IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 September 2023, accepted 4 October 2023, date of publication 26 October 2023, date of current version 1 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3327789

RESEARCH ARTICLE

Security-Reliability Analysis in CR-NOMA IoT Network Under I/Q Imbalance

HUNG NGUYEN[1], TAN N. NGUYEN[2], (Member, IEEE), BUI VU MINH[3], THU-HA THI PHAM[4], ANH-TU LE[5], (Member, IEEE), AND MIROSLAV VOZNAK[5], (Senior Member, IEEE)

[1]HUTECH Institute of Engineering, HUTECH University, Ho Chi Minh City 70000, Vietnam
[2]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam
[3]Faculty of Engineering and Technology, Nguyen Tat Thanh University, Ho Chi Minh City 754000, Vietnam
[4]Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam
[5]Faculty of Electrical Engineering and Computer Science, VSB—Technical University of Ostrava, 70800 Ostrava, Czech Republic

Corresponding author: Tan N. Nguyen (nguyennhattan@tdtu.edu.vn)

The research leading to the published results was supported by the European Union within the REFRESH project - Research Excellence For Region Sustainability and High-tech Industries ID No. CZ.10.03.01/00/22_003/0000048 of the European Just Transition Fund and by the Ministry of Education, Youth and Sports of the Czech Republic (MEYS CZ) through the project SGS ID No. SP 7/2023 conducted by VSB - Technical University of Ostrava.

ABSTRACT This paper presents a controllable analysis framework for evaluating the reliability and security of underlay cognitive radio networks (CRs) relying on non-orthogonal multiple access (NOMA). In such systems, a secondary base station (BS) transmits confidential information to multiple secondary users uniformly distributed in the presence of a nearby located external eavesdropper. Moreover, transmit power constraints are introduced to limit the interference to the primary imposed by cognitive base stations. As an effective approach of multiple input single output (MISO) systems, the transmit antenna selection (TAS) is selected in the BS to improve the secrecy performance of the primary networks. Furthermore, we first consider the impact of quadrature-phase imbalance (IQI) to characterize the secure performance of the considered network in practice. Then, the degraded performance is evaluated in terms of outage probability (OP), intercept probability (IP), and effective secrecy throughput (EST) of two NOMA users. The optimal EST can be achieved through simulations while the results of OP and IP provide guidelines in the design of IQI-aware CR-NOMA systems. Finally, the trade-off between OP and IP with transmit signal-to-noise ratio (SNR) at the BS is investigated for reflecting the security characteristic. Finally, the trade-off between OP and IP with transmit signal-to-noise ratio (SNR) at the BS is studied for displaying the security characteristic. Numerical results show that increasing the number of transmit antennas at the BS and other main parameters improves performance. Moreover, when the system parameters are reasonably set, the secondary NOMA user in CR-NOMA can be reached secure requirements regardless of the controlled IQI.

INDEX TERMS Non-orthogonal multiple access, cognitive radio, physical layer security, quadrature-phase imbalance.

I. INTRODUCTION

To tackle critical problems in fifth-generation (5G) wireless networks, security using encryption keys and complex encoding/decoding algorithms need to be addressed. Such cryptographic techniques are implemented on upper layers. However, significant challenges to tackle security in such networks arise when deploying traditional cryptographic paradigms in several future wireless networks. Different traditional methods, physical layer security (PLS) without complicated encoding/decoding algorithms or keys has been introduced as an alternative to solve security and provide secure data transmission [1], [2], [3], [4]. Recently, non-orthogonal multiple access (NOMA) is researched for future mobile communication networks to overcome the challenging requirements including high data speed, low

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

latency, massive connectivity, and spectral efficiency [5], [6], [7], [8]. There are increasing research interests in the scenario of NOMA enabling PLS (e.g., [9], [10], [11], [12], [13], [14]). For example, research work in [9] and [10] investigated the PLS mechanism in NOMA networks with perfect knowledge of eavesdroppers' channel state information (CSI). In [9], an anonymous user was treated as a potential eavesdropper, and an efficient secrecy rate maximization technique for downlink NOMA in a multiple-input multiple-output (MIMO) cellular network was presented. In another study, the PLS of a relay selection-based cooperative NOMA system was proposed with a fixed power allocation scheme for providing the secrecy performance of all the users subject to a predefined quality of service (QoS) requirement [10]. In addition, the results in [9] and [10] indicated that NOMA exhibits a significant secrecy performance improvement compared to traditional orthogonal multiple access (OMA). Moreover, a practical scenario without the instantaneous knowledge of the eavesdropper's CSI at the transmitter was studied in [11], [12], [13], and [14]. In particular, to improve the secrecy performance the authors in [11] investigated some transmit antenna selection (TAS) schemes to benefit NOMA systems. The authors in [11] derived the exact closed-form formula of secrecy outage probability (SOP) and asymptotic SOP was further provided. Another work in [12] presented the scenario of randomly deployed users and eavesdroppers in large-scale networks with the exact and asymptotic expressions for the SOP. In other NOMA systems, a scheme was proposed to maximize the minimum confidential information rate under constraints of the SOP and transmit power [13]. Furthermore, to protect the confidential information of legitimate users, the authors in [14] studied an artificial noise (AN)-based beamforming scheme and examined a worse case of imperfect successive interference cancellation (SIC) which is applied to MISO-NOMA systems.

Furthermore, [15], [16], [17], and [18] indicated that the systems based on NOMA outperform traditional OMA in terms of the secrecy performance. In addition, the authors in [16] and [17] deployed power allocation policies and beamforming to alleviate the impacts of internal eavesdroppers. In [16], the authors presented a NOMA-assisted multicast-unicast system related to the threat from multicast receivers which intercept the unicasting information. The SOP was studied to show the performance of a cooperative NOMA vehicular communication (VC) system, in which the relay can be operated in either half-duplex (HD) or full-duplex (FD) modes [17]. The authors in [18] presented NOMA to enhance security by investigating the PLS of the information from the weak device against interception by the strong device.

Recently, to provide coverage extension an outage minimization, underlay cognitive radio (CR)-based NOMA networks using a decode-and-forward (DF) relaying scheme were examined [19], [20], [21], [22]. In particular, cooperative CR-NOMA was investigated to allow secondary users to cooperate with primary users and then this mechanism compensates the primary spectrum consumption [19]. Moreover, cooperative CR-NOMA were studied in [20] and [21] in terms of the outage probability (OP) and throughput to exhibit the achievable performance gain of the considered system and then is compared with the performance of non-cooperative CR-NOMA networks. Different models of spectrum-sharing NOMA networks including underlay NOMA, overlay NOMA and cognitive NOMA was proposed in [23], in which a novel secondary NOMA-relay-assisted spectrum sharing scheme satisfies first the QoS of the primary user employing maximal ratio combining (MRC) and then the performance of the secondary user was maximized in terms of the sum-rate. The system model is introduced in [24], the primary network shares the spectrum with the secondary network to form such kind of cooperation and such cooperative NOMA-based spectrum sharing system allows the secondary transmitter to transmit the primary user's information as well as its own information. In another work, a dual-hop underlay CR-NOMA network is explored to show the end-to-end OP as the main performance metric for secondary NOMA users [25]. A multiuser multiple-input single-output (MISO) NOMA network using CR was studied subject to an individual QoS constraint and energy efficiency optimization for each primary user [26]. The outage performance of the CR-NOMA system is studied for two users which are benefited by the decode-and-forward scheme [27]. There is no interference from the primary transmitter to the secondary receivers as the assumption reported in [27], and the transmission from the relay does not make any interference to the primary receiver. The authors in [28] considered the situation that the interference occurs from the relay to the primary network while the interference occurs from the primary network to the secondary network. They examined the outage performance of a similar system in case of imperfect CSI.

It can be guaranteed the QoS requirement of the quality of the service-sensitive user (QSU) in a cognitive power allocation scheme, while the hybrid automatic repeat request (HARQ) technique is applied to alleviate the SIC errors and enhance the secrecy performance of the security-required user (SRU) [29]. The authors in [30] investigated CR-inspired NOMA (CR-NOMA) networks using PLS with multiple primary and secondary users. To assist the cell-edge group considered as the primary user multicast group (PU-MG), the spectrum efficient CR-NOMA framework is proposed, in which the cell-center group designated as the secondary user multicast group (SU-MG) benefits from spectrum access opportunity [31]. They provided the system to allow the BS requires a pair of users from another multicast group located in its vicinity to perform relaying and jamming signal at the same time. Such a system is proven related to its improvement in terms of the reception reliability of the weaker users as well as ensuring minimum interception. In another work, the secondary users are employed the NOMA scheme to

send the uplink privacy data, which is comminated by the eavesdropper [32].

A. RELATED WORK AND MOTIVATIONS

The authors in [29], [30], [31], and [32] considered secure CR-NOMA networks with perfect hardware paradigms. Actually, according to the previous analysis, the inherent benefit can be achieved to enhance system performance by combining overlay CR with NOMA. In addition, CR-NOMA can improve secure performance and highly meet the real scenario of hardware impairment [33], [34], [35]. Although most of the wireless system is greatly degraded in terms of performance due to impacts of hardware impairments, IQI is known as the most significant source of analog impairments [33]. The performance and the effects of transmitter/receiver IQI in NOMA systems were considered in [33] and [34]. The performance of FD NOMA relaying systems is explored in the presence of in-phase and IQI [30]. Regarding the security of cooperative dual-hop NOMA for internet-of-thing (IoT) networks, the transceivers are considered in terms of a detrimental factor related to in-phase and IQI [34].

The PLS performance in underlay CR-NOMA networks under the impact of hardware impairment is still a topic of discussion, which motivates our study. However, there are some special issues to overcome for PLS in underlay CR-NOMA networks. Firstly, the application of NOMA in CR-NOMA networks establishes more interferences among users, increasing the complexity of transmission scheme design. Moreover, by implementing the TAS scheme in the CR-NOMA system, some improvement issues should be considered, which increases the difficulty of interference control. Furthermore, the existing works cannot be introduced PLS in CR-NOMA networks in the presence of hardware impairment (HI) and it is very challenging to achieve the closed-form formula for several secrecy metrics in such CR-NOMA networks. We aim to fill these missing issues in this article.

B. MAIN CONTRIBUTION AND ORGANIZATION

Our main contributions and insights are summarized as:

- We propose the secure CR-NOMA in secondary network transmission to provide high spectrum efficiency, which means the secondary transmitter first allocates power to satisfy the QoS of the first secondary user and then uses the rest of the power to serve the second user. We consider a scenario including two secondary users and an eavesdropper. A sector secrecy guard zone containing these users is invoked to evaluate PLS. Furthermore, TAS is deployed to improve PLS.
- To provide the secure performance of the considered system, we derive the closed-form expressions of OP, intercept probability (IP), and effective secrecy throughput (EST), which shows that the secondary users can achieve better performance in the sector secrecy guard zone. Notably, the EST examines the optimal performance at the specific level of SNR at the BS.
- We have investigated the performance of two secondary users, and it is shown that: *i) the strong secondary user can get the same secure performance as comparing IQI and ideal cases, while the weak secondary user decreases its secure performance significantly*; *ii) when the key parameters of the system are reasonably constituted, the secondary user can be reached optimal EST*; *iii) the resulting analysis shows that a high number of transmit antennas at the BS can be also implemented to enhance secrecy performance*. In general, an easy choice of transmit power is provided to achieve higher secrecy performance for secondary users.

The remainder of this paper is organized as follows. Section II introduces the system model of IQI-aware CR-NOMA. Section III, we derive the exact analytical expressions for the OP, IP, and EST. To verify our theoretical analyses, we provide numerical and simulation results in Section IV. Finally, we summarize the main achievements of this paper in Section V.

II. SYSTEM MODEL

This section provides details of the network setup and the main parameters of the system model can be seen in Table 1. Such considered CR-NOMA is illustrated in Fig. 1.

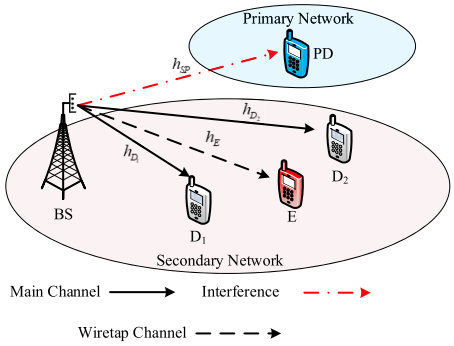

FIGURE 1. System model of secure CR-NOMA.

We recommend possible applications of such CR-NOMA in IoT systems as follows

- The IoT applications of 6G cellular networks, where the BS or access point needs the assistance of the primary network (sharing spectrum) to directly talk to each IoT device. By employing NOMA, such a system can mitigate the situation of weak signals received at destinations due to obstacles or bad quality of transmission. We will evaluate the impact of the eavesdropper by considering it as an unwanted signal from adjacent IoT devices.
- The actuators need reliable signals directly transmitted from a central controller industrial in the context of IoT or smart grid. In this scenario, it is critically important to ensure information secrecy, even if such an attacker intends to overhear transmission from a central controller.
- As an emerging low power wide area networking (LPWAN) technique, NOMA benefits to Long Range

TABLE 1. Main parameter.

Symbol	Definition
x_i	The message from the BS to NOMA user D_i
Θ_1, Θ_2	The power allocation factors with $\Theta_1 + \Theta_2 = 1$ and $\Theta_1 > \Theta_2$
φ_t	The transmitter (TX) amplitude
φ_r	The receiver (RX) amplitude
ϕ_t	The transmitter (TX) phase mismatch levels
ϕ_r	The receiver (RX) phase mismatch levels
P_S	The transmit power at the BS
Q	The maximum average allowed transmit power at the BS
I_P	the interference temperature constraint at primary destination
n_i, n_E	The additive white Gaussian noise
$\mathbf{h}_{D_i}$	The N × 1 channel vector between base station and D_i
$\mathbf{h}_E$	The N × 1 channel vector between the BS and E
$\mathbf{h}_{SP}$	The N × 1 channel vector between the BS and PD

Radio (LoRa) networking. In particular, it is vulnerable to eavesdropping attacks since LoRa technology utilizes a symmetric key cryptographic approach with the advanced encryption standard (AES), without any update. By exploiting PLS and CR-NOMA schemes, the access point is considered as a resilient approach which can be utilized to guarantee reliable communication for LoRa networking.

In the context of CR-NOMA, we consider the secondary BS to be equipped with N antennas, two legitimate users including user $D_i (i \in \{1, 2\})$, and an eavesdropper (E). In this scenario, the primary network is assumed that a primary destination (PD) with an interference effect from the secondary network, shown in Figure 1. However, from the viewpoint of PLS, the unsecured transmission would occur in the presence of an eavesdropper in the considered zone (containing a group of NOMA users). It is assumed that all receivers meet additive white Gaussian noise (AWGN) with mean zero and variance N_0. Furthermore, all the wireless channels are modeled to be independent quasi-static block Rayleigh fading channels. Furthermore, $\mathbf{h}_z (z \in \{D_1, D_2, SP, E\})$ is the channel vector and modeled by $\mathcal{CN}(0, \lambda_z)$.

First, the time-domain baseband representation of the IQI-impaired signal is formulated as [41] and [42]

$$\hat{x} = \omega_{t/r} x + \bar{\omega}_{t/r} x^*, \tag{1}$$

where x stands for the baseband transmitted signal under perfect transmitter/receiver (TX/RX) IQI matching. We denote x^* as the mirror signal after being affected by IQI. Regarding detailed IQI coefficients $\omega_{t/r}$ and $\bar{\omega}_{t/r}$ are expressed by [33] respectively

$$\omega_t = \frac{(1 + \varphi_t \exp(j\phi_t))}{2}, \tag{2a}$$

$$\bar{\omega}_t = \frac{(1 - \varphi_t \exp(j\phi_t))}{2}, \tag{2b}$$

$$\omega_r = \frac{(1 + \varphi_r \exp(j\phi_r))}{2}, \tag{2c}$$

$$\bar{\omega}_t = \frac{(1 - \varphi_r \exp(j\phi_r))}{2}. \tag{2d}$$

It's noticed that in the case of ideal IQI, these parameters should be $\varphi_t = \varphi_r = 1$ and $\phi_r = \phi_t = 0^o$.

To guarantee the normal operation of the primary network, the cognitive transmitter power at the BS should satisfy [28]

$$P_S = \min\left(\frac{I_P}{Z_{SP}}, Q\right), \tag{3}$$

To make the generality and easy to analyze the following performances, we denote $Z_z = \max\left\{|\mathbf{h}_z|^2\right\}, (z \in \{D_1, D_2, SP, E\})$. Noticing the principle of NOMA transmission, the BS transmits the superimposed signal $x_S = \sqrt{\Theta_1} x_1 + \sqrt{\Theta_2} x_2$ to the secondary users D_i.

Then, by considering the existence of IQI on both the TX and the RF front-end, the received signal at D_i and E are given respectively

$$y_i = \omega_i \left(\mathbf{h}_{D_i} \left(\omega_S x_S + \bar{\omega}_S (x_S)^*\right) + n_i\right) + \bar{\omega}_i \left(\mathbf{h}_{D_i} \left(\omega_S x_S + \bar{\omega}_S (x_S)^*\right) + n_i\right)^*, \tag{4}$$

$$y_E = \omega_E \left(\mathbf{h}_E \left(\omega_S x_S + \bar{\omega}_S (x_S)^*\right) + n_E\right) + \bar{\omega}_E \left(\mathbf{h}_E \left(\omega_S x_S + \bar{\omega}_S (x_S)^*\right) + n_E\right)^*. \tag{5}$$

Next, the signal to interference plus noise ratio (SINR) at D_1 when decoding the own signal x_1 is given by

$$\Gamma_{1,1} = \frac{P_S Z_{D_1} \Theta_1 \vartheta_1}{P_S Z_{D_1} \Theta_2 \vartheta_1 + P_S Z_{D_1} \nu_1 + \upsilon_1 N_0}, \tag{6}$$

where $\vartheta_i = \left|\omega_i \omega_S + \bar{\omega}_i \bar{\omega}_S^*\right|^2$, $\nu_i = \left|\omega_i \bar{\omega}_S + \bar{\omega}_i \omega_S^*\right|^2$ and $\upsilon_i = |\omega_i|^2 + |\bar{\omega}_i|^2, (i \in \{1, 2\})$. In addition, it can be written ϑ_i as $\vartheta_i \approx |\omega_i \omega_S|^2 + \left|\bar{\omega}_i \bar{\omega}_S^*\right|^2$ [3].

Similarly, the SINR at D_2 when decode interference signal x_1 is given by

$$\Gamma_{2,1} = \frac{P_S Z_{D_2} \Theta_1 \vartheta_2}{P_S Z_{D_2} \Theta_2 \vartheta_2 + P_S Z_{D_2} \nu_2 + \upsilon_2 N_0}. \tag{7}$$

Applying SIC enabled at the dedicated receiver,[1] the SINR at D_2 when decoding the own signal x_2 is given by

$$\Gamma_{2,2} = \frac{P_S Z_{D_2} \Theta_2 \vartheta_2}{P_S Z_{D_2} \Theta_1 \bar{\vartheta}_2 + P_S Z_{D_2} \nu_2 + \upsilon_2 N_0}, \tag{8}$$

where $\bar{\vartheta}_2 = \left|\omega_2 \omega_S - 1 + \bar{\omega}_2 \bar{\omega}_S^*\right|^2 \approx |\omega_2 \omega_S - 1|^2 + \left|\bar{\omega}_2 \bar{\omega}_S^*\right|^2$.

Regarding signal processing at illegal users, the SINR at the eavesdropper when detecting signal x_1 and x_2 are expressed by [36]

$$\Gamma_{E,1} = \frac{P_S Z_E \Theta_1 \vartheta_E}{P_S Z_E \Theta_2 \vartheta_E + P_S \nu_E |h_E|^2 + \upsilon_E N_0}, \tag{9}$$

$$\Gamma_{E,2} = \frac{P_S Z_E \Theta_2 \vartheta_E}{P_S Z_E \Theta_1 \bar{\vartheta}_E + P_S Z_E \nu_E + \upsilon_E N_0}, \tag{10}$$

where $\vartheta_E = \left|\omega_E \omega_S + \bar{\omega}_E \bar{\omega}_S^*\right|^2 \approx |\omega_E \omega_S|^2 + \left|\bar{\omega}_E \bar{\omega}_S^*\right|^2$, $\nu_E = \left|\omega_E \bar{\omega}_S + \bar{\omega}_E \omega_S^*\right|^2, \upsilon_E = |\omega_E|^2 + |\bar{\omega}_E|^2$, $\bar{\vartheta}_E = \left|\omega_E \omega_S - 1 + \bar{\omega}_E \bar{\omega}_S^*\right|^2 \approx |\omega_E \omega_S - 1|^2 + \left|\bar{\omega}_E \bar{\omega}_S^*\right|^2$.

[1] In this consideration, we only study the two-users model for NOMA, the extended number of users can be analyzed in a similar way in term of mathematical perceptive [10], [11], [12], [13], [14], [15]. We also assume that fixed power allocation schemes corresponding to static signal decoding order are designed with SIC and non-SIC users at the receiver side. Such classification related to SIC ability is decided based on which is the strong user or not.

III. SECURE PERFORMANCE ANALYSIS

In this section, two secondary users, are considered for the downlink cognitive network in the context of the CR-NOMA. We first analyze the secondary secrecy performance, and then we compare the performance of two users and evaluate which factor make a significant influence on such secure performance. How IQI make influence the performance of legal users to remain their operation satisfying QoS requirement and more verification are expected based on such a main analysis. In particular, we provide details of the step-by-step derivations of secure metrics such as OP, IP, and EST. It is expected that we can claim the closed-form expressions for these metrics.

A. CHANNEL MODEL

In this case, adopting transmit antenna selection the probability density function (PDF) and cumulative density function (CDF) of channel Z_z are given [46] respectively by

$$f_{Z_z}(x) = \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^{n-1} n}{\lambda_z} e^{-\frac{nx}{\lambda_z}}, \tag{11}$$

$$F_{Z_z}(x) = 1 - \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} e^{-\frac{nx}{\lambda_z}}. \tag{12}$$

B. OUTAGE PROBABILITY

Before determining OP, we denote $R_i, i = \{1, 2\}$ as target rates for users D_i corresponding QoS requirements. The outage probability of D_1 is determined by [44]

$$\mathcal{OP}_{D_1} = \Pr\left(\Gamma_{1,1} < \gamma_1 - 1\right). \tag{13}$$

where $\gamma_1 = 2^{R_1} - 1$.

Proposition 1: The closed-form OP of D_1 can be given as (14), as shown at the bottom of the page, in which $\psi_1 = \frac{\gamma_1 \upsilon_1}{\Theta_1 \vartheta_1 - \gamma_1 (\Theta_2 \bar{\vartheta}_1 + \nu_1)}$.

Please refer to Appendix A for detailed proof of derivation of (14). Next, we derive the OP of D_2 which is given by

$$\mathcal{OP}_{D_2} = \Pr\left(\Gamma_{2,2} < 2^{R_2} - 1\right). \tag{15}$$

Replacing (3) and (8) into (15), we get

$$\begin{aligned}\mathcal{OP}_{D_2} &= 1 - \Pr\left(\Gamma_{2,2} > 2^{R_2} - 1\right) \\ &= 1 - \Pr\left(\frac{\rho Z_{D_2} \Theta_2 \vartheta_2}{\rho Z_{D_2} \Theta_1 \bar{\vartheta}_2 + \rho Z_{D_2} \nu_2 + \upsilon_2} > \gamma_2, Z_{SP} < \frac{\rho_I}{\rho}\right) \\ &\quad - \Pr\left(\frac{\rho_I Z_{D_2} \Theta_2 \vartheta_2}{\rho_I Z_{D_2} \Theta_1 \bar{\vartheta}_2 + \rho_I Z_{D_2} \nu_2 + Z_{SP} \upsilon_2} > \gamma_2, Z_{SP} > \frac{\rho_I}{\rho}\right),\end{aligned} \tag{16}$$

where $\gamma_2 = 2^{R_2} - 1$. Following the approach of Appendix A, the closed-form OP of D_2 can be obtained, thus, we have (17), as shown at the bottom of the next page, in which $\psi_2 = \frac{\gamma_2 \upsilon_2}{\Theta_2 \vartheta_2 - \gamma_2 (\Theta_1 \bar{\vartheta}_2 + \nu_2)}$.

Remark 1: It can be concluded from proposition 1 that the OPs of the two users are a decreasing function of the transmit SNR at the BS ρ. This implies that when the transmit power at the BS increases, the reliability performance of the two users is strengthened. In (16), (17), we found that the number of transmit antennas N, transmit SNR ρ, and channel gains are the main factors affecting secure performance metrics. Furthermore, decreasing the target rate R_i of the two users can reduce the OP of these users. It means that reducing the requirement of target rates is another way to enhance reliability. As a result, we do not need to change the transmit power at the BS.

C. INTERCEPT PROBABILITY

In the context of the PLS technique, the eavesdropper can decode confidential information from the BS by applying a signal detection technique. As further metric, the IP of D_1 can be given as [44]

$$\mathcal{IP}_{D_1} = \Pr\left(\Gamma_{E,1} > 2^{R_1} - 1\right), \tag{18}$$

Proposition 2: The closed-form expression of IP for user D_1 is computed by

$$\begin{aligned}\mathcal{IP}_{D_1} &= \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right) \\ &\quad \times \sum_{n_E=1}^{N} \binom{N}{n_E} (-1)^{n_E-1} e^{-\frac{\psi_{E,1} n_E}{\rho \lambda_E}} \\ &\quad + \sum_{n_E=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_E}\binom{N}{n_{SP}} (-1)^{n_E+n_{SP}-2} \\ &\quad \times \frac{n_{SP}\rho_I \lambda_E}{\psi_{E,1} n_1 \lambda_{SP} + \rho_I \lambda_E n_{SP}} e^{-\frac{\psi_{E,1} n_E \lambda_{SP} + \rho_I \lambda_E n_{SP}}{\rho \lambda_E \lambda_{SP}}}\end{aligned} \tag{19}$$

where $\psi_{E,1} = \frac{\gamma_1 \upsilon_E}{\Theta_2 \vartheta_E - (\gamma_2 \Theta_1 \bar{\vartheta}_E + \nu_E)}$.

Proof: See Appendix B.

Looking at the performance of the second user, the IP of D_2 is given by

$$\mathcal{IP}_{D_2} = \Pr\left(\Gamma_{E,2} > 2^{R_2} - 1\right). \tag{20}$$

$$\begin{aligned}OP_{D_1} &= 1 - \sum_{n_1=1}^{N} \binom{N}{n_1} (-1)^{n_1-1} e^{-\frac{\psi_1 n_1}{\rho \lambda_{D_1}}} \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right) \\ &\quad - \sum_{n_1=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_1}\binom{N}{n_{SP}} \frac{(-1)^{n_1+n_{SP}-2} n_{SP}\rho_I \lambda_{D_1}}{\psi_1 n_1 \lambda_{SP} + \rho_I \lambda_{D_1} n_{SP}} e^{-\frac{\psi_1 n_1 \lambda_{SP} + \rho_I \lambda_{D_1} n_{SP}}{\rho \lambda_{D_1} \lambda_{SP}}}\end{aligned} \tag{14}$$

Similarly, the closed-form expression of IP for user D_2 is formulated by

$$\mathcal{IP}_{D_2} = \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right) \times \sum_{n_E=1}^{N} \binom{N}{n_E} (-1)^{n_E-1} e^{-\frac{\psi_{E,2} n_E}{\rho\lambda_E}} + \sum_{n_E=1}^{N}\sum_{n_{SP}=1}^{N} \binom{N}{n_E}\binom{N}{n_{SP}} (-1)^{n_E+n_{SP}-2} \times \frac{n_{SP}\rho_I\lambda_E}{\psi_{E,2} n_1 \lambda_{SP} + \rho_I\lambda_E n_{SP}} e^{-\frac{\psi_{E,2} n_E \lambda_{SP} + \rho_I\lambda_E n_{SP}}{\rho\lambda_E\lambda_{SP}}} \quad (21)$$

where $\psi_{E,2} = \frac{\gamma_2 \upsilon_E}{\Theta_2 \vartheta_E - (\gamma_2\Theta_1\bar{\vartheta}_E + \upsilon_E)}$.

Remark 2: It can be deduced from Proposition 2 that the IP of the two users are different. Two values of power allocation Θ_1, Θ_2 result in a performance gap. Besides, channel gains also contribute to varying the reliability performance of these. In derived expressions, the number of transmit antennas at the BS, N is a further factor reflecting an improvement of secure performance. Then, the level of IQI can be confirmed as a factor related to degraded performance when we consider two metrics, i.e. OP and IP.

D. EFFECTIVE SECRECY THROUGHPUT

In the previous section, OP and IP are the metrics to indicate reliability and security performance, respectively. These metrics are inadequate to evaluate the performance of both reliability and security. As a further evaluation, we compute EST to characterize the efficiency and security of the considered system. In particular, the EST of D_1 and D_2 are formulated respectively by

$$\tau_1 = R_1 \Pr\left(\Gamma_{1,1} > 2^{R_1} - 1, \Gamma_{E,1} < 2^{R_1} - 1\right), \quad (22)$$

$$\tau_2 = R_2 \Pr\left(\Gamma_{2,2} > 2^{R_2} - 1, \Gamma_{E,2} < 2^{R_2} - 1\right). \quad (23)$$

Proposition 3: The closed-form expression of EST for user D_1 is given as (24), as shown at the bottom of the next page.

Proof: See Appendix C.

Similarly, the closed-form expression of EST for user D_2 is given as (25), as shown at the bottom of the next page.

IV. NUMERICAL RESULTS

We set main parameters before simulation as $\Theta_1 = 0.75$, $\Theta_2 = 0.25$, $\lambda_{D_1} = \lambda_{D_2} = 1$, $\lambda_E = 0.1$, $R_1 = R_2 = 1$, (BPCU) in which BPCU is short for bit per channel use, $\varphi_t = \varphi_r = 1.05$, $\phi_r = \phi_t = 20^o$ and $\varphi_t = \varphi_r = 1$, $\phi_r = \phi_t = 0^o$ for ideal IQI.

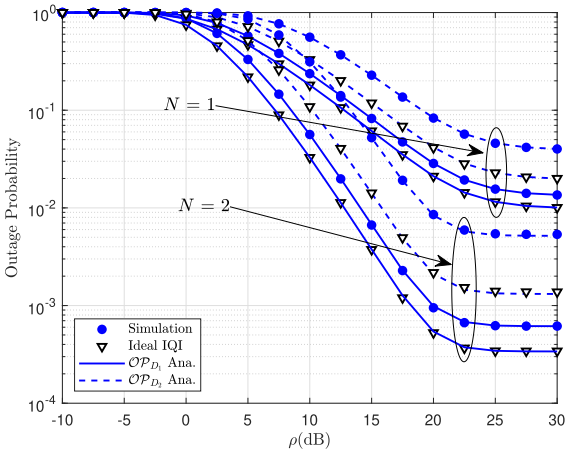

FIGURE 2. The OP versus transmit ρ(dB) varying N with $\rho_I = 20$ dB.

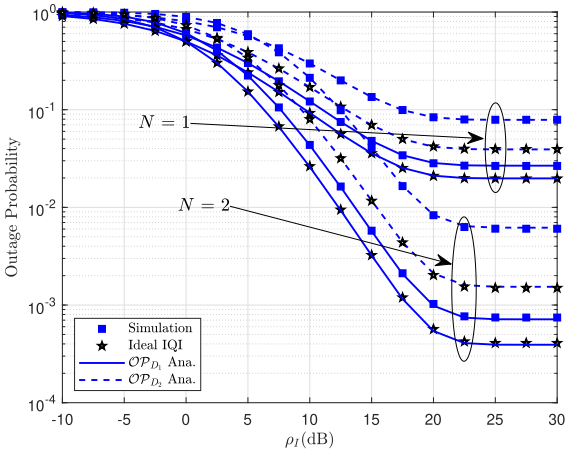

FIGURE 3. The OP versus transmit ρ_I(dB) varying N with $\rho = 20$ dB.

Fig. 2 illustrates the OP of two users versus the transmit SNR ρ at the BS in such NOMA and we further compare system performance in two cases, i.e. IQI imbalance and ideal case. Such performance can be obtained from (14) and (17). It is important to report that the accuracy computation is achieved since the simulation of the derived expressions of OP is consistent with the results by performing the Monte-Carlo simulations. As expected, the OP increases as ρ increases and significant improvement is obtained with

$$\mathcal{OP}_{D_2} = 1 - \sum_{n_2=1}^{N} \binom{N}{n_2} (-1)^{n_2-1} e^{-\frac{\psi_2 n_2}{\rho\lambda_{D_2}}} \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right) - \sum_{n_2=1}^{N}\sum_{n_{SP}=1}^{N} \binom{N}{n_2}\binom{N}{n_{SP}} \frac{(-1)^{n_2+n_{SP}-2} n_{SP}\rho_I\lambda_{D_1}}{\psi_2 n_2\lambda_{SP} + \rho_I\lambda_{D_2} n_{SP}} e^{-\frac{\psi_2 n_2\lambda_{SP} + \rho_I\lambda_{D_2} n_{SP}}{\rho\lambda_{D_2}\lambda_{SP}}} \quad (17)$$

the number of antennas is $N = 2$. As indicated from a mathematical perspective, OP in the ideal case for user D_2 clearly outperforms the IQI case. When $N = 1$, the OP would be unchanged at a high SNR regime. That means OP performance is still limited at a high point of SNR because it depends on other parameters such as power allocation factors or channel gains. A similar trend of OP can be seen in Fig. 3 as we vary the interference power (related to ρ_I).

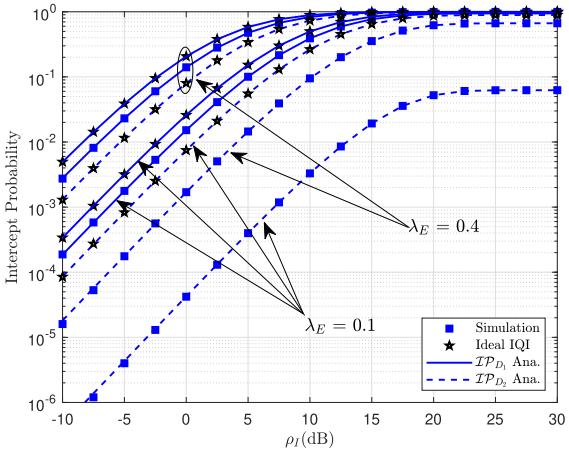

FIGURE 4. The IP versus transmit ρ_I(dB) varying λ_E with $N = 2$ and $\rho = 20$dB.

In Fig. 4, we plot IP curves versus ρ_I under many cases of λ_E. Significantly, we find that the Monte Carlo simulation curves match precisely with the analytical ones, which confirms the exactness of our analysis. We first observe that, for both users, the curves of IP increase due to the increase of ρ_I. It can be observed that a stronger channel of eavesdropper leads to worse performance, i.e. λ_E exhibits the worst IP for both users. In contrast with the reliability performance shown in Fig. 2 and 3, the secrecy performance can be improved because of the increase in transmit power. In addition, there is a gap in the IP performance of the two users. This situation can be explained that different power factors Θ_1, Θ_2 allocated to different users. It demonstrates that careful selection of power allocation ratio can realize the tradeoff of the secrecy performance of two users.

In a similar experiment, Fig. 5 shows IP performance with some cases of target rates. It can be concluded that the better IP corresponds to the lower target rate required. In particular, the requirement for secrecy rate R_1, R_2 of two users is certainly a factor to achieve varying IP performance.

In another experiment, Fig. 6 indicates that IP performance can be improved significantly if we increase transmit SNR ρ from -5dB to 15dB. However, IP keeps unchanged afterward. It can be explained that IP relies on many variables rather than only transmitting SNR. This is the limitation of IP performance at a high SNR regime.

Fig. 7 presents the effects of transmit SNR on the EST for user two users with different values of the number of transmit antennas $N = 1$, $N = 2$, and $N = 3$. Interestingly, there

$$\begin{aligned}\tau_1 = {} & R_1 \sum_{n_1=1}^{N} \binom{N}{n_1} (-1)^{n_1-1} e^{-\frac{\psi_1 n_1}{\rho\lambda_{D_1}}} \left(1 - \sum_{n_E=1}^{N} \binom{N}{n_E} (-1)^{n_E-1} e^{-\frac{\psi_{E,1} n_E}{\rho\lambda_E}}\right) \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right). \\ & + R_1 \sum_{n_1=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_1}\binom{N}{n_{SP}} (-1)^{n_1+n_{SP}-2} \frac{n_{SP}\rho_I\lambda_{D_1}}{\psi_1 n_1\lambda_{SP} + \rho_I\lambda_{D_1} n_{SP}} e^{-\frac{\psi_1 n_1\lambda_{SP}+\rho_I\lambda_{D_1} n_{SP}}{\rho\lambda_{D_1}\lambda_{SP}}} \\ & - R_1 \sum_{n_1=1}^{N} \sum_{n_E=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}}\binom{N}{n_E}\binom{N}{n_1} \frac{(-1)^{n_E+n_1+n_{SP}-3} n_{SP}\lambda_E\lambda_{D_1}\rho_I e^{-\frac{n_1\psi_1\lambda_{SP}\lambda_E+\lambda_{D_1}\lambda_{SP} n_E\psi_{E,1}+\lambda_{D_1}\lambda_E\rho_I n_{SP}}{\lambda_{D_1}\rho}}}{n_1\psi_1\lambda_{SP}\lambda_E + \lambda_{D_1}\lambda_{SP} n_E\psi_{E,1} + \lambda_{D_1}\lambda_E\rho_I n_{SP}}.\end{aligned} \tag{24}$$

$$\begin{aligned}\tau_2 = {} & R_2 \sum_{n_2=1}^{N} \binom{N}{n_2} (-1)^{n_2-1} e^{-\frac{\psi_2 n_2}{\rho\lambda_{D_2}}} \left(1 - \sum_{n_E=1}^{N} \binom{N}{n_E} (-1)^{n_E-1} e^{-\frac{\psi_{E,2} n_E}{\rho\lambda_E}}\right) \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right). \\ & + R_2 \sum_{n_2=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_2}\binom{N}{n_{SP}} (-1)^{n_2+n_{SP}-2} \frac{n_{SP}\rho_I\lambda_{D_2}}{\psi_2 n_2\lambda_{SP} + \rho_I\lambda_{D_2} n_{SP}} e^{-\frac{\psi_2 n_2\lambda_{SP}+\rho_I\lambda_{D_2} n_{SP}}{\rho\lambda_{D_2}\lambda_{SP}}} \\ & - R_2 \sum_{n_2=1}^{N} \sum_{n_E=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}}\binom{N}{n_E}\binom{N}{n_2} \frac{(-1)^{n_E+n_2+n_{SP}-3} n_{SP}\lambda_E\lambda_{D_2}\rho_I e^{-\frac{n_2\psi_2\lambda_{SP}\lambda_E+\lambda_{D_2}\lambda_{SP} n_E\psi_{E,2}+\lambda_{D_2}\lambda_E\rho_I n_{SP}}{\lambda_{D_2}\rho}}}{n_2\psi_2\lambda_{SP}\lambda_E + \lambda_{D_2}\lambda_{SP} n_E\psi_{E,2} + \lambda_{D_2}\lambda_E\rho_I n_{SP}}.\end{aligned} \tag{25}$$

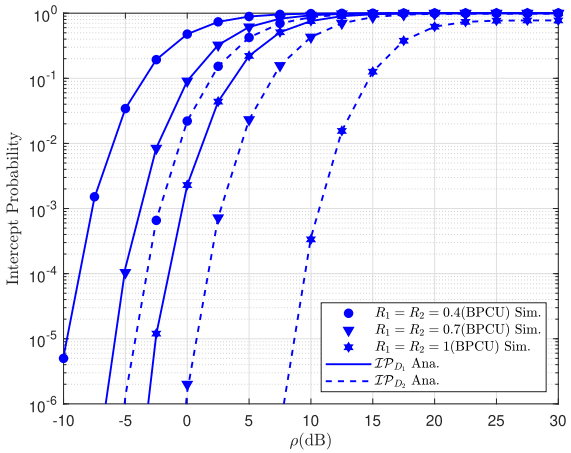

FIGURE 5. The IP versus transmit ρ(dB) varying R_1, R_2 with $N = 2$ and $\rho_I = 20$ dB.

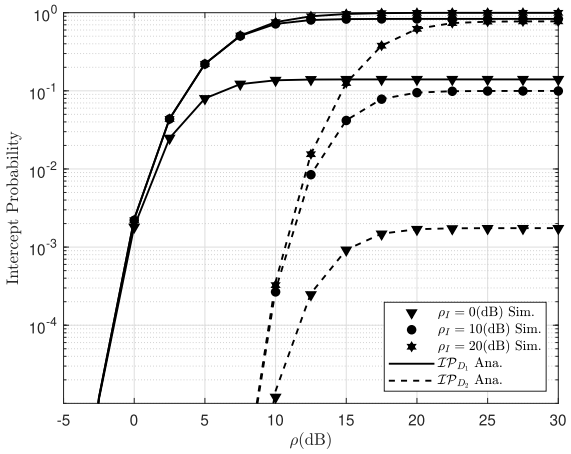

FIGURE 6. The IP versus transmit ρ (dB) varying ρ_I with $N = 2$.

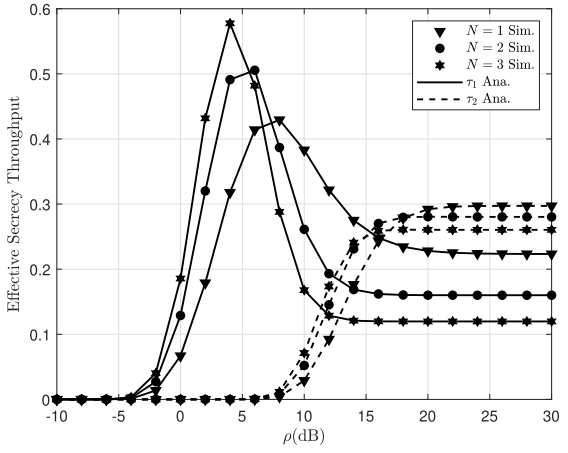

FIGURE 7. The EST versus transmit ρ(dB) varying N with $\rho_I = 10$(dB).

is an optimal SNR that maximizes the EST of two users. It is important to have a set of transmit power at the BS and a higher number of transmit antennas can be selected to achieve optimal performance in terms of EST. We can see that the EST of the user D_1 outperforms that of the user D_2 and a big gap between the two users can be reported for three cases of N.

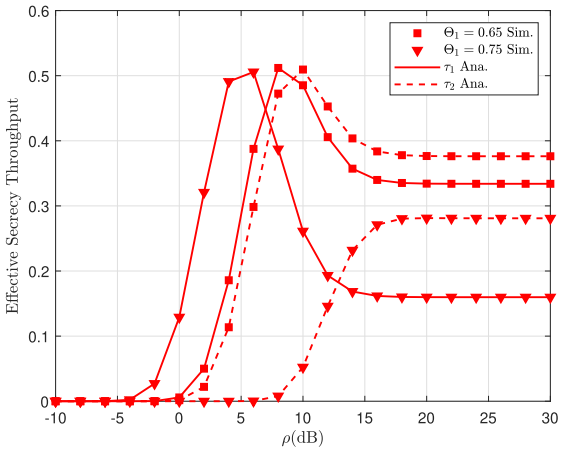

FIGURE 8. The EST versus transmit ρ(dB) varying Θ_1 with $\rho = 10$(dB) and N = 2.

Fig. 8 presents the relationship between the EST and ρ_I with the different target date rates Θ. It is worth noting that optimal EST still can be obtained by controlling the value of ρ_I. It means that there are optimal power allocation factors and ρ_I to guarantee secure performance for two users. Furthermore, it is more important to select a reasonable set of these parameters rather than increasing transmit SNR at the BS.

V. CONCLUSION

In this paper, we have studied secrecy performance for downlink in underlay CR-NOMA systems. It is more important to consider PLS and IQI problems in such systems to remain normal operation for the whole system. We deployed the TAS scheme for the base station to improve secure performance. Specifically, after the QoS of secondary users with high priority is satisfied, the suitable power allocation scheme and the number of transmit antennas at the base station can be adjusted to serve secondary users better. Considering the reasonable set of these parameters, we achieve optimal EST by numerical method, while still satisfying the OP, and IP performance for the proposed CR-NOMA systems. By limiting the impact of IQI, such a system still operates with acceptable secure performance. Moreover, our results have certain reference values for different demands of secondary users in such IQI-aware CR-NOMA systems. Especially, such a system model is beneficial to design the IoT in potential applications as recommended, in which some users have higher priority of services, and some users need higher security demand. In future works, more users and practical scenarios are goals for our study.

APPENDIX A

With the help (3) and (6), we can rewrite $\mathcal{OP}_{D_1}$ as (26), as shown at the bottom of the next page, in which $\gamma_1 = 2^{R_1} - 1$, $\rho = \frac{Q}{N_0}$ and $\rho_I = \frac{I_P}{N_0}$.

Then, the first term of (26), A_1 can be calculated by

$$A_1 = \Pr\left(Z_{D_1} > \psi_1 \ , Z_{SP} < \frac{\rho_I}{\rho}\right) = \bar{F}_{Z_{D_1}}\left(\frac{\psi_1}{2}\right) F_{Z_{SP}}\left(\frac{\rho_I}{\rho}\right) \quad (27)$$

where $\bar{F}(.) = 1 - F(.)$ and $\psi_1 = \frac{\gamma_1 \upsilon_1}{\Theta_1 \vartheta_1 - \gamma_1(\Theta_2 \vartheta_1 + \nu_1)}$.

Based on (12), A_1 is obtained by

$$A_1 = \sum_{n_1=1}^{N} \binom{N}{n_1} (-1)^{n_1-1} e^{-\frac{\psi_1 n_1}{\rho \lambda_{D_1}}} \times \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right) \quad (28)$$

Moreover, the second term of (26), A_2 is rewritten by

$$A_2 = \Pr\left(Z_{D_1} > \frac{\psi_1 Z_{SP}}{\rho_I} \ , Z_{SP} > \frac{\rho_I}{\rho}\right) = \int_{\frac{\rho_I}{\rho}}^{\infty} f_{Z_{SP}}(x) \bar{F}_{Z_{D_1}}\left(\frac{\psi_1 x}{\rho_I}\right) dx \quad (29)$$

Putting (11) and (12) into (29), A_2 is re-expressed by

$$A_2 = \sum_{n_1=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_1}\binom{N}{n_{SP}} \times \frac{(-1)^{n_1+n_{SP}-2} n_{SP}}{\lambda_{SP}} \int_{\frac{\rho_I}{\rho}}^{\infty} e^{-\frac{\psi_1 n_1 x}{\rho_I \lambda_{D_1}} - \frac{n_{SP} x}{\lambda_{SP}}} dx \quad (30)$$

The closed-form of A_2 can be formulated by

$$A_2 = \sum_{n_1=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_1}\binom{N}{n_{SP}} (-1)^{n_1+n_{SP}-2} \times \frac{n_{SP}\rho_I \lambda_{D_1}}{\psi_1 n_1 \lambda_{SP} + \rho_I \lambda_{D_1} n_{SP}} e^{-\frac{\psi_1 n_1 \lambda_{SP} + \rho_I \lambda_{D_1} n_{SP}}{\rho \lambda_{D_1} \lambda_{SP}}} \quad (31)$$

Substituting (28) and (31) into (26), it is obtained the closed-form OP of D_1.

It is the end of the proof.

APPENDIX B

Substituting (3) and (9) into (19), we have

$$\begin{aligned}\mathcal{IP}_{D_1} &= \Pr\left(\frac{P_S Z_E \Theta_1 \vartheta_E}{P_S Z_E \Theta_2 \vartheta_E + P_S Z_E \nu_E + \upsilon_E N_0} > \gamma_1\right) \\ &= \underbrace{\Pr\left(\frac{\rho Z_E \Theta_1 \vartheta_E}{\rho Z_E \Theta_2 \vartheta_E + \rho Z_E \nu_E + \upsilon_E} > \gamma_1, Z_{SP} < \frac{\rho_I}{\rho}\right)}_{B_1} \\ &\quad + \underbrace{\Pr\left(\frac{\rho_I Z_E \Theta_1 \vartheta_E}{\rho_I Z_E \Theta_2 \vartheta_E + \rho_I Z_E \nu_E + Z_{SP}\upsilon_E} > \gamma_1, Z_{SP} > \frac{\rho_I}{\rho}\right)}_{B_2},\end{aligned} \quad (32)$$

Similarly, it can be obtained the closed-form B_1 and B_2 respectively by

$$B_1 = F_{Z_{SP}}\left(\frac{\rho_I}{\rho}\right) \bar{F}_{Z_E}\left(\frac{\psi_{E,1}}{\rho}\right) = \left(1 - \sum_{n_{SP}=1}^{N} \binom{N}{n_{SP}} (-1)^{n_{SP}-1} e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right) \times \sum_{n_E=1}^{N} \binom{N}{n_E} (-1)^{n_E-1} e^{-\frac{\psi_{E,1} n_E}{\rho \lambda_E}}, \quad (33)$$

and

$$B_2 = \int_{\frac{\rho_I}{\rho}}^{\infty} f_{Z_{SP}}(x) \bar{F}_{Z_E}\left(\frac{\psi_{E,1} x}{\rho_I}\right) dx = \sum_{n_E=1}^{N} \sum_{n_{SP}=1}^{N} \binom{N}{n_E}\binom{N}{n_{SP}} (-1)^{n_E+n_{SP}-2} \times \frac{n_{SP}\rho_I \lambda_E}{\psi_{E,1} n_1 \lambda_{SP} + \rho_I \lambda_E n_{SP}} e^{-\frac{\psi_{E,1} n_E \lambda_{SP} + \rho_I \lambda_E n_{SP}}{\rho \lambda_E \lambda_{SP}}} \quad (34)$$

where $\psi_{E,1} = \frac{\gamma_1 \upsilon_E}{\Theta_1 \vartheta_E - (\gamma_1 \Theta_2 \vartheta_E + \nu_E)}$. Putting (33) and (34) into (32), we complete the proof.

APPENDIX C

With the help (3), (6) and (9), we can rewrite τ_1 as (35), as shown at the top of the next page.

$$\begin{aligned}\mathcal{OP}_{D_1} &= 1 - \Pr\left(\frac{P_S Z_{D_1} \Theta_1 \vartheta_1}{P_S Z_{D_1} \Theta_2 \vartheta_1 + P_S \nu_1 Z_{D_1} + \upsilon_1 N_0} > \gamma_1\right) \\ &= 1 - \underbrace{\Pr\left(\frac{\rho Z_{D_1} \Theta_1 \vartheta_1}{\rho Z_{D_1} \Theta_2 \vartheta_1 + \rho Z_{D_1} \nu_1 + \upsilon_1} > \gamma_1, \rho < \frac{\rho_I}{Z_{SP}}\right)}_{A_1} - \underbrace{\Pr\left(\frac{\rho_I Z_{D_1} \Theta_1 \vartheta_1}{\rho_I Z_{D_1} \Theta_2 \vartheta_1 + \rho_I Z_{D_1} \nu_1 + Z_{SP}\upsilon_1} > \gamma_1, \rho < \frac{\rho_I}{Z_{SP}}\right)}_{A_2}\end{aligned} \quad (26)$$

$$\tau_1 = R_1 \Pr\left(\frac{\rho Z_{D_1}\Theta_1\vartheta_1}{\rho Z_{D_1}\Theta_2\vartheta_1 + \rho Z_{D_1}\nu_1 + \upsilon_1} > \gamma_1, \frac{\rho Z_E\Theta_1\vartheta_E}{\rho Z_E\Theta_2\vartheta_E + \rho Z_E\nu_E + \upsilon_E} < \gamma_1, Z_{SP} < \frac{\rho_I}{\rho}\right)$$
$$+ R_1 \Pr\left(\frac{\rho_I Z_{D_1}\Theta_1\vartheta_1}{\rho_I Z_{D_1}\Theta_2\vartheta_1 + \rho_I Z_{D_1}\nu_1 + Z_{SP}\upsilon_1} > \gamma_1, \frac{\rho_I Z_E\Theta_1\vartheta_E}{\rho_I Z_E\Theta_2\vartheta_E + \rho_I Z_E\nu_E + Z_{SP}\upsilon_E} < \gamma_1, Z_{SP} > \frac{\rho_I}{\rho}\right)$$
$$= R_1\bar{F}_{Z_{D_1}}\left(\frac{\psi_1}{\rho}\right)F_{Z_E}\left(\frac{\psi_{E,1}}{\rho}\right)F_{Z_{SP}}\left(\frac{\rho_I}{\rho}\right) + R_1\int_{\frac{\rho_I}{\rho}}^{\infty} f_{Z_{SP}}(x)\bar{F}_{Z_{D_1}}\left(\frac{\psi_1 x}{\rho_I}\right)F_{Z_E}\left(\frac{\psi_{E,1}x}{\rho_I}\right)dx. \quad (35)$$

Then, we define the first and second terms of (35) are C_1 and C_2 respectively. In particular, C_1 can be obtained as

$$C_1 = R_1\sum_{n_1=1}^{N}\binom{N}{n_1}(-1)^{n_1-1}e^{-\frac{\psi_1 n_1}{\rho\lambda_{D_1}}} \times\left(1-\sum_{n_E=1}^{N}\binom{N}{n_E}(-1)^{n_E-1}e^{-\frac{\psi_{E,1}n_E}{\rho\lambda_E}}\right) \times\left(1-\sum_{n_{SP}=1}^{N}\binom{N}{n_{SP}}(-1)^{n_{SP}-1}e^{-\frac{n_{SP}\rho_I}{\lambda_{SP}\rho}}\right). \quad (36)$$

Then, C_2 is rewritten as

$$C_2 = R_1\int_{\frac{\rho_I}{\rho}}^{\infty} f_{Z_{SP}}(x)\bar{F}_{Z_{D_1}}\left(\frac{\psi_1 x}{\rho_I}\right) - R_1\int_{\frac{\rho_I}{\rho}}^{\infty} f_{Z_{SP}}(x)\bar{F}_{Z_{D_1}}\left(\frac{\psi_1 x}{\rho_I}\right)\bar{F}_{Z_E}\left(\frac{\psi_{E,1}x}{\rho_I}\right)dx. \quad (37)$$

The closed-form of C_2 is calculated as

$$C_2 = R_1\sum_{n_1=1}^{N}\sum_{n_{SP}=1}^{N}\binom{N}{n_1}\binom{N}{n_{SP}}(-1)^{n_1+n_{SP}-2} \times\frac{n_{SP}\rho_I\lambda_{D_1}}{\psi_1 n_1\lambda_{SP}+\rho_I\lambda_{D_1}n_{SP}}e^{-\frac{\psi_1 n_1\lambda_{SP}+\rho_I\lambda_{D_1}n_{SP}}{\rho\lambda_{D_1}\lambda_{SP}}}$$
$$- R_1\sum_{n_1=1}^{N}\sum_{n_E=1}^{N}\sum_{n_{SP}=1}^{N}\binom{N}{n_{SP}}\binom{N}{n_E}\binom{N}{n_1} \times\frac{(-1)^{n_E+n_1+n_{SP}-3}n_{SP}\lambda_E\lambda_{D_1}\rho_I}{n_1\psi_1\lambda_{SP}\lambda_E+\lambda_{D_1}\lambda_{SP}n_E\psi_{E,1}+\lambda_{D_1}\lambda_E\rho_I n_{SP}} \times e^{-\frac{n_1\psi_1\lambda_{SP}\lambda_E+\lambda_{D_1}\lambda_{SP}n_E\psi_{E,1}+\lambda_{D_1}\lambda_E\rho_I n_{SP}}{\lambda_{D_1}\rho}} \quad (38)$$

Putting (36) and (38) into (35). It completes the proof. Similar proof as τ_1, τ_2 can be obtained as (25).

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[2] Y. Feng, Z. Yang, S. Yan, N. Yang, and B. Lv, "Physical layer security enhancement in multi-user multi-full-duplex-relay networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–7.
[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[4] 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 Trans. Commun.*, vol. 67, no. 1, pp. 83–96, Jan. 2019.
[5] 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.
[6] T. L. Nguyen, T.-L. Nguyen, V. V. Nguyen, and T. T. Phu, "Outage performance of full-duplex unmanned aerial vehicle-aided cooperative non-orthogonal multiple access," *Adv. Electr. Electron. Eng.*, vol. 21, no. 1, pp. 1–8, May 2023.
[7] A.-T. Le, N. X. Ha, D.-T. Do, S. Yadav, and B. M. Lee, "Enabling NOMA in overlay spectrum sharing in hybrid satellite-terrestrial systems," *IEEE Access*, vol. 9, pp. 56616–56629, 2021.
[8] N.-T. Nguyen, H.-N. Nguyen, N.-L. Nguyen, A.-T. Le, T. N. Nguyen, and M. Voznak, "Performance analysis of NOMA-based hybrid satellite-terrestrial relay system using mmWave technology," *IEEE Access*, vol. 11, pp. 10696–10707, 2023.
[9] M. Jiang, Y. Li, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MIMO nonorthogonal multiple access networks," *IEEE Signal Process. Lett.*, vol. 24, no. 12, pp. 1852–1856, Dec. 2017.
[10] Z. Wang and Z. Peng, "Secrecy performance analysis of relay selection in cooperative NOMA systems," *IEEE Access*, vol. 7, pp. 86274–86287, 2019.
[11] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
[12] 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 Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[13] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.
[14] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.
[15] D.-T. Do, A.-T. Le, Y. Liu, and A. Jamalipour, "User grouping and energy harvesting in UAV-NOMA system with AF/DF relaying," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11855–11868, Nov. 2021.
[16] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.
[17] W. Xie, J. Liao, C. Yu, P. Zhu, and X. Liu, "Physical layer security performance analysis of the FD-based NOMA-VC system," *IEEE Access*, vol. 7, pp. 115568–115573, 2019.
[18] R. M. Christopher and D. K. Borah, "Physical layer security for weak user in MISO NOMA using directional modulation (NOMAD)," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 956–960, May 2020.

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

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

[21] D.-T. Do, A.-T. Le, and B. M. Lee, "NOMA in cooperative underlay cognitive radio networks under imperfect SIC," *IEEE Access*, vol. 8, pp. 86180–86195, 2020.

[22] X. Zhang, D. Guo, K. An, Z. Chen, B. Zhao, Y. Ni, and B. Zhang, "Performance analysis of NOMA-based cooperative spectrum sharing in hybrid satellite-terrestrial networks," *IEEE Access*, vol. 7, pp. 172321–172329, 2019.

[23] B. Chen, Y. Chen, Y. Chen, Y. Cao, N. Zhao, and Z. Ding, "A novel spectrum sharing scheme assisted by secondary NOMA relay," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 732–735, Oct. 2018.

[24] L. Lv, Q. Ni, Z. Ding, and J. Chen, "Application of non-orthogonal multiple access in cooperative spectrum-sharing networks over Nakagami-*m* fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5506–5511, Jun. 2017.

[25] S. Arzykulov, G. Nauryzbayev, T. A. Tsiftsis, and B. Maham, "Performance analysis of underlay cognitive radio nonorthogonal multiple access networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9318–9322, Sep. 2019.

[26] Y. Zhang, Q. Yang, T.-X. Zheng, H.-M. Wang, Y. Ju, and Y. Meng, "Energy efficiency optimization in cognitive radio inspired non-orthogonal multiple access," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.

[27] S. Arzykulov, T. A. Tsiftsis, G. Nauryzbayev, M. Abdallah, and G. Yang, "Outage performance of underlay CR-NOMA networks with detect-and-forward relaying," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

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

[29] 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.

[30] 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.

[31] S. Bhattacharjee, "Friendly jamming assisted secure cooperative multicasting in cognitive radio-NOMA networks," in *Proc. IEEE Globecom Workshops*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[32] D. Wang and S. Men, "Secure energy efficiency for NOMA based cognitive radio networks with nonlinear energy harvesting," *IEEE Access*, vol. 6, pp. 62707–62716, 2018.

[33] X. Li, M. Liu, C. Deng, P. T. Mathiopoulos, Z. Ding, and Y. Liu, "Full-duplex cooperative NOMA relaying systems with I/Q imbalance and imperfect SIC," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 17–20, Jan. 2020.

[34] X. Li, M. Zhao, X.-C. Gao, L. Li, D.-T. Do, K. M. Rabie, and R. Kharel, "Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance," *IEEE Access*, vol. 8, pp. 51189–51199, 2020.

[35] D.-T. Do and A.-T. Le, "NOMA based cognitive relaying: Transceiver hardware impairments, relay selection policies and outage performance comparison," *Comput. Commun.*, vol. 146, pp. 144–154, Jan. 2019.

[36] H. Lei, R. Gao, K.-H. Park, I. S. Ansari, K. J. Kim, and M.-S. Alouini, "On secure downlink NOMA systems with outage constraint," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7824–7836, Dec. 2020.

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

[38] 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.

[39] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 210–222, 2020.

[40] Z. Xiang, W. Yang, G. Pan, Y. Cai, and X. Sun, "Secure transmission in non-orthogonal multiple access networks with an untrusted relay," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 905–908, Jun. 2019.

[41] T. Schenk, *RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation*. Cham, Switzerland: Springer, 2008.

[42] T. P. Huynh, P. N. Son, and M. Voznak, "Exact throughput analyses of energy-harvesting cooperation scheme with best relay selections under I/Q imbalance," *Adv. Electr. Electron. Eng.*, vol. 15, no. 4, pp. 290–585, Nov. 2017.

[43] J. Qi, S. Aïssa, and M.-S. Alouini, "Impact of I/Q imbalance on the performance of two-way CSI-assisted AF relaying," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 2507–2512.

[44] 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, 2019.

[45] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.

[46] H. A. David and H. N. Nagaraja, *Order Statistics*, 3rd ed. New York, NY, USA: Wiley, 2003.

HUNG NGUYEN was born in Vietnam. He received the B.S. and M.S. degrees from the Electrical and Electronics Engineering Department, Ho Chi Minh City University of Technology (HCMUT), Vietnam, in 2000 and 2004, respectively, and the Ph.D. degree from Pukyong National University, South Korea, in 2010. He is currently an Associate Professor with the HUTECH Institute of Engineering, HUTECH University, Vietnam. His research interests include robust and nonlinear control, the control and stability of power systems, the IoT, and AI applications in energy systems. He has published many articles that are indexed in the WoS and Scopus databases. In addition, he has served as a reviewer for numerous international journals and conferences.

TAN N. NGUYEN (Member, IEEE) was born in Nha Trang, Vietnam, in 1986. He received the B.S. degree in electronics from the Ho Chi Minh University of Natural Sciences, in 2008, the M.S. degree in telecommunications engineering from Vietnam National University, in 2012, and the Ph.D. degree in communications technologies from the Faculty of Electrical Engineering and Computer Science, VSB—Technical University of Ostrava, Czech Republic, in 2019. He joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam, in 2013, and since then, he has been lecturing. He was the Editor-in-Chief of *Advances in Electrical and Electronic Engineering* (AEEE) journal, in 2023. His major research interests include cooperative communications, cognitive radio, signal processing, satellite communication, UAV, and physical layer security.

BUI VU MINH was born in Dong Nai, Vietnam, in March 1991. He received the Graduate degree in electrical and electronic engineering from Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam, in 2015, and the master's degree in electrical engineering from the Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, in 2019. In 2014, he joined the Faculty of Engineering and Technology, Nguyen Tat Thanh University, as a Laboratory-Practice Management, and until 2017, he was a Lecturer. His major research interests include wireless networks, robot, artificial neural networks, and power electronics.

THU-HA THI PHAM was born in Ha Tinh City, Vietnam, in 2003. She is currently pursuing the B.S. degree in electronics and telecommunications engineering with Ton Duc Thang University, Vietnam. Her current research interests include non-orthogonal multiple access (NOMA), energy harvesting, full-duplex, physical layer security, and reconfigurable intelligent surface (RIS).

ANH-TU LE (Member, IEEE) was born in Lam Dong, Vietnam, in 1997. He received the B.S. degree from the Industrial University of Ho Chi Minh City, Vietnam, in 2019, and the M.S. degree from Ton Duc Thang University, Vietnam, in 2022. He is currently pursuing the Ph.D. degree in communication technology with the VSB—Technical University of Ostrava, Czech Republic. He has authored and coauthored over 25 ISI-indexed journals. His research interests include wireless channel modeling, NOMA, cognitive radio, MIMO, and machine learning.

MIROSLAV VOZNAK (Senior Member, IEEE) received the Ph.D. degree in telecommunications from the Faculty of Electrical Engineering and Computer Science, VSB—Technical University of Ostrava, and the Habilitation degree, in 2009. He was appointed as a full professor in electronics and communications technologies, in 2017. He is a Principal Investigator in the research project QUANTUM5 funded by NATO, which focuses on the application of quantum cryptography in 5G campus networks. He participated in six projects funded by the EU in programs managed directly by European Commission. He has authored and coauthored more than 100 articles in SCI/SCIE journals. His research interests include ICT, especially on the quality of service and experience, network security, wireless networks, and big data analytics. According to the Stanford University study released, in 2020, he is one of the World's Top 2% of Scientists in networking and telecommunications, and information and communications technologies. He has served as the General Chair for the 11th IFIP Wireless and Mobile Networking Conference, in 2018, and the 24th IEEE/ACM International Symposium on Distributed Simulation and Real-Time Applications, in 2020.