

Medical Sensor Data Security: A DNN Framework for SOP Prediction in Two-Way Relay NOMA Systems

Astitva Kamble¹, Harsh Dalwadi¹, Mahendra K. Shukla^{1*}, Om Jee Pandey^{2*}, and Vishal Krishna Singh³

¹Department of Information Technology, ABV-Indian Institute of Information Technology and Management, Gwalior, India

²Department of Electronics Engineering, Indian Institute of Technology (BHU) Varanasi, India

³School of Computer Science and Electronics Engineering, University of Essex, CO4 3SQ Colchester, U.K

*Senior Member, IEEE

Abstract—Securing medical sensor data is imperative due to the susceptibility of wireless transmissions to eavesdropping. In this letter, we focus on improving the security of two-way communication in medical networks by investigating Deep Neural Networks (DNN) for two-way relay non-orthogonal multiple access (NOMA) systems. Utilizing a decode-and-forward relay and considering both maximum ratio combining (MRC) and selection combining (SC) at the eavesdropper, we derive analytical expressions for the secrecy outage probability (SOP), leveraging the exact SOP expression from [1]. Due to the system's complexity, deriving a closed-form SOP is challenging. To address this, we introduce a DNN framework for real-time SOP prediction, which not only validates the theoretical model but also significantly reduces offline execution time and computational complexity.

Index Terms—Physical layer security, NOMA, two-way relay networks, secrecy outage probability, Deep Neural Networks (DNN).

I. INTRODUCTION

In modern healthcare networks, lightweight biosensors, placed inside or outside the human body, capture vital signs such as blood pressure and temperature [2]. This real-time data empowers medical professionals to make informed decisions, improving patient outcomes and reducing medical costs. However, safeguarding data integrity and ensuring secure, timely transmission are critical, as medical data must remain private. The challenge of maintaining both confidentiality and timeliness in wireless healthcare networks motivates our work. To address the risk of eavesdropping inherent in wireless transmissions, physical-layer security (PLS) exploits signal propagation and channel characteristics to enhance protection [3], [4].

In addition to ensuring security, improving data rates is critical, especially during patient emergencies. Non-orthogonal multiple access (NOMA) has gained significant attention due to its superior spectrum efficiency [5]. Recently, NOMA has been applied in cooperative relaying, enhancing coverage, throughput, and reliability [6]. Furthermore, [7] evaluates outage probability and ergodic sum rate in NOMA-based two-way relay (TWR) systems, which offer better spectral efficiency compared to one-way relaying.

Few studies have explored physical-layer security (PLS) in cooperative NOMA systems. In [8], the secrecy outage probability (SOP) was analyzed for cooperative NOMA using amplify-and-forward (AF) and decode-and-forward (DF) protocols. The secrecy performance of untrusted relay networks in cooperative NOMA was discussed in [9], while [10] investigated the security-reliability tradeoff, deriving SOP expressions. These works, however, focus on one-way relay NOMA. More recently, secrecy energy efficiency and ergodic secrecy rates for TWR-NOMA systems were evaluated in [1], [11], and [12].

Recent developments have shown deep learning (DL) as an effective tool to address various challenges in wireless communication networks, such as congestion control, resource allocation, and queue management [13]. In [14], a deep neural network (DNN) was utilized to enhance wireless-powered cognitive radio NOMA IoT relay networks. Similarly, [15] employed DNNs for classification and regression in relay selection for cognitive two-way relaying networks. Furthermore, [16] demonstrated the integration of DNNs in NOMA systems, improving channel encoding, decoding, and detection.

Building on previous work with DNNs in wireless communications, this paper investigates their application for SOP evaluation in two-way relay NOMA systems operating under Rayleigh fading channels, as detailed in [1]. The main contributions of this study are as follows:

- To analyze the SOP performance of TWR NOMA systems by leveraging DNN.
- To minimize computational complexity and reduce offline execution time in the SOP evaluation process by utilizing DNN techniques, while validating theoretical findings through simulation-based analysis.

II. SYSTEM MODEL

A comprehensive depiction of a secure medical sensor data transmission through NOMA-based cellular multiuser TWR systems is provided in Fig. 1, where two single-antenna users, U_1 and U_2 , engaged in bidirectional communication through a single-antenna, half-duplex decode-and-forward (DF) relay R . This exchange occurs under the threat of eavesdropping by a passive, single-antenna eavesdropper E^1 . The direct links between U_1 and U_2 are assumed to be absent and all the channels are reciprocal and subject to

¹The proposed model combines NOMA, TWR, and eavesdropper channels (MRC and SC) to address security and real-time SOP prediction challenges in medical sensor networks. This novel approach integrates traditional system elements with a DNN framework, offering an efficient and scalable solution for large-scale applications.

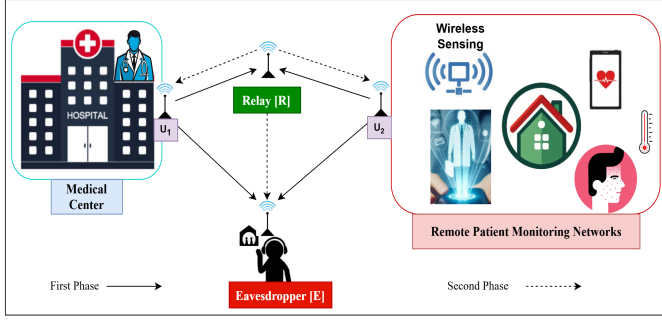


Fig. 1: Illustration of a secure medical sensor data transmission through cellular multiuser TWR systems.

independent quasi-static frequency-flat Rayleigh fading. The two-way communication is completed in two time phases, during which E intercepts the signals transmitted by U_1 , U_2 , and R . The channel coefficient h_1 for the link $U_1 - R$ is modeled as $CN(0, \Omega_1)$. Likewise, the channel coefficient h_2 for the link $R - U_2$ is $CN(0, \Omega_2)$. Furthermore, the channel coefficients for $U_1 \rightarrow E$, $U_2 \rightarrow E$, and $R \rightarrow E$ links are modeled as $h_{1,E} \sim CN(0, \Omega_{1,E})$, $h_{2,E} \sim CN(0, \Omega_{2,E})$, and $h_{R,E} \sim CN(0, \Omega_{R,E})$, respectively. The channel model and estimation technique employed adhere to the methodology outlined in [1]. Following the principle of successive interference cancellation (SIC) the relay decodes message of U_1 before recovering the message of U_2 ².

III. SECRECY PERFORMANCE ANALYSIS

The secrecy capacity for the DF-based NOMA system can be represented as follows

$$C_{\text{SEC},j}^{(\theta)} = [CM_j - CE_j^{(\theta)}]^+, \quad (1)$$

The secrecy capacity can be expressed based on the weakest terminal, where $j \in 1, 2$ and $\theta \in \{\text{MRC}, \text{SC}\}$. Ultimately, the overall secrecy rate is determined by the terminal with the lowest capacity, and it is formulated as:

$$C_{\text{SEC}}^{(\theta)} = \min\{C_{\text{SEC},1}^{(\theta)}, C_{\text{SEC},2}^{(\theta)}\}, \quad (2)$$

The expressions for $C_{\text{SEC},1}^{(\theta)}$ and $C_{\text{SEC},2}^{(\theta)}$, representing the secrecy capacities for each user under the combining scheme θ , can be obtained from (1) by substituting $j \in 1, 2$.

$$\text{SOP}^{(\theta)} = \Pr \left[C_{\text{SEC}}^{(\theta)} < \mathcal{R}_s \right]. \quad (3)$$

The expressions for $\text{SOP}^{(\text{MRC})}$ and $\text{SOP}^{(\text{SC})}$ can be found in detail in [1].

IV. ARCHITECTURE OF THE DEEP NEURAL NETWORK

This section introduces a DNN-based framework designed to efficiently estimate the SOP, prioritizing both computational simplicity and rapid execution. By bypassing the challenges and time-intensive

²Our work demonstrates the viability of a DNN framework for real-time SOP prediction in a two-way relay NOMA system. Additionally, exploring the unique channel characteristics of body area networks (BANs) could provide more detailed and context-specific insights. This approach requires a new perspective and will be thoroughly explored in our future work.

Table 1: Input Parameters for DNN Training and Testing

Parameters (Input)	Values
SNR _i (dB)	[0, 40]
\mathcal{R}_s	[0, 1]
Ω_1 and Ω_2	[5, 20]
$\Omega_{1,E} = 2$ and $\Omega_{2,E}$	[5, 20]
$a_{1,R}$	[0.1, 0.9]
$a_{R,1}$	[0.1, 0.9]

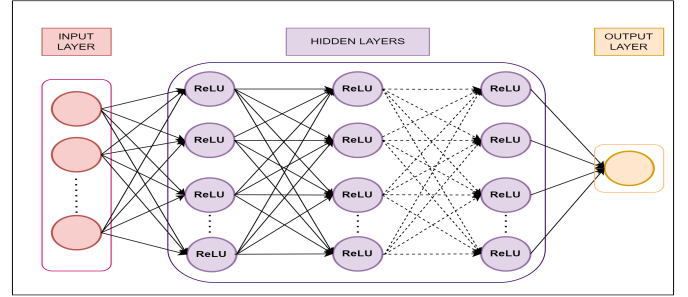


Fig. 2: Structure of the proposed DNN-based SOP evaluation model.

nature of conventional mathematical analysis and Monte Carlo simulations, the proposed approach leverages a neural network to model the intricate relationships between the SOP and the system parameters, as outlined in Table I.

A. Technique for Generating Datasets

In this study, we utilize a Deep Neural Network (DNN) to address the regression challenge of predicting the SOP under various system conditions. The DNN is trained using a dataset generated from the SOP expressions provided in equation (5). The SOP calculation is influenced by multiple factors, such as SNR in dB, target secrecy rate, variance, and power allocation factor. To create the dataset, each parameter is varied within the specified ranges detailed in Table I.

System parameters are uniformly sampled within their respective ranges, and various combinations of these values are used to compute SOP based on the derived expressions. This method ensures a diverse dataset, which improves the robustness of the DNN across a broad spectrum of potential input values.

The generated dataset, referred to as D , comprises a row vector for each sample d , represented as $[d] = [X[d], (P_{\text{out}})]$. Here, $X[d]$ denotes the feature vector encompassing all input variables, which include $[\text{SNRdB}, \mathcal{R}_s, \Omega_1, \Omega_2, \Omega_{1,E} = 2, \Omega_{2,E}, a_{1,R}, \text{ and } a_{R,1}]$, each within the specified ranges outlined in Table I. The feature vector $X[d]$ is employed to calculate the corresponding Secrecy Outage Probability (SOP) using the established expressions.

The overall dataset, denoted as D_s , consists of 25×10^3 samples. Of these, 80% are designated for training ($D_{s,\text{train}}$), while the remaining 20% are reserved for testing ($D_{s,\text{test}}$). Our analysis demonstrates that this sample size is adequate to achieve precise predictions. The comprehensive nature of the dataset significantly contributes to refining the DNN training process, thereby enhancing the accuracy of the predictions.

B. DNN Architecture for SOP Estimation

The architecture of the proposed DNN is designed with the following layers:

- **Input Layer:** This layer accepts five features corresponding to the parameters SNRdB, \mathcal{R}_s , Ω_1 , Ω_2 , $\Omega_{1,E} = 2$, $\Omega_{2,E}$, $a_{1,R}$, and $a_{R,1}$.

- **Hidden Layer:** The network comprises five fully connected hidden layers. Three of these layers each contain 64 neurons, while the other two layers have 32 neurons each. To model complex relationships and introduce non-linearity, the ReLU (Rectified Linear Unit) activation function is used throughout these layers.
- **Output Layer:** The output layer consists of a single neuron with a linear activation function, designed specifically to predict the log-transformed SOP.

The ReLU activation function is utilized to apply a threshold operation at the output of each neuron within the hidden layers. The ReLU function is mathematically expressed as follows:

$$\text{ReLU}(x) = \begin{cases} x, & \text{if } x \geq 0 \\ 0, & \text{if } x < 0 \end{cases} \quad (4)$$

In this context, x denotes the input parameter. The ReLU activation function is chosen due to its simplicity and computational efficiency, which are particularly advantageous in deep learning networks. Its ability to mitigate the vanishing gradient problem and accelerate convergence during training makes it highly effective.

As this is a regression task focused on predicting the SOP value, the network's output layer is configured with a single neuron devoid of an activation function. This design choice ensures the output is a continuous value, suitable for accurate SOP predictions.

The output F_n^m of the n th neuron in the m th layer is derived from the outputs of all neurons in the $(m-1)$ th layer as

$$F_n^m = \text{ReLU} \left(\sum_{j=1}^{U_{m-1}} W_{j,n}^m F_j^{m-1} + C_n^m \right), \quad (5)$$

where U_{m-1} denotes the total number of neurons in the $(m-1)$ th layer. The term $W_{j,n}^m$ represents the weight associated with the connection from neuron j in layer $(m-1)$ to neuron n in layer m , whereas C_n^m signifies the scalar bias in the m th layer.

C. Real-Time Prediction of SOP

Training a DNN involves the precise optimization of the network's weights and biases using the dataset described in Section II.A. To improve the model's ability to discern complex patterns, we apply a log transformation to the SOP values. This approach is particularly beneficial for regression tasks where the relationships between the input features and the target variable exhibit multiplicative characteristics rather than additive ones.

We utilize the Adam optimization algorithm, a robust gradient descent method, to fine-tune the network's weights and biases via backpropagation. The model's prediction accuracy is evaluated using the mean-squared error (MSE) as the loss function, guiding the iterative adjustment of weights and biases throughout the optimization process. In this context, Y_d and \bar{Y}_d represent the true and predicted outputs of the DNN for each training sample, respectively, while $D_{s,test}$ indicates the total number of test samples in the dataset.

$$\text{Loss}(Y_d, \bar{Y}_d) = \frac{1}{D_{s,test}} \sum_{d=1}^{D_{s,test}} (Y_d - \bar{Y}_d)^2. \quad (6)$$

The Adam optimization algorithm is used to update the network's weights and biases. As an advanced variant of gradient descent, Adam adjusts the learning rates for individual parameters according to their gradients. This adaptive approach accelerates convergence and improves the overall performance of the network.

Table 2: R^2 Performance Metrics for Linear Regression and DNN Models

Model	R^2 (Training)	R^2 (Test)
Linear Regression	0.864	0.859
DNN	0.988	0.952

Table 3: Comparative Analysis of MSE for Linear Regression and DNN Models

Model	MSE (Training)	MSE (Test)
Linear Regression	16.527	16.471
DNN	0.1752	0.1721

D. Model Performance Evaluation

We assessed the performance of our dataset, as described in Section IV-A, by employing both a linear regression model and a DNN model. In the context of regression, we evaluated the models using the R^2 score and Mean Squared Error (MSE) metrics. The R^2 coefficient of determination indicates the degree to which the regression predictions correspond to the actual data points, with a value of 1 representing a perfect fit. Conversely, the MSE measures the average of the squared differences between predicted and actual values, with lower values signifying superior model performance. Detailed R^2 scores and MSE values for each model are provided in Table 2 and Table 3, respectively. As illustrated in Table II, the linear regression model yielded an R^2 score of 0.864 on the training dataset and 0.859 on the test dataset, accompanied by MSE values of 16.527 and 16.471, respectively. In comparison, the DNN model exhibited markedly superior performance, achieving R^2 scores of 0.968 and 0.952 for the training and test sets, respectively, and significantly lower MSE values of 0.1752 and 0.1721.

Table 4: Comparison of Average Runtime

Analytical	MCS	DNN
28.52s	52.86s	0.0472s

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we provide both numerical and simulation results to substantiate our theoretical analysis of TWR NOMA systems. To validate our analytical predictions, we utilized MATLAB version R2021a. The DL model employed in this study is comprised of five hidden layers: three layers, each with 64 neurons, and two additional layers, each with 32 neurons. This model underwent end-to-end training over 20 epochs. Additionally, we conducted Monte Carlo simulations across 10^4 independent trials. For consistency, we assumed that the transmit SNR is equal for both ρ_U and ρ_R .

Figure 3 and 4 illustrates the SOP performance as a function of the SNR for various values of Ω_1 and \mathcal{R}_s (in bps/Hz) for the Maximum Ratio Combining (MRC) and Selection Combining (SC) at the eavesdropper (E), respectively. The parameters used for the analysis include $a_{1,R} = 0.9$, $a_{R,1} = 0.6$, $\Omega_2 = 5$, $\Omega_{1,E} = 2$, and $\Omega_{2,E} = 1$. The figure demonstrates a strong alignment between the analytical SOP results and the simulation outcomes for both MRC and SC schemes.

The plot shows that improved channel quality of the main link ($U_1 \rightarrow R$) leads to a decrease in SOP. For instance, at $\mathcal{R}_s = 1$

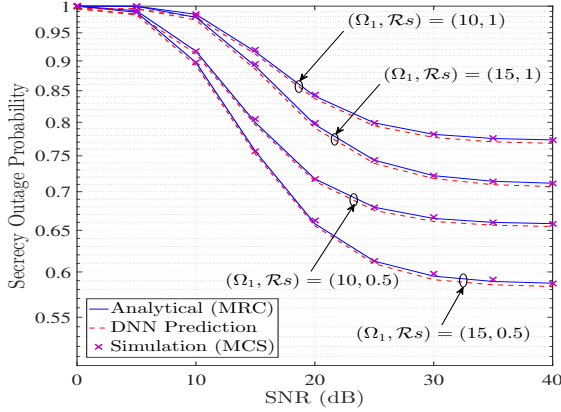


Fig. 3: Comparative analysis of SOP performance using DNN versus Monte Carlo methods under MRC.

bps/Hz, increasing Ω_1 from 10 to 15 lowers SOP. A similar trend is observed for the main link $U_2 \rightarrow R$. The SOP also deteriorates with a higher target secrecy rate \mathcal{R}_s , due to increased power requirements. Additionally, SOP tends to saturate at high SNR levels because of the eavesdropper's presence. For the same settings, the MRC scheme at the eavesdropper performs worse than the SC scheme, as MRC allows the eavesdropper to capture more information, albeit with greater hardware complexity.

Moreover, the DNN predictions align closely with simulation and analytical results, as shown in Fig. 3 and Fig. 4. Compared to the computationally intensive and time-consuming Monte Carlo simulations detailed in Table IV, the DNN offers a faster and more efficient alternative. By learning data patterns during training, the DNN delivers rapid, accurate predictions with less computational overhead, making it especially suitable for real-time and large-scale applications. This efficiency is particularly valuable in real-time medical applications in securing medical sensor data, where timely and secure data processing is crucial for protecting patient information and ensuring prompt medical responses.

VI. CONCLUSIONS

In this paper, we have demonstrated a significant advancement in securing medical sensor data by enhancing two-way communication security using DNN within NOMA systems. By employing a decode-and-forward relay and analyzing MRC and SC at the eavesdropper, we derived analytical expressions for the SOP based on [1]. Given the complexity of closed-form SOP derivation, our proposed DNN framework effectively predicts SOP in real-time, validating the theoretical model and markedly reducing both computational complexity and execution time. This approach represents a substantial improvement in safeguarding medical sensor data and optimizing communication security in healthcare networks.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the financial support provided by the DST-SERB and the Anusandhan National Research Foundation (ANRF) under the Startup Research Grant (SRG) project (SRG/2023/001422) which has been instrumental in facilitating the research and publication of this manuscript.

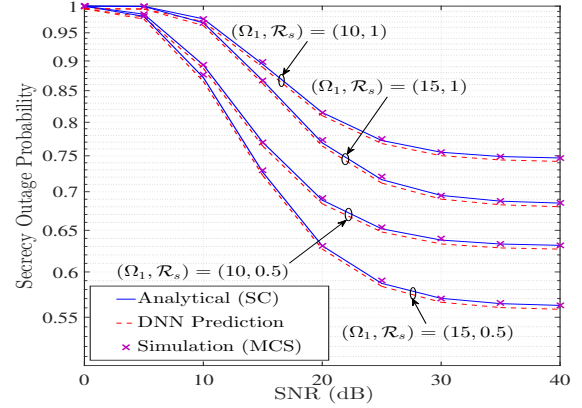


Fig. 4: Comparison of SOP performance using DNN and Monte Carlo methods under SC.

REFERENCES

- [1] M. K. Shukla, H. H. Nguyen and O. J. Pandey, "Secrecy Performance Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems," in *IEEE Access*, vol. 8, pp. 39502-39512, 2020.
- [2] Y. Qiu, H. Zhang, and K. Long, "Computation offloading and wireless resource management for healthcare monitoring in fog-computing-based Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15875-15883, Nov. 2021.
- [3] S. Yadav, "Secrecy Performance of Cognitive Radio Sensor Networks Over Fading Channels," *IEEE Sensors Letters*, vol. 4, no. 9, pp. 1-4, Sept. 2020.
- [4] J. Zhou, W. Hou, Y. Mao and C. Tellambura, "Securing Medical Sensor Data: A Novel Uplink Scheme With Rate Splitting and Active Intelligent Reflecting Surface," in *IEEE Communications Letters*, vol. 28, no. 3, pp. 493-497, March 2024.
- [5] Z. Ding et al., "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185-191, Feb. 2017.
- [6] M. F. Kader, M. B. Shahab, and S. Y. Shin, "Exploiting non-orthogonal multiple access in cooperative relay sharing," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1159-1162, May 2017.
- [7] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Y. Chen, "Modeling and analysis of two-way relay non-orthogonal multiple access systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 3784-3796, Sept. 2018.
- [8] J. Chen, L. Yang, and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645-4649, May 2018.
- [9] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 210-222, 2020.
- [10] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, and R. Q. Hu, "Security-reliability tradeoff analysis for cooperative NOMA in cognitive radio networks," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 83-96, Jan. 2019.
- [11] B. Zheng et al., "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426-1440, Jul. 2018.
- [12] M. K. Shukla and H. H. Nguyen, "Ergodic Secrecy Sum Rate Analysis of a Two-Way Relay NOMA System," in *IEEE Systems Journal*, vol. 15, no. 2, pp. 2222-2225, June 2021.
- [13] H. Huang et al., "Deep learning for physical-layer 5G wireless techniques: Opportunities, challenges and solutions," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 214-222, Feb. 2020.
- [14] T.-H. Vu, T.-V. Nguyen, and S. Kim, "Wireless powered cognitive NOMA-based IoT relay networks: Performance analysis and deep learning evaluation," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3913-3929, Mar. 2022.
- [15] Z. Zhang, Y. Lu, Y. Huang, and P. Zhang, "Neural network-based relay selection in two-way SWIPT-enabled cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6264-6274, Jun. 2020.
- [16] G. Gui, H. Huang, Y. Song, and H. Sari, "Deep learning for an effective nonorthogonal multiple access scheme," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8440-8450, Sep. 2018.