IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 January 2024, accepted 21 January 2024, date of publication 30 January 2024, date of current version 8 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3359753

RESEARCH ARTICLE

Physical Layer Secrecy Performance Analysis of Jamming-Assisted Overlay Cognitive NOMA Networks With Hardware Impairments and Multiple Non-Colluding Eavesdroppers

P. P. HEMA, (Student Member, IEEE), AND A. V. BABU, (Senior Member, IEEE)
Department of Electronics and Communication Engineering, National Institute of Technology Calicut, Calicut, Kerala 673601, India
Corresponding authors: P. P. Hema (hema_p210071ec@nitc.ac.in) and A. V. Babu (babu@nitc.ac.in)

ABSTRACT This paper investigates the physical layer security (PLS) of non-orthogonal multiple access (NOMA)-enabled overlay cognitive radio networks (NOMA-OCRNs), considering multiple non-colluding eavesdroppers. Here PLS is evaluated in terms of: (i) secrecy outage probability (SOP) of primary user (PU) and secondary user (SU) and (ii) system SOP (SSOP), system secrecy throughput (SST) and secrecy energy efficiency (SEE) of the network. Residual hardware impairments arising from non-ideal hardware and imperfect successive interference cancellation conditions are considered. Firstly, we derive new analytical expressions for the SOPs of PU and SU. Numerical evaluation results show that both PU as well as SU suffer very high SOPs that tend to unity in the high transmit power region. Further, RHI and i-SIC have a significant impact on the secrecy performance. To improve the PLS performance, we propose a jamming-assisted framework and develop novel analytical models for determining the SOPs of PU and SU. We derive the asymptotic SOP expressions as well. Detailed analytical and simulation results are presented to demonstrate that the proposed jamming-assisted framework leads to a significant reduction of the SOPs of both PU and SU while exhibiting considerable enhancement of SST and SEE of the network compared to the no-jammer scenario. In the final part of this paper, we utilize a deep learning framework for the precise and fast prediction of the SOPs of PU and SU, that can replace complex mathematical modeling.

INDEX TERMS Overlay cognitive radio networks, non-orthogonal multiple access, physical layer security, multiple eavesdroppers, residual hardware impairments, performance analysis.

I. INTRODUCTION

Currently, fifth-generation (5G) wireless communication systems are being rolled out worldwide to provide high-speed, ultra-reliable, low-latency communications. However, incessant growth in the number of smart devices and the emergence of Internet-of-Everything (IoE) applications will result in a substantial burden on 5G wireless networks [1]. In this context, sixth generation (6G) wireless networks are being explored by academia and industries to provide (a) a maximum data rate of 100Gbps, (b) reliability of the order of 99.99999 percent, (c) air interface latency of the order of 0.1ms, (d) increased connectivity and coverage compared to 5G and (e) highly energy efficient, secure communications [2], [3]. Recently, non-orthogonal multiple access (NOMA) has emerged as a popular multiple access technology for 5G and beyond 5G (B5G) wireless networks, since it improves spectral efficiency by allowing multiple users to share the same transmission resources simultaneously [4], [5], [6]. In power domain NOMA, super-position coding is applied at the transmitter while successive interference cancellation (SIC) is used as the multi-user detection technique at the receiver [4]. In a downlink cooperative NOMA system, strong (i.e., cell-center) users or

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

dedicated relay nodes are employed to improve the reliability of weak (i.e., cell-edge) users. Utilizing cooperative relaying in NOMA system results in very high reliability for weak users, while achieving higher diversity gain and improved system throughput [7], [8].

On the other hand, cognitive radio (CR) technology has been proposed to resolve spectrum scarcity in wireless communication systems [9]. The use of CR technology in 5G and B5G wireless networks can alleviate spectrum crunch as well as spectrum under-utilization, since it allows the unlicensed secondary users (SUs) to access the licensed spectrum occupied by the primary users (PUs) based on either interweave, underlay or overlay principle. In the interweave mode, the SUs can transmit only if the primary spectrum is unoccupied, while the underlay mode enables the SUs to transmit concurrently with the PUs in the same frequency spectrum as long as the interference induced on the PU receiver remains below a tolerable threshold. Likewise, the overlay mode allows SUs and PUs to transmit concurrently utilizing the same frequency spectrum, where the SUs act as relays to enhance the performance of the PUs [9]. From the perspective of a practical application scenario, the integration of CR with the Internet- of-Things (IoT) system has the potential to bring significant benefits to both wireless communication systems and IoT applications [10]. In cognitive IoT systems, the IoT devices can act as the SUs and can opportunistically use the available spectrum to communicate with other devices or with the Internet. Thus, cognitive IoT systems can enhance spectrum utilization efficiency and improve the quality of service (QoS) for IoT applications. Additionally, cognitive IoT systems can enable seamless integration of wireless communication and IoT technologies, enabling the development of new and innovative applications such as smart cities, industrial internet, and smart healthcare [10].

Since both CR as well as NOMA techniques aim to enhance the spectrum utilization efficiency, the NOMA-enabled CR networks (NOMA-CRNs) are capable of further improving the spectral efficiency and connectivity [11]. Here NOMA can be applied in the secondary network to enhance the spectrum utilization efficiency and to achieve massive connectivity, As a consequence, several authors have investigated the performance of NOMA-enabled underlay CRNs (i.e., NOMA-UCRNs) and NOMA-enabled overlay CRNs (NOMA-OCRNs), see [12], [13], [14], [15] and references therein. In NOMA-UCRN, the QoS of SU cannot be guaranteed since the transmit powers of secondary transmitters (STs) are limited by the interference constraint of the PU receiver. On the other hand, the QoS of both SU as well as PU can be ensured, when the overlay paradigm is employed since SU assists the PU through cooperative NOMA, while simultaneously getting access to the PU's licensed spectrum. Accordingly, the present work focuses on NOMA-OCRNs.

Secure transmission is a key challenge for the next generation wireless networks owing to the broadcast nature of the wireless channel, since external eavesdroppers may exist to intercept the messages intended for the legitimate users (LUs) [16], [17], [18]. Security and privacy protection are fundamental requirements for cognitive IoT systems as well. The communication links in IoT systems, i.e., uplink communications from sensors to controllers, downlink communications from controllers to actuators, etc., are highly susceptible to eavesdropping. Recently, the notion of physical layer security (PLS) has received remarkable attention since it exploits the randomness of wireless fading channels rather than cryptography techniques to secure the communication link. The fundamental idea of PLS is that a wireless communication system can be theoretically secured without using any traditional cryptographic methods if the capacity of the legitimate channel is higher than that of eavesdroppers. Of late, PLS has been envisaged as an additional level of security protection on top of the existing cryptography-based security schemes [16], [17], [18]. The major objective of this paper is to propose efficient techniques for enhancing the PLS performance of both PU as well as SU in NOMA-OCRNs.

A. LITERATURE SURVEY AND PROBLEM FORMULATION

Several research papers have appeared to analyse the PLS performance of NOMA-UCRNs, see [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30] and references therein. The authors of [19] have considered user scheduling and power allocation to improve the PLS performance of NOMA-UCRNs. The authors of [20] have analyzed connection outage probability (COP) and SOP performance of PUs in NOMA-UCRN, while the authors of [21] have investigated COP, intercept probability and effective secrecy throughput (EST) of NOMA-UCRN considering outdated channel state information (CSI). The authors of [22] have introduced hybrid automatic repeat request technique to improve the secrecy performance of NOMA-UCRNs, while the authors of [23] and [24] have independently analyzed the PLS performance of NOMA-UCRNs. In [25], the authors have investigated optimal power allocation to maximize the secrecy sum rate (SSR) of the SUs in NOMA-UCRN while the work in [26] investigated the secrecy rate maximization in NOMA-UCRN. In [27], the authors have investigated techniques for the selection of SUs to enhance the PLS performance of PU in NOMA-UCRN. In [28], the authors have analyzed COP, SOP and EST of NOMA-UCRN, assuming imperfect CSI. In [29], the intercept probability performance was examined for NOMA-enabled underlay cognitive hybrid satellite-terrestrial networks (NOMA-UCHSTNs) in the presence of an eavesdropper. In [30], the authors have examined the sum secrecy rate maximization problem in NOMA-UCHSTN, where an external eavesdropper is present. Notice that the research works reported in [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], and [30] examined the PLS performance of NOMA-UCRN in the presence of an external eavesdropper, while the focus of the current work is to investigate the PLS performance of NOMA-OCRNs, where multiple eavesdroppers are present in the network.

Recently, a few authors have analysed the PLS performance of NOMA-OCRNs as well [31], [32], [33], [34], [35]. In [31], the authors have investigated the COP, SOP and EST of primary network in NOMA-OCRN, where the SUs are considered as internal eavesdroppers. The authors of [32] have employed a multi-antenna secondary full-duplex (FD) relay to enhance the PLS of the PU in NOMA-OCRN. In [33], the authors have investigated optimal beamforming design to maximize the secrecy rate of the SU in NOMA-OCRN. Notice that the PLS performance of SU was overlooked in [31] and [32], while that of PU was ignored in [33]. The authors of [34] have analyzed the intercept probability of PU and SU in NOMA-OCRN, where the ST selects one SU from among a set of M SUs to operate as a relay for assisting the communication to the PU. In [35], the authors have studied the secrecy performance of the NOMA-enabled overlay cognitive ambient backscatter communication system in the presence of an eavesdropper. Notice that the authors of [31], [32], [33], [34], and [35] have considered that only one eavesdropper is present in the network. Further, none of the above papers have considered a jamming-assisted framework for improving the PLS performance of PU and SU in NOMA-OCRNs.

In recent studies, a few authors have conducted investigations on the influence of multiple eavesdroppers on the secrecy performance of NOMA-enabled systems [36], [37], [38], [39], [40], [41], [42], [43], [44], [45]. Considering wiretapping by many numbers of non-colluding eavesdroppers, the authors of [36] have evaluated the secrecy performance of a NOMA system in terms of SOP, where the BS directly communicates to the downlink users with the near user assumed as untrusted. In [37], the authors have examined the SOPs of downlink users in a cooperative NOMA system with multiple decode and forward (DF) relays considering both colluding and non-colluding wiretap scenarios. In [38], the authors have considered the impact of non-colluding eavesdroppers on the SOPs of downlink users in user-assisted cooperative NOMA systems. The authors of [39] have evaluated the SOP and the EST performance of a cooperative NOMA -based FD relay sharing system, with multiple eavesdroppers. The research work in [40] focused on the evaluation of ergodic secrecy rate (ESR), where a two-way FD relay network was considered that relies on cooperative NOMA technique. In [41], the authors have independently investigated the SOPs of downlink users in FD-cooperative NOMA systems in the presence of multiple eavesdroppers. In [42], the authors have examined the SOPs experienced by the downlink users in NOMA-enabled hybrid satellite-terrestrial network with colluding/non-colluding eavesdroppers, considering hardware impairments. In [43], the authors have researched the joint effects of channel estimation errors and hardware impairments on the secrecy performance of NOMA-UCHSTN in the presence of multiple non-colluding eavesdroppers. The authors of [44] have investigated the SOP performance of downlink users in a directly connected NOMA network, where multiple eavesdroppers are present. In [45], the authors have examined the SOP performance of downlink users for both code-domain NOMA and power-domain NOMA scenarios, where both external and internal eavesdropping cases are considered.

It is worth noticing that comprehensive analytical models for evaluating the PLS performance of NOMA-OCRN in the presence of multiple eavesdroppers has not appeared in the literature so far. Even though multiple eavesdroppers were considered in the context of cooperative NOMA systems [36], [37], [38], [39], [40], [41], [42], these studies are not directly applicable to a spectrum-sharing scenario such as NOMA-OCRN. Although the authors of [43] have analyzed the PLS performance of NOMA-UCHSTNs, the results are not directly applicable to a terrestrial wireless networking scenario such as NOMA-OCRN considered in this paper. Further, none of the above papers [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43] have proposed suitable methods for enhancing the secrecy performance. Furthermore, these studies [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43] mentioned above have ignored the problem of determining optimal transmit powers to be apportioned for the downlink users for enhancing the secrecy performance. Secondly, most of the above research works have considered ideal radio frequency (RF) transceivers. However, RF transceivers employed in communication systems suffer from hardware impairments (HIs), which leads to distortion noise in the system [46]. Even though several techniques were proposed for the mitigation of HIs, RF transceivers still experience residual HI (i.e., RHI), which has a detrimental impact on the performance of wireless communication systems [47], [48], [49], [50]. Accordingly, we need to consider RHI as well, for the evaluation of PLS of NOMA-OCRN. Thirdly, in a downlink NOMA system, the strong user has to firstly decode the message corresponding to the weak user from the received superposition coded NOMA signal and thereafter use the SIC procedure to decode its own message [4], [5]. Considering a more practical scenario, we need to study the impact of residual interference generated at the strong user due to imperfect SIC (i-SIC) [51], [52] on the PLS performance of NOMA-OCRN, which has been ignored in the above papers [31], [32], [33], [34], [35]. Recently, many researchers have utilized deep neural network (DNN) for evaluating the performance of wireless networks, instead of relying on complex mathematical modeling and the time-consuming Monte-Carlo simulation approaches, see [53], [54], [55], [56] and references therein. The authors of [53] have proposed a DNN model for determining the SOP of ground-to-air communications, while the authors of [54] and [55] have independently investigated the use of DNN for selecting the best relay for enhancing the performance of CR networks. In [56], the authors have exploited DNN for enhancing the performance of cell-edge user in NOMA-CRN. The above-mentioned investigations have demonstrated the

powerful capability of DNN to predict various performance metrics of wireless networks with high level of accuracy and reduced prediction time, compared to analytical modeling and Monte-Carlo simulations-based approaches. Motivated by these observations, the objectives of the current works are the following: (i) to formulate analytical models for investigating the PLS performance of NOMA-OCRN considering multiple non-colluding eavesdroppers, RHI and i-SIC (ii) to propose a jamming-assisted frame work and evaluate its effectiveness in enhancing the security performance; (iii) to determine the transmit power allocation for PU as well as SU at the ST that further enhances the security performance of NOMA-OCRN and (iv) to formulate a DNN framework for the prediction of SOPs of PU and SU with high level of accuracy and lowest execution time.

B. CONTRIBUTIONS

The key contributions of this paper are as outlined below:

- First, we consider NOMA-OCRN where the primary network consists of a primary transmitter (PT)-primary destination (PD) pair. In the secondary network, the ST acts as a relay to assist primary transmissions while getting access to the PU's spectrum for transmitting its own message to the secondary receiver (SR) by utilizing the power domain NOMA technique. We derive new analytical expressions for the SOPs of both PU as well as SU in the presence of multiple non-colluding eavesdroppers, considering both RHI as well as i-SIC. With the help of numerical results, it is shown that both PU as well as SU suffer very high SOPs that tend to unity in the high transmit power region. Moreover, it is established that RHI and i-SIC have significant impact on the secrecy performance of the considered NOMA-OCRN.
- A jammer-assisted framework is considered in order to improve the PLS performance, where an external jamming node transmits jamming signals to confuse the eavesdroppers. Analytical expressions are obtained for the SOPs of both PU as well as SU for the jammer-assisted scenario as well. It is shown that the considered jammer-assisted framework provides significant reduction of the SOPs of both PU as well as SU compared to the no-jammer case.
- Results are provided for comparing the SOPs experienced by both PU as well as SU in the proposed NOMA-OCRN against orthogonal multiple access (OMA)-based OCRN, i.e., OMA-OCRN. It is demonstrated that the SOPs are lower in the proposed NOMA-OCRN compared to its OMA counterpart.
- We then formulate the SSOP minimization problem and determine the optimal transmit power allocation for both PU as well as SU at the ST that minimizes the System SOP (SSOP) of the jammer-assisted NOMA-OCRN. We find the optimal power allocation coefficients (OPACs) and demonstrate that both the SSOP as well as the SOPs are considerably reduced under the proposed OPAC, compared to random/equal setting of the PACs. Moreover, it is also demonstrated that the OPAC provides significant enhancement of the SEE and SST of the jammer-assisted NOMA-OCRN compared to the no-jammer case.
- Finally, we describe a DNN model for the precise prediction of the SOPs with reduced execution time and demonstrate the effectiveness of the proposed approach.

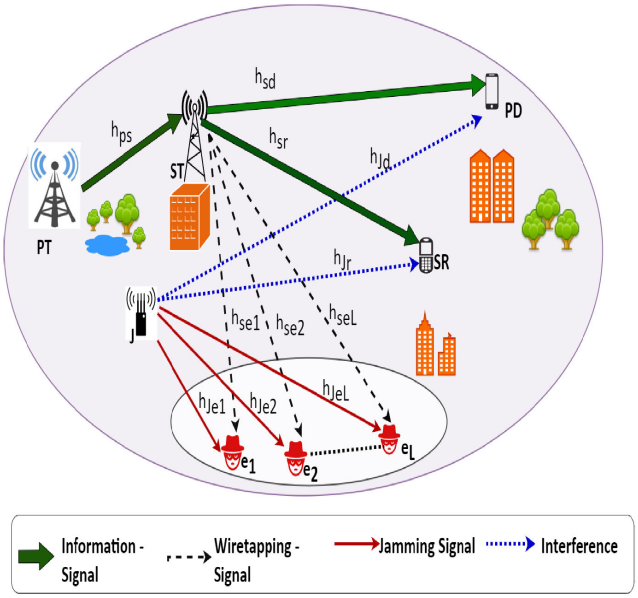

FIGURE 1. NOMA-OCRN with Non-colluding eavesdroppers and jammer.

The rest of this paper is organized as follows. Section II describes the system model and provides signal-to-interference and distortion plus noise ratio (SIDNR) calculations. Section III describes the SOP analysis, followed by the description of the asymptotic SOP expressions. The SSOP minimization problem is introduced in Section IV and DNN framework for predicting SOPs is described in Section V. Finally, Section VI describes the results, while the paper is concluded in Section VII.

II. SYSTEM MODEL

We consider the NOMA-OCRN shown in FIGURE 1, where the primary network comprises of a PT-PD pair, while the secondary network comprises of a ST-SR pair. The direct link from PT to PD suffers heavy shadowing, which makes it impossible to communicate directly from PT to PD. Accordingly, based on the notion of the overlay mode of operation, PT uses ST as a DF relay to forward its messages to PD. To facilitate this, PT initially transmits the symbol intended for PD. From the received signal, ST attempts to regenerate a clean copy of PD's symbol so that it can be forwarded to PD in the next time slot. In return, ST can simultaneously send its own messages to SR by utilizing the primary spectrum based on the power domain NOMA

principle i.e., ST applies superposition coding technique based on the power domain NOMA principle to combine the message symbol intended for PD and its own symbol intended for SR, and transmits the combined signal in the second time slot. Thus, the considered NOMA-OCRN facilitates simultaneous access of both PT as well as ST in the spectrum occupied by the primary network. The NOMA-OCRN model investigated is equivalent to the cognitive IoT scenario considered in [57] and [58], where the primary network could be the one, which has been allocated the licensed frequency band (such as a cellular network). The secondary network resembles a downlink IoT network [57], [58], where a controller (i.e., ST) intends to transmit confidential messages to an actuator (i.e., SR) in the presence of L potential passive eavesdroppers. Since the secondary network does not have a dedicated spectrum, it relies on the primary spectrum for the ST-to-SR, i.e., controller-to-actuator communications. Based on the overlay principle, the controller acts as a DF relay to forward messages from PT to PD. As a reward, the controller can simultaneously send its own message to the actuator by employing power domain NOMA. To enhance the spectrum utilization efficiency and to achieve massive connectivity, NOMA is employed in the secondary network. Accordingly, the controller applies superposition coding based on power domain NOMA principle to combine its message to the actuator along with the message for the PD. The nodes ST and SR in the secondary network could also represent femtocell users who do not have dedicated spectrum for their communications and hence rely on primary spectrum [59]. Let us assume that L external passive non-colluding eavesdroppers E_l; $l\epsilon\,(1\,,2\,,\ldots,\,L)$ are present that attempt to wire-tap the messages transmitted by ST. We consider a jamming-assisted scenario, in which a jammer node (J) is assumed to be present in the network that discombobulates the eavesdroppers so as to improve the PLS of the considered NOMA-OCRN.

Let $h_{ps}, h_{sd}, h_{sr}, h_{se_l}$, h_{Je_l}, h_{Jd} and h_{Jr} be the fading channel coefficients corresponding to the links: PT-ST, ST-PD, ST-SR, ST-E_l, J-E_l, J-PD, and J-SR respectively; $l\epsilon\,(1\,,2,\ldots,\,L)$. All the nodes in the network are assumed to have single-antenna and operate in half-duplex (HD) mode. We assume frequency non-selective block Rayleigh fading so that the channel coefficients remain time-invariant over each block period T; but varies over sucessive block periods. The power gains $\left\{\left|h_{ij}\right|^2;\, i\,\epsilon\,(p,s,J)\,;j\,\epsilon\,(s,d,r,e_l)\,;l\,\epsilon\,(1,2,\ldots,L);\, i\neq j\right\}$ adher to exponential probability density function (PDF) with mean value λ_{ij}. Finally, the additive white Gaussian noise (AWGN) at all the receiving terminals in the network are assumed to be of equal variance σ^2.

A. SIGNAL MODEL AND SIDNR CALCULATIONS IN THE PRESENCE OF RHI

In the considered NOMA-OCRN, the transmissions are carried out in two half cycles of duration $\frac{T}{2}$ each, with NOMA technique employed by ST in the second half cycle. During the first half cycle, PT transmits the signal $x_p(t)$ to ST with power P_p. The received signal at ST in the presence of RHI is given by:

$$y_s\,(t) = h_{ps}\left(\sqrt{P_p}\,x_p\,(t) + \eta_{ps}\right) + n_s\,(t)\,, \tag{1}$$

where $n_s(t)$ is the AWGN present at ST; $\eta_{ps} \sim C\mathcal{N}(0,\ \theta_{ps}^2 P_p)$ denotes the RHI at both PT and ST and $\theta_{ps} = \sqrt{\theta_{p_{tx}}^2 + \theta_{s_{rx}}^2}$ represents the aggregate RHI of the PT-ST link with $\theta_{p_{tx}}^2$ and $\theta_{s_{rx}}^2$ respectively representing the HIs at PT and ST [47], [48], [49], [50]. The SIDNR and the achievable data rate corresponding to the decoding of x_p at ST (i.e., Γ_{s,x_p} and R_{s,x_p} respectively) are given by:

$$\Gamma_{s,x_p} = \frac{\rho_p\left|h_{ps}\right|^2}{\rho_p\left|h_{ps}\right|^2\theta_{ps}^2 + 1}, \tag{2a}$$

and

$$R_{s,x_p} = \frac{1}{2}\log(1 + \Gamma_{s,x_p}), \tag{2b}$$

where $\rho_p = \frac{P_p}{\sigma^2}$. Assuming R_{th}^P to be the target data rate for successfully decoding x_p at ST, which is possible if and only if $R_{s,x_p} \geq R_{th}^P$ or $\Gamma_{s,x_p} \geq \gamma_{th}^P$, where $\gamma_{th}^P = 2^{2R_{th}^P} - 1$ is the corresponding target SIDNR.

During the second half cycle, assuming that ST succeeds in decoding x_p in the previous time slot, it regenerates x_p and applies power domain NOMA technique, to combine x_p with its own message x_s intended for SR. If ST is unable to successfully decode x_p, it will send x_s alone in the second half cycle. Accordingly, the signal transmitted by ST during the second time slot is given by:

$$x(t) = \begin{cases} \sqrt{\alpha_p P_s}\,x_p(t) + \sqrt{\alpha_s P_s}\,x_s(t); & \Gamma_{s,x_p} \geq \gamma_{th}^P \\ \sqrt{\delta P_s}\,x_s(t); & \Gamma_{s,x_p} < \gamma_{th}^P, \end{cases} \tag{3}$$

where P_s is the total power of ST, α_p and α_s respectively are the power allocation coefficients for x_p and x_s at ST such that $\alpha_s < \alpha_p$, $\alpha_p + \alpha_s = 1$. Thus, higher power is allocated for the weak user (i.e., PD) at ST, following the conventional NOMA principle. Further, $\delta\,(0 < \delta \leq 1)$ is the power allocation coefficient for x_s at ST, if x_p is not successfully decoded previously. Meanwhile, the jammer transmits the jamming signal $x_J(t)$ with power P_J during the second half cycle to confound the eavesdroppers. The received signal at PD and SR during the second half cycle (i.e., $y_d(t)$ and $y_r(t)$ respectively) in the presence of RHI are given by:

$$y_i(t) = h_{si}(x(t) + \eta_{si}) + wh_{Ji}(\sqrt{P_J}x_J(t) + \eta_{Ji}) + n_i(t);\ \ i\epsilon(d,r), \tag{4}$$

where $w = 0$ means the no-jammer (NJ) case while $w = 1$ means the jamming assisted (JA) case; $n_d(t)$ and $n_r(t)$ represent AWGN at PD and SR respectively; $\eta_{sd} \sim C\mathcal{N}(0,\ \theta_{sd}^2 P_s)$ is the RHI at both ST and PD;

$\eta_{sr} \sim C\mathcal{N}(0, \theta_{sr}^2 P_s)$ is the RHI at both ST and SR;$\eta_{Jd} \sim C\mathcal{N}(0, \theta_{Jd}^2 P_J)$ is the RHI at both J and PD; $\eta_{Jr} \sim C\mathcal{N}(0, \theta_{J_r}^2 P_J)$ is the RHI at both J and SR; $\theta_{sd} = \sqrt{\theta_{s_{tx}}^2 + \theta_{d_{rx}}^2}$ represents the aggregate RHI of the ST-PD link with $\theta_{s_{tx}}^2$ and $\theta_{d_{rx}}^2$ representing the HIs at ST and PD respectively. Further $\theta_{sr} = \sqrt{\theta_{s_{tx}}^2 + \theta_{r_{rx}}^2}$ is the aggregate RHI of the ST-SR link with $\theta_{r_{rx}}^2$ representing the HI at SR. Also $\theta_{Jd} = \sqrt{\theta_{J_{tx}}^2 + \theta_{d_{rx}}^2}$ is the aggregate RHI of the J-PD link with $\theta_{J_{tx}}^2$ and $\theta_{d_{rx}}^2$ representing the HIs at J and PD respectively. Also $\theta_{Jr} = \sqrt{\theta_{J_{tx}}^2 + \theta_{r_{rx}}^2}$ represents the aggregate RHI of the J-SR link with $\theta_{J_{tx}}^2$ and $\theta_{r_{rx}}^2$ representing the HIs at J and SR respectively [47], [48], [49], [50]. We assume that the jamming signal is pre-shared and perfectly known at PD and SR.[1] Accordingly, the SIDNR corresponding to the decoding of x_p at PD can be determined as (5), shown at the bottom of the page. At SR, SIC is implemented to decode the symbol x_s. Towards this, SR firstly decodes x_p and then uses SIC to decode x_s, after removing the decoded symbol x_p from the received signal. Assuming i-SIC conditions, the SIDNRs corresponding to the decoding of x_p and x_s at SR (i.e., Γ_{r,x_p} and Γ_{r,x_s} respectively) are given by (6) and (7), as shown at the bottom of the page. Notice that (5)-(7) are formulated assuming that both PD and SR are capable of perfectly cancelling the jamming signal while decoding the messages. Further, notice that both (6) and (7) consider the event that ST is not able to decode the symbol x_p in the first half cycle. Furthermore, the term $\beta\alpha_p\rho_s |h_{sr}|^2$ in (7) represents the residual interference generated at SR due to i-SIC, where β ($0 < \beta < 1$) is the i-SIC coefficient [51], [52].

At the eavesdroppers, we assume a worst-case scenario in which they are assumed to possess very efficient multi-user detection capabilities. The foregoing assumption has been extensively applied in literature, see [44], [60] and references therein. Apart from this, a non-colluding scenario is considered, where each eavesdropper can decode the symbols x_p and x_s independently of others [40], [41], [42], [43]. The most detrimental eavesdropper that can wiretap the message symbols intended for the LUs with the highest SIDNR is considered in this paper. The received signal at an arbitrary eavesdropper E_l in the presence of RHI is given by:

$$y_{e_l}(t) = \begin{cases} h_{se_l}\left(\sqrt{\alpha_p P_s}\, x_p(t) + \sqrt{\alpha_s P_s}\, x_s(t) + \eta_{se_l}(t)\right) \\ +wh_{Je_l}\left(\sqrt{P_J} x_J(t) + \eta_{Je_l}(t)\right) + n_{e_l}(t); \Gamma_{s,x_p} \geq \gamma_{th}^P \\ h_{se_l}\left(\sqrt{\delta P_s}\, x_s(t) + \eta_{se_l}(t)\right) + wh_{Je_l}\left(\sqrt{P_J} x_J(t)\right. \\ \left.+\eta_{Je_l}(t)\right) + n_{e_l}(t) \quad ; \Gamma_{s,x_p} < \gamma_{th}^P, \end{cases} \tag{8}$$

where the second case in (8) corresponds to ST not able to successfully decode x_p in the first half cycle due to which it transmits x_s alone in the second half cycle. Here $w = 1$ corresponds to JA and $w = 0$ means NJ scenario; $n_{e_l}(t)$ is the AWGN at E_l; $\eta_{se_l} \sim C\mathcal{N}(0, \theta_{se_l}^2 P_s)$ is the RHI at ST and E_l where $\theta_{se_l}=\sqrt{\theta_{s_{tx}}^2 + \theta_{e_{lrx}}^2}$ represents the aggregate RHI of ST-E_l link with $\theta_{s_{tx}}$ and $\theta_{e_{lrx}}$ representing the HIs at ST and E_l respectively. $\eta_{Je_l} \sim C\mathcal{N}(0, \theta_{Je_l}^2 P_J)$ is the RHI at J and E_l where $\theta_{Je_l}=\sqrt{\theta_{J_{tx}}^2 + \theta_{e_{lrx}}^2}$ represents the aggregate RHI of J-E_l link with $\theta_{J_{tx}}$ and $\theta_{e_{lrx}}$ representing the HIs at J and E_l respectively [47], [48], [49], [50]. The SIDNR corresponding to the decoding of x_p and x_s at the most detrimental eavesdropper (i.e., Γ_{e,x_p} and Γ_{e,x_s} respectively) are given by (9) and (10), as shown at the bottom of the next page, where $\rho_J = \frac{P_J}{\sigma^2}$. In (9) and (10), $w = 1$ corresponds to the JA case for which $\Gamma_{e,i} = \Gamma_{e,i}^{JA}$; and $w = 0$ corresponds to the NJ case for which $\Gamma_{e,i} = \Gamma_{e,i}^{NJ}$; $i \in (x_p, x_s)$.

B. SECRECY RATE CALCULATIONS

The achievable data rate corresponding to the decoding of x_p at PD and x_s at SR are determined as $R_{d,x_p} = \frac{1}{2}\log_2(1 +$

[1]This assumption has been made for analytical tractability. Imperfect knowledge of jamming signal will be part of future work. Nevertheless, our present results serve as a benchmark for future investigations in this domain.

$$\Gamma_{d,x_p} = \begin{cases} \dfrac{\alpha_p\rho_s |h_{sd}|^2}{\alpha_s\rho_s |h_{sd}|^2 + \theta_{sd}^2\rho_s |h_{sd}|^2 + w^2\theta_{Jd}^2\rho_J |h_{Jd}|^2 + 1}; & \Gamma_{s,x_p} \geq \gamma_{th}^P \\ 0; & \Gamma_{s,x_p} < \gamma_{th}^P \end{cases} \tag{5}$$

$$\Gamma_{r,x_p} = \begin{cases} \dfrac{\alpha_p\rho_s |h_{sr}|^2}{\alpha_s\rho_s |h_{sr}|^2 + \theta_{sr}^2\rho_s |h_{sr}|^2 + w^2\theta_{Jr}^2\rho_J |h_{Jr}|^2 + 1}; & \Gamma_{s,x_p} \geq \gamma_{th}^P \\ 0; & \Gamma_{s,x_p} < \gamma_{th}^P, \end{cases} \tag{6}$$

$$\Gamma_{r,x_s} = \begin{cases} \dfrac{\alpha_s\rho_s |h_{sr}|^2}{\beta\alpha_p\rho_s |h_{sr}|^2 + \theta_{sr}^2\rho_s |h_{sr}|^2 + w^2\theta_{Jr}^2\rho_J |h_{Jr}|^2 + 1}; & \Gamma_{s,x_p} \geq \gamma_{th}^P \\ \dfrac{\delta\rho_s |h_{sr}|^2}{\theta_{sr}^2\delta\rho_s |h_{sr}|^2 + w^2\theta_{Jr}^2\rho_J |h_{Jr}|^2 + 1}; & \Gamma_{s,x_p} < \gamma_{th}^P \end{cases} \tag{7}$$

Γ_{d,x_p}) and $R_{r,x_s} = \frac{1}{2}\log_2(1+\Gamma_{r,x_s})$ respectively. The data rate over the eavesdropper's channel for the JA/NJ cases are respectively determined as $R^y_{e,x_p} = \frac{1}{2}\log_2(1+\Gamma^y_{e,x_p})$ and $R^y_{e,x_s} = \frac{1}{2}\log_2(1+\Gamma^y_{e,x_s})$; $y\epsilon\,(JA, NJ)$. Accordingly, the achievable secrecy rates of PU and SU for the JA/NJ cases are determined as:

$$R^{PU,y}_{sec} = \left[R_{d,x_p} - R^y_{e,x_p}\right]^+ = \left[\frac{1}{2}\log\left(\frac{1+\Gamma_{d,x_p}}{1+\Gamma^y_{e,x_p}}\right)\right]^+, \tag{11}$$

and

$$R^{SU,y}_{sec} = \left[R_{r,x_s} - R^y_{e,x_s}\right]^+ = \left[\frac{1}{2}\log\left(\frac{1+\Gamma_{r,x_s}}{1+\Gamma^y_{e,x_s}}\right)\right]^+, \tag{12}$$

where $y \in (JA, NJ)$ and $[\,]^+$ implies that $R^{PU,y}_{sec}, R^{SU,y}_{sec} > 0$.

III. SECRECY OUTAGE PROBABILITY (SOP) ANALYSIS

This section describes analytical models for the SOPs of PU and SU, considering the JA/NJ cases, in the presence of multiple non-colluding eavesdroppers. We also describe the asymptotic SOP expressions, which provide valuable insights on the SOP performance. Let $R^{PU}_{sec,th}$ and $R^{SU}_{sec,th}$ respectively be the target secrecy rates of PU and SU. The corresponding target secrecy SIDNR thresholds are $b = 2^{2R^{PU}_{sec,th}} - 1$ and $\varpi = 2^{2R^{SU}_{sec,th}} - 1$ respectively.

A. SOP EXPERIENCED BY PU

Notice that the PU will experience a secrecy outage, when the achievable secrecy rate, i.e., $R^{PU,y}_{sec}$; $y\epsilon\,(JA, NJ)$, falls below the target secrecy rate, i.e., $R^{PU}_{sec,th}$. Accordingly, the SOP of PU for the JA/NJ cases is determined as $\phi^y_{PU} = \Pr(R^{PU,y}_{sec} < R^{PU}_{sec,th})$; $y \in (JA, NJ)$. Recall that the successful delivery of the symbol x_p at PD in the second half cycle requires that it be successfully decoded at ST during the first half cycle, i.e., $\Gamma_{s,x_p} > \gamma^P_{th}$. Accordingly ϕ^y_{PU} is determined as:

$$\begin{aligned}\phi^y_{PU} &= \Pr(R^{PU,y}_{sec} < R^{PU}_{sec,th} \mid \Gamma_{s,x_p} \geq \gamma^P_{th})\Pr(\Gamma_{s,x_p} \geq \gamma^P_{th}) \\ &\quad + \Pr(R^{PU,y}_{sec} < R^{PU}_{sec,th} \mid \Gamma_{s,x_p} < \gamma^{PU}_{th})\Pr(\Gamma_{s,x_p} < \gamma^P_{th}).\end{aligned} \tag{13a}$$

Now $\Gamma_{s,x_p} < \gamma^P_{th}$ implies $\Pr(R^{PU,y}_{sec} < R^{PU}_{sec,th}) = 1$, so that ϕ^y_{PU} can be determined as:

$$\phi^y_{PU} = \Pr(R^{PU,y}_{sec} < R^{PU}_{sec,th}, \Gamma_{s,x_p} \geq \gamma^P_{th}) + \Pr(\Gamma_{s,x_p} < \gamma^P_{th}). \tag{13b}$$

Proposition 1: Utilizing the Gaussian-Chebyshev quadrature approximation [61], an approximate analytical expression for ϕ^{JA}_{PU} can be obtained as in (14), shown at the bottom of the next page, where $\kappa_0 = e^{\frac{-\gamma^P_{th}}{\rho_p\lambda_{ps}(1-\theta^2_{ps}\gamma^P_{th})}}$, $\kappa_1 = 1 - e^{\frac{-\gamma^P_{th}}{\rho_p\lambda_{ps}(1-\theta^2_{ps}\gamma^P_{th})}}$, $\kappa_2 = e^{-\left(\frac{\psi_{j1}+b}{\lambda_{sd}(\alpha_p\rho_s-\rho_s(\alpha_s+\theta^2_{sd})(\psi_{j1}+b))}\right)}$, $\kappa_3 = (2^{2R^{PU}_{sec,th}}\alpha_p\rho_s\lambda_{se})$, $\kappa_4 = -\theta^2_{se}\rho_s\lambda_{se}$, $\kappa_5 = \rho_J\lambda_{Je} - \theta^2_{se}\rho_s\lambda_{se}$, $\upsilon_1 = \min\left(\frac{\alpha_p}{\alpha_s+\theta^2_{sd}} - b, \frac{2^{2R^{PU}_{sec,th}}\alpha_p}{\theta^2_{se}}\right)$, $\epsilon_j = \cos\left(\frac{(2j-1)\pi}{2N}\right)$, $\psi_{j1} = \left(\frac{\upsilon_1}{2}\right)(\epsilon_j+1)$ and N is the complexity accuracy trade-off parameter in the above approximation. Here (14) is valid if and only if $\alpha_p > \frac{b(1+\theta^2_{sd})}{b+1}$; otherwise ϕ^{JA}_{PU} becomes unity.

Proof: Refer Appendix A.

Corollary 1: An approximate expression for ϕ^{NJ}_{PU} is given by (15), shown at the bottom of the next page, where $\alpha_p > \frac{b(1+\theta^2_{sd})}{b+1}$. Otherwise $\phi^{NJ}_{PU} \to 1$.

Remark 1: From (14) and (15), it is evident that both ϕ^{JA}_{PU} and ϕ^{NJ}_{PU} depend on mean channel gains, target secrecy rates and the transmit powers. Further, the numerical results described in section VI demonstrate that both ρ_p as well as ρ_s has significant influence on the SOP of PU.

B. SOP EXPERIENCED BY SU

Notice that the SU will experience a secrecy outage, when the achievable secrecy rate, i.e., $R^{SU,y}_{sec}$; $y \in (JA, NJ)$, falls below the target secrecy rate, i.e., $R^{SU}_{sec,th}$. Thus the SOP of SU is determined as $\phi^y_{SU} = \Pr(R^{SU,y}_{sec} < R^{SU}_{sec,th})$; $y \in (JA, NJ)$. Recall that the symbol x_s is transmitted by ST in the second half cycle either with power $\alpha_s\rho_s$ or $\delta\rho_s$ (i.e., depending on whether ST decodes x_p successfully or not in the first half cycle). Further, assuming that ST successfully decodes x_p in the first half cycle, SR has to successfully decode x_p firstly before decoding x_s. Accordingly, ϕ^y_{SU}; $y \in (JA, NJ)$,

$$\Gamma_{e,x_p} = \begin{cases} \max\limits_{l=1,2,\ldots,L} \dfrac{\alpha_p\rho_s\left|h_{se_l}\right|^2}{\theta^2_{se_l}\rho_s\left|h_{se_l}\right|^2 + w^2\rho_J\left|h_{Je_l}\right|^2(1+\theta^2_{Je_l})+1}; & \Gamma_{s,x_p} \geq \gamma^P_{th} \\ 0; & \Gamma_{s,x_p} < \gamma^P_{th}, \end{cases} \tag{9}$$

$$\Gamma_{e,x_s} = \begin{cases} \max\limits_{l=1,2,\ldots,L} \dfrac{\alpha_s\rho_s\left|h_{se_l}\right|^2}{\theta^2_{se_l}\rho_s\left|h_{se_l}\right|^2 + w^2\rho_J\left|h_{Je_l}\right|^2(1+\theta^2_{Je_l})+1}; & \Gamma_{s,x_p} \geq \gamma^P_{th} \\ \max\limits_{l=1,2,\ldots,L} \dfrac{\delta\rho_s\left|h_{se_l}\right|^2}{\theta^2_{se_l}\delta\rho_s\left|h_{se_l}\right|^2 + w^2\rho_J\left|h_{Je_l}\right|^2(1+\theta^2_{Je_l})+1}; & \Gamma_{s,x_p} < \gamma^P_{th} \end{cases} \tag{10}$$

is determined as:

$$\begin{aligned}\phi_{SU}^{y} &= \Pr(R_{sec}^{SU,y} < R_{sec,th}^{SU} \mid \Gamma_{s,x_p} \geq \gamma_{th}^{P}, \Gamma_{r,x_p} \geq \gamma_{th}^{P}) \\ &\quad \times \Pr(\Gamma_{s,x_p} \geq \gamma_{th}^{P}, \Gamma_{r,x_p}^{\geq} \gamma_{th}^{P}) \\ &\quad + \Pr(R_{sec}^{SU,y} < R_{sec,th}^{SU} \mid \Gamma_{s,x_p} \geq \gamma_{th}^{P}, \Gamma_{r,x_p} < \gamma_{th}^{P}) \\ &\quad \times \Pr(\Gamma_{s,x_p} \geq \gamma_{th}^{P}, \Gamma_{r,x_p} < \gamma_{th}^{P}) \\ &\quad + \Pr(R_{sec}^{SU,y} < R_{sec,th}^{SU} \mid \Gamma_{s,x_p} < \gamma_{th}^{P}) \Pr(\Gamma_{s,x_p} < \gamma_{th}^{P}) \end{aligned} \tag{16a}$$

$$\begin{aligned} &= \Pr(R_{sec}^{SU,y} < R_{sec,th}^{SU}, \Gamma_{s,x_p} \geq \gamma_{th}^{P}, \Gamma_{r,x_p} \geq \gamma_{th}^{P}) \\ &\quad + \Pr(\Gamma_{s,x_p} \geq \gamma_{th}^{P}, \Gamma_{r,x_p} < \gamma_{th}^{P}) \\ &\quad + \Pr(R_{sec}^{SU,y} < R_{sec,th}^{SU}, \Gamma_{s,x_p} < \gamma_{th}^{P}); \ y \epsilon (JA, NJ) \end{aligned} \tag{16b}$$

Proposition 2: Utilizing the Gaussian-Chebyshev quadrature approximation [61], an approximate analytical expression for ϕ_{SU}^{JA} can be obtained as in (17), shown at the bottom of the next page, where $\kappa_7 = (2^{2R_{sec,th}^{SU}}\alpha_s\rho_s\lambda_{se})$, $\kappa_8 = (2^{2R_{sec,th}^{SU}}\delta\rho_s\lambda_{se})$, $\kappa_9 = -\theta_{se}^2\delta\rho_s\lambda_{se}$, $\kappa_{10} = \rho_J\lambda_{Je} - \theta_{se}^2\delta\rho_s\lambda_{se}$, $\kappa_{13} = e^{-\left(\frac{\psi_{j2}+\varpi}{\lambda_{sr}\left(\alpha_s\rho_s-\rho_s\left(\beta\rho_p+\theta_{sr}^2\right)\left(\psi_{j2}+\varpi\right)\right)}\right)}$, $\kappa_{14} = e^{-\left(\frac{\psi_{j3}+\varpi}{\lambda_{sr}\left(\delta\rho_s-\rho_s\left(\delta\theta_{sr}^2\right)\left(\psi_{j3}+\varpi\right)\right)}\right)}$, $\upsilon_2 = \min\left(\frac{\alpha_s}{\beta\alpha_p+\theta_{sr}^2} - \varpi, \frac{2^{2R_{sec,th}^{SU}}\alpha_s}{\theta_{se}^2}\right)$, $\upsilon_3 = \min\left(\frac{1}{\theta_{sr}^2} - \varpi, \frac{2^{2R_{sec,th}^{SU}}}{\theta_{se}^2}\right)$, $\epsilon_j = \cos\left(\frac{(2j-1)\pi}{2N}\right)$, $\psi_{j2} = \left(\frac{\upsilon_2}{2}\right)\left(\epsilon_j+1\right)$, $\psi_{j3} = \left(\frac{\upsilon_3}{2}\right)\left(\epsilon_j+1\right)$, and N is the complexity accuracy trade-off parameter in the above approximation. Here (17) is valid if and only if $0 < \alpha_p < \frac{1-\varpi\theta_{se}^2}{1+\beta\varpi}$; otherwise ϕ_{SU}^{JA} becomes unity.

Proof: Refer Appendix B.

Corollary 2: An approximate expression for ϕ_{SU}^{NJ} is given by (15), where $0 < \alpha_p < \frac{1-\varpi\theta_{se}^2}{1+\beta\varpi}$; otherwise ϕ_{SU}^{NJ} becomes unity.

Remark 2: It is evident from (17) and (18), shown at the bottom of the next page, that the SOP of SU depends on mean channel gains, target secrecy rates and transmit power. The numerical results presented in Section VI illustrate that both ϕ_{SU}^{JA} and ϕ_{SU}^{NJ} are largely independent of ρ_p; however, ρ_s has a significant impact on the SOP performance of SU.

C. ASYMPTOTIC SOPS EXPERIENCED BY PU AND SU

Since the SOP expressions outlined above are intricate, it is difficult to deduce insights on the impact of various parameters on the SOPs of PU and SU. Accordingly, we provide asymptotic SOP expressions as given below.

1) ASYMPTOTIC SOP OF PU AS $\rho_P \to \infty$

Setting $\rho_p \to \infty$ and $\lim_{\rho_p\to\infty} e^{\frac{-x}{\rho_p}} \simeq 1$ in (14) and (15), we obtain the following results.

Proposition 3: The asymptotic SOP of PU (as $\rho_p \to \infty$) for the JA/NJ cases are given by the expressions (19a) and (19b), shown at the bottom of the next page.

Proof: Refer Appendix C.

Remark 3: From (19a)-(19b), it is evident that, as $\rho_p \to \infty$, the asymptotic SOPs experienced by PU for both JA and NJ cases are independent of ρ_p. This happens because, as $\rho_p \to \infty$, the message symbol x_p transmitted by PT in the first half cycle can be successfully decoded at ST. Thereafter, during the second half cycle, ST will attempt to regenerate a clean copy of x_p so that it can be forwarded to PD (i.e., ST acts as a DF relay to forward x_p to PD in the second half cycle). Thus, the successful decoding of x_p at PD in the second half cycle depends on transmit SNR of ST alone (i.e., $\rho_s = P_s/\sigma^2$) and is independent of the transmit SNR of PT (i.e., $\rho_p = P_p/\sigma^2$). Accordingly, the SOP of PU becomes independent of ρ_p, as $\rho_p \to \infty$. These results are applicable to both JA as well as NJ cases.

2) ASYMPTOTIC SOP OF PU AS $\rho_S, \rho_J \to \infty$

Setting $\rho = \rho_s = \rho_J \to \infty$ and $\lim_{\rho\to\infty} e^{\frac{-x}{\rho}} \simeq 1$ in (14), we have the following results.

Proposition 4: As $\rho_s, \rho_J \to \infty$, ϕ_{PU}^{JA} is obtained as:

$$\begin{aligned}&\phi_{PU}^{JA}(\rho \to \infty) \\ &\simeq \kappa_1 + \kappa_0\left[1 - \left(1 - \frac{\alpha_p\lambda_{se} - \kappa_6\lambda_{se}\theta_{se}^2}{\lambda_{Je}\kappa_6 + \alpha_p\lambda_{se} - \kappa_6\lambda_{se}\theta_{se}^2}\right)^{L}\right],\end{aligned} \tag{20}$$

where $\kappa_6 = \frac{\alpha_p}{\alpha_s+\theta_{sd}^2} - b$. Setting $\rho_s \to \infty$ and $\lim_{\rho_s\to\infty} e^{\frac{-x}{\rho_s}} \simeq 1$ in (15), we obtain $\phi_{PU}^{NJ}(\rho_s \to \infty) \simeq 1$.

$$\begin{aligned}\phi_{PU}^{JA} \simeq \kappa_1 + \kappa_0\Bigg[1 - \Bigg(\left(\frac{\upsilon_1}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_2\Bigg(1 - e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}} \times \frac{\kappa_3+\kappa_4\psi_{j1}}{\kappa_3+\kappa_5\psi_{j1}}\Bigg)^{L-1} \frac{e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}}{\kappa_3+\kappa_5\psi_{j1}} \\ \times \left(\frac{\kappa_3}{\kappa_3+\kappa_4\psi_{j1}} + \frac{\kappa_3\left(\kappa_5-\kappa_4\right)}{\kappa_3+\kappa_5\psi_{j1}}\right)\Bigg)\Bigg],\end{aligned} \tag{14}$$

$$\phi_{PU}^{NJ} \simeq \kappa_1 + \kappa_0\left[1 - \left(\left(\frac{\upsilon_1}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_2\left(1 - e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}\right)^{L-1} \frac{e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}}{\left(\kappa_3+\kappa_4\psi_{j1}\right)^2} \times \kappa_3\right)\right], \tag{15}$$

Proof: Refer Appendix C.

Remark 4: Notice that, as $\rho_s \to \infty$, $\phi_{PU}^{NJ} \to 1$. i.e., the SOP of PU tends to unity for the NJ case, as $\rho_s \to \infty$. In the NJ case, as ρ_s becomes higher, the SIDNR corresponding to the decoding of PD's symbol x_p at the most detrimental eavesdropper increases, which results in higher achievable data rate (i.e., corresponding to the decoding of x_p) over the eavesdropper's channel. This makes the achievable secrecy rate of PU to fall below the target secrecy rate, which ultimately leads to very high SOP for PU, On the other hand, (20) shows that ϕ_{PU}^{JA} is independent of ρ_s as $\rho_s, \rho_J \to \infty$. for the JA case, i.e., the SOP of PU becomes a constant, independent of ρ_s as $\rho_s, \rho_J \to \infty$. In the JA case, the presence of jamming signal reduces the SIDNR at the eavesdropper. Accordingly, even though the increase of ρ_s results in a higher achievable data rate (i.e., corresponding to the decoding of x_p) over the eavesdropper's channel, it is equally nullified by the presence of jamming signal, as $\rho_J \to \infty$. As a result, the SOP of PU becomes independent of ρ_s as $\rho_s, \rho_J \to \infty$.

3) ASYMPTOTIC SOP OF SU AS $\rho_P \to \infty$

Setting $\rho_p \to \infty$ and $\lim_{\rho_p \to \infty} e^{\frac{-x}{\rho_p}} \simeq 1$ in (17) and (18), we obtain the following results.

Proposition 5: The asymptotic SOP of SU (as $\rho_p \to \infty$) in NOMA-OCRN for the JA/NJ cases are given by the expressions (21a) and (21b), as shown at the bottom of the next page.

Proof: Refer Appendix D.

Remark 5: From (21a) - (21b), it is evident that, as $\rho_p \to \infty$, the asymptotic SOPs experienced by SU in both JA and NJ cases are independent of ρ_p. Recall that the message symbol intended for SR (i.e., x_s) is transmitted by ST during the second time slot along with the message symbol x_p intended for PD, i.e., ST applies superposition coding technique based on the power domain NOMA principle to combine the message symbol intended for PD and its own symbol intended for SR and transmits the combined signal in the second time slot. Thus, the successful decoding of x_s at SR in the second half cycle depends on the transmit SNR of ST alone (i.e., ρ_s) and is independent of transmit SNR of PT (i.e., ρ_p).

$$\phi_{SU}^{JA} \simeq \kappa_0\Bigg[1-\left(\left(\frac{\upsilon_2}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_{13}\left(1-e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}\times\frac{\kappa_7+\kappa_4\psi_{j2}}{\kappa_7+\kappa_5\psi_{j2}}\right)^{L-1}\frac{e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}}{\kappa_7+\kappa_5\psi_{j2}}\left(\frac{\kappa_7}{\kappa_7+\kappa_4\psi_{j2}}+\frac{\kappa_7\left(\kappa_5-\kappa_4\right)}{\kappa_7+\kappa_5\psi_{j2}}\right)\right)$$
$$-\left(1-e^{\frac{-1}{\rho_s\lambda_{sr}\left(\frac{\alpha_p}{\gamma_{th}^P}-\alpha_s-\theta_{sr}^2\right)}}\right)\Bigg]+\left[e^{\frac{-\gamma_{th}^P}{\delta\lambda_{ps}\left(1-\theta_{ps}^2\gamma_{th}^P\right)}}\times\left(1-e^{\frac{-1}{\rho_s\lambda_{sr}\left(\frac{\alpha_p}{\gamma_{th}^P}-\alpha_s-\theta_{sr}^2\right)}}\right)\right]+\kappa_1\Bigg[1-\left(\left(\frac{\upsilon_3}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_{14}$$
$$\times\left(1-e^{\frac{-\psi_{j3}}{\kappa_8+\kappa_9\psi_{j3}}}\times\frac{\kappa_8+\kappa_{10}\psi_{j3}}{\kappa_8+\kappa_{10}\psi_{j3}}\right)^{L-1}\frac{e^{\frac{-\psi_{j3}}{\kappa_8+\kappa_9\psi_{j3}}}}{\kappa_8+\kappa_{10}\psi_{j3}}\left(\frac{\kappa_8}{\kappa_8+\kappa_9\psi_{j3}}+\frac{\kappa_8\left(\kappa_{10}-\kappa_9\right)}{\kappa_8+\kappa_{10}\psi_{j3}}\right)\right)\Bigg], \tag{17}$$

$$\phi_{SU}^{NJ} \simeq \kappa_0\Bigg[1-\left(\left(\frac{\upsilon_2}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_{13}\left(1-e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}\right)^{L-1}\left(\frac{e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}\kappa_7}{(\kappa_7+\kappa_4\psi_{j2})^2}\right)\right)-\left(1-e^{\frac{-1}{\rho_s\lambda_{sr}\left(\frac{\alpha_p}{\gamma_{th}^P}-\alpha_s-\theta_{sr}^2\right)}}\right)\Bigg]$$
$$+\left[e^{\frac{-\gamma_{th}^P}{\delta\lambda_{ps}\left(1-\theta_{ps}^2\gamma_{th}^P\right)}}\left(1-e^{\frac{-1}{\rho_s\lambda_{sr}\left(\frac{\alpha_p}{\gamma_{th}^P}-\alpha_s-\theta_{sr}^2\right)}}\right)\right]$$
$$+\kappa_1\Bigg[1-\left(\left(\frac{\upsilon_3}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_{14}\left(1-e^{\frac{-\psi_{j3}}{\kappa_8+\kappa_9\psi_{j3}}}\right)^{L-1}\left(\frac{e^{\frac{-\psi_{j3}}{\kappa_8+\kappa_9\psi_{j3}}}\kappa_8}{(\kappa_8+\kappa_9\psi_{j3})^2}\right)\right)\Bigg], \tag{18}$$

$$\phi_{PU}^{JA}(\rho_p\to\infty) \simeq 1-\Bigg[\left(\frac{\upsilon_1}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_2\left(1-e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}\times\frac{\kappa_3+\kappa_4\psi_{j1}}{\kappa_3+\kappa_5\psi_{j1}}\right)^{L-1}\frac{e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}}{\kappa_3+\kappa_5\psi_{j1}}$$
$$\times\left(\frac{\kappa_3}{\kappa_3+\kappa_4\psi_{j1}}+\frac{\kappa_3\left(\kappa_5-\kappa_4\right)}{\kappa_3+\kappa_5\psi_{j1}}\right)\Bigg], \tag{19a}$$

$$\phi_{PU}^{NJ}(\rho_p\to\infty) \simeq 1-\Bigg[\left(\frac{\upsilon_1}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_2\left(1-e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}\right)^{L-1}\times\frac{e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}\kappa_3}{(\kappa_3+\kappa_4\psi_{j1})^2}\Bigg], \tag{19b}$$

Accordingly, the SOP of SU becomes independent of ρ_p, as $\rho_p \to \infty$. These results are applicable to both JA as well as NJ cases.

4) ASYMPTOTIC SOP OF SU AS $\rho = \rho_S = \rho_J \to \infty$

Setting $\rho = \rho_s = \rho_J \to \infty$ and $\lim_{\rho_s \to \infty} e^{\frac{-x}{\rho_s}} \simeq 1$ in (17), we obtain the following result shown in (22), at the bottom of the next page, where $\kappa_{11} = \frac{\alpha_s - \varpi(\beta\alpha_p + \theta_{sr}^2)}{2^{2R_{sec,th}^{SU}}(\beta\alpha_p + \theta_{sr}^2)}$, $\kappa_{12} = \frac{1-\varpi\theta_{sr}^2}{2^{2R_{sec,th}^{SU}}\theta_{sr}^2}$.

Setting $\rho_s \to \infty$ and $\lim_{\rho_s \to \infty} e^{\frac{-x}{\rho_s}} \simeq 1$ in (18), we obtain $\phi_{SU}^{NJ}(\rho_s \to \infty) = 1$.

Proof: Refer Appendix D.

Remark 6: Notice that, as $\rho_s \to \infty$, $\phi_{SU}^{NJ} \to 1$, i.e., the SOP of SU tends to unity for the NJ case, as $\rho_s \to \infty$. In the NJ case, as ρ_s becomes higher, the SIDNR corresponding to the decoding of SR's symbol x_s at the most detrimental eavesdropper increases, which results in higher achievable data rate (i.e., corresponding to the decoding of x_s) over the eavesdropper's channel. This makes the achievable secrecy rate of SU to fall below the target secrecy rate, which ultimately leads to very high SOP for SU. On the other hand, (22) shows that ϕ_{SU}^{JA} is independent of ρ as $\rho = \rho_s = \rho_J \to \infty$ for the JA case, i.e., the SOP of SU becomes a constant, independent of ρ, as $\rho \to \infty$. In the JA case, the presence of jamming signal reduces the SIDNR at the eavesdropper. Accordingly, even though increase of ρ_s results in higher achievable data rate (i.e., corresponding to the decoding of x_s) over the eavesdropper's channel, it is equally nullified by the presence of jamming signal, as $\rho_J \to \infty$. As a result, the SOP of SU becomes independent of ρ as $\rho = \rho_s = \rho_J \to \infty$.

IV. ANALYSIS OF SYSTEM SECRECY OUTAGE PROBABILITY (SSOP)

In this section, we determine the SSOP of the considered NOMA-OCRN for the JA/NJ cases. The SSOP, which is described as the probability that either PU or SU suffers secrecy outage, is an effective metric to evaluate the PLS of the NOMA-OCRN. We define SSOP as: $\phi_{SSOP}^{y} = 1 - [(1-\phi_{PU}^{y})(1-\phi_{SU}^{y})]$; $y \epsilon (JA, NJ)$, which can be determined utilizing the SOP expressions derived earlier. Lower values of SSOP implies that both PU as well as SU suffers lower SOPs, which leads to improved PLS performance. Obviously, ϕ_{SSOP}^{JA} depends on the power allocation coefficients (PACs) for PU and SU at ST, i.e., α_p and α_s respectively. When α_p is increased such that $\alpha_p + \alpha_s = 1$, the power allocation for SU's symbol x_s is reduced which leads to higher SOP for SU. On the other hand, when α_s becomes larger, PU experiences higher SOP due to reduced power allocation at ST. Both of these events result in an elevation of the SSOP of the network. Accordingly, we determine the OPAC, i.e., α_s^* or α_p^* that minimizes the SSOP of jamming assisted NOMA-OCRN (ϕ_{SSOP}^{JA}). The optimization problem is formulated as follows:

$$\min_{\alpha_p = \alpha_p^*} \quad \phi_{SSOP}^{JA}$$
$$\text{s.t.} \quad \alpha_p + \alpha_s = 1,\ \alpha_p > \alpha_s,\ 0 < \alpha_s < 0.5\,. \tag{23}$$

Since the expression for ϕ_{SSOP}^{JA} is highly non-linear and complex, it is cumbersome to derive an analytical solution for α_p^*. On the other hand, with the help of analytical and numerical investigations, we verify that ϕ_{SSOP}^{JA} is a convex function, of α_p (details of analytical proof are omitted due to complex and long terms in the expressions).The modified Polak-Rebiere conjugate gradient method (CGM) is employed [62], [63] to determine α_p^*. Defining $\Lambda^{JA} \triangleq 1 - \left((1-\phi_{PU}^{JA})(1-\phi_{SU}^{JA})\right)$, we try to find α_p^* that minimizes Λ^{JA}. Algorithm 1 describes the steps used in CGM, where the descent direction is determined by utilizing the first derivative of the objective function. The step size Ξ_i in the i^{th} iteration is determined using the Armijo rule. In order to verify the accuracy of the findings we have calculated α_p^* using the Simulated Annealing (SA) based method as well as exhaustive search method. The details are described in Section VI.

A. SYSTEM SECRECY THROUGHPUT (SST) AND SECRECY ENERGY EFFICIENCY (SEE)

The secrecy throughput of PU and SU are respectively determined as: $\eta_{PU}^{y} = (1-\phi_{PU}^{y}) R_{sec,th}^{PU}$ and $\eta_{SU}^{y} = (1-\phi_{SU}^{y}) R_{sec,th}^{SU}$;

$$\phi_{SU}^{JA}(\rho_p \to \infty) \simeq \left[1 - \left(\left(\frac{\upsilon_2}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_{13}\left(1 - e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}} \times \frac{\kappa_7+\kappa_4\psi_{j2}}{\kappa_7+\kappa_5\psi_{j2}}\right)^{L-1}\frac{e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}}{\kappa_7+\kappa_5\psi_{j2}} \times \left(\frac{\kappa_7}{\kappa_7+\kappa_4\psi_{j2}} + \frac{\kappa_7(\kappa_5-\kappa_4)}{\kappa_7+\kappa_5\psi_{j2}}\right)\right) - \left(1 - e^{\frac{-1}{\rho_s\lambda_{sr}(\frac{\alpha_p}{\gamma_{th}^P} - \alpha_s - \theta_{sr}^2)}}\right)\right] + \left[1 - e^{\frac{-1}{\rho_s\lambda_{sr}(\frac{\alpha_p}{\gamma_{th}^P} - \alpha_s - \theta_{sr}^2)}}\right], \tag{21a}$$

$$\phi_{SU}^{NJ}(\rho_p \to \infty) \simeq \left[1 - \left(\left(\frac{\upsilon_2}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_{13}\left(1 - e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}\right)^{L-1}\frac{e^{\frac{-\psi_{j2}}{\kappa_7+\kappa_4\psi_{j2}}}}{(\kappa_7+\kappa_4\psi_{j2})^2} \times \kappa_7 - \left(1 - e^{\frac{-1}{\rho_s\lambda_{sr}(\frac{\alpha_p}{\gamma_{th}^P} - \alpha_s - \theta_{sr}^2)}}\right)\right)\right] + \left[e^{\frac{-\gamma_{th}^P}{\delta\lambda_{ps}(1-\theta_{ps}^2\gamma_{th}^P)}}\left(1 - e^{\frac{-1}{\rho_s\lambda_{sr}(\frac{\alpha_p}{\gamma_{th}^P} - \alpha_s - \theta_{sr}^2)}}\right)\right], \tag{21b}$$

Algorithm 1 : Determination of α_p^* - Conjugate Gradient Method

1) Initialization: Set index $i = 0$ and let $\epsilon_1 > 0$ be the tolerance level; choose $\alpha_p \in (0.5, 1)$;
2) Let $\Lambda^{JA} \triangleq 1 - \left(\left(1 - \phi_{PU}^{JA}\right)\left(1 - \phi_{SU}^{JA}\right)\right)$
3) Repeat
4) Set $i = i + 1$
5) Compute $\alpha_{p_{i+1}} = \left(\alpha_{p_i} + \Xi_i s_i\right)^+$
6) Set conjugate direction $s_i = \nabla\Lambda^{JA}\left(\alpha_{p_i}\right) + \lambda_i s_{i-1}$, where $\lambda_i = \frac{\nabla\Lambda^{JA}(\alpha_{p_i})[\nabla\Lambda^{JA}(\alpha_{p_i}) - \Lambda^{JA}(\alpha_{p_{(i-1)}})]}{\left\|\nabla\Lambda^{JA}\left(\alpha_{p_{(i-1)}}\right)\right\|^2}$
7) Until $\left\|\nabla\Lambda^{JA}(\alpha_{p_i})\right\| \leq \epsilon_1$

$y \in (JA, NJ)$. The SST given by $\eta^y = \eta_{PU}^y + \eta_{SU}^y$; $y \in (JA, NJ)$, is a crucial metric for evaluating the secrecy rates achieved in the network. On the other hand, an appropriate metric to combine effectively secrecy and energy is the SEE, which is defined as the ratio of achievable sum secrecy rates to the total power consumed in the network [63], [64]. Thus SEE is determined as: $S^y = \frac{R_{sec}^{PU,y} + R_{sec}^{SU,y}}{P_p + P_s + wP_J}$ where $y \in (JA, NJ)$ and $w \in (0, 1)$, i.e., $w = 1$ for JA and $w = 0$ for NJ case.

V. DNN FRAMEWORK FOR PREDICTING SOPs

This section presents a DNN framework designed for the efficient prediction of SOPs with minimal latency. This methodology is significantly different from the traditional methods for SOP evaluation, which include complex analytical modeling and time-consuming Monte-Carlo simulations.

A. DATASET CREATION AND LEARNING MODEL

The dataset utilized in this research was generated by utilizing the SOP expressions given by (14) and (17). These expressions are associated with parameters such as the transmit SNR of PU (ρ_p), transmit SNR of SU (ρ_s), secrecy threshold rates of PU and SU ($R_{sec,th}^{PU}$,$R_{sec,th}^{SU}$ respectively), target SIDNR γ_{th}^P, PACs (α_p, and δ), i-SIC coefficient (β), number of non-colluding eavesdroppers (L), and RHI (θ). The selected range of values of these parameters are listed in Table 1. The resulting dataset encompasses a total of 2×10^5 samples, with 80% designated for training and the remaining portion reserved for testing. The experiments indicate that this sample size generally produces highly accurate estimates of SOPs.

As illustrated in FIGURE 2, the DNN modeled for this scenario consists of an input layer, four hidden layers, and an output layer. The DNN operates in a feed-forward manner. The DNN for the prediction of SOP of PU has the input layer with seven neurons, which correspond to the seven parameters listed in Table1, while that corresponding to SU has nine neurons (nine parameters listed in Table 1). For performing threshold operations, the Rectified Linear Unit (ReLU) activation function is used. The ReLU function introduces non-linearity to the network and is mathematically represented as ReLU (x) = max(0, x). Here the function returns the input x if the input is greater than 0 and 0 otherwise. The best activation function for the considered DNN model is based on the estimates of root mean square error (RMSE), which is defined below.

TABLE 1. Input parameters for training and testing in DNN model.

	Input Parameters	Value
PU	ρ_p	[0 to 70]
	ρ_s	[-20 to 70]
	$R_{sec,th}^{PU}$	[0.1 to 0.4]
	γ_{th}^P	[0.1 to 0.4]
	α_p	[0.55 to 0.9]
	θ	[0.01 to 0.5]
	L	[1 to 5]
SU	ρ_p	[0 to 70]
	ρ_s	[-20 to 70]
	$R_{sec,th}^{SU}$	[0.1 to 0.4]
	γ_{th}^P	[0.1 to 0.4]
	α_p	[0.55 to 0.9]
	δ	[0.5 to 0.8]
	β	[0.1 to 0.5]
	θ	[0.01 to 0.5]
	L	[1 to 5]

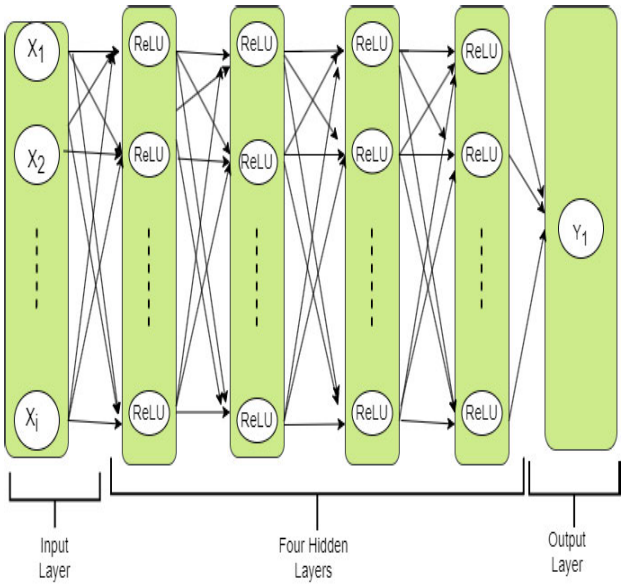

FIGURE 2. DNN architecture.

B. PROMPT SOP FORECAST

During the training phase, the neural network acquires knowledge of the input-output correlations by utilizing the

$$\phi_{SU}^{JA}(\rho \to \infty) \simeq \kappa_0\left[1 - \left(1 - \frac{\alpha_s\lambda_{se} - \kappa_{11}\lambda_{se}\theta_{se}^2}{\lambda_{Je}\kappa_{11} + \alpha_s\lambda_{se} - \kappa_{11}\lambda_{se}\theta_{se}^2}\right)^L\right] + \kappa_1\left[1 - \left(1 - \frac{\lambda_{se} - \kappa_{12}\lambda_{se}\theta_{se}^2}{\lambda_{Je}\kappa_{12} + \lambda_{se} - \kappa_{12}\lambda_{se}\theta_{se}^2}\right)^L\right], \quad (22)$$

Adam optimizer. Adam is utilized in the backpropagation process to compute and adjust the weights of the given DNN model. Let $\phi^m_{i,pred}$ and $\phi^m_{i,act}$ respectively be the predicted and the actual values of SOPs corresponding to the m^{th} data set, where $i \epsilon (PU, SU)$. A popular metric for assessing the effectiveness of a trained model is the mean square error (MSE), which is expressed as follows:

$$\text{MSE}(i) = \frac{1}{M_{test}} \sum_{m=1}^{M_{test}} (\phi^m_{i,act} - \phi^m_{i,pred})^2 \tag{24}$$

RMSE is evaluated as:

$$\text{RMSE}(i) = \sqrt{\frac{1}{M_{test}} \sum_{m=1}^{M_{test}} (\phi^m_{i,act} - \phi^m_{i,pred})^2}, \tag{25}$$

where M_{test} is the entire quantity of data in the test collection. An adept DNN excels at generating real-time predictions and can accurately estimate SOPs by processing fresh data inputs. Using this strategy, the DNN model rapidly calculates the SOP within a short duration. Additionally, the configuration of the DNN can be flexibly tuned during the training phase to reduce errors. This adaptability enables the augmentation of DNN's capability by incorporating additional hidden layers or neurons into the DNN model. We report the corresponding results in Section VI.

VI. NUMERICAL AND SIMULATION RESULTS

This section describes the results for SOPs, SSOP, SST and SEE. The analytical results were validated by performing Monte-Carlo simulations, considering 10^6 independent trials. A 2D network topology is considered, where (x_i, y_i) represents the coordinates of node i. Unless otherwise specified, we assume PT, ST, PD, SR and J to be placed at $(0, 0), (200, 0), (325, 25), (275, -25)$ and $(175, -175)$ respectively. We consider the eavesdroppers to be clustered relatively closer to each other so that they have more or less equal distances to ST, SR, PD and J [13], [41]. The link distances (normalized with respect to a reference distance $d_0 = 100$m) are given by $d_{ps} = 2$, $d_{sd} = 1.27$, $d_{sr} = 0.79$, $d_{sel} = 2.0$ and $d_{Jel} = 0.79$ (i.e., corresponding to the links $PT \rightarrow ST, ST \rightarrow PD, ST \rightarrow SR, ST \rightarrow E_l, J \rightarrow E_l$ respectively). We fix the following parameters for the SOP evaluations: $\alpha_p = 0.8$, $\alpha_s = 0.2$, $\delta = 0.7$, $R^{PU}_{sec,th} = R^{SU}_{sec,th} = 0.3$ b/s/Hz and $N = 100$ [12], [32], [65], [66]. The mean channel gains $\lambda_{ij} = \left(d_{ij}\right)^{-\mu}$, where the path loss exponent $\mu = 3$ [67]. In all the figures, 'Ana' represents the analytical results, while 'Sim' denotes the simulation results.

For implementing the proposed DNN framework, we have used the Python 3.11 environment, with four hidden layers, featuring 32, 64, 128, and 32 hidden neurons respectively, and executed it using Keras (TensorFlow 2.14.0). The training process for this DNN extended over 100 epochs, commencing with the initiation of random weight initialization facilitated by the Adam optimizer. All experiments and assessments were conducted on a computer equipped with an Intel Core i7 CPU, 32GB of RAM, and a clock speed of 3.80GHz.

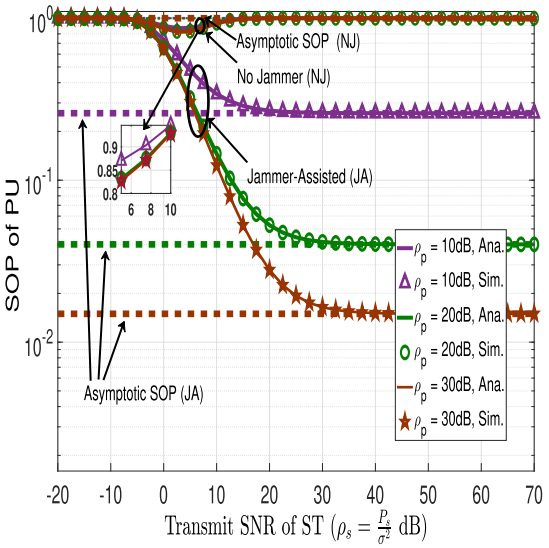

FIGURE 3. SOP of PU vs. ρ_s for distinct ρ_p.

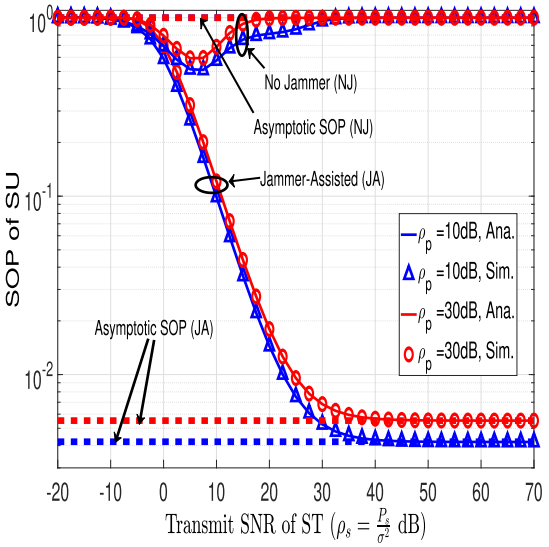

FIGURE 4. SOP of SU vs. ρ_s for distinct ρ_p ($\beta = 0.1$).

A. EVALUATION OF SOP, SST AND SEE

FIGURES 3 and 4 show the SOPs of PU and SU respectively, in NOMA-OCRN for JA/NJ cases against the transmit SNR of ST, i.e., $\rho_s = \frac{P_s}{\sigma^2}$, for distinct values of the transmit SNR of PT, i.e., $\rho_p = \frac{P_p}{\sigma^2}$. It is evident that both PU as well as SU experience significantly lower SOPs in the JA scenario. The transmission of jamming signals significantly reduces the SIDNR at the eavesdroppers, which makes the secrecy rates of both PU as well as SU to become higher so that they experience lower SOPs. Since jamming signals are absent in the NJ case, the eavesdroppers are able to successfully decode the messages intended for both PU as well as SU, which

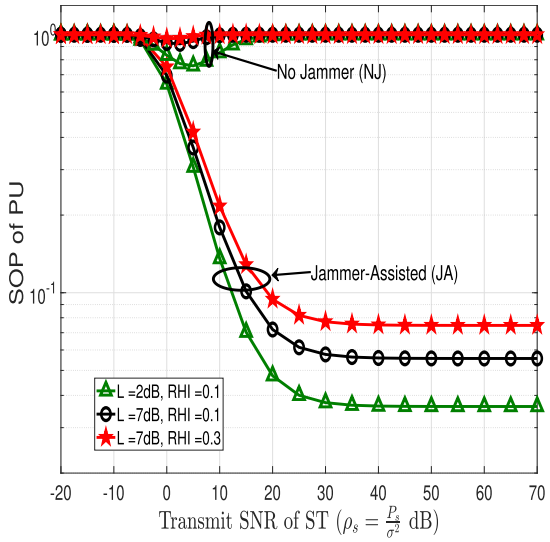

FIGURE 5. SOP of PU vs. ρ_S for distinct L and RHI ($\rho_P = 20dB$).

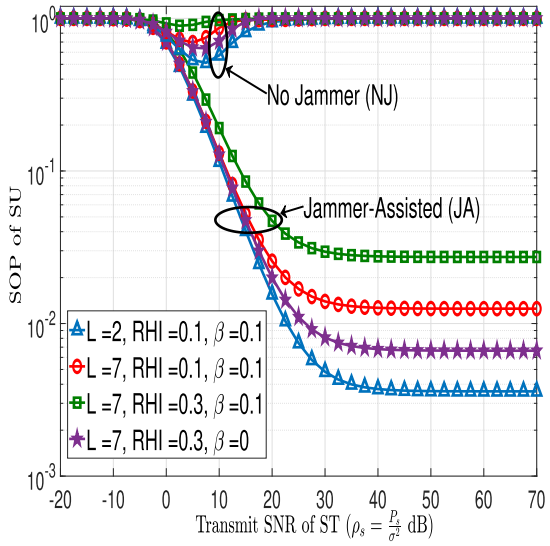

FIGURE 6. SOP of SU vs. ρ_S for distinct L, RHI, β.

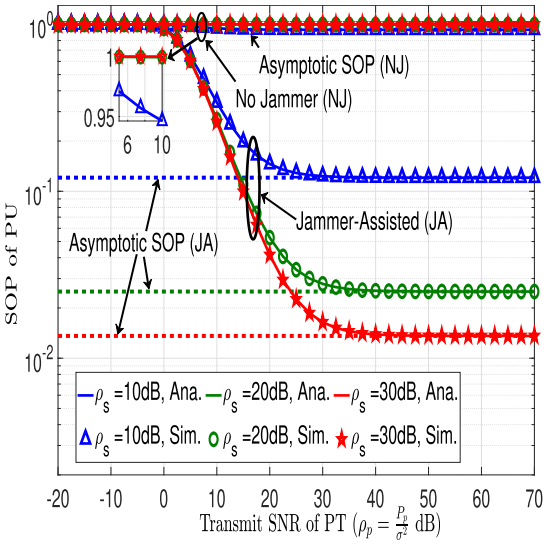

FIGURE 7. SOP of PU vs. ρ_P for distinct ρ_S.

makes their achievable secrecy rates to become lower than the corresponding target secrecy rates. As a result, both PU as well as SU experience very high SOPs. With $\rho_s = 10\,dB$ and $\rho_p = 20\,dB$, the SOP of PU is reduced by 71% while that of SU is reduced by 95% under the proposed JA framework, compared to the NJ case.

As can be seen in FIGURES 3 and 4, the SOPs of both PU and SU initially decrease as ρ_s is increased and later the SOPs saturate and become independent of ρ_s, for the JA case whereas the SOPs show an increasing trend as ρ_s becomes larger, for the NJ case. For lower values of ρ_s, the eavesdroppers fail to decode the messages intended for PU and SU, which causes the SOPs to decrease with ρ_s initially. In the NJ case, the eavesdroppers are able to successfully decode the messages, as ρ_s becomes larger, which results in degradation of the secrecy rates of PU and SU. This causes the SOPs to become very large showing an increasing trend, when ρ_s is further increased. For very high values of ρ_s, the eavesdropper's channel capacity becomes so large that the SOPs become unity and an outage floor appears for the NJ case. However, the proposed JA framework reduces the SIDNR at the most detrimental eavesdropper corresponding to the decoding of the symbols x_p and x_s. This enhances the secrecy rates of both PU as well as SU, which significantly reduces the SOPs experienced by them. However, an outage floor is also observed in the high ρ_s region for the JA case, as shown in FIGURES 3 and 4. This happens owing to the fact that, as ρ_s becomes larger, the eavesdroppers are also able to successfully decode the messages intended for PU as well as SU. At the same time, we assume that $\rho_s = \rho_J$ for the JA case in FIGURES 3 and 4 so that ρ_J tends to be very high which makes the SOPs to be independent of ρ_s. Furthermore, the proposed JA framework extends the range of values of ρ_s at which the decreasing trend of the SOP continues, as is evident from FIGURES 3 and 4. Furthermore, as shown in FIGURE 4, ρ_p has a minor influence on the SOP of SU for the entire range of values of ρ_s considered, because successful decoding of message x_s at SR does not depend on ρ_p. At the same time, an increase of ρ_p improves the SOP of PU for a selected range of ρ_s, as is evident from FIGURE 3. Increase of ρ_p will improve the successful decoding probability of x_p at ST in the first half cycle, which effectively reduces the SOP of PU, provided ρ_s is sufficient enough to ensure successful decoding of x_p at PD in the second half cycle. The asymptotic SOP results for PU as well as SU (i.e., as $\rho_s \to \infty$) are also shown in FIGURES 3 and 4 respectively, which validate the claims made in section III-C.

FIGURES 5 and 6 respectively show the SOPs of PU and SU for the JA/NJ cases against ρ_s for distinct values of L (i.e., number of eavesdroppers) and θ (i.e., RHI). Since increase of L enhances the SIDNR and the achievable rate at the most

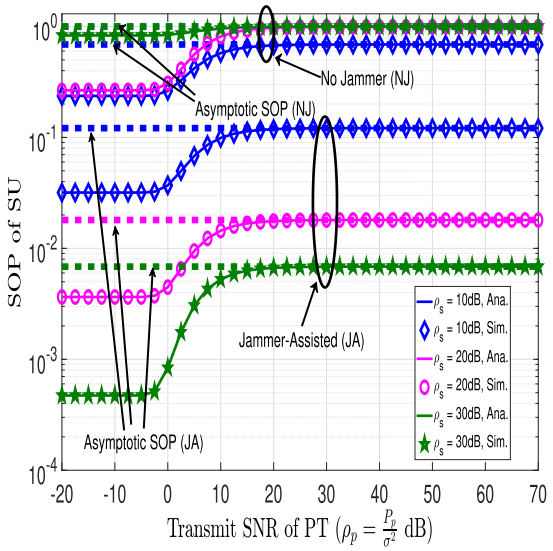

FIGURE 8. SOP of SU vs. ρ_P for distinct ρ_S ($\beta = 0.1$).

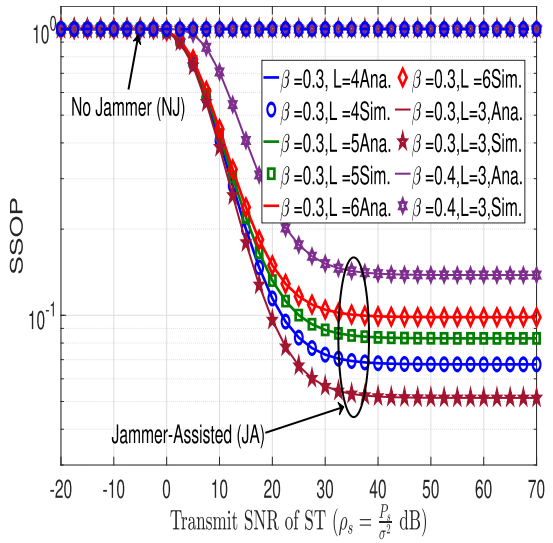

FIGURE 9. SSOP vs. ρ_S for distinct β, L ($\delta = 0.7$).

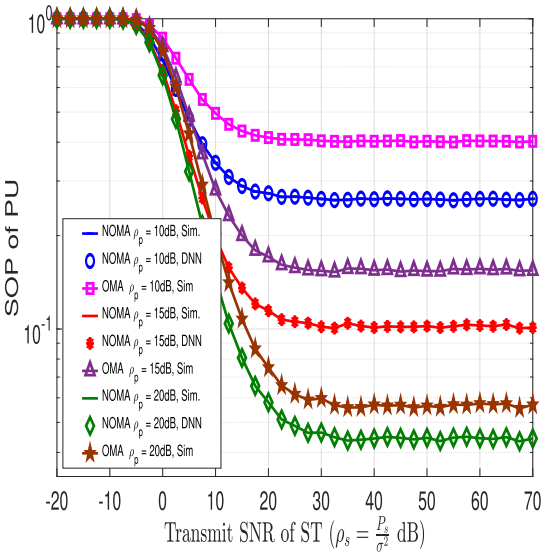

FIGURE 10. SOP of PU: NOMA-OCRN vs. OMA-OCRN.

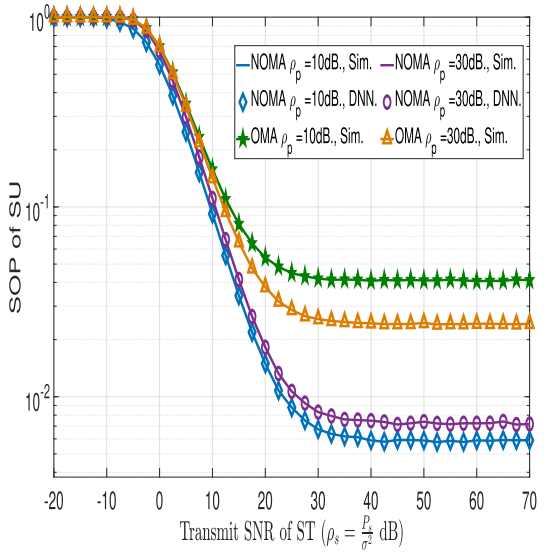

FIGURE 11. SOP of SU: NOMA-OCRN vs. OMA-OCRN ($\beta = 0.1$).

detrimental eavesdropper, both PU as well as SU experience larger SOPs, when L becomes higher. Likewise, an increase of θ will trigger the SIDNR and the achievable rate of both PU as well as SU to decrease, which makes their SOPs to be higher as θ is increased. The impact of β (i.e., i-SIC coefficient at SR) on the SOP of SU is shown in FIGURE 6 for JA/NJ cases. When β becomes larger, the SIDNR at SR corresponding to the decoding of x_s will reduce, which results in higher SOP for the SU. As can be seen, the impact of β is more predominant when ρ_s becomes larger since larger ρ_s increases the residual interference at SR due to i-SIC, which leads to significant increase of SOP.

FIGURES 7 and 8 respectively show the SOPs of PU and SU in NOMA-OCRN for the JA/NJ cases against ρ_p for distinct values of ρ_s. As can be seen in FIGURE 7, the SOP of PU initially decreases as ρ_p is increased because an increase in ρ_p ensures the successful decoding of x_p at ST so that it is forwarded to PD in the second half cycle. Thereafter, the successful decoding of x_p at PD did not depend on ρ_p. Thus, the SOP of PU becomes independent of ρ_p, when it increases. On the other hand, symbol x_s is transmitted by ST, regardless of whether x_p is successfully decoded at ST or not. When ρ_p is small, x_p may not be successfully decoded at ST, which causes ST to transmit x_s with power δP_s, where $0 < \delta < 1$. When ρ_p is increased, x_p is successfully decoded at ST which causes ST to transmit x_s with power $\alpha_s \rho_s$, where $0 < \alpha_s < 0.5$. Accordingly, the SOP of SU is largely independent of ρ_p; but depends on the transmit power allocation for x_s at ST. The asymptotic SOP results for PU as well as SU (i.e., as $\rho_p \to \infty$) are also shown in

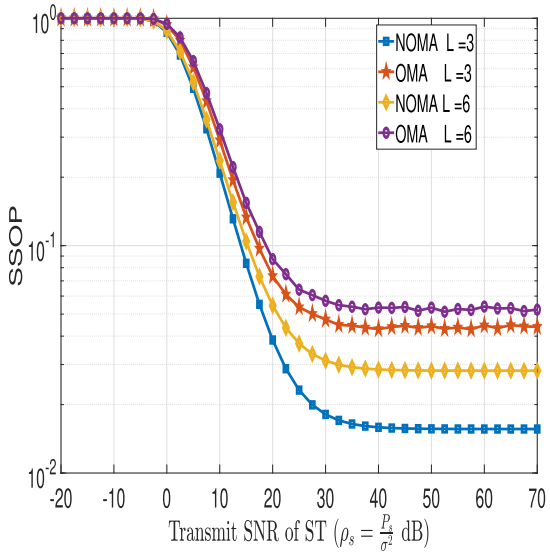

FIGURE 12. SSOP: NOMA-OCRN vs. OMA-OCRN for distinct L ($\delta = 0.7$).

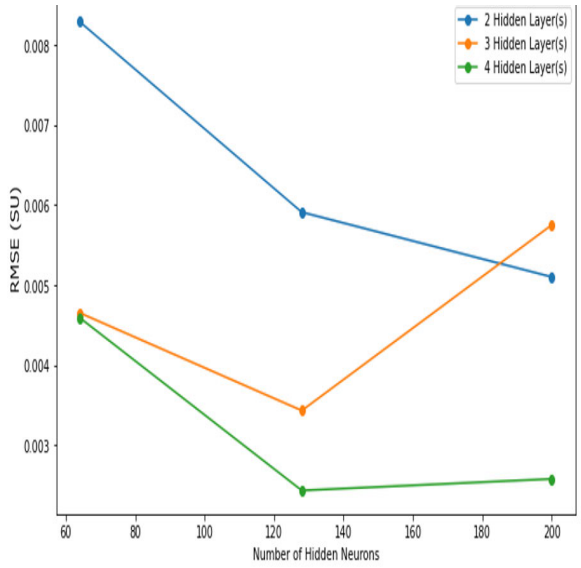

FIGURE 14. RMSE results: prediction of SOP of SU.

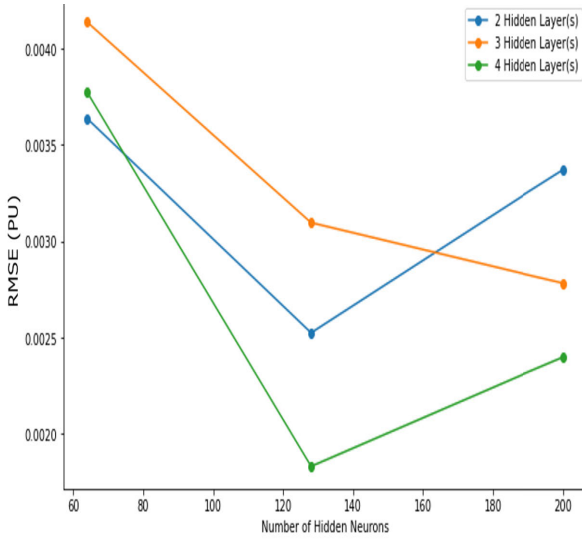

FIGURE 13. RMSE results: prediction of SOP of PU.

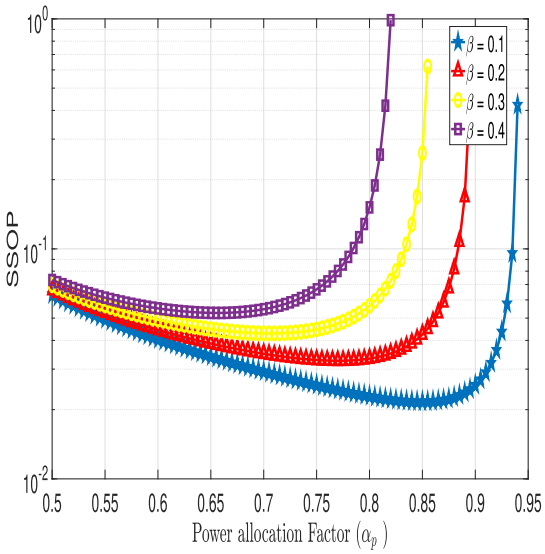

FIGURE 15. SSOP vs. α_p ($\delta = 0.7$) for distinct β.

FIGURES 7 and 8 respectively, which validate the asymptotic SOP analysis covered in Section III-C. FIGURE 9 shows the results for the SSOP against ρ_s for distinct values of L and β. It is evident that the proposed JA framework reduces SSOP whereas an increase in L or β leads to a larger SSOP.

FIGURES 10 and 11 respectively compare the SOPs experienced by PU and SU in NOMA-OCRN against that of OMA-OCRN, while FIGURE 12 shows the comparison results for the SSOP. In order to ensure a fair comparison among NOMA and OMA systems, we assume the target secrecy rates of both PU as well as SU to be the same in both systems. Further, the power allocated at PT and ST for PU's symbol and that allocated at ST for the SU's symbol are the same in both the systems considered. Recall that the transmissions in NOMA-OCRN is accomplished in two half cycles of duration $\frac{T}{2}$ each. However, when OMA-OCRN is considered, transmissions happen in three distinct slots of duration $\frac{T}{3}$ each. In the first time slot, PT will send the symbol x_p intended for PD. Assuming that ST succeeds in decoding x_p, it forwards x_p to PD during the second half cycle. Finally, ST will be sending its own symbol x_s to SR in the third half cycle. To prevent the eavesdropper from wiretapping the signal transmitted by ST, the jammer will transmit the jamming signal $x_J(t)$ with power P_J during the second and third half cycles to confound the eavesdropper. Since the considered OMA system requires more time slots to complete the transmissions, the achieved data rate for both PU as well as SU is reduced, which leads to the degradation of achieved secrecy rates as well. As a result, both PU as well

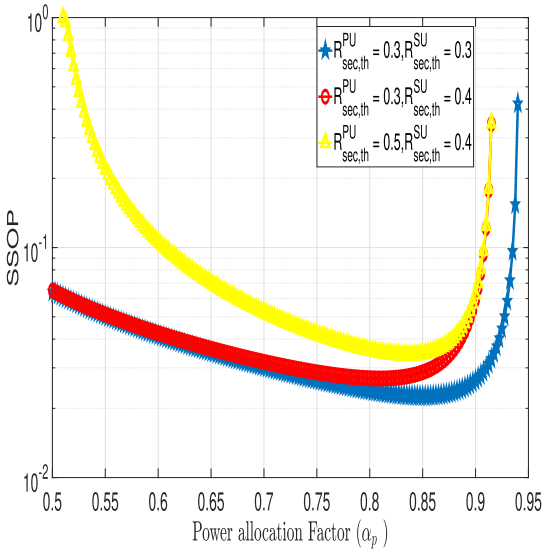

FIGURE 16. SSOP vs. α_p ($\delta = 0.7, \beta = 0.3$) distinct target secrecy rates.

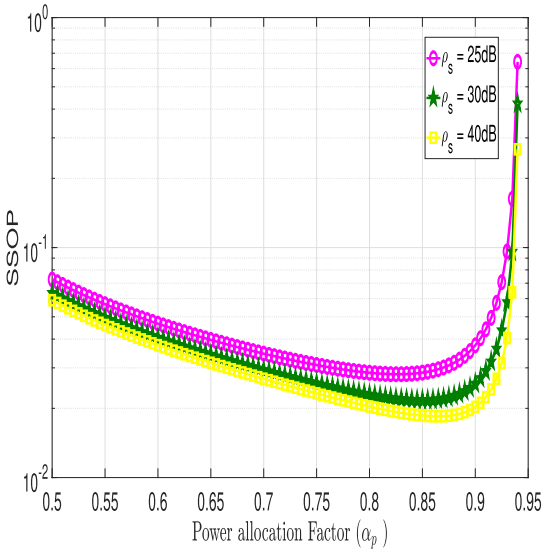

FIGURE 18. SSOP vs. α_p ($\delta = 0.7, \beta = 0.3$) for distinct ρ_s.

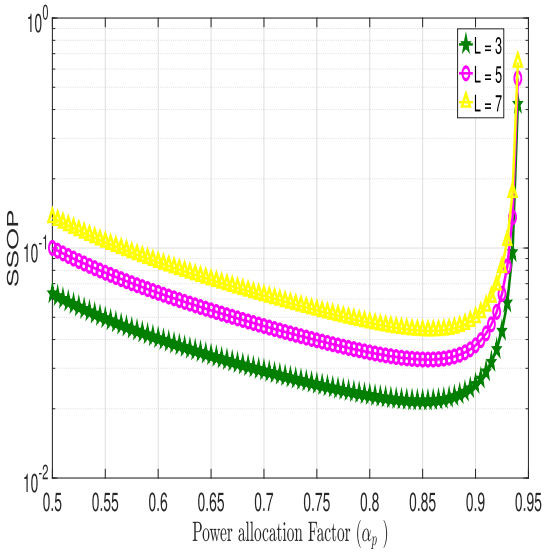

FIGURE 17. SSOP vs. α_p ($\delta = 0.7, \beta = 0.3$) for distinct L.

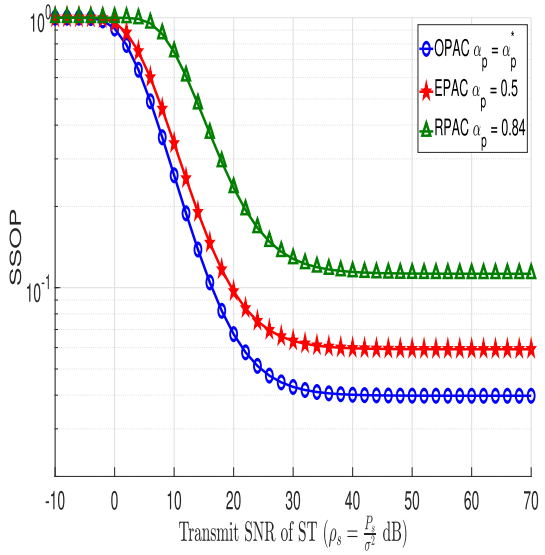

FIGURE 19. SSOP vs. ρ_s: OPAC, RPAC, EPAC ($\beta = 0.3, R^{PU}_{sec,th} = 0.3, R^{SU}_{sec,th} = 0.3$).

as SU experience higher SOP in OMA-OCRN compared to the proposed NOMA-OCRN, as is evident in FIGURES 10 and 11 respectively. Further, SSOP is higher for OMA-OCRN compared to the proposed NOMA-OCRN, as can be observed in FIGURE 12. The DNN predicted values of SOPs are also shown in FIGURES 10 and 11. It is evident that the predicted values closely match with those values obtained through analytical modeling and Monte-Carlo simulations, showcasing the superior performance of the proposed DNN framework.

FIGURES 13 and 14 show the RMSE corresponding to the prediction of SOPs of PU and SU (considering the number of hidden neurons and the number of hidden layers as variables). It is observed that, with an increase in the number of hidden layers, RMSE decreases; however increasing the number of hidden neurons beyond a limit increases the complexity of the model. Thus there should be a balance between the number of hidden layers and the number of hidden neurons to achieve the best performance. Table 2 shows the comparison of execution time for obtaining the SOPs of PU and SU using Monte-Carlo simulations and the DNN prediction method. The proposed DNN framework exhibits minimal execution time and very low RMSE, making it well-suited for real-time application scenarios.

B. EVALUATION OF OPAC (α_p^*)

Next, we determine the OPAC for PU at ST (α_p^*) that minimizes the SSOP of the jammer-assisted NOMA-OCRN. In FIGURES 15-18, we plot the SSOP against the PAC α_p,

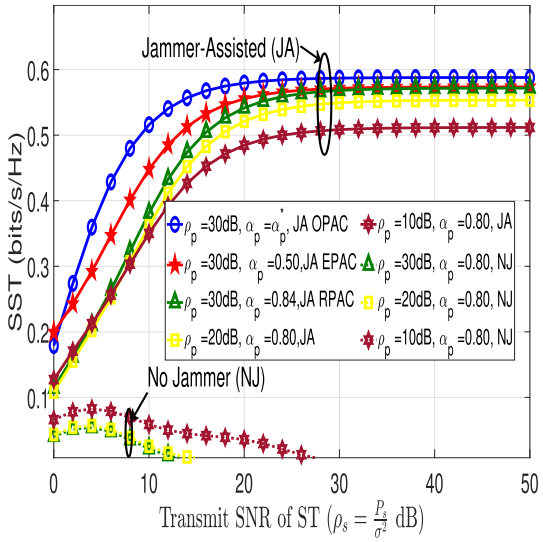

FIGURE 20. SST vs. ρ_S: OPAC, RPAC, EPAC, JA, NJ ($\beta = 0.3, R^{PU}_{sec,th} = 0.3$, $R^{SU}_{sec,th} = 0.3$).

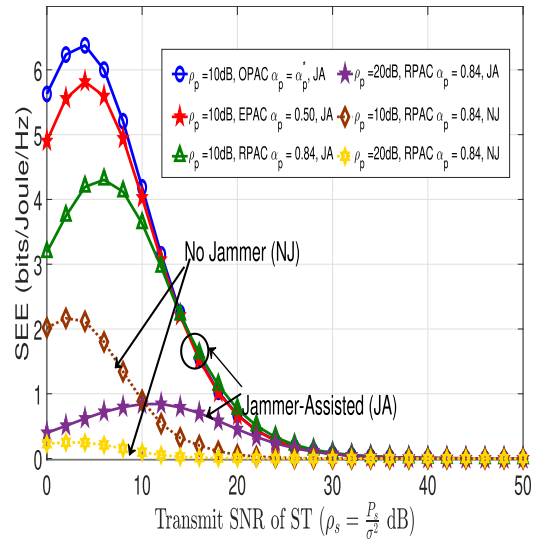

FIGURE 21. SEE vs. ρ_S: OPAC, RPAC, EPAC, JA, NJ ($\beta = 0.3, R^{PU}_{sec,th} = 0.3$, $R^{SU}_{sec,th} = 0.3$).

TABLE 2. Comparison of execution time.

Execution time (sec)		
SOP of	Monte-Carlo Simulation	DNN prediction
PU	7.8	0.031
SU	8.6	0.068

where $\alpha_p > \alpha_s$. Selecting smaller values for α_p increases the SOP of PU, while higher values of α_p will lead to higher SOP for SU. Both these cases lead to increase of SSOP. It is evident that, an optimal PAC α_p^* exists that minimizes the SSOP. The parameters β, target secrecy rates of SU and PU ($R^{SU}_{sec,th}$ and $R^{PU}_{sec,th}$ respectively), L and ρ_s are considered as variables in FIGURES 15-18 respectively. As described

TABLE 3. α_p^* for distinct β, $R^{PU}_{sec,th}$ and $R^{SU}_{sec,th}$ ($\rho_p = 30dB$, $\rho_s = 30dB$).

Target Secrecy Rate ($R^{PU}_{sec,th}$,$R^{SU}_{sec,th}$)	β	α_p^*		
		SA	CGM	ES
0.3, 0.3	0.1	0.8497	0.8497	0.8497
	0.2	0.7703	0.7705	0.7705
	0.3	0.7065	0.7065	0.7065
	0.4	0.6572	0.6563	0.6563
	0.5	0.6160	0.6168	0.6163
0.3, 0.4	0.1	0.8096	0.8096	0.8096
	0.2	0.7177	0.7177	0.7177
	0.3	0.6502	0.6500	0.6500
	0.4	0.5999	0.6001	0.6001
	0.5	0.5620	0.5621	0.5620
0.5, 0.4	0.1	0.8356	0.8356	0.8359
	0.2	0.7614	0.7607	0.7605
	0.3	0.7058	0.7059	0.7059
	0.4	0.6649	0.6650	0.6649
	0.5	0.6332	0.6332	0.6332

before, an increase of β or $R^{SU}_{sec,th}$ increases the SOP of SU, which leads to increase of SSOP. In this scenario, α_p^* shall be decreased so that the SOP of SU becomes lower, which leads to decrease of SSOP. On the other hand, an increase of $R^{PU}_{sec,th}$ leads to higher SOP for PU, which makes the SSOP to increase further. For this case, α_p^* shall be increased so that the SOP of PU becomes lower, which results in decrease of SSOP. However, we observe that α_p^* is insensitive to the changes in both L and ρ_s, as can be observed in FIGURE 17 and FIGURE 18 respectively. The numerical values for α_p^* determined by applying CGM [68] and the SA algorithm are tabulated in Table 3, where the values obtained from the exhaustive search (ES) method are also listed. It can be seen that α_p^* obtained from the proposed CGM are in close agreement with those obtained from ES and SA method. FIGURE 19 shows the SSOP evaluated for the following cases: (i) proposed OPAC ($\alpha_p = \alpha_p^*$), (ii) equal PACs-EPAC (i.e., $\alpha_p = \alpha_s = 0.5$), random PACs-RPAC ($\alpha_p = 0.84$, $\alpha_s = 0.16$). The results show that the proposed OPAC provides a significant decrease in the SSOP compared to RPAC and EPAC. With $\rho_s = 30\,dB$ and $\rho_p = 30\,dB$, the proposed OPAC provides 67% and 33% decrease of SSOP compared to RPAC and EPAC respectively. To summarize, the results have shown that careful selection of PACs at ST can lead to significant reduction of the system secrecy outage probability of the considered network.

FIGURE 20 shows SST evaluated for the three cases mentioned above, i.e., OPAC, EPAC and RPAC, considering the JA scenario, where the SST for the NJ case is also shown. The results show that the SST is significantly higher for the JA case compared to the NJ case. Further, the proposed OPAC provide additional enhancement of SST for the JA framework. With $\rho_s = 10\,dB$ and $\rho_p = 30\,dB$, the proposed OPAC provides 37% and 21% increase of SST compared to RPAC and EPAC respectively. FIGURE 21 shows the SEE evaluated for the three cases mentioned above, i.e., OPAC, EPAC and RPAC, considering the JA scenario, where the SEE for the NJ case is also shown. The results show that the SEE is

significantly higher for the JA case compared to the NJ case. Further, the proposed OPAC provide additional enhancement of SEE for the JA framework. With $\rho_p = 10\,dB$ and $\rho_s = 4\,dB$, the SEE of the jammer-assisted NOMA-OCRN is enhanced approximately by 180%, compared to the NJ case. Finally, the results of this paper have demonstrated that the proposed JA framework can significantly reduce the SOPs of both PU as well as SU, while considerably lowering the SSOP of the NOMA-OCRN. Moreover, appropriate selection of OPAC at the ST can provide further enhancement of SSOP, SST and SEE performance of the network. The findings of this paper will be crucial for the development of design guidelines for ameliorating security in future generation wireless networks.

VII. CONCLUSION

The primary objective of this paper was to evaluate the PLS performance of NOMA-OCRN in the presence of multiple non-colluding eavesdroppers and non-ideal hardware for the transceivers. Firstly, an analytical model was developed to determine the SOPs of PU and SU in NOMA-OCRN. A jamming-assisted framework was proposed for enhancing the PLS performance. Analytical models were developed to evaluate the SOPs of PU and SU for the jamming-assisted scenario as well. Further, the SST and SEE of the network were also evaluated. With the help of detailed analytical and simulation studies, it was demonstrated that the proposed jamming-assisted framework would lead to significant reduction of the SOPs of the users while considerably improving both the SST as well as SEE of the network. In the second part, OPAC for minimizing SSOP was determined. The results showed that the proposed OPAC further reduced the SOPs and SSOP significantly. Finally, a DNN framework was proposed to accurately predict the SOPs of both PU as well SU with reduced execution time. The PLS framework discussed in this article can be seamlessly investigated into cognitive IoT systems to ensure reliable and secure communications.

APPENDIX A

A. DERIVATION OF (14)

Recall the following expression for ϕ_{PU}^{JA} given by (13b):

$$\phi_{PU}^{JA} = \underbrace{\Pr(R_{sec}^{PU,JA} < R_{sec,th}^{PU}, \Gamma_{s,x_p} \geq \gamma_{th}^{P})}_{A_1} + \underbrace{\Pr(\Gamma_{s,x_p} < \gamma_{th}^{P})}_{A_2}. \tag{A.1}$$

Let $X = |h_{ps}|^2$, $Y = |h_{sd}|^2$, $Z = |h_{sr}|^2$, $U_l = |h_{se_l}|^2$ and $V_l = |h_{Je_l}|^2$. Substituting for $R_{sec}^{PU,JA}$ and Γ_{s,x_p} given by (11) and (2a) respectively in (A.1) and rearranging, A_1 becomes:

$$A_1 = \underbrace{\Pr\left(\Gamma_{d,x_p} < S_1 + b\right)}_{A_{11}} \underbrace{\Pr\left(X > \frac{\gamma_{th}^{P}}{\rho_p(1-\theta_{sp}^2\gamma_{th}^{P})}\right)}_{A_{12}}, \tag{A.2}$$

where $S_1 = 2^{2R_{sec,th}^{PU}}\Gamma_{e,x_p}^{JA}$ and $b = 2^{2R_{sec,th}^{PU}} - 1$. Substituting for Γ_{d,x_p} given by (5) in (A.2), A_{11} becomes as shown in (A.3), at the bottom of the next page. $A_{11}^{(1)}$ in (A.3) can be further simplified as:

$$A_{11}^{(1)} = \int_{s_1=0}^{\frac{\alpha_p}{\alpha_s+\theta_{sd}^2}-b} \left(1 - e^{\frac{-(s_1+b)}{\lambda_{sd}\left(\alpha_p\rho_s - \rho_s(\alpha_s+\theta_{sd}^2)(s_1+b)\right)}}\right) f_{S_1}(s_1)\, ds_1, \tag{A.4}$$

where $f_{S_1}(s_1)$ is the PDF of S_1 and $\frac{\alpha_p}{\alpha_s+\theta_{sd}^2} - b > 0$, which implies that $\alpha_p > \frac{b(1+\theta_{sd}^2)}{b+1}$. To evaluate (A.4), we determine the CDF of S_1, that is, $F_{S_1}(s_1)$, as follows:

$$\begin{aligned} F_{S_1}(s_1) &= \Pr\left[\max_{l=\{1,2,\ldots,L\}}\left(\frac{2^{2R_{sec,th}^{PU}}\alpha_p\rho_s U_l}{\theta_{se}^2 U_l\rho_s + \rho_J V_l + 1} < s_1\right)\right] \\ &= \left[\Pr\left(U_1 < \frac{s_1(\rho_J V_1 + 1)}{2^{2R_{sec,th}^{PU}}\alpha_p\rho_s - \theta_{se}^2 s_1\rho_s}\right)\right]^L. \end{aligned} \tag{A.5}$$

Noting that $U_1 \sim \exp(\lambda_{se})$ and $V_1 \sim \exp(\lambda_{Je})$ are independent random variables and $s_1 < \frac{2^{2R_{sec,th}^{PU}}\alpha_p}{\theta_{se}^2}$, $F_{S_1}(s_1)$ can be obtained as:

$$F_{S_1}(s_1) = \left(1 - \left(e^{\frac{-s_1}{\kappa_3+\kappa_4 s_1}} \times \frac{\kappa_3+\kappa_4 s_1}{\kappa_3+\kappa_5 s_1}\right)\right)^L, \tag{A.6}$$

where $\kappa_3 = 2^{2R_{sec,th}^{PU}}\alpha_p\rho_s\lambda_{se}$, $\kappa_4 = -\theta_{se}^2\rho_s\lambda_{se}$ and $\kappa_5 = \rho_J\lambda_{Je} - \theta_{se}^2\rho_s\lambda_{se}$ The PDF $f_{S_1}(s_1)$ can be obtained by differentiating (A.6) *w.r.t.* s_1 and is given by:

$$\begin{aligned} f_{S_1}(s_1) = L\left[1 - \left(e^{\frac{-s_1}{\kappa_3+\kappa_4 s_1}} \times \frac{\kappa_3+\kappa_4 s_1}{\kappa_3+\kappa_5 s_1}\right)\right]^{L-1} \frac{e^{\frac{-s_1}{\kappa_3+\kappa_4 s_1}}}{\kappa_3+\kappa_5 s_1} \\ \times \left[\frac{\kappa_3(\kappa_5-\kappa_4)}{\kappa_3+\kappa_5 s_1} + \frac{\kappa_3}{\kappa_3+\kappa_4 s_1}\right]. \end{aligned} \tag{A.7}$$

Utilizing $f_{S_1}(s_1)$ given by (A.7) in (A.4), $A_{11}^{(1)}$ can be determined as follows:

$$\begin{aligned} A_{11}^{(1)} \simeq \left(1 - \left(e^{\frac{-\upsilon_1}{\kappa_3+\kappa_4\upsilon_1}} \times \frac{\kappa_3+\kappa_4\upsilon_1}{\kappa_3+\kappa_5\upsilon_1}\right)\right)^L \\ - \int_{s_1=0}^{\upsilon_1} e^{\frac{-(s_1+b)}{\lambda_{sd}\left(\alpha_p\rho_s - \rho_s(\alpha_s+\theta_{sd}^2)(s_1+b)\right)}} f_{S_1}(s_1)\, ds_1, \end{aligned} \tag{A.8}$$

where $\upsilon_1 = \min\left(\frac{\alpha_p}{\alpha_s+\theta_{sd}^2} - b, \frac{2^{2R_{sec,th}^{PU}}\alpha_p}{\theta_{se}^2}\right)$. However we observe that it is very difficult to obtain a closed-form solution for the second term in (A.8). Accordingly, we use the Gaussian Chebyshev quadrature formula [61] to obtain an approximation for the second term in (A.8). Accordingly, $A_{11}^{(1)}$ becomes as shown in (A.9), at the bottom of the next page, where $\kappa_2 = e^{-\left(\frac{\psi_{j1}+b}{\lambda_{sd}\left(\alpha_p\rho_s - \rho_s(\alpha_s+\theta_{sd}^2)(\psi_{j1}+b)\right)}\right)}$, $\epsilon_j = \cos\left(\frac{(2j-1)\pi}{2N}\right)$, $\psi_{j1} = \left(\frac{\upsilon_1}{2}\right)(\epsilon_j + 1)$ and N is the complexity accuracy trade-off parameter in the above approximation.

utilizing $F_{S_1}(s_1)$ given by (A.6), $A_{11}^{(2)}$ in (A.3) can be simplified as:

$$A_{11}^{(2)} = 1 - \left(1 - \left(e^{\frac{-\upsilon_1}{\kappa_3+\kappa_4\upsilon_1}} \times \frac{\kappa_3+\kappa_4\upsilon_1}{\kappa_3+\kappa_5\upsilon_1}\right)\right)^L, \quad \text{(A.10)}$$

Now $A_{11} = A_{11}^{(1)} + A_{11}^{(2)}$. Since $X \sim \exp(\lambda_{ps})$, $A_{12} = e^{\frac{-\gamma_{th}^P}{\rho_p \lambda_{ps}\left(1-\theta_{ps}^2\gamma_{th}^P\right)}}$ and $A_2 = 1 - e^{\frac{-\gamma_{th}^P}{\rho_p \lambda_{ps}\left(1-\theta_{ps}^2\gamma_{th}^P\right)}}$. Utilizing the expression for A_{11}, A_{12} and A_2 in (A.1), ϕ_{PU}^{JA} given by (14) can be obtained, where $\alpha_p > \frac{b(1+\theta_{sd}^2)}{b+1}$. Otherwise $\phi_{PU}^{JA} \to 1$. This completes the proof.

APPENDIX B

A. DERIVATION OF (17)

Recall (16b) for finding ϕ_{SU}^{JA}:

$$\begin{aligned}\phi_{SU}^{JA} = &\underbrace{\Pr(R_{sec}^{SU,JA} < R_{sec,th}^{SU}, \Gamma_{s,x_p} \geq \gamma_{th}^P, \Gamma_{r,x_p} \geq \gamma_{th}^P)}_{D_1} \\ &+ \underbrace{\Pr(\Gamma_{s,x_p} \geq \gamma_{th}^P, \Gamma_{r,x_p} < \gamma_{th}^P)}_{D_2} \\ &+ \underbrace{\Pr(R_{sec}^{SU,JA} < R_{sec,th}^{SU}, \Gamma_{s,x_p} < \gamma_{th}^P)}_{D_3}. \end{aligned} \quad \text{(B.1)}$$

Substituting for $R_{sec}^{SU,JA}$ and Γ_{s,x_p} given by (12) and (2a) respectively in (B.1) and rearranging the terms, D_1 becomes:

$$\begin{aligned}D_1 = &\underbrace{\Pr(R_{sec}^{SU,JA} < R_{sec,th}^{SU} \mid \Gamma_{r,x_p} \geq \gamma_{th}^P)\Pr(\Gamma_{r,x_p} \geq \gamma_{th}^P)}_{D_{11}} \\ &\times \underbrace{\Pr(\Gamma_{s,x_p} \geq \gamma_{th}^P)}_{D_{12}}. \end{aligned} \quad \text{(B.2)}$$

D_{11} in (B.2) can be rewritten as:

$$\begin{aligned}D_{11} = &\Pr(R_{sec}^{SU,JA} < R_{sec,th}^{SU}) \\ &- \left(\left(1 - \Pr(R_{sec}^{SU,JA} > R_{sec,th}^{SU} \mid \Gamma_{r,x_p} < \gamma_{th}^P)\right)\right. \\ &\left.\times \Pr(\Gamma_{r,x_p} < \gamma_{th}^P)\right). \end{aligned} \quad \text{(B.3)}$$

At SR, the symbol x_p shall be decoded successfully before decoding x_s. So $\Pr(R_{sec}^{SU,JA} > R_{sec,th}^{SU} \mid \Gamma_{r,x_p} < \gamma_{th}^P)$=0. Accordingly, D_{11} is modified as follows:

$$D_{11} = \underbrace{\Pr(R_{sec}^{SU,JA} < R_{sec,th}^{SU})}_{D_{111}} - \underbrace{\Pr(\Gamma_{r,x_p} < \gamma_{th}^P)}_{D_{112}}. \quad \text{(B.4)}$$

Substituting for $R_{sec}^{SU,JA}$ given by (12) in (B.4) and rearranging the terms, D_{111} becomes:

$$D_{111} = \Pr\left(\Gamma_{r,x_s} < Q_1 + \varpi\right), \quad \text{(B.5)}$$

where $Q_1 = 2^{2R_{sec,th}^{SU}}\Gamma_{e_i,x_s}$ and $\varpi = 2^{2R_{sec,th}^{SU}} - 1$. Substituting for Γ_{r,x_s} given by (7) in (B.5), D_{111} becomes as shown in (B.6), at the bottom of the next page. Next, $D_{111}^{(1)}$ can be further simplified as:

$$\begin{aligned}D_{111}^{(1)} = &\int_{q_1=0}^{\frac{\alpha_s}{\beta\alpha_p+\theta_{sr}^2}-\varpi} \left(1 - e^{\frac{-(q_1+\varpi)}{\lambda_{sr}\left(\alpha_s\rho_s - \beta\rho_p(\alpha_s+\theta_{sr}^2)(q_1+\varpi)\right)}}\right) \\ &\times f_{Q_1}(q_1)\, dq_1, \end{aligned} \quad \text{(B.7)}$$

where $f_{Q_1}(q_1)$ is the pdf of Q_1 and $\frac{\alpha_s}{\beta\alpha_p+\theta_{sr}^2} - \varpi > 0$, which implies that $0 < \alpha_p < \frac{1-\varpi\theta_{se}^2}{1+\beta\varpi}$. Similar to $f_{S_1}(s_1)$ given by (A.7) in Appendix A, $f_{Q_1}(q_1)$ can be determined as:

$$\begin{aligned}f_{Q_1}(q_1) = &L\left[1 - \left(e^{\frac{-q_1}{\kappa_7+\kappa_4 q_1}} \times \frac{\kappa_7+\kappa_4 q_1}{\kappa_7+\kappa_5 q_1}\right)\right]^{L-1} \frac{e^{\frac{-q_1}{\kappa_7+\kappa_4 q_1}}}{\kappa_7+\kappa_5 q_1} \\ &\times \left[\frac{\kappa_7(\kappa_5-\kappa_4)}{\kappa_7+\kappa_5 q_1} + \frac{\kappa_7}{\kappa_7+\kappa_4 q_1}\right], \end{aligned} \quad \text{(B.8)}$$

$$\begin{aligned}A_{11} = &\underbrace{\int_{s_1=0}^{\frac{\alpha_p}{\alpha_s+\theta_{sd}^2}-b} \Pr\left(Y < \frac{(s_1+b)}{\alpha_p\rho_s - \rho_s\left(\alpha_s+\theta_{sd}^2\right)(s_1+b)}\right) f_{S_1}(s_1)\, ds_1}_{A_{11}^{(1)}} \\ &+ \underbrace{\int_{s_1=\frac{\alpha_p}{\alpha_s+\theta_{sd}^2}-b}^{\infty} \Pr\left(Y > \frac{(s_1+b)}{\alpha_p\rho_s - \rho_s\left(\alpha_s+\theta_{sd}^2\right)(s_1+b)}\right) f_{S_1}(s_1)\, ds_1}_{A_{11}^{(2)}}. \end{aligned} \quad \text{(A.3)}$$

$$\begin{aligned}A_{11}^{(1)} \simeq &\left(1 - \left(e^{\frac{-\upsilon_1}{\kappa_3+\kappa_4\upsilon_1}} \times \frac{\kappa_3+\kappa_4\upsilon_1}{\kappa_3+\kappa_5\upsilon_1}\right)\right)^L - \left(\left(\frac{\upsilon_1}{2}\right)\frac{\pi L}{N}\sum_{j=1}^{N}\sqrt{1-\epsilon_j^2}\,\kappa_2\left(1 - e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}} \times \frac{\kappa_3+\kappa_4\psi_{j1}}{\kappa_3+\kappa_5\psi_{j1}}\right)^{L-1}\right. \\ &\left.\times \frac{e^{\frac{-\psi_{j1}}{\kappa_3+\kappa_4\psi_{j1}}}}{\kappa_3+\kappa_5\psi_{j1}}\left(\frac{\kappa_3}{\kappa_3+\kappa_4\psi_{j1}} + \frac{\kappa_3(\kappa_5-\kappa_4)}{\kappa_3+\kappa_5\psi_{j1}}\right)\right), \end{aligned} \quad \text{(A.9)}$$

where $\kappa_7 = 2^{2R^{PU}_{sec,th}}\alpha_s\rho_s\lambda_{se}$. utilizing $f_{Q_1}(q_1)$ given by (B.8) in (B.7), $D^{(1)}_{111}$ can be determined as:

$$D^{(1)}_{111} \simeq \left(1-\left(e^{\frac{-\upsilon_2}{\kappa_7+\kappa_4\upsilon_2}}\times\frac{\kappa_7+\kappa_4\upsilon_2}{\kappa_7+\kappa_5\upsilon_2}\right)\right)^L - \int_{q_1=0}^{\upsilon_2}\left(e^{\frac{-(q_1+\varpi)}{\lambda_{sr}\left(\alpha_s\rho_s-\beta\rho_p(\alpha_s+\theta^2_{sr})(q_1+\varpi)\right)}}\right)f_{Q_1}(q_1)\,dq_1\,, \tag{B.9}$$

where $\upsilon_2 = \min(\frac{\alpha_s}{\beta\alpha_p+\theta^2_{sr}}-\varpi, \frac{2^{2R^{SU}_{sec,th}}\alpha_s}{\theta^2_{se}})$. We use the Gaussian Chebyshev quadrature formula [61] to get an approximation for the second term in (B.9) Accordingly, $D^{(1)}_{111}$ becomes as shown in (B.10), at the bottom of the next page, where $\kappa_{13} = e^{-\left(\frac{\psi_{j2}+\varpi}{\lambda_{sr}\left(\alpha_s\rho_s-\rho_s\left(\beta\alpha_p+\theta^2_{sr}\right)\left(\psi_{j2}+\varpi\right)\right)}\right)}$, $\epsilon_j = \cos\left(\frac{(2j-1)\pi}{2N}\right)$, $\psi_{j2} = \left(\frac{\upsilon_2}{2}\right)\left(\epsilon_j+1\right)$ and N is the complexity accuracy trade-off parameter in the above approximation. Now utilizing $f_{Q_1}(q_1)$ given by (B.8), $D^{(2)}_{111}$ in (B.6) can be simplified as:

$$D^{(2)}_{111} = 1-\left(1-\left(e^{\frac{-\upsilon_2}{\kappa_7+\kappa_4\upsilon_2}}\times\frac{\kappa_7+\kappa_4\upsilon_2}{\kappa_7+\kappa_5\upsilon_2}\right)\right)^L. \tag{B.11}$$

See that $D_{111} = D^{(1)}_{111} + D^{(2)}_{111}$ and $D_1 = (D_{111}-D_{112})\,D_{12}$, where $D_{112} = (1-e^{\frac{-1}{\rho_s\lambda_{sr}\left(\frac{\alpha^p}{\gamma^P_{th}}-\alpha_s-\theta^2_{sr}\right)}})$, $D_{12} = e^{\frac{-\gamma^P_{th}}{\rho_p\lambda_{ps}\left(1-\theta^2_{ps}\gamma^P_{th}\right)}}$.

To determine D_2, we substitute for Γ_{r,x_p} and Γ_{s,x_p} in (B.1) so that D_2 becomes:

$$D_2 = \underbrace{\left(1-e^{\frac{-1}{\rho_s\lambda_{sr}\left(\frac{\alpha^p}{\gamma^P_{th}}-\alpha_s-\theta^2_{sr}\right)}}\right)}_{D_{21}}\underbrace{\left(e^{\frac{-\gamma^P_{th}}{\delta\lambda_{ps}\left(1-\theta^2_{ps}\gamma^P_{th}\right)}}\right)}_{D_{22}}. \tag{B.12}$$

To determine D_3, we substitute for $R^{SU}_{sec,th}$ and Γ_{s,x_p} in (B.1) so that D_3 becomes:

$$D_3 = \underbrace{\Pr(R^{SU,JA}_{sec} < R^{SU}_{sec,th} \mid \Gamma_{s,x_p} < \gamma^P_{th})}_{D_{31}}\underbrace{\Pr(\Gamma_{s,x_p} < \gamma^P_{th})}_{D_{32}}. \tag{B.13}$$

Substituting for $R^{SU,JA}_{sec}$ given by (12) in (B.13) and rearranging the terms, D_{31} becomes:

$$D_{31} = \Pr\left(\Gamma_{r,x_s} < Q_2+\varpi\right), \tag{B.14}$$

where $Q_2 = 2^{2R^{SU}_{sec,th}}\Gamma_{e,x_s}$. Substituting for Γ_{r,x_s} given by (7) in (B.14), D_{31} becomes (B.15), as shown at the bottom of the next page.

Notice that $f_{Q_2}(q_2)$ can be determined similar to $f_{S_1}(s_1)$ given by (A.7) in Appendix A. Further, $D_{31} \triangleq D^{(1)}_{31}+D^{(2)}_{31}$ can be simplified similar to $D_{111} \triangleq D^{(1)}_{111}+D^{(2)}_{111}$ given by (B.6). Accordingly, $f_{Q_2}(q_2)$, $D^{(1)}_{31}$ and $D^{(1)}_{31}$ are given by (B.16), (B.17) and (B.18), respectively, as shown at the bottom of the next page, where $\kappa_8 = 2^{2R^{SU}_{sec,th}}\delta\rho_s\lambda_{se}$, $\kappa_9 = -\theta^2_{se}\delta\rho_s\lambda_{se}$, $\kappa_{10} = \rho_J\lambda_{Je} - \theta^2_{se}\delta\rho_s\lambda_{se}$ $\upsilon_3 = \min\left(\frac{1}{\theta^2_{sr}}-\varpi, \frac{2^{2R^{SU}_{sec,th}}}{\theta^2_{se}}\right)$, $\psi_{j3} = \left(\frac{\upsilon_3}{2}\right)\left(\epsilon_j+1\right)$ $\kappa_{14} = e^{-\left(\frac{\psi_{j3}+\varpi}{\lambda_{sr}\left(\delta\rho_s-\rho_s\delta\theta^2_{sr}\left(\psi_{j3}+\varpi\right)\right)}\right)}$ and N is the complexity accuracy trade-off parameter in the above approximation. Now utilizing $f_{Q_2}(q_2)$ given by (B.16), $D^{(2)}_{31}$ in (B.15) can be simplified to obtain the following expression:

$$D^{(2)}_{31} = 1-\left(1-\left(e^{\frac{-\upsilon_3}{\kappa_8+\kappa_9\upsilon_3}}\times\frac{\kappa_8+\kappa_9\upsilon_3}{\kappa_8+\kappa_{10}\upsilon_3}\right)\right)^L. \tag{B.19}$$

Notice that $D_{31} = D^{(1)}_{31} + D^{(2)}_{31}$. Since $X \sim \exp\left(\lambda_{ps}\right)$, $D_{32} = 1-e^{\frac{-\gamma^P_{th}}{\rho_p\lambda_{ps}\left(1-\theta^2_{ps}\gamma^P_{th}\right)}}$ and $D_3 = D_{31}\,D_{32}$. Utilizing the expressions for D_1, D_2 and D_3 in (B.1), ϕ^{JA}_{SU} given by (17) can be obtained, where $0 < \alpha_p < \frac{1-\varpi\theta^2_{se}}{1+\beta\varpi}$. Otherwise $\phi^{JA}_{SU} \to 1$. This completes the proof.

APPENDIX C

A. DERIVATION OF (19a)

From Appendix A, $\phi^{JA}_{PU} \triangleq A_{11}A_{12}+A_2$. As $\rho_p \to \infty, A_{12} \to 1$ and $A_2 \to 0$ so that $\phi^{JA}_{PU}(\rho_p \to \infty) = A_{11}$, which is given by (19a).

B. DERIVATION OF (19b)

In (15) as $\rho_p \to \infty$, $\kappa_0 = 1$ and $\kappa_1 = 0$ so that $\phi^{NJ}_{PU}(\rho_p \to \infty)$ is given by (19b).

C. DERIVATION OF (20)

Notice that $\phi^{JA}_{PU} \triangleq A_{11}A_{12}+A_2$ as given in Appendix A. Setting $\rho = \rho_s = \rho_J \to \infty$ in (A.2), A_{11} $(\rho \to \infty)$ can be

$$D_{111} = \underbrace{\int_{q_1=0}^{\frac{\alpha_s}{\beta\alpha_p+\theta^2_{sr}}-\varpi}\Pr\left(Z < \frac{(q_1+\varpi)}{\alpha_s\rho_s-\rho_s\left(\beta\alpha_p+\theta^2_{sr}\right)(q_1+\varpi)}\right)f_{Q_1}(q_1)\,dq_1}_{D^{(1)}_{111}} + \underbrace{\int_{q_1=\frac{\alpha_s}{\beta\alpha_p+\theta^2_{sr}}-\varpi}^{\infty}\Pr\left(Z > \frac{(q_1+\varpi)}{\alpha_s\rho_s-\rho_s\left(\beta\alpha_p+\theta^2_{sr}\right)(q_1+\varpi)}\right)f_{Q_1}(q_1)\,dq_1}_{D^{(2)}_{111}}. \tag{B.6}$$

obtained as:

$$A_{11}(\rho \to \infty) \simeq \left(1 - \left(1 - \frac{\alpha_p \lambda_{se} - \kappa_6 \lambda_{se} \theta_{se}^2}{\lambda_{Je} \kappa_6 + \alpha_p \lambda_{se} - \kappa_6 \lambda_{se} \theta_{se}^2}\right)^L\right), \tag{C.1}$$

where $\kappa_6 = \frac{\alpha_p}{\alpha_s + \theta_{sd}^2} - b$. Notice that A_{12} and A_2 which are given in Appendix A do not depend on ρ_s and ρ_J. Utilizing these expressions for A_{12} and A_2 given in Appendix A and $A_{11}(\rho \to \infty)$ given in (C.1) above, $\phi_{PU}^{JA}(\rho \to \infty)$ can be obtained as in (20). This completes the proof.

APPENDIX D

A. DERIVATION OF (21a)

In Appendix B, $\phi_{SU}^{JA} \triangleq (D_{111} - D_{112}) D_{12} + D_{21} D_{22} + D_{31} D_{32}$. As $\rho_p \to \infty$, $D_{12}, D_{22} \to 1$ and $D_3 \to 0$ so that $\phi_{SU}^{JA}(\rho_p \to \infty) = (D_{111} - D_{112}) + D_{21}$, which is given by (21a).

B. DERIVATION OF (21b)

In (18) as $\rho_p \to \infty, \kappa_0 = 1$ and $\kappa_1 = 0$ so that $\phi_{SU}^{NJ}(\rho_p \to \infty)$ is given by (21b).

C. DERIVATION OF (22)

In Appendix B, $\phi_{SU}^{JA} \triangleq (D_{111} - D_{112}) D_{12} + D_{21} D_{22} + D_{31} D_{32}$. Setting $\rho = \rho_s = \rho_J \to \infty$ in (B.4), $D_{112}(\rho \to \infty) = 0$, $D_{111}(\rho \to \infty)$ can be obtained as:

$$D_{111}(\rho \to \infty) = \left(1 - \left(1 - \frac{\alpha_s \lambda_{se} - \kappa_{11} \lambda_{se} \theta_{se}^2}{\lambda_{Je} \kappa_{11} + \alpha_s \lambda_{se} - \kappa_{11} \lambda_{se} \theta_{se}^2}\right)^L\right), \tag{D.1}$$

where $\kappa_{11} = \frac{\alpha_s - \varpi(\beta \alpha_p + \theta_{sr}^2)}{2^{2R_{sec,th}^{SU}}(\beta \alpha_p + \theta_{sr}^2)}$. Setting $\rho = \rho_s = \rho_J \to \infty$ in (B.12) and (B.14) we get $D_{21} = 0$ and D_{31} as:

$$D_{31}(\rho \to \infty) = \left(1 - \left(1 - \frac{\lambda_{se} - \kappa_{12} \lambda_{se} \theta_{se}^2}{\lambda_{Je} \kappa_{12} + \lambda_{se} - \kappa_{12} \lambda_{se} \theta_{se}^2}\right)^L\right), \tag{D.2}$$

where $\kappa_{12} = \frac{1 - \varpi \theta_{sr}^2}{2^{2R_{sec,th}^{SU}} \theta_{sr}^2}$. Note that D_{12} and D_{32} which are provided in Appendix B do not depend on ρ_s and ρ_J. Utilizing these expressions for D_{12} and D_{32} given in Appendix B and $D_{111}(\rho \to \infty)$ given in (D.1) and $D_{31}(\rho \to \infty)$ given in (D.2) above, $\phi_{SU}^{JA}(\rho \to \infty)$ can be obtained as in (22). This completes the proof.

$$D_{111}^{(1)} \simeq \left(1 - \left(e^{\frac{-\upsilon_2}{\kappa_7 + \kappa_4 \upsilon_2}} \times \frac{\kappa_7 + \kappa_4 \upsilon_2}{\kappa_7 + \kappa_5 \upsilon_2}\right)\right)^L - \left(\left(\frac{\upsilon_2}{2}\right) \times \frac{\pi L}{N} \sum_{j=1}^{N} \sqrt{1 - \epsilon_j^2}\, \kappa_{13} \left(1 - e^{\frac{-\psi_{j2}}{\kappa_7 + \kappa_4 \psi_{j2}}} \times \frac{\kappa_7 + \kappa_4 \psi_{j2}}{\kappa_7 + \kappa_5 \psi_{j2}}\right)^{L-1} \times \frac{e^{\frac{-\psi_{j2}}{\kappa_7 + \kappa_4 \psi_{j2}}}}{\kappa_7 + \kappa_5 \psi_{j2}} \left(\frac{\kappa_7}{\kappa_7 + \kappa_4 \psi_{j2}} + \frac{\kappa_7 (\kappa_5 - \kappa_4)}{\kappa_7 + \kappa_5 \psi_{j2}}\right)\right), \tag{B.10}$$

$$D_{31} = \underbrace{\int_{q_2=0}^{\frac{1}{\theta_{sr}^2} - \varpi} \Pr\left(Z < \frac{(q_2 + \varpi)}{\delta \rho_s - \rho_s \delta \theta_{sr}^2 (q_2 + \varpi)}\right) f_{Q_2}(q_2)\, dq_2}_{D_{31}^{(1)}} + \underbrace{\int_{q_2 = \frac{1}{\theta_{sr}^2} - \varpi}^{\infty} \Pr\left(Z > \frac{(q_2 + \varpi)}{\delta \rho_s - \rho_s \delta \theta_{sr}^2 (q_2 + \varpi)}\right) f_{Q_2}(q_2)\, dq_2}_{D_{31}^{(2)}}. \tag{B.15}$$

$$f_{Q_2}(q_2) = L\left[1 - \left(e^{\frac{-q_2}{\kappa_8 + \kappa_9 q_2}} \times \frac{\kappa_8 + \kappa_9 q_2}{\kappa_8 + \kappa_{10} q_2}\right)\right]^{L-1} \frac{e^{\frac{-q_2}{\kappa_8 + \kappa_9 q_2}}}{\kappa_8 + \kappa_{10} q_2} \left[\frac{\kappa_8 (\kappa_{10} - \kappa_9)}{\kappa_8 + \kappa_{10} q_2} + \frac{\kappa_8}{\kappa_8 + \kappa_9 q_2}\right], \tag{B.16}$$

$$D_{31}^{(1)} \simeq \left(1 - \left(e^{\frac{-\upsilon_3}{\kappa_8 + \kappa_9 \upsilon_3}} \times \frac{\kappa_8 + \kappa_9 \upsilon_3}{\kappa_8 + \kappa_{10} \upsilon_3}\right)\right)^L - \int_{q_2=0}^{\upsilon_3} \left(e^{\frac{-(q_2 + \varpi)}{\lambda_{sr}(\delta \rho_s - \rho_s \delta \theta_{sr}^2 (q_2 + \varpi))}}\right) f_{Q_2}(q_2)\, dq_2, \tag{B.17}$$

$$D_{31}^{(1)} \simeq \left(1 - \left(e^{\frac{-\upsilon_3}{\kappa_8 + \kappa_9 \upsilon_3}} \times \frac{\kappa_8 + \kappa_9 \upsilon_3}{\kappa_8 + \kappa_{10} \upsilon_3}\right)\right)^L - \left(\left(\frac{\upsilon_3}{2}\right) \frac{\pi L}{N} \sum_{j=1}^{N} \sqrt{1 - \epsilon_j^2}\, \kappa_{14} \left(1 - e^{\frac{-\psi_{j3}}{\kappa_8 + \kappa_9 \psi_{j3}}} \times \frac{\kappa_8 + \kappa_{10} \psi_{j3}}{\kappa_8 + \kappa_{10} \psi_{j3}}\right)^{L-1} \times \frac{e^{\frac{-\psi_{j3}}{\kappa_8 + \kappa_9 \psi_{j3}}}}{\kappa_8 + \kappa_{10} \psi_{j3}} \left(\frac{\kappa_8}{\kappa_8 + \kappa_9 \psi_{j3}} + \frac{\kappa_8 (\kappa_{10} - \kappa_9)}{\kappa_8 + \kappa_{10} \psi_{j3}}\right)\right), \tag{B.18}$$

REFERENCES

[1] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[2] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?" *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sep. 2018.

[3] S. Chen, Y. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 218–228, Apr. 2020.

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

[5] Y. Liu, W. Yi, Z. Ding, X. Liu, O. A. Dobre, and N. Al-Dhahir, "Developing NOMA to next generation multiple access: Future vision and research opportunities," *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 120–127, Dec. 2022.

[6] Y. Chen, A. Bayesteh, Y. Wu, B. Ren, S. Kang, S. Sun, Q. Xiong, C. Qian, B. Yu, Z. Ding, S. Wang, S. Han, X. Hou, H. Lin, R. Visoz, and R. Razavi, "Toward the standardization of non-orthogonal multiple access for next generation wireless networks," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 19–27, Mar. 2018.

[7] Z. Ding, H. Dai, and H. V. Poor, "Relay selection for cooperative NOMA," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 416–419, Aug. 2016.

[8] M. Vaezi, G. A. A. Baduge, Y. Liu, A. Arafa, F. Fang, and Z. Ding, "Interplay between NOMA and other emerging technologies: A survey," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 4, pp. 900–919, Dec. 2019.

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

[10] F. Li, K.-Y. Lam, X. Li, Z. Sheng, J. Hua, and L. Wang, "Advances and emerging challenges in cognitive Internet-of-Things," *IEEE Trans Ind. Informat.*, vol. 16, no. 8, pp. 5489–5496, Aug. 2020.

[11] L. Lv, J. Chen, Q. Ni, Z. Ding, and H. Jiang, "Cognitive non-orthogonal multiple access with cooperative relaying: A new wireless frontier for 5G spectrum sharing," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 188–195, Apr. 2018, doi: 10.1109/MCOM.2018.1700687.

[12] V. Aswathi and A. V. Babu, "Performance analysis of NOMA-based underlay cognitive radio networks with partial relay selection," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4615–4630, May 2021.

[13] 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.

[14] V. Singh, P. K. Upadhyay, K.-J. Lee, and D. B. da Costa, "Cooperative and cognitive hybrid satellite-terrestrial networks," in *Cognitive Radio, Mobile Communications and Wireless Networks* (EAI/Springer Innovations in Communication and Computing), M. H. Rehmani and R. Dhaou, Eds. Cham, Switzerland: Springer, 2019.

[15] V. Singh, S. Solanki, G. Eappen, R. Palisetty, T. X. Vu, J. C. Merlano-Duncan, S. Chatzinotas, and B. Ottersten, "On the performance of cache-free/cache-aided STBC-NOMA in cognitive hybrid satellite-terrestrial networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 12, pp. 2655–2659, Dec. 2022.

[16] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

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

[18] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.

[19] 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.

[20] 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.

[21] 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.

[22] Z. Xiang, W. Yang, Y. Cai, Z. Ding, and Y. Song, "Secure transmission design in HARQ assisted cognitive NOMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2528–2541, 2020.

[23] I. Budhiraja, N. Kumar, S. Tyagi, S. Tanwar, and M. S. Obaidat, "URJA: Usage jammer as a resource allocation for secure transmission in a CR-NOMA-based 5G femtocell system," *IEEE Syst. J.*, vol. 15, no. 2, pp. 1776–1785, Jun. 2021.

[24] S. Bhattacharjee, "Friendly jamming assisted secure cooperative multi-casting in cognitive radio-NOMA networks," in *Proc. IEEE Globecom Workshops*, Dec. 2019, pp. 1–6.

[25] L. Wei, T. Jing, X. Fan, Y. Wen, and Y. Huo, "The secrecy analysis over physical layer in NOMA-enabled cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[26] C. Hu, Q. Li, L. Yang, and J. Qin, "Joint power allocation and collaborative beamforming for physical layer security in underlay CR NOMA relay systems," *Phys. Commun.*, vol. 48, Oct. 2021, Art. no. 101442.

[27] M. Qin, S. Yang, H. Deng, and M. H. Lee, "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection," *IEEE Access*, vol. 6, pp. 32624–32636, 2018.

[28] 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.

[29] H.-N. Nguyen, N.-L. Nguyen, N.-T. Nguyen, A.-T. Le, N.-D. X. Ha, D.-T. Do, and M. Voznak, "Reliable and secure transmission in multiple antennas hybrid satellite-terrestrial cognitive networks relying on NOMA," *IEEE Access*, vol. 8, pp. 215044–215056, 2020.

[30] H. Li, S. Zhao, Y. Li, and C. Peng, "Sum secrecy rate maximization in NOMA-based cognitive satellite-terrestrial network," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2230–2234, Oct. 2021.

[31] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Top. Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.

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

[33] Q. Li and S. Zhao, "Robust secure beamforming design for cooperative cognitive radio nonorthogonal multiple access networks," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, Mar. 2021.

[34] M. Li, H. Yuan, C. Maple, W. Cheng, and G. Epiphaniou, "Physical layer security analysis of cognitive NOMA Internet of Things networks," *IEEE Syst. J.*, vol. 17, no. 1, pp. 1045–1055, Mar. 2023.

[35] Y. Zheng, X. Li, H. Zhang, M. D. Alshehri, S. Dang, G. Huang, and C. Zhang, "Overlay cognitive ABCom-NOMA-Based ITS: An in-depth secrecy analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2217–2228, Feb. 2023.

[36] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930–2943, 2020.

[37] C. Yu, H.-L. Ko, X. Peng, and W. Xie, "Secrecy outage performance analysis for cooperative NOMA over Nakagami-*m* channel," *IEEE Access*, vol. 7, pp. 79866–79876, 2019.

[38] G. M. da Silva, D. P. M. Osorio, and M. Latva-aho, "Imperfect jamming cancellation on NOMA networks with randomly located eavesdroppers," in *Proc. IEEE 32nd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2021, pp. 708–713.

[39] Y. Feng, Z. Yang, and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Dec. 2017, pp. 1–6.

[40] B. Zheng, M. Wen, C.-X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[41] T. M. Hoang, L. T. Dung, B. C. Nguyen, X. N. Tran, and T. Kim, "Secrecy outage performance of FD-NOMA relay system with multiple non-colluding eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12985–12997, Dec. 2021.

[42] K. Guo, K. An, F. Zhou, T. A. Tsiftsis, G. Zhang, and S. Chatzinotas, "On the secrecy performance of NOMA-based integrated satellite multiple-terrestrial relay networks with hardware impairments," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3661–3676, Apr. 2021.

[43] K. Guo, C. Dong, and K. An, "NOMA-based cognitive satellite terrestrial relay network: Secrecy performance under channel estimation errors and hardware impairments," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17334–17347, Sep. 2022.
[44] 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.
[45] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure communications in a unified non-orthogonal multiple access framework," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2163–2178, Mar. 2020.
[46] T. Schenk, *RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation*. Cham, Switzerland: Springer, 2008.
[47] E. Björnson, M. Matthaiou, and M. Debbah, "A new look at dual-hop relaying: Performance limits with hardware impairments," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4512–4525, Nov. 2013.
[48] L. Chen, A. G. Helmy, G. Yue, S. Li, and N. Al-Dhahir, "Performance analysis and compensation of joint TX/RX I/Q imbalance in differential STBC-OFDM," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6184–6200, Jul. 2017.
[49] A. A. Boulogeorgos, P. C. Sofotasios, B. Selim, S. Muhaidat, G. K. Karagiannidis, and M. Valkama, "Effects of RF impairments in communications over cascaded fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 8878–8894, Nov. 2016.
[50] N. Maletic, M. Cabarkapa, N. Neskovic, and D. Budimir, "Hardware impairments impact on fixed-gain AF relaying performance in Nakagami-*m* fading," *Electron. Lett.*, vol. 52, no. 2, pp. 121–122, Jan. 2016.
[51] V. Aswathi and A. V. Babu, "Full/half duplex cooperative NOMA under imperfect successive interference cancellation and channel state estimation errors," *IEEE Access*, vol. 7, pp. 179961–179984, 2019.
[52] G. Im and J. H. Lee, "Outage probability for cooperative NOMA systems with imperfect SIC in cognitive radio networks," *IEEE Commun. Lett.*, vol. 23, no. 4, pp. 692–695, Apr. 2019.
[53] T. Bao, J. Zhu, H.-C. Yang, and M. O. Hasna, "Secrecy outage performance of ground-to-air communications with multiple aerial eavesdroppers and its deep learning evaluation," *IEEE Wireless Commun. Lett.*, vol. 9, no. 9, pp. 1351–1355, Sep. 2020.
[54] T.-V. Nguyen, T.-N. Tran, K. Shim, T. Huynh-The, and B. An, "A deep-neural-network-based relay selection scheme in wireless-powered cognitive IoT networks," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7423–7436, May 2021.
[55] Z. Zhang, Y. Lu, Y. Huang, and P. Zhang, "Neural network-based relay selection in two-way SWIPT-enabled cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6264–6274, Jun. 2020.
[56] T.-H. Vu, T.-V. Nguyen, and S. Kim, "Wireless powered cognitive NOMA-based IoT relay networks: Performance analysis and deep learning evaluation," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3913–3929, Mar. 2022.
[57] S. Arzykulov, G. Nauryzbayev, M. S. Hashmi, A. M. Eltawil, K. M. Rabie, and S. Seilov, "Hardware- and interference-limited cognitive IoT relaying NOMA networks with imperfect SIC over generalized non-homogeneous fading channels," *IEEE Access*, vol. 8, pp. 72942–72956, 2020.
[58] 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.
[59] M. Xia and S. Aïssa, "Modeling and analysis of cooperative relaying in spectrum-sharing cellular systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9112–9122, Nov. 2016.
[60] H. Lei, R. Gao, K. Park, I. S. Ansari, K. J. Kim, and M. Alouini, "On secure downlink NOMA systems with outage constraint," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7824–7836, Dec. 2020.
[61] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.
[62] M. J. D. Powell, "Convergence properties of algorithms for nonlinear optimization," *SIAM Rev.*, vol. 28, no. 4, pp. 487–500, Dec. 1986.
[63] 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.
[64] H. Song, H. Wen, J. Tang, P.-H. Ho, and R. Zhao, "Secrecy energy efficiency maximization for distributed intelligent-reflecting-surface-assisted miso secure communications," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4462–4474, Mar. 2023.
[65] I. T. S. Sesia and M. Baker, *LTE—The UMTS Long Term Evolution: From Theory to Practice*. Hoboken, NJ, USA: Wiley, 2011.
[66] 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.
[67] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[68] D. P. Bertsekas, *Constrained Optimization and Lagrange Multiplier Methods*, 1st ed. Nashua, NH, USA: Athena Sci., 1996.

P. P. HEMA (Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the University of Kerala, India, in 2011, and the M.Tech. degree in communication engineering from the Vellore Institute of Technology, India, in 2014. She is currently pursuing the Ph.D. degree with the Electronics and Communication Department, National Institute of Technology Calicut, Calicut. She was an Assistant Professor with the Department of Electronics and Communication Engineering, Mar Baselios College of Engineering and Technology, Kerala, India, from 2014 to 2021. Her current research interests include machine learning for wireless communications, nonorthogonal multiple access, cognitive radio networks, and physical-layer security.

A. V. BABU (Senior Member, IEEE) received the Master of Engineering degree in telecommunication from the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India, in 2002, and the Ph.D. degree from the Department of Electronics and Communication Engineering, National Institute of Technology Calicut, India, in 2008. He is currently a Professor with the Department of Electronics and Communication Engineering, National Institute of Technology Calicut. He has authored or coauthored more than 100 papers in reputed international journals and conferences. His research interest includes resource allocation in wireless networks.