Physical Layer Security Analysis of Cognitive NOMA Internet of Things Networks

Meiling Li[1], Hu Yuan[2], Carsten Maple[2], Wenjie Cheng[1], and Gregory Epiphaniou[2]

***Abstract*—The implementation of advanced communication technologies such as non-orthogonal multiple access technologies (NOMA) and cognitive radio technology (CR) in the Internet of Things (IoT) networks facilitates wide bandwidth, massive access and low latency. However, the development and deployment of IoT systems are hampered by network security issues. Physical layer security (PLS) is an emerging technique to complement and significantly improve communication security in wireless networks. This paper analyses the PLS performance of cooperative NOMA cognitive wireless networks. Furthermore, a cognitive collaboration method is proposed, combining legitimate links and eavesdropping links. More specifically, new closed expressions of the outage probability (OP) of the primary user (PU) and secondary users (SUs), as well as the intercept probability (IP) of an eavesdropper (E), are derived to evaluate the proposed scheme's PLS transmission performance. Monte Carlo simulations verify the analysis. The results show the SU selection scheme incorporated with the eavesdropping link can slightly improve the security performance compared with the legitimate link. It can also be obtained that increasing the transmit power and increasing the number of SUs could enhance the security performance of PU and SUs.**

***Index Terms*—Non-orthogonal multiple access, cognitive radio, physical layer security, outage probability, intercept probability.**

I. Introduction

THE communication characteristics of the Internet of Things (IoT) networks are low latency, low power consumption and wide coverage. The IoT can efficiently allocate manufacturing resources, customer demanding production, optimised manufacturing process, and fast environment adaptation [1]. However, the massive IoT's terminals connecting to the internet wirelessly will create much data to be transferred in IoT communications, which challenges the available spectrum resources. Consequently, the communication requirement for each IoT's terminal cannot be guaranteed [2]. Cognitive radio (CR) technology has been deemed efficient in dynamic spectrum sharing to improve spectrum efficiency in limited spectrum scenarios.

Recently, researchers addressed the CR for IoT in various domains. First, the authors highlight potential applications of CR-based IoT systems in [3]. Then, in [4], the authors investigated how to combine CR technology and IoT to reduce the blocking probability of higher-priority cognitive user calls while maintaining a sufficient channel utilisation level. In [5], the authors demonstrated that cognitive IoT can achieve sufficient spectrum resources through spectrum sharing with primary users, thus easing the strain on the spectrum resources efficiently.

On the other hand, since building industrial wireless network is one of the most important things for fourth industrial revolution, it requires the next generation communication technology. Non-Orthogonal Multiple Access (NOMA) is the most promising spectrum access technology that can simultaneously transmit multiple signals on the same resource block, thus enabling IoT connection communication at a large scale [6]. Consequently, combining NOMA technology and CR technology to realize more intelligent and efficient communication for heterogeneous IOT devices is an important scenario [7], [8].

Preventing IoT networks from malicious users during wireless communication is critical for the IoT application [9]. The broadcast nature of the wireless medium makes IoT communications susceptible to potential security threats such as eavesdropping and impersonation. Furthermore, the IoT devices or sensors usually lack the computing power to apply complex key management, especially for massive heterogeneous networks. Consequently, traditional cryptographic techniques may result in high latency, which cannot satisfy the stringent latency requirement in IoT communications. As a result, it is a great challenge to realise the security by the traditional signalling process in IoT. On the other hand, physical layer security (PLS) is a low complexity approach to provide security to the users by utilising the dynamic properties of wireless communication [10]–[14], which is more suitable to solve the secure transmission for a heterogeneous network like IoT.

A. Related Work

Typically, the combined network architecture of NOMA and CR is in those three main areas: 1) overlay CR-NOMA, under this architecture, cognitive users opportunistically use the idle spectrum resources of primary users; 2) underlay CR-NOMA, cognitive users share spectrum resources with primary users under certain interference constraints; 3) cooperative CR-

This work was partly supported by the National Natural Science Foundation of China under Grant 62001320, Central government funds for guiding local scientific and technological development of Shanxi under Grant YDZJSX2021A037, Research Project Supported by Shanxi Scholarship Council of China under Grant 2021-133 and 2020-126. It was also supported by UKRI grants EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research - University of Warwick), EP/N510129/1 (The Alan Turing Institute) and EP/S035362/1 (PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity). (Corresponding author: Meiling Li.)

[1] M. Li, and W. Cheng are with School of Electronics Information Engineering, Taiyuan University of Science and Technology, 030024 Taiyuan, China (e-mail: meilingli@tyust.edu.cn, S20170436@stu.tyust.edu.cn).

[2] H. Yuan, C. Maple and G. Epiphaniou are with the WMG, University of Warwick, Coventry, CV4 7AL, UK (e-mail: H.Yuan.4@warwick.ac.uk, CM@warwick.ac.uk and gregory.epiphaniou@warwick.ac.uk).

NOMA, cognitive users as the auxiliary transmission of primary users to assist them in communication. In the first stage of cooperative CR-NOMA, the base station (BS) transmits composite signal including primary user (PU) and secondary user (SU) to the primary and secondary receivers. Then, the secondary receiver uses successive interference cancellation (SIC) to decode the received composite signal. In the second stage, the secondary receiver forwards the successfully decoded signal to the primary receiver, which combines the signals received in the two stages to enhance its received signal strength [7].

The communication networks are benefiting from the combination of the CR and NOMA. The related researches are focused on the clustering optimisation and communication reliability problem. In [15], the authors studied optimising the power allocation scheme of a large-scale underlay CR-NOMA network. The random geometric model is used to analyse the NOMA clustering problem. The outage performance of cognitive users was studied by considering cooperative NOMA transmission of underlay CR-NOMA in [16]. The authors studied how to select the optimal cognitive user to assist primary user transmission and realise secondary user transmission simultaneously, and the outage probability (OP) of the cognitive user and the primary user was analysed. The exploitation of NOMA in CR networks has also demonstrated a benevolent solution for efficient spectrum sharing in cognitive IoT networks [15]. A NOMA-based hybrid spectrum access scheme was proposed for 6G-enabled cognitive IoT in [2], in which the uplink resource allocations for the cognitive IoT was considered. In [1], an uplink secondary IoT device scheduling and power allocation problem based on imperfect channel state information and imperfect spectrum sensing is investigated for industrial cognitive IoT over cognitive heterogeneous NOMA networks.

However, network security is a significant challenge of the IoT because of the massive heterogeneous open-access environment. Meanwhile, the CR-NOMA increase the complexity of the physical layer security because the different network architectures refer to different physical layer security transmission issues for CR-NOMA wireless networks.

The authors in [17] investigated the cognitive power allocation scheme to evaluate the reliability and secrecy performance of the secondary user in mmWave NOMA networks, where a base station (BS) provided primary and secondary users services. In [18], the authors proposed a downlink cascaded transmitting zero-forcing-beamforming technique to secure communications in a two-cell multiple-input multiple-output NOMA-based CRN, where they also considered that a BS serves for primary and secondary users concurrently, the similar model was also considered in [19], [20]. The authors in [21]–[24] considered that a cognitive transmitter serves as a relay and assists primary/cognitive transmissions using the NOMA principle.

Apart from the above CR-NOMA networks, the authors provided a cooperative CR-NOMA network in [7], [25], where a BS sends two different messages to a unicast PU and a group of multicast SUs. SU can be recruited as a cooperative relay to help improve the reception reliability of the primary receiver. This scheme can be applied to increase network throughput and promise user fairness, which is highly suitable for multicast content transmission in IoT scenarios. However, there is little research on the secure IoT under this cooperative CR-NOMA network to the best of the authors' knowledge.

B. Contributions and Paper Structure

This paper studied a cooperative CR-NOMA network's physical layer security performance in IoT scenarios. One of the best SU from multiple SUs is selected to forward the reencoded composite signal from IOT BS, in which the selected SU and the PU form a NOMA pair (E-MCU-CR-NOMA). Consequently, The SUs can access the primary network for their communications whilst providing cooperative transmission for PU located far from the BS. The main contributions are as follows.

1) A cognitive collaboration method was proposed, by combining legitimate links and eavesdropping links.
2) Closed-form expressions for the exact outage probabilities (OP) for both PU and SUs and the intercept probabilities (IP) are developed to facilitate the performance analysis of the proposed cooperative transmission scheme.
3) To obtain further insights, we performed an asymptotic analysis of both OP and IP in the high signal-to-noise ratio (SNR) regime.
4) We have verified the analysis by simulations. We show that the proposed scheme can achieve lower IP for SU and PU than without considering the eavesdropping link when selecting the appropriate SU for transmission. Also, the security performance of both PU and SU can be enhanced by increasing the number of SU.

The rest of the paper is structured as follows: Section II defines the communication system model. Then, in Section III, the cooperative user selection scheme was presented, and the security performance for the relative cooperative selection was examined in Section IV. Finally, the simulation results were presented in Section V, and the conclusion was in section VI.

II. System Model

In this paper, the system considered IoT-enabled technologies in industrial environments. It can help improve efficiency and safety of the industry operates in many ways; for example, monitoring the state of equipment or processes enhanced situational awareness and minimised the need for humans in dangerous environments. Generally, the primary users are defined as the properties located in a fixed place for dedicated tasks. Meanwhile, the secondary users are set as the properties with multiple tasks and autonomous available. As shown in Fig.1, which includes a BS, a group of cognitive users SU_i, $(i = 1, 2, ..., M)$ a primary user (PU) and an eavesdropper (E). The near user SU can be used as a relay to assist PU's communication thereby improving the communication reliability of PU. Distributed matching algorithm can be used for user-pairing [26], the paired two users share the same spectrum of resources to allocate different power levels. Specifically, when both their rate requirements are satisfied, the PU with

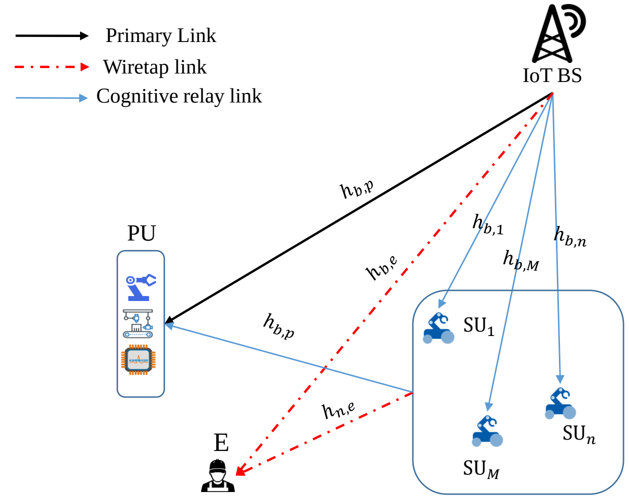


Fig. 1: Coexistence of a primary network and a cognitive multiply relay network. One primary user and M secondary users (SU) and a eavesdropper.

poor channel condition is paired with a SU with good channel condition. The quality of service for weak users (PU) can be guaranteed since the transmit power allocated to strong users (SUs) is constrained following the concept of cognitive radio. The assumption was made as 1) all nodes equipped with a single antenna, 2) all nodes work in half-duplex mode, 3) communication channel is a Rayleigh fading channel.

The channel fading coefficient from BS to SU_n is $h_{b,n}$, BS to PU is $h_{n,p}$ and BS to PU is $h_{b,p}$ where $|h_{b,n}|^2 > |h_{b,p}|^2$. The channel fading coefficient from BS and SU_n to the E are $h_{b,e}$ and $h_{n,e}$ respectively. $h_{n,m}$ is the fading coefficient from SU_n to SU_m. According to the principle of NOMA, the BS sends a composite signal $\alpha_{PU}P_1\kappa_{PU}+\alpha_{SU}P_1\kappa_{SU}$ containing PU information κ_{PU} and SU information κ_{SU} to PU and SU with power P_1, α_{PU} and α_{SU} are the power distribution coefficients of PU and SU respectively. In this paper, the power allocation coefficient of the SU is equal to that at the BS in the first time slot [25]. The power allocation coefficients satisfied the conditions as $\alpha_{PU} + \alpha_{SU} = 1$ and $\alpha_{PU}>\alpha_{SU}$. Firstly, SU_i decodes the received composite signal by using the successive interference cancellation (SIC) technology, and then re-encodes the composite signal and forwards it to PU. Then PU processes the received combining signals. At the same time, due to the broadcasting characteristics of wireless communication the signal sent by BS and SU could be wiretapped by E. It is noted that the considered cooperative transmission is different from traditional relay cooperative transmission as considered in [27]. In the considered system model, the unsuccessfully decoded SUs will also get help from the selected successfully decoded SU to realize secondary transmission. The detailed signal process of the considered system model is following.

In the first slot, the signal received by SU_n and PU (E) from BS can be expressed as:

$$y_n = \sqrt{P_1}h_{b,n}\left(\alpha_{PU}\kappa_{PU} + \alpha_{SU}\kappa_{SU}\right) + n_{SU}, \qquad (1)$$

$$y_{x,1} = \sqrt{P_1}h_{b,x}\left(\alpha_{PU}\kappa_{PU} + \alpha_{SU}\kappa_{SU}\right) + n_x, \qquad (2)$$

where x represents PU for legitimate link and E for eavesdropping link. n_{SU} and n_x represents the different AWGN received at SU and x, respectively.

In order to distinguish different channel conditions between legitimate links and eavesdropping links, we assumed that n_{SU} and n_{PU} are 0 mean and variance is σ^2. For the eavesdropping link, n_E is 0 mean and variance is σ_e^2 [28].

Once the SU_n received the composite signal from BS, firstly the signal κ_{PU} was decoded with SIC, and then κ_{SU} was decoded. Only when κ_{PU} and κ_{SU} were successfully decoded, it could be regarded that SU_n decoded successfully, otherwise the decoding fails. The two sets of successful and failed decoding are denoted as D and $\overline{D}$, respectively.

In the second slot, the decoded signal was forwarded from SU to the PU for improving the received signal quality. $SU_{\tilde{n}}$ is selected to assist in forwarding the composite signal to the PU, with the transmission power of P_2. Thus the signal received by the PU (E) can be expressed as:

$$y_{x,2} = \sqrt{P_2}h_{\tilde{n},x}\left(\alpha_{PU}\kappa_{PU} + \alpha_{SU}\kappa_{SU}\right) + n_x, \qquad (3)$$

where $h_{\tilde{n},x}$ is the channel gain between $SU_{\tilde{n}}$ and x. In the next section, the optimisation scheme of the selection of SU to assist transmission from BS to PU was analysed.

III. Cognitive User Selection Scheme

A. The secondary user selection scheme

Based on the E-MCU-CR-NOMA system model illustrated in Fig. 1, the SUs who successfully decoded the received signal from BS could be a potential relay to assist the communication between BS to PU. The straightforward way is that all SUs with success decoding forward the signal to PU, alternatively the SU_n by the selection scheme can forward.

1) Ideal selection model: This paper considers the channel conditions of the eavesdropping link and the cognitive transmission link and proposes an optimal cognitive user selection scheme to make the SUs that can not successfully decoded the BS's signal can also get fair service. Specifically, select the set $\overline{D}$ to minimise each group $h_{n,m}$ to form a subset, and then select $SU_{\tilde{n}}$ from the set D to maximise the channel difference between the cognitive transmission link and the eavesdropping link. The proposed optimal cognitive user selection scheme can be described as:

$$SU_{\tilde{n}} = \arg\max_{n\in D}\left\{\min_{m\in\bar{D}}\left(|h_{n,m}|^2\right) - |h_{n,e}|^2\right\}, \qquad (4)$$

where $h_{n,m}$ is the channel gain between SU_n and SU_m, $h_{n,e}$ is the channel gain between SU_n and E.

2) Sub-optimal scheme: Since the E is in a hidden state in the actual wireless transmission environment, it is difficult for the BS and SU to obtain the link channel state information of E. Therefore, we also consider a sub-optimal cognitive user selection scheme for E-MCU-CR-NOMA system:

$$SU_{\tilde{n}}^{\text{sub}} = \arg\max_{n\in D}\left\{\min_{m\in\bar{D}}\left(|h_{n,m}|^2\right)\right\}. \qquad (5)$$

B. Link data rate

Firstly, the SU_n decodes the signal κ_{PU} and then decodes the κ_{SU}. When the link capacity $C = \log_2(1 + \mathrm{SINR})$ is greater than the required user transmission rate R, the user can decode the current signal successfully [29]. It can be seen that the Signal to Interference Noise Ratio (SINR) is the main factor affecting the link capacity.

In the first slot, SU and PU decode the received composite signal from BS using SIC technology. Firstly, SU decodes κ_{PU} signal and treats κ_{SU} as the interference, and then decodes κ_{SU}. PU decodes κ_{PU} signal directly and regards κ_{SU} as the interference. Therefore, in the first slot, the SINR obtained by PU decoding κ_{PU} signal can be expressed as:

$$\gamma_{p,p}^1 = \frac{\alpha_{PU}|h_{b,p}|^2}{\alpha_{SU}|h_{b,p}|^2 + \rho_1^{-1}}, \quad \gamma_{s,p} = \frac{\alpha_{PU}|h_{b,n}|^2}{\alpha_{SU}|h_{b,n}|^2 + \rho_1^{-1}}, \tag{6}$$

where $\rho_1 = P_1/\sigma^2$.

Similarly, the SINR obtained by SU decoding κ_{PU} and κ_{SU} can be expressed as $\gamma_{s,s} = \alpha_{SU}\rho_1|h_{b,n}|^2$. At the same time, the SINR of the E wiretap κ_{PU} and κ_{SU} in the first slot are expressed as

$$\gamma_{e,p}^1 = \frac{\alpha_{PU}|h_{b,e}|^2}{\alpha_{SU}|h_{b,e}|^2 + \rho_e^{-1}}, \quad \gamma_{e,s}^1 = \frac{\alpha_{SU}|h_{b,e}|^2}{\alpha_{PU}|h_{b,e}|^2 + \rho_e^{-1}}, \tag{7}$$

where $\rho_e = P_1/\sigma_e^2$.

It should be noticed that E does not know the content of the relayed SU. Thus, the E will not decode the received signal from the relayed SU by SIC. So, we are considering a weaker intercepting ability of E not strong abilities as shown in [30], [31]. Therefore, in the second slot, according to the optimal cognitive user selection scheme proposed, an optimal secondary user $SU_{\tilde{n}}$ is selected from the set D that can be decoded successfully. Then the composite signal is assisted to forward to the PU, and at the same time, the cognitive user SU who fails to decode SU_m will also receive the signal forwarded by $SU_{\tilde{n}}$ for cognitive transmission. The SINR can be expressed as follow when PU decodes the κ_{PU} signal:

$$\gamma_{p,p}^2 = \frac{\alpha_{PU}|h_{\tilde{n},p}|^2}{\alpha_{SU}|h_{\tilde{n},p}|^2 + \rho_2^{-1}}, \tag{8}$$

where $\rho_2 = P_2/\sigma^2$. After SU_m received the signal from $SU_{\tilde{n}}$, the SINR of decoding κ_{PU} and κ_{SU} can be expressed as:

$$\gamma_{\tilde{n},m}^p = \frac{\alpha_{PU}|h_{\tilde{n},m}|^2}{\alpha_{SU}|h_{\tilde{n},m}|^2 + \rho_2^{-1}}, \quad \gamma_{\tilde{n},m}^s = \alpha_{SU}\rho_2|h_{\tilde{n},m}|^2, \tag{9}$$

The PU would receive two-way signals in two slots. This paper uses the selective combination to process the two-way signals received by PU to facilitate the calculation complexity. However, if the maximum ratio combining method is used to process the two-way signals, the received SINR will be higher than by selective combination method. Therefore, the SINR obtained by PU when decoding its own signal can be expressed as $\gamma_p = \max\left(\gamma_{p,p}^1, \gamma_{p,p}^2\right)$. The SINR of the E in the second time slot with κ_{PU} and κ_{SU} can be expressed as:

$$\gamma_{e,p}^2 = \frac{\alpha_{PU}|h_{\tilde{n},e}|^2}{\alpha_{SU}|h_{\tilde{n},e}|^2 + \rho_e^{-1}}, \quad \gamma_{e,s}^2 = \frac{\alpha_{SU}|h_{\tilde{n},e}|^2}{\alpha_{PU}|h_{\tilde{n},e}|^2 + \rho_e^{-1}}, \tag{10}$$

Like the PU, the E uses the selective combination to process the two received signals from PU and SU. When E wiretaps PU and SU signals, so the SINR can be expressed as follows:

$$\gamma_e^p = \max\left(\gamma_{e,p}^1, \gamma_{e,p}^2\right), \quad \gamma_e^s = \max\left(\gamma_{e,s}^1, \gamma_{e,s}^2\right). \tag{11}$$

IV. Security performance analysis

This section uses two parameters to measure the communication system: the communication outage probability and the probability of communication interception. The subsequent analysis of the security performance is based on the SU selection model in section III.

A. Communication Outage Probability

1) Outage probability of SU: The communication outage of SU is occurred in two cases:

- The $D = \emptyset$, SU_n cannot decode the composite signal sent by BS;
- $D \neq \emptyset$, the outage occurred while $SU_{\tilde{n}}$ sending the decode signal to PU.

Let D_k is a subset of the SU successful decoding set, $|D_k| = k$, $k = 1, 2 \cdots 2^M - 1$. $\Pr(D = D_k)$ represents the probability that SU_n belongs to the decoding set D_k, and $P_{out,s}(D = D_k)$ represents the outage probability when SU in the decoding set D_k is selected for transmission.

Therefore, the total outage probability (OP) expression of SU can be expressed as:

$$P_{\text{out}}^{\text{SU}} = \Pr(D = \emptyset) + \sum_{k=1}^{2^M-1} P_{\text{out},s}(D = D_k)\Pr(D = D_k), \tag{12}$$

The communication links are set as a Rayleigh fading channels, thus the probability density function (PDF) of any link $a \to b$ can be expressed as:

$$f_{|h_{ab}|^2}(x) = \frac{1}{\lambda_{ab}}\exp\left(-\frac{x}{\lambda_{ab}}\right), \tag{13}$$

where λ_{ab} is the average SINR of link $a \to b$, and $\lambda_{ab} = E(|h_{ab}|^2)$.

According to the rules of SIC technology, firstly SU_n decodes κ_{PU} and then κ_{SU}. Therefore, there are two cases in which SU_n fails to decode the composite signal sent by BS: (i) the first is that SU_n fails to decode κ_{PU}; (ii) the second is that SU_n decodes κ_{PU} successfully but fails to decode κ_{SU}. So $\Pr(D = \emptyset)$ can be expressed as:

$$\begin{aligned}\Pr(D = \emptyset) &\overset{\varphi \geq 0}{=} \prod_{n=1}^{M}\Bigg[\underbrace{\Pr(\gamma_{s,p} < \xi_p)}_{P_{s,1}} + \underbrace{\Pr(\gamma_{s,p} > \xi_p, \gamma_{s,s} < \xi_s)}_{P_{s,2}}\Bigg] \\ &\overset{\varphi \geq 0}{=} \prod_{n=1}^{M}\left[1 - \exp\left(-\frac{\beta}{\rho_1\lambda_{b,n}}\right)\right],\end{aligned} \tag{14}$$

where $\varphi = \alpha_{PU} - \alpha_{SU}\xi_p$, $\xi_p = 2^{2R_{PU}} - 1$, $\xi_s = 2^{2R_{SU}} - 1$, R_{PU} and R_{SU} are the target rates for decoding κ_{PU} and κ_{SU}, and $\beta = \max\left[\xi_p/(\alpha_{PU} - \alpha_{SU}\xi_p), \xi_s/\alpha_{SU}\right]$.

Proof. The proof is in Appendix A. □

$$\begin{aligned} P_{out}^{SU} &= \Pr\left(D=\emptyset\right) + \sum_{n=1}^{2^M-1} P_{out,s}\left(D=D_k\right)\Pr\left(D=D_k\right) = \prod_{n=1}^{M}\left[1-\exp\left(\frac{-\beta}{\rho_1\lambda_{b,n}}\right)\right] \\ &+ \sum_{k=1}^{2^M-1}\prod_{n\in D_k}\left[1-\frac{\exp\left(-\sum\limits_{m\in\bar{D}_k}\frac{\beta}{\rho_2\lambda_{n,m}}\right)}{\lambda_{n,e}\sum\limits_{m\in\bar{D}_k}\lambda_{n,m}^{-1}+\lambda_{n,e}^{-1}}\right]\left\{e^{-\sum\limits_{n\in D_k}\frac{\beta}{\rho_1\lambda_{b,n}}}\prod_{m\in\bar{D}_k}\left[1-\exp\left(-\frac{-\beta}{\rho_1\lambda_{b,m}}\right)\right]\right\}. \end{aligned} \tag{17}$$

$\Pr\left(D=D_k\right)$ presents SU_n successful decodes κ_{PU} and κ_{SU}. It can be expressed as:

$$\begin{aligned} \Pr\left(D=D_k\right) &= \prod_{n\in D_k}\underbrace{\Pr\left(\gamma_{s,p}>\xi_p,\gamma_{s,s}>\xi_s\right)}_{P_{s,3}} \\ &\times\prod_{m\in\bar{D}_k}\left(1-\underbrace{\Pr\left(\gamma_{s,p}>\xi_p,\gamma_{s,s}>\xi_s\right)}_{P_{s,4}}\right) \\ &= \exp\left(-\sum_{n\in D_k}\frac{\beta}{\rho_1\lambda_{b,n}}\right)\times\prod_{m\in\bar{D}_k}\left[1-\exp\left(-\frac{\beta}{\rho_1\lambda_{b,m}}\right)\right], \end{aligned} \tag{15}$$

Proof. Similarly to the method to obtain (16), using (8) we can obtain the results of (17). □

According to the optimal cognitive user selection scheme, the result of $P_{out,s}\left(D=D_k\right)$ is:

$$\begin{aligned} &P_{\text{out},s}\left(D=D_k\right) \\ &= \Pr\left(\gamma_{\tilde{n},m}^{p}<\xi_p\right)+\Pr\left(\gamma_{\tilde{n},m}^{p}>\xi_p,\gamma_{\tilde{n},m}^{s}<\xi_s\right) \\ &= \prod_{n\in D_k}\left[1-\frac{\exp\left(-\sum\limits_{m\in\bar{D}_k}\frac{\beta}{\rho_2\lambda_{n,m}}\right)}{\lambda_{n,e}\sum\limits_{m\in\bar{D}_k}\lambda_{n,m}^{-1}+\lambda_{n,e}^{-1}}\right], \end{aligned} \tag{16}$$

Proof. Proof: Please see Appendix B. □

By substituting Eq. (14), Eq.(15) and Eq.(16) into Eq. (12), the OP of SU of E-MCU-CR-NOMA system under DF mode can be obtained, and the result is as shown in Eq. (17)

2) Outage probability of PU: There are two cases of the PU communication outage:

- In the first slot, when SU_n fails to decode the composite signal sent by BS $(D=\emptyset)$ and the direct transmission link BS to PU is not available.
- In the second slot, according to the proposed optimal cognitive user selection scheme, $SU_{\tilde{n}}$ is selected to send the composite signal to the PU, and the PU also receives the direct link signal sent from the base station, and the outages occur when the two signals are selectively combined.

Therefore, the outage probability of PU can be expressed as:

$$\begin{aligned} \mathrm{P}_{out}^{PU} &= \Pr\left(\gamma_{p,p}^{1}<\xi_p\right)\Pr\left(D=\emptyset\right) \\ &+ \sum_{k=1}^{2^M-1}\mathrm{P}_{out,p}\left(D=D_k\right)\Pr\left(D=D_k\right), \end{aligned} \tag{18}$$

In the first slot, when the $\text{SINR}_{p,1}$ is less than the minimum required transmission rate R, the PU will not be able to decode its signal correctly. Therefore, (19) can be obtained by applying (6).

$$\Pr\left(\gamma_{p,p}^{1}<\xi_p\right)=\Pr\left(\left(\alpha_{PU}-\alpha_{SU}\xi_p\right)\left|h_{b,p}\right|^2<\frac{\xi_p}{\rho_1}\right), \tag{19}$$

If $\alpha_{PU}-\alpha_{SU}\xi_p<0$, that $\Pr\left(\gamma_{p,p}^{1}<\xi_p\right)$ =1. Else-if $\alpha_{PU}-\alpha_{SU}\xi_p>0$, the (19) can be further written as:

$$\Pr\left(\gamma_{p,p}^{1}<\xi_p\right)=1-\exp\left(-\frac{\chi}{\rho_1\lambda_{b,p}}\right), \tag{20}$$

where $\chi=\xi_p/\left(\alpha_{PU}-\alpha_{SU}\xi_p\right)$.

In the second slot, PU combines the received signals at the first slot and the second slot, so according to (6) and (8) the outage probability when PU combines the two signals is:

$$\begin{aligned} &P_{out,p}\left(D=D_k\right)=Pr\left[\max(\gamma_{p,p}^{1},\gamma_{p,p}^{2})<\xi_p\right] \\ &=\Pr\left(\left|h_{b,p}\right|^2<\frac{\chi}{\rho_1}\right)\sum_{n\in D_k}\Pr\left(\tilde{n}=n\right)\Pr\left(\left|h_{n,p}\right|^2<\frac{\chi}{\rho_2}\right). \end{aligned} \tag{21}$$

Where the closed form expression of $P_{\tilde{n}}=\Pr\left(\tilde{n}=n\right)$ is shown in Eq.(22).

Proof. Please see the Appendix C. □

By substituting Eq. (14), Eq.(15), Eq.(20), Eq.(21) and Eq. (22) into Eq. (18), the outage probability of the PU is shown in Eq. (23).

B. Interception Probability

1) SU Intercept Probability: As shown in Fig. 1, there are two cases of SU interception event: (i) during the transmission from BS to SU_n, E can decode information κ_{SU}; (ii) during the transmission from SU to PU, E can decode the information κ_{SU}. So the interception probability of SU can be expressed as:

$$\begin{aligned} P_{int}^{SU} &= \Pr\left(\gamma_{e,s}^{1}>\xi_s\right)\Pr\left(D=\emptyset\right) \\ &+ \sum_{k=1}^{2^M-1}\mathrm{P}_{int,s}\left(D=D_k\right)\Pr\left(D=D_k\right), \end{aligned} \tag{24}$$

$$P_{\tilde{n}} = \frac{1}{\sum\limits_{m\in\bar{D}_k} \frac{\lambda_{n,e}}{\lambda_{n,m}} + 1} \left[1 + \sum_{r=1}^{2^{|D_k|-1}-1} (-1)^{\left|\tilde{D}_k(r)\right|} \prod_{l\in\tilde{D}_k(r)} \frac{\sum\limits_{m\in\bar{D}_k} \frac{1}{\lambda_{n,m}}}{\left(\sum\limits_{m'\in\bar{D}_k} \frac{\lambda_{l,e}}{\lambda_{l,m'}} + 1 \right)\left(\sum\limits_{l\in\tilde{D}_k(r)} \sum\limits_{m'\in\bar{D}_k} \frac{1}{\lambda_{l,m'}} + \sum\limits_{m\in\bar{D}_k} \frac{1}{\lambda_{n,m}} \right)} \right], \quad (22)$$

$$\begin{aligned} P_{out}^{PU} &= \prod_{n=1}^{M} \left[1 - \exp\left(-\frac{\beta}{\rho_1 \lambda_{b,n}} \right) \right] \left[1 - \exp\left(-\frac{\chi}{\rho_1 \lambda_{b,p}} \right) \right] + \sum_{k=1}^{2^M-1} \left[1 - \exp\left(-\frac{\chi}{\rho_1 \lambda_{b,p}} \right) \right] \\ &\times \sum_{n\in D_k} P_{\tilde{n}} \left[1 - \exp\left(-\frac{\chi}{\rho_2 \lambda_{n,p}} \right) \right] \exp\left(-\sum_{n\in D_k} \frac{\beta}{\rho_1 \lambda_{b,n}} \right) \prod_{m\in\bar{D}_k} \left[1 - \exp\left(-\frac{\beta}{\rho_1 \lambda_{b,m}} \right) \right]. \end{aligned} \quad (23)$$

$$\begin{aligned} P_{int}^{SU} &= \prod_{n=1}^{M} \left[1 - \exp\left(-\frac{\beta}{\rho_1 \lambda_{b,n}} \right) \right] \exp\left(-\frac{\delta}{\lambda_{b,e} \rho_{e,1}} \right) + \sum_{k=1}^{2^M-1} \left\{ 1 - \left[1 - \exp\left(-\frac{\delta}{\rho_{e,1} \lambda_{b,e}} \right) \right] \right\} \\ &\times \sum_{n\in D_k} P_{\tilde{n}} \left[1 - \exp\left(-\frac{\delta}{\rho_{e,2} \lambda_{n,e}} \right) \right] \left\{ \exp\left(-\sum_{n\in D_k} \frac{\beta}{\rho_1 \lambda_{b,n}} \right) \prod_{m\in\bar{D}_k} \left[1 - \exp\left(-\frac{\beta}{\rho_1 \lambda_{b,m}} \right) \right] \right\}. \end{aligned} \quad (27)$$

In the first slot, when the BS sends the composite signal to SU_n, an intercept event is defined as when the channel capacity of the eavesdropping link is greater than the transmission rate R_{SU}. Therefore, according to the achievable SINR of E, (25) can be obtained by applying (7):

$$\Pr\left(\gamma_{e,s}^1 > \xi_s\right) = \Pr\left(\left(\alpha_{SU} - \alpha_{PU}\xi_s\right) |h_{b,e}|^2 > \frac{\xi_s}{\rho_{e,1}} \right), \quad (25)$$

If $\alpha_{SU} - \alpha_{PU}\xi_s < 0$ that $\Pr\left(\gamma_{e,s}^1 > \xi_s\right)$=0; else-if $\alpha_{SU} - \alpha_{PU}\xi_s > 0$, equation (25) can be written as: $\Pr\left(\gamma_{e,s}^1 > \xi_s\right) = \exp\left(-\delta/\rho_{e,1}\lambda_{b,e}\right)$ where $\delta = \xi_s/\left(\alpha_{SU} - \alpha_P U\xi_s\right)$.

The expression for the probability of an intercept event in the second slot can be written as:

$$\begin{aligned} &P_{int,s}\left(D = D_k\right) = \Pr\left(\gamma_e^s > \xi_s\right) \\ &= 1 - \Pr\left(|h_{b,e}|^2 < \frac{\delta}{\rho_{e,1}} \right) \times \sum_{n\in D_k} P_{\tilde{n}} \Pr\left(|h_{n,e}|^2 < \frac{\delta}{\rho_{e,2}} \right), \end{aligned} \quad (26)$$

Substituting Eq. (14), (15) and (26) into Eq. (24), the interception probability of SU is shown in (27).

2) PU Intercept Probability: There are two cases of intercept events in PU:(i) in the first slot, when BS sends a composite signal to PU through the direct transmission link, the E can decode information κ_{PU} of PU; (ii) in the second slot, according to the proposed optimal cognitive user selection scheme, when $SU_{\tilde{n}}$ is selected to send the composite signal to the PU, the E can decode the useful information κ_{PU} of the PU. So the interception of PU can be expressed as:

$$\begin{aligned} P_{int}^{PU} &= \Pr\left(\gamma_{e,p}^1 > \xi_p\right) \Pr\left(D = \emptyset\right) \\ &+ \sum_{k=1}^{2^M-1} \mathrm{P}_{int,p}\left(D = D_k\right) \Pr\left(D = D_k\right), \end{aligned} \quad (28)$$

In the first slot, the interception occurs when the channel capacity of the eavesdropping link is greater than the transmission rate R_{PU}. Given the channel capacity of the eavesdropping link, the probability of an intercept event can be expressed as:

$$\Pr\left(\gamma_{e,p}^1 > \xi_p\right) = \Pr\left[\left(\alpha_{PU} - \alpha_{SU}\xi_p\right) |h_{b,e}|^2 > \frac{\xi_p}{\rho_{e,1}} \right], \quad (29)$$

If $\alpha_{PU} - \alpha_{SU}\xi_p < 0$ that $\Pr\left(\gamma_{e,p}^1 > \xi_p\right)$=0; else if $\alpha_{PU} - \alpha_{SU}\xi_p > 0$, the Eq. (29) can be written as:

$$\Pr\left(\gamma_{e,p}^1 > \xi_p\right) = \exp\left(-\frac{\chi}{\rho_{e,1}\lambda_{b,e}} \right), \quad (30)$$

The interception probability in the second slot can be written as:

$$\begin{aligned} &P_{int,p}\left(D = D_k\right) = \Pr\left(\gamma_e^p > \xi_p\right) \\ &= \Pr\left[\max\left(\frac{\alpha_{PU}|h_{b,e}|^2}{\alpha_{SU}|h_{b,e}|^2 + \rho_{e,1}^{-1}}, \frac{\alpha_{PU}|h_{\tilde{n},e}|^2}{\alpha_{SU}|h_{\tilde{n},e}|^2 + \rho_{e,2}^{-1}} \right) > \xi_p \right] \\ &= 1 - \Pr\left(|h_{b,e}|^2 < \frac{\chi}{\rho_{e,1}} \right) \sum_{n\in D_k} P_{\tilde{n}} \Pr\left(|h_{n,e}|^2 < \chi\rho_{e,2} \right), \end{aligned} \quad (31)$$

The IP of PU can be obtained by substituting equations (14), (15), (30) and (31) into equation (28), so the IP of PU is given by (32).

$$P_{int}^{PU}=\prod_{n=1}^{M}\left[1-\exp\left(\frac{-\beta}{\rho_1\lambda_{b,n}}\right)\right]\exp\left(\frac{-\chi}{\rho_{e,1}\lambda_{b,e}}\right)+\sum_{k=1}^{2^M-1}\left\{1-\left[1-\exp\left(\frac{-\chi}{\rho_{e,1}\lambda_{b,e}}\right)\right]\sum_{n\in D_k}P_{\tilde{n}}\left[1-\exp\left(\frac{-\chi}{\rho_{e,2}\lambda_{n,e}}\right)\right]\right\}$$
$$\times\left\{\exp\left(-\sum_{n\in D_k}\frac{\beta}{\rho_1\lambda_{b,n}}\right)\prod_{m\in\bar{D}_k}\left[1-\exp\left(-\frac{\beta}{\rho_1\lambda_{b,m}}\right)\right]\right\}. \tag{32}$$

C. Asymptotic Analysis

This section investigates the asymptotic secrecy outage performance of the considered system to gain more insights into the system performance in the high SNR regime. By letting $\rho_1=\rho_2=\rho$, the asymptotic performance is investigated as the SNR is sufficiently high, i.e., ($\rho\to\infty$) and the SNR of the channel between the BS and Eve maintain an arbitrary value. The secrecy diversity order can be expressed as $d=-\lim\frac{\log(P_\infty(\rho))}{\log\rho}$ with $P_\infty=P_{out,\infty}$ for outage performance and $P_\infty=P_{int,\infty}$ for intercept performance.

1) SU Outage Probability: When $x\to 0$, $1-e^{-x}\approx x$, then in the high SNR range, (17) can be written as:

$$P_{out,\infty}^{SU}\approx\sum_{k=0}^{2^M-1}\prod_{n\in D_k}\left[1-\frac{\left(1-\sum\limits_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{n,m}}\right)}{\sum\limits_{m\in\bar{D}_k}\lambda_{n,e}\lambda_{n,m}^{-1}+1}\right]\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}. \tag{33}$$

From (33), we can see that the diversity order of SU is equal to the number of SUs M.

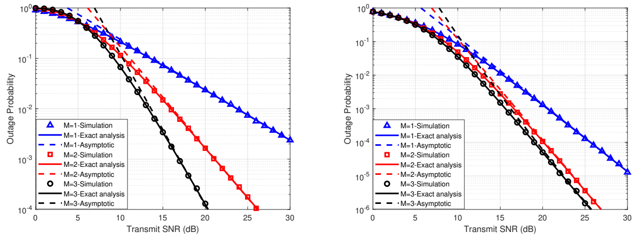
2) PU Outage Probability: By applying the same approximation principle used in equation (33), in the high SNR range, (23) can be written as:

$$\begin{aligned}&P_{out,\infty}^{PU}\\&\approx\frac{1}{\rho^{M+1}}\prod_{n=1}^{M}\frac{\beta\chi}{\lambda_{b,n}\lambda_{b,p}}+\sum_{k=1}^{2^M-1}\sum_{n\in D_k}\frac{P_{\tilde{n}}\chi^2}{\rho\lambda_{b,p}\lambda_{n,p}}\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}\\&\approx\sum_{k=0}^{2^M-1}\sum_{n\in D_k}\frac{P_{\tilde{n}}\chi^2}{\rho\lambda_{b,p}\lambda_{n,p}}\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}.\end{aligned} \tag{34}$$

From (34), we can see that the diversity order of PU is equal to $1+M$, in which additional diversity gain of 1 can be obtained due to the direct link from BS to PU for PU.

3) SU Interception Probability: In the high SNR range, (27) can be written as :

$$\begin{aligned}&P_{int,\infty}^{SU}\approx\prod_{n=1}^{M}\frac{\beta}{\rho\lambda_{b,n}}+\\&\sum_{k=1}^{2^M-1}\sum_{n\in D_k}P_{\tilde{n}}\left(1-\frac{\delta^2}{\rho_{e,1}\lambda_{b,e}\rho_{e,2}\lambda_{b,n}}\right)\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}\\&\approx\sum_{k=0}^{2^M-1}\sum_{n\in D_k}P_{\tilde{n}}\left(1-\frac{\delta^2}{\rho_{e,1}\lambda_{b,e}\rho_{e,2}\lambda_{b,n}}\right)\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}.\end{aligned} \tag{35}$$



(a) SU outage probability (b) PU outage probability

Fig. 2: OP as a function of transmitting SNR for SU and PU under different cognitive users M

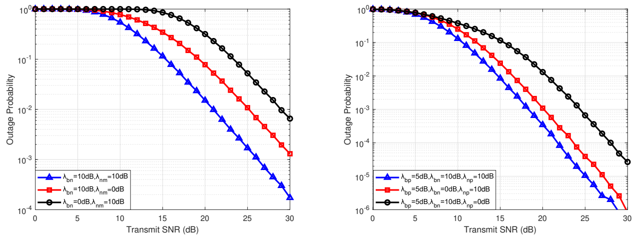
4) PU Intercept Probability: Similarly, in the high SNR range, the equation (32) can be written as:

$$\begin{aligned}&P_{int,\infty}^{PU}\approx\prod_{n=1}^{M}\frac{\beta}{\rho\lambda_{b,n}}+\\&\sum_{k=1}^{2^M-1}\sum_{n\in D_k}P_{\tilde{n}}\left(1-\frac{\chi^2}{\rho_{e,1}\lambda_{b,e}\rho_{e,2}\lambda_{b,n}}\right)\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}\\&\approx\sum_{k=0}^{2^M-1}\sum_{n\in D_k}P_{\tilde{n}}\left(1-\frac{\chi^2}{\rho_{e,1}\lambda_{b,e}\rho_{e,2}\lambda_{b,n}}\right)\prod_{m\in\bar{D}_k}\frac{\beta}{\rho\lambda_{b,m}}.\end{aligned} \tag{36}$$

From (35) and (36), we can see that the diversity order for intercepting PU and SU are equal to M. This is because the E did not utilize SIC to decode the wiretap signals. Consequently, the same diversity order for intercepting PU and SU can be obtained.

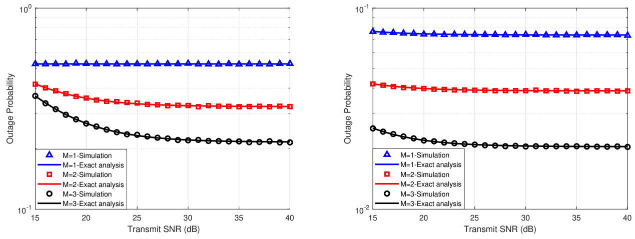
D. Complexity analysis

The main difference in complexity lies in the proposed secondary user cooperation scheme and the traditional secondary users that only consider legitimate link channels. According to the comparison of 1) the optimal sub-user cooperation scheme and 2) the sub-optimal sub-user cooperation scheme in Section 3.1, it can be seen that when the eavesdropping link channel states information can be predicted in advance, it is compared with the sub-optimal sub-user cooperation. As far as the solution is concerned, the optimal sub-user collaboration solution only adds subtraction operations, so the implementation complexity will not increase too much.



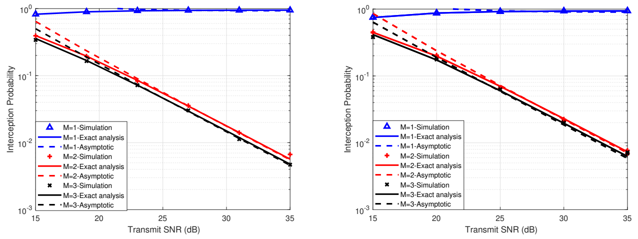
(a) SU outage probability (b) PU outage probability

Fig. 3: OP as a function of transmitting SNR for SU and PU under different link conditions



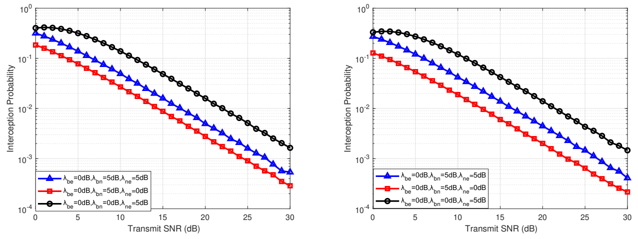
(a) SU outage probability (b) PU outage probability

Fig. 4: OP as a function of transmitting SINR ρ_2 for SU and PU under different cognitive users M



(a) SU interception probability (b) PU interception probability

Fig. 5: IP as a function of transmitting SINR for SU and PU under different cognitive users M



(a) SU interception probability (b) PU interception probability

Fig. 6: IP as a function of transmitting SINR for SU and PU under different link conditions

V. NUMERICAL RESULTS

The OP and IP performance of SU and PU are studied for both the proposed optimal cognitive user selection scheme and that only considering the main link state in [25] under the proposed E-MCU-CR-NOMA system. We also focus on the impact of the transmitted SINR and the number of SUs on the performance of the considered system.

The parameters are set as: $\rho_1 = \rho_2 = \rho$, $\rho_{e,1} = \rho_{e,2} = 10$ dB; $\lambda_{bp} = \lambda_{bn} = \lambda_{np} = \lambda_{nm} = 10$ dB and $\lambda_{be} = \lambda_{ne} = 0$ dB. In the considered model, the PU channel condition is relatively poor, while the SU is close to the base station and has better channel conditions. Therefore, R_{PU} and R_{SU} are set to 1 bit/sHz^{-1} and $1.5bit/sHz^{-1}$ respectively [25]. If it is not specially defined, $\alpha_{PU} = 0.8$, $\alpha_{SU} = 0.2$.

A. Outage Probability Analysis

Figure 2 shows the OP vs. SNR for SU and PU under different number of SUs when the proposed optimised scheme is utilized. It can be seen that the simulation results are consistent with the analysis results very well, and the asymptotic matches the analysis results in high SNR regions, which verifies the accuracy of the analysis results. Furthermore, it can be seen from Fig. 2(a) and Fig. 2(b) that with the increase of SNR, the OP of SU and PU decreases, especially in the case of high SNR, the user outage performance is improved significantly. In other words, the outage performance of the E-MCU-CR-NOMA system can be enhanced by increasing the transmission power at BS. In addition, it can be seen from Fig. 2(a) and Fig. 2(b) that the OP of SU and PU obtained by the proposed scheme decreases with the increase of the number of SUs M. Moreover, the outage performance of SU is significantly improved, however which is not the case for PU when M increases from 2 to 3. This is because with the increase of M, the probability of a non-empty decoding set of SU is close to 1. Therefore, the OP of PU is mainly determined by the transmitted SNR and the target data rate. It is noted that PU can achieve a greater outage diversity order than SU by comparing 2(a) and Fig. 2(b).

Figure 3 shows the variation of OP vs. SNR for both SU and PU under different link conditions when the proposed optimised scheme is adopted to assist PU transmission. It can be seen from Fig. 3(a) that, the outage performance of SU can be effectively improved by improving the channel conditions of the link from BS to SU and the secondary link. For details, the OP of SU under the condition that $\lambda_{nm} = 0dB$ and $\lambda_{bn} = 0dB$ is less than that $\lambda_{bn} = 0dB$ and $\lambda_{nm} = 10dB$. It can also be seen from Fig. 3(b) that, when the channel conditions of the links from BS to SU and SU to PU are improved, the outage performance of PU can be improved. However, compared with the BS to PU link, improving the channel conditions of the SU to PU link can significantly improve the outage performance of PU.

Fig. 4 shows OP vs. SNR for SU and PU with different SU number M, where the proposed optimised scheme is used to assist PU's transmission, it can be seen from Fig. 4(a) and 4(b) that the OP of SU and PU tends to upper floor with the increase of SNR at SU. Furthermore, according to 26 and 32, it can be seen that the transmission SNR of SU has little impact on the outage performance of SU and PU.

B. Interception Probability Analysis

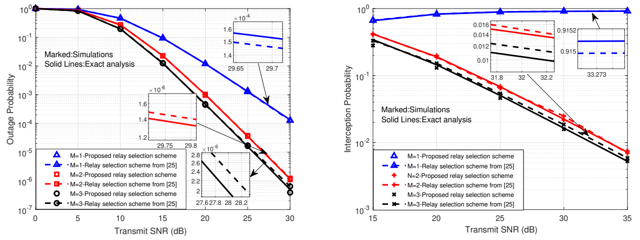
Fig.5(a) and Fig.5(b) show the IP.vs SNR of SU and PU uder different SU number M, where the proposed optimised scheme is selected to assist PU transmission. It can be seen that the analysis results are consistent with the simulation results very well, and the asymptotic is consistent with the analysis results in the high SNR region, which verifies the accuracy of the analysis results. It can be seen from Fig.5(a) that when M = 1, the IP of SU tends to a fixed value with the increase of SNR ρ_1. We can see from 27 that this fixed value is non-related with ρ_1. It can also be seen from Fig.5(b) that the IP of PU will gradually decrease with the increase of the transmitted SNR of BS, which indicates that the signal of PU will be more difficult to be intercepted with the increase of ρ_1. On the other hand, when $M = 1$, the IP of PU tends to be constant, which can be seen from 32 that the IP of PU tends to be a fixed value with the increase of ρ_1. Finally, it is noted that PU can achieve higher intercept diversity order than SU by comparing 5(a) and Fig. 5(b). Therefore, a better secrecy performance can be achieved by PU than by SU, which is less sensitive to eavesdroppers, especially when M increases, which can be concluded by combining Fig. 2 and Fig. 5.

Fig.6 shows IP vs. SNR of SU and PU under different link conditions when the proposed optimised scheme is used to assist PU transmission. It can be seen from Fig.6(a) and Fig.6(b) that improving the channel conditions of the main link or deteriorating the channel conditions of the eavesdropping link can reduce the intercept performance of SU and PU and improve the security of the system. In addition, from Fig.6(a) and Fig.6(b), we can see that the intercept performance of SU and PU can be better reduced by improving the channel conditions of the main link compared with deteriorating the channel conditions of the eavesdropping link.

Fig.7 shows the OP and IP vs. SNR of PU with different number of SUs M under the relay selection scheme in [25] and the proposed optimised scheme. As can be seen from Fig.7(a) and Fig.7(b), when $M = 1$ and 2, the proposed optimised scheme in this paper and the relay selection scheme in [25] have little impact on the outage performance and intercept performance of PU; when $M = 3$, we can see that the outage performance and intercept performance of the proposed optimised scheme in this paper are slightly better than the relay selection scheme in [25], especially under high SNR. Therefore, in the low SNR range, we can use a suboptimal relay selection scheme to improve the outage performance and intercept performance of PU.

VI. Conclusions and Further works

This paper proposes an E-MCU-CR-NOMA system model based on DF. From the perspective of outage performance and interception performance of SU and PU, an optimal cognitive user selection scheme is proposed and analysed for E-MCU-CR-NOMA. The impact of the physical layer security performance of the system is considered, and the closed expressions of the outage probability and interception probability of SU and PU are derived. The simulation results show that increasing the number of secondary users can effectively improve the outage performance and interception performance of SUs and PU. At the same time, we found a sub-optimal secondary user selection scheme by which PU can achieve the same level as that proposed in this paper.



(a) PU outage probability

(b) PU interception probability

Fig. 7: OP and IP as a function of transmitting SNR for PU under two relay selection schemes

It is noted that the effective secrecy throughput is an essential criterion in evaluating the achievable secrecy rate for the QoS requirement of the communication system [14], the throughput of the PU and SU can be obtained based on the known SINR in this paper. However, due to the aims of this paper, we did not analyse it in the manuscript. Instead, we will study secrecy throughput and power allocation optimisation in future work.

Appendix A: Proof of FORMULA 14

The first item $P_{s,1}$ in (14) can be written as:

$$\begin{aligned} P_{s,1} &= \Pr\left(|h_{b,n}|^2 < \frac{\xi_p}{\rho_1\left(\alpha_{PU} - \alpha_{SU}\xi_p\right)}\right) \\ &= 1 - \exp\left(-\frac{\xi_p}{\rho_1\lambda_{b,n}\left(\alpha_{PU} - \alpha_{SU}\xi_p\right)}\right), \end{aligned} \tag{A.1}$$

The second item $P_{s,2}$ in (14) can be written as:

$$P_{s,2} = \Pr\left(|h_{b,n}|^2 > \frac{\xi_p}{\rho_1\left(\alpha_{PU} - \alpha_{SU}\xi_p\right)}, |h_{b,n}|^2 < \frac{\xi_s}{\rho_1\alpha_{SU}}\right), \tag{A.2}$$

When $\frac{\xi_p}{(\alpha_{PU} - \alpha_{SU}\xi_p)} > \frac{\xi_s}{\alpha_{SU}}$, (A.2) can be further calculated as

$$P_{s,2} = \exp\left[-\frac{\xi_p}{\rho_1\lambda_{b,n}\left(\alpha_{PU} - \alpha_{SU}\xi_p\right)}\right] - \exp\left(-\frac{\xi_s}{\rho_1\lambda_{b,n}\alpha_{SU}}\right), \tag{A.3}$$

Combined (A.1), (A.3) and (14), $\Pr\left(D = \emptyset\right)$ can be written as:

$$\Pr\left(D = \emptyset\right) = \prod_{n=1}^{M}\left[1 - \exp\left(-\frac{\xi_s}{\alpha_{SU}\rho_1\lambda_{b,n}}\right)\right], \tag{A.4}$$

When $\frac{\xi_p}{(\alpha_{PU} - \alpha_{SU}\xi_p)} < \frac{\xi_s}{\alpha_{SU}}$, $P_{s,2} = 0$, thusly $\Pr\left(D = \emptyset\right)$ can be written as follows:

$$\Pr\left(D = \emptyset\right) = \prod_{n=1}^{M}\left[1 - \exp\left(-\frac{\xi_p}{\left(\alpha_{p,1} - \alpha_{s,1}\xi_p\right)\rho_1\lambda_{b,n}}\right)\right]. \tag{A.5}$$

In summary, combining (A.4) and (A.5), (14) can be obtained.

APPENDIX B: PROOF OF FORMULA 16

According to the best secondary user selection criteria described in section III, $P_{out,s}\left(D=D_k\right)$ can be expressed as:

$$\begin{aligned} P_{out,s}\left(D=D_k\right) &= \Pr\left(\left|h_{\tilde{n},m}\right|^2 < \frac{\beta}{\rho_2}\right) \\ &= \Pr\left(\max_{n\in D_k}\left\{\min_{m\in\bar{D}_k}\left\{\left|h_{n,m}\right|^2\right\} - \left|h_{n,e}\right|^2\right\} < \frac{\beta}{\rho_2}\right) \\ &= \prod_{n\in D_k}\left[1-\Pr\left(\underbrace{\min_{m\in\bar{D}_k}\left\{\left|h_{n,m}\right|^2\right\}}_{X} > \frac{\beta}{\rho_2} + \underbrace{\left|h_{n,e}\right|^2}_{Y}\right)\right] \\ &= \prod_{n\in D_k}\left\{1-\int_0^\infty\left[1-F_X\left(\frac{\beta}{\rho_2}+y\right)\right]f_Y\left(y\right)dy\right\}, \end{aligned} \tag{B.1}$$

The cumulative distribution function of (CDF) X and the probability density function (PDF) of Y are as [25]:

$$F_X\left(x\right) = 1-\exp\left(-\sum_{m\in\bar{D}_k}\frac{x}{\lambda_{n,m}}\right), \tag{B.2}$$

$$f_{Y(y)} = \frac{1}{\lambda_{n,e}}\exp\left(-\frac{y}{\lambda_{n,e}}\right). \tag{B.3}$$

Substituting (B.2) and (B.3) into (B.1) and performing integral operation, we can get the expression of (16).

APPENDIX C: PROOF OF FORMULA 22

According to the best secondary user selection criteria described in section III, $P_{\tilde{n}}$ can be expressed as the probability of $\underbrace{\min_{m\in\bar{D}_k}\left\{\left|h_{n,m}\right|^2\right\} - \left|h_{n,e}\right|^2}_{Q} > \underbrace{\min_{m'\in\bar{D}_k}\left\{\left|h_{l,m'}\right|^2\right\} - \left|h_{l,e}\right|^2}_{R}$).

Using the law of conditional probability [25], We can obtain that:

$$P_{\tilde{n}} = \int_0^\infty \underbrace{\prod_{l\in D_k-\{n\}} F_R\left(q\right)}_{\Delta} f_Q\left(q\right)dq, \tag{C.1}$$

Let $X_1 = \min_{m\in\bar{D}_k}\left\{\left|h_{n,m}\right|^2\right\}$, $Y_1 = \left|h_{n,e}\right|^2$. Then the CDF of $Q = X_1 - Y_1$ can be expressed as:

$$\begin{aligned} F_Q\left(q\right) &= \Pr\left(X_1 - Y_1 \le q\right) \\ &= 1-\frac{1}{\sum\limits_{m\in\bar{D}_k}\frac{\lambda_{n,e}}{\lambda_{n,m}}+1}\exp\left(-\sum_{m\in\bar{D}_k}\frac{q}{\lambda_{n,m}}\right), \end{aligned} \tag{C.2}$$

It is easy to get the PDF of $Q = X_1 - Y_1$ by making derivation of (C.2). We can obtain that

$$f_Q\left(q\right) = \frac{\sum\limits_{m\in\bar{D}_k}\frac{1}{\lambda_{n,m}}}{\sum\limits_{m\in\bar{D}_k}\frac{\lambda_{n,e}}{\lambda_{n,m}}+1}\exp\left(-\sum_{m\in\bar{D}_k}\frac{q}{\lambda_{n,m}}\right), \tag{C.3}$$

Similarly, let $X_2 = \min_{m'\in\bar{D}_k}\left\{\left|h_{l,m'}\right|^2\right\}$, $Y_2 = \left|h_{l,e}\right|^2$. Then the CDF of $Y = X_2 - Y_2$ can be expressed as:

$$\begin{aligned} F_R(r) &= P_r(X_2 - Y_2 \leqslant r) \\ &= 1-\frac{1}{\sum\limits_{m'\in\bar{D}_{k,k}}\frac{\lambda_{l,e}}{\lambda_{l,m'}+1}}\exp\left(-\sum_{m'\in\bar{D}_k}\frac{r}{\lambda_{l,m'}}\right), \end{aligned} \tag{C.4}$$

Substituting (C.4) into (C.1), and using the polynomial expansion [32], then Δ can be expressed as:

$$\begin{aligned} \Delta = 1+ &\sum_{r=1}^{2^{|D_k|-1}-1}(-1)^{\left|\tilde{D}_k(r)\right|}\exp\left(-\sum_{l\in\tilde{D}_k(r)}\sum_{m'\in\bar{D}_k}\frac{q}{\lambda_{l,m'}}\right) \\ &\times\prod_{l\in\tilde{D}_k(r)}\frac{1}{\sum\limits_{m'\in D_{k,k}}\frac{\lambda_{l,e}}{\lambda_{l,m'}}+1}. \end{aligned} \tag{C.5}$$

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

Substituting (C.3) and (C.5) into (C.1) and performing the required integration, the closed expression of $P_{\tilde{n}}$ can be obtained.

REFERENCES

[1] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial internet of things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78 238–78 259, 2018.

[2] X. Liu, H. Ding, and S. Hu, "Uplink resource allocation for noma-based hybrid spectrum access in 6g-enabled cognitive internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15 049–15 058, 2021.

[3] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 17–25, 2017.

[4] A. Ali, L. Feng, A. K. Bashir, S. El-Sappagh, S. H. Ahmed, M. Iqbal, and G. Raja, "Quality of service provisioning for heterogeneous services in cognitive radio-enabled internet of things," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 328–342, 2020.

[5] X. Liu and X. Zhang, "Noma-based resource allocation for cluster-based cognitive industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5379–5388, 2020.

[6] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular iot: Potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.

[7] 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, 2018.

[8] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-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, 2018.

[9] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. K. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green internet-of-things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, 2021.

[10] V.-P. Hoang, V.-L. Dao, and C.-K. Pham, "Design of ultra-low power aes encryption cores with silicon demonstration in sotb cmos process," *Electronics Letters*, vol. 53, no. 23, pp. 1512–1514, 2017.

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

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

[13] H. Lei, Z. Yang, K.-H. Park, I. S. Ansari, Y. Guo, G. Pan, and M.-S. Alouini, "Secrecy outage analysis for cooperative noma systems with relay selection scheme," *arXiv preprint arXiv:1811.03220*, 2018.

[14] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.

[15] Y. Liu, Z. Ding, M. Elkashlan, and J. Yuan, "Nonorthogonal multiple access in large-scale underlay cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 152–10 157, 2016.

[16] S. Lee, T. Q. Duong, D. B. da Costa, D.-B. Ha, and S. Q. Nguyen, "Underlay cognitive radio networks with cooperative non-orthogonal multiple access," *IET Communications*, vol. 12, no. 3, pp. 359–366, 2018.

[17] Y. Song, W. Yang, Z. Xiang, H. Wang, and F. Cao, "Research on cognitive power allocation for secure millimeter-wave noma networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 424–13 436, 2020.

[18] N. Nandan, S. Majhi, and H.-C. Wu, "Secure beamforming for mimo-noma-based cognitive radio network," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1708–1711, 2018.

[19] 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, 2018.

[20] Z. Xiang, W. Yang, Y. Cai, Z. Ding, and Y. Song, "Secure transmission design in harq assisted cognitive noma networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2528–2541, 2020.

[21] 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, 2018.

[22] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired noma network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700–714, 2019.

[23] 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 Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7214–7219, 2019.

[24] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, and R. Q. Hu, "Security-reliability tradeoff analysis for cooperative noma in cognitive radio networks," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 83–96, 2018.

[25] L. Lv, J. Chen, and Q. Ni, "Cooperative non-orthogonal multiple access in cognitive radio," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2059–2062, 2016.

[26] W. Liang, Z. Ding, Y. Li, and L. Song, "User pairing for downlink non-orthogonal multiple access networks using matching algorithm," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5319–5332, 2017.

[27] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Z. Ding, "Exploiting full/half-duplex user relaying in noma systems," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 560–575, 2018.

[28] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail, and C. Maple, "Adaptive and optimum secret key establishment for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2310–2321, 2021.

[29] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[30] 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," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[31] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure communications in a unified non-orthogonal multiple access framework," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 2163–2178, 2020.

[32] D.-T. Do, T. A. Le, T. N. Nguyen, X. Li, and K. M. Rabie, "Joint impacts of imperfect csi and imperfect sic in cognitive radio-assisted noma-v2x communications," *IEEE Access*, vol. 8, pp. 128 629–128 645, 2020.

Meiling Li is a Professor with the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. She was also a Visiting Scholar at the University of Warwick, U.K and Tsinghua University. 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.

Hu Yuan is a research fellow at the University of Warwick, where his research focus on the security and privacy aspects of IoT, including internet of bio-nano things, vehicular communication networks, user behaviours identification and further space system. He was invited to the House of Lord to present the IoT's cyber security research findings. He was the leading researcher for the project IoT-Tram (IoT Transport and Mobility Demonstrator) the first real word cyber security test in the UK.

Carsten Maple is the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research at the University and Professor of Cyber Systems Engineering in WMG. He is also a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. He is a Fellow of the Alan Turing Institute, the National Institute for Data Science and AI in the UK, where he is a principal investigator on a $ 5 million project developing trustworthy national identity to enable financial inclusion.

Weijie Cheng received his M.Sc degree in electronic communication engineering from Taiyuan University of Science and Technology.

Gregory Epiphaniou currently holds a position as an Associate Professor of Security Engineering at the University of Warwick. Part of his current research activities are formalised around Cyber Effects modelling and Physical Layer Security, exploiting V-V channels' time-domain physical attributes. He led and contributed to several research projects funded by EPSRC, IUK and local authorities totalling over £4M and authored over 100 publications.