, Z. Li, Y. Wang, and K. Wong, “State of the art, taxonomy, and open issues on cognitive radio networks with NOMA,” *IEEE Wireless Communications*, vol. 25, no. 2, pp. 100–108, Apr. 2018.

[11] X. Sun, W. Yang, Y. Cai, R. Ma, and L. Tao, “Physical layer security in millimeter wave SWIPT UAV-based relay networks,” *IEEE Access*, vol. 7, pp. 35851–35862, Mar. 2019.

[12] M. Li, H. Yuan, X. Yue, S. Muhaidat, C. Maple, and M. Dianati, “Secrecy outage analysis for alamouti space¨Ctime block coded non-orthogonal multiple access,” *IEEE Communications Letters*, vol. 24, no. 7, pp. 1405–1409, Jul. 2020.

[13] M. Li, X. Yang, F. Khan, M. A. Jan, W. Chen and Z. Han, ”Improving Physical Layer Security in Vehicles and Pedestrians Networks With Ambient Backscatter Communication,” in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 9380-9390, Jul. 2022.

[14] Z. Qin, Y. Liu, Z. Ding, Y. Gao and M. Elkashlan, ”Physical layer security for 5G non-orthogonal multiple access in large-scale networks,” 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016.

[15] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu and A. Nallanathan, ”Secure Communications in a Unified Non-Orthogonal Multiple Access Framework,” in IEEE Transactions on Wireless Communications, vol. 19, no. 3, pp. 2163-2178, Mar. 2020.

[16] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security:Technical challenges, recent advances, and future trends,” Proceedingsof the IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.

[17] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, “Secrecy sum rate max-imization in non-orthogonal multiple access,” IEEE Communications Letters, vol. 20, no. 5, pp. 930–933, 2016.

[18] M. Li, H. Yuan, C. Maple, W. Cheng and G. Epiphaniou, ”Physical Layer Security Analysis of Cognitive NOMA Internet of Things Networks,” in IEEE Systems Journal, vol. 17, no. 1, pp. 1045-1055, Mar. 2023.

[19] Y. Song, W. Yang, and Z. Xiang, “Research on cognitive power allocation for secure millimeter-wave NOMA networks,” IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 13 424–13 436, Sep. 2020.

$$
\begin{aligned}
\Pr\left(i^{*}=i\right) &= \int_{0}^{\infty}\left(1+\sum_{r=1}^{2^{|D_k|-1}-1}(-1)^{\left|\tilde{D}_k(r)\right|}\exp\left(-\sum_{i'\in\tilde{D}_k(r)}\sum_{l\in\bar{D}_k}\frac{q}{\lambda_{SU_{i'}-SU_l}}\right)\prod_{i'\in\tilde{D}_k(r)}\frac{1}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_{i'}-E}}{\lambda_{SU_{i'}-SU_l}}+1}\right)\\
&\qquad\times\frac{\sum\limits_{l\in\bar{D}_k}\frac{1}{\lambda_{SU_i-SU_l}}}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_i-E}}{\lambda_{SU_i-SU_l}}+1}\exp\left(-\sum_{l\in\bar{D}_k}\frac{q}{\lambda_{SU_i-SU_l}}\right)dq\\
&= \frac{1}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_i-E}}{\lambda_{SU_i-SU_l}}+1}\left(1+\sum_{r=1}^{2^{|D_k|-1}-1}(-1)^{\left|\tilde{D}_k(r)\right|}\prod_{l\in\tilde{D}_k(r)}\frac{1}{\sum\limits_{l\in\bar{D}_k}\frac{\lambda_{SU_{i'}-E}}{\lambda_{SU_{i'}-SU_l}}+1}\frac{\sum\limits_{l\in\bar{D}_k}\frac{1}{\lambda_{SU_i-SU_l}}}{\sum\limits_{i'\in\tilde{D}_k(r)}\sum\limits_{l\in\bar{D}_k}\frac{1}{\lambda_{SU_{i'}-SU_l}}+\sum\limits_{l\in\bar{D}_k}\frac{1}{\lambda_{SU_i-SU_l}}}\right).
\end{aligned}
\tag{A.8}
$$

[20] Z. Xiang, W. Yang, G. Pan, Y. Cai and Y. Song, ”Physical Layer Security in Cognitive Radio Inspired NOMA Network,” in IEEE Journal of Selected Topics in Signal Processing, vol. 13, no. 3, pp. 700-714, Jun. 2019.

[21] Z. Xiang, W. Yang, and Y. Cai, “Secure transmission design in HARQ assisted cognitive NOMA networks,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2528–2541, Jan. 2020.

[22] D. Wang and S. Men, “Secure energy efficiency for NOMA based cognitive radio networks with nonlinear energy harvesting,” IEEE Access, vol. 6, pp. 62 707–62 716, Oct. 2018.

[23] Z. Zhang, J. Chen, and L. Lv, “Utilizing cooperative jamming to secure cognitive radio NOMA networks,” in GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, Jan. 2021.

[24] B. Chen, Y. Chen, Y. Chen, Y. Cao, Z. Ding, N. Zhao, and X. Wang, “Secure primary transmission assisted by a secondary full-duplex NOMA relay,” IEEE Trans. Veh. Technol., vol. 68, no. 7, pp. 7214–7219, Jun. 2019.

[25] Y. Chen, T. Zhang, Y. Liu, and X. Qiao, “Physical layer security in NOMA-enabled cognitive radio networks with outdated channel state information,” *IEEE Access*, vol. 8, pp. 159480–159492, Sep. 2020.

[26] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, “Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, Apr. 2018.

[27] X. Chen, D. W. K. Ng, W. H. Gerstacker and H. - H. Chen, ”A Survey on Multiple-Antenna Techniques for Physical Layer Security,” in IEEE Communications Surveys Tutorials, vol. 19, no. 2, pp. 1027-1053, Secondquarter 2017.

[28] S. Bhattacharjee, “Friendly jamming assisted secure cooperative multicasting in cognitive radio-NOMA networks,” In: *IEEE Globecom Workshops (GC Wkshps)*, Waikoloa, USA, Dec. 2019.

[29] J. Huang, and A. L. Swindlehurst, “Cooperative jamming for secure communications in MIMO relay networks,” *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[30] H. Wang, M. Luo, X. Xia, and Q. Yin, “Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper’s CSI,” *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[31] Y. Zou, B. Champagne, W. -P. Zhu and L. Hanzo, ”Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems,” in IEEE Transactions on Communications, vol. 63, no. 1, pp. 215-228, Jan. 2015.

[32] C. Deng, M. Liu, X. Li and Y. Liu, ”Hardware Impairments Aware Full-Duplex NOMA Networks Over Rician Fading Channels,” *IEEE Systems Journal*, vol. 15, no. 2, pp. 2515-2518, Jun. 2021.

[33] H. A. Suraweera, G. K. Karagiannidis and P. J. Smith, ”Performance analysis of the dual-hop asymmetric fading channel,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 2783-2788, Jun. 2009.

[34] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products. 6th ed. New York, NY, USA: Academic, 2000.

[35] F. B. Hildebrand, Methods of applied mathematics. Courier Corporation, 2012.

Meiling Li is a Professor with the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. She visited the University of Warwick in 2019 and the Tsinghua University in 2020. Her research interests include cognitive radio, V2X, cooperative communications, non-orthogonal multiple access, and physical layer security technology. She received M. S. and Ph.D degrees in signal and information processing from the Beijing University of Posts and Telecommunications, Beijing, in 2007 and 2012, respectively.

Peng Xue was born in Yuncheng, Shanxi, China in 1997. he is currently pursuing the the M.Sc degree in the school of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. His research interests include cognitive radio, cooperative jamming, non-orthogonal multiple access.

Hu Yuan is a Lecturer in Cyber Security at Kingston University. He received his PhD from the University of Warwick (2016). His research focuses on the security and privacy aspects of IoT, including the internet of bio-nano things, vehicular communication networks, user behaviours identification and space systems. He was the leading researcher for the IoT Transport and Mobility Demonstrator.

Yuxing Han (Senior Member, IEEE) received the B.S. degree in electrical engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2006, and the Ph.D. degree in electrical engineering from the University of California at Los Angeles, Los Angeles, CA, USA, in 2011. She is currently a Professor with Shenzhen International Graduate Shool, Tsinghua University, Shenzhen, China. Her research area focuses on artificial intelligence, precision agriculture, edge computing, virtual reality, multimedia communication over challenging networks, and big data analysis.