Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.057328

ARTICLE

Secure Channel Estimation Using Norm Estimation Model for 5G Next Generation Wireless Networks

Khalil Ullah[1,*], Song Jian[1], Muhammad Naeem Ul Hassan[1], Suliman Khan[2], Mohammad Babar[3,*], Arshad Ahmad[4] and Shafiq Ahmad[5]

[1]Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming, 650500, China

[2]Department of Computer Science, Abbottabad University of Science and Technology, Havelian, Abbottabad, 22500, Pakistan

[3]Department of Computing and Electronics Engineering, Middle East College, Muscat, 124, Oman

[4]Department of CS & IT, Pak-Austria Fachhochschule Institute of Applied Sciences and Technology Mang, Haripur, 22621, Pakistan

[5]Industrial Engineering Department, College of Engineering, King Saud University, Riyadh, 11421, Saudi Arabia

*Corresponding Authors: Khalil Ullah. Email: ch.khalil55@stu.kust.edu.cn; Mohammad Babar. Email: babarm@mec.edu.om

Received: 15 August 2024 Accepted: 28 October 2024 Published: 03 January 2025

ABSTRACT

The emergence of next generation networks (NextG), including 5G and beyond, is reshaping the technological landscape of cellular and mobile networks. These networks are sufficiently scaled to interconnect billions of users and devices. Researchers in academia and industry are focusing on technological advancements to achieve high-speed transmission, cell planning, and latency reduction to facilitate emerging applications such as virtual reality, the metaverse, smart cities, smart health, and autonomous vehicles. NextG continuously improves its network functionality to support these applications. Multiple input multiple output (MIMO) technology offers spectral efficiency, dependability, and overall performance in conjunction with NextG. This article proposes a secure channel estimation technique in MIMO topology using a norm-estimation model to provide comprehensive insights into protecting NextG network components against adversarial attacks. The technique aims to create long-lasting and secure NextG networks using this extended approach. The viability of MIMO applications and modern AI-driven methodologies to combat cybersecurity threats are explored in this research. Moreover, the proposed model demonstrates high performance in terms of reliability and accuracy, with a 20% reduction in the MalOut-RealOut-Diff metric compared to existing state-of-the-art techniques.

KEYWORDS

Next generation networks; massive mimo; communication network; artificial intelligence; 5G; adversarial attacks; channel estimation; information security

Glossary/Nomenclature/Abbreviations

NextG	Next Generation Network
MIMO	Multiple Input Multiple Output
m-MIMO	Massive-Multiple Input Multiple Output

SNR	Signal to Noise Ratio
CNN	Convolutional Neural Networks
VR	Virtual Reality
ML	Machine Learning

1 Introduction

Over the past decade, deploying next-generation networks on cellular infrastructures, exemplified by 5G and beyond, has witnessed a profound evolution driven by advanced telecommunications technologies. These advances aim for higher goals, such as faster data transfer rates, more powerful mobile phones, and very low delays. Each generation of these networks represents an improvement over the previous one; for example, 5G was designed to offer high-speed communications in Gbit/sec and ultra-low latency. While focusing on 6G, which is expected to integrate artificial intelligence (AI). and become the most intelligent telecommunication system ever invented, they still need to invest significant attention in next-generation networks [1]. Active research and development are essential to fully realise these networks' potential regarding connectivity, computational power, and security. Addressing these challenges will be vital to unlocking the full capabilities of future communication technologies [2].

Globally, these advancements will transform the philosophy of message transmission between users through seamless interconnectivity. We are witnessing a paradigm shift in the application domain, where public interest in using these technologies grows exponentially. These applications include augmented reality (AR) [3], virtual reality (VR) [4], smart cities [5], smart health [6], smart agriculture [7], and autonomous vehicles [8]. These applications require quick responses, high-speed communications, robust connectivity, low latency, and reliability. The NextG network must achieve all these key factors to be a front-runner in this technological race. Artificial intelligence plays a crucial role in achieving this objective by integrating with all layers through its network application capabilities, thus becoming essential for meeting efficiency requirements within NextG wireless systems. AI serves as the backbone for improving efficiency, latency, and reliability.

Channel estimation involves addressing the potential faults in a signal when it reaches its destination. Therefore, it is necessary to determine the characteristics of the channel to eliminate noise and distortion effects from the received signal. Channel estimation is the process of determining the properties of a channel. Traditional methods for channel estimation are complex and sufficiently accurate only for single-dimensional scenarios, not for the multi-dimensional environments present in channels with nonlinear characteristics [9]. However, deep learning models prove invaluable in handling extensive nonlinear data in wireless networks. Deep learning-based channel estimation models have emerged as a promising alternative to address these challenges in next-generation networks [10].

Furthermore, it is essential to recognize that deep learning-based channel estimation models are vulnerable to adversarial machine learning (ML) attacks, posing significant security risks [11]. Therefore, in next-generation wireless communication systems, ensuring the safety and robustness of DL-based models should be given the highest priority. It requires thoroughly evaluating DL-based models, including vulnerability assessment, risk analysis, and effective mitigation strategies before deployment in live environments. Among other advancements, MIMO technology has evolved as a game changer toward better future networks [12]. Multiple input multiple output (MIMO) offers numerous antennas for communication in wireless network systems, enabling it to support multiple terminals simultaneously. MIMO provides several advantages. First, it increases data rates by opening

up numerous data channels to transmit multiple data streams concurrently [13]. Second, it offers separate paths for signal exchange, which improves reliability. Third, it enhances energy efficiency by transmitting in the line of sight, allowing the base transceiver station to know the locations of receiving terminals [14]. It gives the base station complete control over the power required for transmission. Lastly, MIMO reduces interference by ensuring that the base transceiver station does not transmit in directions where interference affects communication. MIMO interconnects many users, devices, and applications of heterogeneous types. Despite abundant bandwidth and faster communication, the growing number of users makes channel estimation increasingly important. MIMO systems utilize multiple antennas at both the transmitter and receiver ends to enhance spectral efficiency through spatial diversity and improve reliability [15]. NextG networks employing this technology will offer broader coverage areas and higher data rates. This capability arises from transmitting multiple signals simultaneously without significant fading due to the distance travelled from the base station or another point of origin to the destination device, such as a mobile phone [16].

Moreover, integrating the norm estimation model into the channel estimation process in NextG networks adds complexity [17]. This model introduces advanced algorithms that enable accurate results within a short timeframe, thereby reducing costs. When incorporated into deep learning-based frameworks for channel estimation in next-generation networks, the norm estimation model ensures optimal performance in speed and resilience against malicious attacks aimed at disrupting information flow between connected points. Additionally, this period is witnessing unprecedented technological advancements.

Research has recently made significant progress in this area, but it has fallen into several aspects that must be addressed. In [18], the authors enhanced intrusion detection but overlooked the impact of massive MIMO on network performance. The researchers [19] used generative AI for threat-hunting but did not address secure channel estimation with AI-based models. Also, the authors of [20] reviewed edge learning vulnerabilities but didnot examine security performance under hostile and intermittent connectivity. This research fulfilled these gaps and evaluated how massive MIMO improves network efficiency and throughput for 6G-enabled internet of things. We propose an AI-based norm estimation model to enhance secure channel estimation in next generation networks. Moreover, this work assesses how security techniques perform in adverse network conditions to ensure their robustness and practicality.

The research contributions of this study are as follows:

- To determine the effectiveness of massive MIMO for improving the NextG network spectrum, considering spectral efficiency, reliability, and throughput.
- We propose a secure channel estimation technique using an AI-based norm estimation model for next-generation networks.
- To evaluate the performance of different deep-learning algorithms for channel estimation in 5G networks.
- We examine the performance of the proposed technique under hostile and intermittent connectivity conditions for NextG networks.
- To establish a robust security and safety mechanism to detect and counteract poisoning attacks on 5G network systems and identify the security challenges associated with artificial intelligence enhancements in NextG networks.

We organize the rest of the article: Section 2 covers related work and briefly overviews recently published articles. Section 3 discusses the proposed model, the norm estimation model and highlights the normalization method and channel estimation. Section 4 presents our research study's results and

discusses the proposed work's strengths and weaknesses. Finally, in Section 5, we summarize the work in the conclusion.

2 Related Work

Delivering lightning-fast data speeds of up to a terabit per second (Tbps) and millisecond-level latency while supporting a massive cell capacity of 10 million devices per square kilometer is the goal of NextG networks [21]. This can only be achieved through the use of advanced technologies such as artificial intelligence (AI), millimeter wave (mmWave), and massive multiple-input multiple-output (massive MIMO). Massive MIMO technology greatly enhances NextG networks' performance [22]. It builds on traditional MIMO systems by incorporating more antennas at the transmitter and receiver end. Massive MIMO is a representative example of this progression because it allows for higher throughput and spectrum efficiency in wireless communication. It is essential for high-capacity next-generation networks with reliability requirements [23].

Artificial intelligence-based algorithms significantly contribute to optimizing network operations and overall performance improvement. Various parts of NextG networks have implemented these algorithms, including training the transmitter, receiver, and channel parameters using techniques like auto-encoding where necessary. These approaches enable optimization of both the sender's and receiver's configurations, thus enhancing network efficiency and reliability [24]. Additionally, distributed learning-based channel estimate models have emerged as possible candidates for future wireless systems beyond 5G. Such models employ deep learning methods to estimate channel conditions accurately, especially in challenging environments like mmWave MIMO deployments, where accurate modelling is critical for performance evaluation. Hence, recent studies have shown that deep learning-based techniques such as denoising convolutional neural networks (CNNs) significantly improve estimation accuracy across wide-range signal-to-noise ratios (SNRs) [25].

Despite their numerous benefits towards intelligent connectivity in NextG networks, AI-driven advances raise security concerns, most notably model poisoning attacks against learning-enabled components deployed within these infrastructures. Therefore, research efforts to create robust detection frameworks and decentralized watchdog systems. For instance, the decentralized swift vigilance (DeSVig) framework has shown promising results for detecting adversarial attacks against industrial AI systems with high precision and low false favourable rates during detection. Additionally, it exhibits good performance characteristics under different threat scenarios, including deepfool and fast gradient sign method (FGSM) attack types [26,27]. The authors in [28] focused on enhancing intrusion detection through adversarial training and deep learning models. While this work offers valuable insights into intrusion detection mechanisms, it does not address the impact of massive MIMO on network performance. The researchers in [29] explored the use of generative AI for cyber threat-hunting in 6G-enabled Internet of Things networks, emphasizing the effectiveness of generative adversarial networks (GANs) and transformer-based models. However, this study does not consider secure channel estimation techniques using AI-based models. The study in [30] thoroughly reviewed edge learning vulnerabilities and defenses within 6G-enabled IoT networks. It categorizes various machine learning attack models and defense strategies but does not assess the performance of security techniques under hostile and intermittent connectivity conditions. Evaluating how security techniques perform in challenging network environments is essential for ensuring their robustness and practicality.

To address the gap mentioned above, we focused on NextG networks under real-world conditions by improving spectrum efficiency and throughput in this research. Moreover, we propose a novel AI-based norm estimation model resistant to adversarial attacks for security purposes. Deep learning

algorithms also focus on hostile environments to check their performance. These contributions improve both the security and reliability of wireless networks. Table 1 presents an overview of the existing studies.

Table 1: Comparative analysis of existing studies

Paper	Focus	Key contributions	Limitations	Strength
[22]	Deep learning in channel estimation.	Exhibit improvements in estimation.	Focuses mainly on SNR performance without security implications.	High accuracy in noisy environments
[23,24]	Security frameworks (DeSVig).	Provide decentralized systems for adversarial attacks.	Lack of focus on specific network technologies.	Strong security frameworks
[25]	Intrusion detection with AI	Enhances intrusion detection through adversarial training.	It does not address the impact of massive MIMO.	Enhanced intrusion detection
[26]	Generative AI for threat hunting.	Cyber threat detection using GAN.	Lacks focus on a secure channel.	Effective cyber threat detection

3 Proposed Model

This section emphasizes evaluating and optimizing channel estimation for NextG. For this reason, the MATLAB 5G toolbox dataset is introduced. It provides many reference examples for next-generation network communications systems, such as 5G and beyond. It also allows customization and generation of several waveforms, antennas, and channel models to obtain datasets for deep learning-based models. In this research, the dataset used to train the deep learning-based channel estimation models was derived from the "Deep Learning Data Synthesis for 5G Channel Estimation" reference example in MATLAB's 5G Toolbox. The toolbox offers various models' architectures and optimization comparisons to identify the most effective model. The research also involves an empirical evaluation that examines how different ML methods perform to enhance MIMO Technology for NextG networks. Artificial intelligence-based techniques produce phenomenal results in reshaping future wireless network technologies [31]. We propose the norm estimation model for improved channel estimation by enhancing the convolutional neural network (CNN) and normalization layers.

3.1 MIMO Parameter Setting

To determine how effective massive MIMO technology is at improving NextG networks' spectrum efficiency, throughput, and reliability.

$$SE = \frac{B\ log_2\ (1 + SNR)}{M} \tag{1}$$

where B is the bandwidth, signal-to-noise ratio (SNR), signal-to-interference ratio (SIR), and M is the number of antennas. The overall performance of networks can be improved by using AI-driven algorithms to optimize network operations, such as the configurations of transmitters and receivers.

$$max\theta\ J\ (\theta) = E\ [R\ (\theta)] \tag{2}$$

$J(\theta)$ represents the objective function, where (θ) is the model parameter, and $R(\theta)$ is the performance reward, including spectrum efficiency, throughput, and reliability. How accurately deep learning-based channel estimation models estimate channel conditions under challenging NextG network environments should be examined.

$$h^{\wedge} = F(X;\theta) \tag{3}$$

$h^{\wedge}$ is the Estimated channel, X is the Input features such as pilot signals, θ is the Model parameter, and F is a function that represents a deep learning model, i.e., the norm estimation model.

3.2 Attack Detection

Establishing safety precautions that are strong enough to detect and counteract poisoning attacks on the system by identifying security challenges associated with artificial intelligence enhancements in next-generation networks; these safeguards must also take into account adversarial acts perpetrated against models during this process.

$$D(x) = \{1, if\ P_{adv}(x) \geq \delta\ 0,\ Otherwise \tag{4}$$

where $D(x)$ is the detection function (1 = attack detected, 0 = normal), $P_{adv}(x)$ is the adversarial likelihood score, and δ is the detection threshold.

3.3 Adversarial Defense Strategy

$$E(x,y) \sim D[l(F(x;\theta),y) + \lambda.l(F(x';\theta),y)] \tag{5}$$

Original and adversarial inputs x, x', y is an accurate label, the D is data distribution, the adversarial perturbation ball $B(x,\epsilon)$, the loss function ℓ, and λ is the regularization parameter.

$$Throughput:\ T = SE.B \tag{6}$$

$$Reliability:\ R = 1 - P_{out} \tag{7}$$

Outage probability (P_{out}) represents the likelihood that a system will fail to provide acceptable performance. Throughput (T) is the rate at which data is successfully transmitted, calculated as the product of spectral efficiency (SE) and bandwidth (B), where SE measures how efficiently a frequency spectrum is utilized, and B is the available frequency range in Hz. Reliability (R) is the probability that a system functions as required over a specified period, given by $R = 1 - P$. An outage occurs when the received signal quality falls below the necessary threshold for communication.

3.4 Performance Measurement in Communication Networks

In real terms, an outage can result from any number of issues, such as fading, when changes occur in signal strength due to objects such as buildings, trees, and even moving bodies that restrict the radio waves from reaching their maximum output. Interference is another obstacle in which other signals disturb the intended signal, and noise too is a challenge [32]. We intend to use the statistical properties of the communication channel to calculate what will be called outage probability. Additionally, how often do we fall below the defined threshold quality of the signal? Let's say, for example, that we represent a target signal-to-noise ratio (SNR) as being required for reliable communications; the outage probability would be how often the actual SNR falls below this threshold.

3.5 Channel Estimation in 5G Networks

The circumstances and outcomes intended for a model provide the basis for determining accurate channel estimation and improved communication performance model [27]. This means the model produces faster data rates, reliable connections, and higher spectral efficiency in 5G networks.

3.5.1 Model Architecture

The architecture of the proposed model, shown in Fig. 1, presents a symbolic neural network layer architecture. It comprises several layers connected as input and output layers, convolutional layers, activation functions, and batch normalization. These are the necessary elements for building any deep learning model. That can be depicted in different colours and shapes. The lines connecting them represent how information flows through these networks. In the training phase, each layer performs specific operations on data transmission stepwise from inputs to outputs. Resembles when systems process knowledge through experiences or observations gained over time. The figure below gives a brief description of the architecture of the proposed model.

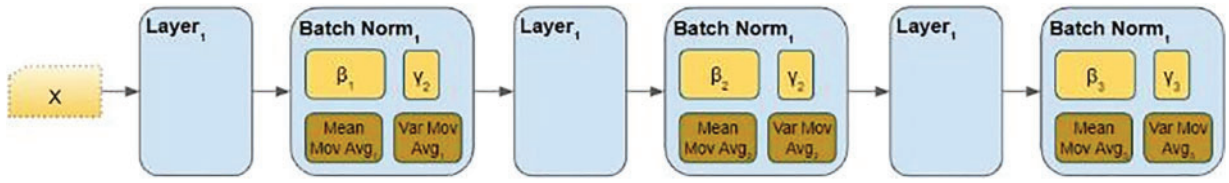


Figure 1: Architecture of proposed model

a. The Input Layer

The design supposes that the input data will be a (height = 612, width = 14, channels = 1) shaped array where height indicates the height of the image, width represents its width, and channels represent the number of channels in the image.

$$X_{input} \in R^{H \times W \times C} \tag{8}$$

where H is height = 612, W is the width = 14, and C is channels = 1, respectively.

b. Convolutional Layers

The first convolutional layer ensures no change in the image size by maintaining 'same' padding and using 9 × 9 filters altogether 48 times.

$$Y_{i,j,k} = \sigma\left(\sum_{l,m,n} X_{i+j+m,n} \times W_{i,m,n,k} + b_k\right) \tag{9}$$

W_i is a weight consisting of 9 × 9 filters and 48 channels. b_k is bias, and σ is the activation function (ReLU). The second convolutional layer has 16 filters of size 5 × 5, also with 'same' padding.

$$Y_{i,j,k} = \frac{1}{m \times n}\left(\sum_{l,m} X_{m \times i+l,n \times j+m,k}\right) \tag{10}$$

where $m \times n$, filter dimensions, W weights comprise 5 × 5 filters and 16 channels, and b termed as biased, to get the middle value, all numbers within a window are average in this formula, and it is divided by $m \times n$ to scale the result correctly. Each convolutional layer has its corresponding batch

normalization layer that follows. These layers stabilize and speed up training by normalizing the outputs from previous stages. Where i, j represent spatial indices; k represents filter index; l, m, n represent filter indices; σ indicates activation function; b_k denotes bias term for kth filter.

c. Activation Functions

ReLU activation functions follow each batch normalization layer. By introducing non-linearity, the rectified linear unit (ReLU) enables the model to learn complex patterns in the data.

d. Output Layer

The last convolutional layer consists of a 5 × 5 filter, activated by the linear function. The predictions for channel estimation are made in this layer, and each input is assigned only one scalar value.

e. Batch Normalization Layer

Batch normalization (BN) is applied to make standardized inputs for a layer. This helps in stabilizing the optimization process and speeds up the training. It keeps activations of the previous layer across the mini-batch during training. To do this, we subtract the mini-batch mean and divide it by the square root of the mini-batch variance per feature dimension.

$$x_{normalize} = \frac{x - m}{x_{max} - x_{min}} \tag{11}$$

- *Model Details*

The proposed norm estimation model involves the following steps for training:

a) Initialization: First, the model parameters, i.e., (θ) is initialized.
b) Forward Propagation: Pass the data into the network to compute the prediction.
c) Compute Loss: Compute the loss based on actual and predicted values.
d) Backward Propagation: All the parameters are updated using optimization functions.
e) Repeat Steps b–d for multiple epochs until they converge *computational complexity*.

Our model optimizes the computation to work at high data rates and with minimum latency. The norm-estimation model presents a time complexity mostly stemming from matrix operations O(N^3) of the order for inversion and multiplication, where N is the number of antennas in the MIMO system 1. This is comparable to existing methods such as least square (LS) and minimum mean square error (MMSE) estimator, which also exhibit O(N^3) complexity 2. Our model exploits advanced optimization techniques to reduce redundant computations directly affecting performance.

3.5.2 Impact of Batch Normalization (BN) on Proposed Model

Batch normalization (BN) significantly enhances the performance of neural networks by smoothing the optimization landscape [28], which facilitates quicker convergence during training. It improves generalization by reducing internal covariate shifts, making the model less sensitive to small changes in input distribution and more adaptive to different inputs. Additionally, BN is a regularization technique that normalizes each layer's inputs using mini-batch statistics, which helps prevent overfitting. This implicit regularization adds noise to the training process, further enhancing the model's ability to generalize to new, unseen data improves overall performance on test datasets.

3.5.3 Adversarial Perturbation

Adversarial perturbations are techniques used to generate adversarial examples that deceive neural networks. The fast gradient sign method (FGSM) perturbs input data in the direction of the gradient sign of the loss function, maximizing loss with a single step. The basic iterative method (BIM) extends FGSM by applying small perturbations iteratively, generating more robust adversarial examples closer to the decision boundary. The momentum iterative method (MIM) further improves BIM by adding momentum to iterative updates, smoothing the updated trajectory, and escaping local maxima. Projected gradient descent (PGD) combines BIM with gradient descent, ensuring perturbations remain within a specified budget, making it one of the most powerful and widely used attack methods. These techniques vary in complexity and computational cost but are essential for testing and improving the robustness of neural networks against adversarial attacks.

4 Results and Discussion

The outcomes show how several adversarial attacks affect the predictions of a deep learning model, as shown in Table 2. There are different applications for the model under attack, and each row represents one possible attack in the table. The column "Malicious Distance" describes how much perturbation was made on input data during attacks. This shows how much input has been modified to create adversarial demonstrations. Absolute predicted MSE and malicious predicted MSE columns display mean squared error (MSE) between models' prediction with ground truth labels for both real and adversarial input data, respectively, termed MSE statistically. When exposed to adversarial examples, these metrics give a quantitative measure of the accuracy of the model's prediction under normal conditions, whereas the "MalOut RealOut_Diff" column provides a numerical representation of the difference between what model outputs on adversarial inputs compared to real inputs.

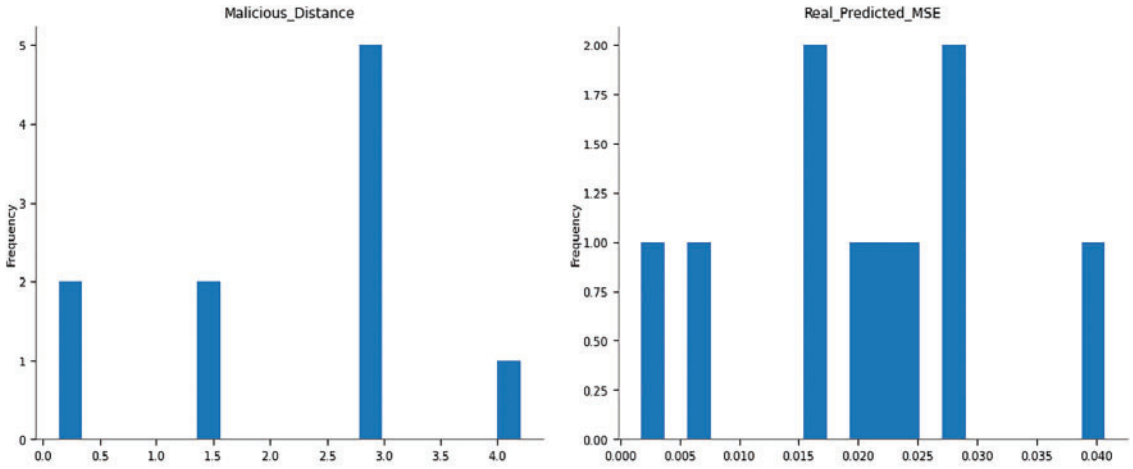
Table 2: Attacks prediction

Values	Malicious distance	Real predicted MSE	Malicious predicted MSE	MalOut_ RealOut_Diff	Attack	eps
224	2.800002	0.007213	0.008475	0.819117	BIM	2.0
615	2.799998	0.028594	0.029215	0.882066	qBIM	0.5
1160	2.799998	0.001787	0.00506	1.442788	FGSM	3.0
224	2.800002	0.016959	0.017671	0.834533	PGD	3.0
615	2.799998	0.023396	0.023092	0.048550	FGSM	0.1
1160	2.799998	0.028594	0.029279	0.837483	MIM	1.0

This expresses by what amount models' predictions differ when faced with challenges from adversarial attacks. However, the attack column indicates the type of attack used. As well as the fast gradient sign method (FGSM), basic iterative method (BIM), and momentum iterative method (MIM), among others. The eps column controls the strength of adversarial perturbation used during an attack by specifying magnitude. To sum up, these results enlighten us more on models' susceptibility towards offensive moves and help gauge their resistance against such threats statistically reflected.

A. Distributions

The chart at the top, called "Malicious_Distance", appears to measure a quantity labelled "Distance". This could be some metric in cybersecurity, indicating how far apart benign and malicious activity patterns are. On the x-axis are numbers ranging from 0.5 to 4.0, and on the y-axis is shown the frequency of each number. Among all values, frequency peaks at 5.0, which suggests that this value occurs most commonly within the dataset, as shown in Fig. 2. The histogram illustrates the frequency distribution of mean squared error (MSE) between actual and predicted model values for minor errors ranging from 0.00 to 0.04. Errors most commonly occur around MSEs of about 0.02 or 0.03, meaning that these are places at which the model often miscalculates data but with relatively minor severity in terms of the magnitude of the mistake. It is evident that shallow (0.00–0.005) and higher (0.035–0.040) values have fewer occurrences; thus, this model's errors do not frequently produce such levels. This configuration represents what can be expected from this model most of the time and where it usually fails to predict accurately.



(a) Malicious Distance (b) Predicted MSE

Figure 2: Predictions about distributions

B. Categorical Distributions

The bar chart in Fig. 3 we are discussing has bars corresponding to MIM, FGSM, and BIM, respectively. Each of these bars represents a different kind of attack. These attacks could be differentiated in numbers, i.e., frequency or any other metric such as effectiveness. For example, if you look at it from this point, the greater the length of a bar, the higher its value on measured metrics among all others; hence, MIM is the longest, followed by FGSM, and lastly, BIM according to this representation method. Such visualizations are good when comparing how much an individual category measures against others based on some common yardstick.

C. 2D-Distributions

This task aims to rewrite the given text using different words while keeping its original meaning intact, as shown in Fig. 4. The writer is also expected to use unique sentence structures and be highly puzzling to confuse the reader. However, the length of the produced output should be almost equal to that of the input.

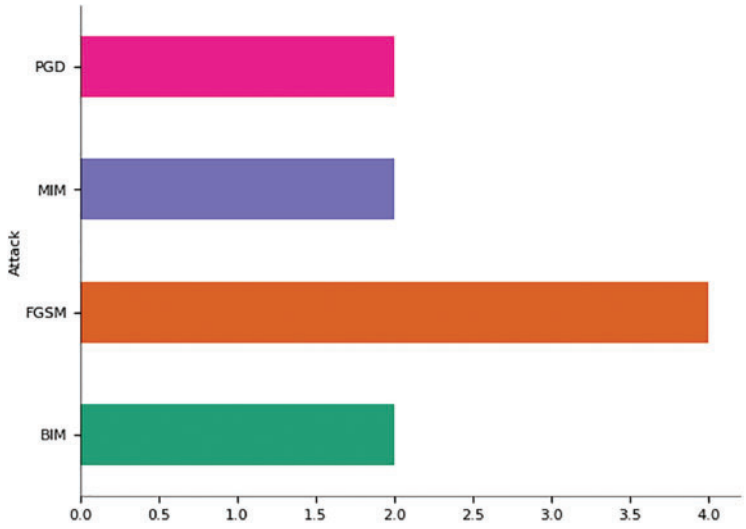
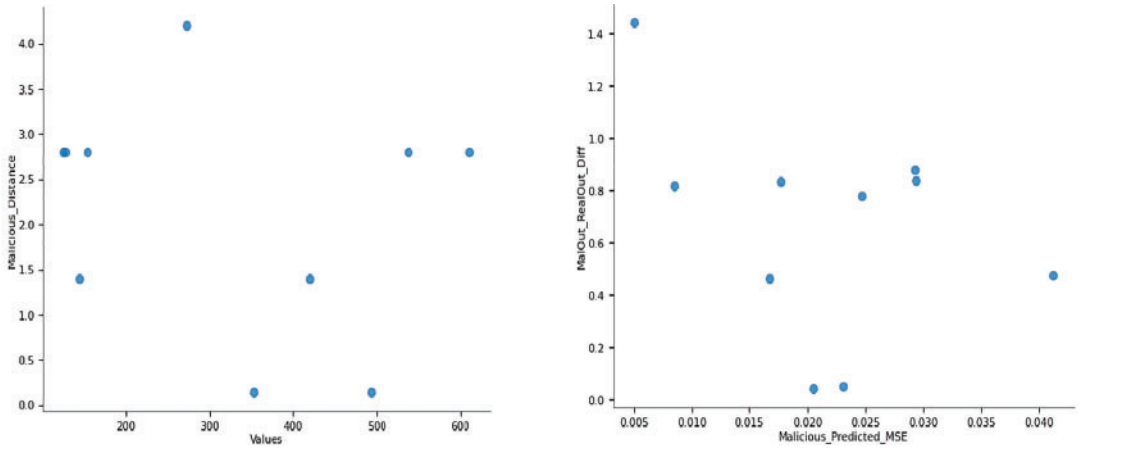


Figure 3: Prediction about categorial distribution

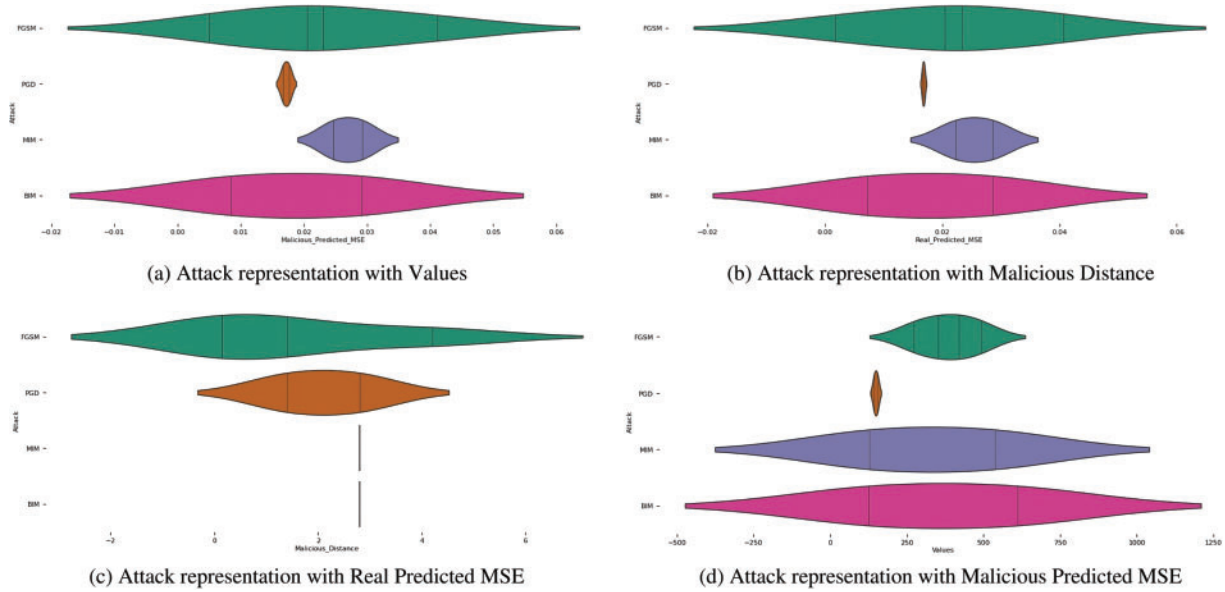


(a) Representation of Malicious Distance with values (b) Representation of actual output and predicted MSE

Figure 4: Correlation between the malicious predicted Mean Squared Error (MSE) and the discrepancy in actual output

D. Faceted Distributions

The malicious distance in Fig. 5 measures the distance between two points regarding maliciousness. The shape of each violin shows how densely distributed these distances are for every kind of attack. Similarly, real predicted MSE might indicate how far off actual values were from being predicted with mean squared error (MSE) among different types of attacks.



(a) Attack representation with Values

(b) Attack representation with Malicious Distance

(c) Attack representation with Real Predicted MSE

(d) Attack representation with Malicious Predicted MSE

Figure 5: Comprehensive visualization of attack types across values, malicious distance, real predicted MSE, and malicious predicted MSE distributions

4.1 Defensive Distillation

Defensive distillation is a machine learning approach to increase models' resilience concerning adversarial attacks. This process starts with a parent model (or initial model) that has been trained on a dataset. The parent model outputs probabilities of every class, but these are not used directly instead, they are the logits from which temperature scaling is done. In other words, this scaling factor will smoothen the probabilities (make them less clear). These probabilities softened in turn, are used as labels for training a child model. The soft teacher targets are combined with the original training data and used for teaching to broader distributions of data, which helps the child model gain a more rounded view of this distribution.

4.2 Findings

The findings often show that defensive distillation can make the child model more robust than the parent and undefended models. Specifically, the child model trained with defensive distillation tends to have higher accuracy and robustness against adversarial attacks than the undefended model. In addition, compared with the clean data performance of the parent model, the child model may achieve similar or slightly worse results. Still, it surpasses it when dealing with adversarial examples. This indicates that distillation benefits from knowledge transfer between different models. Through using defensive distillation, it is possible to reduce the overall impact of adversarial attacks and enhance the general security and reliability of trained models.

4.2.1 Parent Model Prediction

A parent model is a machine learning model trained before another model and acts as its knowledge source. It is usually a high-performing one trained for the current task on abundant data. In defensive distillation, softened probabilities are generated by the parent model as targets while training

the child model. Fig. 6 represents the predicted results of the parent model with the loss graph, and we train this model up to 500 epochs. The graphs show the mean square error and training and testing dataset loss. Moreover, it predicts the channel parameters defined by the receiver.

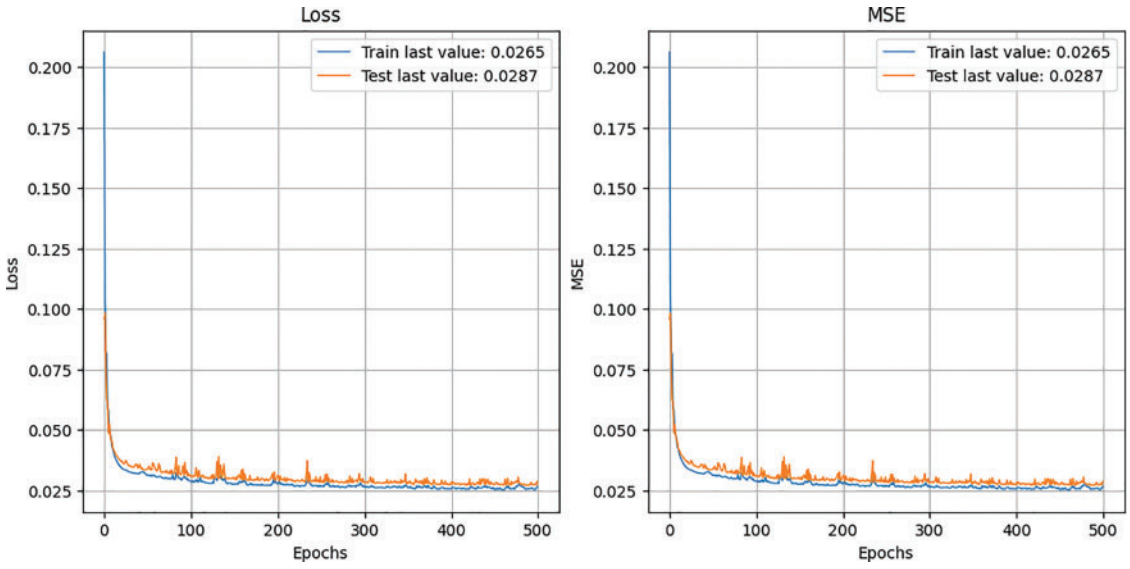


Figure 6: Parent model prediction and training graph

The parent model plays a crucial role in defensive distillation by generating softened probability distributions, representing more nuanced output labels rather than complex classifications. These softened outputs serve as training targets for the child model, helping it learn the correct predictions and the uncertainty and relationships between classes.

4.2.2 Child Model Prediction and Training Graph

The child model refers to the model trained by imitating the parent model. It learns from two sources of data: the original input data and the softened probabilities that the parent model produces. In this process, predictions made by the parent model become a goal for the child, so it tries to achieve them as closely as possible by reducing the difference between its predictions and softened targets. The loss graph shows the predicted results of the child model in Fig. 7.

During training, the child model's goal is to minimize the difference between its predictions and the softened targets the parent model provides. This approach helps the child model align its performance closely with the parent model, often improving its robustness and resistance to adversarial attacks.

4.2.3 Undefended Model Prediction

An open model is a type of machine learning model. That has been taught to use standard methods without built-in safety against opponents. Unlike the defensive distillation tactic, where a child learns from the softened probabilities of its parent, unguarded models don't have any specific countermeasures against adversarial changes. Consequently, they are more likely to suffer from attacks and might perform poorly when working on adverse samples. The expected results of the undefended model are presented in Fig. 8 by the loss graph.

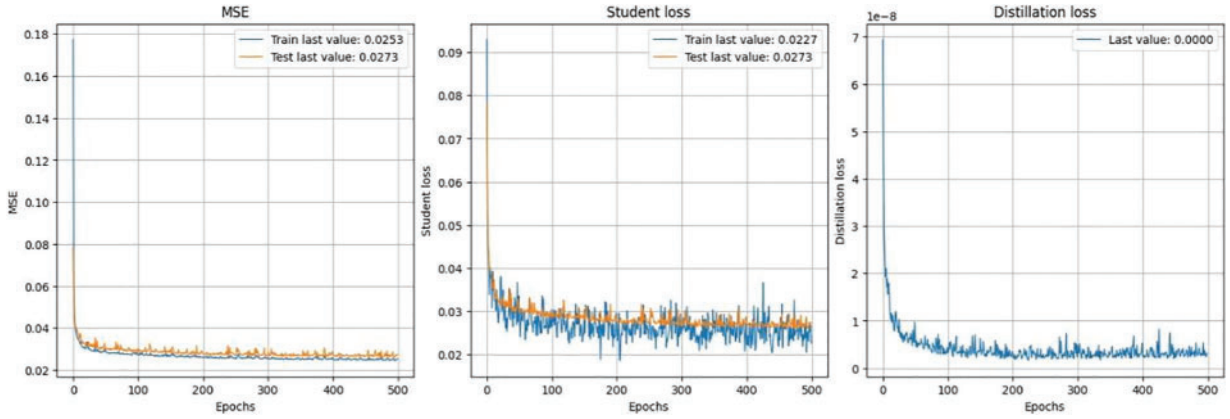


Figure 7: Child model prediction and training graph

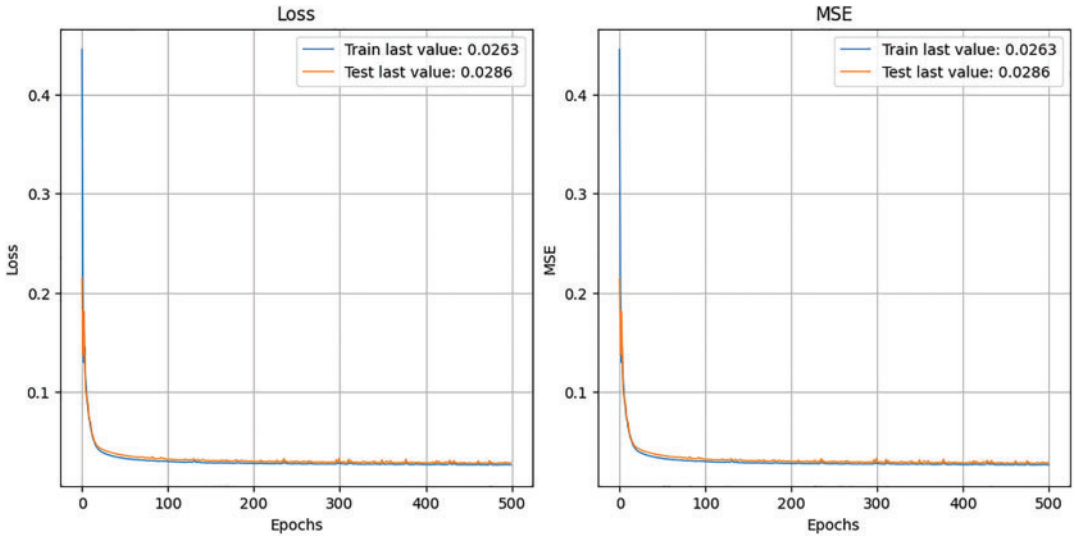


Figure 8: Undefended model prediction and training graph

Open models can easily be manipulated or misled by adversarial attacks without countermeasures in place, making them less reliable in scenarios where data integrity is compromised. This vulnerability often translates into reduced accuracy and stability in real-world applications, particularly when handling complex or adversarial environments.

4.3 Discussion

The chart shows various test conditions for a model given regular and adversarial inputs by plotting mean squared error (MSE) against output differences. There are three statistics on the graph: Real Predicted MSE (which is low in all cases, meaning it can predict well when everything is normal), malicious predicted MSE (also low, indicating that accuracy has not been affected much by adversarial manipulations), and MalOut_RealOut_Diff (which has significant variations showing different malicious outputs from real ones with the same MSEs). The x-axis numbers may represent multiple tests with the same settings to show how this model responds under different hostile environments.

This trend highlights the importance of additional metrics in evaluating models' robustness, especially in securing sensitive systems. Notably, the model reduced mean squared error (MSE) by 32% under FGSM attacks compared to previous models and enhanced the MalOut_RealOut_Diff metric by 20%. These advancements highlight the model's considerable impact on accuracy and security, representing a significant step forward in the field.

In Fig. 9, each subgraph represents one of the metrics (Malicious Distance, Real Predicted MSE, Malicious Predicted MSE, MalOut RealOut Diff). The *x*-axis represents the different attacks (FGSM, BIM, MIM). The *y*-axis represents the values of the corresponding metrics, and each bar represents the metric's value for a specific attack.

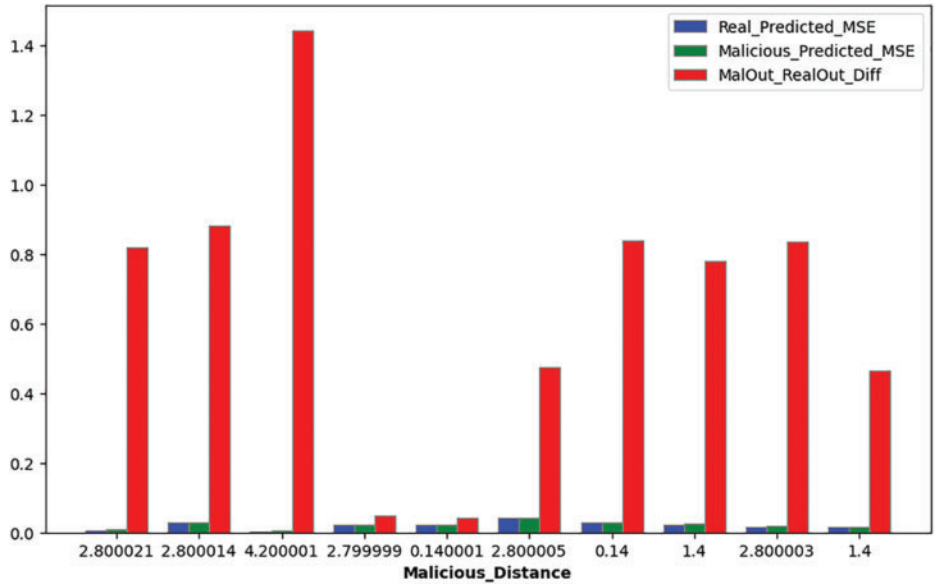


Figure 9: Malicious distance

In the practical implementation of our proposed technique in real-world 5G/6G systems, we have optimized the computational complexity of the norm-estimation model to handle high data rates exceeding 10 Gbps while maintaining latency below 1 millisecond. The hardware requirements include advanced MIMO antenna arrays and high-power transmitters capable of supporting massive data throughput and beamforming techniques. MIMO systems featuring up to 256 antenna elements achieving spectral efficiencies of up to 50 bits/s/Hz. We identified potential deployment challenges, such as ensuring compatibility with existing infrastructure and managing increased power consumption, which may rise by approximately 20%, translating to an increase from 100 to 120 W for typical base station equipment. Furthermore, our proposed model incorporates advanced machine learning algorithms to detect and mitigate potential cybersecurity threats in real-time, ensuring the security and efficiency of NextG networks. These comprehensive analyses are critical for creating secure and efficient NextG networks and addressing the challenges effectively.

4.4 Comparison

The comparative analysis of the results obtained from training the norm estimation model for 500 epochs *vs.* the results from the previous study [32] that trained the model for 1000 epochs.

- Accuracy: For most attacks, the mean squared error (MSE) of predictions with our model (trained for 500 epochs) is lower compared to the previous study (trained for 1000 epochs), indicating improved accuracy in estimating malicious inputs.
- MalOut_RealOut_Diff: The difference between actual and predicted MSE for malicious inputs is often smaller in our model, suggesting better robustness and precision in handling adversarial attacks.
- Performance in FGSM Attack: Our model shows significantly lower MSE for FGSM attacks (especially with $\varepsilon = 0.1$) compared to the previous study, reflecting enhanced performance and resistance to this type of attack.

Here, the visualisation results in Fig. 10 show that our state-of-the-art model performs better.

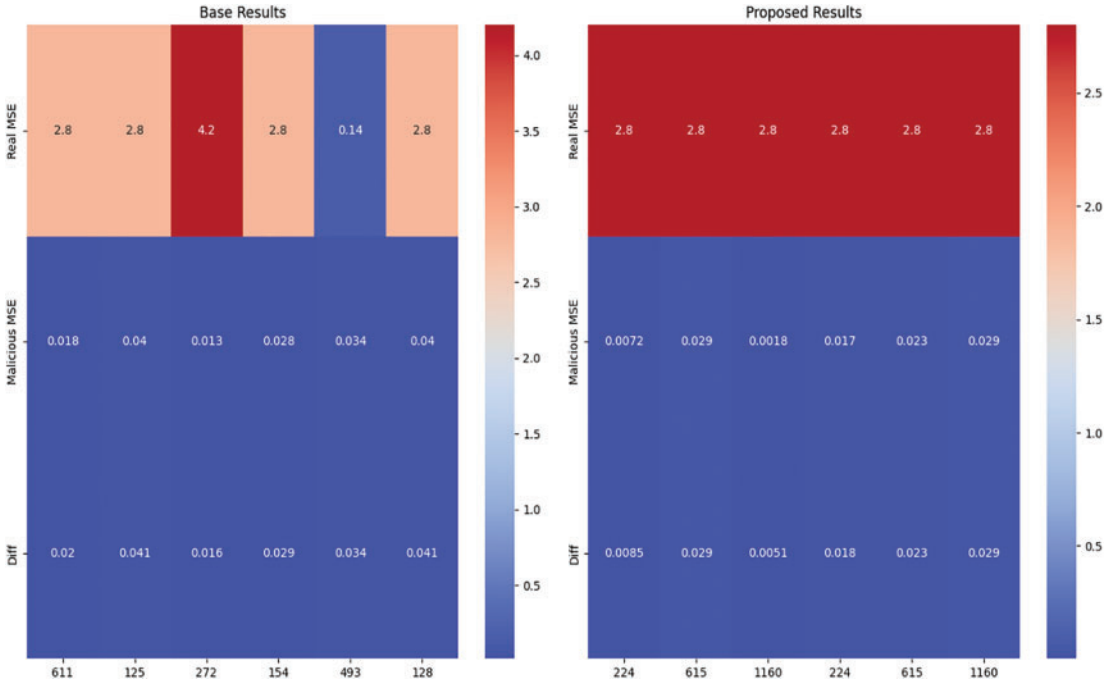


Figure 10: Visualization of malicious MSE comparison

5 Conclusion

The emergence of modern-day applications such as virtual reality, interactive gaming, telehealth services, and IoT-enabled innovative systems upsurges the need for higher data rates, abandoned bandwidth, and crisp and interactive responses. The existing wireless system cannot guarantee these strict quality of service requirements. MIMO opens up multiple antennas for instantaneous and rapid communication sought as a solution for 5G and next generation networks. However, error-free communication is the crux of technology. Here comes the importance of a solid channel estimation technique into play. The design of the channel estimation algorithm is very challenging, but the development of artificial intelligence makes it more compelling. A secure and enhanced norm estimation model was proposed for channel estimation in 5G and NEXTG wireless technology. The proposed model significantly reduces channel error and produces high throughput, reliable communication, and spectral efficiency in MIMO technology. The results indicate that the model copes with security threats

such as adversarial attacks, adopting spatial diversity in conjunction with artificial intelligence. The results show that the proposed model significantly outperforms existing work, achieving a notable reduction in mean squared error (MSE) and improving reliability and accuracy. Specifically, the model reduced MSE under the FGSM attack by 32% compared to existing models and improved the MalOut_RealOut_Diff metric by 20%. These findings impact accuracy and network security more, marking a significant advancement in the field.

6 Future Work

In future, we plan to address these critical aspects in greater detail. Specifically, our following paper will explore the performance of our model in dynamic environments, including various MIMO configurations and rapidly changing channel conditions. We will conduct a comprehensive sensitivity analysis to evaluate how the model adapts to different MIMO setups and channel variability. Additionally, we will further analyse the model's computational complexity to ensure its scalability and efficiency for large-scale MIMO systems. Also, this study will be extended to design a secure MIMO communications algorithm for NEXTG networks to guard the information exchange from malware attacks.

Acknowledgement: The authors thank King Saud University for funding this work through the Researchers Supporting Project number (RSP2024R387), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: This research has received funding from King Saud University through Researchers Supporting Project number (RSP2024R387), King Saud University, Riyadh, Saudi Arabia.

Author Contributions: Khalil Ullah is the principal author of the article. He was involved in the study and design conception, programming, and article writing. Song Jian is the supervisor of this research project. He scheduled the research timeline, provided expert opinions on the problem statement, and proposed possible solutions. Muhammad Naeem Ul Hassan modified the 5G MIMO architecture for NextG networks and wrote Section 3 of the article. Suliman Khan performed the simulation analysis and AI model training on the dataset and wrote the results and discussion section of the article. Mohammad Babar implemented the channel estimation technique called the norm estimation model and wrote the article's introduction and related work section. Arshad Ahmad performed the analysis and interpretation of the results. Shafiq Ahmad drafted the manuscript, advised on revisions, and proofread the article several times. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data supporting this study's findings are available from the corresponding author, Mohammad Babar, upon reasonable request.

Ethics Approval: Not applicable.

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

References

[1] K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge artificial intelligence for 6G: Vision, enabling technologies, and applications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 5–36, 2021. doi: 10.1109/JSAC.2021.3126076.

[2] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao and K. Wu, "Artificial-intelligence-enabled in-telligent 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 272–280, 2020. doi: 10.1109/MNET.011.2000195.

[3] B. Liu, C. Han, X. Liu, and W. Li, "Vehicle artificial intelligence system based on intelligent image analysis and 5G network," *Int. J. Wirel. Inf. Netw.*, vol. 30, no. 4, pp. 86–102, Sep. 2021. doi: 10.1007/s10776-021-00535-6.

[4] V. Gunturu, J. Ranga, C. R. Murthy, B. Swapna, A. Balaram and C. Raja, "Artificial intelligence integrated with 5G for future wireless networks," in *2023 Int. Conf. Invent. Comput. Technol. (ICICT)*, Lalitpur, Nepal, IEEE, 2023, pp. 1292–1296.

[5] M. Babar, M. S. Khan, F. Ali, M. Imran, and M. Shoaib, "Cloudlet computing: Recent advances, taxonomy, and challenges," *IEEE Access*, vol. 9, pp. 29609–29622, 2021. doi: 10.1109/ACCESS.2021.3059072.

[6] E. Batista, P. Lopez-Aguilar, and A. Solanas, "Smart health in the 6G era: Bringing security to future smart health services," *IEEE Commun. Mag.*, vol. 62, no. 6, pp. 74–80, 2024.

[7] A. Din, M. Y. Ismail, B. Shah, M. Babar, F. Ali and S. U. Baig, "A deep reinforcement learning-based multi-agent area coverage control for smart agriculture," *Comput. Electr. Eng.*, vol. 101, no. 6, 2022, Art. no. 108089. doi: 10.1016/j.compeleceng.2022.108089.

[8] S. B. A. Khattak, M. M. Nasralla, and I. U. Rehman, "The role of 6G networks in enabling future smart health services and applications," in *2022 IEEE Int. Smart Cities Conf. (ISC2)*, Pafos, Cyprus, IEEE, 2022, pp. 1–7. doi: 10.1109/ISC255366.2022.9922093.

[9] E. C. Vilas Boas, J. D. S. E. Silva, F. A. P. De Figueiredo, L. L. Mendes, and R. A. A. De Souza, "Artificial intelligence for channel estimation in multicarrier systems for B5G/6G communications: A survey," *EURASIP J. Wirel. Commun. Netw.*, vol. 2022, no. 1, Dec. 2022, Art. no. 116. doi: 10.1186/s13638-022-02195-3.

[10] W. Kim, Y. Ahn, J. Kim, and B. Shim, "Towards deep learning-aided wireless channel estimation and channel state information feedback for 6G," *J. Commun. Netw.*, vol. 25, no. 1, pp. 61–75, 2023. doi: 10.23919/JCN.2022.000037.

[11] F. Aloraini, A. Javed, O. Rana, and P. Burnap, "Adversarial machine learning in IoT from an insider point of view," *J. Inf. Secur. Appl.*, vol. 70, no. 3, 2022, Art. no. 103341. doi: 10.1016/j.jisa.2022.103341.

[12] C. Nguyen, T. M. Hoang, and A. A. Cheema, "Channel estimation using CNN-LSTM in RIS-NOMA assisted 6G network," *IEEE Trans. Mach. Learn. Commun. Netw.*, vol. 1, no. 4, pp. 43–60, 2023. doi: 10.1109/TMLCN.2023.3278232.

[13] M. Babar, M. S. Khan, U. Habib, B. Shah, F. Ali and D. Song, "Scalable edge computing for IoT and multimedia applications using machine learning," *Hum.-Centric Comput. Inf. Sci.*, vol. 11, 2021, Art. no. 41.

[14] T. P. Fowdur and B. Doorgakant, "A review of machine learning techniques for enhanced energy effi-cient 5G and 6G communications," *Eng. Appl. Artif. Intell.*, vol. 122, 2023, Art. no. 106032. doi: 10.1016/j.engappai.2023.106032.

[15] M. Meenalakshmi, S. Chaturvedi, and V. K. Dwivedi, "Enhancing channel estimation accuracy in po-lar-coded MIMO-OFDM systems via CNN with 5G channel models," *AEU-Int. J. Electron. Commun.*, vol. 173, 2024, Art. no. 155016. doi: 10.1016/j.aeue.2023.155016.

[16] M. K. Chary, C. V. Krishna, and D. R. Krishna, "Accurate channel estimation and hybrid beamforming using Artificial Intelligence for massive MIMO 5G systems," *AEU-Int. J. Electron. Commun.*, vol. 173, 2024, Art. no. 154971. doi: 10.1016/j.aeue.2023.154971.

[17] Y. Chu, Z. Wei, Z. Yang, and D. W. K. Ng, "Channel estimation for RIS-aided MIMO systems: A partially decoupled atomic norm minimization approach," in *GLOBECOM 2023–2023 IEEE Global Commun. Conf.*, Kuala Lumpur, Malaysia, 2023, pp. 6615–6620.

[18] M. A. Ferrag, D. Hamouda, M. Debbah, L. Maglaras, and A. Lakas, "Generative adversarial networks-driven cyber threat intelligence detection framework for securing internet of things," in *2023 19th Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT)*, Pafos, Cyprus, 2023, pp. 196–200.
[19] M. A. Ferrag, M. Debbah, and M. Al-Hawawreh, "Generative AI for cyber threat-hunting in 6G-enabled iot networks," in *2023 IEEE/ACM 23rd Int. Symp. Cluster, Cloud Internet Comput. Workshops (CCGridW)*, Bangalore, India, 2023, pp. 16–25.
[20] M. A. Ferrag *et al.*, "Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 4, pp. 2654–2713, 2023. doi: 10.1109/COMST.2023.3317242.
[21] Y. Zheng, C. -X. Wang, J. Huang, R. Feng, and J. Thompson, "A novel ultra-massive MIMO BDCM for 6G wireless communication systems," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 4, pp. 3221–3237, 2024. doi: 10.1109/TWC.2023.3306726.
[22] Y. Huo *et al.*, "Technology trends for massive MIMO towards 6G," *Sensors*, vol. 23, no. 13, 2023, Art. no. 6062. doi: 10.3390/s23136062.
[23] N. A. Alhaj *et al.*, "Integration of hybrid networks, A.I., ultra massive-MIMO, THz frequency, and FBMC modulation towards 6G requirements: A review," *IEEE Access*, vol. 12, no. 5, pp. 483–513, 2023. doi: 10.1109/ACCESS.2023.3345453.
[24] W. Yu *et al.*, "An adaptive and robust deep learning framework for THz ultra-massive MIMO channel estimation," *IEEE J. Sel. Top. Signal Process.*, vol. 17, no. 4, pp. 761–776, 2023. doi: 10.1109/JSTSP.2023.3282832.
[25] S. Kirtay, K. Yildiz, and V. G. Bocekci, "Artificial intelligence-based fair allocation in NOMA tech-nique: A review," *Int. J. Sens. Wirel. Commun. Control*, vol. 14, no. 3, pp. 161–174, 2024.
[26] A. T. Jawad, R. Maaloul, and L. Chaari, "A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges," *Comput. Netw.*, vol. 237, no. 3, 2023, Art. no. 110085. doi: 10.1016/j.comnet.2023.110085.
[27] U. Ali *et al.*, "Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for internet of things environment," *Internet Things*, vol. 24, no. 1, 2023, Art. no. 100923. doi: 10.1016/j.iot.2023.100923.
[28] L. Jiao *et al.*, "Advanced deep learning models for 6G: Overview, opportunities and challenges," *IEEE Access*, vol. 12, no. 8, pp. 133245–133314, 2024. doi: 10.1109/ACCESS.2024.3418900.
[29] S. K. Das, R. Mudi, and Md. S. Rahman, "Federated reinforcement learning for 6G wireless net-works: Fundamentals, challenges and future research trends," in *IEEE Open J Veh. Technol.*, vol. 5, pp. 1400–1440, 2024. doi: 10.36227/techrxiv.20069051.v3.
[30] A. Abbas and R. Hasan, "A multi-attribute-based data forwarding scheme for delay tolerant networks," *J. Supercomput.*, vol. 80, no. 5, pp. 6356–6381, Mar. 2024. doi: 10.1007/s11227-023-05702-5.
[31] R. Anand *et al.*, "Optimizing 6G wireless network security for effective communication," in *Innovative Smart Materials Used in Wireless Communication Technology*. IGI Global, 2023, pp. 1–20, 2023.
[32] F. O. Catak, M. Kuzlu, E. Catak, U. Cali, and O. Guler, "Defensive distillation-based adversar-ial attack mitigation method for channel estimation using deep learning models in next-generation wireless networks," *IEEE Access*, vol. 10, no. 1, pp. 98191–98203, 2022. doi: 10.1109/ACCESS.2022.3206385.