Computer Modeling in
Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.066669

ARTICLE

System Modeling and Deep Learning-Based Security Analysis of Uplink NOMA Relay Networks with IRS and Fountain Codes

Phu Tran Tin[1], Minh-Sang Van Nguyen[2], Quy-Anh Bui[1], Agbotiname Lucky Imoize[3] and Byung-Seo Kim[4,*]

[1]Data Science Laboratory, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, 70000, Vietnam
[2]Faculty of Telecommunications 2, Posts and Telecommunications Institute of Technology, Ho Chi Minh City, 70000, Vietnam
[3]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos, 100213, Nigeria
[4]Department of Software and Communications Engineering, Hongik University, Sejong, 30016, Republic of Korea

*Corresponding Author: Byung-Seo Kim. Email: jsnbs@hongik.ac.kr

Received: 14 April 2025; Accepted: 18 July 2025; Published: 31 August 2025

ABSTRACT: Digital content such as games, extended reality (XR), and movies has been widely and easily distributed over wireless networks. As a result, unauthorized access, copyright infringement by third parties or eavesdroppers, and cyberattacks over these networks have become pressing concerns. Therefore, protecting copyrighted content and preventing illegal distribution in wireless communications has garnered significant attention. The Intelligent Reflecting Surface (IRS) is regarded as a promising technology for future wireless and mobile networks due to its ability to reconfigure the radio propagation environment. This study investigates the security performance of an uplink Non-Orthogonal Multiple Access (NOMA) system integrated with an IRS and employing Fountain Codes (FCs). Specifically, two users send signals to the base station at separate distances. A relay receives the signal from the nearby user first and then relays it to the base station. The IRS receives the signal from the distant user and reflects it to the relay, which then sends the reflected signal to the base station. Furthermore, a malevolent eavesdropper intercepts both user and relay communications. We construct mathematical equations for Outage Probability (OP), throughput, diversity evaluation, and Interception Probability (IP), offering quantitative insights to assess system security and performance. Additionally, OP and IP are analyzed using a Deep Neural Network (DNN) model. A deeper comprehension of the security performance of the IRS-assisted NOMA system in signal transmission is provided by Monte Carlo simulations, which are also carried out to confirm the theoretical conclusions.

KEYWORDS: Copyright management; deep neural network; fountain codes; intelligent reflecting surface; non-orthogonal multiple access; physical layer security; uplink

1 Introduction

Due to its improved spectrum efficiency, Non-Orthogonal Multiple Access (NOMA) is crucial for sixth-generation (6G) and future wireless networks [1]. NOMA significantly enhances user connection and spectrum efficiency compared to conventional Orthogonal Multiple Access (OMA) methods [2]. In the meanwhile, Intelligent Reflecting Surfaces (IRSs) are becoming a cutting-edge and reasonably priced technology that maximizes energy efficiency (EE) and minimizes transmit power [3,4]. Therefore, combining IRS with NOMA is a viable approach to enhancing the overall performance of wireless communication systems. Furthermore, a downlink IRS-assisted NOMA network functioning on Rician fading channels is examined by the authors in [5–7]. They offer accurate and asymptotic formulas for the throughput, ergodic rate, and outage probability (OP). The findings show that the IRS-NOMA system performs better than the IRS-OMA system, especially as the Rician factor and reflecting component count rise.

Recently, digital contents like games, extended realities (XRs), and movies have been widely and easily distributed over wireless networks. As a result, concerns about unauthorized access, copyright infringement by third parties or eavesdroppers, and cyberattacks have grown significantly. This highlights the urgent need to address content protection and security issues. Consequently, safeguarding against copyright violations and illegal content distribution has become a critical consideration in the design of modern wireless networks [8,9]. Moreover, wireless communication networks are now susceptible to serious information leakage due to eavesdropping attacks, primarily because of the broadcast nature of radio propagation and the inherent instability of transmission links. A potential approach to safeguarding wireless communications is physical layer security (PLS), which seeks to create information-theoretic protection against hackers [1,10]. Historically, techniques such as beamforming, cooperative jamming, and cooperative relaying have been employed to provide secure communication, often in conjunction with the use of artificial noise [11–13]. But there is still a basic problem, especially at higher frequencies. Although these techniques have improved the performance of wireless communication systems' PLS, they still require the placement of numerous relays, which can be costly and power-hungry. Moreover, to strengthen PLS in Internet of Things (IoT) networks against eavesdropping risks, the authors in [14,15] investigate an IRS-NOMA system. Their study demonstrates that IRS-NOMA outperforms conventional OMA by analyzing key metrics, such as OP, secrecy outage probability (SOP), and secrecy capacity, particularly when power allocation is optimized and IRS placement is properly considered.

In wireless communication, Fountain Codes (FCs) provide a viable option for dependable data transfer. In contrast to conventional codes, FCs dynamically adjust to shifting channel circumstances by producing an infinite number of encoded symbols from a finite set [8,16,17]. Due to their versatility, they work effectively in various settings with different noise and interference levels. Additionally, FCs achieve great performance with minimal computing cost and are robust against burst errors. Their adaptability encompasses a wide range of applications, including distributed storage systems, multimedia streaming, and satellite communication. Because of this, FCs are now widely used as a flexible and effective error-correcting method in wireless communication [18]. Furthermore, FCs are members of a family of linear block codes that are well-known for producing an infinite number of encoded packets [19,20]. Due to their outstanding coding performance, systematic forward error correction (FEC) codes like Raptor-Q codes have gained widespread acceptance as Application-Layer Forward Error Correction (AL-FEC) codes in the 3GPP Multimedia Broadcast and Multicast Services (MBMS) standard [21].

Recently, deep learning has emerged as a powerful data-driven approach for addressing various challenging issues, including wireless communication applications, pattern recognition, and image processing [22,23]. The authors created a deep neural network (DNN) model in [24] to forecast the likelihood of coverage in random wireless networks. Interestingly, the DNN model performs better than conventional mathematical techniques, which are typically limited to network settings that are overly simplistic. Additionally, in [25], the authors outperformed simulation and analytical findings in unmanned aerial vehicle networks by using a DNN model to forecast the SOP, demonstrating the fastest running time for SOP prediction. Furthermore, a NOMA-based downlink system with IRS and a PLS environment is examined by the authors in [8]. While addressing the possibility of a malevolent eavesdropper, their work also incorporates the usage of FCs. This paper's primary contribution is the derivation of exact closed-form formulas for the suggested system's OP, EE, intercept probability (IP), and average secrecy rate (ASR). In addition, they create a DNN model to assess the average number of time slots (ATS), OP, IP, and ASR. In [26], this study investigates the security of a downlink IRS-assisted NOMA relay network enhanced with FC and DNN. Closed-form expressions for OP and IP are derived, and Monte Carlo simulations are used for validation. The results confirm the performance gains of IRS-NOMA, especially under varying numbers of reflecting elements, user threshold rates, and encoded packet limits.

1.1 Motivation and Major Contributions

In documents [27] and [28], the authors examined an uplink secure relay network combined with the NOMA technique, considering the case where an eavesdropper (E) intercepts signals from both the relay (R) and direct links between users and the base station (BS). However, these studies did not incorporate the IRS or the FC technique. In the document [1], the authors introduced several improvements over the previous works by integrating IRS into the uplink secure system model. Nevertheless, none of these studies applied the FC technique to enhance system security. Furthermore, our research incorporates the DNN technique to predict system performance and security. Additionally, we analyze system performance through OP and evaluate security performance using the IP.

The main contributions of this study are succinctly summarized as follows:

- This study investigates an IRS-NOMA network uplink using a new secure communication protocol that makes good use of FC properties. This protocol, in contrast to conventional techniques, guarantees that packets are encrypted securely, making it far more difficult for the E to collect and decode the original data. Additionally, adding an IRS to the system enhances the transmission quality of the uplink signal.
- In this study, the PLS of the suggested system using FCs is examined. Analytical techniques are used to calculate key performance measures, such as the OP, throughput, diversity evaluation for two users. The study also evaluates the IP necessary for safe communication between users and between authorized users and possible adversaries. In addition to highlighting the benefits of FCs in enhancing communication security, the study provides a comprehensive examination of security and reliability concerns associated with their use.
- Unlike previous research, our proposed IRS-based uplink NOMA system utilizes FC and DNN techniques to evaluate OP and IP. Moreover, when paired with FC characteristics, the DNN model is a valuable tool for assessing system performance, particularly when closed-form analytical expressions are hard to come by. This method yields precise approximations of system performance measures by streamlining the assessment of highly nonlinear functions. Consequently, the application of DNN and FCs is closely related to performance evaluation. In this study, we have created closed-form formulae for both OP and IP, but we also use the DNN model to forecast more accurate results with real-world applications. Additionally, simulations were conducted to gather useful technical data and validate the theoretical approach. By examining various outcomes, the advantages of integrating IRS, NOMA, and FCs to enhance system performance, particularly in scenarios involving eavesdropping, were further investigated.

1.2 Organization

The structure of this paper is set up as follows: The system model is presented in Section 2, and the OP of the system is discussed in Section 3. Moreover, the IP of the system is discussed in Section 4. The DNN application is examined in Section 5. Lastly, Sections 6 and 7 show the simulation findings and the research conclusion.

2 System Model

Fig. 1 illustrates the uplink NOMA relay network security system supported by an IRS and employing the FC technique. The system model consists of a BS, a R, an IRS with H elements, two users (D_1 and D_2), and an E. We assume that user D_2 is located farther from both the BS and R compared to user D_1 and thus requires IRS assistance.

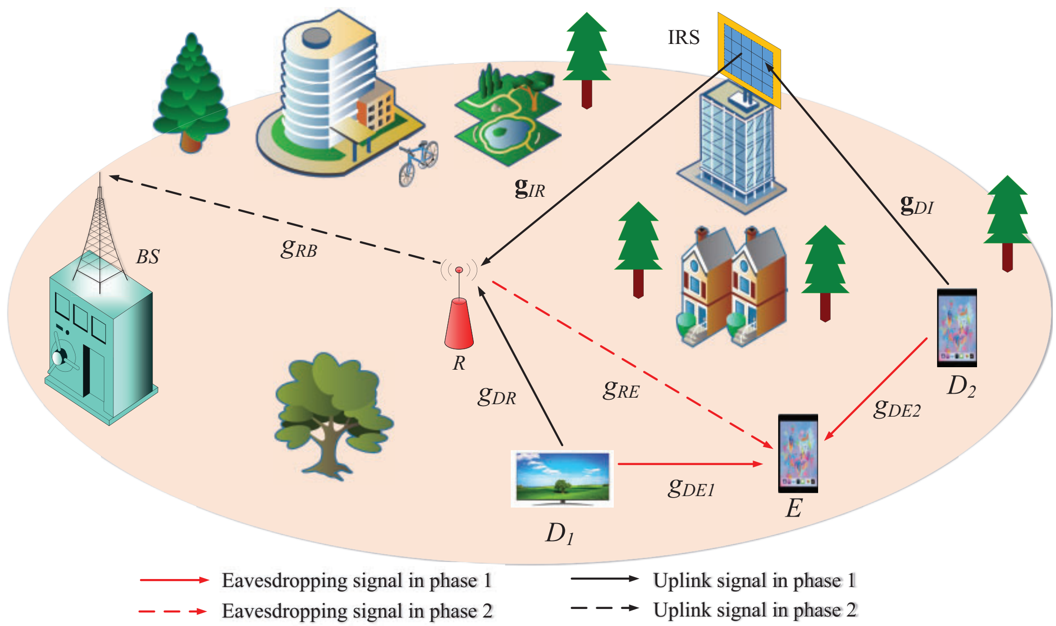

Figure 1: IRS-assisted secure network model for a NOMA relay system

The signal transmission process occurs in two phases:

i) First phase: The signal from user D_1 is transmitted directly to R, while D_2, being farther away, relies on IRS assistance before forwarding its signal to R. At the same time, E attempts to eavesdrop on the signals from both D_1 and D_2.

ii) Second phase: R decodes the signals from both users and then transmits them to the BS. Meanwhile, E also eavesdrops on the signals from D_1 and D_2 as they are relayed by R.

It is important to note that the IRS only reflects signals during transmission and does not participate in signal decoding. At R, the successive interference cancellation (SIC) decoding process is performed to separate the signals from D_1 and D_2 before forwarding them to the BS, as R receives signals from both users simultaneously. Furthermore, we assume that there is no direct signal transmission from D_i, $(i = 1, 2)$ to BS or from BS to E.

To create the encoded packets, the user divides its original data into C packets and makes sure they are correctly encoded. D_i sends each of these encoded packets to the BS separately at each time slot, and E tries to intercept them. Suppose both the BS and E properly receive at least G-encoded packets, where $A = C(1 + \zeta)$ and ζ is the decoding overhead, which varies depending on the particular code design. In that case, it is assumed that both can successfully retrieve the original data [8,29]. Additionally, the BS signals D_i to stop the transmission by sending an acknowledgment (ACK) message when a sufficient number of encoded packets have been gathered. The E cannot obtain D_i's data if it is unable to record the necessary quantity of encrypted packets. On the other hand, it can reassemble the original data if it can intercept enough packets.

2.1 Evaluation of Signal in Phase 1

Let$B$ denote the length of each FC packet. Assume that D_1 sends the packets $u_1[b]$ (indicating the b-th packet of D_1) and D_2 sends the packets $u_2[b]$ (indicating the b-th packet of D_2) to the BS if the D_i delivers the signal $q_i[b], (b = 1, \ldots, B)$ to the BS [8]. The signal that is received at R from D_i is supplied by [27,30]

$$y_{DR} = g_{DR} d_{DR}^{-\frac{\rho}{2}} \sqrt{\mu_1 P_{D_1}} q_1[b] + \mathbf{g}_{DI} \Phi \mathbf{g}_{IR} d_{DI}^{-\frac{\rho}{2}} d_{IR}^{-\frac{\rho}{2}} \sqrt{\mu_2 P_{D_2}} q_2[b] + \vartheta_R[b], \tag{1}$$

where the link between D_1 and R, denoted by $g_{DR} \sim CN\left(0, \sigma_{g_{DR}}\right)$ in the Rayleigh fading model, fades on a small scale. In particular, the complex channel coefficients for D_2-IRS and IRS-R are denoted by $\mathbf{g}_{DI} = \left[g_{DI,1}, \ldots, g_{DI,h}, \ldots, g_{DI,H}\right]$ and $\mathbf{g}_{IR} = \left[g_{IR,1}, \ldots, g_{IR,h}, \ldots, g_{IR,H}\right]^T$, respectively. With unique fading parameters ($m_{g_{DI}}$ and $m_{g_{IR}}$, respectively), each element in $\mathbf{g}_{DI}$ and $\mathbf{g}_{IR}$ adheres to the Nakagami-m fading model. The distance between D_1-R link and D_2-IRS link and IRS-R link are represented by d_{DR}, d_{DI}, d_{IR}, respectively. The path loss exponents are represented by ρ. $\Phi = \mathrm{diag}\left[\alpha_1 e^{j\chi_1}, \ldots, \alpha_h e^{j\chi_h}, \ldots, \alpha_H e^{j\chi_H}\right], \left(j = \sqrt{-1}\right)$ stands for the reflection coefficient matrix related to the D_2-IRS-R, whereas $\alpha_H \in [0, 1]$ represents the amplitude-reflection coefficient, and we assume that $\alpha_1 = \cdots = \alpha_h = \cdots = \alpha_H$ [30]. The IRS can control the h-th element's adjustable phase shift variables using $\chi_h \in [0, 2\pi)$, which are supposed to be represented by $(h = 1, \ldots, H)$. μ_1 and μ_2 stand for the power allocation coefficients for D_1 and D_2, respectively. Notably, we assume a fixed power allocation share between the two users and set $\mu_1 < \mu_2$ for user fairness, and $\mu_1 + \mu_2 = 1$ [4,30]. The transmitted signals of the b-th symbol of $u_1[b]$ and $u_2[b]$ are denoted by $q_1[b]$ and $q_2[b]$, respectively. The transmission power of the D_i is denoted by P_{D_i}. The additive white Gaussian noise (AWGN) at R is indicated by the symbol $\vartheta_R[b] \sim CN\left(0, \omega_0^2\right)$.

The signal for D_1 acts as interference at R, and the signal for D_2 is deciphered first. Consequently, the following formula provides the signal to interference plus noise ratio (SINR) for decoding the signal for D_2 at R:

$$\gamma_{DR}^{(q_2)} = \frac{\left|\mathbf{g}_{DI} \Phi \mathbf{g}_{IR}\right|^2 d_{DI}^{-\rho} d_{IR}^{-\rho} \mu_2 \beta_{D_2}}{\left|g_{DR}\right|^2 d_{DR}^{-\rho} \mu_1 \beta_{D_1} + 1}, \tag{2}$$

where $\beta_{D_1} = \frac{P_{D_1}}{\omega_0^2}, \beta_{D_2} = \frac{P_{D_2}}{\omega_0^2}$.

We then use SIC to decode the D_1 signal. The signal-to-noise ratio (SNR) for decoding the signal for D_1 at R is now shown as follows:

$$\gamma_{DR}^{(q_1)} = \left|g_{DR}\right|^2 d_{DR}^{-\rho} \mu_1 \beta_{D_1}. \tag{3}$$

At the same time, the E also intercepts the signals from D_1 and D_2. At this point, the signal intercepted by E from both users D_1 and D_2 is given by the following expression [27,31]:

$$y_{E_1} = g_{DE1} d_{DE1}^{-\frac{\rho}{2}} \sqrt{\mu_1 P_{D_1}} q_1[b] + g_{DE2} d_{DE2}^{-\frac{\rho}{2}} \sqrt{\mu_2 P_{D_2}} q_2[b] + \vartheta_E[b], \tag{4}$$

where the between D_1-E link denoted by $g_{DE1} \sim CN\left(0, \sigma_{g_{DE1}}\right)$ in the Rayleigh fading model, fades on a small scale; the between D_2-E link denoted by $g_{DE2} \sim CN\left(0, \sigma_{g_{DE2}}\right)$ in the Rayleigh fading model, fades on a small scale. The distance between D_1-E link and D_2-E link are represented by d_{DE1}, d_{DE2}, respectively. The AWGN at E is indicated by the symbol $\vartheta_E[b] \sim CN\left(0, \omega_E^2\right)$.

Based on the operating principle of SIC, the E device will attempt to detect and decode the signal for D_2 first, as D_2 is assumed to have better channel conditions. The quality of the signal for D_2 at the E is evaluated through SINR. The SINR at E for detecting the signal for D_2 is given by the following expression:

$$\gamma_{E_1}^{(q_2)} = \frac{|g_{DE2}|^2 d_{DE2}^{-\rho} \mu_2 \beta_{E_2}}{|g_{DE1}|^2 d_{DE1}^{-\rho} \mu_1 \beta_{E_1} + 1}, \tag{5}$$

where $\beta_{E_1} = \frac{P_{D_1}}{\omega_E^2}, \beta_{E_2} = \frac{P_{D_2}}{\omega_E^2}$.

Following the detection of the D_2 signal at E, we use SIC to find the D_1 signal. The following equation provides the SNR for detecting the signal for D_1 at E:

$$\gamma_{E_1}^{(q_1)} = |g_{DE1}|^2 d_{DE1}^{-\rho} \mu_1 \beta_{E_1}. \tag{6}$$

2.2 Evaluation of Signal in Phase 2

Following the successful decoding of the signals for D_i at R, R proceeds to send the signals from D_i to the BS. The following equation represents the signal received at the BS at this time [27]:

$$y_{RB} = g_{RB} d_{RB}^{-\frac{\rho}{2}} \left(\sqrt{\mu_1 P_{RB}} q_1 [b] + \sqrt{\mu_2 P_{RB}} q_2 [b] \right) + \vartheta_{BS} [b], \tag{7}$$

where the between R-BS link denoted by $g_{RB} \sim CN \left(0, \sigma_{g_{RB}}\right)$ in the Rayleigh fading model, fades on a small scale. The distance between R-BS link is represented by d_{RB}. The transmission power of the R is denoted by P_{RB}. The AWGN at BS is indicated by the symbol $\vartheta_{BS} [b] \sim CN \left(0, \omega_0^2\right)$.

As in (2), the D_2 signal is decoded first, and the D_1 signal is regarded as interference. At this stage, the following formula provides the SINR for decoding the signal for D_2 at the BS:

$$\gamma_{RB}^{(q_2)} = \frac{|g_{RB}|^2 d_{RB}^{-\rho} \mu_2 \beta_{RB}}{|g_{RB}|^2 d_{RB}^{-\rho} \mu_1 \beta_{RB} + 1}, \tag{8}$$

where $\beta_{RB} = \frac{P_{RB}}{\omega_0^2}$.

At the BS, use SIC to decode the D_1 signal. At this stage, the following formula provides the SNR at the BS for decoding the signal for D_1:

$$\gamma_{RB}^{(q_1)} = |g_{RB}|^2 d_{RB}^{-\rho} \mu_1 \beta_{RB}. \tag{9}$$

The eavesdropping device E concurrently intercepts the signal from R as it is sent to the BS. The following is the expression for the signal that was received at E from R [32,33]:

$$y_{RE} = g_{RE} d_{RE}^{-\frac{\rho}{2}} \left(\sqrt{\mu_1 P_{RB}} q_1 [b] + \sqrt{\mu_2 P_{RB}} q_2 [b] \right) + \vartheta_E [b], \tag{10}$$

where the between R-E link denoted by $g_{RE} \sim CN \left(0, \sigma_{g_{RE}}\right)$ in the Rayleigh fading model, fades on a small scale. The distance between R-E link is represented by d_{RE}.

The E device will attempt to detect and decode the signal for D_2 first. The SINR at E from R for detecting the signal for D_2 is given by the following expression:

$$\gamma_{RE}^{(q_2)} = \frac{|g_{RE}|^2 d_{RE}^{-\rho} \mu_2 \beta_{RE}}{|g_{RE}|^2 d_{RE}^{-\rho} \mu_1 \beta_{RE} + 1}, \tag{11}$$

where $\beta_{RE} = \frac{P_{RB}}{\omega_E^2}$.

Next, we use SIC to find the D_1 signal. The following equation provides the SNR for detecting the signal for D_1 at E:

$$\gamma_{RE}^{(q_1)} = |g_{RE}|^2 d_{RE}^{-\rho} \mu_1 \beta_{RE}. \tag{12}$$

3 OP-Based System Reliability

The OP in communication systems is the probability that an outage will occur when a user's information rate drops below a certain goal rate. A commonly used statistic for assessing system performance in situations involving fixed-rate transmission is OP. In this part, we examine the uplink IRS-NOMA networks' outage performance.

3.1 D_1's OP Assessment

Since the SIC operation is assumed to be flawless in this study, the OP for D_1 of one FC packet may be found as follows: i) D_1 fails to decode the signal packet $q_1[b]$ during the first transmission phase. ii) D_1 cannot interpret the signal packet $q_1[b]$ once more during the second transmission phase. Consequently, the OP of one FC packet at D_1 may be written as follows [27,30]:

$$\Omega_{D_1} = 1 - \Pr\left(\gamma_{DR}^{(q_1)} > \gamma_1^{(th)}, \gamma_{RB}^{(q_1)} > \gamma_1^{(th)}\right), \tag{13}$$

where $\gamma_i^{(th)} = 2^{2R_{D_i}} - 1$, and the target date rate for user D_i is denoted by R_{D_i}.

As stated in [4,30], the probability density function (PDF) and cumulative distribution function (CDF) for $J \in \{g_{RB}, g_{DR}, g_{RE}, g_{DE1}, g_{DE2}\}$ may be written as

$$f_{|J|^2}(x) = \frac{1}{\sigma_J} e^{-\frac{x}{\sigma_J}}, \tag{14}$$

$$F_{|J|^2}(x) = 1 - e^{-\frac{x}{\sigma_J}}. \tag{15}$$

Based on Eq. (13), Ω_{D_1} may be written as follows:

$$\begin{aligned} \Omega_{D_1} &= 1 - \Pr\left(\gamma_{DR}^{(q_1)} > \gamma_1^{(th)}\right) \Pr\left(\gamma_{RB}^{(q_1)} > \gamma_1^{(th)}\right) \\ &= 1 - \Pr\left(|g_{DR}|^2 > \frac{\gamma_1^{(th)}}{d_{DR}^{-\rho}\mu_1\beta_{D_1}}\right) \Pr\left(|g_{RB}|^2 > \frac{\gamma_1^{(th)}}{d_{RB}^{-\rho}\mu_1\beta_{RB}}\right). \end{aligned} \tag{16}$$

Using the CDF function of (15), Ω_{D_1} is further calculated as follows:

$$\begin{aligned} \Omega_{D_1} &= 1 - \left[1 - F_{|g_{DR}|^2}\left(\frac{\gamma_1^{(th)}}{d_{DR}^{-\rho}\mu_1\beta_{D_1}}\right)\right]\left[1 - F_{|g_{RB}|^2}\left(\frac{\gamma_1^{(th)}}{d_{RB}^{-\rho}\mu_1\beta_{RB}}\right)\right] \\ &= 1 - \exp\left(-\frac{\gamma_1^{(th)}}{d_{DR}^{-\rho}\mu_1\beta_{D_1}\sigma_{g_{DR}}}\right)\exp\left(-\frac{\gamma_1^{(th)}}{d_{RB}^{-\rho}\mu_1\beta_{RB}\sigma_{g_{RB}}}\right). \end{aligned} \tag{17}$$

The OP of D_1 in the case of one FC packet is represented by (17). The following is how we analyze the OP of D_1 for the case of A FC packets using these equations: The number of time slots given or the number of FC packet transfers by the D_1 is restricted because of the latency limitation. We represent Z_{D_i} as the number of transmission times utilized by the D_i, where $Z_{th} \geq Z_{D_i} \geq A$, and Z_{th} as the maximum number of transmission times for the D_i. This implies that the D_i will cease transmission after Z_{th} transmissions, and if

BS does not receive at least A-encoded packets, it will either experience an outage or be unable to reconstruct the original data. Additionally, we represent Z_{BS} and Z_E as the number of FC packets that nodes BS and E have successfully received, respectively. D_i is in the outage if Z_{BS} is smaller than A. Consequently, the OP at D_1 for A FC packets may be written as [8,16]

$$OP_{D_1,A} = \Pr\left(Z_{BS} < A \middle| Z_{D_1} = Z_{th} \right). \tag{18}$$

Next, using [16, Eq. (21)], we may get the precise formula for D_1's OP for A FC packets as follows:

$$OP_{D_1,A} = \sum_{Z_{BS}}^{A-1} \begin{pmatrix} Z_{th} \\ Z_{BS} \end{pmatrix} \left(1 - \Omega_{D_1}\right)^{Z_{BS}} \left(\Omega_{D_1}\right)^{Z_{th}-Z_{BS}}. \tag{19}$$

3.2 D_2's OP Assessment

One FC packet's OP for D_2 is determined as follows: i) It is impossible to interpret the $q_1[b]$ signal packet during the initial transmission phase. ii) The $q_1[b]$ signal packet is also undecodable during the second transmission phase. At this stage, one FC packet's OP for D_2 may be written as follows [8,30]:

$$\Omega_{D_2} = 1 - \Pr\left(\gamma_{DR}^{(q_2)} > \gamma_2^{(th)}, \gamma_{RB}^{(q_2)} > \gamma_2^{(th)}\right) = 1 - \underbrace{\Pr\left(\gamma_{DR}^{(q_2)} > \gamma_2^{(th)}\right)}_{\Theta_{1a}} \underbrace{\Pr\left(\gamma_{RB}^{(q_2)} > \gamma_2^{(th)}\right)}_{\Theta_{1b}}. \tag{20}$$

Based on [3,30], our goal for the D_2-IRS-R connection is to optimize the channel quality for D_2 by modifying the IRS's characteristics[1]. With $g_{DI,h}$ and $g_{IR,h}$ being the h-th elements of $\mathbf{g}_{DI}$ and $\mathbf{g}_{IR}$, respectively, this is done in order to maximize $\left|\mathbf{g}_{DI}\Phi\mathbf{g}_{IR}\right| = \left|\sum_{h=1}^{H} \alpha_h g_{DI,h} g_{IR,h} e^{j\chi_h}\right|$. To do this, each element's phase-shift variable χ_h may be adjusted such that all $g_{DI,h} g_{IR,h} e^{j\chi_h}$ phases are set to the same. Since $\widetilde{\chi}$ is an arbitrary constant that ranges in $[0, 2\pi)$, there is more than one solution for $\{\chi_h\}$, and $\chi_h = \widetilde{\chi} - \arg\left(g_{DI,h} g_{IR,h}\right)$ provides the generalized solution. Following the adoption of the optimum $\{\chi_h\}$, we have

$$\left|\mathbf{g}_{DI}\Phi\mathbf{g}_{IR}\right|^2 = \alpha^2 \left(\sum_{h=1}^{H} \left|g_{DI,h}\right| \left|g_{IR,h}\right|\right)^2, \tag{21}$$

where $\alpha = \alpha_h, \forall_h$ are assumed without sacrificing generality.

According to [3,30], the PDF and CDF of $\Upsilon = \frac{\left(\sum_{h=1}^{H} |g_{DI,h}||g_{IR,h}|\right)^2}{H(1-\kappa)}$ are written as follows:

$$f_{\Upsilon}(w) = e^{-\frac{w+\sigma_{DIR}}{2}} \sum_{n=0}^{\infty} \frac{\sigma_{DIR}^n w^{n-\frac{1}{2}}}{n! 2^{2n+\frac{1}{2}} \Gamma\left(n + \frac{1}{2}\right)}, \tag{22}$$

and

$$F_{\Upsilon}(w) = e^{-\frac{\sigma_{DIR}}{2}} \sum_{n=0}^{\infty} \frac{\sigma_{DIR}^n \gamma\left(i + \frac{1}{2}, \frac{w}{2}\right)}{n! 2^n \Gamma\left(n + \frac{1}{2}\right)}, \tag{23}$$

[1]To streamline the analysis and concentrate on phase shift optimization, the IRS's placement and number of elements are set in this study. Future studies will examine the open research question of optimizing the IRS deployment position and number of elements to improve system performance and communication security

where $\sigma_{DIR} = \frac{H\kappa}{1-\kappa}$, $\kappa = \frac{1}{m_{g_{DI}} m_{g_{IR}}} \left(\frac{\Gamma\left(m_{g_{DI}} + \frac{1}{2}\right)}{\Gamma\left(m_{g_{DI}}\right)} \right)^2 \left(\frac{\Gamma\left(m_{g_{IR}} + \frac{1}{2}\right)}{\Gamma\left(m_{g_{IR}}\right)} \right)^2$. The distribution of Υ tends to be noncentral chi-squared as $\Upsilon \sim \Upsilon^2\left(\sigma_{DIR}\right)$ when the number of reflecting components H is large. Gamma and lower incomplete gamma functions are denoted by $\Gamma\left(.\right)$ and $\gamma\left(.,.\right)$, respectively.

From (20), Θ_{1a} can be rewritten as

$$\begin{aligned}
\Theta_{1a} &= \Pr\left(\left|\mathbf{g}_{DI}\Phi\mathbf{g}_{IR}\right|^2 > \frac{\gamma_2^{(th)}\left(\left|g_{DR}\right|^2 d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right) \\
&= \Pr\left(\frac{\alpha\left(\sum\limits_{h=1}^{H}\left|g_{DI,h}\right|\left|g_{IR,h}\right|\right)^2}{H\left(1-\kappa\right)} > \frac{\gamma_2^{(th)}\left(\left|g_{DR}\right|^2 d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right) \\
&= \Pr\left(\left(\sum_{h=1}^{H}\left|g_{DI,h}\right|\left|g_{IR,h}\right|\right)^2 > \frac{\gamma_2^{(th)} H\left(1-\kappa\right)\left(\left|g_{DR}\right|^2 d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right).
\end{aligned} \tag{24}$$

Given (14) and (23), Θ_{1a} may be expressed as follows:

$$\begin{aligned}
\Theta_{1a} &= \int_0^\infty \left[1 - F_{\left(\sum\limits_{h=1}^{H}\left|g_{DI,h}\right|\left|g_{IR,h}\right|\right)^2}\left(\frac{\gamma_2^{(th)} H\left(1-\kappa\right)\left(x d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right) \right] f_{\left|g_{DR}\right|^2}\left(x\right) dx \\
&= 1 - \frac{\exp\left(-\frac{\sigma_{DIR}}{2}\right)}{\sigma_{g_{DR}}} \sum_{n=0}^{\infty} \frac{\sigma_{DIR}^n}{n! 2^n \Gamma\left(n+\frac{1}{2}\right)} \int_0^\infty \gamma\left(i + \frac{1}{2}, \frac{\gamma_2^{(th)} H\left(1-\kappa\right)\left(x d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{2\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right) \\
&\quad \times \exp\left(-\frac{x}{\sigma_{g_{DR}}} \right) dx.
\end{aligned} \tag{25}$$

It is rather challenging to derive the above equation in a closed form for the end outcome. As a result, we estimate the integral between 0 and a big number L [4,34]. Θ_{1a} is now rewritten as:

$$\begin{aligned}
\Theta_{1a} &= 1 - \frac{\exp\left(-\frac{\sigma_{DIR}}{2}\right)}{\sigma_{g_{DR}}} \sum_{n=0}^{\infty} \frac{\sigma_{DIR}^n}{n! 2^n \Gamma\left(n+\frac{1}{2}\right)} \int_0^L \gamma\left(i + \frac{1}{2}, \frac{\gamma_2^{(th)} H\left(1-\kappa\right)\left(x d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{2\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right) \\
&\quad \times \exp\left(-\frac{x}{\sigma_{g_{DR}}} \right) dx.
\end{aligned} \tag{26}$$

Next, we let $u = \frac{2x-L}{L} \Rightarrow x = \frac{uL+L}{2}$, and at this point, Θ_{1a} is rewritten as follows:

$$\begin{aligned}
\Theta_{1a} &= 1 - \frac{L\exp\left(-\frac{\sigma_{DIR}}{2}\right)}{2\sigma_{g_{DR}}} \sum_{n=0}^{\infty} \frac{\sigma_{DIR}^n}{n! 2^n \Gamma\left(n+\frac{1}{2}\right)} \\
&\quad \times \int_{-1}^{1} \gamma\left(i + \frac{1}{2}, \frac{\gamma_2^{(th)} H\left(1-\kappa\right)\left(\frac{uL+L}{2} d_{DR}^{-\rho}\mu_1\beta_{D_1} + 1\right)}{2\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}} \right) \exp\left(-\frac{\frac{uL+L}{2}}{\sigma_{g_{DR}}} \right) du.
\end{aligned} \tag{27}$$

Gaussian-Chebyshev quadrature is applied [35], and we obtain

$$\Theta_{1a} = 1 - \frac{\pi L \exp\left(-\frac{\sigma_{DIR}}{2}\right)}{2V\sigma_{g_{DR}}} \sum_{n=0}^{\infty}\sum_{v=1}^{V} \frac{\sqrt{1-u_v^2}\sigma_{DIR}^n}{n!2^n\Gamma\left(n+\frac{1}{2}\right)} \times \gamma\left(i+\frac{1}{2}, \frac{\gamma_2^{(th)} H(1-\kappa)\left(\psi_v d_{DR}^{-\rho}\mu_1\beta_{D_1}+1\right)}{2\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}}\right)\exp\left(-\frac{\psi_v}{\sigma_{g_{DR}}}\right), \tag{28}$$

where $\psi_v = \frac{u_v L + L}{2}$, $u_v = \cos\left[\frac{(2v-1)\pi}{2V}\right]$, and the accuracy and complexity trade-off parameter is called V.

Using (15) and (20), Θ_{1b} may be expressed as:

$$\Theta_{1b} = \Pr\left(|g_{RB}|^2 > \frac{\gamma_2^{(th)}}{d_{RB}^{-\rho}\beta_{RB}\left(\mu_2 - \gamma_2^{(th)}\mu_1\right)}\right) = 1 - F_{|g_{RB}|^2}\left(\frac{\gamma_2^{(th)}}{d_{RB}^{-\rho}\beta_{RB}\left(\mu_2 - \gamma_2^{(th)}\mu_1\right)}\right) = \exp\left(-\frac{\gamma_2^{(th)}}{d_{RB}^{-\rho}\beta_{RB}\sigma_{g_{RB}}\left(\mu_2 - \gamma_2^{(th)}\mu_1\right)}\right). \tag{29}$$

By combining (28) and (29) into (20), the closed-form expression of Ω_{D_2} is rewritten as follows:

$$\Omega_{D_2} = 1 - \left[1 - \frac{\pi L \exp\left(-\frac{\sigma_{DIR}}{2}\right)}{2V\sigma_{g_{DR}}} \sum_{n=0}^{\infty}\sum_{v=1}^{V} \frac{\sqrt{1-u_v^2}\sigma_{DIR}^n}{n!2^n\Gamma\left(n+\frac{1}{2}\right)} \times\gamma\left(i+\frac{1}{2}, \frac{\gamma_2^{(th)} H(1-\kappa)\left(\psi_v d_{DR}^{-\rho}\mu_1\beta_{D_1}+1\right)}{2\alpha d_{DI}^{-\rho} d_{IR}^{-\rho}\mu_2\beta_{D_2}}\right)\exp\left(-\frac{\psi_v}{\sigma_{g_{DR}}}\right)\right] \times \exp\left(-\frac{\gamma_2^{(th)}}{d_{RB}^{-\rho}\beta_{RB}\sigma_{g_{RB}}\left(\mu_2 - \gamma_2^{(th)}\mu_1\right)}\right). \tag{30}$$

As with (18), the OP at D_2 for A FC packets may be expressed exactly as follows:

$$OP_{D_2,A} = \sum_{Z_{BS}}^{A-1}\binom{Z_{th}}{Z_{BS}}(1-\Omega_{D_2})^{Z_{BS}}(\Omega_{D_2})^{Z_{th}-Z_{BS}}. \tag{31}$$

3.3 Throughput Assessment

One crucial performance indicator for wireless communication systems is system throughput. System throughput research is very important for real-world applications. Information is sent continuously from the *BS* to D_i in the delay-limited transmission mode, which causes outages because of the impact of wireless fading channels. Thus, in the delay-limited transmission mode, the OP determines the system throughput. The expression for D_i's delay-limited throughput is [5]

$$\Im_{D_i,A} = (1 - OP_{D_i,A})R_{D_i}. \tag{32}$$

Moreover, by applying (32), the system throughput can be expressed as follows:

$$\Im_{SYM,A} = \Im_{D_1,A} + \Im_{D_2,A}. \tag{33}$$

3.4 Diversity Evaluation

The slope of the OP curve in the high SNR range is the definition of diversity order in communication systems. It is frequently used to evaluate the outage performance of wireless communication networks and demonstrates how quickly the OP drops as the broadcast SNR increases. The following is a mathematical expression for the diversity order [4,5]:

$$d_{d_i} = -\lim_{\beta\to\infty} \frac{\log\left(OP^{\infty}_{D_i,A}(\beta)\right)}{\log(\beta)}. \tag{34}$$

where we assume that $\beta = \beta_{D_i} = \beta_{RB}$. In this case, $OP^{\infty}_{D_i,A}$ stands for the OP value of the user D_i in question. It is important to remember that the system has zero diversity order for every user while $\lim_{\beta\to\infty} \exp(-x/\beta) \approx 1 - (x/\beta)$ holds [4,36]. The impact of additional limiting parameters outside the SNR results in the saturation of outage performance.

4 IP-Based Security Evaluation

An important PLS metric is the IP, which measures the probability that a hacker may successfully collect and decode private data sent over a wireless channel. It is the likelihood that a security breach will occur if the *E*'s data rate is higher than the difference between the source transmission rate and the channel capacity of the authorized user.

4.1 D_1's IP Assessment

Eqs. (6) and (12) may be used to determine user D_1's IP for one FC packet, as shown [8,37]

$$\begin{aligned}\Delta_{D_1} &= \Pr\left(\gamma^{(q_1)}_{E_1} > \gamma^{(th)}_1, \gamma^{(q_1)}_{RE} > \gamma^{(th)}_1\right)\\ &= \Pr\left(|g_{DE1}|^2 d^{-\rho}_{DE1}\mu_1\beta_{E_1} > \gamma^{(th)}_1\right)\Pr\left(|g_{RE}|^2 d^{-\rho}_{RE}\mu_1\beta_{RE} > \gamma^{(th)}_1\right)\\ &= \Pr\left(|g_{DE1}|^2 > \frac{\gamma^{(th)}_1}{d^{-\rho}_{DE1}\mu_1\beta_{E_1}}\right)\Pr\left(|g_{RE}|^2 > \frac{\gamma^{(th)}_1}{d^{-\rho}_{RE}\mu_1\beta_{RE}}\right).\end{aligned} \tag{35}$$

Next, based on the CDF function mentioned in (15), Δ_{D_1} is calculated as follows:

$$\begin{aligned}\Delta_{D_1} &= \left[1 - F_{|g_{DE1}|^2}\left(\frac{\gamma^{(th)}_1}{d^{-\rho}_{DE1}\mu_1\beta_{E_1}}\right)\right]\left[1 - F_{|g_{RE}|^2}\left(\frac{\gamma^{(th)}_1}{d^{-\rho}_{RE}\mu_1\beta_{RE}}\right)\right]\\ &= \exp\left(-\frac{\gamma^{(th)}_1}{d^{-\rho}_{DE1}\mu_1\beta_{E_1}\sigma_{g_{DE1}}}\right)\exp\left(-\frac{\gamma^{(th)}_1}{d^{-\rho}_{RE}\mu_1\beta_{RE}\sigma_{g_{RE}}}\right)\\ &= \exp\left(-\frac{\gamma^{(th)}_1}{d^{-\rho}_{DE1}\mu_1\beta_{E_1}\sigma_{g_{DE1}}} - \frac{\gamma^{(th)}_1}{d^{-\rho}_{RE}\mu_1\beta_{RE}\sigma_{g_{RE}}}\right).\end{aligned} \tag{36}$$

From (36), in the case of one FC packet, represent the IP of D_1. We continue with the IP analysis for A FC packets based on these two equations. It should be noted that the data meant for the *BS* will be intercepted if E gathers enough A-encoded packets before D_1's transmission concludes. Consequently, the IP of D_1 for A FC packets may be used as follows [8,38]:

$$IP_{D_1,A} = \Pr\left(Z_E = A \middle| Z_{D_1} \le Z_{th}\right). \tag{37}$$

Continuing, the IP of D_1 for A FC packets may be found using the binomial distribution definition [39, Eq. (9)]:

$$IP_{D_1,A} = \sum_{y=A}^{Z_{th}} \begin{pmatrix} y-1 \\ y-A \end{pmatrix} (\Delta_{D_1})^A (1-\Delta_{D_1})^{y-A}. \tag{38}$$

4.2 D_2's IP Assessment

Just as in (35), and based on (5) and (11), user D_2's IP is determined as shown in [8,37]:

$$\Delta_{D_2} = \Pr\left(\gamma_{E_1}^{(q_2)} > \gamma_2^{th}, \gamma_{RE}^{(q_2)} > \gamma_2^{th}\right) = \underbrace{\Pr\left(\gamma_{E_1}^{(q_2)} > \gamma_2^{th}\right)}_{\Theta_{2a}} \underbrace{\Pr\left(\gamma_{RE}^{(q_2)} > \gamma_2^{th}\right)}_{\Theta_{2b}}. \tag{39}$$

Using (39), Θ_{2a} is computed as follows:

$$\begin{aligned}
\Theta_{2a} &= \Pr\left(\gamma_{E_1}^{(q_2)} > \gamma_2^{th}\right) = \Pr\left(|g_{DE2}|^2 > \frac{\gamma_2^{th}\left(|g_{DE1}|^2 d_{DE1}^{-\rho}\mu_1\beta_{E_1} + 1\right)}{d_{DE2}^{-\rho}\mu_2\beta_{E_2}}\right) \\
&= \int_0^\infty \left(1 - F_{|g_{DE2}|^2}\left(\frac{\gamma_2^{th}\left(x d_{DE1}^{-\rho}\mu_1\beta_{E_1} + 1\right)}{d_{DE2}^{-\rho}\mu_2\beta_{E_2}}\right)\right) f_{|g_{DE1}|^2}(x)\, dx \\
&= \frac{1}{\sigma_{g_{DE1}}} \exp\left(-\frac{\gamma_2^{th}}{d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}}\right) \int_0^\infty \exp\left(-\left(\frac{\gamma_2^{th} d_{DE1}^{-\rho}\mu_1\beta_{E_1}}{d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}} + \frac{1}{\sigma_{g_{DE1}}}\right) x\right) dx \\
&= \frac{d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}}{\gamma_2^{th} d_{DE1}^{-\rho}\mu_1\beta_{E_1}\sigma_{g_{DE1}} + d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}} \exp\left(-\frac{\gamma_2^{th}}{d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}}\right).
\end{aligned} \tag{40}$$

Next, Θ_{2b} can be expressed as follows:

$$\begin{aligned}
\Theta_{2b} &= \Pr\left(\gamma_{RE}^{(q_2)} > \gamma_2^{th}\right) = \Pr\left(|g_{RE}|^2 > \frac{\gamma_2^{th}}{d_{RE}^{-\rho}\beta_{RE}\left(\mu_2 - \gamma_2^{th}\mu_1\right)}\right) \\
&= 1 - F_{|g_{RE}|^2}\left(\frac{\gamma_2^{th}}{d_{RE}^{-\rho}\beta_{RE}\left(\mu_2 - \gamma_2^{th}\mu_1\right)}\right) = \exp\left(-\frac{\gamma_2^{th}}{d_{RE}^{-\rho}\beta_{RE}\sigma_{g_{RE}}\left(\mu_2 - \gamma_2^{th}\mu_1\right)}\right).
\end{aligned} \tag{41}$$

By combining (40) and (41) into (39), the closed-form expression of Δ_{D_2} is rewritten as follows:

$$\Delta_{D_2} = \frac{d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}}{\gamma_2^{th} d_{DE1}^{-\rho}\mu_1\beta_{E_1}\sigma_{g_{DE1}} + d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}} \exp\left(-\frac{\gamma_2^{th}}{d_{DE2}^{-\rho}\mu_2\beta_{E_2}\sigma_{g_{DE2}}} - \frac{\gamma_2^{th}}{d_{RE}^{-\rho}\beta_{RE}\sigma_{g_{RE}}\left(\mu_2 - \gamma_2^{th}\mu_1\right)}\right). \tag{42}$$

As with (37), the IP at D_2 for A FC packets may be expressed exactly as follows:

$$IP_{D_2,A} = \sum_{y=A}^{Z_{th}} \begin{pmatrix} y-1 \\ y-A \end{pmatrix} (\Delta_{D_2})^A (1-\Delta_{D_2})^{y-A}. \tag{43}$$

5 DNN Approach for Predicting Main OP/IP

Here, we provide a DNN model for OP/IP evaluation[2]. In situations where the system model is complex and conventional mathematical derivation techniques are challenging to apply, this approach offers a data-driven solution. The DNN model will be utilized to reduce execution time and enhance accuracy.

5.1 The DNN Configuration Description

A feed-forward neural network is the type of DNN model that was employed in this investigation. Please see Fig. 2 for a thorough description of its setup. An input layer, S_q hidden layers, and an output layer are among the several layers that make up the DNN architecture.

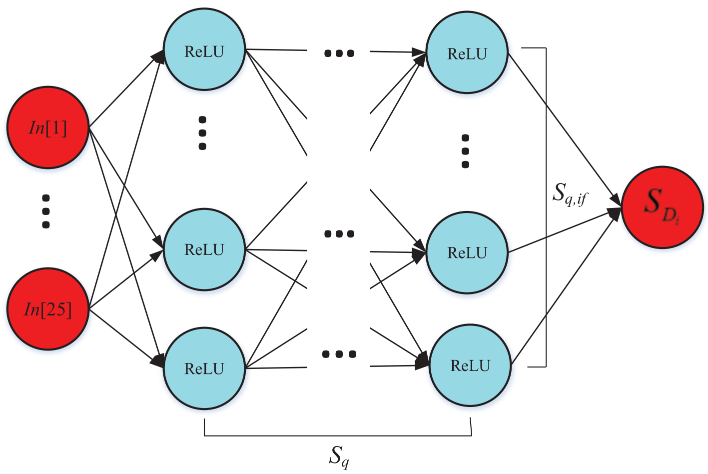

Figure 2: Building a DNN model for prediction

According to Table 1, the main system parameters are sent to the server as input values in this model. Each of these values corresponds to one of the 25 neurons. Predictions for OP or IP are produced by the output layer, which consists of a single neuron. According to sources [8,42,43], this procedure involves applying a linear function and the corresponding activation function. Furthermore, the parameters include solely weights and biases, and the neurons are 25 in number, matching the 25 input characteristics. The system uses the rectified linear unit (ReLU) activation function, and each hidden layer (designated as layer q with parameter $q = 1, \ldots, S_q$) has $S_{q,if}$ neurons.

Table 1: The parameters of the DNN [3,8,27,30,42,43]

Inputs	Values	Inputs	Values	Inputs	Values
β	[10:50] dBm	$\sigma_{g_{DE2}}$	10	d_{DE1}	2 m
β_E	[5:60] dBm	ρ	2	d_{DE2}	7 m

(Continued)

[2]Although the DNN model offers a quick and efficient method for predicting key performance metrics like OP and IP, it's crucial to understand that the accuracy of these predictions is directly impacted by the model's quality [8,40,41]. Since the model is data-driven by nature, factors that affect its output include the training dataset, the network architecture, and the optimization strategies used during training. Consequently, meticulous training procedures and thorough validation are required to ensure the accuracy of the forecasts. Instead of replacing traditional analytical equations, the DNN is employed in this study as an auxiliary approach to address scenarios when regular mathematical modeling is not viable due to the system's complexity.

Table 1 (continued)

Inputs	Values	Inputs	Values	Inputs	Values
Z_{th}	OP: [10,12,14]; IP: 10	R_{D_1}	0.1 bps/Hz	d_{DI}	10 m
μ_1	0.1	R_{D_2}	0.1 bps/Hz	d_{IR}	10 m
μ_2	0.9	$m_{g_{DI}}$	2	d_{RE}	10 m
$\sigma_{g_{RB}}$	1	$m_{g_{IR}}$	2	d_{RB}	5 m
$\sigma_{g_{DR}}$	1	H	10	d_{DR}	5 m
$\sigma_{g_{RE}}$	10	α	0.9		
$\sigma_{g_{DE1}}$	10	A	OP: 10; IP: [6,8,10]		

5.2 Data Set Building

The link between input and output is represented by parameter $Da[q] = [In[q], OP_{D_i,sim}]$, whereas parameter $In[q]$ is a feature vector that contains all of the input parameters specified in Table 1. The server that is connected to the base station processes q samples from the dataset. The feature vector $In[q]$ is used in Monte Carlo simulations, which then yield an expected secure metric, parameter $OP_{D_i,sim}$. In conclusion, the dataset is created by concatenating a total of 5×10^5 data points. Next, three subsets of the dataset are created: 80% for training ($\wp_{tra}$), 10% for validation ($\wp_{va}$), and 10% for testing ($\wp_{te}$).

The performance of the suggested DNN technique is assessed using the Mean Square Error, or MSE, which is specified by parameter $Mse = \frac{1}{|\wp_{te}|}\sum_{q=0}^{|\wp_{te}|-1}(S_{D_i} - OP_{D_i,sim})$. The main procedures for training and assessing this deep neural network are outlined in Algorithm 1 from references [8,42,43].

6 Mathematical Results

The performance of the network is assessed numerically in this section. Monte Carlo simulations are also used to confirm correctness. The main simulation parameters utilized in this work are selected based on recent studies in the field. Specifically, the power allocation coefficient is set to $\mu_1 = 0.1$, and the users' rate thresholds are configured as $R_{D_1} = R_{D_2} = 0.1$ bps/Hz, following the approach in [8,42,43]. The path loss factor is set to $\rho = 2$ as commonly used in related works [30]. Regarding distances, we consider $d_{DI} = d_{IR} = d_{RE} = 10$ m, $d_{RB} = d_{DR} = 5$ m, $d_{DE1} = 2$ m, $d_{DE2} = 7$ m, which are consistent with the setups in [27]. Additional system parameters include $\sigma_{g_{RB}} = \sigma_{g_{DR}} = 1$, $\sigma_{g_{RE}} = \sigma_{g_{DE1}} = \sigma_{g_{DE2}} = 10$, $m_{g_{DI}} = m_{g_{IR}} = 2$, $H = 10$, $\alpha = 0.9$, $A = Z_{th} = 10$, $V = 100$. These numbers were selected to ensure fair comparison and consistency with other studies [3]. Moreover, we assume that $\beta = \beta_{D_i} = \beta_{RB}$, and $\beta_E = \beta_{E_i} = \beta_{RE}$.

By contrasting the training and validation curves, Fig. 3 verifies that the DNN attains the desired accuracy. Interestingly, the MSE successfully approaches its minimal level, as seen by the tight alignment of these two curves. It takes 12 epochs to attain the lowest MSE.

The OP of the uplink IRS-NOMA system for different values of β and Z_{th} is shown in Fig. 4. Both users' simulation results are in good agreement with the analytical findings obtained from equations (18) and (19). Furthermore, as seen in Fig. 4, user D_i's OP dramatically drops as β rises. In particular, when β goes from 18 dBm to 50 dBm, the OP for user D_1 reduces significantly, and when β climbs from 10 to 47 dBm, the OP for user D_2 significantly decreases. This benefit stems from the fact that an increase in β implies a higher SNR for the transmission process. By strengthening the received signal at the destination and reducing its susceptibility to noise and fading effects, increased transmission power enhances signal recognition capabilities and significantly reduces the chance of an outage. Additionally, user D_2's OP is considerably lower than user D_1's. Another important finding from this figure is that as Z_{th} rises from 10 to 14, user D_i's OP drastically decreases. This is to be expected as the BS can send data more effectively when there are more time slots available. Increased packet transmission time reduces network congestion, thereby lowering packet loss and enhancing user throughput. As a result, the total system performance is greatly improved by this change. These results underscore the importance of employing dynamic power allocation techniques and optimizing time slot allocation in uplink IRS-NOMA-assisted communication systems. Furthermore, the suggested DNN techniques are further validated by the high agreement between the simulation and analytical results.

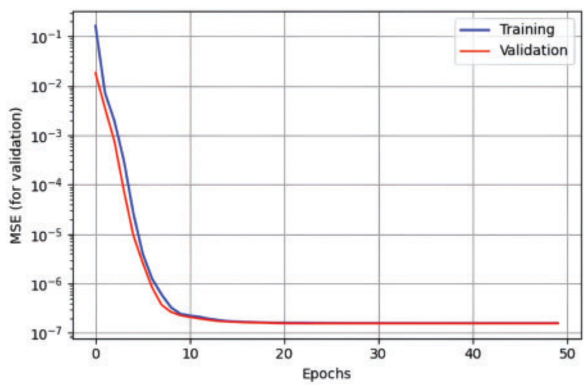

Figure 3: The convergence of the MSE for user D_1's OP across the DNN's training and validation phases

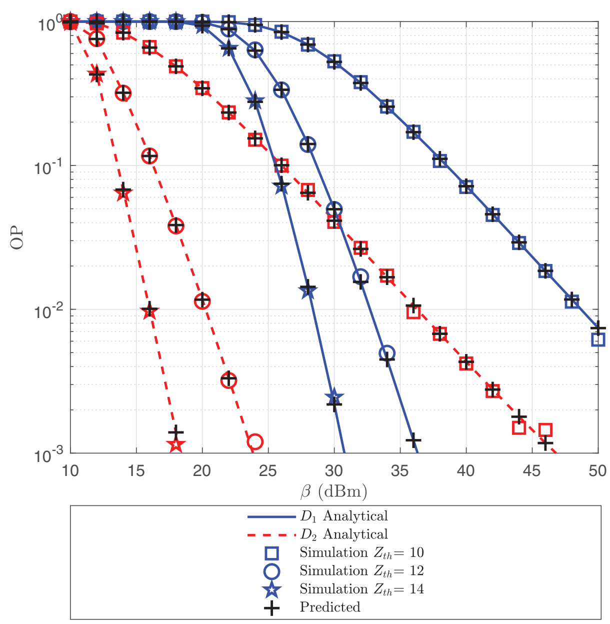

Figure 4: OP of D_1 and D_2 in comparison to β, with $Z_{th} = \{10; 12; 14\}$

Fig. 5 displays the OP of the uplink IRS-NOMA system for a range of β values with varying $R_{D_1} = R_{D_2}$ values. As in the preceding figure, it is evident that user D_2's OP is substantially lower than user D_1's. Furthermore, within the operating range of the system, user D_i's OP significantly drops as β rises. Additionally, user D_i's OP improves noticeably when $R_{D_1} = R_{D_2}$ goes from 0.1 to 0.3 bps/Hz. This suggests that parameter changes in $R_{D_1} = R_{D_2}$ significantly affect the system's overall performance.

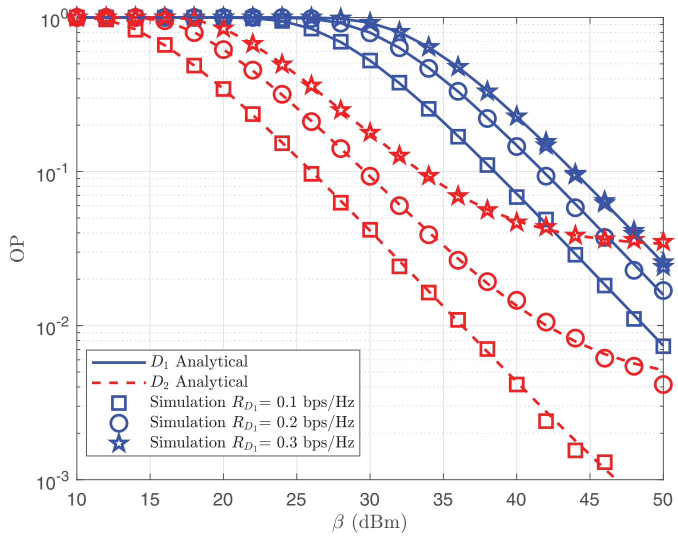

Figure 5: OP of D_1 and D_2 in comparison to β, with $R_{D_1} = R_{D_2} = \{0.1; 0.2; 0.3\}$ bps/Hz

As the number of elements H varies, Fig. 6 shows the OP of both users as a function of β. By looking at the figure, we can observe that both users D_1 and D_2's OP drastically drop within the system's operating range as β rises. Additionally, the OP of D_2 substantially decreases as H rises. Moreover, the OP of D_2 is greater than that of D_1 when H is set to 1, yet it stays lower than that of D_1 when H is increased from 5 to 20. The increase of IRS elements, which improves signal transmission, is responsible for this improvement in OP. The findings highlight that better overall OP performance is correlated with a greater number of IRS components. This result highlights the importance of optimizing the IRS design to enhance end-user signal quality and reliability significantly. It is important to remember, too, that adding more IRS features also makes the system more complex. This includes higher computing costs for optimization techniques, a more complex beamforming design, and increased overhead for channel estimates. As a result, while more IRS parts enhance performance, they also require an effective system design to strike a balance between acceptable complexity and performance improvements.

As we modify parameter A, we exhibit the IP for two users as a function of parameter β_E in Fig. 7. The numerical results obtained from Eqs. (37) and (43), respectively, match the simulation findings for users D_1 and D_2. Examining the figure, we can observe that the interception probability of user D_i increases in tandem with the rise in parameter β_E from 5 to 60 dBm. This trend might be explained by the fact that as β_E increases, the SNR at the E also significantly improves. A higher SNR enables the E to receive a stronger and clearer version of the broadcast signal, making unauthorized interception easier and more effective. This result is consistent with real-world scenarios, where better reception conditions raise the likelihood of successfully eavesdropping on authorized users' messages. Furthermore, user D_1 has a far lower chance of being intercepted than user D_2. Because D_1 is closer to both the R and the BS, it has superior transmission circumstances and larger channel gains, which explains this. However, the channel quality is worse, and eavesdropping is more possible due to D_2's greater distance. As a result, for the majority of parameter values, D_1 continuously shows a lower interception probability than D_2. One important finding from this figure is that user D_i's interception probability significantly drops when parameter A rises from 6 to 10. This is because eavesdropping or signal interception at the eavesdropper gets more difficult as the number of encoded A packets rises. Unauthorized access becomes more challenging due to the increased volume of signal packets. The potential of machine learning paradigms to improve network security and performance forecasting in upcoming wireless communication systems is further highlighted by the validation of DNN-based predictions against accepted approaches.

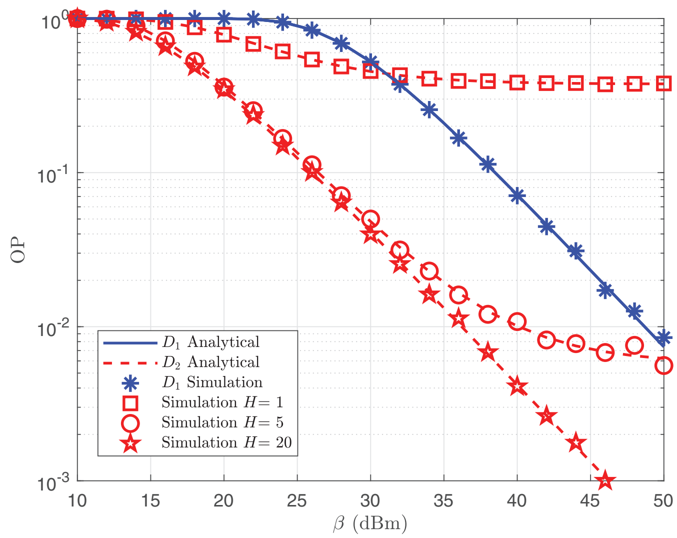

Figure 6: OP of D_1 and D_2 in comparison to β, with $H = \{1; 5; 20\}$

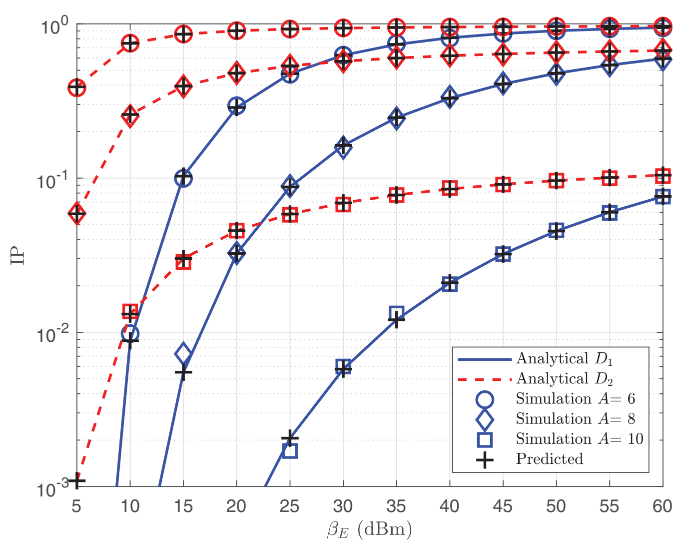

Figure 7: IP of D_1 and D_2 in comparison to β_E, with $A = \{6; 8; 10\}$

The IP is displayed vs. the threshold parameter β_E for a range of μ_1 values in Fig. 8. First, we see that user D_i's IP rises in tandem with β_E increasing from 5 to 60 dBm. Second, user D_1's IP dramatically increases while user D_2's IP significantly lowers as μ_1 increases from 0.1 to 0.2. This suggests that the system's interception likelihood is influenced dramatically by the power allocation coefficient of the two users. The IP plotted against the threshold parameter β_E for various values of $d_{DE1} = d_{DE2}$ is also shown in Fig. 9. In the last figure, user D_i's IP climbs dramatically when β_E increases. Furthermore, user D_1's IP is still significantly lower than user D_2's. A critical finding from this figure is that user D_i's IP drastically drops when the parameter $d_{DE1} = d_{DE2}$ increases. This may be explained by the fact that eavesdropping on user D_i's signal gets more difficult as the distance between the eavesdropper and user D_i rises.

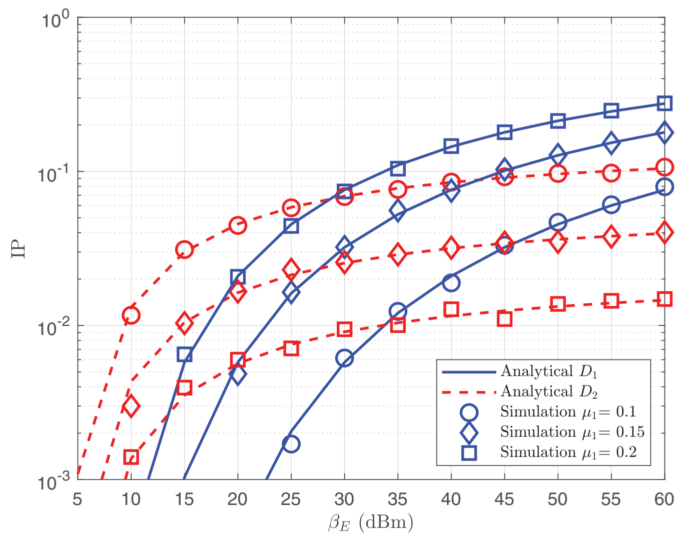

Figure 8: IP of D_1 and D_2 in comparison to β_E, with $\mu_1 = \{0.1; 0.15; 0.2\}$

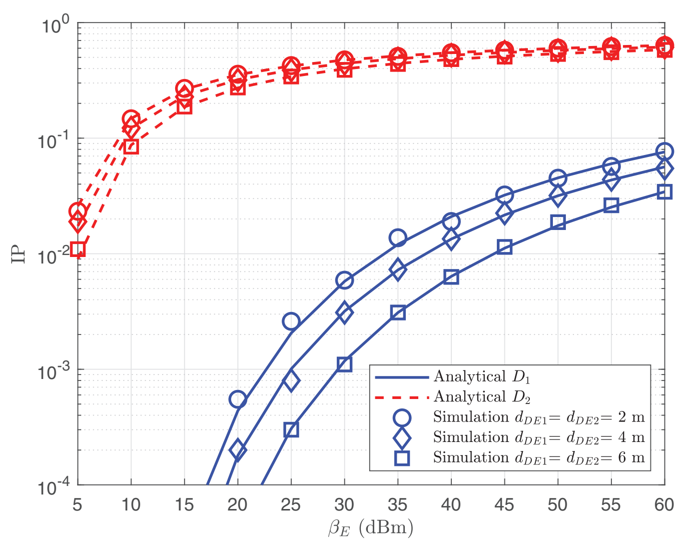

Figure 9: IP of D_1 and D_2 in comparison to β_E, with $d_{DE1} = d_{DE2} = \{2; 4; 6\}$ m

The throughput performance of user D_i and the system as a whole about parameter β is shown in Fig. 10 for a range of parameter $d_{DI} = d_{IR} = d_{DR}$ values. It is evident that the throughput of user D_i and the system as a whole greatly improves when β rises from 10 to 60 dB. Among them, the system throughput is the highest, while the throughput of user D_1 is the lowest. This observation aligns with the previous explanations and simulations regarding OP. However, it is important to note that when β exceeds approximately 57 dB, the throughput of both user D_i and the overall system reaches a saturation point. Utilizing this information can help optimize system design and increase throughput. Additionally, a key discovery from this figure is the effect of changes in the parameters $d_{DI} = d_{IR} = d_{DR}$ on throughput. When $d_{DI} = d_{IR} = d_{DR}$ increases from 5 to 25 m, user D_i's throughput and the system's overall throughput substantially decrease. This might be explained by the fact that signal transmission and reception become more difficult with increasing device distance, lowering system throughput. These findings demonstrate the importance of distance-related factors in the realistic design and implementation of these types of communication systems.

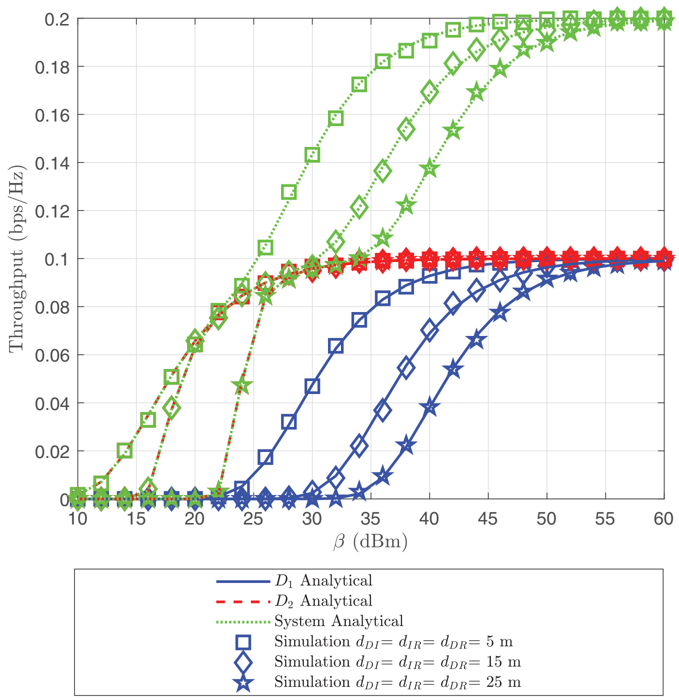

Figure 10: Throughput of D_1 and D_2 in comparison to β, with $d_{DI} = d_{IR} = d_{DR} = \{5; 15; 25\}$ m

The obtained results clearly demonstrate that the system's outage and intercept performance are susceptible to variations in key parameters such as H, β, β_E, μ_1, A, d_{DE1}, d_{DE2}, etc. These findings suggest that careful parameter tuning is necessary to maintain an optimal trade-off between security and reliability. This result is consistent with previous studies [3,27,28], which similarly emphasized the significance of parameter sensitivity in real-world system design. Our study provides an important foundation for future research on robust and adaptable deployment strategies in real-world scenarios by integrating these findings into our proposed IRS-NOMA paradigm.

7 Conclusions

This study analyzes the OP and IP of an uplink NOMA system assisted by an IRS and utilizing FC, while also considering the presence of an eavesdropper. Additionally, a DNN is integrated into the system to predict its performance. The uplink NOMA transmission system demonstrates strong security performance due to the use of dual transmission links (including relay forwarding) from end users to the *BS*, combined with IRS assistance. Closed-form expressions for OP and IP are derived to evaluate the system's reliability and security. Simulation results indicate that the system's security performance is influenced by factors such as power allocation, the number of IRS reflecting elements, user threshold rates, encoded packet limitations, and power allocation coefficients. The theoretical findings in this study have broad applicability for deploying uplink NOMA in mobile networks. Simulations show strong agreement between theoretical and empirical results, with simulation points closely matching analytical predictions. This validates the accuracy of the proposed formulas and ensures the reliability of the data analysis in this study.

We are conscious of several limitations in our research. Despite the performance improvements enabled by the IRS, the system's OP and IP remain sensitive to several practical factors, such as user distance, channel fading, and IRS configuration. These factors may limit the achievable gains in realistic scenarios, particularly when users are located far from the IRS or experience severe path loss. Therefore, further research is needed to develop adaptive IRS designs and robust optimization strategies to maintain system reliability under diverse deployment conditions. This highlights the need for future studies that explore more resilient IRS-assisted communication schemes and investigate their effectiveness under practical constraints. Additionally, the present system model has a fixed user count and a more straightforward network design. The scalability of the proposed method may be constrained in real-world scenarios where user density is increasing or network architecture is changing dynamically. Future studies should include more flexible and scalable designs to maintain performance in a range of complex network situations. The research can be extended by applying the model to systems with a larger number of users, allowing for security performance analysis in more complex environments. Potential scenarios include multi-user environments with resource competition or urban settings with numerous obstacles affecting signal transmission. Finally, to verify the accuracy and feasibility of the theoretical model and developed algorithms, conducting real-world experiments would be a crucial step in demonstrating the effectiveness of the proposed solutions.

Acknowledgement: The authors are grateful to all the editors and anonymous reviewers for their comments and suggestions.

Funding Statement: This work was supported in part by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant 102.04-2021.57; and in part by Culture, Sports and Tourism R&D Program through the Korea Creative Content Agency grant funded by the Ministry of Culture, Sports and Tourism in 2024 (Project Name: Global Talent Training Program for Copyright Management Technology in Game Contents, Project Number: RS-2024-00396709, Contribution Rate: 100%).

Author Contributions: Phu Tran Tin, Quy-Anh Bui, and Minh-Sang Van Nguyen designed the algorithm, performed the theoretical analysis, checked the results, and wrote the manuscript. Phu Tran Tin and Minh-Sang Van Nguyen implemented the simulation and contributed to the manuscript preparation. Agbotiname Lucky Imoize and Byung-Seo Kim were responsible for formulating the research issues and revising the paper. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analyzed during this study are included in this published article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Hamza KM, Basharat S, Jung H, Gidlund M, Hassan SA. Secrecy analysis of RIS-assisted uplink NOMA systems under nakagami-m fading. In: 2024 IEEE International Conference on Communications Workshops (ICC Workshops). Denver, CO, USA; 2024. p. 1511–6.
2. Dai L, Wang B, Yuan Y, Han S, Chih-lin I, Wang Z. Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends. IEEE Commun Mag. 2015;53(9):74–81. doi:10.1109/mcom.2015.7263349.
3. Tin PT, Nguyen MSV, Tran DH, Nguyen CT, Chatzinotas S, Ding Z, et al. Performance analysis of user pairing for active RIS-enabled cooperative NOMA in 6G cognitive radio networks. IEEE Internet Things J. 2024;11(23):37675–92. doi:10.1109/jiot.2024.3439377.
4. Van Nguyen MS, Do DT, Vahid A, Muhaidat S, Sicker D. Enhancing NOMA backscatter IoT communications with RIS. IEEE Internet Things J. 2024;11(4):5604–22. doi:10.1109/jiot.2023.3308786.
5. Gong X, Huang C, Yue X, Yang Z, Liu F. Performance analysis of RIS assisted NOMA networks over rician fading channels. Comput Model Eng Sci. 2023;135(3):2531–55. doi:10.32604/cmes.2023.024940.
6. Le AT, Vu TH, Benevides da Costa D, Voznak M. Hybrid power-frequency multiple access with SIC-free for holographic reconfigurable intelligent surface-based systems. IEEE Wirel Commun Lett. 2025;14(5):1566–70. doi:10.1109/lwc.2025.3549228.
7. Le AT, Vu TH, Nguyen TN, Minh BV, Voznak M. On performance of cooperative satellite-AAV-secured reconfigurable intelligent surface systems with phase errors. IEEE Commun Lett. 2025;29(4):799–803. doi:10.1109/lcomm.2025.3543732.
8. Tran Tin P, van Nguyen MS, Trung Duy T, Vu Minh B, Kim BS, Rejfek L. Enhancing secrecy performance using fountain codes and NOMA under joint cooperative jamming technique and intelligent reflective surface. IEEE Access. 2024;12:117399–417. doi:10.1109/access.2024.3447531.
9. Sang NQ, Kim HY, Nguyen TN, Vu MB, Tran PT, Duy TT, et al. Performance of RIS-secured short-packet NOMA systems with discrete phase-shifter to protect digital content and copyright against untrusted user. IEEE Access. 2025;13:21580–93. doi:10.1109/access.2025.3535813.
10. Tang X, Liu R, Spasojevic P, Poor HV. Interference-assisted secret communication. In: 2008 IEEE Information Theory Workshop. Porto, Portugal; 2008. p. 164–8. doi:10.1109/itw.2008.4578643.
11. Zhang R, Song L, Han Z, Jiao B, Debbah M. Physical layer security for two way relay communications with friendly jammers. In: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010. Miami, FL, USA; 2010. p. 1–6.
12. Richter J, Scheunert C, Engelmann S, Jorswieck EA. Weak secrecy in the multiway untrusted relay channel with compute-and-forward. IEEE Trans Inf Forens Secur. 2015;10(6):1262–73. doi:10.1109/tifs.2015.2405903.
13. Zhang W, Chen J, Kuo Y, Zhou Y. Artificial-noise-aided optimal beamforming in layered physical layer security. IEEE Commun Lett. 2019;23(1):72–5. doi:10.1109/lcomm.2018.2881182.
14. Van Nguyen MS, Do DT, Tin PT, Vahid A. Secure performance analysis of user pairs in active reconfigurable intelligent surface-aided IoT systems. IEEE Syst J. 2025;19(2):370–81. doi:10.1109/jsyst.2025.3553818.
15. Nguyen SQ, Tran PT, Minh BV, Duy TT, Le AT, Rejfek L, et al. Statistical analysis of the sum of double random variables for security applications in RIS-assisted NOMA networks with a direct link. Electronics. 2025;14(2):390. doi:10.3390/electronics14020392.
16. Zheng Z, Yuan L, Fang F. Performance analysis of fountain coded non-orthogonal multiple access with finite blocklength. IEEE Wirel Commun Lett. 2021;10(8):1752–6. doi:10.1109/lwc.2021.3078811.
17. Yuan L, Kim KJ, Zhang J. Cross-Layer design for fountain coded non-orthogonal multiple access transmission. In: ICC 2019—2019 IEEE International Conference on Communications (ICC). Shanghai, China; 2019. p. 1–5.
18. Douglass NP, Langel J, Moore WJ, Ng L, Dudukovich RM, Mal-Sarkar S. Application of fountain code to high-rate delay tolerant networks. IEEE Access. 2023;11:100845–55. doi:10.1109/access.2023.3315659.
19. Yue J, Lin Z, Vucetic B. Distributed fountain codes with adaptive unequal error protection in wireless relay networks. IEEE Trans Wirel Commun. 2014;13(8):4220–31. doi:10.1109/twc.2014.2314632.
20. Tu LT, Nguyen TN, Duy TT, Tran PT, Voznak M, Aravanis AI. Broadcasting in cognitive radio networks: a fountain codes approach. IEEE Trans Veh Technol. 2022;71(10):11289–94. doi:10.1109/tvt.2022.3188969.

21. Ali A, Kwak KS, Tran NH, Han Z, Niyato D, Zeshan F, et al. RaptorQ-based efficient multimedia transmission over cooperative cellular cognitive radio networks. IEEE Trans Veh Technol. 2018;67(8):7275–89. doi:10.1109/tvt.2018.2832292.
22. Nguyen TN, Minh BV, Tran DH, Le TL, Le AT, Nguyen QS, et al. Security-reliability analysis of AF full-duplex relay networks using self-energy recycling and deep neural networks. Sensors. 2023;23(17):7618. doi:10.3390/s23177618.
23. Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Commun Surv Tutor. 2020;22(3):1646–85.
24. Hammouti HE, Ghogho M, Raza Zaidi SA. A machine learning approach to predicting coverage in random wireless networks. In: 2018 IEEE Globecom Workshops (GC Wkshps). Abu Dhabi, United Arab Emirates; 2018. p. 1–6. doi:10.1109/glocomw.2018.8644199.
25. Bao T, Zhu J, Yang HC, Hasna MO. Secrecy outage performance of ground-to-air communications with multiple aerial eavesdroppers and its deep learning evaluation. IEEE Wirel Commun Lett. 2020;9(9):1351–5. doi:10.1109/lwc.2020.2990337.
26. Tin PT, Van Nguyen MS, Duy TT, Pham VH, Kim BS. Combination of RIS and fountain codes in NOMA relay wireless networks for enhancing system performance and security. ICT Express. 2025;11(4):5604. doi:10.1016/j.icte.2025.05.012.
27. Nguyen MSV, Do DT, Afghah F, Islam SMR, Le AT. Exploiting secrecy performance of uplink NOMA in cellular networks. IEEE Access. 2021;9:95135–54. doi:10.1109/access.2021.3092830.
28. Lv L, Jiang H, Ding Z, Yang L, Chen J. Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay. IEEE Trans Commun. 2020;68(3):1698–715. doi:10.1109/tcomm.2019.2960345.
29. Li W, Du Q, Sun L, Ren P, Wang Y. Security enhanced via dynamic fountain code design for wireless delivery. In: 2016 IEEE Wireless Communications and Networking Conference. Doha, Qatar; 2016. p. 1–6.
30. Cheng Y, Li KH, Liu Y, Teh KC, Vincent Poor H. Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA. IEEE Trans Wirel Commun. 2021;20(6):3988–4000. doi:10.1109/twc.2021.3054841.
31. Kader MF, Shin SY. Coordinated direct and relay transmission using uplink NOMA. IEEE Wirel Commun Lett. 2018;7(3):400–3. doi:10.1109/lwc.2017.2779778.
32. Chen J, Yang L, Alouini MS. Physical layer security for cooperative NOMA systems. IEEE Trans Veh Technol. 2018;67(5):4645–9. doi:10.1109/tvt.2017.2789223.
33. Cao K, Ding H, Wang B, Lv L, Tian J, Wei Q, et al. Enhancing physical-layer security for IoT with nonorthogonal multiple access assisted semi-grant-free transmission. IEEE Internet Things J. 2022;9(24):24669–81. doi:10.1109/jiot.2022.3193189.
34. Zhang Q, Zhang L, Liang YC, Kam PY. Backscatter-NOMA: a symbiotic system of cellular and Internet-of-Things networks. IEEE Access. 2019;7:20000–13. doi:10.1109/access.2019.2897822.
35. Gradshteyn IS, Ryzhik IM. Table of integrals, series, and products. San Diego, CA, USA: Academic Press; 2014.
36. Do DT, Nguyen MSV, Jameel F, Jäntti R, Ansari IS. Performance evaluation of relay-aided CR-NOMA for beyond 5G communications. IEEE Access. 2020;8:134838–55. doi:10.1109/access.2020.3010842.
37. Song Y, Yang W, Xiang Z, Wang B, Cai Y. Secure transmission in mmWave NOMA networks with cognitive power allocation. IEEE Access. 2019;7:76104–19. doi:10.1109/access.2019.2920963.
38. Niu H, Iwai M, Sezaki K, Sun L, Du Q. Exploiting fountain codes for secure wireless delivery. IEEE Commun Lett. 2014;18(5):777–80. doi:10.1109/lcomm.2014.030914.140030.
39. Wang X, Chen W, Cao Z. A rateless coding based multi-relay cooperative transmission scheme for cognitive radio networks. In: GLOBECOM 2009—2009 IEEE Global Telecommunications Conference. Honolulu, HI, USA; 2009. p. 1–6.
40. Yadav K, Upadhyay PK, Moualeu JM, Osman AAF, Nardelli PHJ. Deep learning-based secrecy performance of UAV-IRS NOMA systems with friendly jamming. IEEE Open J Commun Soc. 2025;6:4533–48. doi:10.1109/ojcoms.2025.3570923.
41. Kamble A, Dalwadi H, Shukla MK, Pandey OJ, Singh VK. Medical sensor data security: a DNN framework for SOP prediction in two-way relay NOMA systems. IEEE Sens Lett. 2025;9(2):1–4. doi:10.1109/lsens.2025.3528978.

42. Shim K, Do TN, Nguyen TV, DBd Costa, An B. Enhancing PHY-security of FD-enabled NOMA systems using jamming and user selection: performance analysis and DNN evaluation. IEEE Internet Things J. 2021;8(24):17476–94. doi:10.1109/jiot.2021.3080425.
43. Do TN, Kaddoum G, Nguyen TL, da Costa DB, Haas ZJ. Aerial reconfigurable intelligent surface-aided wireless communication systems. In: 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). Helsinki, Finland; 2021. p. 525–30.