Received 6 April 2025; revised 30 April 2025; accepted 14 May 2025. Date of publication 16 May 2025; date of current version 3 June 2025.

Digital Object Identifier 10.1109/OJCOMS.2025.3570923

Deep Learning-Based Secrecy Performance of UAV-IRS NOMA Systems With Friendly Jamming

KAJAL YADAV [1] (Graduate Student Member, IEEE), PRABHAT K. UPADHYAY [1] (Senior Member, IEEE), JULES M. MOUALEU [2,3] (Senior Member, IEEE), AMANI A. F. OSMAN [2], AND PEDRO H. J. NARDELLI [3] (Senior Member, IEEE)

[1] Department of Electrical Engineering, Indian Institute of Technology Indore, Indore 453552, India
[2] School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg 2000, South Africa
[3] School of Energy Systems, Lappeenranta-Lahti University of Technology, 53850 Lappeenranta, Finland

CORRESPONDING AUTHOR: J. M. MOUALEU (e-mail: jules.moualeu@wits.ac.za)

This work was supported in part by the Prime Minister's Research Fellows (PMRF) Scheme under the Government of India; in part by the Research Council of Finland under Grant ECO-NEWS n.358928 and Grant X-SDEN n. 349965; and in part by the EU MSCA Project "COALESCE" under Grant 101130739.

ABSTRACT The Internet of Things (IoT) landscape is rapidly evolving driven by recent advances in key emerging technologies. In this paper, we explore the integration of the intelligent reflecting surface (IRS), non-orthogonal multiple access (NOMA), and unmanned aerial vehicle (UAV) to enhance spectral and energy efficiencies, as well as wireless connectivity in IoT applications. However, such applications are vulnerable to eavesdropping threats that can compromise both their integrity and privacy. To circumvent this, we incorporate a friendly jamming technique into the proposed UAV-borne IRS NOMA system. Moreover, we analyze the secrecy performance of the underlying system with friendly jamming by deriving analytical expressions of the and the secrecy outage probability (SOP) and the probability of strictly positive secrecy capacity. In addition, we obtain explicit and simplified expressions to approximate the SOP at high signal-to-noise ratio values and to highlight useful insights of various parameters into the system design. Subsequently, the accuracy of the proposed theoretical framework is validated through comprehensive Monte Carlo simulations. We also propose an algorithm that determines an optimal power allocation. Finally, a fully optimized deep neural network model is developed to predict the SOP under dynamic conditions. Numerical results demonstrate the efficacy of the proposed jamming-enabled system over its non-jamming counterpart. Specifically, it shows that the proposed system outperforms its non-jamming counterpart in terms of SOP by about 72%, and the runtime of the deep neural network model is 5.7 times faster than Monte Carlo simulations while maintaining a good accuracy.

INDEX TERMS Deep neural network, intelligent reflecting surface, Internet of Things, jammer, non-orthogonal multiple access, physical layer security, unmanned aerial vehicle.

I. INTRODUCTION

THE GROWING and inevitable issue of spectrum scarcity in next-generation networks has been brought to light by the proliferation of high-rate data transmission services and applications, the sharp rise in mobile traffic, and the rapid development of wireless technologies beyond the fifth generation (5G). To meet the real-time demands of the sixth generation (6G) use cases, for example, a massive amount of bandwidth is required. In light of this, it is now urgent to investigate high-frequency bands (such as terahertz bands) that will guarantee a broad spectrum with improved quality of service (QoS) [1].

Although high-frequency bands are likely to address the aforementioned spectrum scarcity problem, it remains imperative to develop key-enabling techniques that yield efficient use of the radio spectrum. To begin with, non-orthogonal multiple access (NOMA) is envisioned as a promising paradigm that not only improves spectrum efficiency, but also improves user fairness and reduces latency in wireless networks [2]. In NOMA, multiple users are accommodated simultaneously within the same time or frequency resource block, leveraging varying power levels (referred to as power-domain NOMA) or employing unique signal signatures (known as code-domain NOMA). A transmitter generates a combined signal that contains information from multiple users, each transmitting at varying power levels, following the NOMA protocol. At the receiving end, decoding is performed using successive interference cancellation (SIC) [3]. In addition, an intelligent reflecting surface (IRS) is considered a viable and cost-effective technology to address the challenges of limited network coverage commonly faced by various wireless transmission scenarios [4]. Reconfigurable surfaces are made up of an array of passive reflecting devices that can be installed on walls or building facades with the ability to reconfigure the wireless environment by adjusting radio or electromagnetic waves [5]. Finally, the unmanned aerial vehicle (UAV) technology can be used to expand the coverage area of future wireless communication networks thanks to the mobility and agility advantages of UAVs. To reap the promising benefits of the aforementioned technologies, the adoption of UAV technology in IRS-assisted NOMA systems has recently gained considerable momentum in the research community [6], [7], [8].

Meanwhile, the leakage of confidential information by unauthorized users remains an intricate challenge that must be tackled to meet the fundamental requirements of next-generation wireless networks. Despite achieving high spectral efficiency, NOMA-based systems are prone to eavesdropping threats. Specifically, unauthorized users can compromise the integrity of the shared superimposed signal among multiple users [9]. The concept of physical layer security (PLS) has recently attracted substantial attention, primarily for its effectiveness in mitigating security challenges within wireless networks and its relevance to next-generation technological advancements. Thus, the incorporation of safe beamforming, artificial noise, and specifically engineered jamming constitutes essential PLS strategies to guarantee protection. In order to safeguard wireless systems against information leakage, physical layer security has been implemented by taking advantage of the inherent unpredictability of noise and fading channels [10], [11], [12].

A. LITERATURE REVIEW

Inspired by the advantages of UAV, IRS, and NOMA,[1] a significant number of studies have investigated the potential of combining these technologies into a unified system to enhance network performance. In an effort to simultaneously bolster cellular coverage and system reliability, recent studies have explored the interplay between the IRS and NOMA technologies in wireless networks [16], [17], [18], [19]. In [16], an efficient transmission control in IRS-aided NOMA systems with finite block length was proposed. A non-convex optimization problem was formulated with the objective of maximizing the total effective capacity while ensuring the statistical delay QoS requirements are met. In [17], the authors presented a novel design for downlink IRS-assisted NOMA systems and investigated the effects of hardware impairments on the system performance. The work of [18] examined the performance of an IRS-assisted NOMA network from a physical layer security perspective. In [19], the authors proposed a novel segmented symbiotic backscatter NOMA system which integrates a simultaneous transmitting and reflecting reconfigurable intelligent surface, and provided a theoretical framework of the underlying system considering both perfect and imperfect SIC scenarios. Common to the aforementioned works is the position of the IRSs that are mounted on fixed objects (e.g., walls, building facades, etc.) leading to limited coverage area and flexibility as they need to be strategically positioned to ensure line of sight (LoS) links with the transmitter. To address this issue, the UAV technology can be used as an efficient and flexible approach to enhance network connectivity. In [20], the authors proposed a UAV-assisted powerline inspection framework with secure and time-sensitive communication and focused on ensuring a trade-off between accuracy and computational efficiency, suitable for resource-constrained UAV networks. In [21], the authors focused on application-oriented UAV communications in conjunction with edge systems. In [22], Tao et al. investigated the performance of aerial IRS (AIRS) cooperative reflection schemes in heterogeneous networks (HetNets). A novel theoretical framework was developed for the downlink coverage probability, user-association probability, and energy efficiency. In [23], the authors investigated the energy efficiency (EE) optimization in IRS-UAV communication networks with simultaneous wireless information and power transfer (SWIPT). The study focused on subchannel assignment, SIC decoding order, beamforming design, power splitting factor, and IRS discrete reflecting phase shift optimization to maximize the system EE. The proposed problem is a challenging mixed-integer nonlinear programming (MINLP) problem due to the strong coupling between parameters. It was shown that the approach significantly improves EE especially in dense networks, and that increasing the IRS reflecting elements enhances the system performance, while a higher IRS phase resolution can decrease the EE due to increased power consumption. In [24], the authors investigated active IRS-assisted UAV-relaying networks to maximize the average sum rate (ASR) for the users. The proposed system integrates an IRS on a UAV to reflect signals from a ground base station (GBS) to users via a NOMA scheme. To tackle the non-convex ASR maximization problem, the authors decomposed it into three subproblems: beamforming optimization at the GBS (solved via semidefinite relaxation), reflection matrix optimization of the AIRS, and UAV trajectory design (solved through successive convex approximation).

[1] Among the NOMA techniques, the power-domain NOMA is widely regarded in the existing literature as the most prominent one, owing to its exceptional spectral efficiency and extensive connectivity (see [13], [14], [15] and the references therein).

However, the works reported in [16], [17], [18], [19], [20], [21], [22], [23] do not simultaneously provide improved spectral and energy efficiencies as well as user fairness. In [25], the status update framework of an IRS-UAV assisted communication scheme was investigated considering an uplink power domain NOMA system. The authors formulated an optimization problem aimed at minimizing the average age of information while taking into account constraints related to the transmit power and the movement limitations of UAVs. In an effort to improve the communication for ground users, the authors in [26] studied the outage performance of an IRS-aided UAV in a NOMA downlink wireless network under Nakagami-m fading. A comparison between NOMA-based and orthogonal multiple access (OMA)-based systems showed the efficacy of the former over the latter. In [27], Singh et al. proposed a robust UAV-mounted active IRS-assisted NOMA network to enhance air-to-ground communications. The authors of [28] explored the performance of a wireless system that employs an IRS to assist in decode-and-forward communication between a low-altitude UAV and its corresponding ground control station. The authors in [29] investigated a secure multi-user UAV communication system with an IRS, taking into account hardware impairments at the transceiver and IRS. Moreover, they examined the optimization of the transmit precoding matrix, IRS phase shift matrix, and UAV trajectory to maximize the average sum secrecy rate. In [30], the performance of a NOMA-based UAV-RIS system was investigated in the presence of imperfect SIC and hardware impairments. Inspired by the challenge in deriving analytical expressions of system performance using traditional mathematical methodologies, a deep neural network (DNN) framework was developed to accurately predict the outage probability and the ergodic sum capacity in both [27] and [30].

B. MOTIVATIONS AND CONTRIBUTIONS

Despite achieving great mobility and agility, the works in [25], [26], [27], [28], [29], [30] did not address the security aspect of the UAV-IRS-aided NOMA systems. In [32], Souzani et al. investigated strategies aimed at improving the information-theoretic security of an IRS-assisted NOMA system with no direct links between the transmitter and the users. In [33], the authors focused on guaranteeing a secure multiple-input single-output (MISO)-NOMA by adopting some jamming techniques and an optimization framework for the secrecy rate. In [34], Zhang et al. investigated the deployment of an IRS to assist secure transmissions in a NOMA-based system with a robust and cost-effective beamforming design. In [35], Han et al. studied the PLS of an IRS-aided NOMA system by leveraging artificial jamming against internal and external eavesdropping attacks. Different from [32], [33], [34], [35], the work in [8] considered a covert communication in an aerial IRS-assisted NOMA system. Specifically, the authors proposed a system in which an IRS-empowered UAV relays confidential information to a legitimate user while avoiding the warden's detection.

Although the above studies considered the information-theoretic security of IRS-assisted NOMA systems, they are limited in terms of coverage area due to the fixed IRS setting leading to performance degradation in certain scenarios, especially in very dynamic environments such as disaster-stricken zones. Moreover, most reported studies rely heavily on Monte Carlo simulations that are high in computational costs. These are the research gaps our proposed work aims to partially fill by exploring the security of a mobile IRS-empowered NOMA system. Unlike [8], our work does not have covert communication capabilities and relies solely on a friendly jammer to suppress eavesdropping threats. The main contributions of this paper are summarized as follows.

- We first provide analytical expressions of the signal-to-interference-plus-noise ratio (SINR) of the proposed system model. Capitalizing on these statistical properties, we derive the closed-form expressions of key secrecy performance metrics, including the secrecy outage probability (SOP) and the probability of strictly positive secrecy capacity (SPSC), in both jamming and non-jamming scenarios.
- To obtain valuable insights into the system design, we develop explicit asymptotic expressions of the SOP in the high signal-to-noise-ratio (SNR) regime in both jamming and non-jamming scenarios. We subsequently formulate a power allocation optimization problem aimed at minimizing the SOP.
- We provide extensive Monte Carlo simulations to assess the correctness of the proposed mathematical derivations, and to demonstrate the effectiveness of the proposed system under various wireless scenarios.
- Since Monte Carlo simulations are typically resource-intensive that result in long processing times, we propose a DNN framework in an effort to circumvent this problem. This framework offers a data-driven approach that enables low-latency predictions of the system's SOP with a high degree of accuracy.

The remainder of the paper is organized as follows. Section II outlines the proposed system model, followed by the theoretical analysis of secrecy performance in Section III. The design of the DNN framework to accurately predict secrecy performance is elaborated in Section IV, while the numerical results are discussed in Section V to underscore some useful insights. Some concluding remarks are drawn in Section VI.

II. SYSTEM MODEL

As illustrated in FIGURE 1, we consider an IRS-assisted UAV relay communication network consisting of a transmitter (S), two legitimate NOMA receivers (U_1 and U_2), an IRS-UAV relay (R), an eavesdropper (E) and a friendly jammer (J). Herein, U_1 is a cell-edge user and U_2 is a cell-center user that can communicate directly with S. It is assumed that there is no direct link between S and U_1 due to the presence of

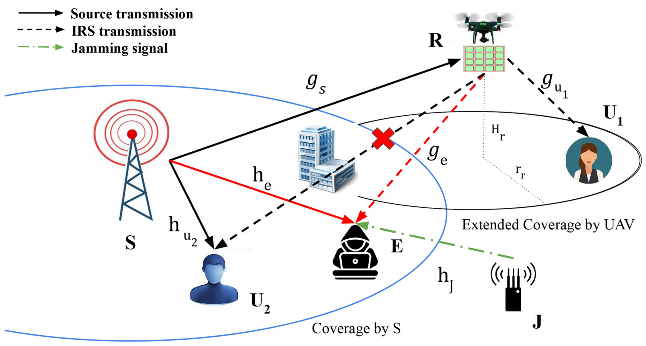


FIGURE 1. System model.

some obstacles (e.g., trees, buildings). In order to facilitate end-to-end transmissions between S and the users and in particular U_1, an IRS mounted on the UAV is employed.[2] Despite its relative small size, it is practically feasible to equip a UAV with an IRS as this has been widely adopted in the existing literature (see [22], [24], [25], [27], [30], [31] and the references therein). Since we are focusing on the theoretical underpinning of the secrecy performance, our study assumes perfect channel state information (CSI) and ideal passive beamforming to maximize the received signal power at the legitimate users.

The communication links between ground nodes and the UAV can be categorized as LoS or non-LoS, based on the prevailing environmental conditions and the angles of elevation. Consequently, the likelihood of LoS is given by

$$P_{LS}(\theta_i) = \Big(1 + \xi_i \exp\big(-\varepsilon_i(\theta_i - \xi_i)\big)\Big)^{-1}, \tag{1}$$

where the variables ξ_i and ε_i with $i \in \{s, u_1, u_2\}$, denote the environmental parameters derived from the curve fitting of the Damped Least-Squares method [37]. The corresponding path-loss coefficient is expressed as

$$\alpha_{r,i}(\theta_i) = P_{LS}(\theta_i)\Xi_i + \nu_i, \tag{2}$$

where Ξ_i and ν_i with $i \in \{s, u_1, u_2, e\}$, are constants. These constants are influenced by the conditions of the downlink and uplink environments, respectively [38]. We represent the aerial channel vector of dimension $N \times 1$ between S and R as $\mathbf{g}_s$, while the channel vectors between R, and user U_1, and between R and E are denoted by $\mathbf{g}_{u_1}$, and $\mathbf{g}_e$, respectively.

[2]Here, the IRS is typically configured to reflect the impinging signals towards the intended NOMA users, and particularly the far user. The jamming signals reflected by the IRS are not considered in this work based on the assumption that the jammer is deliberately placed far from the IRS such that the power of any reflected jamming signal is negligible in comparison to the direct jamming to the eavesdropper. In the case where the jamming signals are reflected by the IRS, authorized receivers can use interference cancellation, since they can be aware of the jamming transmissions. This will require exchange of control information between the friendly jammer and the legitimate users, such as synchronization data. The transmitter does not need to have knowledge about the jammer's CSI and transmit beamforming vector (obtaining information about the jammer channel and the transmit beamforming vector is an intricate task in practice [36]).

The eavesdropper E attempts to intercept the signals sent by the transmitter S and the UAV-relay equipped with an IRS. The purpose of the IRS is to provide a communication link between S and U_1 while improving the information-theoretic security of the overall system. While S, U_1, U_2 and E are equipped with a single antenna,[3] R equipped with the IRS, consists of N reflecting elements that can be intelligently configured and adjusted to optimize the received SINRs at the users. The diagonal phase-shift matrix of the IRS with dimension $N \times N$ is given by

$$\Phi = \mathrm{diag}\Big(\beta_1 e^{j\phi_1},\ \beta_2 e^{j\phi_2}, \ldots,\ \beta_N e^{j\phi_N}\Big), \tag{3}$$

where $\phi_n \in [0, 2\pi)$ represents the nth phase-shift variable, and $\beta_n \in (0, 1]$ denotes the nth amplitude-reflection coefficient with $\beta_n = 1$ ensuring a lossless reflection.

Furthermore, the wireless channels in our proposed aerial IRS-NOMA-based system are characterized by a Rayleigh fading model [39]. In this regard, the channel coefficients between S and the nth element of the IRS, the nth element of the IRS and U_1, S and U_2, E and J and S and E are denoted by $g_{s,n}$, $g_{u_1,n}$, h_{u_2}, h_j, and h_e, respectively, and modeled as $\mathcal{CN}(0, 1)$. The path-loss exponent for the terrestrial channels is denoted by α. The distances associated with the links S-U_2, S-E, and J-E are represented by d_{s,u_2}, $d_{s,e}$, and $d_{j,e}$, respectively.

The positions of U_1, S, U_2, E, and J are represented by 3-dimensional Cartesian coordinates, i.e., $O_{u_1} = (\mathcal{X}_{u_1}, \mathcal{Y}_{u_1}, 0)$, $O_s = (\mathcal{X}_s, \mathcal{Y}_s, 0)$, $O_{u_2} = (\mathcal{X}_{u_2}, \mathcal{Y}_{u_2}, 0)$, $O_j = (\mathcal{X}_j, \mathcal{Y}_j, 0)$, and $O_e = (\mathcal{X}_e, \mathcal{Y}_e, 0)$, respectively. The UAV is expected to travel at a steady speed such that $\mathcal{H}_r \in [\mathcal{H}_r^{\min}, \mathcal{H}_r^{\max}]$, where $\mathcal{H}_r^{\max}$ and $\mathcal{H}_r^{\min}$ are the maximum and minimum allowed altitudes, respectively. In addition, the UAV is aligned at an angle φ_r with respect to the x-axis. Consequently, the expression $O_r = (r_r \cos\varphi_r,\ r_r \sin\varphi_r,\ \mathcal{H}_r)$ can be utilized to determine the position of the UAV. The calculated elevation angles (in radians) from the ground nodes U_1, U_2, S, and E are denoted by θ_{u_1}, θ_{u_2}, θ_s, and θ_e, respectively. These angles can be obtained with the help of $\theta_i = \arctan\Big(\frac{\mathcal{H}_r}{|O_r - O_i|}\Big)$, with $i \in \{u_1, u_2, s, e\}$.

A. TRANSMISSION RATES THROUGH LEGITIMATE CHANNELS

The combined message signal $x_s = \sqrt{\delta_1 P_s} x_1 + \sqrt{\delta_2 P_s} x_2$ is broadcast by S according to the NOMA scheme. Here, x_1 and x_2 denote the unit-power signals meant for users U_1 and U_2, respectively, δ_1 and δ_2 are the corresponding power allocation coefficients such that $\delta_1 > \delta_2$ and $\delta_1 + \delta_2 = 1$, and P_s denotes the transmit power of the source.

The signal received at U_1, which is a relayed link via the UAV-IRS can be written as

[3]This assumption is realistic in practical scenarios that consist of lightweight and low-power devices. Moreover, the ensuing results represent a baseline for multi-antenna configurations that will be considered in future research studies.

$$y_{u_1} = \left(\frac{\mathbf{g}_{u_1}^H \Phi \mathbf{g}_s}{\sqrt{d_{r,s}^{\alpha_{r,s}(\theta_s)} d_{r,u_1}^{\alpha_{r,u_1}(\theta_{u_1})}}} \right) x_s + w_{u_1}, \tag{4}$$

where w_{u_1} is the additive white Gaussian noise (AWGN) at U_1 and modeled as $\mathcal{CN}(0, N_0)$. In order to optimize the power of the received signal, the phase shifts ϕ_n of the IRS can be dynamically and optimally adjusted using a controller based on precise information about the channel phases of $\mathbf{g}_s$ and $\mathbf{g}_{u_1}$ [40], [41]. The signal received at U_2 is given by

$$y_{u_2} = \left(\frac{h_{u_2}}{\sqrt{d_{s,u_2}^{\alpha}}} \right) x_s + w_{u_2}, \tag{5}$$

where w_{u_2} is the AWGN variable at U_2. The NOMA principle indicates that the message x_2 from the nearby user is perceived as interference by the remote user U_1 while decoding its message x_1. As such, the SINR at U_1 is deduced as

$$\Gamma_{u_1}^{x_1} = \frac{\delta_1\, \rho_s \left(b_1 \sum_{n=1}^{N} |g_{u_1,n}|\, |g_{s,n}| \right)^2}{\delta_2\, \rho_s \left(b_1 \sum_{n=1}^{N} |g_{u_1,n}|\, |g_{s,n}| \right)^2 + 1}, \tag{6}$$

where $g_{s,n}$ and $g_{u_1,n}$ are the nth elements of $\mathbf{g}_s$ and $\mathbf{g}_{u_1}$, respectively, and $\beta_n = \beta\, \forall\, n$ without loss of generality, $b_1 = \beta / \sqrt{d_{r,s}^{\alpha_{r,s}(\theta_s)} d_{r,u_1}^{\alpha_{r,u_1}(\theta_{u_1})}}$, and $\rho_s = \frac{P_s}{N_0}$ represents the transmit SNR. To facilitate the analysis, it is assumed that the IRS utilizes an ideal passive beamforming with perfect channel estimation, ensuring that all elements maintain a uniform reflection amplitude.

On the other hand, the signal x_1 of U_1 is decoded first at the near user U_2, and the corresponding SINR is given by

$$\Gamma_{u_2}^{x_1} = \frac{\delta_1\, \rho_s \left(a_2 |h_{u_2}| \right)^2}{\delta_2\, \rho_s \left(a_2 |h_{u_2}| \right)^2 + 1}, \tag{7}$$

where $a_2 = 1/\sqrt{d_{s,u_2}^{\alpha}}$. The probability density function (PDF) and cumulative distribution function (CDF) of the random variable (RV) $|h_{u_2}|^2$ are given respectively by

$$f_{|h_{u_2}|^2}(x) = \frac{1}{\lambda_{u_2}} e^{-\frac{x}{\lambda_{u_2}}}, \tag{8}$$

$$F_{|h_{u_2}|^2}(x) = 1 - e^{-\frac{x}{\lambda_{u_2}}}. \tag{9}$$

After a successful cancellation of the signal x_1 via SIC, U_2 is can now decode its own message x_2. As a result, the corresponding SNR is defined as

$$\Gamma_{u_2}^{x_2} = \delta_2\, \rho_s \left(a_2 |h_{u_2}| \right)^2. \tag{10}$$

It should be noted that x_1 depends on the decoding rates achieved by users U_1 and U_2, given that the signal x_1 is processed by both users based on the NOMA technique. Consequently, the rates of x_1 and x_2 are respectively given by

$$C_\ell^{x_1} = \log_2\left(1 + \min\{\Gamma_{u_1}^{x_1}, \Gamma_{u_2}^{x_1}\}\right), \tag{11}$$

$$C_\ell^{x_2} = \log_2\left(1 + \Gamma_{u_2}^{x_2}\right). \tag{12}$$

B. RATES OF TRANSMISSION OVER EAVESDROPPING CHANNELS

The eavesdropper has the ability to wiretap multiple users and is capable of performing parallel interference cancellation to distinguish between messages that overlap[4] x_1 and x_2 [43]. This ability is based on the premise that the eavesdropper has the capacity to intercept signals from both the transmitter and the UAV-IRS. In what follows, we examine two jamming-related scenarios: *without jammer* and *with jammer*.

1) WITHOUT JAMMER CASE

Combining the direct and relayed links via the UAV-IRS, the signal received at E can be expressed as

$$y_e = \left(\frac{h_e}{\sqrt{d_{s,e}^{\alpha}}} + \frac{\mathbf{g}_e^H \Phi \mathbf{g}_s}{\sqrt{d_{r,s}^{\alpha_{r,s}(\theta_s)} d_{r,e}^{\alpha_{r,e}(\theta_e)}}} \right) x_s + w_e, \tag{13}$$

where w_e is the AWGN variable at the eavesdropper. If E intercepts the message x_i from user U_i, $i \in \{1, 2\}$, the SNR is formulated as

$$\begin{aligned} \Gamma_e^{x_i} &= \delta_i \left| \sqrt{\chi_{se}} h_e + \sqrt{\chi_{sre}} \sum_{n=1}^{N} g_{e,n}\, g_{s,n} e^{j\phi_n} \right|^2 \\ &= \delta_i \Lambda_e, \end{aligned} \tag{14}$$

where $\chi_{se} = \rho_s / d_{s,e}^{\alpha}$, $\chi_{sre} = \beta\rho_s / d_{r,s}^{\alpha_{r,s}(\theta_s)} d_{r,e}^{\alpha_{r,e}(\theta_e)}$ and $g_{e,n}$ represents the nth element of $\mathbf{g}_e$. The rate of x_i across the eavesdropping channel is given by

$$C_e^{x_i} = \log_2\left(1 + \Gamma_e^{x_i}\right),\ i \in \{1, 2\}. \tag{15}$$

The central limit theorem (CLT) provides a framework to approximate the sum $\sum_{n=1}^{N} g_{e,n}\, g_{s,n} e^{j\phi_n}$ as an RV that follows a complex Gaussian distribution, as demonstrated in (14). Thus, Λ_e is governed by an exponential distribution that is characterized by the parameter $\lambda_e = (\chi_{se} + N\chi_{sre})$. Therefore, the PDF and CDF associated with Λ_e can be expressed respectively as

$$f_{\Lambda_e}(x) = \frac{1}{\lambda_e} e^{-\frac{x}{\lambda_e}}, \tag{16}$$

$$F_{\Lambda_e}(x) = 1 - e^{-\frac{x}{\lambda_e}}. \tag{17}$$

At the legitimate users U_1 and U_2, the instantaneous secrecy rates of x_1 and x_2 can be given in a compact form by

$$C_{u_i} = \max\{C_\ell^{x_i} - C_e^{x_i}, 0\},\ i \in \{1, 2\}. \tag{18}$$

2) WITH JAMMER CASE

Here, the jammer transmits an intentional interference signal x_j to confuse the eavesdropper. The signal detected at E can be characterized by a mixture of the jamming signal originating from the jammer, along with the signals transmitted via both the direct and relayed connections facilitated by the UAV-IRS, and can be expressed as

[4]For the worst case scenario, one can refer to [42].

$$y_e^J = \left(\frac{h_e}{\sqrt{d_{s,e}^{\alpha}}} + \frac{\mathbf{g}_e^H \Phi \mathbf{g}_s}{\sqrt{d_{r,s}^{\alpha_{r,s}(\theta_s)} d_{r,e}^{\alpha_{r,e}(\theta_e)}}}\right) x_s + \left(\frac{h_J}{\sqrt{d_{j,e}^{\alpha}}}\right) x_j + w_e^J. \tag{19}$$

The received SINR at E used to decode the message signal for user U_i, with $i \in \{1, 2\}$, is given by

$$\Gamma_{e,j}^{x_i} = \frac{\delta_i \Lambda_e}{\rho_j \left(a_j |h_J|\right)^2 + 1}, \tag{20}$$

where $a_j = 1/\sqrt{d_{j,e}^{\alpha}}$ and $\rho_j = \frac{P_j}{N_0}$. Subsequently, the PDF and CDF of $|h_J|^2$ can be given respectively by

$$f_{|h_J|^2}(x) = \frac{1}{\lambda_J} e^{-\frac{x}{\lambda_J}}, \tag{21}$$

$$F_{|h_J|^2}(x) = 1 - e^{-\frac{x}{\lambda_J}}. \tag{22}$$

Assuming the eavesdropping channel, the rate of x_i is given by

$$C_{e,j}^{x_i} = \log_2\left(1 + \Gamma_{e,j}^{x_i}\right), \; i \in \{1, 2\}. \tag{23}$$

The instantaneous secrecy rates at the authorised users U_1 and U_2 for x_1 and x_2 can be defined in a compact form as

$$C_{u_i,j} = \max\{C_{\ell}^{x_i} - C_{e,j}^{x_i}, 0\}, \; i \in \{1, 2\}. \tag{24}$$

Here, the SNRs at users U_1 and U_2 are unaffected by the interference signal x_j since both NOMA users are already aware of the signal jamming.

III. SECRECY PERFORMANCE ANALYSIS

This section outlines a theoretical framework for the secrecy performance of the proposed aerial IRS-assisted NOMA system, focusing on the SOP and the probability of SPSC. Furthermore, an asymptotic analysis of the SOP in the high-SNR regime is presented to elucidate the system's secrecy performance.

A. SOP EVALUATION

In the underlying system, the SOP is defined as the probability that the instantaneous secrecy rate of either one of the two NOMA users falls below a predetermined threshold secrecy rate. In what follows, we discuss the SOP performance based on the two jamming-related scenarios highlighted in the previous section.

1) WITHOUT JAMMER CASE

The SOP can be mathematically defined as

$$\begin{aligned} \text{SOP} &= \Pr\{C_{u_1} < R_{\text{th}_1} \text{ or } C_{u_2} < R_{\text{th}_2}\} \\ &= 1 - \Pr\{C_{u_1} \geq R_{\text{th}_1}, C_{u_2} \geq R_{\text{th}_2}\}, \end{aligned} \tag{25}$$

where $\Pr\{.\}$ denotes the probability operator, R_{th_1} and R_{th_2} are the predefined threshold secrecy rates for users U_1 and U_2, respectively. Using (11), (12), (15) and (18), the SOP can be evaluated as

$$\text{SOP} = 1 - \Pr\left\{\frac{1 + \min\{\Gamma_{u_1}^{x_1}, \Gamma_{u_2}^{x_1}\}}{1 + \Gamma_e^{x_1}} \geq \gamma_{\text{th}_1}, \frac{1 + \Gamma_{u_2}^{x_2}}{1 + \Gamma_e^{x_2}} \geq \gamma_{\text{th}_2}\right\}. \tag{26}$$

Both $\Gamma_e^{x_1}$ and $\Gamma_e^{x_2}$ in (26) are functions of Λ_e, which explains their correlation. In this regard, it is challenging to determine the exact closed-form representation of the SOP. To simplify the evaluation of the secrecy performance, we employ the upper bound on the SOP, as used in [42]. Based on basic statistical theory, the likelihood that two correlated events occur together is consistently less than the combined probabilities that two separate events occur independently. Hence, the SOP can be upper bounded by

$$\text{SOP} \leq \text{SOP}^{u_1} + \text{SOP}^{u_2} - \text{SOP}^{u_1}\text{SOP}^{u_2}. \tag{27}$$

Assuming perfect CSI conditions, the SOP of U_1 is given by

$$\begin{aligned} \text{SOP}^{u_1} &= \Pr\{C_{u_1} < R_{\text{th}_1}\} \\ &= 1 - \Pr\left\{\frac{1 + \min\{\Gamma_{u_1}^{x_1}, \Gamma_{u_2}^{x_1}\}}{1 + \Gamma_e^{x_1}} \geq \gamma_{\text{th}_1}\right\}, \end{aligned} \tag{28}$$

where $\gamma_{\text{th}_i} = 2^{R_{\text{th}_i}}, i \in \{1, 2\}$. Due to the complexity in evaluating a closed-form expression of the exact SOP in (28) using $\Gamma_{u_1}^{x_1}, \Gamma_{u_2}^{x_1}$ from (6)-(7), we resort to an approximation approach proposed in [43] assuming a high SNR and applying the following upper bounds $\Gamma_{u_1}^{x_1} < \frac{\delta_1}{\delta_2}$ and $\Gamma_{u_2}^{x_1} < \frac{\delta_1}{\delta_2}$. Consequently, following a series of simplifications, we get

$$\begin{aligned} \text{SOP}^{u_1} &\cong 1 - \Pr\left\{\Lambda_e \leq \frac{\varrho}{\delta_1}\right\} \\ &\cong e^{-\frac{\varrho}{\delta_1 \lambda_e}}, \end{aligned} \tag{29}$$

where $\varrho = \frac{1 - \delta_2 \gamma_{\text{th}_1}}{\delta_1 \delta_2 \gamma_{\text{th}_1}}$.

The SOP of U_2 is given by

$$\begin{aligned} \text{SOP}^{u_2} &= \Pr\{C_{u_2} < R_{\text{th}_2}\} \\ &= \Pr\left\{\frac{1 + \Gamma_{u_2}^{x_2}}{1 + \Gamma_e^{x_2}} < \gamma_{\text{th}_2}\right\}. \end{aligned} \tag{30}$$

After further simplifications, (30) can be further expressed as

$$\begin{aligned} \text{SOP}^{u_2} &= \Pr\{|h_{u_2}|^2 < \beta_1 + \beta_2 \Lambda_e\} \\ &= \int_0^{\infty} \left[F_{|h_{u_2}|^2}(\beta_1 + \beta_2 x)\right] f_{\Lambda_e}(x) dx, \end{aligned} \tag{31}$$

where $\beta_1 = \frac{\gamma_{\text{th}_2} - 1}{\delta_2 \rho_s a_2^2}$ and $\beta_2 = \frac{\gamma_{\text{th}_2}}{\rho_s a_2^2}$.

Substituting the CDF of $|h_{u_2}|^2$ from (9) and the PDF of Λ_e from (16) in (31) and after further simplifications, the SOP of U_2 yields

$$\text{SOP}^{u_2} = 1 - \frac{\lambda_{u_2}}{\beta_2 \lambda_e + \lambda_{u_2}} e^{-\frac{\beta_1}{\lambda_{u_2}}}. \tag{32}$$

2) WITH JAMMER CASE

In this scenario, the SOP can be formulated as

$$\mathrm{SOP}_J = \Pr\{C_{u_1,j} < R_{\mathrm{th}_1} \text{ or } C_{u_2,j} < R_{\mathrm{th}_2}\}. \tag{33}$$

Similarly to the case *without jammer*, it is challenging to formulate a closed-form expression for the SOP. Hence, we seek to derive an upper bound on the SOP. The expression for the SOP_J upper bound can be expressed

$$\mathrm{SOP}_J \leq \mathrm{SOP}_J^{u_1} + \mathrm{SOP}_J^{u_2} - \mathrm{SOP}_J^{u_1}\mathrm{SOP}_J^{u_2}. \tag{34}$$

The SOP of U_1 in (34) assuming perfect CSI conditions is given by

$$\begin{aligned}\mathrm{SOP}_J^{u_1} &= \Pr\{C_{u_1,j} < R_{\mathrm{th}_1}\}\\ &= 1 - \Pr\left\{\frac{1+\min\{\Gamma_{u_1}^{x_1}, \Gamma_{u_2}^{x_1}\}}{1+\Gamma_{e,j}^{x_1}} \geq \gamma_{\mathrm{th}_1}\right\}.\end{aligned} \tag{35}$$

After some mathematical manipulations, we can express (35) as

$$\begin{aligned}\mathrm{SOP}_J^{u_1} &\cong 1 - \Pr\left\{\Lambda_e \leq \alpha_1 |h_J|^2\right\}\\ &= 1 - \int_0^\infty \left[F_{\Lambda_e}(\alpha_1 y)\right] f_{|h_J|^2}(y)dy,\end{aligned} \tag{36}$$

where $\alpha_1 = \frac{\varrho_1}{\delta_1}\rho_j a_j^2$ and $\varrho_1 = \frac{1-\delta_2\gamma_{\mathrm{th}_1}}{\delta_2\gamma_{\mathrm{th}_1}}$.

After substituting the PDF of $|h_J|^2$ from (21) and the CDF of Λ_e from (17) in (36), and after further manipulations, $\mathrm{SOP}_J^{u_1}$ is given by

$$\mathrm{SOP}_J^{u_1} = \frac{\lambda_e}{\lambda_e + \alpha_1\lambda_J}. \tag{37}$$

The SOP of U_2 is given by

$$\begin{aligned}\mathrm{SOP}_J^{u_2} &= \Pr\{C_{u_2,j} < R_{\mathrm{th}_2}\}\\ &= 1 - \Pr\left\{\frac{1+\Gamma_{u_2}^{x_2}}{1+\Gamma_{e,j}^{x_2}} \geq \gamma_{\mathrm{th}_2}\right\}.\end{aligned} \tag{38}$$

After further simplifications, $\mathrm{SOP}_J^{u_2}$ is given by

$$\begin{aligned}\mathrm{SOP}_J^{u_2} &\cong 1 - \Pr\left\{\Lambda_e \leq \frac{|h_{u_2}|^2|h_J|^2}{\beta_3} - \frac{\beta_1}{\beta_3}|h_J|^2\right\}\\ &= 1 - \int_{z=0}^\infty \int_{y=\beta_1}^\infty \left[F_{\Lambda_e}\left(\frac{zy}{\beta_3} - \frac{\beta_1 z}{\beta_3}\right)\right] f_{|h_{u_2}|^2}(y)\\ &\quad\times f_{|h_J|^2}(z)dydz,\end{aligned} \tag{39}$$

where $\beta_3 = \frac{\gamma_{\mathrm{th}_2}}{\rho_s a_2^2 \rho_j a_j^2}$. After substituting the PDF of $|h_{u_2}|^2$, $|h_J|^2$ from (8) and (21) and the CDF of Λ_e from (17) in (37), and after further manipulations, $\mathrm{SOP}_J^{u_2}$ is given by

$$\mathrm{SOP}_J^{u_2} = 1 - e^{-\frac{\beta_1}{\lambda_{u_2}}} + \frac{\lambda_e\beta_3}{\lambda_{u_2}\lambda_J}\mathrm{E}_1\left(\frac{\beta_1\lambda_J + \beta_4}{\lambda_J\lambda_{u_2}}\right)e^{\frac{\beta_4}{\lambda_J\lambda_{u_2}}}, \tag{40}$$

where $\beta_4 = \lambda_e\beta_3 - \beta_1\lambda_J$ and $\mathrm{E}_1(x) = -\mathrm{Ei}(-x)$, with $\mathrm{Ei}(x)$ being the exponential integral defined in [45, eq. (8.211.1)].

B. PROBABILITY OF SPSC EVALUATION

The probability of SPSC is defined as the probability that the capacity of the main link is greater than the capacity of the wiretap link. It is a fundamental metric that is used to assess the secrecy performance of a wireless system. In what follows, we investigate this key performance metric for the two aforementioned jamming-related cases.

1) WITHOUT JAMMER CASE

The probability of SPSC is expressed mathematically as follows

$$\begin{aligned}\mathrm{SPSC} &= \Pr\{C_{u_1} \geq 0 \text{ or } C_{u_2} \geq 0\}\\ &\approx \Pr\left\{|h_{u_2}|^2 \geq \frac{\Lambda_e}{\rho_s a_2^2}, \Lambda_e \leq \frac{1}{\delta_2}\right\}.\end{aligned} \tag{41}$$

After some manipulations, (41) yields

$$\mathrm{SPSC} = \frac{\lambda_{u_2}\rho_s a_2^2}{\lambda_e + \rho_s a_2^2\lambda_{u_2}}\left(1 - e^{-\frac{\lambda_e + \rho_s a_2^2\lambda_{u_2}}{\delta_2\rho_s a_2^2\lambda_e\lambda_{u_2}}}\right). \tag{42}$$

2) WITH JAMMER CASE

Herein, the probability of SPSC can be formulated as

$$\begin{aligned}\mathrm{SPSC}_J &= \Pr\{C_{u_1,j} \geq 0 \text{ or } C_{u_2,j} \geq 0\}\\ &= \Pr\left\{\min\{\Gamma_{u_1}^{x_1}, \Gamma_{u_2}^{x_1}\} \geq \Gamma_{e,j}^{x_1}, \text{ or } \Gamma_{u_2}^{x_2} \geq \Gamma_{e,j}^{x_2}\right\}.\end{aligned} \tag{43}$$

Both $\Gamma_{e,j}^{x_1}$ and $\Gamma_{e,j}^{x_2}$ in (43) are correlated since they both are functions of $|h_J|^2$. Formulating a closed-form expression for the probability of SPSC involves a challenging and intricate analytical approach. To put it simply, we assess the performance of the system secrecy capacity in this scenario using the upper bound on the probability of SPSC. With the help of the basic statistical theory, as aforementioned in the case of the SOP, the upper bound on the probability of SPSC in (43) is further expressed as

$$\mathrm{SPSC}_J \leq \mathrm{SPSC}_J^{u_1} + \mathrm{SPSC}_J^{u_2} - \mathrm{SPSC}_J^{u_1}\mathrm{SPSC}_J^{u_2}. \tag{44}$$

The probability of SPSC that pertains to U_1 can be expressed as

$$\begin{aligned}\mathrm{SPSC}_J^{u_1} &= \Pr\left\{C_{u_1,j} \geq 0\right\}\\ &= \Pr\left\{\Lambda_e \leq \alpha_2|h_J|^2\right\}\\ &= \int_0^\infty \left[F_{\Lambda_e}(\alpha_2 y)\right] f_{|h_J|^2}(y)dy,\end{aligned} \tag{45}$$

where $\alpha_2 = \frac{\rho_j a_j^2}{\delta_2}$. After further simplifications, (45) yields

$$\mathrm{SPSC}_J^{u_1} = 1 - \frac{\lambda_e}{\alpha_2\lambda_J + \lambda_e}. \tag{46}$$

The probability of SPSC that pertains to U_2 can be expressed as

$$\begin{aligned}\mathrm{SPSC}_J^{u_2} &= \Pr\{C_{u_2,j} \geq 0\}\\ &= \Pr\{\Lambda_e \leq \alpha_3|h_{u_2}|^2|h_J|^2\}\\ &= \int_{z=0}^\infty \int_{y=0}^\infty \left[F_{\Lambda_e}(\alpha_3 yz)\right] f_{|h_{u_2}|^2}(y) f_{|h_J|^2}(z)dydz,\end{aligned} \tag{47}$$

where $\alpha_3 = \rho_j a_j^2 \rho_s a_2^2$. After further manipulations, we get

$$\mathrm{SPSC}_J^{u_2} = 1 - \frac{\lambda_e}{\lambda_{u_2}\alpha_3\lambda_J}\mathrm{E}_1\left(\frac{\lambda_e}{\alpha_3\lambda_J\lambda_{u_2}}\right)e^{\frac{\lambda_e}{\alpha_3\lambda_J\lambda_{u_2}}}. \quad (48)$$

C. ASYMPTOTIC SOP EVALUATION

In this subsection, we analyze the asymptotic behaviour of the SOP at high SNR ($\rho_s \to \infty$) to extract important insights in both jamming-related cases.

1) WITHOUT JAMMER CASE

In (29) and (32), we employ the approximation $e^{-x} \simeq 1 - x$ as $x \to 0$ to derive the asymptotic expressions for the SOP related to U_1 and U_2, respectively as follows

$$\mathrm{SOP}^{u_1,\infty} \cong 1 - \frac{\varrho}{\delta_1\lambda_e}, \quad (49)$$

$$\mathrm{SOP}^{u_2,\infty} \cong 1 - \frac{\lambda_{u_2}}{\beta_2\lambda_e + \lambda_{u_2}}\left(1 - \frac{\beta_1}{\lambda_{u_2}}\right). \quad (50)$$

2) WITH JAMMER CASE

We use the following approximations $e^{-x} \simeq 1 - x$ and $e^x \simeq 1 + x$ in (37) and (40), respectively, to get the asymptotic expressions of the SOP associated to U_1 and U_2 respectively as follows

$$\mathrm{SOP}_J^{u_1,\infty} = \frac{\lambda_e}{\lambda_e + \alpha_1\lambda_J}, \quad (51)$$

$$\mathrm{SOP}_J^{u_2,\infty} = \frac{\beta_1}{\lambda_{u_2}} + \frac{\lambda_e\beta_3}{\lambda_{u_2}\lambda_J}\mathrm{E}_1\left(\frac{\beta_1}{\lambda_{u_2}}\right)\left(1 + \frac{\beta_4}{\lambda_J\lambda_{u_2}}\right). \quad (52)$$

D. POWER ALLOCATION OPTIMIZATION

The SOP for each user can be expressed as a function of the power allocation coefficient, represented by $\mathrm{SOP}_J^{u_i}(\delta_1, \delta_2)$, where $i \in \{1, 2\}$. In what follows, we formulate and solve an optimization problem that aims to minimize the SOP of the proposed system.

$$\mathbf{P}\colon \mathrm{SOP}_J{}^* = \min_{\delta_1} \mathrm{SOP}_J(\delta_1), \quad (53)$$

$$s.t. \quad (0.5 + \epsilon) \le \delta_1 \le (1 - \epsilon), \quad \text{for } \epsilon \approx 0, \quad (54)$$

$$\delta_1 + \delta_2 = 1. \quad (55)$$

Using the derivatives of $\mathrm{SOP}_J^{u_1}$ in (37) with respect to δ_1 and $\mathrm{SOP}_J^{u_2}$ in (40) with respect to δ_1, it can be shown that $\mathrm{SOP}_J^{u_1}$ is an increasing function of δ_1 while $\mathrm{SOP}_J^{u_2}$ is a decreasing function of δ_1, as further illustrated in FIGURE 2.

After equating the aforementioned derivatives to zero, i.e., $\frac{\partial \mathrm{SOP}_J^{u_1}}{\partial \delta_1} = 0$ and $\frac{\partial \mathrm{SOP}_J^{u_2}}{\partial \delta_1} = 0$, it is challenging to obtain their closed-form solutions mainly due to the presence of several fractional terms in the high-SNR region. To this end, we introduce Algorithm 1, which offers a straightforward search method for identifying the optimal value of δ_1 with a high degree of accuracy.

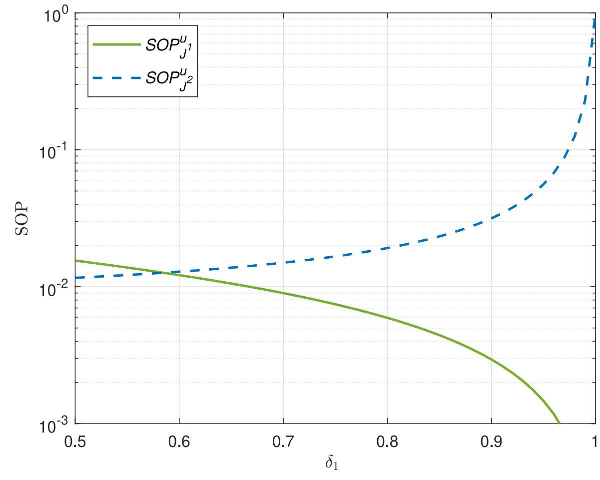


FIGURE 2. SOP of both NOMA users versus δ_1.

Algorithm 1 Optimal Power Allocation Coefficient Calculation

Input: Initialize: Optimal $\delta_1 \leftarrow 0$, min SOP $\leftarrow \infty$
for $\delta_1 \leftarrow 0.5$ **to** 1 **step** 0.01 **do**
  $\delta_2 \leftarrow 1 - \delta_1$
  Calculate $\mathrm{SOP}_J^{u_1}$ using (37) with the provided δ_1
  Calculate $\mathrm{SOP}_J^{u_2}$ using (40) with the provided δ_1
  $total\_\mathrm{SOP} \leftarrow \mathrm{SOP}_J^{u_1} + \mathrm{SOP}_J^{u_2} - \mathrm{SOP}_J^{u_1} \cdot \mathrm{SOP}_J^{u_2}$
  if *total*_SOP < min SOP **then**
    min SOP ← *total*_SOP
    Optimal $\delta_1 \leftarrow \delta_1$
  end if
end for
Output: Optimal δ_1; (Optimal power allocation coefficient)

IV. DEEP NEURAL NETWORK FRAMEWORK DESIGN

As noted in Section III, we have obtained the closed-form expressions of the upper bound on the SOP for both U_1 and U_2 of the proposed model. However, a closed-form analysis of the exact SOP is difficult to obtain due to the challenging channel conditions that are highly dynamic and intricate stemming from factors such as mobility (e.g., UAV movement), multiple reflecting surfaces, and non-LoS paths. It is worth highlighting that most future wireless communication systems are equally complex if not more complex than the underlying one, and may result in finding an approximate theoretical analysis. To address this issue, we propose a DNN framework that accurately predicts the exact SOP with less computational complexity and low latency. A conventional feed-forward DNN architecture consists of a single input layer, three intermediate hidden layers, and a final output layer. This is illustrated in FIGURE 3. The DNN framework uses pre-trained models to reduce runtime by eliminating the requirements for recurrent analytical or simulation-based computations. Dynamic and non-linear relationships in the system can be handled by DNNs, which

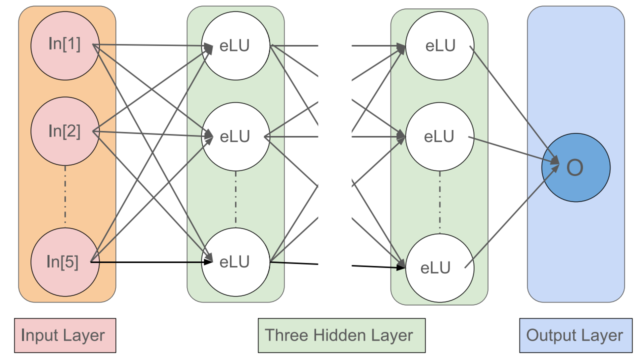


FIGURE 3. Architecture of DNN.

can adjust to changes in the system parameters and channel conditions without the need for analytical modifications.

Algorithm 2 SOP Prediction Using DNN

Input: Load dataset
Data preprocessing:
Normalize features using StandardScaler
Split dataset into training (80%) and test (20%) sets
repeat
  Adjust hyperparameters
  Compile model (Adam optimizer, MSE loss)
  Train model
  Validate using 20% of training data
  Predict SOP values on test data
  Compute MSE and RMSE
until Accuracy achieved ?
Output: Predict SOP for new inputs
Record execution time for different processes

A. DATASET GENERATION

The suggested feedforward DNN model is made up of one input layer, several hidden layers, and one output layer. Five neurons (i.e., ρ_s, R_{th_1}, δ_1, δ_2, and N) are found in the input layer. Each of the three hidden layers consists of 128 neurons, and the activation function applied to each of these neurons is the Exponential Linear Unit (eLU). Each input parameter x across all hidden layers is subjected to a threshold operation using an activation function known as eLU and given by [44]

$$\text{eLU}(x) = \begin{cases} x, & \text{if } x \geq 0, \\ \Gamma(e^x - 1) & \text{if } x < 0, \end{cases} \tag{56}$$

where the negative values are leveled up to zero, and Γ is a constant value.[5] The choice of eLU is motivated by its numerous advantages in deep learning, particularly in mitigating the vanishing-gradient problem and improving the convergence speed. Unlike the Rectified Linear Unit (ReLU) which can suffer from "dead neurons" when the inputs fall into the negative region, eLU allows small negative outputs which helps maintain activations during the backpropagation. Furthermore, eLU is particularly beneficial for regression tasks, such as the prediction of SOP in the current work, because it stabilizes gradient updates and helps the network adapt better to unseen data.

For regression problems, the single neuron in the output layer has a linear activation function. We define the mean squared error (MSE) as the loss function in the model, which makes use of the adaptive moment estimation (Adam) optimizer. For regression tasks such as SOP prediction, the feedforward DNN works well. The Adam optimizer, which dynamically adjusts learning rates and usually ensures convergence for well-conditioned problems, is used in the proposed DNN model. We have used non-simplified theoretical formulas in (28) and (31), and the simplified theoretical formulas in (29) and (32), to construct an enriched dataset for this work, that captures the effects of dynamic channel conditions with good accuracy.

To train a robust model, a variety of realistic situations based on channel models and system characteristics are simulated using random data. There might not always be access to real data, particularly for dynamic systems. Synthetic data guarantees that the DNN performs well under a wide range of scenarios. Data are generated from validated theoretical models, such as closed-form SOP expressions, to ensure its applicability. By standardizing inputs and using enough training examples to span a range of scenarios, bias is reduced, and the model is prevented from favoring specific parameter values. The following system parameters are used: SNR $\rho_s \in [-10, 40]$, target rate $R_{\text{th}_1} \in [0.05, 0.5]$, power allocation coefficients ($\delta_1 \in [0.5, 1]$), ($\delta_2 \in [0, 0.5]$), and reflecting elements $N \in [1, 40]$. Every system parameter is created consistently based on the size of the network and is used as an input variable during training.

The dataset comprises 1.2×10^6 samples, 80% of which is allocated for training purposes (D_{trn}), while the remaining 20% is evenly divided between the testing set (D_{tes}) and the validation set (D_{val}). After the training phase is completed, the model undergoes an evaluation procedure that uses the test set. Here, the model's performance is analyzed by determining key performance metrics, such as MSE and root mean squared error (RMSE). These metrics are critical for evaluating the model's predictive accuracy and its overall proficiency in delivering reliable forecasts.

B. TRAINING PROCESS FOR DNN

Algorithm 2 shows the training, testing, and prediction of the DNN model.

C. SOP REAL-TIME PREDICTION

The architecture of the DNN model consists of two primary phases: training and prediction. The neural network can efficiently learn the correlations between inputs and outputs during the training phase using the Adam optimization

[5] This is a scaling parameter used to control the saturation level of the negative values in the activation output. In this work, we set $\Gamma = 1$ (by default) to balance centering and computational efficiency.

method. The focus is to optimize a collection of parameters derived from the dataset. During the backpropagation process, the Adam optimizer is employed to compute and adjust the weights and biases of the DNN model. In the context of the dth testing dataset for the DNN model, let M^d denote the actual output values, while $\bar{M}^d$ denotes the expected output values. The following MSE loss function is given by

$$\text{Loss}\left(M^d, \bar{M}^d\right), = \frac{1}{D_{\text{tes}}} \sum_{d=1}^{D_{\text{tes}}} \left(M^d - \bar{M}^d\right)^2, \tag{57}$$

and is implemented to analyze the discrepancy between the predicted values generated by the model and the corresponding estimated values. The next step involves calculating the RMSE, which is determined using

$$\text{RMSE} = \sqrt{\frac{1}{D_{\text{tes}}} \sum_{d=1}^{D_{\text{tes}}} (M^d - \bar{M}^d)^2}, \tag{58}$$

where D_{tes} is the total sample size associated with the test set. The Adam optimization algorithm facilitates adjustment of the network's weights and biases, leading to a reduction in the MSE and an enhancement in the accuracy of the network's predictive capabilities.

D. ANALYSIS OF THE DNN MODEL'S COMPLEXITY

The complexity involved in calculating the proposed DNN model is evaluated by determining the floating-point operations per second (FLOPs), which is determined by the aggregate number of weights and biases present within the network. Let $v_{\text{in}} = 5$ denote the quantity of input variables, $v_0 = 128$ signify the number of neurons in the input layer, $v_{\text{hid}}[m] = 128$ indicate the number of neurons in the mth hidden layer, where m belongs to the set $\{1, 2, 3\}$, and $v_{\text{out}} = 1$ represent the number of neurons in the output layer. Consequently, the DNN model that was generated comprises around 50,561 parameters and 99,840 FLOPs.

E. PERFORMANCE ANALYSIS OF DNN

FIGURE 4 represents both the training and validation loss of the DNN model (measured in MSE) over multiple epochs. The x-axis represents the number of epochs, while the y-axis (log scale) shows the loss (MSE) values. This curve illustrates how the model error decreases as it learns from the training data over epochs. A consistent downward trend indicates effective learning. The validation loss curve also follows a similar downward trend. The graph suggests that the DNN is converging as both losses decrease over time. FIGURE 5 represents the distribution of prediction errors in the DNN model, comparing the actual and predicted values of the SOP performance. The majority of prediction errors are concentrated around zero, suggesting that the predictions of the DNN model are generally close to the actual values. The highest frequency occurs for small error values, indicating good overall model accuracy.

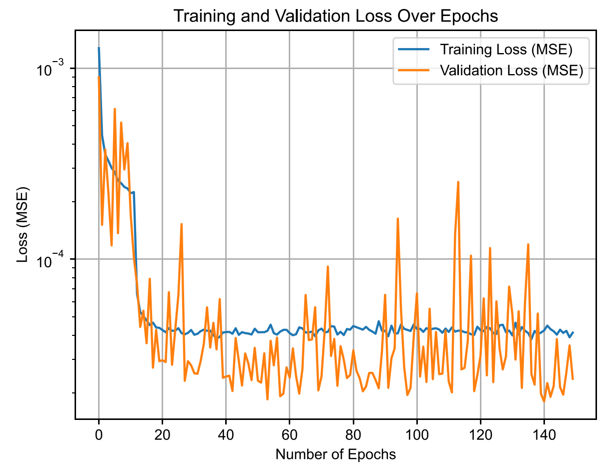


FIGURE 4. Training and validation loss over epochs.

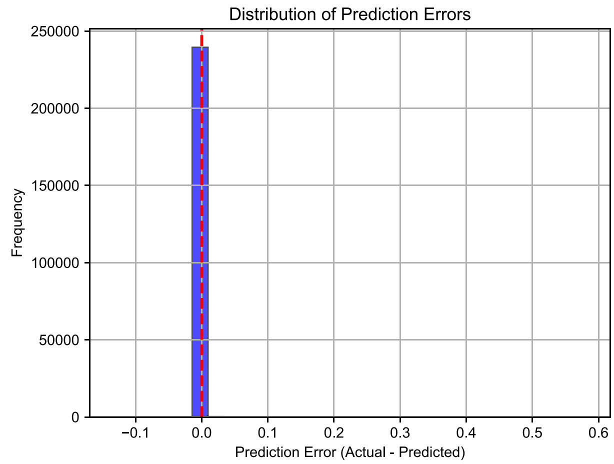


FIGURE 5. Distribution of prediction errors.

TABLE 1. Performance analysis of the DNN model.

Error Metric	Training Set	Validation Set	Test Set
MSE	4.13E-05	2.37E-05	2.01E-05
RMSE	0.006425238	0.004864984	0.004482324
MAE	0.000700995	0.000697606	0.000697606
R^2 Score	0.999830589	0.999852807	0.999852807

In what follows, we describe the outcome of Table 1 and the interpretation of the corresponding performance as follows:

1) Mean absolute error (MAE): It measures the average absolute difference between actual and predicted values.
2) R-squared (R^2) score: It indicates how well the model explains variance in the data.
3) The MSE values for training, validation, and testing are all very low ($\sim 10^{-5}$), indicating a minimal prediction error. A lower MSE indicates a better fit of the model.
4) The RMSE values for training, validation, and test sets are close to each other and very low, further indicating high accuracy.

5) The MAE values across all datasets are very small (∼0.0007), indicating that the predictions are close to the actual values. Unlike the MSE, it does not square the errors, making it less sensitive to outliers.
6) The R^2-score values used for training, validation, and test sets are all ∼0.9998, suggesting that the model explains nearly all the variance in the data. A value close to 1 indicates an excellent fit.
7) The low values of the MSE, RMSE, and MAE indicate that the model is highly accurate in predicting the SOP performance.
8) The R^2-score values close to 1 confirm that the model captures the relationship between inputs and outputs very well.
9) The low RMSE and high R^2-score suggest that the model parameters and hyperparameters (such as learning rate, number of layers, and activation functions) have been appropriately chosen.
10) The consistency of error metrics across the training, validation, and test sets suggests that the model generalizes well and is not merely memorizing the training data.
11) The validation and test errors are slightly lower than the training error, which suggests that the model is not overfitting. If the validation error was significantly higher than the training error, it would indicate overfitting. However, this is not observed in the table.

V. NUMERICAL RESULTS

In this section, the accuracy of the proposed theoretical framework is validated through Monte Carlo simulations. Without loss of generality, the following parameters are used unless otherwise specified $O_s = (-3, 0, 0)$, $O_{u_1} = (3.3, 0, 0)$, $O_{u_2} = (-1.1, -0.4, 0)$, $O_e = (1.3, 1.7, 0)$, $O_j = (2.3, 1.7, 0)$ $\mathcal{H}_r = 0.1$ km, $r_r = 0.3$ km, $\varphi_r = 0$, and $\alpha = 2.0$. Similar to [37], we have also considered $\xi_i = 2.0$, $\varepsilon_i = 0.5$, $\Xi_i = -1.5$ and $\nu_i = 4$ with $i \in \{s, u_1, u_2\}$. In addition, we define the parameter for a lossless reflection as $\beta = 1$. The threshold rate shown in all of the plotted figures is expressed in bps/Hz. Using TensorFlow 2.17.0 alongside Python 3.12.5, a DNN model is built featuring three hidden layers, each comprising 128 hidden neurons. The learning rate is set at 0.0001, which is subsequently reduced by 90% after 10 epochs. The weights of the DNN model are randomly assigned and refined over 150 training epochs, employing the Adam optimizer with a gradient decay value of 0.95. This method dynamically modifies the learning rate in response to performance, helping to avoid overfitting and guarantees that the model does not get stagnant throughout the training phase. A laptop equipped with an AMD Ryzen 5 5600U Radeon graphics processor and 16 GB of RAM was used for all testing.

FIGURE 6 presents the SOP performance of the proposed system in two distinct scenarios: with jammer (J) and without jammer (WJ). It can be seen that while increasing the SNR enhances secrecy performance in a jamming scenario, the jammer reduces the eavesdropper's ability to wiretap the legitimate transmissions by lowering the eavesdropper's SNR, and the jammer's strength increases in tandem with an increase in ρ_s. It can also be observed that the markers for the simulations align well with the analytical curves, validating the accuracy of the theoretical framework. It is worthwhile noting that such a comparison between Monte Carlo simulations and the proposed theoretical framework is depicted subsequently under various system configurations, with a good match in all cases.

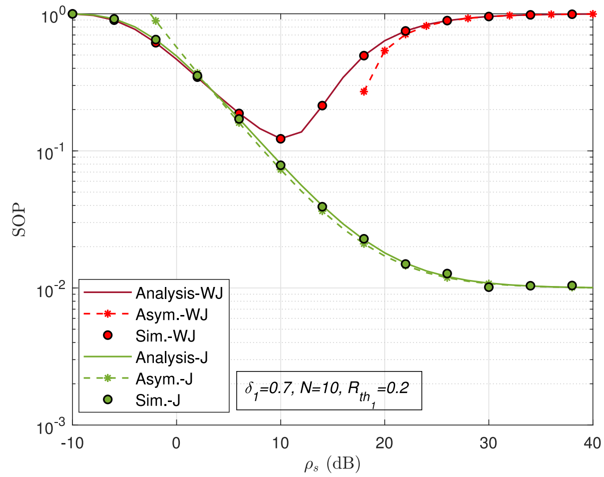


FIGURE 6. SOP versus ρ_s for both jamming and non-jamming cases.

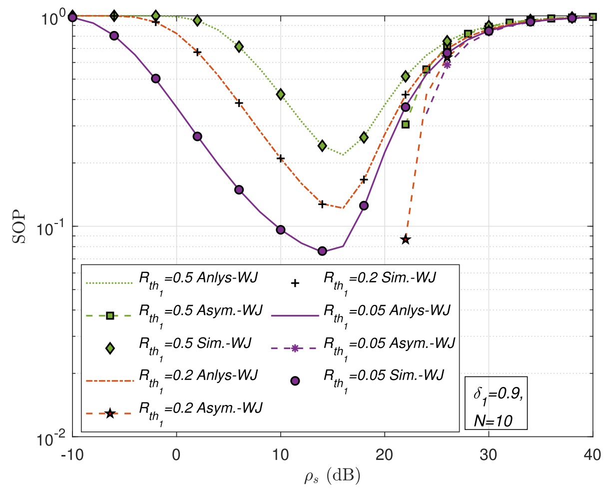


FIGURE 7. SOP versus ρ_s for different values of R_{th_1} (without jammer).

FIGURES 7 and 8 show how changing R_{th_1} affects the SOP performance of the underlying system in both with/without jammer scenarios. As the threshold secrecy rate decreases, the SOP improves, indicating that the system is more secure. In other words, low threshold rates reduce the likelihood that the system is unable to maintain secrecy. In the scenario with a jammer, the SOP performance is further improved. On the other hand, in the case without a jammer, the SOP performance degrades in high-SNR regions because the eavesdropper's capacity increases with increasing values of

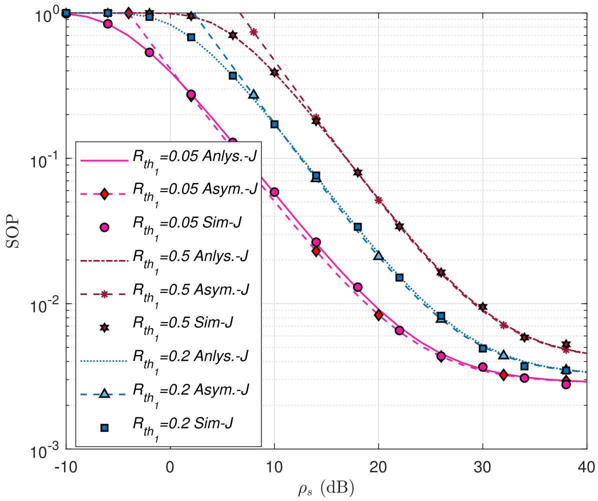


FIGURE 8. SOP **versus** ρ_s **for different values of** R_{th_1} **(with jammer).**

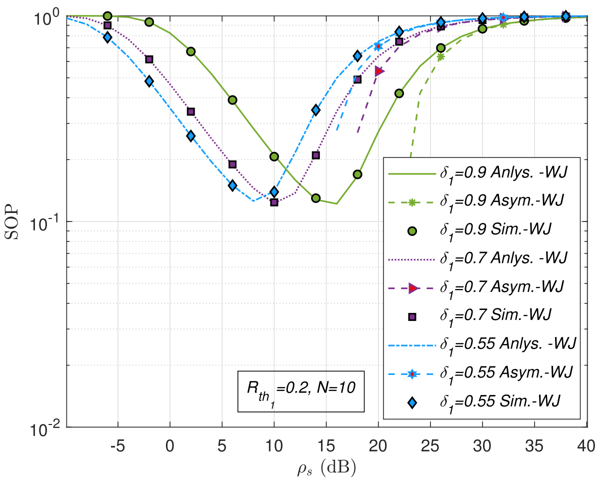


FIGURE 9. SOP **versus** ρ_s **for different values of** δ_1 **(without jammer).**

ρ_s. However, when a jammer operates, the SOP performance continuously improves since the capacity of the eavesdropper decreases while the capacity of NOMA users increases with an increase in ρ_s.

FIGURES 9 and 10 illustrate the SOP performance versus ρ_s considering different values of δ_1 for both cases with and without jammer. A higher value of δ_1 leads to improved secrecy performance, as evidenced by the rapid decline in the SOP with increasing ρ_s. This is due to U_1 being located far from the transmitter, which increases the likelihood that the SOP performance of the underlying falls below the threshold level due to U_1. However, as δ_1 increases, the overall capacity of U_1 increases, which leads to an improvement in the SOP performance.

FIGURES 11 and 12 depict the SOP performance versus ρ_s, for different values of $d_{s,e}$, which represents the distance between the source and the eavesdropper. When the eavesdropper is close to the source, the system integrity can easily be compromised due to the improved eavesdropper's ability

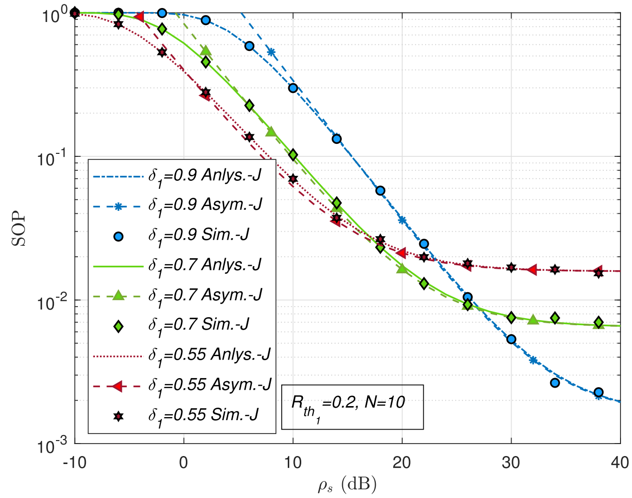


FIGURE 10. SOP **versus** ρ_s **for different values of** δ_1 **(with jammer).**

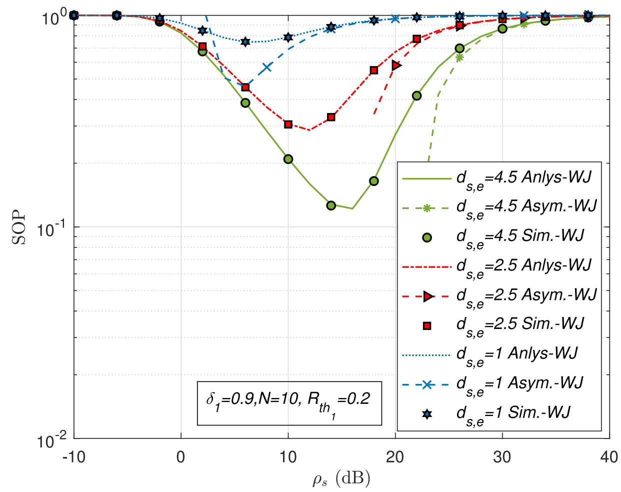


FIGURE 11. SOP **versus** ρ_s **for different values of** $d_{s,e}$ **(without jammer).**

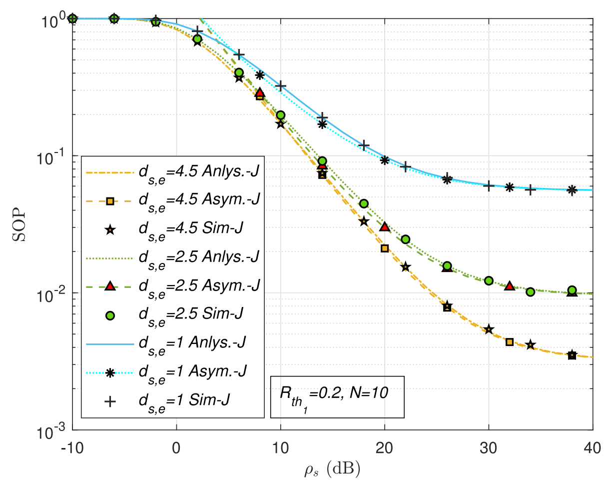


FIGURE 12. SOP **versus** ρ_s **for different values of** $d_{s,e}$ **(with jammer).**

(strong eavesdropper's signal) to decode the transmitted message. In addition, reducing the distance between the jammer and eavesdropper also enhances the SOP performance

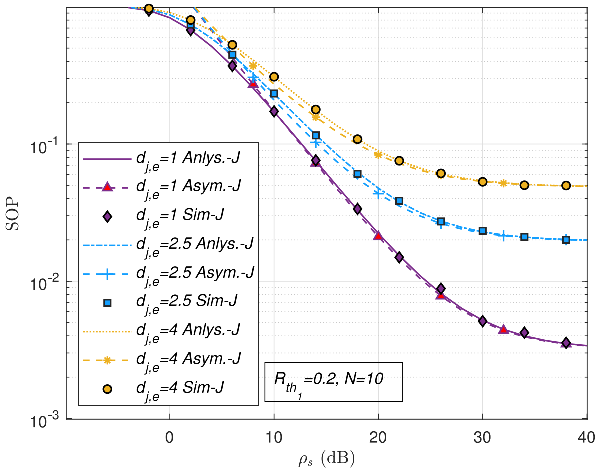


FIGURE 13. SOP **versus** ρ_s **for varying** $d_{j,e}$ **values (with jammer).**

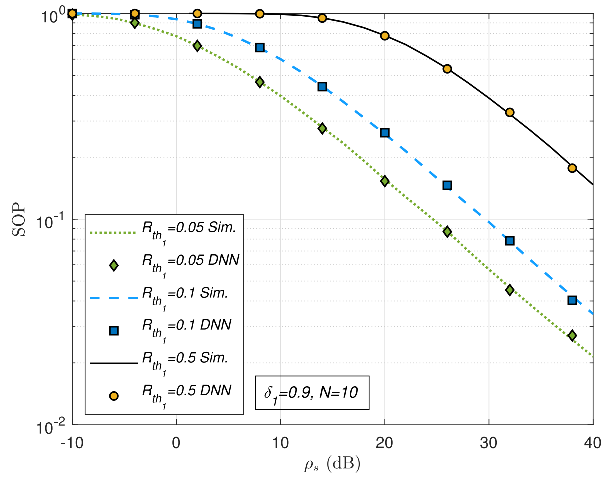


FIGURE 15. SOP **versus** ρ_s **for varying values of the threshold rate (with jammer).**

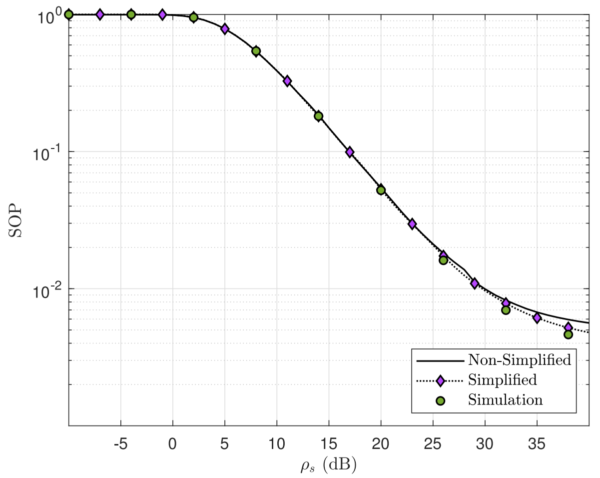


FIGURE 14. SOP versus ρ_s **for both non-simplified theoretical formulas and simplified theoretical formulas.**

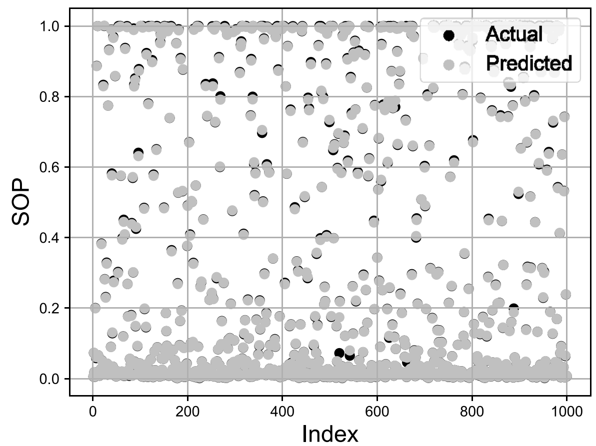


FIGURE 16. Predicted (DNN) and analytical values of SOP.

due to the strong ability of the jammer to degrade the SNR at the eavesdropper, resulting in a better overall secrecy performance. A similar performance behaviour can be observed in FIGURE 13 which depicts the SOP performance for various values of $d_{j,e}$, the distance between the jammer and the eavesdropper. As $d_{j,e}$ decreases, the jammer is more detrimental to the eavesdropper, limiting its ability to compromise the overall system.

FIGURE 14 compares the DNN predictions with the SOP values obtained from both non-simplified theoretical formulas and simplified theoretical formulas. It is evident from the figure that the DNN-based predictions with non-simplified theoretical formulas closely match the simplified theoretical formulas values and simulation values. More importantly, this plot illustrates the robustness of the DNN approach to capture complex system behaviors in dynamic scenarios.

FIGURE 15 shows a comparison between the predicted SOP obtained through the DNN model and the SOP based on the proposed analytical framework. It is evident from the figure that the DNN-based predictions with an MSE of about 10^{-5}, closely match the theoretical values. The Monte Carlo simulations and the DNN-based approach differ significantly in terms of execution time. The findings show that while Monte Carlo simulations take 7.8748 seconds, the prediction of the SOP using the DNN only takes 1.382 seconds.

To further illustrate the merits of the DNN model, we plot the actual and predicted SOP values as shown in FIGURE 16. Our model appears to be efficient, yielding accurate predictions, as evidenced by the overlapping between the points for the actual values (in black) and the predicted values (in silver).

FIGURE 17 illustrates the performance of the probability of SPSC as a function of ρ_s for various values of $d_{s,e}$ in the absence of a jammer. When the eavesdropper is close to the source, the eavesdropper's SNR is much stronger, which drastically increases its ability to decode the transmissions between S and the users/IRS. In the scenario where a jammer is absent, the overall performance of the probability of SPSC is adversely affected, since the increase in ρ_s does not

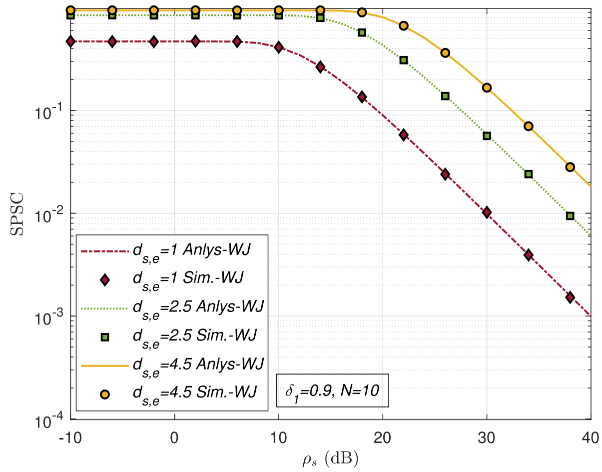


FIGURE 17. Probability of SPSC versus ρ_s for varying $d_{s,e}$ values (without jammer).

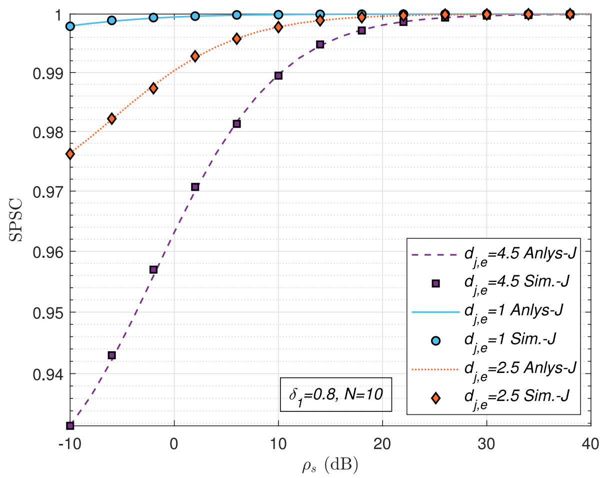


FIGURE 18. Probability of SPSC versus ρ_s for different values of $d_{j,e}$ (with jammer).

correspondingly enhance the capacity of legitimate links in comparison to the capacity of the eavesdropper's link.

FIGURE 18 shows the performance of the probability of SPSC as a function of ρ_s for various values of $d_{j,e}$ in the presence of a jammer. The results presented in this figure demonstrate that the performance of the SPSC probability improves as ρ_s increases. Additionally, bringing the jammer closer to the eavesdropper results in an improved system performance concerning the probability of SPSC, as the robust jamming effect further complicates the eavesdropper's efforts to decode the messages intended for the users.

VI. CONCLUSION

In this paper, we investigated an aerial RIS-UAV NOMA-based system in the presence of an eavesdropper and a friendly jammer. We first developed both exact and asymptotic analytical representations of the SOP, followed by a closed-form analytical expression of the probability of SPSC. Moreover, the obtained results demonstrated the advantages in adopting a jammer to improve the secrecy performance. Our study introduced an algorithm that calculates the optimal power allocation coefficient to minimize the SOP performance of the underlying system. Finally, a DNN approach was developed to accurately predict the SOP. Despite the fact that the current work contributes to the advancement of the current state-of-the-art, several challenges remain open for future studies. For example, the present work assumes perfect CSI, which is unrealistic in practical scenarios. A potential avenue for future studies could explore robust beamforming and adaptive power allocation techniques under imperfect CSI conditions. Furthermore, the impact of mobility on secrecy performance, particularly when both eavesdropper and NOMA users move dynamically, warrants further study. The proposed DNN-based approach, while effective, requires generalization in diverse network topologies and varying environmental conditions. Addressing these challenges will enhance the practical applicability of IRS-assisted UAV NOMA systems in real-world IoT deployments.

REFERENCES

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[2] Y. Cheng, K. H. Li, Y. Liu, K. C. Teh, and G. K. Karagiannidis, "Non-orthogonal multiple access (NOMA) with multiple intelligent reflecting surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7184–7195, Nov. 2021.

[3] T. -T. Nguyen, T.-V. Nguyen, T.-H. Vu, D. B. da Costa, and C. D. Ho, "IoT-based coordinated direct and relay transmission with non-orthogonal multiple access," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 503–507, Mar. 2021.

[4] Y. Cheng, K. H. Li, Y. Liu, K. C. Teh, and H. V. Poor, "Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3988–4000, Jun. 2021.

[5] Q. Wu, and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[6] S. Solanki, J. Park, and I. Lee, "On the performance of IRS-aided UAV networks with NOMA," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 9038–9043, Aug. 2022.

[7] S. Liu, Z. Huang, G. He, A. A. Nasir, H. Yu, and Z. Sheng, "NOMA and IRS-assisted secure UAV communications," in *Proc. 10th Int. Conf. Commun. Electron. (ICCE)*, Danang, Vietnam, 2024, pp. 36–41.

[8] X. Qin, Z. Na, Z. Wen, and X. Wu, "Relaying IRS-UAV assisted covert communications in uplink C-NOMA network," *IEEE Commun. Lett.*, vol. 28, no. 9, pp. 2136–2140, Sep. 2024.

[9] L. Lv, H. Jiang, Z. Ding, Q. Ye, N. Al-Dhahir, and J. Chen, "Secure non-orthogonal multiple access: An interference engineering perspective," *IEEE Netw.*, vol. 35, no. 4, pp. 278–285, Jul./Aug. 2021.

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

[11] A. A. F. Osman, J. M. Moualeu, F. Takawira, K. Yadav, and P. K. Upadhyay, "On secure hybrid RF-FSO MIMO-NOMA systems with colluding and non-colluding eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 13, no. 9, pp. 2472–2476, Sep. 2024.

[12] M. H. Khoshafa et al., "RIS-assisted physical layer security in emerging RF and optical wireless communication systems: A comprehensive survey," *IEEE Commun. Surveys Tuts*, early access, Oct. 28, 2024, doi: 10.1109/COMST.2024.3487112.

[13] A. K. Shukla, K. Yadav, P. K. Upadhyay, and J. M. Moualeu, "Exploiting deep learning in the performance evaluation of EH-based coordinated direct and relay transmission system with cognitive NOMA," *IEEE Commun. Lett.*, vol. 27, no. 6, pp. 1501–1505, Jun. 2023.

[14] K. Yadav, P. K. Upadhyay, J. Lehtomäki, and J. M. Moualeu, "Physical layer security of overlay cognitive NOMA systems with control-jamming," in *Proc. IEEE 96th Veh. Technol. Conf.*, 2022, pp. 1–7.

[15] 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.

[16] T. M. T. Nguyen, T. V. Nguyen, W. Noh, and S. Cho, "Statistical delay guarantee for the URLLC in IRS-assisted NOMA networks with finite blocklength coding," *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 19852–19869, Dec. 2024.

[17] Z. Ding, and H. Vincent Poor, "A simple design of IRS-NOMA transmission," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1119–1123, May 2020.

[18] C. Gong, X. Yue, X. Wang, X. Dai, R. Zou, and M. Essaaidi, "Intelligent reflecting surface aided secure communications for NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2761–2773, Mar. 2022.

[19] Z. Wen et al., "Outage analysis for a STAR-RIS-segmented symbiotic backscatter NOMA system," *IEEE Trans. Commun.*, vol. 72, no. 11, pp. 7263–7277, Nov. 2024.

[20] A. K. Sangaiah, J. Anandakrishnan, N. K. Son, H. Darmawan, G.-B. Bian, and M. J. F. Alenazi, "LCUT-Sv9: UAV-assisted powerline inspection framework with secure time-sensitive communication for industry 5.0," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2837–2852, 2025.

[21] A. K. Sangaiah et al., "R-UAV-Net: Enhanced YOLOv4 with graph-semantic compression for transformative UAV sensing in paddy agronomy," *IEEE Trans. Cogn. Commun. Netw.*, vol. 11, no. 2, pp. 1197–1209, Apr. 2025.

[22] R. Tao, W. Liu, Y. Wu, J. Zhang, X. Chu, and J. Zhang, "Performance analysis of cooperative-aerial-IRS-assisted heterogeneous networks," *IEEE Internet Things J.*, vol. 12, no. 4, pp. 3816–3831, Feb. 2025.

[23] X. Zhang, H. Zhang, W. Du, K. Long, and G. K. Karagiannidis, "Joint resource allocation and reflecting design in IRS-UAV communication networks with SWIPT," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 2533–2546, Apr. 2024.

[24] Q. Huang, Z. Song, Z. Xiong, G. Xu, N. Zhao, and D. Niyato, "Joint resource and trajectory optimization in active IRS-aided UAV relaying networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 13082–13094, Oct. 2024.

[25] H. M. Hariz, S. S. Z. Mosaddegh, N. Mokari, M. R. Javan, B. A. Arand, and E. A. Jorswieck, "AI-based radio resource management and trajectory design for IRS-UAV-assisted PD-NOMA communication," *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 3, pp. 3385–3400, Jun. 2024.

[26] Y. Liu, K. Xiong, Y. Zhu, H.-C. Yang, P. Fan, and K. B. Letaief, "Outage analysis of IRS-assisted UAV NOMA downlink wireless networks," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9298–9311, Mar. 2024.

[27] C. K. Singh, D. Kumar, J. J. Lehtomäki, Z. Khan, M. Latva-Aho, and P. K. Upadhyay, "Analysis with deep learning of robust UAV-mounted active IRS NOMA networks with imperfections," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 7878–7899, 2024.

[28] O. S. Badarneh, M. K. Awad, S. Muhaidat, and F. S. Almehmadi, "Performance analysis of intelligent reflecting surface-aided decode-and-forward UAV communication systems," *IEEE Syst. J.*, vol. 17, no. 1, pp. 246–257, Mar. 2023.

[29] T. Cheng, B. Wang, K. Cao, R. Dong, and D. Diao, "IRS-assisted secure UAV communication system for multiuser with hardware impairments," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4946–4957, Sep. 2023.

[30] C. K. Singh, P. K. Upadhyay, J. Lehtomäki, and M. Juntti, "Performance analysis with deep learning assay for cooperative UAV-borne IRS NOMA networks under non-ideal system imperfections," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 1065–1083, Jan. 2024.

[31] B. Shang, E. S. Bentley, and L. Liu, "UAV swarm-enabled aerial reconfigurable intelligent surface: Modeling, analysis, and optimization," *IEEE Trans. Commun.*, vol. 71, no. 6, pp. 3621–3636, Jun. 2023.

[32] A. Souzani, M. A. Pourmina, P. Azmi, and M. Naser-Moghadasi, "Physical layer security enhancement via IRS based on PD-NOMA and cooperative jamming," *IEEE Access*, vol. 11, pp. 65956–65967, 2023.

[33] N. Zhao et al., "Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2294–2305, Mar. 2019.

[34] J. Zhang, W. Wang, J. Tang, N. Zhao, K.-K. Wong, and X. Wang, "Robust secure transmission for IRS-aided NOMA networks with hybrid beamforming," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3086–3101, Apr. 2024.

[35] H. Han, Y. Cao, M. Sheng, J. Liu, N. Zhao, and D. Niyato, "IRS-aided secure MISO-NOMA networks towards internal and external eavesdropping," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Rio de Janeiro, Brazil, 2022, pp. 4364–4370.

[36] Y. Sun et al., "RIS-assisted robust hybrid beamforming against simultaneous jamming and eavesdropping attacks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 9212–9231, Nov. 2022.

[37] A. Al-Hourani and K. Gomez, "Modeling cellular-to-UAV path-loss for suburban environments," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 82–85, Feb. 2018.

[38] K. Yadav, P. K. Upadhyay, and M. Magarini, "Physical layer security analysis of IRS-aided UAV relaying systems with NOMA," in *Proc. IEEE Int. Mediterr. Conf. Commun. Netw. (MeditCom)*, Dubrovnik, Croatia, 2023, pp. 157–163.

[39] H.-P. Dang, M.-S. V. Nguyen, D.-T. Do, M.-H. Nguyen, M.-T. Pham, and A.-T. Kim, "Secure performance analysis of aerial RIS-NOMA-aided systems: Deep neural network approach," *Electronics*, vol. 11, no. 16, p. 2588, 2022.

[40] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[41] Z. Ding, R. Schober, and H. V. Poor, "On the impact of phase shifting designs on IRS-NOMA," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1596–1600, Oct. 2020.

[42] 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.

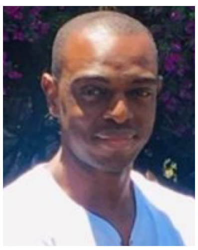
[43] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[44] D.-A. Clevert, T. Unterthiner, and S. Hochreiter, "Fast and accurate deep network learning by exponential linear units (ELUs)," 2015, *arXiv:1511.07289*.

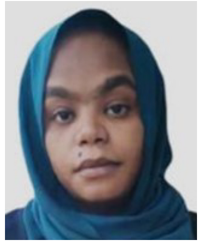
[45] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series and Products*, 7th ed. New York, NY, USA: Academic, 2007.

KAJAL YADAV (Graduate Student Member, IEEE) received the B.E. degree in electronics and communication engineering from the M. B. M. Engineering College, Jodhpur, India, in 2019, and the M.Tech. degree in communication and signal processing from the Indian Institute of Technology Indore, Indore, India, in 2022, where she is currently pursuing the Ph.D. degree with the Electrical Engineering Department. Her research interests include 5G and 6G wireless communication systems, nonorthogonal multiple access technique, physical-layer security, cognitive radio techniques, cooperative relaying systems, and intelligent reflecting surface.

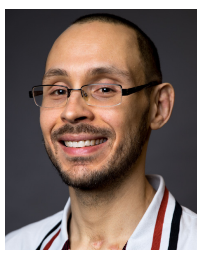
PRABHAT K. UPADHYAY (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the Indian Institute of Technology (IIT) Delhi, New Delhi, India, in 2011. He joined IIT Indore as an Assistant Professor with the Department of Electrical Engineering in 2012, where he became an Associate Professor in 2017 and a Professor in 2022. He was a Visiting Professor with the Centre for Wireless Communications, University of Oulu, Finland, from May 2022 to August 2022 under Nokia Foundation Fellowship. From April 2023 to July 2023, he was a Visiting Professor with the Department of Electronics, Information and Bioengineering, Politecnico di Milano, Italy. His general research interests include wireless and mobile communications, Internet of Things networks, molecular communications, and nano-networks. He received the Exemplary Editor Award of the IEEE COMMUNICATIONS LETTERS in 2021. He has been awarded the Sir Visvesvaraya Young Faculty Research Fellowship under the Ministry of Electronics and Information Technology (MeitY), Government of India from 2018 to 2023. He has been conferred with IETE-NV Gadadhar Memorial Award in 2022 and the IETE-Prof SVC Aiya Memorial Award in 2018. He has co-authored a paper that received the Best Poster Award in COMSNETS, Bengaluru, in 2023 and a paper that received the Best Paper Award in the CommNet, Morocco, in 2018. He is currently serving as an Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He served as an Editor for IEEE COMMUNICATIONS LETTERS from May 2019 to May 2024 and as an Associate Editor for IEEE ACCESS from January 2018 to January 2022. He served as a Guest Editor of the Special Issue on "Energy-Harvesting Cognitive Radio Networks" in the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING in 2018. He has also been involved in the technical program committee of several IEEE premier conferences. He is a Fellow of the IETE and of the Institution of Engineers, India.



JULES M. MOUALEU (Senior Member, IEEE) received the Ph.D. degree in electronic engineering from the University of KwaZulu-Natal, Durban, South Africa, in 2013. During the Ph.D. studies, he was a Visiting Scholar with Concordia University, Montreal, QC, Canada, under the Canadian Commonwealth Scholarship Program offered by the Foreign Affairs and International Trade Canada. In 2015, he joined the Department of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, South Africa, where he is currently an Associate Professor. He is also a Visiting Associate Professor with the Lappeenranta-Lathi University of Technology, Lappeenranta, Finland. From 2018 to 2021, he was an Affiliate Assistant Professor with Concordia University. His current research interests include 5G and 6G enabling technologies, optical wireless communications, reconfigurable intelligent surfaces, and physical-layer security in wireless networks. He received an Exemplary Reviewer Award of IEEE COMMUNICATIONS LETTERS from 2018 to 2022 and IEEE TRANSACTIONS ON COMMUNICATIONS in 2021. He served as an Associate Editor for IEEE ACCESS from 2018 to 2023. He currently serves as an Associate Editor for *Frontiers in Communications and Networks* and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, a Senior Reviewer for the IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, and a Managing Editor for IEEE COMMUNICATION LETTERS.



AMANI A. F. OSMAN received the B.Sc. degree in electronics and the M.Sc. degree in electronics engineering (data and communication networks) from Al Neelain University, Khartoum, Sudan, in 2012 and 2015, respectively, and the Ph.D. degree in electrical engineering (telecommunication systems) from the University of the Witwatersrand, Johannesburg, South Africa, in 2024, where she is currently a Postdoctoral Fellow with the School of Electrical and Information Engineering. Her research interests include cooperative and relay communications, multiple-input multiple-output systems, nonorthogonal multiple access schemes, physical layer security, reconfigurable intelligent surfaces, and mixed radio frequency/free-space optics systems.



PEDRO H. J. NARDELLI (Senior Member, IEEE) received the B.S. and M.Sc. degrees in electrical engineering from the State University of Campinas, Brazil, in 2006 and 2008, respectively, and the Doctoral degree from the University of Oulu, Finland, and the State University of Campinas following a dual degree agreement in 2013. In 2017, he received the Title of Docent with the University of Oulu. In 2018, he started working with LUT, where he is currently a Full Professor.