Physical Layer Security in NOMA-Enabled Cognitive Radio Networks With Outdated Channel State Information

YONG CHEN\textsuperscript{1}, TAO ZHANG\textsuperscript{2}, YONGXIANG LIU\textsuperscript{2}, AND XIAOQIANG QIAO\textsuperscript{2}

\textsuperscript{1}College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
\textsuperscript{2}The Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210007, China

Corresponding authors: Tao Zhang (ztcool@126.com) and Xiaoqiang Qiao (qxq0527@163.com)

This work was supported in part by the Project of Natural Science Foundation of China under Grant 61801496 and Grant 61801497; in part by the National Postdoctoral Program for Innovative Talents of China under Grant BX20180374; in part by the Defense Science Foundations of China under Grant 2019-JCQJ-JJ-221; and in part by the National University of Defense Technology Youth Innovation Award Research Project under Grant 18-QN CXJ-30.

\textbf{ABSTRACT} In this article, we investigate physical layer security (PLS) in non-orthogonal multiple access-enabled (NOMA-enabled) underlay cognitive radio networks (CRNs) with outdated channel state information (CSI). Considering the influence of outdated CSI on the interference of secondary transmitter (Alice) to primary user (PU), the constraint for the power is adopted to guarantee the quality-of-service (QoS) of PU over Nakagami-\(m\) channels. To further analyze the NOMA-enabled underlay CRNs with outdated CSI in PLS perspective, the secrecy performance is evaluated by the closed-form expressions for connection outage probability (COP), the intercept probability (IP) and effective secrecy throughput (EST). In addition, Monte Carlo simulations are provided to verify the derived analytical results. From the analytical results and simulations, it is concluded that a) with the increment of the channel parameter \(m\), the secrecy performance of the considered networks increases in the low SNR region and decreases in the high SNR region, b) the connection performance with the outdated CSI of the interference links only reduce in the high SNR region, because the power margin factor changes significantly in this region, c) considering the impact of the constraint for the power, the secrecy performance and EST performance of the considered networks with the outdated CSI of the interference links increase in the high SNR region, d) the considered networks with NOMA scheme can achieve higher EST than that with orthogonal multiple access (OMA) scheme.

\textbf{INDEX TERMS} Physical layer security, cognitive radio, non-orthogonal multiple access (NOMA), outdated channel state information, effective secrecy throughput.

\section*{1. INTRODUCTION}
With the rapid development of communication technology, the Internet of Things (IoT) leads to a new research dimension in the future, which is a worldwide network that allows people and things to be connected anytime, anywhere, with anything and anyone, ideally using any path/network and any service [1]. In order to implement this network, we need to provide a lot of support includes range, data bandwidth and availability of spectrum. However, due to large-scale access, spectrum resources have become scarce and crowded, and IoT devices undergo severe data exchange interference.

The associate editor coordinating the review of this manuscript and approving it for publication was Jules Merlin Moualeu.

Therefore, applying cognitive radio (CR) and Non-orthogonal multiple access (NOMA) capabilities to the IoT is a promising solution to the problem of scarcity of spectrum in IoT networks [1]–[5].

\textbf{A. BACKGROUND}
Both NOMA and CR show the capability to enable efficient utilization and play the crucial roles in solving the problem of scarce spectrum [6]. Based on this, integrating NOMA and CR techniques into IoT has the tremendous potential to improve spectral efficiency and increase the system capacity with the explosive growth of IoT devices and the rapid increase of wideband wireless services [2].

In cognitive radio networks (CRNs), unlicensed secondary users are allowed to dynamically access the licensed primary...
spectrum while protecting the quality-of-service (QoS) of the primary one, which is a key technology to improve the utilization of spectrum resources [7]. According to existing researches, there are three main CRNs spectrum sharing methods, i.e., underlay, overlay and interweave [8]. The underlay CR is the most widely used method to access the licensed spectrum and easily to be realized in CRNs. Besides CR, the key idea of NOMA is to encourage spectrum sharing among multiple users within one resource block by exploiting power domain multiplexing [9], [10]. Considering both technologies have good application prospects, some researches have combined NOMA and underlay CR appropriately to reduce interference and make better use of the spectrum resources [11]–[15].

Due to the large-scale deployment of devices in communication system, there are frequent information interaction and spectrum sharing in NOMA CRNs, which will make the privacy information of users in NOMA CRNs vulnerable to attacks. At the same time, with the continuous improvement of computer computing power, traditional encryption technology can no longer meet the needs of wireless communication security design. As an important supplement to the traditional communication security method, the physical layer security (PLS) technology utilizes the dynamic characteristics of the link, and guarantees the security of the communication from the perspective of information theory through the difference of the main stealing channel, which is a notion for solving the security of wireless communication [16].

Recently, several works have investigated the security issues from the perspective of the physical layer in NOMA-enabled networks [17]–[19]. In [17] and [18], the authors investigated the physical layer security for cooperative NOMA systems, where both amplify-and-forward (AF) and decode-and-forward (DF) protocols and relay selection scheme are considered. In [19], Lei et al. considered a NOMA network wiretapped by multiple illegitimate receivers and investigate the diversity gain of multiple antennas with a max-min (MM) transmit antenna selection (TAS) strategy. While these prior works have significantly improved our understanding on the impact of cooperative NOMA and multi-antenna techniques to the secrecy diversity gain of the considered networks, they are all done in non-cognitive scenarios and can not be easily applied to the underly CRNs. In [20], the authors introduced CR to NOMA network and propose two secondary user selection schemes, the comprehensive analysis is provided to analyze the effect of multiuser gain on the secrecy performance of the primary user. In [21], Xiang et al. investigated the secrecy performance of NOMA CRNs with multiple primary and secondary users, in which the secondary users were considered as eavesdroppers. In addition, they introduced hybrid automatic repeat request (HARQ) technique to improve the secrecy performance of the NOMA CRNs in [22], where a security-required user (SRU) is paired with a quality of service (QoS)-sensitive user (QSU) to perform NOMA. However, one major drawback of the above works is that the users are equipped with single antenna, hence the multi-antenna gain has not been well understood. In [23], the authors assumed that the primary transmitter of the NOMA CRNs is equipped with multi-antennas, moreover, an artificial-noise-aided cooperative jamming scheme was proposed to improve the secrecy performance of the primary network. Furthermore, NOMA CRNs for mmWave communications have been studied, Song et al. develops secure communication in mmWave NOMA networks based on cognitive power allocation scheme is studied by preferentially satisfying the QoS of primary user [24]. Recently, in [25], the authors studied the security performance of CR-NOMA heterogeneous network with interference base stations to maximize the secure sum rate by using joint user pairing and resource allocation. In [26], the authors modeled the spectrum efficient CR-NOMA framework, where the transmitter hires a pair of users to perform relaying and jamming. However, the key limitations of these aforementioned works are that the perfect knowledge of the channel state information (CSI) of the secondary transmission links and the interference links between the primary user (PU) and secondary transmitter.

In the practical scenario, the perfect CSI is challenging to obtain. Due to the impact of channel estimation error, limited feedback and outdated CSI, the perfect CSI is challenging to obtain, some papers have studied the impact of imperfect CSI in wireless networks [27]–[29]. Moreover, the attractive advantages of PLS depend on reliable CSI at the transmitter, and the maximum secrecy rate is only achievable under perfect CSI at the transmitter. The research on PLS with imperfect CSI plays a significant role for the future deployment of PLS in 5G networks [30]. We comb some recent papers on imperfect CSI in PLS [31]–[33]. These papers revealed that the imperfect CSI will reduce the secrecy performance of the considered networks, and can provide guidance for related research under imperfect CSI. In addition, the outdated CSI is easy to cause interference in the demodulation sequence of the NOMA system. In this article, the impact of outdated CSI on the secrecy performance of NOMA CRNs should be considered.

B. MOTIVATION AND CONTRIBUTION

Different from all previous works, we consider the NOMA-enabled CRNs, in which the secrecy secondary transmitter (Alice) transmits information to two users (user $N$ and user $M$) in the presence of an eavesdropper (Eve) over Nakagami-$m$ channels $^1$ with outdated CSI. Assuming that the poor user $M$ is far away from Alice, we propose an effective approach to use the first user $N$ to cooperatively transmit data to user $M$. For improving the secrecy performance, we propose the constraint for the power and provide a comprehensive analysis of the effect of NOMA-enabled transmission strategy in

$^1$Nakagami-$m$ distribution models provides a good fit to indoor and outdoor multipath propagation, and it is useful for a wider class of fading environments, which comprises the Rayleigh fading ($m = 1$) as a special case.
underlay CRNs. The contributions of this article are summarized as follows:

- In this work, a new NOMA-enabled transmission strategy is designed to improve secrecy performance in underlay CRNs. Significantly, considering the interference caused by secondary transmitter (Alice) to PU due to outdated CSI, the constraint for the power is adopted to guarantee the normal communication of PU. This transmission strategy can not only effectively improve the spectrum utilization of the considered network, but also ensure the security of the data.
- The closed-form expressions for the connection outage probability (COP), intercept probability (IP) and effective secrecy throughput (EST) of secondary users are derived in the proposed secure NOMA-enabled CRNs over Nakagami-$m$ fading channels with outdated CSI, which accurately show the relationship between various variables and the impact on security. What’s more, it provides accurate evaluation indicators for the design of system parameters in the next step.
- We have investigated the performance of the considered networks, and our results demonstrate that: 1) the secrecy performance of the considered networks over Nakagami-$m$ channels as channel parameter $m = 2$ is better than that over Rayleigh channels ($m = 1$) at low SNR, 2) the connection performance of the considered networks reduced with the outdated CSI of the secondary transmission channel links, 3) the constraint for the power can effectively prevent information leakage of secondary users and increase the EST of the considered networks, 4) secondary users of the considered networks with NOMA scheme can achieve a higher EST than that with OMA scheme.

The remainder of the paper is organized as follows. The system models are described in Section II. In Section III, we derive a set of closed-form expressions for the COP, IP and EST with outdated CSI of considered networks. The simulation results and discussions are presented in Section IV. Finally, we conclude this article in Section V.

II. SYSTEM MODEL

We consider a NOMA-enabled system in underlay CRNs, which includes a secondary transmitter (Alice), a primary user (PU), two secondary users (user $N$ and user $M$) and an eavesdropper (Eve) as shown in Fig 1. We assume that there is no direct path between Alice and user $M$, so user $N$ is the relay in this network at the same time. Furthermore, we assume that Alice can be equipped with multiple-antenna due to its relatively high computational power and volume; rather, secondary users are equipped with one antenna due their limited space and power consumption. In order to simplify the system model, Alice is equipped with $N_A$-antenna, and other notes are equipped with a single antenna and operates in half duplex mode. What’s more, we assume all the channel coefficient from node $A$ to node $B$ is denoted as $h_{AB}$, which is assumed to experience independent block Nakagami-$m$ fading with $E|h_{AB}|^2 = \Omega_{AB}$ and fading parameters $m_{AB}$. Letting $\Omega_{AB} = d_{AB}^{-\alpha}$, where $\alpha$ is the path loss exponent. In practical systems, obtaining the perfect CSI of IoT networks is extremely difficult, and the imperfect CSI is a common phenomenon in 5G applications, e.g., the outdated CSI caused by the rapid channel variation in high-speed mobile communications, so in this article the channel coefficient can be modeled as [34], [35]

$$\tilde{h}_{AB} = \rho_{AB} h_{AB} + \sqrt{1 - \rho_{AB}^2} e_{AB}, \quad (1)$$

where $e_{AB}$ is the complex Gaussian variable having the same variance as $h_{AB}$ and is uncorrelated with $h_{AB}$, $\rho_{AB}$ is the time correlation coefficient between $\tilde{h}_{AB}$ and $h_{AB}$. According to Jake’s autocorrelation model, we have $\rho_{AB} = J_0(2\pi fT)$, where $f$ is the represents the maximum Doppler frequency, $T$ is the delay between the selection instant and the transmission instant, and $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind [36, Eq. (8.411)].

In this network, Alice transmits signals to user $N$ include data $x_1$ for user $N$ and $x_2$ for user $M$ according to NOMA principle. The power allocation coefficients satisfy the conditions that coefficient of user $M$, which is defined as $a_2$ is larger than that of user $N$, which is defined as $a_1$, $a_2 > a_1$ and $a_1 + a_2 = 1$ [9], [10]. Without loss of generality, the following assumptions are given: 1) all channels have an additive white Gaussian noise (AWGN) with zero mean and variance $\sigma^2$. 2) Similar to [12], we assume that CSI of the primary transmitter (PT) is not available at the secondary users. Thus, according to the Central Limit Theorem, the interference of all notes from PT can be treated as AWGN noise with $CN(0, \eta \sigma^2)$ in CRNs.

In the first slot, Alice adopts the maximum ratio transmission (MRT) [40]–[43] scheme with the advantages of multiple antennas to send normalized messages to user $N$. The normalized messages $x_1$ and $x_2$ are superimposed coding where $x_1$ is the signal for user $N$ and $x_2$ is the signal for user $M$. Then, considering the feedback delay in the network,
the received signal at user $N$ can be modeled as

$$y_N = \tilde{h}_{AN}^T w \left( \sqrt{P_{s1} a_1 x_1} + \sqrt{P_{s2} a_2 x_2} \right) + g_N + n_N. \tag{2}$$

where $\tilde{h}_{AN} \in \mathbb{C}^{N_1 \times 1}$ is the channel vector which denotes the delayed current channel $h_{AN}$ as previously mentioned. However, due to the variation of feedback channel, the CSI received at Alice is outdated. That is to say, the transmit beamforming is designed based on the outdated channel $\tilde{h}_{AN}^T$, i.e., $w = \tilde{h}_{AN}^T$. And $P_{s1}$ is the total power at the secondary transmitter Alice, $g_N$ is the interference from PT to user $N$ and $n_N$ is the AWGN at user $N$. In order to guarantee the quality of service requirement for PU, interference power at PU must be kept below a tolerable interference threshold $Q$. The total power $P_{s1}$ of the transmission needs to satisfy condition that $P_{s1} = \min \left\{ \frac{Q}{|h_{AP}|^2}, P_I \right\}$, where $P_I$ is the maximum available power of Alice. However, due to the outdated CSI of the interference links, it is not possible to meet the interference power constraint. Instead, the power margin that satisfies the predetermined interference outage probability can be expressed as follows:

$$P_{s1} = \min \left\{ \kappa_1 \frac{Q}{|\tilde{h}_{AP}|^2}, P_I \right\}, \tag{3}$$

where $\kappa_1$ is the power margin factor at Alice, the power margin factor $\kappa_1$ can be numerically expressed as follows:

$$P_{s1} = \int \left( m_{AP} \frac{m_{AP}}{\Omega_{AP}} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{-m_{AP}} \Gamma \left( m_{AP}, \frac{m_{AP} Q}{\Omega_{AP} P_I} \right) - \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AP}} \frac{1}{\Gamma \left( m_{AP} \right)} \int x^{m_{AP} - 1} \exp \left( -\frac{m_{AP} x}{\Omega_{AP}} \right) \right) \times Q_m \left( \frac{2 m_{AP} \rho_x}{1 - \rho_x^2 \Omega_{AP}} \right) \left( \frac{2 m_{AP} \rho_x^2}{1 - \rho_x^2 \Omega_{AP}} \right) dx, \tag{4}$$

where $P_I$ is the outage probability of PU, the upper incomplete gamma function is defined as $\Gamma (\cdot)$ and the generalized Marcum Q function is defined as $Q_m (\cdot, \cdot)$ [36]. The derived process for (4) is provided in Appendix A.

We assume that Eve is a passive eavesdropper, which has been adopted in the researches about secure wireless communication, e.g., [20], [21], [24] and references therein. The received signal symbol is expressed as

$$y_E = \tilde{h}_{AE}^T w \left( \sqrt{P_{s1} a_1 x_1} + \sqrt{P_{s2} a_2 x_2} \right) + g_E + n_E^1, \tag{5}$$

where $\tilde{h}_{AE} \in \mathbb{C}^{1 \times N_2}$ is the channel vector, $g_E$ is the interference from PT to Eve and $n_E^1$ is the AWGN at Eve and $w$ is designed for legal transmission links, which has no diversity gain for Eve.

In the second slot, assume user $N$ performs SIC and transmits $x_2$ to user $M$. The received signal at user $M$ is given by

$$y_M = \tilde{h}_{NM} \left( \sqrt{P_{s2} x_2} \right) + g_M + n_M, \tag{6}$$

where $\tilde{h}_{NM}$ is the channel which denotes the delayed current channel $h_{NM}$, $P_{s2}$ is the total transmit power, $g_M$ is the interference from PT to user $M$, and $n_M$ is the AWGN at user $M$. Similarly, due to the outdated CSI, interference power at PU must be kept below a tolerable interference threshold $Q$. The total power $P_{s2}$ needs to satisfy condition that $P_{s2} = \min \left\{ \kappa_2 \frac{Q}{|\tilde{h}_{AP}|^2}, P_I \right\}$, where $\kappa_2$ is the power margin factor at user $N$, which can be get as the previous solution.

As for Eve, the received signal symbol is expressed as

$$y_E^2 = h_{NE} \left( \sqrt{P_{s2} x_2} \right) + g_E + n_E^2, \tag{7}$$

where $h_{NE}$ is the channel coefficient for user $N$ to Eve link and $n_E^2$ is the AWGN at Eve.

According to the above channel model analysis, the receiver’s SNR can be easily obtained by the received signal. In the first slot, SIC is supposed to be carried out at user $N$. What’s more, Alice adopts the MRT scheme to transmit signals. Thus, the SNR for $x_1$ and $x_2$ can be given by

$$\tilde{\gamma}_{N,N}^1 = \frac{a_1 P_{s1} |\tilde{h}_{AN}|^2}{(1 + \eta) \sigma^2}, \tag{8}$$

and

$$\tilde{\gamma}_{N,M}^1 = \frac{a_2 P_{s1} |\tilde{h}_{AN}|^2}{a_1 P_{s1} |\tilde{h}_{AN}|^2 + (1 + \eta) \sigma^2}, \tag{9}$$

respectively.

For Eve, we assume that Eve is equipped with a single antenna like other sensors to camouflage itself and there is no cooperation between Alice and Eve in this network. Thus, the SNR of the wiretap channel between Alice and Eve for $x_1$ and $x_2$ can be given as

$$\tilde{\gamma}_{E,N}^1 = \frac{a_1 P_{s1} |\tilde{h}_{AE}|^2}{(1 + \eta) \sigma^2}, \tag{10}$$

and

$$\tilde{\gamma}_{E,M}^1 = \frac{a_2 P_{s1} |\tilde{h}_{AE}|^2}{a_1 P_{s1} |\tilde{h}_{AE}|^2 + (1 + \eta) \sigma^2}, \tag{11}$$

respectively.

In the second slot, after SIC, the weak signal $x_1$ no longer has the residual of strong signal $x_2$, and user $N$ recodes the demodulation information $x_2$ and sends it to user $M$. The SNR for decoding $x_2$ to user $M$ is given by

$$\tilde{\gamma}_{M,M}^2 = \frac{P_{s2} |\tilde{h}_{NM}|^2}{(1 + \eta) \sigma^2}, \tag{12}$$

Similarly for Eve, the SNR for $x_2$ is given by

$$\tilde{\gamma}_{E,M}^2 = \frac{P_{s2} |h_{NE}|^2}{(1 + \eta) \sigma^2}. \tag{13}$$

In this article, we assume that the signal is transmitted at a fixed coding rate. $R_1$ and $R_2$ are the encoding rates for $x_1$ and $x_2$, respectively. $R_{s1}$ and $R_{s2}$ are the secret rates for $x_1$ and $x_2$. 

VOLUME 8, 2020
respectively. In order to simplify the content and notational in the later calculations, we define \( \mu = \frac{\sigma^2}{\kappa}, \rho_{AN} = \rho_1, \rho_{NM} = \rho_2, \theta_1 = 2^R_{x_1} - 1, \theta_2 = 2^R_{x_2} - 1, \theta_3 = 2^R_{x_1 - x_1} - 1 \) and \( \theta_4 = 2^R_{x_2 - x_2} - 1 \).

### III. PERFORMANCE ANALYSIS

In this section, we investigate the performance of the dual-hop NOMA-enabled cognitive wiretap networks over Nakagami-\( m \) fading channels with outdated CSI and derive a set of closed-form expressions for key performance metrics, i.e., COP, IP and EST.

#### A. COP OF PROPOSED NETWORKS

1) COP for decoding \( x_1 \) to user \( N \): an outage occurs at user \( N \) in the cases that user \( N \) fails to decode either \( x_1 \) or \( x_2 \). Based on the analysis in Sections II, according to Shannon channel capacity formula [21], the COP for decoding \( x_1 \) to user \( N \) is given by

\[
P^N_{\text{cop}}(R_{11}, R_{12}) = 1 - P\left( \log\left(1 + \frac{1}{\gamma^1_{N,N}}\right) > R_{11}, \log\left(1 + \frac{\gamma^1_{N,M}}{\gamma^2_{N,M}}\right) > R_{12}\right).
\]

(14)

After some manipulations, the COP of user \( N \) over outdated CSI Nakagami-\( m \) channel is given by the following Lemma 1.

Lemma 1: By simplification of (14), the COP of user \( N \) under the condition of Nakagami-\( m \) channel is derived as (15), shown at the bottom of the page, where \( \Gamma (\cdot, \cdot) \) is the incomplete gamma function.

Obviously, when \( a_2 - a_1 \theta_2 < 0 \), \( P^N_{\text{cop}}(R_{11}, R_{12}) = 1 \). For avoiding \( P^N_{\text{cop}}(R_{11}, R_{12}) = 1, \theta_2 \) should satisfy \( a_2 - a_1 \theta_2 < 0 \). Moreover, it can be found that when the number of \( N_A \) increases, the COP will decrease, and there is an obvious antenna gain.

Proof: See Appendix B.

2) COP for decoding \( x_2 \) to user \( M \): an outage occurs at user \( M \) in two cases. The first case is that Alice fails to transmit \( x_2 \) to user \( N \). The second case is that user \( N \) fails to decode either \( x_2 \) even if Alice successfully decode both \( x_2 \). The SNR for \( x_2 \) is given by

\[
\gamma_M = \min\left(\gamma^1_{N,M}, \gamma^2_{N,M}\right).
\]

(16)

Based on Shannon channel capacity formula, the COP for decoding \( x_2 \) to user \( M \) is given by

\[
P^M_{\text{cop}}(R_{11}, R_{12}) = P\left( \log\left(1 + \frac{1}{\gamma^1_{E,M}}\right) < R_{11}\right) + P\left( \log\left(1 + \min\left(\frac{\gamma^1_{E,M}}{\gamma^2_{E,M}}\right)\right) < R_{12}\right).
\]

(17)

**Lemma 2:** The COP of user \( M \) under the condition of outdated Nakagami-\( m \) channels is derived as (18), shown at the bottom of the next page.

Proof: See Appendix C.

#### B. IP OF PROPOSED NETWORKS

Assume that the eavesdropper is the passive eavesdropping and the eavesdropper can decode confidential information from Alice by applying multiuser detection techniques. Based on the analysis in Sections II, according to Shannon channel capacity formula, the IP for decoding \( x_1 \) to user \( N \) is given by

\[
P^N_{\text{ip}}(R_{11}, R_{12}, R_{11}, R_{12}) = P\left( \log\left(1 + \frac{1}{\gamma^1_{E,M}}\right) > R_{11} - R_{12}\right).
\]

(19)

We ask for the conditional IP of user \( N \) and find the mean under non-conditional conditions. After some manipulations, the IP of user \( N \) over outdated CSI Nakagami-\( m \) channel is given by the following Lemma 3.

**Lemma 3:** With Nakagami-\( m \) fading, the IP for decoding \( x_1 \) to user \( N \) is derived as (20), shown at the bottom of the next page.

Proof: See Appendix D.

Assuming the eavesdropper cannot merge the common information of the two phases in the considered networks. As for \( x_2 \), we suppose Eve eavesdrops on two slots, and chooses the best one to receive. The SNR for decoding \( x_2 \) to user \( M \) is given by

\[
\gamma^1_{E,M} = \max\left\{\gamma^1_{E,M}, \gamma^2_{E,M}\right\}.
\]

(21)

According to Shannon channel capacity formula, the IP for decoding \( x_2 \) to user \( M \) is given by

\[
P^M_{\text{ip}}(R_{11}, R_{12}, R_{11}, R_{12}) = P\left( \log\left(1 + \min\left(\gamma^1_{E,M}, \gamma^2_{E,M}\right)\right) > R_{12} - R_{12}\right).
\]

(22)
Lemma 4: With Nakagami-$m$ fading, the IP for decoding $x_2$ to user $M$ is derived as (23), shown at the bottom of next page. Obviously, for avoiding $P^M_{ip}(R_{t1}, R_{t2}, R_{s1}, R_{s2}) = 1$, it should satisfy that $a_2 - a_1t_0 < 0$.

Proof: See Appendix E.

C. EST OF PROPOSED NOMA-ENABLED CRNs

COP and IP are the metrics for reliability and security performance, respectively, which are inadequate to evaluate the performance of both connection and security. It is necessary to comprehensively study the joint performance of the security and the reliability, EST is adopted to holistically characterize this in the system [21], [22], [44]. The EST of user $N$ and user $M$ are formulated as

$$T_N (R_{t1}, R_{t2}, R_{s1}, R_{s2}) = P \left( \gamma_{N,M}^1 > \theta_1, \gamma_{N,M}^1 > \theta_2, \gamma_{E,M}^2 < \theta_3 \right) R_{s1}, \quad (24)$$

and

$$T_M (R_{t1}, R_{t2}, R_{s1}, R_{s2}) = P \left( \gamma_{M}^1 > \theta_1, \gamma_{E,M}^2 < \theta_4 \right) R_{s2}, \quad (25)$$

respectively. And we can get closed-form expressions through calculations, which are derived as (26), shown at the bottom of the next page, and (27), shown at the bottom of 8th page.

Proof: See Appendix F.

The transmission power and transmission rate have opposite effects on the security performance and reliability. When imperfect channel conditions are not considered, EST first increases and then decreases as the transmission power increases. In the process, IP has been rising. In the area of EST decline, the security efficiency and reliability of the system are declining. Therefore, in this power range, it is harmful to increase the power. In the rising area of EST, increasing the transmission power at this time can improve the security transmission efficiency but reduce the reliability. It shows that there is a compromise between security performance and transmission efficiency. In the same way, similar conclusions can be drawn for the transmission rate analysis, and the transmission rate can achieve a compromise between security and efficiency. Although EST can measure security efficiency, higher EST may be obtained at the cost of high IP. Therefore, using EST can more comprehensively evaluate the security performance of the system.

IV. NUMERICAL RESULTS

In this section, we present simulation numerical analysis of the above derived results. By comparing the theoretical analysis with the results of the Monte Carlo simulation, we can

\[
\begin{align*}
\rho_{cop}^M (R_{t1}, R_{t2}) &= 1 - \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AN}N_{AN}-1} \sum_{i=0}^{m_{AN}N_{AN}-i} \left( \frac{m_{AN}(1 + \eta)\sigma^2\varphi_2}{P_i\Omega_{AN}(1 - \rho_1)} \right)^i \frac{1}{i!} \frac{m_{AN}(1 + \eta)\sigma^2\varphi_2}{P_i\Omega_{AN}(1 - \rho_1)} \\
&\quad \times \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{NM}N_{NM}-1} \sum_{j=0}^{m_{NM}N_{NM}-j} \left( \frac{m_{NM}(1 + \eta)\sigma^2\varphi_2}{P_j\Omega_{NM}(1 - \rho_2)} \right)^j \frac{1}{j!} \frac{m_{NM}(1 + \eta)\sigma^2\varphi_2}{P_j\Omega_{NM}(1 - \rho_2)} \\
&\quad \times \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AE}N_{AE}-1} \sum_{i=0}^{m_{AE}N_{AE}-i} \left( \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_i\Omega_{AE}} \right)^i \frac{1}{i!} \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_i\Omega_{AE}} \\
&\quad \times \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AE}N_{AE}-1} \sum_{j=0}^{m_{AE}N_{AE}-j} \left( \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_j\Omega_{AE}} \right)^j \frac{1}{j!} \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_j\Omega_{AE}} \\
&\quad \times \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AE}N_{AE}-1} \sum_{i=0}^{m_{AE}N_{AE}-i} \left( \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_i\Omega_{AE}} \right)^i \frac{1}{i!} \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_i\Omega_{AE}} \\
&\quad \times \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AE}N_{AE}-1} \sum_{j=0}^{m_{AE}N_{AE}-j} \left( \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_j\Omega_{AE}} \right)^j \frac{1}{j!} \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_j\Omega_{AE}} \end{align*}
\]

\[
\begin{align*}
P^N_{ip} (R_{t1}, R_{t2}, R_{s1}, R_{s2}) &= \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AE}N_{AE}-1} \sum_{i=0}^{m_{AE}N_{AE}-i} \left( \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_i\Omega_{AE}} \right)^i \frac{1}{i!} \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_i\Omega_{AE}} \\
&\quad \times \frac{1}{\Gamma (m_{AP})} \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AE}N_{AE}-1} \sum_{j=0}^{m_{AE}N_{AE}-j} \left( \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_j\Omega_{AE}} \right)^j \frac{1}{j!} \frac{m_{AE}(1 + \eta)\sigma^2\varphi_3}{P_j\Omega_{AE}} \end{align*}
\]
Moreover, numerical results of the proposed NOMA scheme are presented and compared with those of the OMA scheme in the same networks. Unless otherwise stated, we set the parameters by [21, 24] as follows $P_{s1} = P_{s2}, \kappa_1 = \kappa_2, \ m_{AP} = m_{AR} = m_{AE} = m_{RE} = m_{RP} = m = \eta = 2, \sigma^2 = 1, R_{s1} = R_{s2} = 1.0, R_{s1} = R_{s2} = 0.7, a_1 = 0.2, a_2 = 0.8$ and $\alpha = 3$.

Fig. 2 presents the effects of the power margin factor $\kappa_1$ versus $P_i/\sigma^2$ under various fading severity parameters $m$ and correlation coefficients $p_{AP}$. It shows that the power margin factor $\kappa_1$ declines with the increase of $P_i/\sigma^2$. It can also be observed that in the low SNR regime, the power margin factor

$$P_{ip}^M (R_{s1}, R_{s2}, R_{s3}, R_{s4})$$

$$= 1 - \left(1 - \frac{1}{\Gamma (m_{AP})} \frac{m_{AP} \Omega_{AP}}{\mu} \sum_{i=0}^{m_{AP}-1} \frac{m_{AE}(1 + \eta)\sigma^2 \phi_4}{P_i \Omega_{AE}} \right) \frac{i}{i!} \frac{m_{AE}(1 + \eta)\sigma^2 \phi_4}{P_i \Omega_{AE}}$$

$$\times \Gamma \left(\frac{m_{AP} + i}{\kappa_1 P_i \Omega_{AE} \mu} + \frac{m_{AP}}{\Omega_{AP}} \right)$$

$$\times \left(1 - \frac{1}{\Gamma (m_{AP})} \frac{m_{AP} \Omega_{AP}}{\mu} \sum_{i=0}^{m_{AP}-1} \frac{m_{NE}(1 + \eta)\sigma^2 \phi_4}{P_i \Omega_{NE}} \right) \frac{i}{i!} \frac{m_{NE}(1 + \eta)\sigma^2 \phi_4}{P_i \Omega_{NE}}$$

$$\times \Gamma \left(\frac{m_{NE}(1 + \eta)\sigma^2 \phi_4}{\kappa_2 P_i \Omega_{NE} \mu} + \frac{m_{AP}}{\Omega_{AP}} \right)$$

$$T_N = R_{s1} \times \frac{1}{\Gamma (m_{AP})} \frac{m_{AP} \Omega_{AP}}{\mu} \left(\sum_{i=0}^{m_{AN} N_{AE}} \frac{m_{AN}(1 + \eta)\sigma^2 \max (\phi_1, \phi_2)}{P_i \Omega_{AN} (1 - \rho_1)} \right) \frac{i}{i!} \frac{m_{AN}(1 + \eta)\sigma^2 \max (\phi_1, \phi_2)}{P_i \Omega_{AN} (1 - \rho_1)}$$

$$+ \frac{m_{AP}}{\Omega_{AP}} \frac{1}{\Gamma (m_{AP})} \sum_{i=0}^{m_{AN} N_{AE} - 1} \frac{m_{AN}(1 + \eta)\sigma^2 \max (\phi_1, \phi_2)}{\kappa_1 P_i \Omega_{AN} \mu (1 - \rho_1)} \frac{i}{i!} \frac{m_{AN}(1 + \eta)\sigma^2 \max (\phi_1, \phi_2)}{\kappa_1 P_i \Omega_{AN} \mu (1 - \rho_1)} + \frac{m_{AP}}{\Omega_{AP}}$$

$$\times \Gamma \left(\frac{m_{AP} + i}{\kappa_1 P_i \Omega_{AN} \mu (1 - \rho_1)} + \frac{m_{AP}}{\Omega_{AP}} \right)$$

$$- \frac{1}{\Gamma (m_{AP})} \frac{m_{AP} \Omega_{AP}}{\mu} \sum_{j=0}^{m_{AE} N_{AE}} \frac{m_{AE}(1 + \eta)\sigma^2 \phi_3}{P_i \Omega_{AE} (1 - \rho_1)} \frac{i}{i!} \frac{m_{AE}(1 + \eta)\sigma^2 \phi_3}{P_i \Omega_{AE} (1 - \rho_1)}$$

$$\times \left(1 + \frac{m_{AP}}{\Omega_{AP}} \sum_{i=0}^{m_{AN} N_{AE} - 1} \frac{m_{AN}(1 + \eta)\sigma^2 \max (\phi_1, \phi_2)}{\kappa_1 P_i \Omega_{AN} \mu (1 - \rho_1)} \right) \frac{i}{i!} \sum_{j=0}^{m_{AE} N_{AE}} \frac{m_{AE}(1 + \eta)\sigma^2 \phi_3}{\kappa_1 P_i \Omega_{AE} \mu (1 - \rho_1)} \frac{i}{i!} \frac{m_{AE}(1 + \eta)\sigma^2 \phi_3}{\kappa_1 P_i \Omega_{AE} \mu (1 - \rho_1)}$$

$$\times \Gamma \left(i + j + m_{AP}, \frac{m_{AN}(1 + \eta)\sigma^2 \max (\phi_1, \phi_2)}{\kappa_1 P_i \Omega_{AN} \mu (1 - \rho_1)} + \frac{m_{AE}(1 + \eta)\sigma^2 \phi_3}{\kappa_1 P_i \Omega_{AE} \mu (1 - \rho_1)} \right)$$

(26)


\( T_M = R_{s2} \)

\[
\begin{align*}
\frac{1}{\Gamma(m_{AP})} \left( m_{AP} e^{\frac{m_{AP}}{\Omega_{AP}} \mu} \right)^{m_{AN} N_A -1} \sum_{i_1=0}^{m_{AN} (1+\eta) \sigma^2 \phi_2} \left( \frac{m_{AN} (1+\eta) \sigma^2 \phi_2}{P_i \Omega_{AN}} \right)^{i_1} \frac{1}{i_1!} e^{-\frac{m_{AN}(1+\eta)\sigma^2 \phi_2}{P_i \Omega_{AN} (1-\rho_1)}} \\
\times \left( 1 - \sum_{i_2=0}^{m_{AE} -1} \left( \frac{m_{AE} (1+\eta) \sigma^2 \phi_4}{P_i \Omega_{AE}} \right)^{i_2} \frac{1}{i_2!} e^{-\frac{m_{AE}(1+\eta)\sigma^2 \phi_4}{P_i \Omega_{AE}}} \right) \times \frac{1}{\Gamma(m_{AP})} \left( m_{AP} + i_1, \left( \frac{m_{AN} (1+\eta) \sigma^2 \phi_2}{\kappa_{11} P_i \Omega_{AN} \mu (1-\rho_1)} + \frac{m_{AP}}{\Omega_{AP}} \right) \mu \right) \\
+ \frac{1}{\Gamma(m_{AP})} \left( m_{AP} \right)^{m_{AN} N_A -1} \sum_{i_1=0}^{m_{AN} (1+\eta) \sigma^2 \phi_2} \left( \frac{m_{AN} (1+\eta) \sigma^2 \phi_2}{\kappa_{11} P_i \Omega_{AN} \mu (1-\rho_1)} \right)^{i_1} \frac{1}{i_1!} \sum_{j_2=0}^{m_{AE} -1} \left( \frac{m_{AE} (1+\eta) \sigma^2 \phi_4}{\kappa_{11} P_i \Omega_{AE} \mu} \right)^{j_2} \frac{1}{j_2!} \\
\times \Gamma(i_1 + j_2 + m_{AP}, \left( \frac{m_{AN} (1+\eta) \sigma^2 \phi_2}{\kappa_{11} P_i \Omega_{AN} \mu (1-\rho_1)} + \frac{m_{AE} (1+\eta) \sigma^2 \phi_4}{\kappa_{11} P_i \Omega_{AE} \mu} + \frac{m_{AP}}{\Omega_{AP}} \right) \mu) \\
\times \frac{1}{\Gamma(m_{NP})} \left( m_{NP} e^{\frac{m_{NP}}{\Omega_{NP}} \mu} \right)^{m_{NM} -1} \sum_{j_1=0}^{m_{NM} (1+\eta) \sigma^2 \phi_2} \left( \frac{m_{NM} (1+\eta) \sigma^2 \phi_2}{P_i \Omega_{NM}} \right)^{j_1} \frac{1}{j_1!} e^{-\frac{m_{NM}(1+\eta)\sigma^2 \phi_2}{P_i \Omega_{NM} (1-\rho_2)}} \\
\times \left( 1 - \sum_{j_2=0}^{m_{NE} -1} \left( \frac{m_{NE} (1+\eta) \sigma^2 \phi_4}{P_i \Omega_{NE}} \right)^{j_2} \frac{1}{j_2!} e^{-\frac{m_{NE}(1+\eta)\sigma^2 \phi_4}{P_i \Omega_{NE}}} \right) \times \frac{1}{\Gamma(m_{NP})} \left( m_{NP} + j_1, \left( \frac{m_{NM} (1+\eta) \sigma^2 \phi_2}{\kappa_{22} P_i \Omega_{NM} \mu (1-\rho_2)} + \frac{m_{NP}}{\Omega_{NP}} \right) \mu \right) \\
+ \frac{1}{\Gamma(m_{NP})} \left( m_{NP} \right)^{m_{NM} -1} \sum_{j_1=0}^{m_{NM} (1+\eta) \sigma^2 \phi_2} \left( \frac{m_{NM} (1+\eta) \sigma^2 \phi_2}{\kappa_{22} P_i \Omega_{NM} \mu (1-\rho_2)} \right)^{j_1} \frac{1}{j_1!} \sum_{j_2=0}^{m_{NE} -1} \left( \frac{m_{NE} (1+\eta) \sigma^2 \phi_4}{\kappa_{22} P_i \Omega_{NE} \mu} \right)^{j_2} \frac{1}{j_2!} \\
\times \Gamma(j_1 + j_2 + m_{NP}, \left( \frac{m_{NM} (1+\eta) \sigma^2 \phi_2}{\kappa_{22} P_i \Omega_{NM} \mu (1-\rho_2)} + \frac{m_{NE} (1+\eta) \sigma^2 \phi_4}{\kappa_{22} P_i \Omega_{NE} \mu} + \frac{m_{NP}}{\Omega_{NP}} \right) \mu) \\
\end{align*}
\]

\( k_1 = 1 \) because of the interference to the PU is less than the preset value. Furthermore, we plot asymptotic cases with infinite secondary transmit power, which using an approximate equivalent \( P_i \rightarrow \infty \) to mimic quantization effects. Besides, this figure indicates that a tighter new interference power constraint (i.e. a smaller \( P_{t1} \)) and a better channel quality of the interference link (i.e. a larger \( m \)) will lead to a better QoS for PU.

Fig. 3 and 4 present the effects of the COP versus \( P_i/\sigma^2 \) with outdated CSI of the interference and secondary transmission links, respectively. From both figures, the Monte Carlo simulation results are in good agreement with analytical results. It can be easily seen that when \( P_i/\sigma^2 \) is low, the COP keeps decreasing while \( P_i/\sigma^2 \) increasing. When \( P_i/\sigma^2 \) is high, the COP appears to be leveled, which means that the \( P_i/\sigma^2 \) is limited by interference threshold \( Q \). In the Fig. 3, it considers the outdated CSI of PU and the CSI of the secondary transmission links is known. Due to the existence of the power margin factor \( k_1 \) and \( k_2 \), the transmission power is limited when the performance appears flat and \( k_1, k_2 \) are still further reducing. Furthermore, we plot asymptotic cases with no interference temperature constraint (\( Q \rightarrow \infty \)). It demonstrates that the COP can be guaranteed when interference constraint \( Q \) is high. Moreover, due to the constraint for the power, the performance decreases when the CSI with the PU is outdated. In the Fig. 4, it considers the outdated CSI of the secondary transmission links and the CSI of Alice to PU is known. We can clearly see that the more CSI of the secondary transmission links were known, the better COP, which is the same as the expected result. Therefore, it show that imperfect
CSI degrades the COP of the signal and the larger the value of $m$, the lower COP.

Fig. 5 presents the effects of the IP of user $N$ and user $M$ versus $P_t/\sigma^2$ with the outdated CSI of the interference links. As can be seen from the figure, the information that Alice leaks to Eve under the fixed rate coding condition is more and more easily while $P_t/\sigma^2$ increasing, which resulting in the outage. In contrast with reliability performance shown in Fig. 3 and Fig. 4, the secrecy performance is weakened because of the increasing of transmit power. In the low transmit power region, the IP keeps ascending due to the secrecy performance being determined by the transmit power. However, in the high transmit power region, the IP keeps constant due to the interference temperature constraint. It demonstrates that IP will approach a value with the highest probability of interruption due to the limitation of transmit power. Regarding the outdated CSI, transmit power will be further limited due to the constraint for the power. What’s more, it demonstrates that secrecy performance of $m = 2$ is better than that of $m = 1$ when SNR in low region.

Fig. 6 plots the EST of user $N$ and user $M$ versus $P_t/\sigma^2$ with the outdated CSI of the interference and secondary transmission links, respectively. We can get the $P_t/\sigma^2$ curve has the tendency of ascending first and then descending, which reveals that there is an optimum $P_t/\sigma^2$ that yields the maximum $P_t/\sigma^2$. Regarding the outdated CSI of the secondary transmission links, EST is lower because of its poor connection performance when the parameter of outdated CSI is set as $\rho_{AN} = \rho_{NM} = 0.9$. Besides, due to the outdated CSI of the interference links, in the high transmit power region,
EST will increase as the constraint for the power reduces the probability of information leakage when the parameter of outdated CSI is set as $\rho_{AP} = \rho_{NP} = 0.9$. It indicates that the impact of the security interruption is greater than the connection interruption at this point.

Fig. 7 plots the EST of user $N$ and user $M$ versus $P_i/\sigma^2$ with the outdated CSI of the interference links, respectively. In the proposed system model, the NOMA-enabled requires two slots to deliver the intended messages to user $N$ and user $M$, whereas the OMA needs three slots to serve both users. Hence, the data requirements for OMA is set as 1.5 times of that for NOMA for a fair comparison of two multiple access techniques. Also, by comparing the maximum EST of NOMA and OMA systems, the NOMA-enabled networks can achieve the same EST of OMA networks with low power, and the peak value of EST is even greater. It demonstrates that the considered networks in NOMA can achieve better EST than that of the same networks with OMA scheme because of NOMA requiring less time slot than that with OMA scheme.

V. CONCLUSION

In this article, we investigated secrecy performance for the downlink wiretap system in underlay CRNs. To improve spectrum utilization and connection reliability, we proposed the NOMA-enabled CRNs, in which the secondary transmitter transmits information to two users in the presence of an eavesdropper. The closed-form expressions for COP, IP and EST are derived to investigate the impact of parameters on secrecy performance. Simulation results are presented to validate the analysis and provide insights into the impact of parameters. In addition, we studied the effect of the power margin factor and the channel parameter $m$ with the outdated CSI on the connection and secrecy performance. In the end, it demonstrates that secondary users with NOMA scheme can achieve a higher EST than that with OMA scheme.

APPENDIX A

The actual interference power at PU from Alice is given as

$$I_1 = \min \left\{ \frac{Q}{|h_{AP}|^2}, P_i \right\} |h_{AP}|^2. \quad (28)$$

To simplify the expression, we assume that the variables $|\hat{h}_{AP}|^2 = \tilde{g}_1$ and $|h_{AP}|^2 = g_1$. The CDF of $I_1$ is given by

$$F_{I_1}(z) = \Pr \left( \min \left\{ \frac{Q}{g_1}, P_i \right\} g < z \right). \quad (29)$$

To characterize the interference at PU, we define the interference probability of PU as the probability that the actual interference at PU is higher than the interference power constraint $Q$. Thus, the interference probability $P_{I_1}$ is expressed as

$$P_{I_1} = 1 - F_{I_1}(Q) = 1 - \Pr \left( \min \left\{ \frac{Q}{g_1}, P_i \right\} g < Q \right) = \int_0^\infty \int_0^\infty f_{g,\tilde{g}}(x, y) dy dx. \quad (30)$$

With the help of [45, Eq.(7)] and [46, Eq.(1)], (4) can be obtained.

APPENDIX B

After some manipulations, the expression for COP of user $n$ can be written as

$$P^n_{\text{cop}}(R_1, R_2) = 1 - P \left( \tilde{\gamma}^1_{N,N} > \theta_1, \tilde{\gamma}^1_{N,M} > \theta_2 \right) = 1 - P \left( a_1 P_{i_1} \left\| \tilde{h}_{AN} \right\|^2 > \theta_1, (a_2 - \theta a_1) P_{i_2} \left\| \tilde{h}_{AN} \right\|^2 > \theta_2 \right). \quad (31)$$

Then we set $\phi_1 = \frac{\theta_1}{a_1}$, $\phi_2 = \left\{ \begin{array}{ll} \frac{\theta_2}{a_2 - a_1 \theta_1} & \text{if } a_2 - a_1 \theta_1 > 0 \\ \infty & \text{else} \end{array} \right.$ and $\tilde{\gamma}_{AN} = \frac{P_{i_1} \left\| \tilde{h}_{AN} \right\|^2}{(1 + \eta)\sigma^2}.$

In order to derive the closed-form expressions of (31), we first give the following the cumulative distribution function (CDF) of $\tilde{\gamma}_{AN}$. With the help of [47, Eq.(11)], the outdated CSI channel gain is given by

$$F_{\tilde{\gamma}_{AN}}(x) = 1 - \sum_{i=0}^{m_{AN} N_{A_i} - 1} \left( \frac{m_{AN}(1 + \eta)\sigma^2 x}{P_{i_1} \Omega_{AN} (1 - \rho_1)} \right)^i \frac{e^{-m_{AN}(1 + \eta)\sigma^2 x}}{i!} P_{i_1} \Omega_{AN} (1 - \rho_1). \quad (32)$$

Substituting (32) into (31), we can obtain the conditional COP of user $n$ as

$$P^n_{\text{cop}}(R_1, R_2 | G_1) = 1 - \sum_{i=0}^{m_{AN} N_{A_i} - 1} \left( \frac{m_{AN}(1 + \eta)\sigma^2 \max(\phi_1, \phi_2)}{P_{i_1} \Omega_{AN} (1 - \rho_1)} \right)^i \times 1 \frac{e^{-m_{AN}(1 + \eta)\sigma^2 \max(\phi_1, \phi_2)}}{P_{i_1} \Omega_{AN} (1 - \rho_1)}. \quad (33)$$
Furthermore, the unconditional COP for user $n$ can be given by

$$P_{\text{cop}}^N (R_1, R_2) = \int_0^\infty f_{G_1} (g_1) P_{\text{cop}}^N (R_1, R_2 | G_1) \, dg_1. \quad (34)$$

With Nakagami-$m$ fading, the probability distribution function (PDF) of $g_1$ can be given by

$$f_{G_1} (g_1) = \left( \frac{m_{AP}}{\Omega_{AP}} \right)^{m_{AP}} \frac{g_1^{m_{AP} - 1} e^{-\frac{g_1}{m_{AP}}}}{\Gamma (m_{AP})}. \quad (35)$$

Finally, exploiting (35) into (34), (15) can be gain.

### APPENDIX C

After some manipulations, the expression for COP of user $m$ can be written as

$$P_{\text{cop}}^M (R_1, R_2) = P \left( \min \left( \gamma_{NM}^2, \gamma_{NM}^2 \right) < \theta_2 \right) = 1 - \left( 1 - F_{\gamma_{NM}^2} (\theta_2) \right) \left( 1 - F_{\gamma_{NM}^2} (\theta_2) \right), \quad (36)$$

where

$$F_{\gamma_{NM}^2} (\theta_2) = P \left( \frac{P_s \| h_{AN} \|^2}{(1 + \eta)^2} < \phi_2 \right) \quad \text{and} \quad F_{\gamma_{NM}^2} (\theta_2) = P \left( \frac{P_s \| h_{NM} \|^2}{(1 + \eta)^2} < \theta_2 \right).$$

Similarly, we set $\gamma_{NM} = P_s \| h_{NM} \|^2 / (1 + \eta)^2$.

In order to derive the closed-form expressions of (38), we present the CDF of $h_{AN}$ and $h_{NM}$. Similarly, the CDF of $\gamma_{NM}$ is given by

$$F_{\gamma_{NM}^2} (x) = 1 - \sum_{i=0}^{m_{NM} - 1} \left( \frac{m_{NM} (1 + \eta) \sigma^2 x}{P_s \Omega_{NM} (1 - \rho_2)} \right)^i \left[ \frac{1}{i!} e^{-\frac{m_{NM} (1 + \eta) \sigma^2 x}{P_s \Omega_{NM} (1 - \rho_2)}} \right]. \quad (37)$$

Similarly, substituting (37) into (36), we can obtain the conditional COP of user $m$ as

$$P_{\text{cop}}^M (R_1, R_2 | G_1, G_2) = 1 - \sum_{i=0}^{m_{NM} - 1} \left( \frac{m_{NM} (1 + \eta) \sigma^2 \phi_2}{P_s \Omega_{AN} (1 - \rho_1)} \right)^i \left[ \frac{1}{i!} e^{-\frac{m_{NM} (1 + \eta) \sigma^2 (\phi_2 + \rho_1)}{P_s \Omega_{AN} (1 - \rho_1)}} \right] \times \sum_{i=0}^{m_{NM} - 1} \left( \frac{m_{NM} (1 + \eta) \sigma^2 \phi_2}{P_s \Omega_{NM} (1 - \rho_2)} \right)^i \left[ \frac{1}{i!} e^{-\frac{m_{NM} (1 + \eta) \sigma^2 (\phi_2 + \rho_1)}{P_s \Omega_{NM} (1 - \rho_2)}} \right]. \quad (38)$$

Furthermore, the unconditional COP for user $m$ can be given by

$$P_{\text{cop}}^M (R_1, R_2) = \int_0^\infty \int_0^\infty f_{G_1} (g_1) f_{G_2} (g_2) P_{\text{cop}}^M (R_1, R_2 | G_1, G_2) \, dg_1 \, dg_2. \quad (39)$$

With Nakagami-$m$ fading, the PDF of $g_2$ can be given by

$$f_{G_2} (g_2) = \left( \frac{m_{NP}}{\Omega_{NP}} \right)^{m_{NP}} \frac{g_2^{m_{NP} - 1} e^{-\frac{g_2}{m_{NP}}}}{\Gamma (m_{NP})}. \quad (40)$$

Finally, exploiting (35) and (40) into (39), (18) can be gain.

### APPENDIX D

After some manipulations, the expression for IP of user $n$ can be written as

$$P_{\text{ip}}^N (R_1, R_2, R_4, R_5) = P \left( \log \left( 1 + \frac{1}{\gamma_{E,N}^2} \right) > R_1 - R_4 \right) = P \left( \frac{P_s \| h_{AE} \|^2}{(1 + \eta) \sigma^2} > \phi_3 \right), \quad (41)$$

where $\phi_3 = \frac{\phi_2}{\rho_1}$. Then we set $\gamma_{AE} = \frac{P_s \| h_{AE} \|^2}{(1 + \eta) \sigma^2}$. With the help of [48, Eq.(18)], the CDF of $\gamma_{AE}$ is given by

$$F_{\gamma_{AE}} (x) = 1 - \sum_{i=0}^{m_{AE} - 1} \left( \frac{m_{AE} (1 + \eta) \sigma^2 \phi_3}{P_s \Omega_{AE}} \right)^i \left[ \frac{1}{i!} e^{-\frac{m_{AE} (1 + \eta) \sigma^2 \phi_3}{P_s \Omega_{AE}}} \right]. \quad (42)$$

By substituting (42) into (41), the conditional IP for decoding $x_1$ to user $n$ is derived as

$$P_{\text{ip}}^N (R_1, R_2, R_4, R_5 | G_1) = \int_0^\infty \int_0^\infty f_{G_1} (g_1) f_{G_2} (g_2) P_{\text{ip}}^M (R_1, R_2 | G_1, G_2) \, dg_1 \, dg_2. \quad (44)$$

To this end, substituting the PDF of $G_1$ into (44), (20) can be gain.

### APPENDIX E

After some manipulations, the expression for IP of user $m$ can be written as

$$P_{\text{ip}}^M (R_1, R_2, R_4, R_5) = P \left( \max \left\{ \gamma_{E,M}^2, \gamma_{E,M}^2 \right\} > \theta_4 \right) = 1 - F_{\gamma_{E,M}^2} (\theta_4) F_{\gamma_{E,M}^2} (\theta_4), \quad (45)$$

where $F_{\gamma_{E,M}^2} (\theta_4) = P \left( \frac{P_s \| h_{AE} \|^2}{(1 + \eta) \sigma^2} < \phi_4 \right)$, $F_{\gamma_{E,M}^2} (\theta_4) = P \left( \frac{P_s \| h_{AE} \|^2}{(1 + \eta) \sigma^2} < \theta_4 \right)$ and $\phi_4 = \frac{\phi_2}{\rho_1}, \rho_2 - \alpha_1, \rho_2 - \alpha_1 \theta_4 > 0$. The CDF of $\gamma_{NE}$ is given by

$$F_{\gamma_{NE}} = \frac{P_s \| h_{NE} \|^2}{(1 + \eta) \sigma^2}. \quad (46)$$

Now, the unconditional IP for decoding $x_2$ to user $n$ can be given by

$$P_{\text{ip}}^N (R_1, R_2, R_4, R_5 | G_1, G_2) = \int_0^\infty \int_0^\infty f_{G_1} (g_1) f_{G_2} (g_2) P_{\text{ip}}^M (R_1, R_2 | G_1, G_2) \, dg_1 \, dg_2. \quad (47)$$

To this end, substituting the PDF of $G_1$ into (44), (20) can be gain.
\[
T_N(R_1, R_2, R_3, R_4 | G_1) = \left( 1 - P^N_{\text{cop}}(R_1, R_2 | G_1) \right) \left( 1 - P^M_{\text{IP}}(R_1, R_2, R_3, R_4 | G_1) \right)
\times R_{s_1}
\]

and

\[
T_M(R_1, R_2, R_3, R_4 | G_1, G_2) = \left( 1 - P^M_{\text{cop}}(R_1, R_2 | G_1, G_2) \right) \times R_{s_2}
\]

respectively. To this end, substituting the PDF of \( G_1 \) and \( G_2 \) into (49) and (50) to find the mean under non-conditional conditions, (26) and (27) can be gain respectively.

**REFERENCES**

[1] A. A. Khan, M. H. Rehmani, and A. Rachidi, “When cognitive radio meets the Internet of Things?” in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Paphos, Cyprus, Sep. 2016, pp. 469–474.

[2] A. A. Khan, M. H. Rehmani, and A. Rachidi, “Cognitive-radio-based Internet of Things: Applications, architectures, spectrum related functionali- ties, and future research directions,” *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 17–25, Jun. 2017.

[3] J. Adu Ansere, G. Han, H. Wang, C. Choi, and C. Wu, “A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks,” *IEEE Internets Things J.*, vol. 6, no. 4, pp. 6748–6759, Aug. 2019.

[4] Q. Wu, W. Chen, D. W. K. Ng, and R. Schober, “Spectral and energy-efficient wireless powered IoT networks: NOMA or TDMA?” *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6663–6667, Jul. 2018.

[5] A. E. Mostafa, Y. Zhou, and V. W. S. Wong, “Connection density maximization of narrowband IoT systems with NOMA,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 10, pp. 4708–4722, Oct. 2019.

[6] L. Ly, J. Chen, Q. Ni, Z. Ding, and H. Xiang, “Cognitive non-orthogonal multiple access with cooperative relaying: A new wireless frontier for 5G spectrum sharing,” *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 188–195, Apr. 2018.

[7] S. Haykin, “Cognitive radio: Brain-empowered wireless communications,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[8] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srivastava, “Breaking spectrum gridlock with cognitive radios: An information theoretic perspective,” *Proc. IEEE*, vol. 97, no. 6, pp. 894–914, May 2009.

[9] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends,” *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[10] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, “Application of non-orthogonal multiple access in LTE and 5G networks,” *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[11] Y. Liu, Z. Ding, M. Elkashlan, and J. Yuan, “Nonorthogonal multiple access in large-scale underlay cognitive radio networks,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10152–10157, Dec. 2016.

[12] S. Arzykulov, T. A. Tsiftsis, G. Naurzybayev, and M. Abbaldah, “Outage performance of cooperative underlay CR-NOMA with imperfect CSI,” *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 176–179, Jan. 2019.

[13] S. Arzykulov, G. Naurzybayev, T. A. Tsiftsis, and M. Aram, “Performance analysis of underlay cognitive radio nonorthogonal multiple access networks,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9318–9322, Sep. 2019.

[14] G. Im and J. H. Lee, “Outage probability for cooperative NOMA systems with imperfect SIC in cognitive radio networks,” *IEEE Commun. Lett.*, vol. 23, no. 4, pp. 692–695, Apr. 2019.

[15] S. Arzykulov, G. Naurzybayev, M. S. Hashmi, A. M. Eltawil, K. M. Rabie, and S. Seirol, “Hardware- and interference-limited cognitive radio IOT relaying NOMA networks with imperfect SIC over generalized non-homogeneous fading channels,” *IEEE Access*, vol. 8, pp. 72942–72956, 2020.

[16] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[17] 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 schemes,” *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6282–6298, Sep. 2019.

[18] J. Chen, L. Yang, and M. Alouini, “Physical layer security for cooperative NOMA systems,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[19] H. Lei, J. Zhang, K.-H. Park, P. Xu, Z. Zhang, G. Pan, and M.-S. Alouini, “Secrecy outage of max–min TAS scheme in MIMO-NOMA systems,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Aug. 2018.

[20] M. Qin, S. Yang, H. Deng, and M. H. Lee, “Enhancing security of primary user in underlay cognitive radio networks with secondary user selection,” *IEEE Access*, vol. 6, pp. 53264–53268, May 2018.

[21] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, “Physical layer security in cognitive radio inspired NOMA network,” *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.
[22] Z. Xiang, W. Yang, Y. Cai, Z. Ding, and Y. Song, “Secure transmission design in HARQ assisted cognitive NOMA networks,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2528–2541, 2020.

[23] 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 J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918–931, Apr. 2018.

[24] Y. Song, W. Yang, Z. Xiang, B. Wang, and Y. Cai, “Secure transmission in mmWave NOMA networks with cognitive power allocation,” *IEEE Access*, vol. 7, pp. 76104–76119, Jun. 2019.

[25] I. Budhiraja, N. Kumar, S. Tyagi, S. Tanwar, and M. S. Obaidat, “URJA: Usage jammer as a resource allocation for secure transmission in a CR-NOMA-Based 5G femtocell system,” *IEEE Syst. J.*, early access, Jun. 16, 2020, doi: 10.1109/JSYST.2020.2999474.

[26] S. Bhattacharjee, “Friendly jamming assisted secure cooperative multicasting in cognitive radio-NOMA systems,” in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.

[27] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, “Residual transceiver hardware impairments on cooperative NOMA networks,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 680–695, Jan. 2020.

[28] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. Kim, “Wiretap channel with secure rate-limited feedback,” *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[29] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, “Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI,” *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 2959–2961, Aug. 2015.

[30] B. He, X. Zhou, and T. D. Abhayapala, “Wireless physical layer security with imperfect channel state information: A survey,” *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, 2013.

[31] Z. Li, S. Wang, P. Mu, and Y.-C. Wu, “Sum rate maximization of secure NOMA transmission with imperfect CSI,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[32] X. Li, W. Yang, M. Zhang, F. Zhou, and N. Al-Dhahir, “Robust secure beamforming for SWIPT-aided relay systems with full-duplex receiver and imperfect CSI,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1867–1878, Feb. 2020.

[33] C. Meng, G. Wang, and X. Dai, “Secure energy-efficient transmission for SWIPT intelligent connected vehicles with imperfect CSI,” *IEEE Access*, vol. 7, pp. 154649–154658, 2019.

[34] J. L. Vicario, A. Bel, J. A. Lopez-Salcedo, and G. Seco, “Opportunistic relay selection with outdated CSI: Outage probability and diversity analysis,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 2872–2876, Jun. 2009.

[35] Y. Huang, F. S. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. M. Alnuweiri, “Cognitive MIMO relaying networks with primary user’s interference and outdated channel state information,” *IEEE Trans. Commun.*, vol. 62, no. 12, pp. 4241–4254, Dec. 2014.

[36] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. San Diego, CA, USA: Academic, 2000.

[37] T. Zhang, Y. Huang, Y. Cai, C. Zhong, W. Yang, and G. K. Karagiannidis, “Secure multiantenna cognitive wiretap networks,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4059–4072, May 2017.

[38] W. Zeng, Y. R. Zheng, and C. Xiao, “Multiantenna secure cognitive radio networks with finite-alphabet inputs: A global optimization approach for precoder design,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3044–3057, Apr. 2016.

[39] H. Zhao, Y. Tao, G. Pan, Y. Chen, and N. Yang, “Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10236–10242, Dec. 2016.

[40] T. K. Y. Lo, “Maximum ratio transmission,” *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct. 1999.

[41] S. Timotheou, I. Krikidis, G. Zheng, and B. Ottersten, “Beamforming for MISO interference channels with QoS and RF energy transfer,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2646–2658, May 2014.

[42] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, “Secure transmission in cooperative relaying networks with multiple antennas,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.

[43] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, “Secure transmissions in a metered wave systems,” *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[44] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, “Optimization of code rates in SISO/MIMO wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.

[45] J. Xing, X. Zhang, J. Wang, Z. Zhang, and W. Wang, “Performance analysis of cognitive relay networks with imperfect channel knowledge over Nakagami-m fading channels,” in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 839–844.

[46] A. Nuttall, “Some integrals involving the Q-function (corresp.),” *IEEE Trans. Inf. Theory*, vol. IT-21, no. 1, pp. 95–96, Jan. 1975.

[47] J. Men, J. Ge, and C. Zhang, “Performance analysis for downlink relaying aided non-orthogonal multiple access networks with imperfect CSI over Nakagami-m fading,” *IEEE Access*, vol. 5, pp. 998–1004, Nov. 2017.

[48] D. Song, J. Wang, Y. Cai, Z. Ding, Y. Song, and Y. Zou, “NOMA-assisted secure short-packet communications in IoT,” *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 8–15, Aug. 2020.