Physical Layer Security of Overlay Cognitive NOMA Systems with Control-Jamming

Kajal Yadav[1], Prabhat K. Upadhyay[1,2], Janne Lehtomäki[2], and Jules M. Moualeu[3]
[1]Department of Electrical Engineering, Indian Institute of Technology Indore, Indore 453552, Madhya Pradesh, India
[2]Centre for Wireless Communications (CWC), University of Oulu, 90014 Oulu, Finland
[3]School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, 2000, South Africa
Email: mtphd2206102001@iiti.ac.in, pkupadhyay@iiti.ac.in, janne.lehtomaki@oulu.fi, jules.moualeu@wits.ac.za

***Abstract*—In this paper, we investigate the physical layer security (PLS) of an overlay cognitive non-orthogonal multiple access (NOMA) system with control-jamming (CJ) under Nakagami-*m* fading. Herein, a cooperative decode-and-forward (DF) relaying technique is adopted at the secondary transmitter, while a maximal ratio combining (MRC) scheme is employed at the primary destination in order to improve the secrecy performance of the underlying system. Under this setup, we derive analytical expressions for the secrecy outage probability (SOP) and the strictly positive secrecy capacity (SPSC). Moreover, we obtain simple and explicit expressions of the SOP in the high signal-to-noise ratio (SNR) region to get useful insights on the system design for both the cases of without and with jamming. Finally, Monte Carlo simulations are provided to: (i) demonstrate the effectiveness and superiority of the proposed system with jamming over its non-jamming counterpart in terms of security; (ii) verify the accuracy of the proposed analytical framework.**

***Index Terms*—Cognitive radio, control-jamming, decode-and-forward, non-orthogonal multiple access (NOMA), physical layer security, maximal ratio combining.**

I. Introduction

The development of high-rate data communication services coupled with the explosive growth of mobile traffic have led to the spectrum scarcity problem for future wireless technologies, i.e., fifth-generation (5G) and beyond. Non-orthogonal multiple access (NOMA) and cognitive radio (CR) are two concepts that have been envisioned as promising candidates to improve spectrum efficiency in future wireless networks. Recent studies have investigated the integration of NOMA with CR termed as cognitive NOMA (CNOMA), and have demonstrated the potential to achieve the criteria for 5G and beyond networks such as massive connectivity, low latency and high throughput (see [1]–[3] and the references therein).

Numerous works based on CNOMA have been reported in the literature since they provide many advantages such as highly efficient spectrum utilization, massive connectivity, low latency and high throughput (e.g., [4]–[7] and the references therein). The authors in [5] investigated a CNOMA model wherein they compared the performance of fixed-power-allocation NOMA and the proposed CNOMA. In that model, a primary user (PU) is the weak user who experiences poor channel conditions and has a higher priority while the secondary user (SU) experiences good channel conditions with lower priority, and the target reception quality for PU is guaranteed. In [6], the authors studied a two-user underlay CNOMA system in which, a relay transmits information to a far user, while at the same time, the base station (BS) transmits information to a near user. In [7], Lv *et al.* considered an overlay CNOMA system wherein a secondary transmitter serves as a relay using the NOMA principle. To this end, the secondary transmitter helps with the simultaneous transmissions of both the primary and secondary messages. However, works in [4]–[7] have some commonality in that they do not address the security and privacy issues which are crucial for such networks due to the broadcast nature of the wireless medium and/or the sharing of the same resource block among multiple users.

Traditionally, the protection of information in wireless networks has been done through cryptography. However, this may not be viable in terms of meeting the security needs of wireless communications with the development of high-performance computing. In light of this, physical layer security (PLS) has recently emerged as a promising and effective solution to address the risk of information leakage in future wireless communication systems by guaranteeing security from an information-theoretic perspective [8]. To fulfill some criteria of 5G networks such as spectrum efficiency and security, authors in [9]–[12] studied the performance of PLS-based CNOMA systems. However, the above-mentioned works considered the underlay paradigm of the CR technology which is very restrictive in terms of the transmit power at the unlicensed user(s). Conversely, such stringent restrictions do not prevail in the overlay paradigm. To the best of our knowledge, there is a paucity of works on the secrecy performance of the overlay CNOMA systems (see [13], [14]). In [13], the authors highlighted that the overlay approach enhances the performance of both the primary and secondary users simultaneously at the expense of security breaches. Authors in [14] studied the secrecy performance of an overlay cognitive ambient backscatter communication NOMA system in the presence of an eavesdropper. However, the impact of a control-jamming (CJ) mechanism is not investigated in these works. While some recent works [15]- [17] have considered jammer-assisted secure communication techniques, they are focused on the conventional NOMA system without spectrum sharing. The authors in [15] described a jammer-based downlink NOMA system with half-duplex (HD) decode-and-forward (DF) relaying in the absence of direct links between source and end users. In [16], authors took into account a network architecture

in which a source uses the NOMA technique to interact with two destination users in the presence of an eavesdropper and a friendly jammer. In [17], a HD-DF relay was employed in a downlink NOMA network and jamming signals were exploited to disrupt the eavesdropping. As such, these works did not exploit the CR model with NOMA system. In fact, the performance of PLS in overlay CNOMA networks is still in its infancy and vastly remains unexplored in many ways.

Motivated by the above consideration, we propose a CJ-aided overlay CNOMA system and illustrate the importance of jamming on the secrecy performance of the overall system. It is noteworthy that there has been no work in the literature that have considered direct link as well as relay link and adopted the maximal ratio combining (MRC) technique to obtain the SOP in a jammer-aided CNOMA system where the eavesdropper has multiuser detection capability. To analyze the proposed system secrecy performance, we first derive expressions of the signal-to-interference-plus-noise ratios (SINRs) for the NOMA users which are subsequently used to obtain closed-form expressions for the SOP and the strictly positive secrecy capacity (SPSC). Based on the derived SOP expressions for the jamming and non-jamming cases, we showcase that the former helps improve the underlying secrecy performance. Moreover, to get useful insights on the system design, we derive simple and explicit expressions of the SOP at high signal-to-noise ratio (SNR) for both the jamming and non-jamming cases. Finally, Monte Carlo simulations are provided to demonstrate the effectiveness of the proposed system with jamming and to validate the accuracy of the proposed theoretical framework.

The rest of the paper is organized as follows. Section II presents the model of the proposed system, followed by the analysis of the secrecy performance metrics in Section III. Numerical results are provided in Section IV, and the concluding remarks are discussed in Section V.

II. System Model and Description

A. System Model

As depicted in Fig. 1, we consider an overlay CNOMA system which consists of the primary and secondary networks. In the primary network, the primary transmitter (S) aims to communicate with the primary receiver (D). The secondary network consists of a secondary transmitter (R), which plays the role of a relay for S in exchange for its spectrum access, as well as a secondary receiver (Q), an eavesdropper (E) and a jamming node (J). Given that there is a direct link between S and D as well as a relay link between R and D, the MRC approach is adopted by D to combine the information from S and R. The jamming node aims at confounding the eavesdropper node which tries to overhear the information sent by R. In this case, E has a multiuser detection capability and can distinguish the superimposed mixture of signals.

It is assumed that all the nodes in the network are operating in HD mode and relay node R employs the DF strategy. The direct link between S and D exists but it is blocked between S and Q or E due to shadowing or large separation. We assume that all the channels experience independent Nakagami-m block fading. We denote the channel coefficient between node i and node j as h_{ij}, where $i \in \{\mathrm{S},\mathrm{R},\mathrm{J}\}$, $j \in \{\mathrm{R},\mathrm{D},\mathrm{Q},\mathrm{E}\}$, with $i \neq j$. The channel gain $|h_{ij}|^2$ follows the gamma distribution with fading severity parameter m_{ij} and average fading power Ω_{ij}. Zero mean additive white Gaussian noise (AWGN) with variance N_0 is assumed at all the receiving nodes. We also assume that the entire communication takes place in two consecutive transmission phases, denoted by t_1 and t_2.

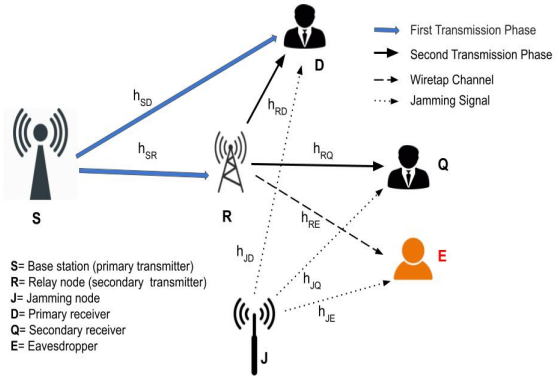

Fig. 1: System model.

B. First Transmission Phase

In the first transmission phase (t_1), node S transmits a unit-power signal x_S. The received signals at the nodes D and R are given by

$$y_i^{t_1} = h_{\mathrm{S}i}\sqrt{P_\mathrm{S}}x_\mathrm{S} + n_i,\ i \in \{\mathrm{D},\mathrm{R}\}, \tag{1}$$

where P_S denotes the transmit power at S and n_i represents the AWGN variable. Hence, the SNR for decoding x_S at R can be written as $\gamma_R = \Delta_\mathrm{S}|h_{\mathrm{SR}}|^2$, where $\Delta_\mathrm{S} \triangleq \frac{P_\mathrm{S}}{N_0}$ represents the transmit SNR for node S. Using the received signal at D, the resulting SNR for decoding x_S can be written as $\gamma_D^{t_1} = \Delta_\mathrm{S}|h_{\mathrm{SD}}|^2$.

C. Second Transmission Phase

During the second transmission phase (t_2), node R first tries to decode the primary signal x_S. After successful decoding of signal x_S, it applies NOMA technique to combine its own signal x_R with x_S. As such, the combined signal z_R is given by

$$z_\mathrm{R} = \sqrt{P_\mathrm{R}a_1}x_\mathrm{S} + \sqrt{P_\mathrm{R}a_2}x_\mathrm{R}, \tag{2}$$

where a_1 and a_2 are the power allocation coefficients for x_S and x_R, respectively, with $a_1 + a_2 = 1$ and $a_1 \geq a_2$ in anticipation to the priority given to primary communication over the secondary communication. The signals received at D and Q are given by

$$y_i^{t_2} = h_{\mathrm{R}i}z_\mathrm{R} + n_i = h_{\mathrm{R}i}(\sqrt{P_\mathrm{R}a_1}x_s + \sqrt{P_\mathrm{R}a_2}x_\mathrm{R}) + n_i, \tag{3}$$

where P_R denotes the transmit power at R and n_i represents the AWGN variable, with $i \in \{\mathrm{D},\mathrm{Q}\}$. The message signal x_S is decoded at D directly from the received signal. So, the SINR

corresponding to the decoding of $x_{\rm S}$ at D is given by $\gamma_{\rm D}^{t_2} = \frac{\chi}{\psi}$, where $\chi = \Delta_{\rm R}|h_{\rm RD}|^2 a_1$, $\psi = \Delta_{\rm R}|h_{\rm RD}|^2 a_2 + 1$, with $\Delta_{\rm R} \triangleq \frac{P_{\rm R}}{N_0}$ representing the transmit SNR at node R. The signals from the relaying link and direct link are combined by using the MRC at D. Consequently, the received SINR after the MRC scheme at D is given by $\gamma_{\rm D} = \gamma_{\rm D}^{t_1} + \gamma_{\rm D}^{t_2}$.

From the received signal $y_{\rm Q}^{t_2}$, Q decodes $x_{\rm S}$ first and then applies successive interference cancellation (SIC) to decode $x_{\rm R}$ as per the NOMA principle. It is assumed that perfect SIC is employed at Q. After SIC, the SINR at Q to detect its own message $x_{\rm R}$ is given by $\gamma_{\rm Q}^{\rm R} = \Delta_{\rm R}|h_{\rm RQ}|^2 a_2$. Similar to [18], we also assume E has multiuser detection capability, which represents the worst-case scenario from a security perspective, and applies parallel interference cancellation (PIC) approach to differentiate the superimposed mixture of signals. In what follows, we review two cases, i.e., *without jammer* and *with jammer*.

1) Without Jammer Case: In this case, the eavesdropper tries to wiretap the data from R. The received signal at E is given by

$$y_{\rm RE} = h_{\rm RE}(\sqrt{P_{\rm R} a_1} x_{\rm S} + \sqrt{P_{\rm R} a_2} x_{\rm R}) + n_{\rm E}, \tag{4}$$

where $n_{\rm E}$ is the AWGN variable at node E. The received SINRs at E for detecting the message symbols of user D and Q are given respectively by $\gamma_{\rm E}^{\rm S} = \Delta_{\rm R}|h_{\rm RE}|^2 a_1$ and $\gamma_{\rm E}^{\rm R} = \Delta_{\rm R}|h_{\rm RE}|^2 a_2$.

2) With Jammer Case: Here, an intended interference signal $x_{\rm J}$ is transmitted by the jammer to confound the eavesdropper. The received signal at E is given by

$$y_{\rm E} = h_{\rm RE}(\sqrt{P_{\rm R} a_1} x_{\rm S} + \sqrt{P_{\rm R} a_2} x_{\rm R}) + h_{\rm JE}\sqrt{P_{\rm J}} x_{\rm J} + n_{\rm E}, \tag{5}$$

where $P_{\rm J}$ is the transmit power at node J. The received SINRs at E for detecting the message symbols of user D and Q can be expressed respectively as $\gamma_{\rm EJ}^{\rm S} = \frac{\zeta}{\varepsilon}$ and $\gamma_{\rm EJ}^{\rm R} = \frac{\varrho}{\varepsilon}$, where $\zeta = \Delta_{\rm R}|h_{\rm RE}|^2 a_1$, $\varepsilon = \Delta_{\rm J}|h_{\rm JE}|^2 + 1$, $\varrho = \Delta_{\rm R}|h_{\rm RE}|^2 a_2$, and $\Delta_{\rm J} \triangleq \frac{P_{\rm J}}{N_0}$ represents the transmit SNR at node J.

Here, we have assumed that this interference signal $x_{\rm J}$ is not affecting the SNRs at users D and Q. This is because both the NOMA users already have the information about jamming signal.

III. Secrecy Performance Analysis

A. SOP Analysis

The SOP is defined as the probability that the secrecy capacity of a user is below a predefined threshold R_{th} [19]. In NOMA-based networks, a superimposed signal is transmitted to users D and Q. Hence, an outage event occurs when the achievable maximum secrecy capacity of any of the two users does not achieve the given threshold rate [20]. To this end, the SOP can mathematically be expressed as $P_{\rm out}^{\rm SOP} = \Pr\big[C_{\rm D} < R_{th}$ or $C_{\rm Q} < R_{th}]$, where $C_{\rm D}$ and $C_{\rm Q}$ are the instantaneous secrecy capacities at users D and Q, respectively [21].

Since R uses the DF protocol, the secrecy capacities of $x_{\rm S}$ and $x_{\rm R}$ over the legitimate channels are given by $C_{\rm S} = \frac{1}{2}\log_2\left(1 + \min\{\gamma_{\rm R}, \gamma_{\rm D}\}\right)$ and $C_{\rm R} = \frac{1}{2}\log_2\left(1 + \gamma_{\rm Q}^{\rm R}\right)$, respectively.

1) Without Jammer Case: The secrecy capacities of $x_{\rm S}$ and $x_{\rm R}$ over the eavesdropping channels are given by $C_{{\rm E}-i} = \frac{1}{2}\log_2\left(1 + \gamma_{\rm E}^{i}\right)$, with $i \in \{{\rm S}, {\rm R}\}$. Using the secrecy capacities $C_{\rm S}$, $C_{\rm R}$ and $C_{{\rm E}-i}$ as defined above, we can write achievable secrecy capacities for users D and Q as $C_{\rm D} = \left[C_{\rm S} - C_{\rm E-S}\right]^+$ and $C_{\rm Q} = \left[C_{\rm R} - C_{\rm E-R}\right]^+$, respectively, with $[x]^+ = \max\{0, x\}$. Now, the SOP expression of the proposed scheme can be formulated as

$$P_{\rm out,WJ}^{\rm SOP} = 1 - \underbrace{\Pr\left[\frac{1 + \min\{\gamma_{\rm R}, \gamma_{\rm D}\}}{1 + \gamma_{\rm E}^{\rm S}} > C_{th}, \frac{1 + \gamma_{\rm Q}^{\rm R}}{1 + \gamma_{\rm E}^{\rm R}} > C_{th}\right]}_{P_1}, \tag{6}$$

where $C_{th} = 2^{2R_{th}}$. On further simplification, P_1 is given by

$$P_1 = \Pr[\gamma_{\rm R} > \alpha, \gamma_{\rm D} > \alpha, \gamma_{\rm Q}^{\rm R} > \beta], \tag{7}$$

where $\alpha = (C_{th} - 1) + C_{th}\gamma_{\rm E}^{\rm S}$ and $\beta = (C_{th} - 1) + C_{th}\gamma_{\rm E}^{\rm R}$.

The evaluation of (7) in closed form is an intricate task. In what follows, we adopt an upper bound approach as $\gamma_{\rm D} < \Delta_{\rm S}|h_{\rm SD}|^2 + \frac{a_1}{a_2}$ for the high SNR values. Therefore, the upper bound of P_1 in (7) is given by

$$P_1 < \Pr[|h_{\rm RQ}|^2 > \mathcal{A}|h_{\rm RE}|^2 + \mathcal{B}, |h_{\rm SR}|^2 > \mathcal{C}|h_{\rm RE}|^2 + \mathcal{D}, |h_{\rm SD}|^2 > \mathcal{E}|h_{\rm RE}|^2 + \mathcal{F}], \tag{8}$$

where $\mathcal{A} = C_{th}$, $\mathcal{B} = \frac{C_{th}-1}{\Delta_{\rm R} a_2}$, $\mathcal{C} = \frac{C_{th} a_1 \Delta_{\rm R}}{\Delta_{\rm S}}$, $\mathcal{D} = \frac{C_{th}-1}{\Delta_s}$, $\mathcal{E} = \frac{C_{th} a_1 \Delta_{\rm R}}{\Delta_{\rm S}}$ and $\mathcal{F} = \frac{C_{th}-1-\frac{a_1}{a_2}}{\Delta_{\rm S}}$. We can further evaluate P_1 as

$$P_1 < \int_0^\infty \left[1 - F_{|h_{\rm RQ}|^2}(\mathcal{A}x + \mathcal{B})\right]\left[1 - F_{|h_{\rm SR}|^2}(\mathcal{C}x + \mathcal{D})\right] \times \left[1 - F_{|h_{\rm SD}|^2}(\mathcal{E}x + \mathcal{F})\right] f_{|h_{\rm RE}|^2}(x)dx. \tag{9}$$

After substituting the cumulative distribution function (CDF) of $|h_{ij}|^2$ using [22, Eq. (6)] into the second term of the integrand of (9), and with the aid of [23, Eq. (3.351.1)], we get

$$1 - F_{|h_{\rm SR}|^2}(\mathcal{C}x + \mathcal{D}) = e^{-\frac{m_{\rm SR}}{\Omega_{\rm SR}}(\mathcal{C}x + \mathcal{D})} \times \sum_{k=0}^{m_{\rm SR}-1} \left(\frac{m_{\rm SR}}{\Omega_{\rm SR}}\right)^k \frac{1}{k!}(\mathcal{C}x + \mathcal{D})^k. \tag{10}$$

Using the same approach as in (10), the final expression of P_1 can be obtained as

$$P_1 < \frac{k_1 k_2 k_3}{\Gamma(m_{\rm RE})}\left(\frac{m_{\rm RE}}{\Omega_{\rm RE}}\right)^{m_{\rm RE}} (\delta - 1)! \left(\frac{m_{\rm RE}}{\Omega_{\rm RE}} + \mathcal{H}_1\right)^{-\delta}, \tag{11}$$

where k_1, k_2 and k_3 are given respectively by

$$k_1 = e^{-\frac{m_{\rm SR}}{\Omega_{\rm SR}}\mathcal{D}} \sum_{k=0}^{m_{\rm SR}-1} \left(\frac{m_{\rm SR}}{\Omega_{\rm SR}}\right)^k \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} \mathcal{D}^{k-i}\mathcal{C}^i, \tag{12}$$

$$k_2 = e^{-\frac{m_{\rm SD}}{\Omega_{\rm SD}}\mathcal{F}} \sum_{l=0}^{m_{\rm SD}-1} \left(\frac{m_{\rm SD}}{\Omega_{\rm SD}}\right)^l \frac{1}{l!} \sum_{j=0}^{l} \binom{l}{j} \mathcal{F}^{l-j}\mathcal{E}^j, \tag{13}$$

$$k_3 = e^{-\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\mathcal{B}} \sum_{M=0}^{m_{\mathrm{RQ}}-1} \left(\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\right)^{M} \frac{1}{M!} \sum_{n=0}^{M} \binom{M}{n} \mathcal{B}^{M-n} \mathcal{A}^{n}, \tag{14}$$

with $\mathcal{H}_1 = \mathcal{C}\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}} + \mathcal{E}\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}} + \mathcal{A}\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}$ and $\delta = i + j + n + m_{\mathrm{RE}}$.

Finally, the SOP expression of the proposed system without jamming is obtained by substituting (11) into (6).

2) With Jammer Case: In the jammer case, the secrecy capacities of x_{S} and x_{R} over the eavesdropping channels are given by $C^{\mathrm{J}}_{\mathrm{E}-i} = \frac{1}{2}\log_2\left(1+\gamma^{i}_{\mathrm{EJ}}\right)$, with $i \in \{\mathrm{S},\mathrm{R}\}$. Using the secrecy rates C_{S}, C_{R} and $C^{\mathrm{J}}_{\mathrm{E}-i}$, we can write achievable secrecy capacities for users D and Q in case of jamming as $C_{\mathrm{D}} = \left[C_{\mathrm{S}} - C^{\mathrm{J}}_{\mathrm{E-S}}\right]^{+}$ and $C_{\mathrm{Q}} = \left[C_{\mathrm{R}} - C^{\mathrm{J}}_{\mathrm{E-R}}\right]^{+}$, respectively, with $[x]^{+} = \max\{0, x\}$.

Using the received SINRs $\gamma^{\mathrm{S}}_{\mathrm{EJ}}$ and $\gamma^{\mathrm{R}}_{\mathrm{EJ}}$ defined after (5), together with $C^{\mathrm{J}}_{\mathrm{E}-i}$, C_{D} and C_{Q}, we can formulate the SOP expression as

$$P^{\mathrm{SOP}}_{\mathrm{out,J}} = 1 - \underbrace{\Pr\left[\frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}}{1+\gamma^{\mathrm{S}}_{\mathrm{EJ}}} > C_{th}, \frac{1+\gamma^{\mathrm{R}}_{\mathrm{Q}}}{1+\gamma^{\mathrm{R}}_{\mathrm{EJ}}} > C_{th}\right]}_{P_2}, \tag{15}$$

where $C_{th} = 2^{2R_{th}}$. We can further evaluate P_2 in (15) as

$$P_2 = \Pr\left[\gamma_{\mathrm{R}} > \alpha_{\mathrm{J}}, \gamma_{\mathrm{D}} > \alpha_{\mathrm{J}}, \gamma^{\mathrm{R}}_{\mathrm{Q}} > \beta_{\mathrm{J}}\right], \tag{16}$$

where $\alpha_{\mathrm{J}} = (C_{th}-1) + C_{th}\gamma^{\mathrm{S}}_{\mathrm{EJ}}$ and $\beta_{\mathrm{J}} = (C_{th}-1) + C_{th}\gamma^{\mathrm{R}}_{\mathrm{EJ}}$. It is worth noting that the variables $\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}$ and $\gamma^{\mathrm{R}}_{\mathrm{Q}}$ in (16) are uncorrelated. Given that evaluating P_2 in closed form is challenging, we adopt the following upper bound $\gamma_{\mathrm{D}} < \Delta_{\mathrm{S}}|h_{\mathrm{SD}}|^2 + \frac{a_1}{a_2}$, $\gamma^{\mathrm{S}}_{\mathrm{EJ}} < a_1$ and $\gamma^{\mathrm{R}}_{\mathrm{EJ}} < a_2$, and therefore, after further simplification, P_2 is given by

$$P_2 < \underbrace{\Pr\left[|h_{\mathrm{SD}}|^2 > a\right]}_{P_{21}} \underbrace{\Pr\left[|h_{\mathrm{SR}}|^2 > b\right]}_{P_{22}} \underbrace{\Pr\left[|h_{\mathrm{RQ}}|^2 > c\right]}_{P_{23}}, \tag{17}$$

where $a = \frac{\alpha_{\mathrm{J}} - \frac{a_1}{a_2}}{\Delta_{\mathrm{S}}}$, $b = \frac{\alpha_{\mathrm{J}}}{\Delta_{\mathrm{S}}}$, and $c = \frac{\beta_{\mathrm{J}}}{\Delta_{\mathrm{R}} a_2}$. We can evaluate P_{21} as

$$P_{21} = \int_{a}^{\infty} \left(\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}\right)^{m_{\mathrm{SD}}} \frac{x^{m_{\mathrm{SD}}-1}}{\Gamma(m_{\mathrm{SD}})} \mathrm{e}^{-\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}x} dx, \tag{18}$$

which, after simplification, is given by

$$P_{21} = e^{-\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}a} \sum_{k=0}^{m_{\mathrm{SD}}-1} \left(\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}\right)^{k} \frac{1}{k!} a^{k}. \tag{19}$$

Similarly, P_{22} and P_{23} are given by

$$P_{22} = e^{-\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}b} \sum_{l=0}^{m_{\mathrm{SR}}-1} \left(\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}\right)^{l} \frac{1}{l!} b^{l}, \tag{20}$$

$$P_{23} = e^{-\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}c} \sum_{n=0}^{m_{\mathrm{RQ}}-1} \left(\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\right)^{n} \frac{1}{n!} c^{n}. \tag{21}$$

Finally, after plugging (19)–(21) into (17) and subsequently the result into (15), the analytical expression of the SOP for the proposed system with jamming can be obtained.

B. SPSC Analysis

The SPSC is defined as the probability that the secrecy capacity is positive.

1) Without Jammer Case: In this scenario, the SPSC is obtained by keeping $R_{th} = 0$ to yield

$$\begin{aligned} SPSC_{\mathrm{WJ}} &= \Pr\left[C_{\mathrm{D}} > 0, C_{\mathrm{Q}} > 0\right] \\ &\approx \Pr\left[\gamma_{\mathrm{R}} > \gamma^{\mathrm{S}}_{\mathrm{E}}, \gamma_{\mathrm{D}} > \gamma^{\mathrm{S}}_{\mathrm{E}}, \gamma^{\mathrm{R}}_{\mathrm{Q}} > \gamma^{\mathrm{R}}_{\mathrm{E}}\right]. \end{aligned} \tag{22}$$

We can further evaluate (22) as

$$\begin{aligned} SPSC_{\mathrm{WJ}} &= \int_{0}^{\infty} \left[1 - F_{|h_{\mathrm{RQ}}|^2}(x)\right]\left[1 - F_{|h_{\mathrm{SR}}|^2}(\mathcal{T}x)\right] \\ &\quad \times \left[1 - F_{|h_{\mathrm{SD}}|^2}(\mathcal{U}x - \mathcal{V})\right] f_{|h_{\mathrm{RE}}|^2}(x) dx \\ &= \frac{q_1 q_2 q_3}{\Gamma(m_{\mathrm{RE}})} \left(\frac{m_{\mathrm{RE}}}{\Omega_{\mathrm{RE}}}\right)^{m_{\mathrm{RE}}} (\nu-1)! \left(\frac{m_{\mathrm{RE}}}{\Omega_{\mathrm{RE}}} + \mathcal{H}_2\right)^{-\nu}, \end{aligned} \tag{23}$$

where $\mathcal{T} = \frac{\Delta_{\mathrm{R}} a_1}{\Delta_{\mathrm{S}}}$, $\mathcal{U} = \mathcal{T}$, $\mathcal{V} = \frac{a_1}{a_2 \Delta_{\mathrm{S}}}$ and q_1, q_2 and q_3 are given by

$$q_1 = \sum_{k=0}^{m_{\mathrm{SR}}-1} \left(\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}\right)^{k} \frac{1}{k!} \mathcal{T}^{k}, \tag{24}$$

$$q_2 = e^{\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}\mathcal{V}} \sum_{l=0}^{m_{\mathrm{SD}}-1} \left(\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}\right)^{l} \frac{1}{l!} \sum_{j=0}^{l} \binom{l}{j} (-\mathcal{V})^{l-j} \mathcal{U}^{j}, \tag{25}$$

$$q_3 = \sum_{n=0}^{m_{\mathrm{RQ}}-1} \left(\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\right)^{n} \frac{1}{n!}, \tag{26}$$

with $\mathcal{H}_2 = \mathcal{T}\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}} + \mathcal{U}\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}} + \frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}$ and $\nu = k + j + n + m_{\mathrm{RE}}$.

It is noted that the secrecy performance of the proposed system without jamming is dominated by the parameters of the $\mathrm{R} \to \mathrm{E}$ link.

2) With Jammer Case: In the presence of a jammer and with $R_{th} = 0$, the analytical expression of the SPSC is given by

$$\begin{aligned} SPSC_{\mathrm{J}} &= \Pr\left[C_{\mathrm{D}} > 0, C_{\mathrm{Q}} > 0\right] \\ &\approx \Pr\left[\gamma_{\mathrm{R}} > a_1, \gamma_{\mathrm{D}} > a_1, \gamma^{\mathrm{R}}_{\mathrm{Q}} > a_2\right] \\ &= \underbrace{\Pr\left[|h_{\mathrm{SD}}|^2 > z_1\right]}_{P_{31}} \underbrace{\Pr\left[|h_{\mathrm{SR}}|^2 > z_2\right]}_{P_{32}} \underbrace{\Pr\left[|h_{\mathrm{RQ}}|^2 > z_3\right]}_{P_{33}}, \end{aligned} \tag{27}$$

where $z_1 = \frac{a_1 - \frac{a_1}{a_2}}{\Delta_{\mathrm{S}}}$ and $z_2 = \frac{a_1}{\Delta_{\mathrm{S}}}$. From (27), it is evident that the value of P_{31} is always equal to 1 since the value of a_2 cannot be greater than 1. After further simplification, the expressions of P_{32} and P_{33} can be expressed as

$$P_{32} = e^{-\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}z_2} \sum_{k=0}^{m_{\mathrm{SR}}-1} \left(\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}\right)^{k} \frac{1}{k!} {z_2}^{k}, \tag{28}$$

$$P_{33} = e^{-\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\frac{1}{\Delta_{\mathrm{R}}}} \sum_{l=0}^{m_{\mathrm{RQ}}-1} \left(\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\right)^{l} \frac{1}{l!} \left(\frac{1}{\Delta_{\mathrm{R}}}\right)^{l}. \tag{29}$$

By inserting (28) and (29) into (27), we get the analytical expression of the SPSC (with jamming) as $SPSC_{\mathrm{J}} = P_{32}P_{33}$.

From this derived expression of the SPSC (with jamming) and the one in (27), it can observed that underlying secrecy performance is independent of the S $\rightarrow$ D link, but is rather governed by the parameters of the S $\rightarrow$ R link.

C. Asymptotic SOP Analysis

1) Without Jammer Case: In this work, the asymptotic SOP is calculated under the assumption that $\Delta_{\mathrm{S}} = \Delta_{\mathrm{R}} \rightarrow \infty$. Therefore, the analytical expression of the SOP in (6) can be asymptotically expressed as

$$SOP_{\mathrm{WJ}}^{\infty} = 1 - \int_0^{\infty} [1 - F_{|h_{\mathrm{RQ}}|^2}(\mathcal{A}x + \mathcal{B})][1 - F_{|h_{\mathrm{SR}}|^2}(\mathcal{C}x + \mathcal{D})] \times [1 - F_{|h_{\mathrm{SD}}|^2}(\mathcal{E}x + \mathcal{F})] f_{|h_{\mathrm{RE}}|^2}(x) dx, \quad (30)$$

and

$$F_{|h_{\mathrm{SR}}|^2}(\mathcal{C}x + \mathcal{D}) = \frac{1}{\Gamma(m_{\mathrm{SR}})} \Upsilon\left(m_{\mathrm{SR}}, \frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}(\mathcal{C}x + \mathcal{D})\right), \quad (31)$$

with $\Upsilon(\cdot, \cdot)$ being the lower incomplete Gamma function defined in [23, Eq. (8.350.1)]. With the aid of [23, Eq. (1.111)], at high SNR, (31) can be approximated as

$$F_{|h_{\mathrm{SR}}|^2}(\mathcal{C}x + \mathcal{D}) \approx \frac{1}{(m_{\mathrm{SR}})!} \left(\frac{m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}\right)^{m_{\mathrm{SR}}} \sum_{j=0}^{m_{\mathrm{SR}}} \binom{m_{\mathrm{SR}}}{j} \mathcal{D}^{m_{\mathrm{SR}}-j} \mathcal{C}^j x^j. \quad (32)$$

Using the same approach to obtain (32), the other two CDF expressions in (30) can be approximated as follows:

$$F_{|h_{\mathrm{SD}}|^2}(\mathcal{E}x + \mathcal{F}) \approx \frac{1}{(m_{\mathrm{SD}})!} \left(\frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}\right)^{m_{\mathrm{SD}}} \sum_{i=0}^{m_{\mathrm{SD}}} \binom{m_{\mathrm{SD}}}{i} \mathcal{F}^{m_{\mathrm{SD}}-i} \mathcal{E}^i x^i. \quad (33)$$

$$F_{|h_{\mathrm{RQ}}|^2}(\mathcal{A}x + \mathcal{B}) \approx \frac{1}{(m_{\mathrm{RQ}})!} \left(\frac{m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\right)^{m_{\mathrm{RQ}}} \sum_{k=0}^{m_{\mathrm{RQ}}} \binom{m_{\mathrm{RQ}}}{k} \mathcal{B}^{m_{\mathrm{RQ}}-k} \mathcal{A}^k x^k. \quad (34)$$

It is worth noting that the high-SNR approximations of the CDF expressions obtained in (32)–(34) are independent of the average SNRs Δ_{S} and Δ_{R}. Moreover, the PDF $f_{|h_{\mathrm{RE}}|^2}(x)$ does not also depend on Δ_{S} and Δ_{R}. Plugging (32)–(34) into (30) yields the asymptotic SOP expression which is independent of Δ_{S} and Δ_{R}. It is clear from the resulting expression that the SOP for this case ($SOP_{\mathrm{WJ}}^{\infty}$) is a constant term in the high-SNR regime. Therefore, we infer that in the absence of jamming, the diversity order of the considered system may reduce to zero.

2) With Jammer Case: In what follows, we approximate the SOP expression in (15) as $SOP_{\mathrm{J}}^{\infty} = 1 - P_{21}P_{22}P_{23}$, where

$$P_{21} = \Pr[|h_{\mathrm{SD}}|^2 > a] = 1 - \frac{1}{\Gamma(m_{\mathrm{SD}})} \Upsilon\left(m_{\mathrm{SD}}, \frac{m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}} a\right). \quad (35)$$

For high SNR values, P_{21} can be approximated as

$$P_{21} \approx 1 - \frac{1}{m_{\mathrm{SD}} \Gamma m_{\mathrm{SD}}} \left(\frac{a \cdot m_{\mathrm{SD}}}{\Omega_{\mathrm{SD}}}\right)^{m_{\mathrm{SD}}}. \quad (36)$$

A similar approach used to obtain (36) can be used to approximate P_{22} and P_{23} respectively as

$$P_{22} \approx 1 - \frac{1}{m_{\mathrm{SR}} \Gamma m_{\mathrm{SR}}} \left(\frac{b \cdot m_{\mathrm{SR}}}{\Omega_{\mathrm{SR}}}\right)^{m_{\mathrm{SR}}}, \quad (37)$$

$$P_{23} \approx 1 - \frac{1}{m_{\mathrm{RQ}} \Gamma m_{\mathrm{RQ}}} \left(\frac{c \cdot m_{\mathrm{RQ}}}{\Omega_{\mathrm{RQ}}}\right)^{m_{\mathrm{RQ}}}, \quad (38)$$

where a, b and c have been defined after (17). By substituting (36)–(38) into $SOP_{\mathrm{J}}^{\infty} = 1 - P_{21}P_{22}P_{23}$, the asymptotic SOP expression for the case *with jammer* is obtained. The possible diversity order (defined by the least negative exponent of Δ_{S}) of the considered system in case of jamming is provided by $\mathcal{G}_d = \min\{m_{\mathrm{SR}}, m_{\mathrm{SD}}, m_{\mathrm{RQ}}\}$ as $SOP_{\mathrm{J}}^{\infty} \propto \frac{1}{\Delta_{\mathrm{S}}^{\mathcal{G}_d}}$.

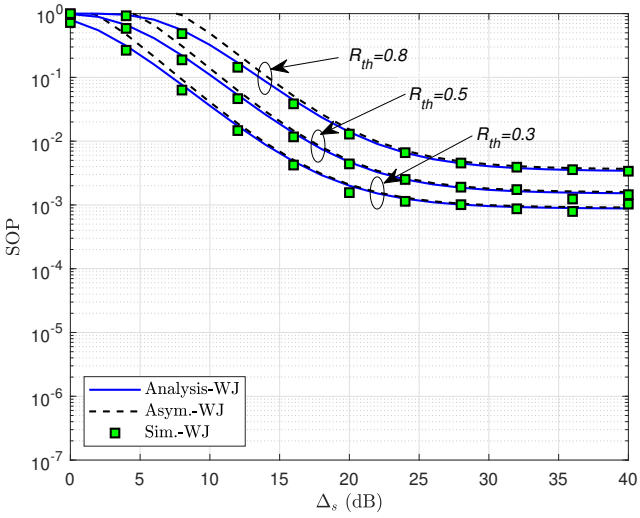

Fig. 2: SOP versus Δ_{S} for the case without jamming.

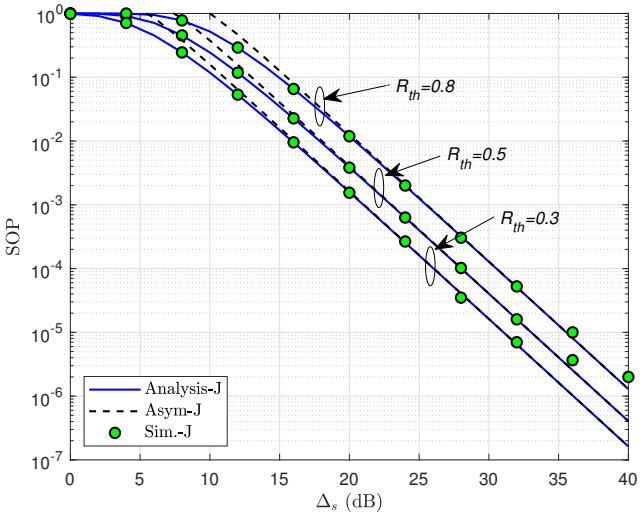

Fig. 3: SOP versus Δ_{S} for the case with jamming.

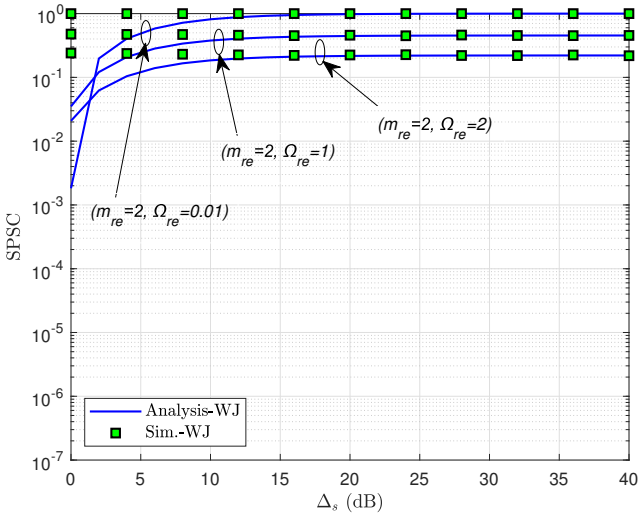

Fig. 4: SPSC versus Δ_S for the case without jamming.

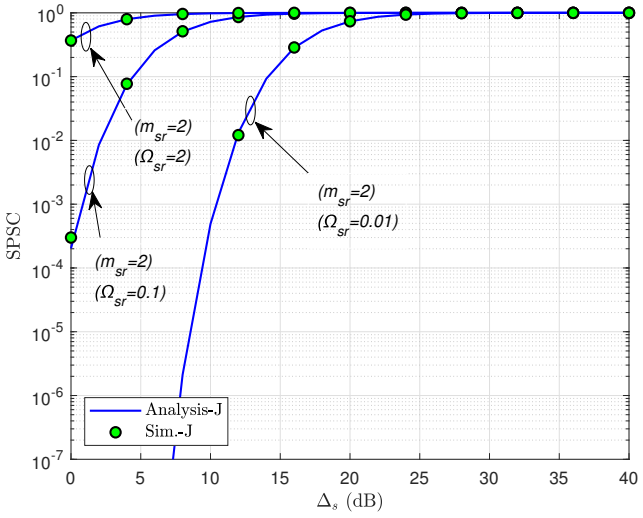

Fig. 5: SPSC versus Δ_S for the case with jamming.

IV. Numerical Analysis

In this section, we perform numerical investigations and verify the correctness of our proposed mathematical derivations. Without loss of generality, we set $\Delta_S = \Delta_R = \Delta_J$, $m_{SR} = m_{SD} = m_{RQ} = m_{RE} = 2$, $\Omega_{SR} = 1, \Omega_{SD} = 2, \Omega_{RQ} = 1$ and $\Omega_{RE} = 0.01$. In all the figures, it can be observed that there is a good agreement between the analytical and simulated results which validates the proposed analytical framework.

In Fig. 2 (without jamming) and Fig. 3 (with jamming), it can be seen that as R_{th} increases, the SOP performance degrades. This behavior comes from the fact that the occurrence of an outage event increases with R_{th}. Moreover, the behavior of the SOP in the high-SNR region for both the jamming and without jamming scenarios is consistent with our derivations, i.e., a diversity gain $\mathcal{G}_d = 2$ and $\mathcal{G}_d = 0$, respectively. The diversity gain in Fig. 3 can be explained by the fact that at high SNR, jamming suppresses the deleterious effect, unlike in Fig. 2 leading to an error floor.

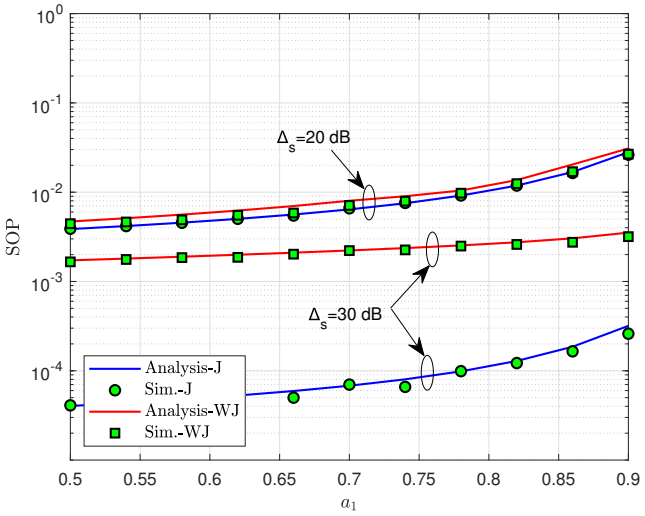

Fig. 6: SOP versus a_1 for both jamming and without jamming cases.

Fig. 4 and Fig. 5 exhibit the performance of the SPSC against Δ_S for the two cases i.e., without jamming and with jamming, respectively. It can be observed that decreasing Ω_{RE} improves the SPSC performance (without external jamming), owing to the fact that an increase in Ω_{RE} positively affects the capability of eavesdropper, which results in the degradation of the SPSC. However, increasing Ω_{SR} (which is tantamount to improving the channel between S and R) in the presence of a jammer yields a better system performance.

Fig. 6 reflects the impact of the power allocation coefficient a_1 on the SOP for both jamming and without jamming case. For $\Delta_S = 30$ dB, SOP performance is better than that for $\Delta_S = 20$ dB. This is because, we have assumed that $\Delta_S = \Delta_J$ and with the increase in the value of transmit SNR of node J i.e., Δ_J, the impact of jammer on the eavesdroppers's SNR increases, and it will deteriorate the SNR of the eavesdropper, so the overall SOP performance will be improved. But for a fixed value of Δ_S, as the value of a_1 increases, the power allocated for the transmission of x_R decreases. This is because of the fact that the received SNR at Q for x_R depends on a_2, and $a_2 = 1 - a_1$. Therefore, the probability of correctly decoding x_R is low. And this degrades the SOP performance.

V. Conclusion

In this paper, we have analyzed the secrecy performance of a CJ-aided overlay CNOMA system under Nakagami-m fading. Closed-form expression of SOP and SPSC have been derived. We have also investigated the asymptotic behavior of the SOP expression for higher values of SNR. The numerical results have revealed that CJ is an efficient technique to guarantee PLS in the proposed system. For future work, we can consider

the cases of imperfect SIC and CSI conditions, which is useful for realistic implementations. The performance of the CJ-aided overlay cognitive NOMA system model is carried out by not considering energy harvesting model. However, in practical scenarios, energy harvesting models are more efficient. So, we can extend this work by deploying an energy harvesting relay to exploit simultaneous wireless information power transfer (SWIPT) technique.

ACKNOWLEDGMENTS

This research work is carried out under the Nokia Foundation Visiting Professor Grant and Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology (MeitY), Government of India, being implemented by Digital India Corporation (formerly Media Lab Asia). The work of J. Lehtomäki is supported in part by the Academy of Finland 6Genesis Flagship under Grant 318927. The work of J. M. Moualeu is supported in part by the South Africa's National Research Foundation (NRF) under Grant No. 116018.

REFERENCES

[1] F. Li, H. Jiang, R. Fan, and P. Tan, "Cognitive non-orthogonal multiple access with energy harvesting: An optimal resource allocation approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7080-7095, Jul. 2019.

[2] L. Luo, Q. Li, and J. Cheng,"Performance analysis of overlay cognitive NOMA systems with imperfect successive interference cancellation," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4709-4722, Aug. 2020.

[3] A. K. Shukla, V. Singh, P. K. Upadhyay, A. Kumar, and J. M. Moualeu, "Performance analysis of energy harvesting-assisted overlay cognitive NOMA systems with incremental relaying," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1558-1576, 2021.

[4] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[5] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G non-orthogonal multiple access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010-6023, Aug. 2016.

[6] M. Mohammadi, B. K. Chalise, A. Hakimi, Z. Mobini, H. A. Suraweera, and Z. Ding, "Beamforming design and power allocation for full-duplex non-orthogonal multiple access cognitive relaying," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 5952-5965, Dec. 2018.

[7] 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.

[8] Y. Liu, H. -H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys and Tuts.*, vol. 19, no. 1, pp. 347-376, Firstquarter 2017.

[9] 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.

[10] L. Xu, A. Nallanathan, X. Pan, J. Yang, and W. Liao, "Security-aware resource allocation with delay constraint for NOMA-based cognitive radio network," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 366-376, Feb. 2018.

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

[12] Z. Shang, T. Zhang, G. Hu, Y. Cai, and W. Yang, "Secure transmission for NOMA-based cognitive radio networks with imperfect CSI," *IEEE Commun. Lett.*, vol. 25, no. 8, pp. 2517-2521, Aug. 2021.

[13] 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, June 2019.

[14] Y. Zheng et al., "Overlay cognitive ABCom-NOMA-based ITS: An in-depth secrecy analysis," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–12, 2022.

[15] C. Yu, H. -L. Ko, X. Peng, W. Xie, and P. Zhu, "Jammer-aided secure communications for cooperative NOMA systems," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 1935-1939, Nov. 2019.

[16] S. Sharma, S. D. Roy, and S. Kundu, "Secrecy at physical layer in NOMA with cooperative jamming," *National Conf. Commun. (NCC)*, Kharagpur, India, pp. 1-6, Feb. 21-23, 2020.

[17] B. Chen, R. Li, Q. Ning, K. Lin, C. Han, and V. C. M. Leung, "Security at physical layer in NOMA relaying networks with cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3883-3888, Apr. 2022.

[18] 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.

[19] B. Li et al., "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3482–3495, May 2019.

[20] C. Yu, H. Ko, X. Peng, W. Xie, and P. Zhu, "Jammer-aided secure communications for cooperative NOMA systems," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 1935–1939, Nov. 2019.

[21] V. Bankey, V. Singh, and P. K. Upadhyay, "Physical layer secrecy of NOMA-based hybrid satellite-terrestrial relay networks," *IEEE Wireless Commun. Netw. Conf. (WCNC)*, Seoul, Korea (South), pp. 1–6, May 25-28, 2020.

[22] C. K. Singh, and P. K. Upadhyay, "Overlay cognitive IoT-based full-duplex relaying NOMA systems with hardware imperfections," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6578–6596, May 2022.

[23] I. S. Gradshteyn, and I. M. Ryzhik, *Tables of Integrals, Series and Products*, 7th ed. New York: Academic Press, 2007.