Hindawi
Journal of Electrical and Computer Engineering
Volume 2023, Article ID 9390660, 11 pages
https://doi.org/10.1155/2023/9390660

Research Article

Secured Wireless Network Based on a Novel Dual Integrated Neural Network Architecture

H. V. Ramachandra,[1] **Pundalik Chavan**,[1] **S. Supreeth**,[1] **H. C. Ramaprasad**,[1] **K. Chatrapathy**,[2] **G. Balaraju**,[2] **S. Rohith**,[3] **and H. S. Mohan**[4]

[1]*School of Computer Science and Engineering, REVA University, Bengaluru, India*
[2]*School of Computing and Information Technology, REVA University, Bengaluru, India*
[3]*Department of ECE, Nagarjuna College of Engineering and Technology, Bengaluru, India*
[4]*New Horizon College of Engineering, Bangalore, India*

Correspondence should be addressed to S. Supreeth; supreeth1588@gmail.com

Received 11 May 2023; Revised 26 July 2023; Accepted 5 September 2023; Published 28 September 2023

Academic Editor: Serena Nicolazzo

The development of the fifth generation (5G) and sixth generation (6G) wireless networks has gained wide spread importance in all aspects of life through the network due to their significantly higher speeds, extraordinarily low latency, and ubiquitous availability. Owing to the importance of their users, components, and services to our everyday lives, the network must secure all of these. With such a wide range of devices and service types being present in the 5G ecosystem, security issues are now much more prevalent. Security solutions, are not implemented, must already be envisioned in order to deal with a range of attacks on numerous services, cutting-edge technology, and more user information available over the network. This research proposes the dual integrated neural network (DINN) for secure data transmission in wireless networks. DINN comprises two neural networks based on sparse and dense dimensions. DINN is designed for any presence of deep learning-based attack in a physical security layer. DINN is evaluated considering the various machine learning attack such as basic_iterative_method attack, momentum_iterative_method attack, post_gradient_descent attack, and C&W attack; comparison is carried out on existing and DINN, considering attack success rate and MSE. Performance analysis suggests that DINN holds a higher level of security against the above attacks.

1. Introduction

The introduction of the first generation of cellular networks in the 1980s marked the beginning of the growth of wireless communication technology (1G). The development of 2G, 3G, and 4G cellular networks has led to substantial improvements in the telecommunications and networking sectors. In 2020, initially the fifth-generation (5G) wireless technology came into light, whilst software development goes on until 2025. The cloudification of networks built utilizing a microservices architecture is the most crucial aspect of 5G. As a result, management functions may be automatically learned and applied as needed. This permits the abstraction of physical resources to logical and virtual contexts.

The development of next-generation networks, also known as 5G and beyond, as well as the growing demand for new communication technologies have both been widely watched in recent years by researchers, corporations, and the general public. ITU predictions [1] predict that NextG-based mobile data traffic would eventually reach tens of thousands of exabytes annually. Next-generation networks, which aim to connect billions of devices, systems, and applications, will enable future applications including delay-sensitive Internet services like digital twins, virtual reality, the metaverse, industry 4.0, autonomous cars, online education, and eHealth services. These applications are made possible by NextGen networks' [2] improved communication, processing, and artificial intelligence (AI) capabilities. AI is one of the 34

significant NextG network technical advancements that must be addressed to overcome upcoming 6G networks consist of issues with security and privacy [3]. The recently proposed innovative 6G architectural framework is prone to a number of security vulnerabilities. To solve security and privacy issues, 6G intelligent networking concepts make use of existing technologies such as blockchain, VLC, TeraHertz (THz), and quantum computing. Physical layer security (PLS), network information security, application security, and deep learning-related security should all be considered while analyzing 6G security challenges. There are several methods [4] that may be used to address the security and privacy concerns in 6G networks. The unusual 6G design framework may provide several security issues, as was previously mentioned. There is a lot of interest in incorporating straight-forward technology into wireless intelligent networking paradigms, including as blockchain, VLC, TeraHertz (THz), and quantum computing, to solve security and privacy problems [5]. Deep learning security, network information security, application security, and physical layer security are all required for 6G security (PLS) [6]. The motivation's objective [7] is to further investigate the past security system faults in preparation for the upcoming security system. It is simple to learn about the many security challenges that mobile networks confront since these attacks commonly undermine the system or protocol that the authors are unaware of throughout the design process. These shortcomings [8] have been looked at in prior attacks on previous generations. The core network must often undergo updates and various sorts of maintenance in order to address security issues. Moreover, the buyers oppose this kind of replacement technique resulting in higher costs. In the initial stage, these issues are not fixed in [9], and hence they become the primary target for upgrading the system in the core network and there are a lot of ways to fix it. Mostly, the vendors here oppose the replacement at a great cost. These issues are not fixed; henceforth, the primary target upgrades the wireless network systems, which forms the basis for future research.

Future security systems [10] should often be upgraded in response to security concerns to avoid the exploitation of old vulnerabilities. These attacks typically expose vulnerabilities in protocols or systems that their developers have not addressed. Learning from such attacks may facilitate understanding of how successive mobile network security developments are leveraged to address known vulnerabilities highlighted by attacks in earlier generations. Basic network operations must frequently be modified, for instance, to fix flaws in the authentication protocol that have been uncovered by security intrusions. Yet, because of the huge cost, the vast majority of suppliers are opposed to such a replacement. As a result, these disclosed vulnerabilities suggest potential targets for wireless networks or act as a foundation point for additional research. Hence, considering the security vulnerabilities based on the deep learning phenomena, this research aims to develop a secure framework. Furthermore, the research contribution is given as follows:

(i) This research work designs and develop DINN (dual integrated neural network) for a secured wireless network against various machine learning-based attacks.

(ii) DINN comprises two distinctive neural networks, a first neural network is densely connected in nature and the second neural network is based on sparse connection. Furthermore, these both are interconnected to predict the attack.

(iii) DINN is evaluated on attack success rate and mean square error considering the major deep learning attack such as basic_iterative_attack, momentum_iterative_attack, post_gradient_descent attack, and C&W attack.

(iv) Comparison is carried out with the existing network to prove the DINN efficiency against the different attacks mentioned above.

This research is organized as follows. Section 1 starts with the background of the wireless network along with the security and its significance towards the data transmission. Furthermore, obstacles and criteria for designing the secured network concerning the physical layer are discussed. Section 2 presents a discussion of various existing secured mechanisms along with its shortcoming. Section 3 presents the security framework of dual integrated neural network architecture along with mathematical modeling and algorithm. Furthermore, DINN is evaluated in Section 4 considering attack success rate and mean square error. In Section 5, conclusions are drawn.

2. Related Work

In cellular networks, security and privacy have been a major concern due to the variety of uses for data transmission such as video, audio, or text. A recent survey has mainly focused on 5G security and major research has been on the physical layer security with active eves discussed in [11–14], pilot spoofing attack was carried out for MMS (multigrain multicasting system) with particular downlink strategy. In [15], imperfect radio frequency impact has been studied on a particular adjustable secrecy rate. Furthermore, the authors in [16] develop secure transmission considering the spatially correlated channels; the authors in [17] focused on analyzing through utilizing the artificial noise inclusion in transmission and trying to achieve a particular secrecy rate. In general, Aps induces the artificial noise sequence in given downlink signals for preventing the eves from any kind of wiretapping without any MTs [18] having an aware sequence. Moreover, a sequence transmission tends to decrease the achievable rate; however, it provides security due to the use of artificial noise sequence though it has a huge negative impact on less rate. Furthermore, the authors in [19] developed a novel algorithm for secrecy rate maximization, whereas in [20] power transfer along with wireless transmission is assumed for eves harvesting the energy and violating the confidential message at the same time. Furthermore, the author also claimed it for being immune towards active eavesdropping. Moreover, a recent study has been divided into three distinctive

categories on the wireless network thus researcher believed that increasing the signal strength among the users through observer channels is very much important for the prevention of eavesdropping and various attacks. In [21], the transmitter shares the information signals with the receiver for learning in advance about the communication channel and should have major secrecy about CSI (channel state information). Furthermore, unpredictable modulation is another popular attack that makes it more difficult for an observer for predicting the next signal. Various methodologies like in [22, 23] used similar mechanisms with an improvised version of it. For instance in [24], offers a method in which the sender employs several random frequency shifts in addition to the standard pilot sequence or frequency hopping to prevent eavesdropping. A novel covert communication technique called friendly jamming deceives listeners on the transmission channel by inserting fake interference signals into the null space of a real user channel. In [22, 23], the physical key generation of communication-specific secret keys (CSI) is made possible by channel state information, which makes advantage of the entropy of unpredictability in transmit-receive channels [24]. To authenticate the broadcast against unreliable partners, the authors of [25, 26] suggest a physical key exchange between the broadcasted and authorized users. Nevertheless, including the encryption and decryption inside the precoding may decrease the efficacy of the transmission and raise the possibility of internal assaults (i.e., the eavesdropper is one of the legitimate users). Although the majority of systems still struggle with excessive energy consumption, using AI/ML technologies (such reinforcement learning [27]) to complement CSI knowledge and apply pertinent defense methods, such as channel hopping, is an emerging prospect. It should be stressed that raising the level of secrecy might greatly limit jamming attacks. It is difficult for an attacker to cause congestion in a communication channel without precise knowledge about communication signals between the transmitter and the authorized receiver given the extremely high cost of overriding all frequencies in modern broadband wireless channels [28, 29]. Frequency-specific assaults have no impact on the functionality of the receiver or inclusive transmitter due to the frequent frequency changes (frequency hopping). The surveys like [30–32] offer further information on jamming attacks and viable defense.

3. Proposed Methodology

A dual neural network comprises two different neural networks, i.e., first neural network is designed based on the dense and the second neural network is on the sparse dimension.

Figure 1 shows the proposed workflow of dual integrated neural network architecture which comprises two neural networks. In the above workflow, following components are used:

(i) Input: the input data are taken.

(ii) First Neural Network: the first neural network is responsible for extracting features from the input data. This is carried out using a series of convolution and pooling layers. Convolution layers perform mathematical operations on the input data to extract features. Pooling layers reduce the size of the feature maps while preserving the most important features.

(iii) Loss Function: the loss function is used to measure the accuracy of the model's predictions. The loss function is minimized during the training process. There are many different loss functions that can be used, such as the cross-entropy loss function and the mean squared error loss function.

(iv) Second Neural Network: the second neural network takes the features extracted by the first neural network and classifies the data. This is carried out using a SoftMax layer. The SoftMax layer outputs a probability distribution for each class. The class with the highest probability is the predicted class.

(v) Prediction: the model outputs a prediction for the input data.

(vi) Deployment: the model is deployed at a base station. This allows the model to be used to make predictions.

3.1. Problem Statement. The research aims to address the pressing security concerns in next-generation wireless networks by proposing a novel security framework called dual integrated neural network (DINN). The goal is to secure data transmission while maintaining high efficiency in communication for applications like digital twins, virtual reality, metaverse, industry 4.0, driverless cars, online education, and eHealth services. DINN combines two neural networks, densely connected and sparse connection-based, to effectively predict and counter machine learning-based attacks, such as basic_iterative_attack and C&W_attack. The research focuses on evaluating DINN's performance against various attacks, comparing it with existing security mechanisms, and exploring the potential of AI/ML technologies like reinforcement learning for dynamic threat adaptation. Ultimately, this study seeks to contribute to the development of robust and efficient security solutions to meet the challenges of 6G networks and beyond.

3.2. System Modeling and Preliminaries. As depicted in Figure 1 which is a single-cell wireless network, where the base_station N onverses with an authenticated user M, amidst the occurrence of the attacker Z. In this instance, the attacker and the authorized user each send a single signal to the base_station. The base_station here is equipped with Z signals, in midway where the authenticated user and the attacker consist of a same single signal. Appropriately, we can define that $\mu = \{M, Z\}$. The transmissions here amid the authenticated user and the base_station are in synchronization with each other. The base_station here is responsible to determine the uplink transmission in the presence of the training symbol. The training symbol set of the index is denoted as W_w in the frame w. Let È the list of the training signals for uplink training. Similarly, the assumption of È in a N shift key mechanism with N training signals is shown as follows:

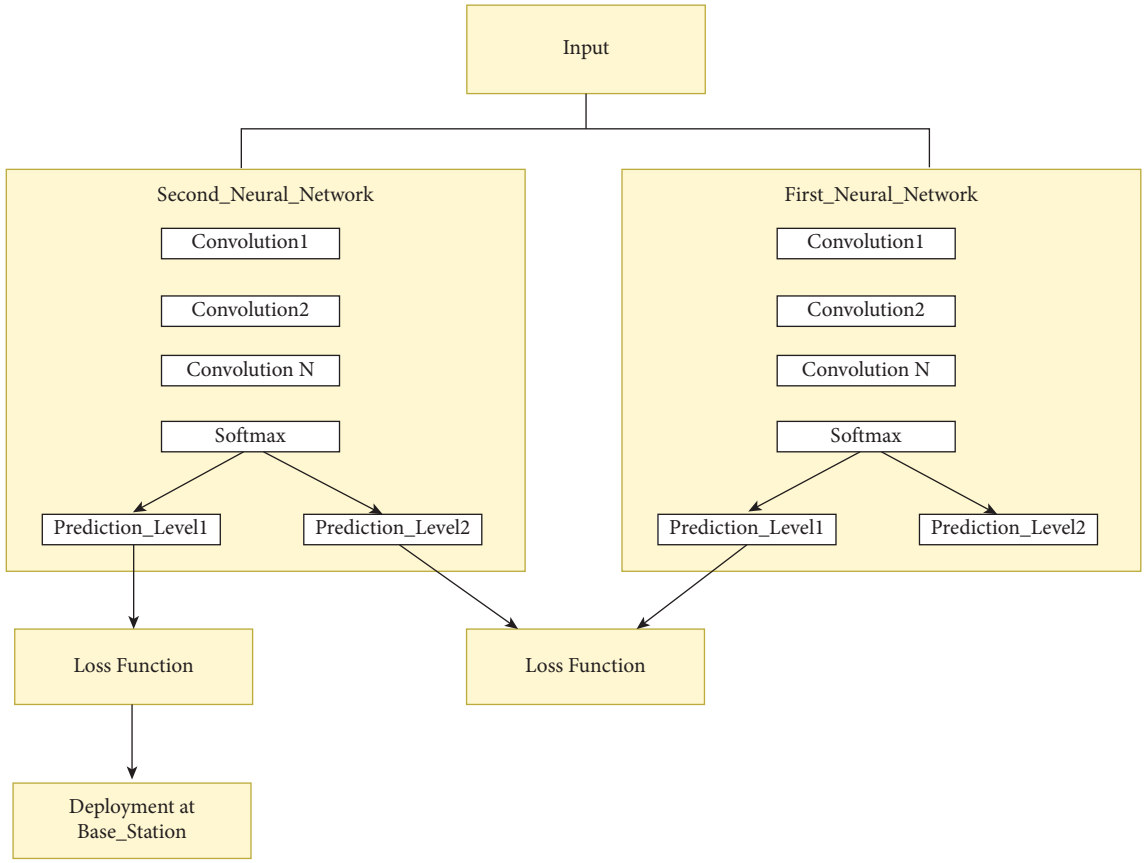

Figure 1: Proposed workflow.

$$\dot{\mathrm{E}} = \left\{ \mathrm{l}^{\mathrm{j2k/N}} : \mathrm{k} \in \mathrm{p}, 0 \le \mathrm{k} \le \mathrm{N} - 1 \right\}. \tag{1}$$

Here, the training is done by the $g \in W_w$, upon assumption of the authenticated user to transmit a random signal $e_{M,w,k} \in W$, which is not probable by an attacker. The standard applications, the collection of training signals set W used by the authenticated users that deals with technical stipulations. The assumption made here such that attacker has previous knowledge of W. This is necessary for training signal transferred to the authenticated user by a training measure. One specific approach that this attacker can apply transmission of a signal selected from W, depicted as $e_{M,w,k} \in W$ that contaminate the uplink training transmission, to reduce the accuracy of channel state information derived from the base_station.

$$e_{M,w,k} = e_{M,w,k} e^{*}_{M,w,k} e_{M,w,k} = e_{w,k} e_{M,w,k}. \tag{2}$$

Here, $\mathbf{e_{w,k}} = \mathbf{e_{M,w,k}} \mathbf{e^{*}_{M,w,k}} \mathbf{e_{M,w,k}} \in \mathbf{W}$ and $\mathbf{e_{M,w,k}} \mathbf{e^{*}_{M,w,k}} \in \mathbf{W}$

3.3. Proposed DINN Algorithm for Secured Transmission. The main aim of the proposed model is to present the secured network termed as p, in coordination with the adversarial machine learning defense. The model was developed in defense of the ML platform to augment the strength of the classification model. In the first phase, the neural network α along with a temperature (T) through a parameter to soften the probability of outputs fed to the deep learning model. This is carried out in a specific way as shown follows:

$$\mathrm{P}_{\mathrm{sm}}(\Upsilon, \mathrm{F}) = \frac{h^{\Upsilon/F}}{\sum_{x=1}^{n} h^{\Upsilon_{(x)}/F}}. \tag{3}$$

Here, n is the number of labels and Υ's the output of the last layer fed to the model. Here, $\mathrm{WM}_n . f_{n-1} + e_n$, where WM_n is the weight matrix and f_{n-1} is to activate the last layer. In the second step, the neural network [33, 34] is trained using the output from the SoftMax probability function α through a low-temperature parameter. The main objective of this function is as follows:

$$\begin{aligned} \Gamma_{\alpha}(F) &= \frac{1}{N} \sum_{x=1}^{N} \sum_{y=1}^{n} \mathrm{s_{xy}} . \log \mathrm{P_{sm}} \left(\Upsilon_{\mathrm{xy}}, F \right) \\ &= \frac{1}{N} \sum_{x=1}^{N} \sum_{y=1}^{n} \mathrm{s_{xy}} . \log \frac{h^{\Upsilon_{\mathrm{xy}}/F}}{\sum_{x=1}^{n} h^{\Upsilon_{\mathrm{xy}}/F}}. \end{aligned} \tag{4}$$

Here, N denotes how many training samples there are, s_{xy} is employed in training and Υ_{xy} is the log function. The neural network β and neural network's objective function is given by the following equation:

$$\Gamma_{\alpha}(F) = -\frac{1}{N} \sum_{x=1}^{N} \sum_{y=1}^{n} \mathrm{s_{xy}} . \log \frac{h^{\Upsilon_{\mathrm{xy}}/F}}{\sum_{x=1}^{n} h^{\Upsilon_{\mathrm{xy}}/F}}. \tag{5}$$

The p is a method wherein the model is trained that is developed for a defense that in turn augments the strength of the models, which in turn is trained by the target generated by the α neural network model. To minimize the objective of the function the model is trained on this basis. The α neural network model is a typical extended deep neural network model whereas the neural network β is a small and narrow neural network. The p consists of the following two phases:

(1) To train the neural network α

(2) p from neural network α to neural network β

The p procedure is carried out through the neural network α capability, the neural network α's activations, or the midway representation of the neural network α. Computer vision tasks involved deep learning mechanisms for many different processes such as image classification, object and action detection, segmentation of the scene and image generation. Deep neural networks need a large amount of training data that is not available for new phases or mechanisms. Various techniques are suggested below to address the issue that can train a smaller neural network β to imitate the prediction of a wide range of appropriate neural network β. p has been widely applied in the domain of smart systems like that as knowledge-based and rule-based systems that reduce the model's size and enhance system performance by raising the standard of the systems knowledge. In the neural network α and neural network β, the differences are distinguished in the form of regularization which is a necessary measure for over fitting. The complete step by step approach has been discussed in the Algorithm 1.

3.4. Detection through DINN. The detection region used is based on a scalar matrix $G_{h,x}$ towards the base_station, enhancing the system performance by raising the standard of the systems. Here, $G_{h,x}$ is the sum obtained by the N – phase shift keying scaled by $f_{Dx,0,w}$ with Gaussian noise along the mean 0 and variance denoted by $\sigma^2_{Dx,0,w}$. The base_station previous to the training phase, has not had access to crucial information on the small-scale fading coefficient. However, this states that the $f_{Dx,0,w}$ and $\sigma^2_{Dx,0,w}$ before analyzing the decision of the jamming signals. The authenticated user and the attacker do not get along ahead of time, for justification which focuses that the base_station precisely determines the large-scale coefficient α_α and $\alpha_{\alpha,O}$, given the modulation for N – phase shift keying is large enough for Z signals, the detection region determines the circle of radius for $\sigma^2_{Dx,0}$ amongst the centers that are scaled for N – phase shift keying with the relevant factor as $\sqrt{W} f_{Dx,0,m}$. The effects here are minimized for detecting accuracy, and we also state the Z, where $Z \geq 2$, the training symbols utilized for attacker detection. The detection region is based on N – phase shift keying for Z training symbols. The step by step approach of detecting the attacker has been discussed in Table 1.

The main focus here is levied on the relevant attacker detection decision, the advantages, the cost of overhead, and related processing complexity. The pairs of training symbols utilize temporal diversity.

3.5. Analysis of Probability Detection. The probability of the proposed method with Z signals at the base_station expands broadly in order to obtain the characteristics of the effect placed on the channel model. The equation obtained is shown as follows:

$$G_{h,x} = e_M + \frac{n_{w,m}}{D_{w,m}}. \tag{6}$$

The proposed detection region is proportional with $V_{Dx,0,m} = \sigma^2_{Dx,0,w}/|f_{Dx,0,m}|^2$. The probability detection mechanism is equalized to zero where $V_{Dx,y,m,w} \leq V_{Dx,0,m,w}$ this enhances the ratio of $V_{Dx,y,m,w}/V_{Dx,0,m,w}$ is large and wide. We can conclude that $V_{Dx,y,m,w}/V_{Dx,0,m,w} = V_{Dx,y,m,m}/V_{Dx,0,m,m}$ for all w. The efficiency of the proposed model allows flexible signal jamming detection.

4. Performance Evaluation

Security is considered one of the major concerns in network functions especially with the development of AI domains such as deep learning. This research work designs an architecture for providing security against different types of attacks at the physical layer. This section of the research evaluates the proposed model DINN; evaluation is carried out considering the system configuration of 16 GB RAM, 16 GB NVIDIA CUDA enabled graphics along with deep learning libraries.

4.1. Evaluation Parameter and Model Training. DINN is evaluated considering the ASR (attack success rate) and MSE (mean squared error); ASR is defined as the test sample to mispredict the attack. A higher attack success rate indicates the model is less secure. Figure 2 shows the training of nonsecured wireless network, Figure 3 shows the MSE of nonsecure network. Figures 4–7 are the extensions of Figure 3 which elaborates the entire concepts of proposed training loss and MSE of first and second training datasets.

4.2. Attack Evaluation

4.2.1. Basic_Iterative_Mechanism_Attack. This is considered as one of the basic attack which tends to compute the loss function with respect to given input. Figure 8 shows the comparison of existing unsecured network and proposed DINN model over various power attack (0.5, 1, 2, and 3) considering the attack success rate. Through Figure 8, it is observed that rise in attack power increases the attack success rate.

Figure 9 shows the MSE comparison of existing wireless network and DINN WN (wireless network); higher MSE (mean square error) indicates the less secured network.

Input: neural network α, neural network β, loss function r, learning parameter Γ Total number of epochs È
Output: neural network β
(1) Start
(2) Neural network β = weight-Initialization
(3) for $h = 1$ to H do
(4) Rearrangement of the *Dataset*
(5) for $x = 1$ to | *Dataset* | do
(6) Extract the x^{th} sample (a_x, b_x) from *Dataset*
(7) Forward propagation of the sample a_x by the neural network α to determine the output probabilities b_x evaluate the loss through the output probability b_x Backpropagate the loss through the neural network β.
(8) Weight-updating of the neural network β by the learning parameter Γ.
(9) end for
(10) end for
(11) return neural network β

Algorithm 1: DINN.

Table 1: Detection approach.

Step 1	The base_station here chooses an appropriate subset of Z radio signals through one or more radio frames that are active at the same time. The base_station, respectively, consists of the number of Z training symbols selected from a set. The maximum pairs for training symbols are $Z(Z-1)/2$
Step 2	Here, each pair necessary for the training signals, the training signal h for the radio frame w in frame Z and training symbol x in radio frame m, i.e., $h \in W_w$ and $x \in W_m$, the base_station here is responsible for performing the following steps: (1) Evaluation of the scalar metric $G_{h,x}$ (2) Evaluate $V_z = \lvert G_{h,x} - \sqrt{W}\, f_{Dx,0,m}^{e^{xz2\Pi/N}} \rvert$ by considering each $\in 0, 1, \cdots, N-1 \in 0,1, \cdot\ \cdot\ \cdot, N-1$, the V_z is the distance from the scalar-valued to receive signal to the Z^{th} scale N-phase shift keying (3) The minimum distance that is defined is given by $V_{\min} = \min_{0 \le z \le (N-1)V_z}$ (4) If $V_{\min} < \sigma^2_{Dx,0}$, the base_station here trains the symbols that are not being contaminated, else it states that the signals are contaminated, and there an attacker exists
Step 3	The major consideration for the detection of results for pairings, the base_station evaluates the presence of jamming signals
Step 4	The base_station decides whether the attacker is present on the entire range of the frames which are widely focused on the attacker detection system parallel with the formed pairs

Through Figure 9, it is observed that as the attack power increases, MSE increases in existing wireless network, whereas MSE for proposed DINN remains stable.

4.2.2. Momentum_Iterative_Method_Attack. Momentum_iterative_method_attack is inherited from the basic_iterative_mechanism which further introduces the momentum term and late integrate it to compute the loss functions. Figure 10 shows the comparison of existing network and proposed DINN WN over the various power attacks as it shows the increase in power attack increases the attack success rate whereas proposed DINN remains stable over different power attack.

4.2.3. Projected_Gradient_Attack. Projected_gradient_attack is considered as one of the hazardous attack in the network which is based on the gradient; after making an effort to determine the loss function with regard to the input, the attacker creates a duplicate by integrating the gradient sign. Figure 11 contrasts attack success rates while accounting for the anticipated gradient attack.

Figure 12 shows the MSE comparison over the post gradient descent attack over various attack power.

4.2.4. C&W Attack. C&W attack is another important attack based on the zero-sum game approach where total value is fixed and winner of the games gets the total value and loser gets

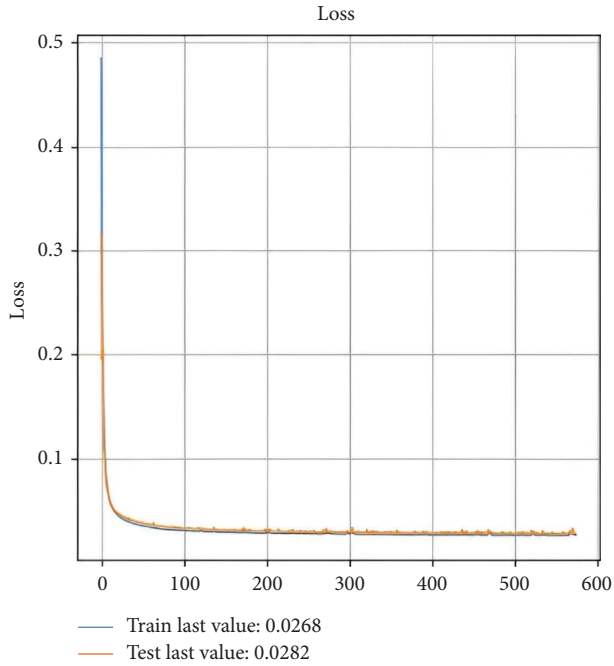

Figure 2: Training of nonsecured model on loss.

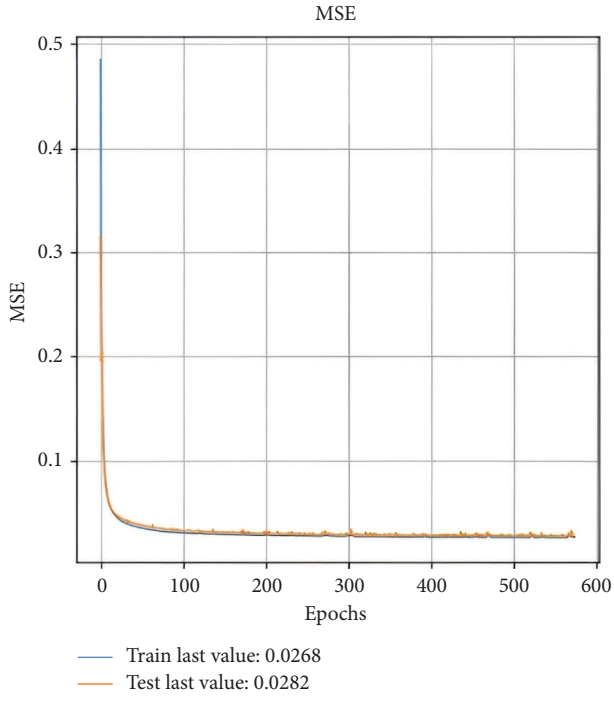

Figure 3: Training of nonsecured model on MSE.

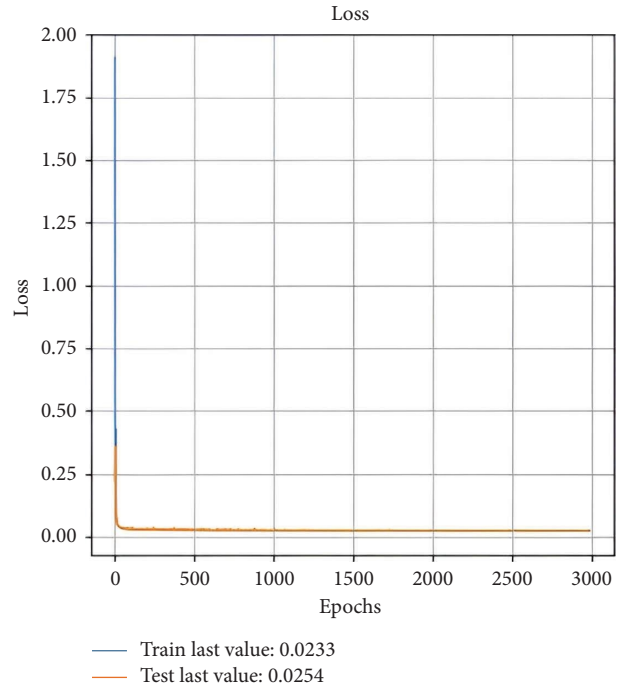

Figure 4: Proposed first training graph of Loss.

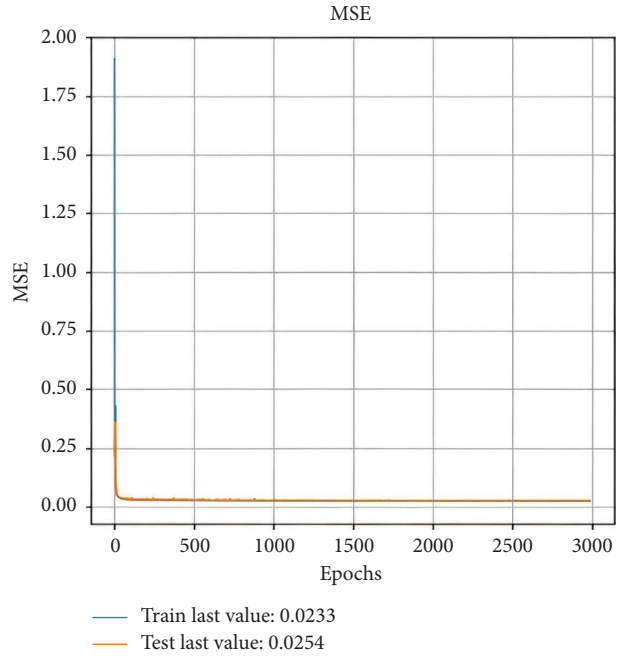

Figure 5: Proposed first training graph of MSE.

nothing. Figure 13 shows the attack success ratio comparison of existing network and DI_NN_network. It presents the performance comparison between the nonsecured" network and the "DINN_secured_network." The "nonsecured" network achieves a performance of approximately 0.079803, while the "DINN_secured_network" demonstrates a higher performance of approximately 0.00693. This indicates an improvement in performance for the "DINN_Secured_network" over the "nonsecured" network, suggesting that the security measures implemented by the "DINN_secured_network" have positively impacted its overall performance.

Figure 14 shows the mean square error comparison of existing network and proposed secured wireless network. It presents the performance comparison between the "nonsecured" network and the "DINN_secured_network."

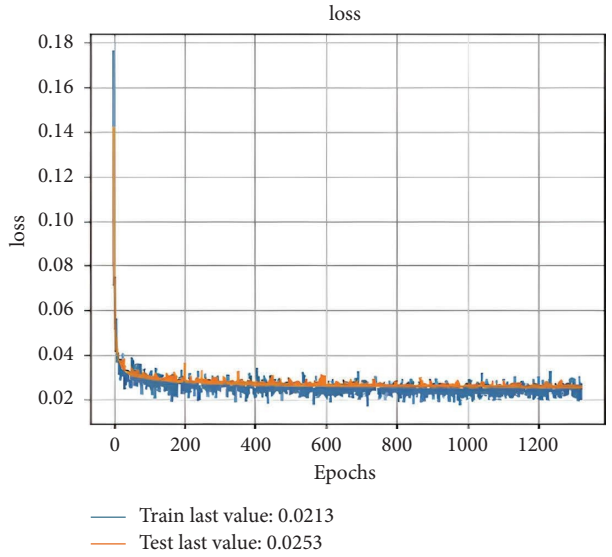

Figure 6: Proposed the second training of Loss.

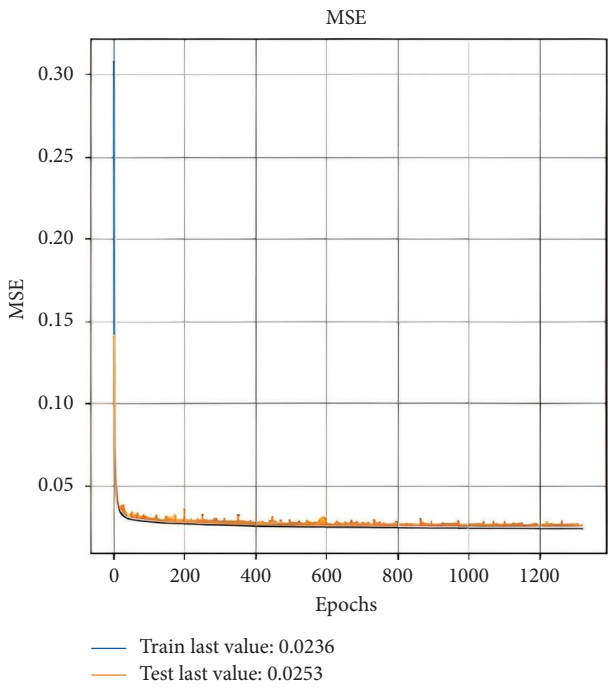

Figure 7: Proposed the second training of MSE.

The "nonsecured" network achieves a performance of approximately 0.116435, while the "DINN_secured_network" demonstrates a higher performance of approximately 0.00693. This indicates an improvement in performance for the "DINN_secured_network" over the "nonsecured" network, suggesting that the security measures implemented by the "DINN_secured_network" have positively impacted its overall performance.

4.3. Comparative Analysis and Discussion. Table 2 displays the attack success rate improvisation (in percentage) for four different attack mechanisms, namely, basic iterative mechanism attack, momentum iterative method attack, projected gradient attack, and projected gradient attack. At each attack power level (0.5, 1, 2, and 3), the "attack success rate improvisation" column demonstrates the percentage difference between the attack success rates of the respective attack mechanism and the baseline attack mechanism. Negative values indicate that the corresponding attack mechanism exhibits lower attack success rates compared to the baseline mechanism. MSE is used to quantify the average squared difference between the original input and the adversarial perturbation generated by the attack mechanism.

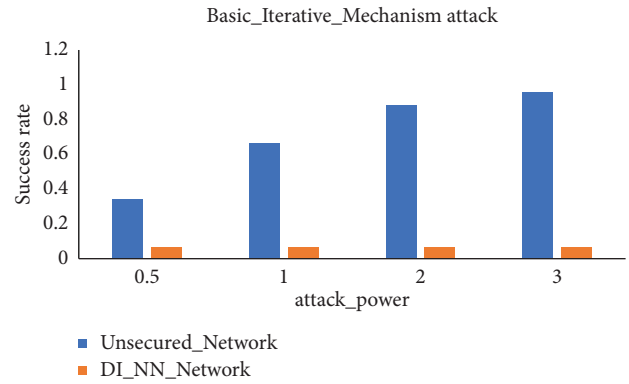

Figure 8: Attack success rate comparison.

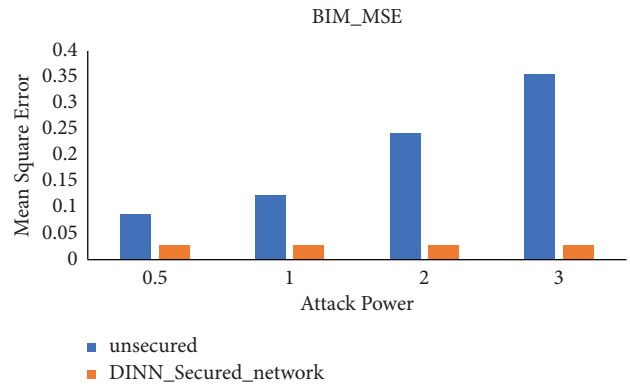

Figure 9: Mean squared error comparison.

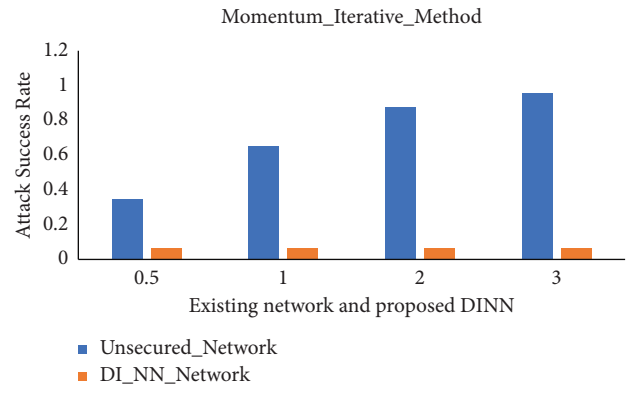

Figure 10: Attack success rate comparison.

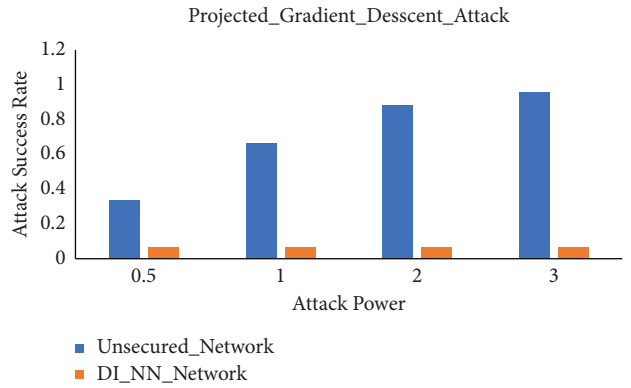

Figure 11: Attack success rate comparison of existing wireless network and proposed DINN-WN.

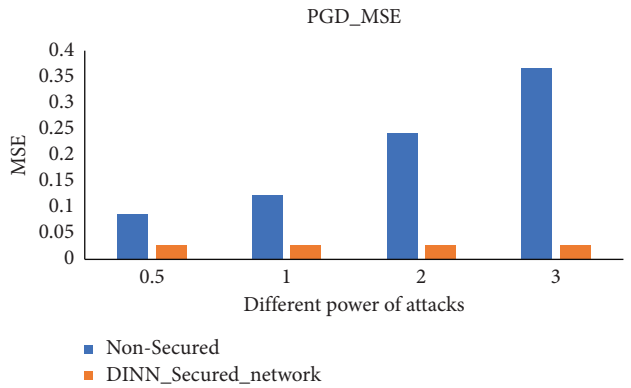

Figure 12: PGD_MSE attack.

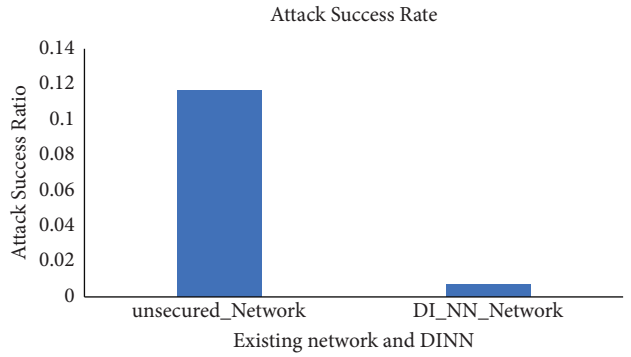

Figure 13: Attack success rate.

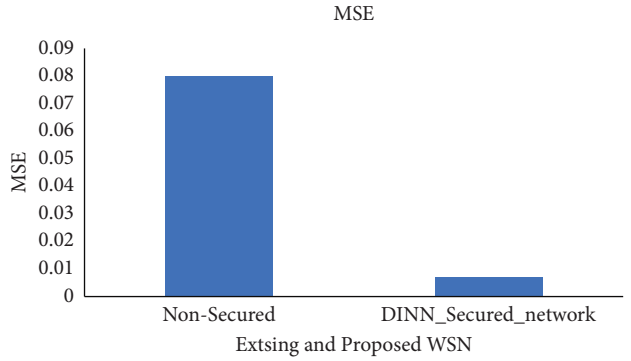

Figure 14: MSE comparison.

Table 2: Improvisation of proposed model DINN over the unsecured network.

Attack_power	Attack success rate improvisation (in percentage)		MSE	
	Basic_iterative_mechanism_attack	Momentum_iterative_method_attack	Projected gradient attack	Projected gradient attack
0.5	80.78	80.48	80.71	67.45
1	90.10	89.55	90.14	77.07
2	92.51	92.25	92.63	88.37
3	93.14	92.93	93.14	92.30

It provides insights into the distortion introduced by the attacks and helps in evaluating the robustness of the defended model.

5. Conclusion

This research designs and develops a DINN for securing the physical layer for data transmission in the network. DINN integrated the two architectures: first neural network architecture are based on the sparse connection and second one is based on the dense connection, both are interconnected to optimize the loss fucntion. DINN based wireless network is evaluated consideirng the two security parameter, i.e., attack success rate and MSE considering the different attack such as basic_gradient_mechanism, momentum_iterative_mehod_attack, projected_gradient_descent attack, and C&W attack. Moreover, the performance evaluation suggests that proposed DINN provides the higher security than the existing wireless network consideirng the evaluation parameter of attack success rate and mean square error. The proposed consistently show improved performance, with improvisation percentages ranging from approximately 80.48% to 93.14% compared to the baseline attack. DINN observes the better security and higher performance rate against the high adversial attack, and there are other types of deep learning-based attack which needs to be considered for future work.

Data Availability

The labeled datasets used to support the findings of this study can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the support from REVA University for the facilities provided to carry out the research.

References

[1] D. C. Nguyen, P. Cheng, M. Ding et al., "Enabling AI in future wireless networks: a data life cycle perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 553–595, 2021.

[2] M. Rekha and B. Mariappan, "6G and next gen networks with ultra-dense heterogeneous networks: system architecture, performance metrics," *Challenges and Risks Involved in Deploying 6G and NextGen Networks*, pp. 15–31, 2022.

[3] N. Aneja, S. Aneja, and B. Bhargava, "AI-enabled learning architecture using network traffic traces over IoT network: a comprehensive review," *Wireless Communications and Mobile Computing*, vol. 2023, Article ID 8658278, 12 pages, 2023.

[4] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6G: a comprehensive survey on technologies, applications, challenges, and research problems," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, 2021.

[5] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2356–2366, 2021.

[6] W. Xu, C. Yuan, S. Xu, H. Q. Ngo, and W. Xiang, "On pilot spoofing attack in massive MIMO systems: detection and countermeasure," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1396–1409, 2021.

[7] T.-X. Zheng, Y. Wen, H.-W. Liu, Y. Ju, and H.-M. Wang, "Physical-layer security of uplink mmWave transmissions in cellular V2X networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 11, pp. 9818–9833, 2022.

[8] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[9] H. Sharma and N. Kumar, "Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: a survey," *Physical Communication*, vol. 57, Article ID 102002, 2023.

[10] Y. Zhang, W. Xia, G. Zheng, H. Zhao, L. Yang, and H. Zhu, "Secure transmission in cell-free massive MIMO with low-resolution DACs over rician fading channels," *IEEE Transactions on Communications*, vol. 70, no. 4, pp. 2606–2621, 2022.

[11] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, 2012.

[12] C. Soni and N. Gupta, "Enhancement of PLS model of massive MIMO by detecting eavesdrop attacks and improving the secrecy capacity of the system based on optimization strategy," *Wireless Personal Communications*, vol. 129, no. 2, pp. 1143–1159, 2023.

[13] W. Xia, G. Zheng, Y. Zhu, J. Zhang, J. Wang, and A. P. Petropulu, "A deep learning framework for optimization of MISO downlink beam forming," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1866–1880, 2020.

[14] W. Xia, T. Q. S. Quek, K. Guo, W. Wen, H. H. Yang, and H. Zhu, "Multi-armed bandit-based client scheduling for federated learning," *IEEE Transactions on Wireless Communications*, vol. 19, no. 11, pp. 7108–7123, 2020.

[15] X. Zhang, D. Guo, K. An, Z. Ding, and B. Zhang, "Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems," *IEEE Access*, vol. 7, pp. 57332–57340, 2019.

[16] X. Zhang, T. Liang, K. An, G. Zheng, and S. Chatzinotas, "Secure transmission in cell-free massive MIMO with RF impairments and low-resolution ADCs/DACs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8937–8949, 2021.

[17] X. Wang, Y. Gao, G. Zhang, and M. Guo, "Security performance analysis of cell-free massive MIMO over spatially correlated Rayleigh fading channels with active spoofing attack," in *Proceedings of the 2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 540–545, Nanjing, China, October 2020.

[18] S. Timilsina, D. Kudathanthirige, and G. Amarasuriya, "Physical layer security in cell- free massive MIMO," in *Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, Abu Dhabi, United Arab Emirates, December 2018.

[19] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: optimal power control against active eavesdropping," *IEEE Transactions on Communications*, vol. 66, no. 10, pp. 4724–4737, 2018.

[20] M. Alageli, A. Ikhlef, F. Alsifiany, M. A. M. Abdullah, G. Chen, and J. Chambers, "Optimal downlink transmission for cell-free SWIPT massive MIMO systems with active eavesdropping," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1983–1998, 2020.

[21] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[22] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 2093–2106, 2018.

[23] W. Zhang, H. Lin, and R. Zhang, "Detection of pilot contamination attack based on uncoordinated frequency shifts," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2658–2670, 2018.

[24] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: from AWGN channel to THz band," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3378–3388, 2020.

[25] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[26] J. Tang, L. Jiao, K. Zeng, H. Wen, and K.-Y. Qin, "Physical layer secure MIMO communications against eavesdroppers with arbitrary number of antennas," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 466–481, 2021.

[27] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: a review," in *Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1010–1015, Las Vegas, NV, USA, January 2020.

[28] P. Chavan and K. Satyanarayan Reddy, "Integrated cross layer optimization approach for quality of service enhancement in wireless network," 2021, https://www.ijcse.com/docs/INDJCSE21-12-04-144.pdf.

[29] P. Chavan and K. S. Reddy, "QoS aware video transmission in wireless network: successful and failure existing technique," *International Journal of Recent Technology and Engineering*, vol. 5, pp. 2277–3878, 2020.

[30] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: threat assessment and mitigation," in *Proceedings of the 2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Kansas City, MO, USA, May 2018.

[31] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2019.

[32] W. Khalid, M. A. U. Rehman, T. V. Chien, Z. Kaleem, H. Lee, and H. Yu, "Reconfigurable intelligent surface for physical layer security in 6G-IoT: designs, issues, and advances," *IEEE Internet of Things Journal*, p. 1, 2023.

[33] G. Dhingra, S. Supreeth, K. R. Neha, R. V. Amruthashree, and D. Eshitha, "Traffic management using convolution neural network," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 146–149, 2019.

[34] G. Shruthi, M. R. Mundada, S. Supreeth, and B. Gardiner, "Deep learning-based resource prediction and mutated leader algorithm enabled load balancing in fog computing," *International Journal of Computer Network and Information Security*, vol. 15, no. 4, pp. 84–95, 2023.