



IMPROVING SECURITY FOR 6G NETWORKS USING BEAMFORMING TECHNOLOGY

Saad Ahmed Ayoob^{*1}, Firas S. Alsharbaty², Zainab Salim Abd³

^{1,2}Department of Communications and Intelligent Digital Systems Engineering, Engineering, University of Mosul, Mosul, Iraq.

³Department of Computer Networks and Internet, College of Information Technology, Ninevah University, Mosul, Iraq.

¹<http://orcid.org/0000-0002-9226-5481>, ²<https://orcid.org/0000-0002-0353-1777>, ³<https://orcid.org/0009-0003-2629-1459>

Email: *sa_ah_ay@uomosul.edu.iq, Firas.alsharbaty@uomosul.edu.iq, Zainab.abd@uoninevah.edu.iq

ARTICLE INFO

Article History

Received: February 10, 2026

Reviewed: April 17, 2026

Accepted: May 17, 2026

Published: June 30, 2026

Keywords:

Sixth Generation 6G,
Beamforming Technology,
Deep Neural Network (DNN),
reconfigurable intelligent surfaces (RIS),
signal-to-noise ratio and
interference (SINR),
Starlink Satellite System,

ABSTRACT

6G offers possibilities through technologies such as millimeter waves, terahertz waves, beamforming, and reconfigurable intelligent surfaces (RIS). Each technology introduces its own challenges. One of the most significant challenges is security, and this is the subject of our study. Vulnerabilities arise from narrow beams when using millimeter waves. Through this study, the security of 6G networks is enhanced with deep learning algorithms and using RIS to guide the smart beam to counter attacks. A multi-layered deep neural network (DNN) is used to predict the signal-to-noise ratio (SINR) and interference with and without the mobility of users. Additionally, a mathematical model was developed to optimize the SINR and counter some security threats, such as jamming, spoofing, and data poisoning. This work contains realistic channel modeling to simulate user mobility and logarithmic shading effects. Our results show that the maximum average SINR was 33.2351 using beamforming with RIS, and after adding deep learning, the improvement was 27.5%. Using a DNN model, SINR levels (25-45 dB) under three attacks and continuous user movement at a speed of $v = 1.5 \text{ m/s}$, and a prediction accuracy of 0.032 was obtained for the root mean square error (RMSE) value. It should be noted that the achieved performance depends on the deployment and channel conditions considered. The proposed system provides a timely security response with a training period of 37 seconds, which is suitable for 6G requirements.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

Millimeter-wave links are strongly affected by changes in the surrounding environment, especially when users are in motion. These factors reduce connection reliability and increase beam misalignment [1], [2]. These limitations are exacerbated by the limited spatial selectivity and increasing density of connected users. Beamforming techniques are applied, aiming to direct most of the signal energy toward intended receivers while limiting unintended radiation [3]. Adaptive beamforming technology has proven effective in improving SINR because it can respond to rapid changes in the environment and user movement (1.1-11.1 m/s), allowing the system to track shifts in channel conditions over a 10 ms period [4]. Each adaptive approach (analog, digital, hybrid) comes with its own set of trade-offs, balancing computational demands, hardware costs, and energy consumption [5- 7]. Artificial intelligence techniques have been added to enhance integration within beamforming frameworks and improve overall performance. It has been proven that data-driven approaches will be used as key tools by manufacturers and operators to meet 6G requirements through the use of unsupervised learning and reinforcement learning [8]. At the same time, user movement adds further challenges that degrade the quality of service, directly impacting the reliability of physical layer security. As movement increases, channel coherence time decreases, leading to obsolescence of channel state information (CSI) and rendering estimated channel parameters obsolete before they are used. Beamforming decisions based on legacy CSI are often incorrect, resulting in beam misalignment. This, in turn, causes the main lobe to deviate from the intended user, while uncontrolled side lobes emerge, facilitating unintended information leakage in multiple spatial directions [9]. Simultaneously, eavesdroppers exploit this vulnerability and enhance the received SNR without altering the encryption mechanisms [10].

The statistical characteristics of the wireless channel are affected by random shading effects caused by physical obstructions, leading to increased channel gain variations. These conditions create a vulnerability for model poisoning attacks [11, 12]. Attackers exploit this vulnerability to inject malicious signals, particularly during deep fade-through periods. Channel estimation and beamforming optimization are affected, and incorrect beamforming weights are generated, making the system susceptible to other attacks such as jamming. Countering these threats is crucial, especially for critical applications supporting 6G technologies, such as remote surgery, autonomous vehicles, 3D communications, and smart city architecture [13]. Ensuring data security is a preventative necessity, not an option, especially given the threats facing quantum computing that compromise high-level encryption systems [14]. Physical-layer security mechanisms based on intrinsic channel characteristics are considered a primary and sustainable line of defense. Recent research to address and mitigate these threats has relied on two main technologies: RIS technology, which utilizes programmable electromagnetic structures (controlled by a microcontroller) capable of adapting the radio propagation environment by creating virtual vision paths (VLS), enhancing signal strength relative to noise, and minimizing information leakage to eavesdroppers [15-17]. The second technology is deep learning techniques, which enable accurate CSI prediction and proactive beamforming design by observing complex, nonlinear channel behaviors that are difficult to model using traditional analytical techniques [18]. The authors [19] presented a comprehensive study of the role and importance of 6G in achieving 99.99999% reliable connectivity, reaching speeds of 1 Tbps, and increasing positioning accuracy through millimeter wave, terahertz frequency, and RIS technologies.

They also highlighted the critical trade-offs between spectrum efficiency and power consumption, and between security and spectrum efficiency. They also highlighted the critical trade-offs between spectral efficiency and power consumption, and between security and spectral efficiency. Another study [20] focused on improving the energy efficiency of multi-user communications using RIS technology, disregarding user mobility. This was achieved by employing a transmission power distribution model and a phase-shift model for reflective elements to mitigate the non-convexity problem. The study demonstrated that RIS technology can achieve up to 300% higher energy efficiency than amplification and retransmission relay systems. The study [21] investigated physical layer security by combining RF and free-space optical (FSO) communications in three eavesdropping scenarios: RF eavesdropping, FSO eavesdropping. Closed-form expressions were derived for average security capacity, probability of security breach, and effective security throughput. The results demonstrated that RIS is effective in securing confidential information and extending coverage and capacity. The above demonstrates that the development of RIS and artificial intelligence has achieved convincing results, but more is needed, and most current studies assume the static nature of user positions. This assumption is unrealistic and ignores the impact of mobility and fading speed, especially for 6G. Research often focuses on a single type of attack (eavesdropping only) without addressing complex attacks (jamming and data poisoning). At the same time, AI-based communication models need to integrate multiple technologies, particularly when channel inputs change abruptly due to user movement. This paper contributes to addressing these challenges by:

1. Using beamforming and RIS, a DNN is proposed with a regular loss function (RDF) that balances prediction accuracy and generalization capability, with an RMSE of 0.032 for stationary users.
2. To simulate a 6G channel, a security model was developed that integrates user traffic (1.5 m/s) and the shading effect (4 dB) to counter three attacks (jamming, poisoning, and spoofing).
3. The proposed system demonstrated the ability to maintain stable security capacity within a SINR security range (25-45 dB) with the worst channel conditions (three attacks and user traffic) through statistical analysis of the SINR distribution.
4. Previous studies [22, 23] focused on a single threat, while this research proposes a comprehensive analytical model of the signal-to-noise ratio and interference (Equation 5) by incorporating the collective spoofing of three attackers. Additionally, a deep learning hybrid cost function (Equation 6) was designed to counter the effects of random shading in 6G environments.

This manuscript consists of the following sections. Section 2 introduces the system model and the detailed methodology adopted in this study. Section 2.1 outlines the main assumptions of the considered network, followed by the passive RIS-assisted beamforming model and the formulation of the secrecy capacity in Section 2.2. Sections 2.3 and 2.4 describe the learning-based formulations and the training procedure of the proposed Robust-DNN, while Section 2.5 addresses the modeling of dynamic environments under user mobility. Section 3 presents the simulation results and their discussion. The impact of multi-mode attacks is analyzed, and the beamforming performance under static user conditions is reported in Sections 3.1 and 3.2, with the evaluation of deep learning optimization in the static scenario provided in Section 3.3. The training performance of the proposed Robust-DNN under mobility conditions is examined in Section 3.4. Finally, the conclusions and future research directions are summarized in the last section.

II. SYSTEM MODEL AND DETAILED METHODOLOGY

Most In this study, we focus on a downlink millimeter-wave (mmWave) network that operates at a carrier frequency of 28 GHz to ensure high-capacity secure communication. The proposed architecture consists of three main entities: a Base Station (BS) with M antennas, a passive RIS having N elements, and a dense cluster of legitimate users ($K=20$) who share the frequency spectrum simultaneously. It is tested at three locations to determine the RIS optimal position for serving a randomly positioned group of users. The system aims to increase the sum secrecy rate (SSR) under multi-attack conditions, as illustrated in Figure 1.

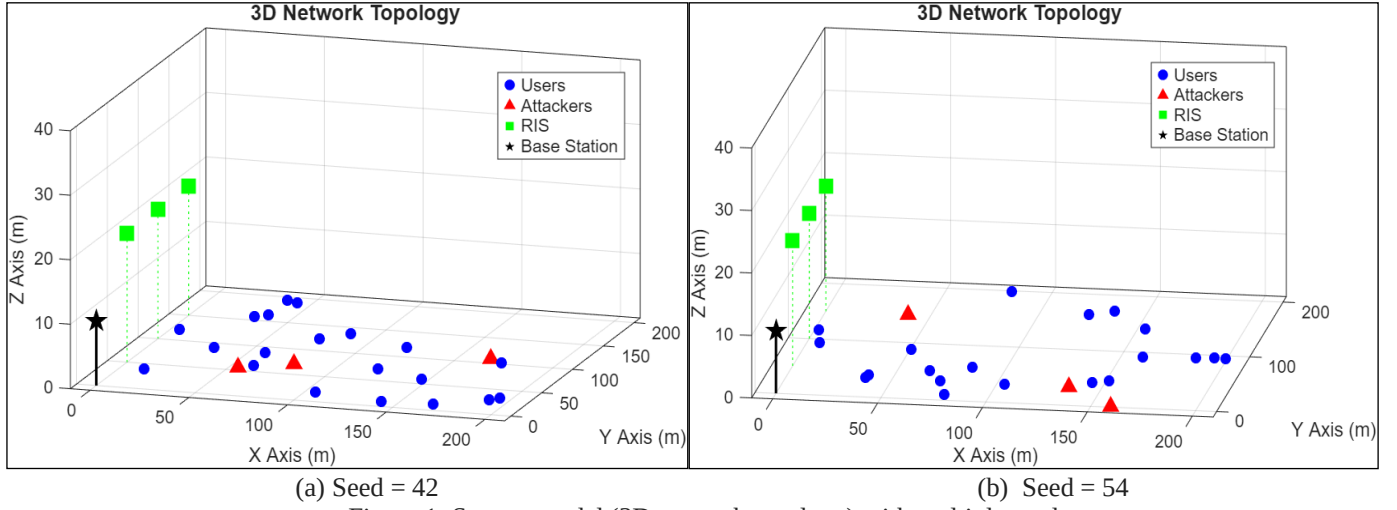


Figure 1: System model (3D network topology) with multiple seeds.

Source: Authors, (2026).

II.1 SYSTEM ASSUMPTIONS

The model is built on assumptions to ensure a realistic simulation approach. The main assumptions are:

- The operating environment: A microcell network using a 28 GHz, making it susceptible to blockage and result in significant path losses.
- Cluster-based users: The model includes $K=20$ users sharing the same frequency resources, with inter-user interference that needs to be addressed.
- Attack Model: Three active non-colluding eavesdroppers in the network. They operate with imperfect Channel State Information (CSI) and execute multi-mode attacks (jamming, spoofing, and poisoning).
- Channel dynamics: channels change randomly due to log-normal shadowing and user mobility, resulting in an imperfect CSI.
- RIS: A passive intelligent reflector surface that controls only the phase (amplitude = 1) and whose position is selected from predefined filters.

The mmWave Channel Model used the Close-In (CI) Free-Space Reference Distance path loss model to characterize the urban environment. The path loss at distance d is expressed as [24, 25]:

$$PL(d)[dB] = FSPL(d_0) + 10\bar{n} \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \quad (1)$$

Where $FSPL(d_0)$ is the free space path loss at reference distance $d_0=1$ m. $\bar{n}$ is path loss exponent = 3.0, and $X_\sigma \sim \mathcal{N}(0, 4 \text{ dB})$ represents the log-normal shadowing.

II.2 PASSIVE RIS-ASSISTED BEAMFORMING MODEL AND SECRECY CAPACITY FORMULATION

The total signal y_k that reaches users k_{th} is the sum of the direct path $h_{d,k}$ and the reflected path $h_{r,k}$ in the absence of an obstacle, so the general equation is [26]:

$$y_k = (h_{r,k}^H \Phi G + h_{d,k}^H)x + n_k \quad (2)$$

Where G is RIS-to-transmitter channel matrix, Φ is the reflection matrix controlled by RIS (diagonal matrix of phase shifts), and n_k is the added noise at the receiver k . The passive RIS-assisted beamforming enhances the received signal power for the intended user through the coherent superposition of the reflected signals from all RIS elements, based on finding the optimal equation below [26].

$$P_{rx} \propto \left| \sum_{n=1}^N \alpha_n e^{j(\theta_n - \phi_{inc} - \phi_{ref})} \right|^2 \approx N^2 \quad (3)$$

α_n represents the reflection amplitude of n RIS element, and θ_n is the adjustable phase shift applied by this element. ϕ_{inc} and ϕ_{ref} refer to the incident and reflected phase components associated with variations in propagation paths. The RIS phase shifts must be optimally adjusted to compensate for the incident and reflected phases, ensuring that all reflection components are constructively combined at the receiver. If the coherent alignment condition is met, the received signal power can be considered to be proportional to the square of the number of RIS elements, i.e., $P_{rx} \propto N^2$. This squared gain enhances the RIS phase, boosting the effective channel power and directly impacting the SINR ratio, thereby increasing the system's security capacity. So, standard secrecy capacity is the capacity that represents the difference between the capacity of the legitimate channel and the capacity of the eavesdropping channel, according to the following equation [22, 26]:

$$C_{sec,k} = \left[\log_2(1 + \text{SINR}_k) - \max_{e \in E} \log_2(1 + \text{SINR}_{e,k}) \right]^+ \quad (4)$$

Where $C_{sec,k}$ is secrecy capacity for user k, i.e., the maximum secure data transfer rate that attackers cannot intercept. $e \in E$ is a specific attacker within the group of attackers. $SINR_{e,k}$ is SINR that an attacker can capture from the user k. $[]^+$ is the strongest listening ability of any attacker in the group E.

II.3 PROPOSED FORMULATIONS

This section is the most important compared to previous works [22, 26] that typically consider a single threat type or a single user, this study introduces three novel formulations to address the complexity of 6G security.

II.3.1 Multi-Threat SINR Formulation

A comprehensive SINR formulation is proposed, combining the interference effects from three different sources and calculating the interference between the dense cluster ($K=20$) with aggregate Jamming from multiple attackers. The proposed interference term is formulated as:

$$SINR_k^{Robust} = \frac{P_t |h_{eff,k}^H w_k|^2}{\underbrace{\sigma^2 + \sum_{j \neq k} P_t |h_{eff,k}^H w_j|^2}_{\text{User Interference}} + \underbrace{\sum_{m=1}^3 P_{J,m} |h_{J,m,k}|^2}_{\text{Aggregate Jamming}}} \quad (5)$$

Where $h_{eff,k}^H$ is effective channel vector for user k after considering the effect of RIS or any channel processing, w_k is beamforming vector used to direct the signal to the user k. σ^2 is noise power, i.e., thermal noise power (AWGN) at the receiver. w_j is beamforming vector for user j: This vector represents the beamforming that directs the signal towards user j. It is used to adjust the phase and amplitude of each element in the transmitting array (such as transmitter antennas or RIS) so that the signal reaches the target user with strength. $P_{J,m}$ is attacker transmission power m: The power used by the attacker m to transmit the jamming signal, which is added to the denominator to reduce the SINR of the user k. $h_{J,m,k}$ is attacker channel m to user k: This represents the effect of the jamming or attack coming from attacker m on user k, i.e., how the jamming signal travels through the channel and reaches the user. It is worth noting that equation (5) combines internal and external interference sources, which is a more rigorous assessment than the simplified models in [22] and [25].

II.3.2 Robust Loss Function of a Robust Neural Network

Reference [27] relied on general organization and did not specify a cost function. In this research, loss function is specifically tailored to serve the purpose of wireless communications by balancing accuracy with weight stability to minimize the effects of X_σ (shading) as show in equation 5. In other words, the loss function ($\mathcal{L}(\theta)$) represents the amount of error between the target values and the outputs predicted by the deep neural network (DNN) model, incorporating regulatory terms to avoid overlearning and improve stability. Dropout was used not only to prevent overfitting but also as a mechanism to simulate channel breakage or estimation error during training. This allows the system to operate efficiently even if the channel data is inaccurate to a certain extent.

$$\mathcal{L}(\theta) = \frac{1}{K} \sum_{k=1}^K \left(SINR_{target,k} - DNN(s_k; \theta) \right)^2 + \underbrace{\lambda_1 |\theta|_2^2}_{\text{Smoothing}} + \underbrace{\lambda_2 \sum \text{Dropout}(\theta)}_{\text{Uncertainty Handling}} \quad (6)$$

Where θ is vector parameters of the DNN model, such as layer weights and neural network parameter in nodes. s_k are the input features of the model for user k include channel properties, user location, and RIS properties. $DNN(s_k; \theta)$ is the output of the neural network after processing the inputs s_k using the parameters θ . $\left(SINR_{target,k} - DNN(s_k; \theta) \right)^2$ is the error squared per user, which is the basic component of the mean squared error (MSE). This term $\lambda_1 |\theta|_2^2$ reduces overfitting and makes the model smoother. Whereas hyperparameters (λ_1, λ_2) determine the importance of each regulation term in relation to the main error component. The addition of λ_2 (utilizes a Dropout mechanism) addresses sudden and rapid channel changes, thereby mitigating uncertainty. This mechanism enhances the model's flexibility during training, increasing its adaptability to channel conditions and improving SINR prediction.

II.3.3 Sum-Rate Based Placement Algorithm

In reference [23], the placement was optimized for a single user. A new placement criterion was developed based on the spectral center of gravity for all users as follows.

$$l_{opt} = \arg \max_{l \in \mathcal{L}} \sum_{k=1}^{20} E [\log_2(1 + SINR_k(l))] \quad (7)$$

This formulation expands the placement optimization problem to accommodate the random spatial distribution of the user cluster, ensuring optimal coverage for the group rather than a single fixed point.

II.4 ROBUST-DNN ARCHITECTURE AND TRAINING

A deep robust neural network (Robust-DNN) with a hierarchical architecture is simulated to treat the non-convex optimization mentioned in equation (7). First, Robust-DNN is designed with static users to capture high-dimensional channel dependencies. The network consists of five fully connected (FC) layers configured as follows:

- **Input Layer:** The normalized feature vector is entered only for the real/imaginary parts of the channel and coordinates. Input data is normalized using the Min-Max scaling technique to map features into the range [0, 1] to achieve stable gradient convergence during training.

- **Hidden Layers:** The network is built as a pyramidal structure with [2048, 1024, 512, 256] neurons. Leaky ReLU activation ($\alpha = 0.01$) is used instead of standard ReLU to mitigate and reduce dying ReLU. Also, we ensure gradient flow in deep layers.
- **Regularization:** A hybrid regularization strategy is used to achieve robustness when there is imperfect CSI. Batch normalization is applied after each of the first three FC layers to accelerate convergence. High dropout rates of 0.5 and 0.4 are applied to the first two layers, respectively, to simulate channel uncertainties. To achieve L2 regularization It is easy to add a factor 0.001 to the loss function.
- **Output Layer:** A single regression neuron is used to predict the normalized secrecy rate.

Second, the model is trained using the Adam optimizer for 300 epochs with a mini-batch size of 128. A piecewise learning rate schedule is used, starting at 0.003 and dropping by a factor of 0.5 every 60 epochs to ensure precise convergence. Finally, a Savitzky-Golay filter (order 2, frame length 7) is applied to the predicted outputs (y_{pred}) to smooth out numerical noise before denormalization, to achieve more stable spectral efficiency curves.

II.5 DYNAMIC ENVIRONMENT MODELING AND MOBILITY TESTING

User motion was added to simulate a 6G reality by extending the simulation of a time-varying dynamic environment that includes user movement and random shading.

II.5.1 Motion and Channel Model

A dynamic scenario was adopted using 500-time snapshot with random user movement at a constant speed $v_{\text{max}} = 1.5\text{m/s}$ to simulate pedestrian behavior. The normal logarithmic shading effect X_σ with a standard deviation of $\sigma = 4$ dB was introduced to represent obstacles in urban microcells. The time-varying path loss for user k at time t was calculated as follows:

$$PL_k(t) = \text{FSPL}(d_0) + 10\bar{n} \log_{10}(d_k(t)) + X_\sigma(t) \quad (8)$$

II.5.2 Robust Deep Neural Network for Dynamic Tracking

A robust, adaptive DNN was built to handle rapid channel fluctuations. The specialized network was trained on the dynamic dataset, and the network structure was optimized for generalization rather than memorization by:

Updating inputs that include dynamic characteristic vectors represented by updated coordinates (x_t, y_t, z_t) and instantaneous distances. The structure consists of two fully connected layers, each containing 1024 and 512 neurons, respectively. The necessary regulation strategy to prevent overshoot in training on specific pathways is achieved by increasing the dropout rates to 0.3 and 0.2 for the first and second layers, respectively, and implementing early stop (verification patience = 10) to halt training when the generalization performance reaches its maximum value.

III. SIMULATION RESULTS AND DISCUSSION

The new models were tested and evaluated based on the design equations in Section 2 using MATLAB R2025b. This simulation included one base station and three RIS test sites to select the optimal site achieving the highest SINR before and after the attack. Twenty users were randomly assigned to ensure comprehensiveness within a 200×200 m area, representing the coverage area for millimeter waves as shown in Figure 1. The analysis was performed by examining beamforming assisted by RIS, then expanding the model to include a DNN, and finally, assessing the effect of user mobility at 1.5 m/s. Table 1 shows the main simulation parameters.

Table 1: The main simulation parameters.

Parameter	Value	Description
Software	MATLAB R2025b	Simulation Platform
Carrier Frequency f_c	28 GHz	mmWave Band
Bandwidth BW	100 MHz	System Bandwidth
Tx Power P_{tx}	30 dBm (1 Watt)	Base Station Power
Noise Power N_0	-100 dBm	Thermal Noise Floor
RIS Elements N	50 - 1000	Variable Array Size
Path Loss Exponent α	3.0	Urban NLoS Environment
Mobility Speed v	1.5 m/s	Pedestrian Motion (Dynamic Scenario)
Shadowing σ	4 dB	Log-Normal Shadowing Std. Dev.
Deep Learning Optimizer	Adam	Adaptive Moment Estimation

Source: Authors, (2026).

III.1 RESULTS OF MULTI-MODE ATTACKS

In this simulation, the SINR average was used because it reflects the reliability of the connection and the quality of the channel, as well as its susceptibility to environmental factors such as interference or attacks. Figure 2 shows the effect of increasing the number of RIS elements (50–1000) (whose positions were changed three times) on the SINR average without any attack. According to Equation (3), increasing N certainly leads to an increase in the SINR average, but not exponentially, due to the increased interference, as illustrated in Figure 2.

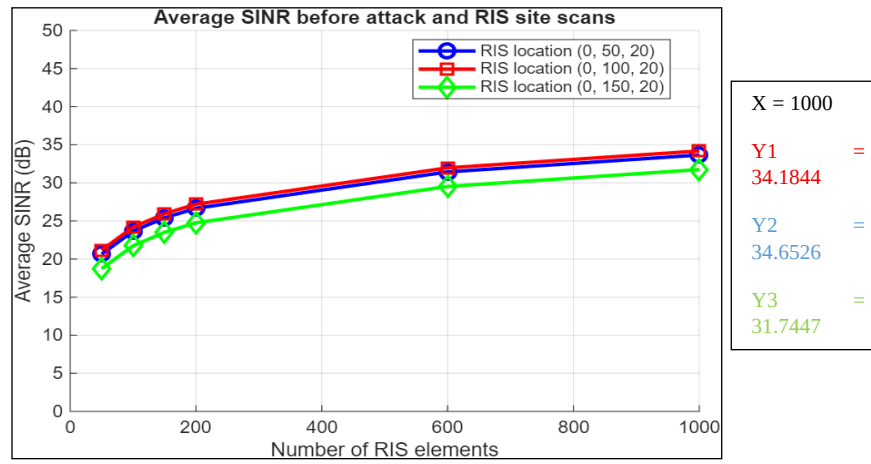


Figure 2: Average SINR vs. number of RIS elements before attack with multiple RIS locations.
Source: Authors, (2026).

System performance tends to deteriorate, especially the average SINR, when under attack with no attack defense measures in place. Figure 3 illustrates the severe impact of a jamming attack, and the user's proximity to the base station is ineffective due to the high noise level. At the same time, for the RIS (0, 100, 20) site, increasing the number of RIS elements does not eliminate this attack but rather mitigates it, as the average SINR drops to 2.6811 dB when $N = 50$ elements and to 15.0394 when $N = 1000$ elements. The severity of the impact varies depending on the type of attack. Figure 4 shows the impact of a spoofing attack, while Figure 5 shows a poisoning attack. It is worth noting that these results were obtained after repeated simulations and varying the seed value. At an $N = 1000$ value, a comparison of the three attacks suggests that the jamming attack (SINR = 15.0394 dB) is the most impactful, then the poisoning attack (SINR = 15.1492 dB), and the spoofing attack (SINR = 21.1785 dB) is the least impactful.

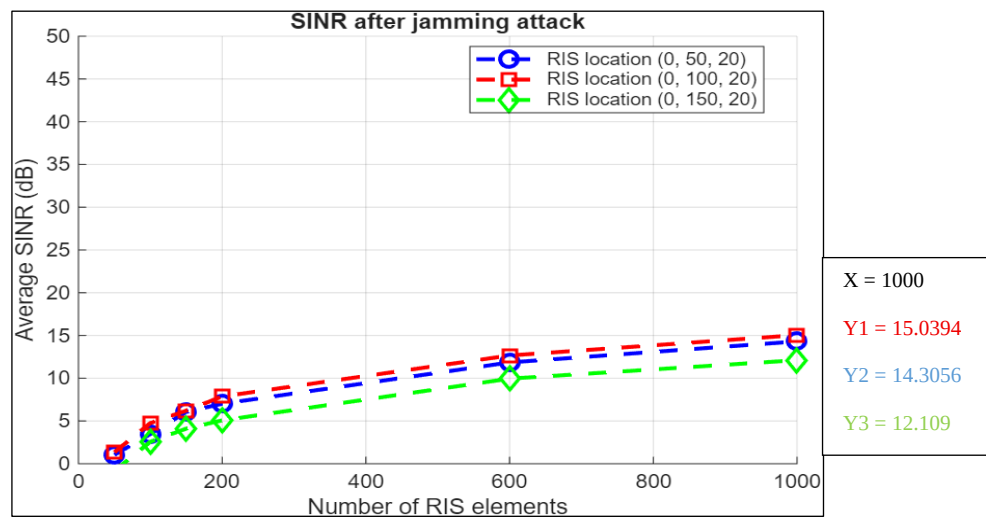


Figure 3: Average SINR vs. number of RIS elements after Jamming attack.
Source: Authors, (2026).

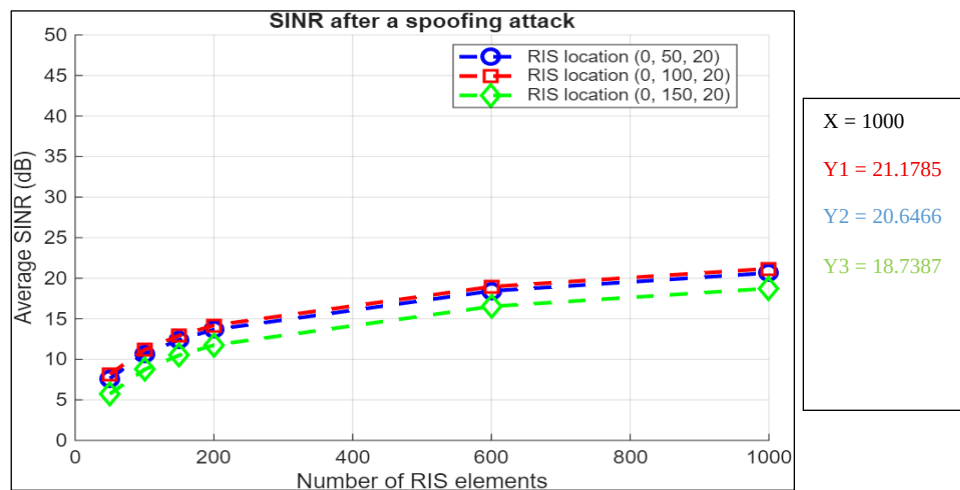


Figure 4: Average SINR vs. number of RIS elements after Spoofing attack.
Source: Authors, (2026).

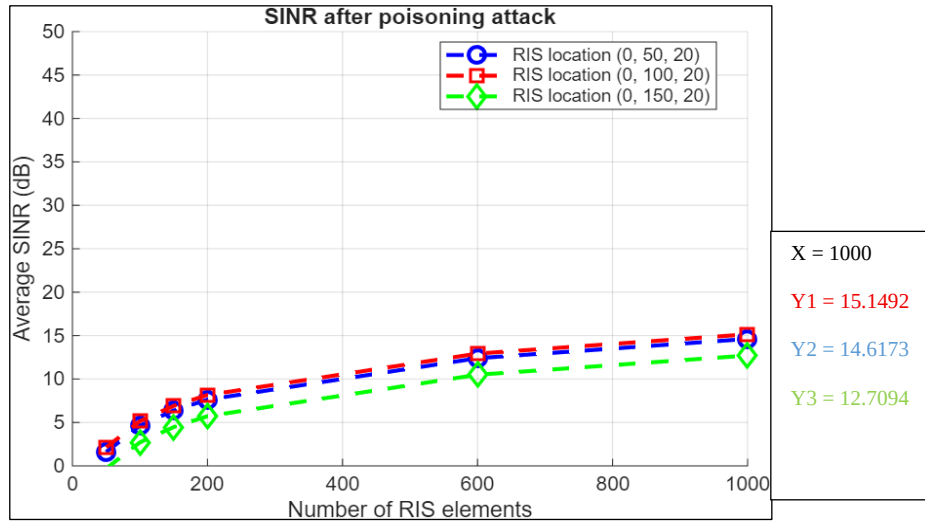


Figure 5: Average SINR vs. number of RIS elements after Poisoning attack.
Source: Authors, (2026).

III.2 RESULTS OF BEAMFORMING IN A STATIC SCENARIO

The proposed RIS-assisted beamforming optimization algorithm was implemented as mention in section 3.2 to mitigate the impact of these threats when user locations are fixed. Figure 6 illustrates the optimization of RIS element phase shifts, beamforming directed towards legitimate users, and interference cancellation. This is achieved by coherently integrating the signal paths reflected from the RIS system, thereby recovering a significant portion of the lost SINR. The beamforming gain increases with the number of RIS elements (see Equation (3)), as evidenced by the improvement in the average SINR for all tested locations to 33.1844, 32.6526, and 30.7447 dB for RIS locations 2, 3, and 1, respectively. This demonstrates the effectiveness of the proposed beamforming technique - especially at location 2- where the SINR was 34.1844 dB before the attack, meaning the attack's impact is now 1 dB and does not affect communication or data. Therefore, beamforming acts as an effective shield against ground-based attackers by establishing a strong virtual link with a direct line of sight.

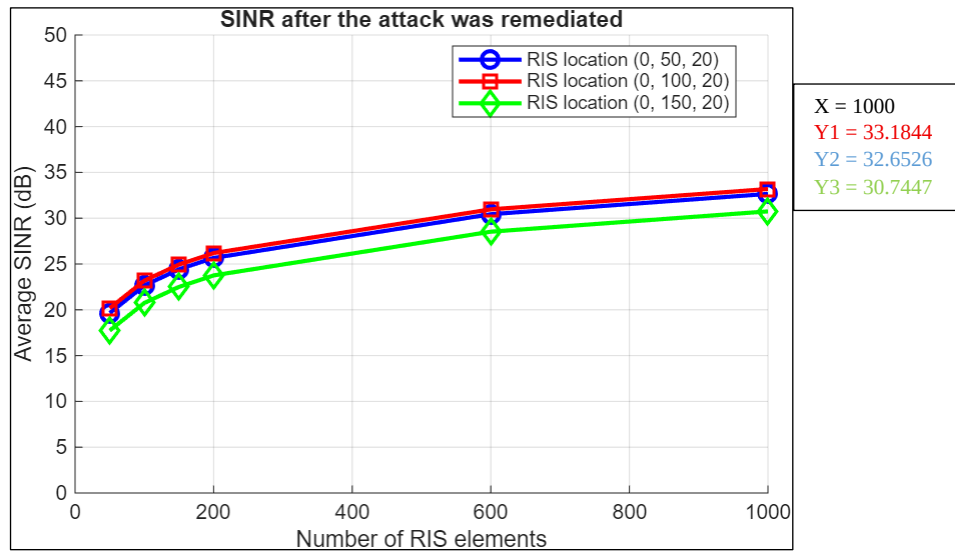


Figure 6: Average SINR after attack remediated using RIS and beamforming.
Source: Authors, (2026).

III.3 RESULTS OF DEEP LEARNING OPTIMIZATION FOR A SCENARIO WITHOUT USER MOBILITY

In the previous section, optimization was performed using an analytical mathematical solution for beamforming, and the improvement was to reduce the impact of attackers. In this section, the proposed DNN was used to optimize phase formation and achieve AI superiority. The objective is to exploit learning-based optimization to compensate for channel impairments that are difficult to capture using purely analytical methods. Figure 7 illustrates the training progress of the proposed deep neural network (DNN) over 300 training cycles in a scenario with no user movement. Convergence behavior was analyzed using two metrics: root mean square error (RMSE) and loss function (MSE). The training curve (solid blue) and validation curve (dashed black) demonstrate the convergence speed over 50 cycles, showing the effectiveness of the integrated Adam optimizer with batch normalization. The gradient vanishing problem was mitigated, and the learning process was accelerated. The model also avoided overfitting by matching the training and validation curves over 300 cycles. The use of dropout rates (0.5 and 0.4) prevented noise from being stored in the training data of the network.

The prediction accuracy was 96.6%, with an RMSE value of 0.0341. The proposed DNN is suitable for application in the 6G system due to the low computational effort, as the training process was completed within 36 seconds, which is suitable as a latency time. Figure 8 illustrates the average SINR as the number of RIS elements increases from 50 to 1000 at three different RIS positions using beamforming with and without DL. The results of the proposed Robust-DNN model show an improvement in the average SINR of 8–12 dB compared to not using it. This gain can be explained by the DNN learning and processing rapid channel changes. In contrast, the beamforming improvement relies on assuming an ideal phase shift, while the DNN model learns the nonlinear relationship between channel characteristics and then examines the SINR values to correct for phase quantization errors and coupling between elements. From the observed trend, the second-position RIS curve can be divided into two sections: increasing N from 50 to 600 leads to an increase in the average SINR in the first section. In the second section, the DL curve reaches saturation at $N=1000$ due to beam concentration sensitivity (microbeamforming) resulting from the large matrix sizes ($N=1000$) and the large gain. This causes the reflected beam to become very narrow, maximizing gain and negatively impacting beam alignment accuracy. At $N=100$, for example, the misalignment loss of the beamforming model is lower, while the misalignment loss increases significantly after the DL estimates an incorrect phase value (due to some unforeseen cause in the channel). In other words, as N increases, the difference between the two models with and without DL increases. At $N = 1000$ elements, the number of users was increased from 2 to 20 users. This illustrates the effect of interference with or without a DL response. Figure 9 shows the effect of this increase on the average SINR. A gradual decrease in the average SINR is observed with a small slope in the presence of DL and a larger slope in the presence of beamforming. At $N = 10$ users, the average SINR for the DL model is 45.8405, and for the beamforming model it is 33.2351, representing a 27.5% improvement in the average SINR. From these results, the DL model continues to operate reliably even as the number of users increases.

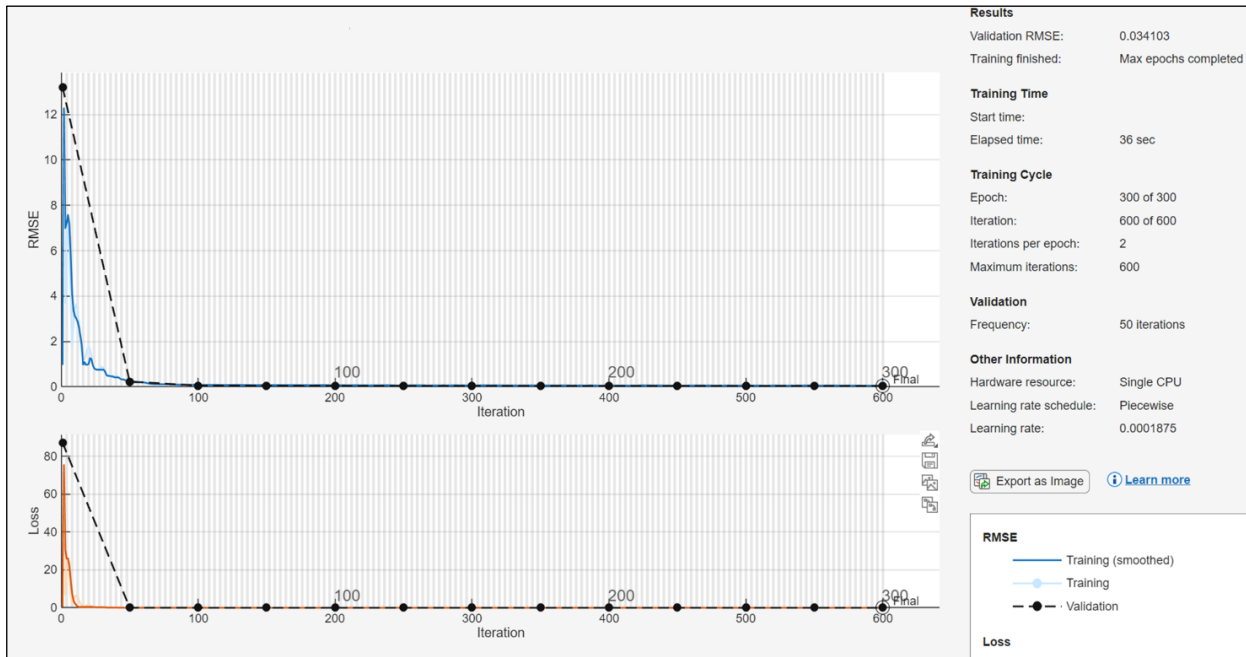


Figure 7: Robust-DNN training performance in static user case.
Source: Authors, (2026).

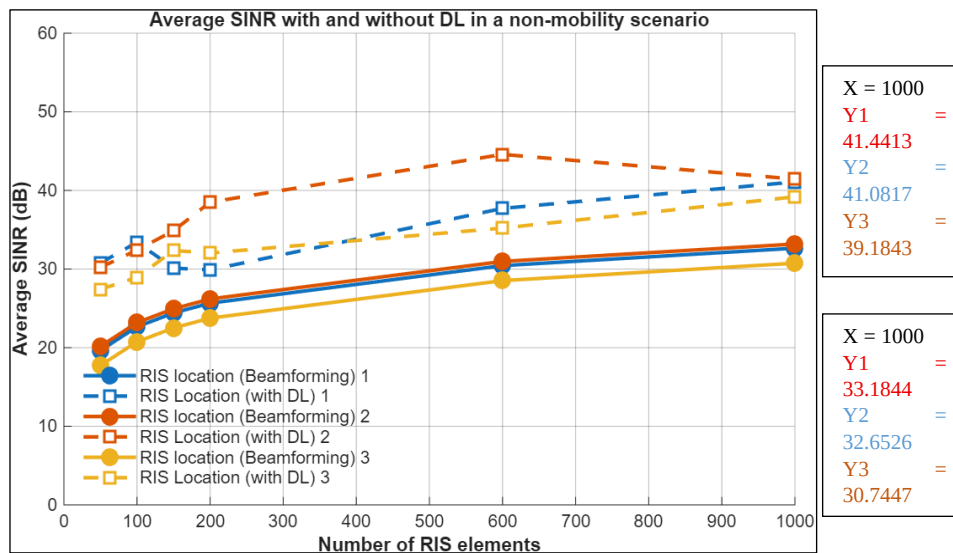


Figure 8: Average SINR vs. number of RIS elements after with and without DL in static user case.
Source: Authors, (2026).

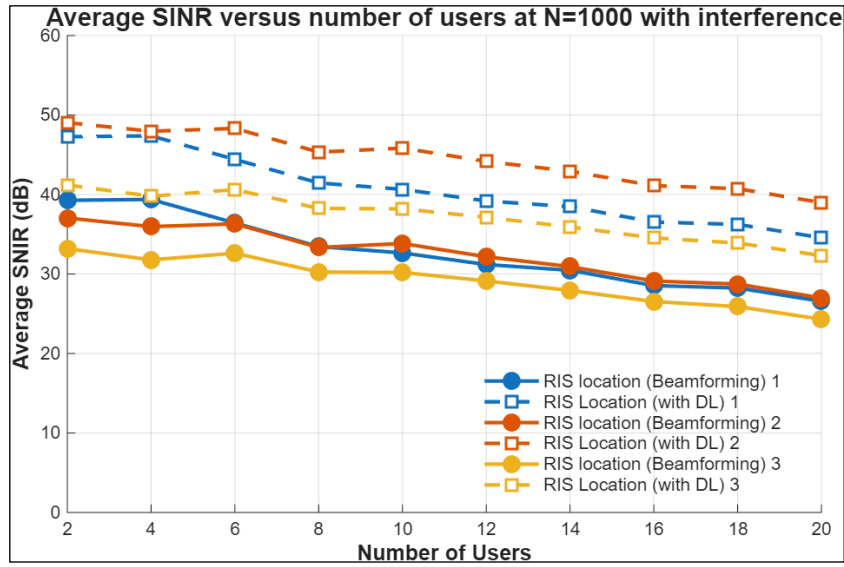


Figure 9: Average SINR vs. number of users in static user case.
Source: Authors, (2026).

III.4 TRAINING RESULTS OF THE PROPOSED ROBUST-DNN IN A MOBILITY SCENARIO

User mobility was added to the previous model to test it practically by increasing the variability and complexity of the 6G channel, as shown in blue in Figure 10. Applying equations 4 and 5, these swings were tracked, and the adaptive network's ability to mitigate the resulting changes at velocity ($v = 1.5 \text{ m/s}$) and shading ($\sigma = 4 \text{ dB}$) was verified. This tracking represents the black validation curve, which changes with the CSI while remaining stable despite these abrupt changes during training through the dropout layers in the flexible model. Figure 10 also shows how these layers filter random noise without storing it. The RMSE in this training reached 5.30, and with this result, our model correctly predicts the direction of the mean signal. The training time was a short 26 s.

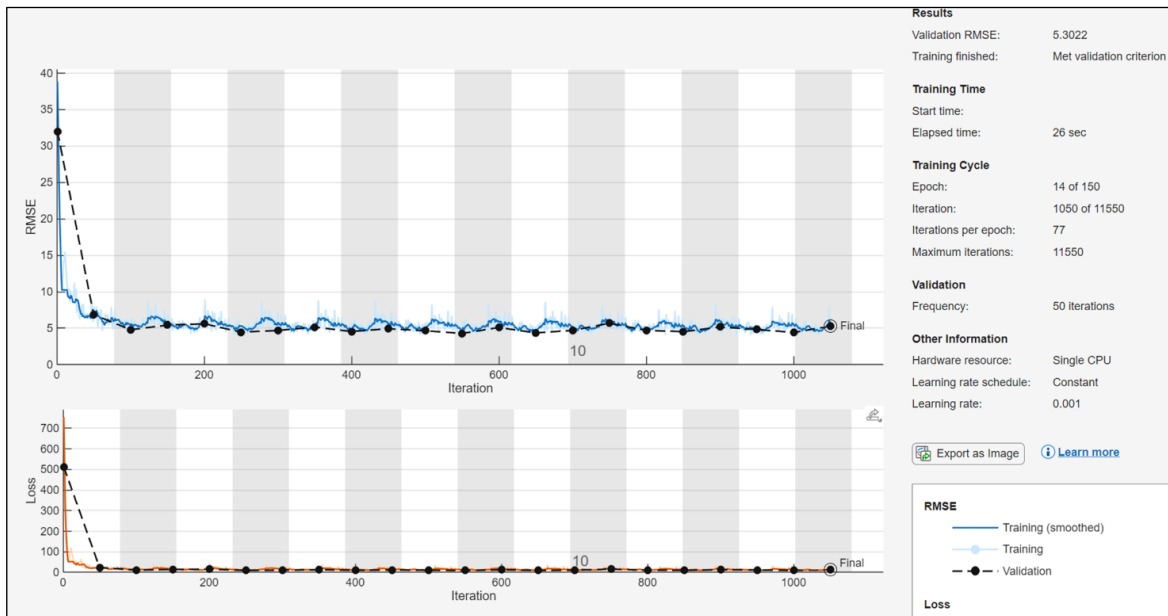


Figure 10: Training of the proposed Robust-DNN in a mobility scenario.
Source: Authors, (2026).

Figure 11 reports the spread of average SINR values observed during the dynamic test with pedestrian motion and shadowing using equation (8). The blue curve represents the actual SINR (applied equations (4) & (5)), while the red curve corresponds to the values estimated by the robust DNN (applied equation (6)). The actual distribution range is 17–57 dB. This behavior is due to pedestrian movement and channel changes when using RIS. The values 25 to 45 dB represent the active range. A slight dispersion is observed at the edges due to the use of mmWave under shadowing and blocking conditions. The predicted SINR values exhibit peaks, showing that the proposed robust DNN tracks the overall channel quality trend using CSI and RIS configuration while reducing random fluctuations caused by attacks and rapid variations. Figure 11 also shows that adding RIS with a robust DNN offers a practical gain in average SINR using equation (3). In practice, higher red values correspond to a more stable average SINR, despite the fluctuations introduced by mobility and shadowing. This behavior also indicates stronger robustness against the considered attacks. As for the horizontal increase, it shows improved beamforming, the best RIS utilization, and enhanced channel quality for the legitimate user. While a decrease leads to the opposite effect.

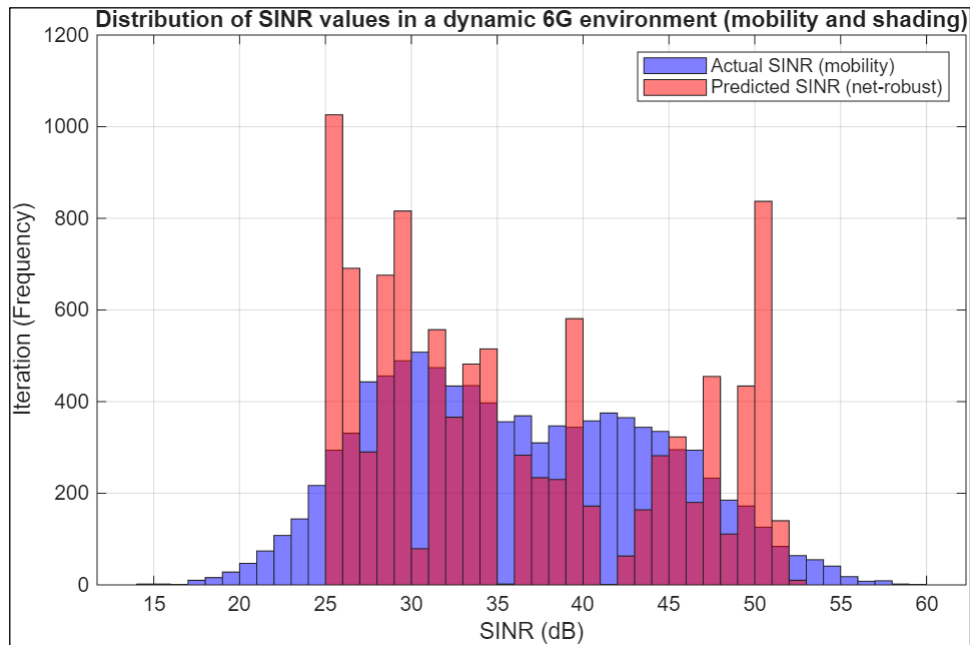


Figure 11: Comparison between actual SINR and the proposed Robust-DNN in mobility case.
Source: Authors, (2026).

IV. CONCLUSIONS AND FUTURE WORK

In this study, we evaluate beamforming with varying RIS sizes (50–1000) and the inclusion of DL to meet 6G design targets. This involved integrating path loss equations and reflection equations with security criteria and fortifying the model with algorithms, most notably Supervised DNN, Adam Optimization with Backpropagation, Dropout, and L2 Regularization. This change shifts the system from simple connectivity optimization to a defence-oriented design framework that improves resistance to practical attack scenarios. Average SINR gains were observed at $N = 1000$ using beamforming optimization without DL: 54.68% for jamming attacks, 54.35% for poisoning attacks, and 36.2% for spoofing attacks. The efficiency of the final model was confirmed in a user mobility scenario. This model was further enhanced by integrating RIS with a robust DNN to handle rapid changes in channel characteristics. It was designed to improve SINR and security performance for 6G networks across diverse scenarios. Our results also suggest the model's resilience with an average SINR (increase of 8–12 dB) when N increased from 50 to 600 elements in a simulated scenario involving pedestrian traffic and shading. One limitation of the current study is that higher user densities were not examined. The Doppler effect at high user speeds will be discussed, and the efficiency of connectivity for maintaining optimal performance in high-mobility scenarios will be evaluated.

V. AUTHOR'S CONTRIBUTION

Conceptualization: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Methodology: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd .

Investigation: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Discussion of results: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Writing – Original Draft: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Writing – Review and Editing: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Resources: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Supervision: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

Approval of the final text: Saad Ahmed Ayoob, Firas S. Alsharbaty, Zainab Salim Abd.

VI. REFERENCES

- [1] R. Priyadarshani, K.-H. Park, Y. Ata, and M.-S. Alouini, "Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview", IEEE Open Journal of the Communications Society, pp. 1–26, 2025, doi: 10.1109/OJCOMS.2025.3594284
- [2] Z. M. Ismail, and S. A. Ayoob, "Analyzing the Doppler Effect on Carrier Aggregation and Millimeter-Wave Performance in 5G Systems", Journal of Communications, vol. 20, no. 5, pp. 549 - 559, 2025.
- [3] D. Kundra, B. Vamalaatha, Y. Jadhav, L. M. Leo, S. Hota, M. P. Sunil, and T. Agarwal, "Adaptive Beamforming Techniques for mmWave and THz Communications in 6G", International Journal of Engineering, Science and Information Technology, vol. 5, no. 1, pp. 591–594, 2025.
- [4] Y. Sasaki, K. Arai, J. Nakazato, and K. Maruta, "Receiver Maximum Eigenmode Beamforming-Based Null-Space Expansion for Multi-User Massive MIMO in Time-Varying Channel", IEEE Transactions on Vehicular Technology, vol. 74, no. 6, pp. 9269–9283, 2025, doi: 10.1109/TVT.2025.3539399
- [5] Z. M. Ismail, and S. A. ayoob, "Enhancing 5G Network Capacity Through Integrated mmWave and Carrier Aggregation Technologies", Communications in Computer and Information Science, Book Series, ISBN 978-303215447-7, Vol. 2798 CCIS, 2026, doi: 10.1007/978-3-032-15448-4_5

- [6] C. Chen, Y. Huang, and H. Zhang, "Beamforming for Millimeter-Wave and Terahertz Communications: A Machine Learning Approach", *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2171–2207, 2021.
- [7] B. J. Qeryaqos and S. A. Ayoob, "Proposed Multiple Reconfigurable Intelligent Surfaces to Mitigate the Inter-User-Interference Problem in NLOS", *Journal of Communications Software and Systems*, vol. 20, no. 3, pp. 245–252, 2024, doi: 10.24138/jcomss-2024-0039
- [8] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies", *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.
- [9] M. Iqbal, T. Ashraf, M. Zubair *et al.*, "A Comprehensive Survey on Reconfigurable Intelligent Surfaces (RIS) and STAR-RIS for Next-Generation Wireless Networks", *Discover Applied Sciences*, vol. 7, p. 1253, 2025, doi: 10.1007/s42452-025-07684-w
- [10] Y. Zhang, Y. Yang, R. Jäntti, Z. Yan, D. Niyato, and Z. Han, "AmbShield: Enhancing Physical Layer Security with Ambient Backscatter Devices against Eavesdroppers", *arXiv preprint*, 2026, doi: 10.48550/arXiv.2601.09867
- [11] H. So and H. Soya, "Evaluation of Shadowing Effect on Channel Observation for Spectrum Sharing Access", *IEICE Communications Express*, vol. 13, no. 9, pp. 379–383, Sep. 2024, doi: 10.23919/comex.2024XBL0106
- [12] S. Shaber, B. S. Krishna, D. A. N. Rao, V. M. Sai, and A. Ganesh, "LoMar: A Secure Federated Learning Approach Against Model Poisoning Attacks", *International Journal on Advanced Computer Engineering and Communication Technology*, vol. 14, no. 1, pp. 103–113, 2025.
- [13] S. R. Ansari, J. Ajani, M. R. Hussain, S. N. Hassan, and M. A. A. Ansari, "Optimizing Network Performance by Exploration of Resource Management Strategies and Challenges in IoT-Based 6G Networks", 2022, doi: 10.13140/RG.2.2.33576.23043
- [14] S. A. Syed, "The Quantum Threat: Preparing for the Impending Impact on Cyber Security", *International Journal of Engineering Technology Research & Management*, vol. 7, no. 3, pp. 167–177, 2023, doi: 10.5281/zenodo.15128515
- [15] H. A. Alsawaf and S. A. Ayoob, "Optimized Wideband Beamforming for mm-wave Communication Systems with Intelligent Reflecting Surfaces", *Journal of Communications Software and Systems*, vol. 20, no. 4, pp. 350–360, 2024, doi: 10.24138/jcomss-2024-0090
- [16] C. Mayaki, "Optimizing Millimeter-Wave Beamforming Algorithms for 5G and Beyond Wireless Networks Using Machine Learning Enhanced Channel State Information", *International Research Journal of Modernization in Engineering Technology and Science*, vol. 7, no. 8, pp. 2887–2908, 2025, doi: 10.56726/IRJMETs82369
- [17] B. J. Qeryaqos and S. A. Ayoob, "Optimizing the Signal-to-Noise Ratio Using the Virtual Line of Sight and Choosing the Appropriate Dimensions", *International Journal of Electronics and Telecommunications*, vol. 70, no. 4, pp. 909–914, 2024, doi: 10.24425/ijet.2024.152077
- [18] S. Shaber, B. S. Krishna, D. A. Rao, V. M. Sai, and A. Ganesh, "A Secure Federated Learning Approach Against Model Poisoning Attacks", *International Journal on Advanced Computer Engineering and Communication Technology*, vol. 14, no. 1, pp. 103–113, 2025, doi: 10.65521/ijacect.v14i1.175
- [19] M. N. A. Siddiky, M. E. Rahman, M. S. Uzzal, and H. M. D. Kabir, "A Comprehensive Exploration of 6G Wireless Communication Technologies", *Computers*, vol. 14, no. 1, p. 15, 2025, doi: 10.3390/computers14010015
- [20] T. Ahmed *et al.*, "Enhancing Physical Layer Secrecy Performance for RIS-Assisted RF-FSO Mixed Wireless System", *IEEE Access*, vol. 11, pp. 127737–127753, 2023, doi: 10.1109/ACCESS.2023.3331593
- [21] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable Intelligent Surfaces for Energy Efficiency in Wireless Communication", *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019, doi: 10.1109/TWC.2019.2922609
- [22] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, "RIS-Aided Physical Layer Security Improvement in Underlay Cognitive Radio Networks", *IEEE Systems Journal*, vol. 17, no. 4, pp. 6437–6448, Dec. 2023, doi: 10.1109/JSYST.2023.3296012
- [23] H. Guo, Z. Yang, Y. Zou, B. Lyu, Y. Jiang, and L. Hanzo, "Joint Reconfigurable Intelligent Surface Location and Passive Beamforming Optimization for Maximizing the Secrecy Rate", *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2098–2110, Feb. 2023, doi: 10.1109/TVT.2022.3211608
- [24] J. Youn, W. Son, and B. C. Jung, "Physical-Layer Security Improvement with Reconfigurable Intelligent Surfaces for 6G Wireless Communication Systems", *Sensors*, vol. 21, no. 4, p. 1439, 2021, doi: 10.3390/s21041439
- [25] D. Do, A. Le, and S. Mumtaz, "Secure Performance Analysis of RIS-Aided Wireless Communication Systems", in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, 2021, pp. 1–6, doi: 10.1109/GLOBECOM46510.2021.9685201
- [26] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network", *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, Jan. 2020, doi: 10.1109/MCOM.001.1900107
- [27] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning", *Genetic Programming and Evolvable Machines*, vol. 19, pp. 305–307, 2018, doi: 10.1007/s10710-017-9314-z