A Secure Deep Autoencoder-based 6G Channel Estimation to Detect/Mitigate Adversarial Attacks

1st Haider W. Oleiwi
Department of Electronic and Electrical Engineering
Brunel University London
UB8 3PH, UK
Haider.Al-Lami@brunel.ac.uk

2nd Doaa N. Mhawi
Technical Institute of Management, Middle Technical University, Baghdad, 10010, Iraq
dododuaaenteesha@mtu.edu.iq

3rd H. S. Al-Raweshidy
Department of Electronic and Electrical Engineering
Brunel University London
UB8 3PH, UK
Hamed.Al-Raweshidy@brunel.ac.uk

Abstract—Channel estimation (CE) is critical in wireless communications. However, it is vulnerable to adversarial attacks (AA) that are associated with the incorporated artificial intelligence (AI) functionality in 6G wireless communication systems/networks. The hazardous threat can compromise communications' confidentiality and integrity due to the expected infrastructure, features, and AI models of the 6G paradigm. This paper proposed a deep autoencoder (DAE)-based 6G CE model to detect and prevent AA. It was trained using a dataset generated from the MATLAB toolbox for AA and incorporated a secure transmission protocol. Simulations were conducted to evaluate the model's performance under different parameters (i.e., CE and DAE) with maximal epsilon values range (0.5-3.0). The results proved the model's sufficiency of accuracy and security to detect AA compared to existing CE techniques. The proposal provided a promising solution for a secure 6G DAE-based CE and showed robustness against AA. Additionally, it offered a feasible solution for the deep learning training data required and avoids overfitting. Overall, the proposed model provides a valuable contribution towards enhancing the security of 6G networks, and its performance should be further validated in real-world scenarios.

Keywords: 6G Wireless Communication Networks, Adversarial Attacks, Artificial Intelligence, Channel Estimation, Cybersecurity, Deep Autoencoder.

I. INTRODUCTION

In wireless communications channel estimation (CE), the security, cost, and complexity measurements represent important metrics for evaluating systems' feasibility and practicability. The CE process is critical for successful communications [1], [2]. The sixth generation (6G) CE represents a very complex operation compared to previous generations due to the upgraded infrastructure, features, applications, network traffic, technologies, and the number of associated gadgets/users connected ubiquitously to cope with the emerging internet of everything (IoE) [3]–[5]. Cellular networks have grown significantly over the past few decades with developments in communications technologies that enable faster data-rates, bigger cell/channel capacities, and lower latency. Such technologies' major objective is to make a variety of unique applications possible (e.g., online learning, telepresence, flying, driverless automobiles, smart cities/ grids, and intelligent manufacturing) [6], [7]. The 6G emerging requirements and features accompany serious security anxiety and increase network computational complexity. According to the jeopardizes of wireless communication networks to renewable various attacks, 6G-related researchers must focus on the necessity for novel artificial intelligence (AI)-based security systems to satisfy the development of adversarial attacks (AA) detection and mitigation for 6G wireless communication networks. It is critically required to confront the threats efficiently, abandoning the current incapable CE-targeted security systems that cannot adapt to the upgradable attacks [8], [9]. In risk-sensitive systems safety, detecting AA is a challenging issue as enormous traffic of suspicious activities is discovered every day. The impact of these complex attacks is increasing, introducing additional complications to the current attacks. Moreover, cybersecurity has become a prioritized essential topic in the modern scientific community. Therefore, monitoring and analyzing network traffic is essential to detect potential AA. The main risk in traditional and machine learning (ML)-based security systems is the insufficiency of distinguishing AA in 6G communication networks as AA manipulates signals or data in ways that are not detectable by traditional measures [10]. To this end, it is important to design 6G networks with security in mind and to implement best practices for securing the network against AA. This may involve developing new security measures that are specifically designed to detect and defend against AA. Deep Autoencoders (DAEs) are a type of NN that can be trained to learn a compressed representation of the input data, also known as the encoding, and then use this encoding to reconstruct the original input, also known as the decoding [11]–[19]. By training an AE on a set of received signals and their corresponding channel characteristics, the AE can learn to extract features that are relevant to CE. The encoding produced by the AE can then be used as a representation of the received signal, which can be fed into a CE to estimate the channel characteristics. This can be particularly useful in scenarios where the channel is highly complex or time-varying, as the AE can adapt to changes in the channel over time and provide more accurate estimates of the channel characteristics.

Hence, this work proposes a secure deep autoencoder (DAE)-based communication environment (CE) model to address the challenges of accurately detecting and preventing adversarial attacks (AA) in 6G wireless communication networks with minimal complexity. To the best of the authors' knowledge, this outperforming integrated DAE model with its performance has not been achieved previously. It presents a valuable contribution to the field by introducing:

- A sufficient DAE-based CE 6G model with a secure transmission protocol that uses transmitted signal parameters to learn and detect AA. The model provides a feasible solution for deep learning training data requirements, avoiding overfitting.

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/GPECOM58364.2023.10175718, 2023 5th Global Power, Energy and Communication Conference (GPECOM)

- A comprehensive evaluation of the proposed model under different CE and DAE parameters to demonstrate its effectiveness and robustness against AA with epsilon values ranging (0.5-3.0).

Overall, the proposed secure DAE-based CE model offers a promising solution to enhance the security of 6G networks against AA with minimal complexity, paving the way for more advanced and effective security mechanisms.

The paper's next section provides brief literature on the related technologies. System methodology with the software (libraries), generated dataset, and DAE model are described in detail in section III. Sections IV and V illustrate the implementation environment and the conducted results, evaluation, and discussion, respectively. And finally, section VI states the conclusion and future work.

II. Background

The CE process is the first step in identifying the characteristics of the radio transmission channel through which the transmitted signal propagates from the transmitter (Tx) to the receiver (Rx). This prerequisite information is called channel state information (CSI) and it requires to be realized by Tx and Rx. The common assessment of CE methods (e.g., mean square error (MSE)) is achieved by a predefined reference (pilot) sequential signal sent with the transmitted signal and compared to the original pilot at the Rx after undergoing influential (e.g., attenuation, distortion, and noise) effects while being transmitted. The traditional CE is poor, non-robust, complicated, and performs inaccurately because of the changeable non-linear channel characteristics and the information's high dimensionality. Its complexity increases with respect to the increase in the number of communication links [2]. Besides, 6G plans assume an upgraded mobile infrastructure, expanding the number of ubiquitously connected communication components and links to deploy ultra-densified networks using UM-MIMO. Providing extremely high data-rates (Terabits/Second) and extremely-low latency with bigger cell/channel capacities is a fundamental objective of 6G networks. The incorporation of the edge of technologies, e.g., AI, UM-MIMO, and terahertz frequency bands (0.1-10 THz) is strongly nominated for 6G networks. The integration of the 6G key enabling technologies/networks provides the targeted performance THz, while very big arrays of antennas are designed at Tx and Rx sides using UM-MIMO. This causes a considerable increase in energy dissipation, procedural/computational complexity, and hardware [2]. Therefore, 6G CE operations require adapting to the upgraded features and satisfying the growing demands of services to certain standards of data-rates, cost-effectiveness, and spectral/energy efficiencies. To this end, AI was intended to embed in the new era's systems to optimize networks' functionalities and improve system performance. As a valuable candidate of 6G key enablers, AI plays a pivotal role in CE processes [20], [21]. DL-based CE is a promising approach for improving the accuracy and efficiency of CE in 6G wireless communication systems by learning the transmitted and the received signals. It has several advantages over traditional CE techniques. It is more adaptive to changing channel conditions in real-time. Additionally, DL-based CE can be performed more efficiently than traditional CE techniques, reducing system computational complexity [22]. AA are typically associated with AI systems and accordingly 6G communication networks by manipulating perturbed input data. They are constructed to deliberately deceive and mislead them into making the wrong prediction or decision. AA in 6G manipulate signals or data in ways that are not detectable and could potentially bypass traditional and existing security measures. They mimic legitimate traffic but contain malicious content or commands [23].

Remarkably, CE is considered an essential topic for academics' cybersecurity research in wireless communication networks resulting in several articles published in recent years. However, CE jeopardizes AA vulnerabilities that degrade 6G system efficiency despite applying ML against these attacks. Therefore; this paper introduces a DAE-based CE.

III. Methodology

Fig. 1 shows the DAE-based CE general structure to track suspicious activity traffic over the 6G entire network.

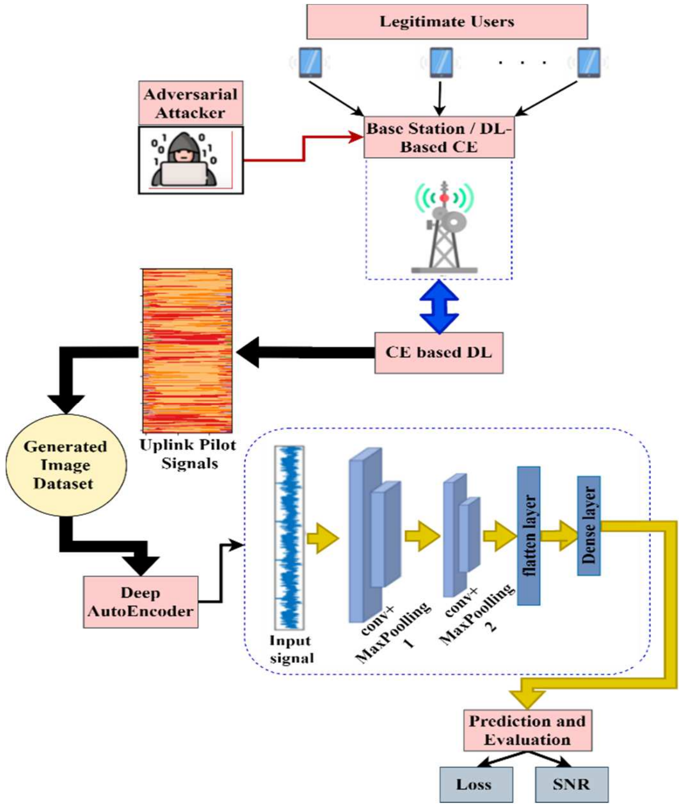


Fig. 1. The General Structure of DAE-Based CE.

Fig. 1 illustrates all processes made at the BS to detect AA and legitimate users using the DAE model. This model starts with pilots' uplink signals using MATLAB tools to generate an image dataset to evaluate system performance and robustness. The generated dataset and programming DAE model are:

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/GPECOM58364.2023.10175718, 2023 5th Global Power, Energy and Communication Conference (GPECOM)

A. Dataset Descriptions and Scenario

Many reference cases are available in Toolbox and other next-generation network communication systems [24]. Collecting datasets for DL-based models enables customization and the generation of various waveforms, antennas, and channel models. A reference example in the MATLAB Toolbox is utilized to generate the training-dataset for DAE-based CE. Table I illustrates a sample of this dataset.

TABLE I. ORIGINAL DATASET DESCRIPTION.

Feature 1	Feature 2	Feature 3	Feature 4
0.15+0.89j	0.14+0.90j	0.17+0.91j	0.11+0.88j
-0.39+0.84j	- 0.26+0.83j	-0.37+0.89j	-0.41+0.89j
-0.56+0.78j	-0.41+0.82j	-0.55+0.79j	-0.26+0.72j
-0.26+0.89j	-0.32+0.87j	-0.44+0.84j	-0.32+0.80j
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
-0.86+0.43j	-0.88+0.15j	-0.33+0.23j	-0.89+0.21j

A new channel characteristic is generated for every set of training-dataset based on different parameters. Table II lists channel characteristics with associated values.

TABLE II. CE PARAMETERS.

Channel Parameters	Values
Doppler-Shift	0.0004-100 MHz
Delay Spread	0.001-0.25 ns
Sample Rate	32950000
NFFT	1024
Windows	36
Symbols/Slot	14
Slots/Frame	20
Slots/Sub-frame	2
Polarity	CoPolar
Transmit Antennas no.	64
Receive Antennas no.	64
Fading Distribution	Rayleigh
Modulation	16QAM

B. Programming Deep Autoencoder-Based Channel Estimation

The DAE model can provide several advantages when used for CE in 6G wireless communication systems:

1. Improving Accuracy: DAEs can learn complex features of a wireless channel, e.g., multipath propagation, noise, and interference, which can improve the accuracy of CE compared to traditional methods.
2. Robustness: DAEs are robust to noise and interference, which can improve the reliability of CE in practical wireless communication scenarios.
3. Reducing Training Data Requirements: DAEs can learn from fewer training samples than traditional methods, which can be especially advantageous in low SNR scenarios where collecting large amounts of training data is difficult.
4. Low Complexity: DAEs have a relatively low computational complexity compared to other ML algorithms, which makes them suitable for implementation in real-time wireless communication systems.
5. Adaptability: DAEs can adapt to changes in the wireless channel over time, which enables enhanced CE performance in dynamic wireless communication scenarios.

The AE-based DL model's hyper-parameters are shown in Table III.

TABLE III. DAE PARAMETERS.

DAE Parameters	Values
Activation Function	ReLu
Batch size	128
Testing samples	30%
Training samples	70%
Loss function	MSR
Learning rate	0.001
Number of epochs	1000
Optimizer	Adam
Momentum	0.9
Input/output size	612 x 14

The DAE model for the CE employed is depicted in Fig. 2.

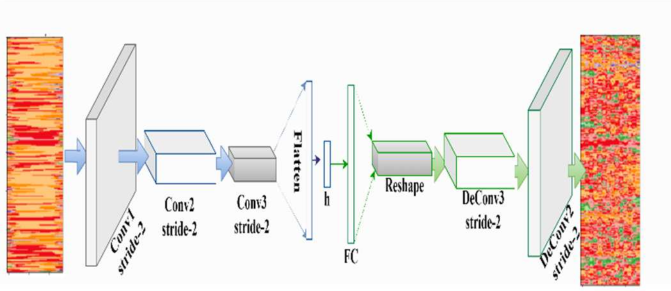


Fig. 2. The DAE-Based CE.

In Fig. 2, DAE works when the dataset is generated then the first stage of AE, i.e., convolution 1 (Conv.1) layer with a stride-2 can be used for features extraction of the input signal. The Conv.1 layer architecture is a set of filters that slide over the input signal to generate a set of feature maps. The basic idea behind using a Conv.1 layer with a stride is performing a local feature extraction, where each filter extracts features from a local region of the input signal. The stride ensures that the filter covers every possible local region of the input signal. To program a DAE using a Conv.1 layer with a stride, the following steps can be followed:

1. Define the Conv.1 layer: it specifies the filters' number, filter size, and stride.
2. Feed the input signal into the Conv.1 layer: it produces a set of feature maps. For example, assuming the input signal is an image of size 128x128 with 3 color channels as follows:
3. Use the feature maps for further processing: it is produced by the Conv.1 layer and can be used as input for further processing in the AE architecture.

By using a Conv.1 layer with a stride-2 in a DAE model, the model can learn to extract local features from the input signal. The local features can be used to reconstruct the input signal in a lower-dimensional feature space, which can be used for various applications, significantly for CE in wireless communication systems. While deconvolution (DeConv.) layers with a stride-2 and flattening layers are often used for various applications, e.g., image dataset processing. These layers help to increase the

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/GPECOM58364.2023.10175718, 2023 5th Global Power, Energy and Communication Conference (GPECOM)

spatial resolution of the feature maps and convert them into a vector form, respectively. These layers work in a DAE as:

1. DeConv. layer with stride-2 (so-called a transpose convolutional layer or a fractionally-strides convolutional layer): it can be used to increase the spatial resolution of the feature maps produced by the previous layers. The DeConv layer performs the opposite operation of a Conv.1 layer, and it can be used to reconstruct the input signal or to up-sample the feature maps.
2. Flattening layer: it is used to convert the 3D feature maps into a 1D vector format. This is typically done before passing the feature vectors through a dense layer for classification or regression tasks, defined as:
3. Using these layers in a deep autoencoder: in a deep autoencoder, a DeConv. layer with stride-2 can be used to up-sample the feature maps, and a flattening layer can be used to convert the feature maps into a 1D vector format.
4. The model is assessed and contrasted using MSE. The MSE scores are used to analyze the model further. The following is the MSE equation.

$$MSE = \frac{\sum(\mathrm{Yt} - \tilde{\mathrm{Y}}\mathrm{t})^2}{\mathrm{n}} \tag{1}$$

Where Yt means the actual attribute and $\tilde{\mathrm{Y}}\mathrm{t}$ means forecasted attribute.

The MSE between the real and predicted scales is measured. Whenever a model is perfect that means the MSE measurement is zero. It is proportional to model-error. Algorithm 1 with pseudo-code demonstrates the main steps of DAE for CE.

```
Algorithm 1: DAE-based CE
1.  Input: Generated and Load the dataset: Load the dataset which consists
    of input signals and corresponding CEs. /*Preprocess the input data:
    Normalize the input data by dividing each element by the maximum
    value*/.
2.  Output: Training dataset, MSR.
3.  Begin:
4.  Define the AE /*the encoder and decoder architecture using Conv. and
    DeConv. layers, respectively in Table III*/.
5.  Define the CE parameters using Table II a dense layer.
6.  Concatenate the input signal and CE.
7.  Define the DAE-based CE model: with the following Pseudocode.
8.  AE-model=Model (concatenated-input, decoded-signal).
9.  CE-model=Model (channel-input, channel-estimate).
10. Combined-input = Input (shape= (64, 64, 1)).
11. Channel-output=CE-model (CE).
12. Combined-output=concatenate ([combined-input, channel-output]).
13. AE-output = AE-model (combined-output)
14. Full-model=Model (inputs= [combined-input, channel-input], outputs=
    [AE-output, channel-output])
15. Compile and train the model: Compile the full model and train it on the
    input data and channel estimates. As follows:
16. Full model. Compile(optimizer=Adam(lr=0.001),
17. loss= ['MSE', MSE], metrics=['accuracy']).
18. history = full-model. Fit ([input-data, CE], [input-data, CE],
    epochs=50, batch-size=32, shuffle=True, validation-split=0.2)
19. Return MSR (accuracy).
20. End.
```

The model examinations of the AA's five attacks (FGSM, BIM, MIM, PGD, and C&W) trained and tested the effectiveness of the suggested mitigation measures to achieve the highest performance (i.e., the lowest possible MSE).

IV. Implementation Enviroment

MATLAB tools, Python, and Collaborator (Colab) are general-purpose programming languages, which are simple to use and learn. They are compatible with numerous operating systems i.e., Windows, Linux, and Mac. TensorFlow and Keras are two open-source DL libraries created to expand the Python library. As a result, this paper uses these languages and libraries to put the suggestions into practice. The DAE is carried out using MATLAB Toolbox to generate the dataset. Furthermore; the DAE model is implemented using Python 3.8 in colab, using TensorFlow and Keras libraries. The laptop used is equipped with a Core i7 CPU, 10th Generation, and 64-bit Operating System Win. 11.

V. Results, Evaluation, and Discussion

A. Performance Results and Evaluation

To assess the effectiveness of DAE-based channel estimate models in the 6G Network, attack success ratio (ASR) was used for evaluation statistics as:

$$ASR = \frac{1}{m}\sum_{i=0}^{m} \frac{MSE\left(X_{(i)}^{adv}, y(i)\right) - MSE\big(X(i), y(i)\big)}{MSE\left(X_{(i)}^{adv}, y(i)\right)} \tag{2}$$

ASR represents the test-samples proportion, which the attacker may incorrectly forecast to all test samples. An attack is more effective if the ASR is higher.

Table IV shows the experimental findings for the suggested AA-based mitigation techniques.

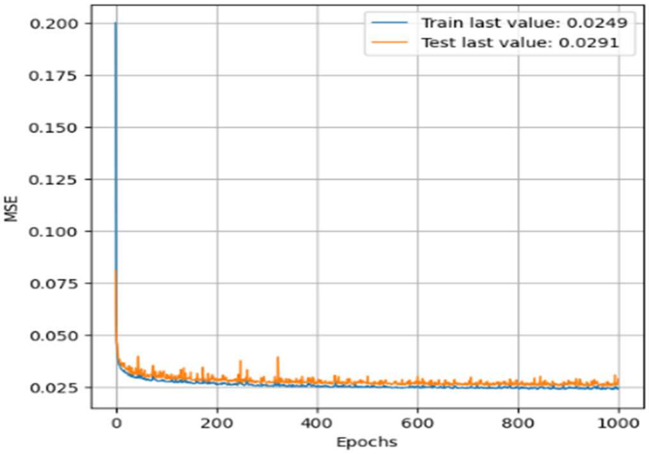
TABLE IV. EXPERIMENTAL TEST RESULTS OF DAE-BASED CE FOR AA.

Attacks Names	**Epsilon**	**MSE**		**ASR**
		Normal	***Attacks***	
FGSM	0.1	0.02812	0.02848	0.018932
	0.5	0.02812	0.03676	0.218932
	1.0	0.02810	0.07848	0.618932
	2.0	0.02822	0.19284	0.818932
	3.0	0.02783	0.30651	0.918932
BIM	0.1	0.02812	0.02848	0.018932
	0.5	0.02812	0.03676	0.218932
	1.0	0.02810	0.07848	0.618932
	2.0	0.02822	0.19284	0.818932
	3.0	0.02783	0.30651	0.918932
MIM	0.1	0.02812	0.02848	0.018932
	0.5	0.02812	0.03676	0.218932
	1.0	0.02810	0.07848	0.618932
	2.0	0.02822	0.19284	0.818932
	3.0	0.02783	0.30651	0.918932
C&W	_	0.028314	0.02980	0.066435
PGD	0.1	0.02812	0.02848	0.018932
	0.5	0.02812	0.03676	0.218932
	1.0	0.02810	0.07848	0.618932
	2.0	0.02822	0.19284	0.818932
	3.0	0.02783	0.30651	0.918932

This article has been accepted for publication in a future proceedings of this conference, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/GPECOM58364.2023.10175718, 2023 5th Global Power, Energy and Communication Conference (GPECOM)

in Table IV, epsilon values typically refer to the maximum amount of perturbation or distortion allowed to be added to the AA original input data (the epsilon value refers to a small perturbation value that is added to the input data to create AA. The objective of AA is to cause an ML model to misclassify an input by making small modifications to the input data. It determines the magnitude of these modifications). That generates more aggressive AA to fool intelligent systems. For example, in the popular Fast Gradient Sign Method (FGSM) attack, the perturbation added to the input image is scaled by a small value of epsilon, which controls the amount of distortion introduced to the original image. By adjusting the value of epsilon, an attacker can control the trade-off between the degree of distortion introduced to the input and the likelihood of AA successfully, fooling the model. The experiments-result demonstrates that the suggested approach can increase the CE model's accuracy. The findings depict that the approach can deliver superior outcomes for AA (FGSM, BIM, MIM, PGD, and C&W). Fig. 3 demonstrates the training and testing dataset's MSE with epochs 1000.

Fig. 3. MSE for Training and Testing Datasets.



The effectiveness of the CE model can be increased by the outcomes of the suggested DAE model. Fig. 4 shows the MSE values change before and after applying a DAE model. The MSE values before the model (left-sided Fig.) are virtually identical to the attacks and the values are maximum. However; when the DAE model is applied, the values of MSE of all attacks are minimum.

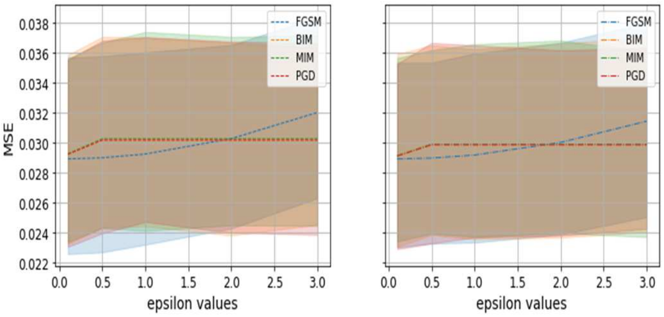


Fig. 4. The experimental results of DAE-based CE between MSE and epsilon.

Fig. 4 shows that DEA-based CE is efficient at predicting and detecting the AA with the epsilon values added to the original data. Table V demonstrates the details about all the AA.

TABLE V. MALICIOUS DISTANCE WITH REAL AND PREDICTED MSE FOR EACH ATTACK.

Index	Malicious Distance	Real Predicted MSE	Malicious Predicted MSE	Attacks	epsilon
377	2.7999999	0.0118651	0.0129488	BIM	3.0
179	2.8000023	0.0329317	0.0329508		2.0
301	0.7000001	0.0100393	0.0100881	FGSM	0.5
290	1.4000003	0.0537686	0.0534277		1.0
490	1.4000003	0.0382549	0.0385098		1.0
510	1.4000003	0.0077401	0.0080595		1.0
529	2.8000063	0.0344316	0.0354635	MIM	2.0
66	2.8000068	0.0269185	0.0276220		1.0
142	2.8000023	0.0296083	0.0299384	PGD	2.0
131	2.8000068	0.0411919	0.0422248		0.5
366	2.8000020	0.0319317	0.0319400	C&W	0.5

Table V shows various forms of attacks. The index-based attacks focus on finding the closest AA, whereas distance-based attacks focus on maximizing the distance between the original data point and AA. The experimental results are consistent across all types of AA (BIM, FGSM, MIM, C&W, and PGD). Furthermore, the epsilon values range was expanded to (0.5-3.0), whereas the MSE values of real and predicted malicious are still similar or close to each other across the different combinations of attack, epsilon value, and distance metrics. These findings prove that the model is highly susceptible to a wide range of adversarial perturbations. Hence, small changes in the perturbation parameters do not significantly affect the quality of AA detection concerning the MSE metric.

VI. Conclusion and Future work

In a nutshell, this study proposed a secure DAE-based 6G CE model to detect and mitigate potential AA. It demonstrated promising results in improving the robustness and effectiveness of CE against AA in 6G networks throughout comprehensive experimental evaluations. The results proved the system's outperformance over traditional CEs per simplicity, accuracy, and resilience against AA (a high accuracy to detect AA (FGSM, BIM, PGD, MIM, and C&W) with minimum MSE of real and predicted malicious) when the epsilon values ranged (0.5-3.0) with various attacks' distances. Overall, the proposed approach paves the way for the development of more advanced and effective security mechanisms in 6G networks to ensure the reliability and availability of 6G communications. In the future, further developments might be made in several directions. Validating this model performance upon the deployment of 6G networks in real-world practice, integrating it with other defense mechanisms and response systems, or extending it to address other types of attacks in 6G networks, e.g., jamming, poisoning, dark net, and spoofing attacks.

References

[1] U. Mutlu and Y. Kabalci, “Deep Learning Aided Channel Estimation Approach for 5G Communication Systems,” *Proc - 2022 IEEE 4th Glob Power, Energy Commun Conf GPECOM 2022*, no. Dl, pp. 655–

660, 2022, doi: 10.1109/GPECOM55404.2022.9815811.

[2] B. Ozpoyraz, A. T. Dogukan, Y. Gevez, U. Altun, and E. Basar, "Deep Learning-Aided 6G Wireless Networks: A Comprehensive Survey of Revolutionary PHY Architectures," *IEEE Open J Commun Soc*, vol. 3, pp. 1749–1809, 2022, doi: 10.1109/OJCOMS.2022.3210648.

[3] H. W. Oleiwi, N. Saeed, and H. S. Al-Raweshidy, "A Cooperative SWIPT-Hybrid-NOMA Pairing Scheme considering SIC imperfection for THz Communications," *Proc - 2022 IEEE 4th Glob Power, Energy Commun Conf GPECOM 2022*, no. June, pp. 638–643, 2022, doi: 10.1109/GPECOM55404.2022.9815677.

[4] H. W. Oleiwi and H. Al-Raweshidy, "SWIPT-Pairing Mechanism for Channel-Aware Cooperative H-NOMA in 6G Terahertz Communications," *Sensors*, vol. 22, no. 16, p. 6200, 2022, doi: 10.3390/s22166200.

[5] H. W. Oleiwi, N. Saeed, H. L. Al-taie, and D. N. Mhawi, "Evaluation of Differentiated Services Policies in Multihomed Networks Based on an Interface-Selection Mechanism," *Sustainability*, vol. 14, no. 20, pp. 1–12, 2022, doi: 10.3390/su142013235.

[6] H. W. Oleiwi and H. Al-Raweshidy, "Cooperative SWIPT THz-NOMA/6G Performance Analysis," *Electron*, vol. 11, no. 6, 2022, doi: 10.3390/electronics11060873.

[7] H. W. Oleiwi, D. N. Mhawi, and H. Al-Raweshidy, "MLTs-ADCNs: Machine Learning Techniques for Anomaly Detection in Communication Networks," *IEEE Access*, vol. 10, no. August, pp. 91006–91017, 2022, doi: 10.1109/ACCESS.2022.3201869.

[8] D. N. Mhawi, H. W. Oleiwi, N. H. Saeed, and H. L. Al-Taie, "An Efficient Information Retrieval System Using Evolutionary Algorithms," *Network*, vol. 2, no. 4, pp. 583–605, 2022, doi: 10.3390/network2040034.

[9] H. W. Oleiwi, D. N. Mhawi, and H. Al-Raweshidy, "A Meta-Model to Predict and Detect Malicious Activities in 6G-Structured Wireless Communication Networks," *Electron*, vol. 12, no. 3, 2023, doi: 10.3390/electronics12030643.

[10] H. W. Oleiwi, N. Saeed, and H. Al-Raweshidy, "Cooperative SWIPT MIMO-NOMA for Reliable THz 6G Communications," *Network*, vol. 2, no. 2, pp. 257–269, 2022, doi: 10.3390/network2020017.

[11] X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen, "Using Bayesian Networks for Probabilistic Identification of Zero-Day Attack Paths," *IEEE Trans Inf Forensics Secur*, vol. 13, no. 10, pp. 2506–2521, 2018, doi: 10.1109/TIFS.2018.2821095.

[12] M. Alazab, "Profiling and classifying the behavior of malicious codes," *J Syst Softw*, vol. 100, pp. 91–102, 2015, doi: 10.1016/j.jss.2014.10.031.

[13] I. Sumaiya Thaseen and C. Aswani Kumar, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM," *J King Saud Univ - Comput Inf Sci*, vol. 29, no. 4, pp. 462–472, 2017, doi: 10.1016/j.jksuci.2015.12.004.

[14] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He, and K. C. Li, "Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain-based Systems," *IEEE Internet Things J*, 2021, doi: 10.1109/JIOT.2021.3053842.

[15] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," *IEEE Internet Things J*, vol. 8, no. 5, pp. 3242–3254, 2021, doi: 10.1109/JIOT.2020.3002255.

[16] M. A. Khan and J. Kim, "Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset," *Electron*, vol. 9, no. 11, pp. 1–17, 2020, doi: 10.3390/electronics9111771.

[17] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," *J Ambient Intell Humaniz Comput*, vol. 12, no. 2, pp. 1559–1576, 2021, doi: 10.1007/s12652-020-02228-z.

[18] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and T. G. Reddy, "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU," *IEEE Trans Netw Sci Eng*, vol. 8, no. 2, pp. 1456–1466, 2021, doi: 10.1109/TNSE.2021.3059881.

[19] D. N. Mhawi and S. H. Hashim, "Proposed Hybrid EnsembleLearninig algorithms for an Efficient Intrusion Detection System," *IJCCE*, vol. 22, no. 2, pp. 73–84, 2022.

[20] D. N. Mhawi and S. H. Hashem, "Proposed Hybrid Correlation Feature Selection Forest Panalized Attribute Approach to advance IDSs," *Karbala Int J Mod Sci*, vol. 7, no. 4, pp. 405–420, 2021, doi: 10.33640/2405-609X.3166.

[21] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G : Opening New Horizons for Integration of Comfort , Security , and Intelligence," *IEEE Wirel Commun*, vol. 27, no. 5, pp. 126–132, 2020.

[22] Q. Hu, F. Gao, H. Zhang, S. Jin, and G. Y. Li, "Deep Learning for Channel Estimation: Interpretation, Performance, and Comparison," *IEEE Trans Wirel Commun*, vol. 20, no. 4, pp. 2398–2412, 2021, doi: 10.1109/TWC.2020.3042074.

[23] D. N. Mhawi, A. Aldallal, and S. Hassan, "Advanced Feature-Selection-Based Hybrid Ensemble Learning Algorithms for Network Intrusion Detection Systems," *Symmetry (Basel)*, vol. 14, no. 7, p. 1461, 2022, doi: 10.3390/sym14071461.

[24] F. O. Catak, M. Kuzlu, E. Catak, U. Cali, and O. Guler, "Defensive Distillation-Based Adversarial Attack Mitigation Method for Channel Estimation Using Deep Learning Models in Next-Generation Wireless Networks," *IEEE Access*, vol. 10, pp. 98191–98203, 2022, doi: 10.1109/ACCESS.2022.3206385.