Physical Communication 52 (2022) 101626

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Security concerns on machine learning solutions for 6G networks in mmWave beam prediction

Ferhat Ozgur Catak [a,*], Murat Kuzlu [b], Evren Catak [c], Umit Cali [d], Devrim Unal [e]

[a] University of Stavanger, Stavanger, Norway
[b] Old Dominion University, VA, USA
[c] Norwegian University of Science and Technology, Gjøvik, Norway
[d] Norwegian University of Science and Technology, Trondheim, Norway
[e] KINDI Center for Computing Research, College of Engineering, Qatar University, Doha, Qatar

ARTICLE INFO

Article history:
Received 21 July 2021
Received in revised form 22 November 2021
Accepted 18 January 2022
Available online 25 January 2022

Keywords:
Machine learning
AI
Millimeter-wave (mmWave)
Beamforming
Adversarial machine learning
6G
Deep learning

ABSTRACT

6G – sixth generation – is the latest cellular technology currently under development for wireless communication systems. In recent years, machine learning (ML) algorithms have been applied widely in various fields, such as healthcare, transportation, energy, autonomous cars, and many more. Those algorithms have also been used in communication technologies to improve the system performance in terms of frequency spectrum usage, latency, and security. With the rapid developments of ML techniques, especially deep learning (DL), it is critical to consider the security concern when applying the algorithms. While ML algorithms offer significant advantages for 6G networks, security concerns on artificial intelligence (AI) models are typically ignored by the scientific community so far. However, security is also a vital part of AI algorithms because attackers can poison the AI model itself. This paper proposes a mitigation method for adversarial attacks against proposed 6G ML models for the millimeter-wave (mmWave) beam prediction using adversarial training. The main idea behind generating adversarial attacks against ML models is to produce faulty results by manipulating trained DL models for 6G applications for mmWave beam prediction. We also present a proposed adversarial learning mitigation method's performance for 6G security in mmWave beam prediction application a fast gradient sign method attack. The results show that the defended model under attack's mean square errors (i.e., the prediction accuracy) are very close to the undefended model without attack.

1. Introduction

Cellular networks have been the most popular wireless communication technology in the last three decades (1G–2G in the early 1990s, 3G in the early 2000s, 4G in the 2010s, 5G in the 2020s), which can support high data rate with long distance for voice and data. Data transmission speed and the number of users have increased sharply, with recent versions such as 4G (WiMAX and LTE), 4.5G (LTE Advanced Pro), 5G, and 6G. Cellular systems typically operate over land areas, called cells, served by fixed-based transceiver stations, i.e., base stations (BSs), in various frequency bands from 850 Mhz to 95 GHz [1]. Latest cellular technologies (4G/5G/6G) support higher data rates, i.e., approximately 33.88 Mbps, 1,100 Mbps, and 1 Tbps, respectively, and low latency, i.e., milliseconds. However, they are still suffering congestion and reduced network performance due to sharing the frequency spectrum with other mobile users.

Introducing the 5G with superfast data speeds is a breakthrough and presents a significant transformation in mobile networking and data communication. It offers a data transmission speed of 20 times faster than the 4G networks and delivers less than a millisecond data latency [2–4]. The main difference of 5G is to use a new technology called massive multiple-input multiple-output (MIMO) and using multiple targeted beams to spotlight [5,6]. Massive MIMO is an extension of MIMO consisting of groups of antennas at the transmitter and receiver to provide better throughput and better spectrum efficiency.

Authors in [7] investigate several MIMO architectures and beamforming solutions for 5G technology. According to the results, the precise antenna array calibration with large-scale antenna arrays for multi-user-MIMO (MU-MIMO) is needed. MIMO can also enable more devices to be used within the same geographic area, i.e., 4,000 devices per square kilometers for 4G, while around one million for 5G [8]. 6G is the last version of this series, which follows up on 4G and 5G. It promises mobile

* Corresponding author.
E-mail addresses: f.ozgur.catak@uis.no (F.O. Catak), mkuzlu@odu.edu (M. Kuzlu), evren.catak@ieee.org (E. Catak), umit.cali@ntnu.no (U. Cali), dunal@qu.edu.qa (D. Unal).

https://doi.org/10.1016/j.phycom.2022.101626

data speeds of 100 times faster with lower latency than the 5G network, i.e., approximately 1 Tbps data speed with 1 ms latency. Although the primary use cases of 6G are still under definition, it is clear that 6G will be used in the connectivity in cars, drones, mobile devices, IoT devices, homes, industries, and many more. The fundamental difference of 6G technology is the use of artificial intelligence (AI) and edge computing to make data communication networks more sophisticated [9,10]. Using AI algorithms provides novel solutions for massive MIMO systems involving many antennas and beam arrays. A beam codeword consists of analogue phase-shifted values and is applied to the antenna elements to form an analogue beam in [11], base beam selection with deep learning (DL) algorithms is proposed for using channel state information for the sub-6 GHz links. In addition to beam prediction, location and size of vehicles information are used to predict the optimal beam pair [12]. Location-based beamforming solutions are more suitable for line-of-sight (LOS) communication. On the other hand, the same locations with the non-line-of-sight (NLOS) transmission need different beamforming solutions.

In the literature, most studies have focused on the communication methods to increase cellular technologies' performance but usually ignore the security and privacy issues and the integration of currently emerging AI tools into 6G. It is expected that 6G networks would provide better performance than 5G ones and satisfy emerging services and applications. Authors in [13] and introduce AI as a critical enabler and offer a comprehensive review of 6G networks, including usage scenarios, requirements, and promising technologies for 6G networks. The review paper indicated that the promising technologies such as blockchain-based spectrum sharing and quantum communications and computing could significantly improve the 6G's spectrum in terms of efficiency and security. The study [14] discusses the key trends and AI-powered methodologies for 6G network design and optimization. Authors in [15] introduce and analyze the key technologies and application scenarios brought by the 6G networks. However, there is also a reason to be concerned about security risks. 6G introduces new risks, which must be addressed to ensure its secure and safe use. The study [16] addresses the fundamental principles of 6G security, discusses significant technologies related to 6G security, and presents several security issues. Authors in [17] investigate the fundamental security and privacy challenges associated with each key technology and potential applications, i.e., real-time intelligent edge, distributed AI, intelligent radio, and 3D intercoms, for 6G networks. The study in [18] proposes a framework incorporating context-awareness in quality of security (QoSec) that leverages physical layer security (PLS) for 6G networks. The framework identifies the security level required and proposes adaptive, dynamic, and risk-aware security solutions. The key component of 6G is the integration of AI, i.e., self-learning architecture based on self-supervised algorithms, to be able to improve the performance of the network for tomorrow's wireless cellular systems [19]. It is expected that a secure AI-powered structure can protect privacy in 6G. However, AI itself may be attacked or abused, resulting in privacy violations. The authors in [20] also indicate that some attackers simply can replace a legitimate model with an already poisoned model prepared ahead of time, i.e., attacking beneficial AI in such a way that the AI works against itself. The study in [21] provides a comprehensive survey of DL and privacy in 6G, with a view to further promoting the development of 6G and privacy protection technologies. With the use of DL algorithms in 6G's physical layer functions, such as channel estimation, modulation recognition, and channel state information (CSI) feedback, the physical layer faces new challenges caused by an adversarial attack. The authors in [22] investigate the impact of possible adversarial attacks on DL-based CSI feedback. According to the results, an adversarial attack may cause a destructive effect on DL-based channel state information (CSI) feedback, and transmitted data can be easily tampered with adversarial perturbation by malicious attackers due to the broadcast nature of wireless communication.

Smart cities have ushered in an era in which everyday objects, such as cars, toasters, window blinds and even toothbrushes, can be connected to the Internet. Indoor-IoT (i-IoT) sector makes up more than half of the total IoT market. Indoor is where most of the time people live and work. Moreover, the majority of the unresolved grand technical challenges hindering the wider adoption of IoT are found in indoor deployments. These include: (1) Non-standardized indoor environment, e.g., homes, devices come from different vendors but still need to interoperate to achieve common goals. (2) i-IoT solutions are often managed by IT novice users (owners of the system), thus systems must be able to self-recover from failures quickly and cost-effectively. (3) IoT devices are commonly installed with a number of security vulnerabilities, which renders them as a backdoor to hack home/corporate networks. (4) i-IoT devices are often connected to actuators, meaning that a successful attack could result in physical harm or risk, e.g., privacy risk through viewing a CCTV camera. i-IoT will connect a diverse range of devices regardless of their vendor, communication technology or software/hardware platform. This lack of interoperability has limited the development of i-IoT applications. In addition to security and privacy, another key challenge in i-IoT is how to manage the avalanche of heterogeneous devices and intelligently deliver smart city services on a consistent quality of service (QoS) basis. Different architectural models, such as the three- and five-layer models [23–25], have been studied in the literature. The outcome can be likened to a home, in which heating, ventilation and air conditioning, TV, audio system, security system, lighting, etc., each has its remote control, but no single one can control all devices; in other words, there is currently a lack of unified reference architecture that addresses the specific needs of i-IoT networks. Furthermore, i-IoT networks need to be self-aware and adaptive, i.e., they should be able to learn users' behavior and act intelligently and proactively on behalf of the users; this self-awareness and adaptiveness still remain largely unexplored to date. There is little discussion in the literature on the next step in the evolution of i-IoT, which is to create a living, intelligent, flexible and dynamic i-IoT that supports autonomous network reconfiguration to provide distributed management through analyzing control data in real-time to deliver the insights user/business need. Past research and development efforts, e.g., [26–28] explored the applications of machine learning (ML)-based techniques to improve the communication infrastructure performance and support existing services. However, these representative examples of previous work show that such efforts have addressed various segments of the overall network control/management optimization problem. The potential of ML techniques and data analytics along with Software Defined Networking (SDN) fosters the development of a coherent intelligent network control solution, which addresses the dynamic and responsive i-IoT. ML-enabled SDN approaches provide learning abilities and better decision-making in networking control, as well as allow operating i-IoT effectively, as it continues to grow and evolve, to achieve optimal user experience (QoS). One of the essential obstacles facing IoT researchers belongs to preparing and processing huge amounts of data [29]. Accordingly, ML and Data Mining (DM) are widely used to improve the performance of cyber-attack detection and prevention systems [30], and to increase the security of transmitting sensitive data to the public cloud. An integration between Multilayer Perceptron Neural Networks (MLP) and Particle Swarm Optimization Algorithm (PSO) was employed in [31].

To sum up, integrating the DL algorithms for the 6G and beyond technologies leads to potential security problems. Mainly, most of the studies focus on building DL algorithms for the 6G communication problems and ignore the security concerns. The mmWave beam prediction for several BSs with multiple users can provide satisfied results by using DL algorithms for different environmental scenarios. However, most of the proposed DL methods cannot work as expected under an attack. The beamforming method may seem naturally secure because it transmits signals in desired directions. More specifically, security can be further guaranteed from the viewpoint of physical security when the beamforming vector is appropriately designed. On the other hand, in DL models, the malicious user can penetrate the legitimate users' device or generate a copy of the users' signal to impersonate users with malicious software. For this, the security concerns for DL models for wireless communication are different from the traditional wireless communication systems. Based on the shortcomings of the literature in regard to security issues, in this paper, we deal with the security problem of DL application for beamforming prediction.

We consider two research questions: (i) Is the proposed DL-based mmWave beam prediction model vulnerable to the adversarial attacks, (ii) Is iterative adversarial training [32] able to mitigate adversarial attacks. First, we implemented a beam prediction algorithm using a DL model to answer these questions. Secondly, we attack the beam prediction algorithm with the Fast-Gradient Sign Method (FGSM) [32], an essential and powerful attack for DL models. FGSM adds the craftily created noise whose direction is the same as the cost function gradient for the input data. Eventually, we compare the mean square error (MSE) values of the undefended DL model and attack the DL model with FGSM. The MSE value increases about 40.14 times higher with the attack. Thirdly, we proposed an adversarial training-based mmWave beam prediction model (i.e., defended model) to protect the model against FGSM adversarial ML attacks. In addition to the beam prediction, our new DL model learns the attack noise injection patterns and trains itself with manipulated input data, denoted as adversarial training. Wireless communication systems are generally built on complex numbers (i.e., real and imaginary parts). On the other hand, current adversarial ML attacks work with real numbers. Therefore, within the scope of this study, we could not use attack tools such as Foolbox,[1] Adversarial Robustness Toolbox[2] or Cleverhans,[3] which are frequently used in the industry. Instead, we implemented the FGSM attack compatible with complex numbers. A proposed solution to this is to use complex numbers as input and output of adversarial training and attack functions. This way, the output of the adversarial function would be a real number and not a complex number. Then, we implemented the attack function. This attack generates malicious inputs for the DL model with complex numbers as input and complex numbers output. It is showed that the modified FGSM attack can be used to fool ML models that are potentially used in the 6G industry in the future.

In our recent work [33], we deployed adversarial training based mitigation method for the DL based beamforming prediction model in O1 ray tracing scenario that is in an open area. The training dataset's pattern was limited only to one scenario. Here, we generalize the adversarial training based mitigation method to the different scenarios; (i) Outdoor scenario, (ii) Outdoor scenario with LOS and blocked users, and (iii) Indoor scenario with distributed massive MIMO.

[1] https://github.com/bethgelab/foolbox

[2] https://github.com/Trusted-AI/adversarial-robustness-toolbox

[3] https://github.com/cleverhans-lab/cleverhans

This study aims to make a more secure DL-based mmWave beam prediction against attack for the DL model. The future of wireless communication must consider using AI models. The attack against AI models is different from well-known wireless physical layer security achieved by exploiting the properties of the physical layer, as the name suggests, such as interference (unwanted signals disrupt wireless communication), thermal noise (also referred to as white noise), channel information (to detect and prevent spoofing attacks), jamming (the deliberate interference with or blocking of such communications), etc. The purpose of the attack on wireless physical layer security is to make the transmitted signal non-predictive to decrease the secrecy capacity. In this way, the legitimate users could not demodulate the transmitted signal. On the other hand, the purpose of the attacks against the DL models is to manipulate the transmitted data. The attacker imitates the legitimate user. In this case, an attack model is developed for the BS to mimic the user's transmitted signal.

It is essential to improve the performance of algorithms against the adversarial threats of evasion, poisoning, extraction, and inference. This study also presents the adversarial learning mitigation method's performance for AI algorithms used in 6G networks to predict RF beamforming vectors. More precisely, the potential application areas of the proposed concepts represent a quite large spectrum, especially in the fields of energy, health, and transportation. For instance, state-of-the-art and upcoming telemedicine applications such as tele-surgery use cases can be considered as potential application areas. Besides, vehicle-to-infrastructure (V2X) and vehicle-to-vehicle (V2V) communication use cases appears to be one of the high potential areas of 5G and possibly for 6G related infrastructure. Furthermore, the energy domain is also a very fruitful ecosystem where the similar or derivative proposed concepts can be applied. Especially, the energy use cases where the expected response times are close to real-time and where cyber–physical resilience plays an important role, the proposed approach can be quite handy and applicable.

1.1. Contributions

The principles of traditional wireless communication system models and DL-based models are different. Wireless communication systems are not prediction or approximation-based. On the other hand, a typical DL model trains its neuron weights to extract the relationship between the input and output of a system. The resulting predictive model is defined as the decision boundaries of the input data. The final decision boundaries are nonlinear lines that separate the outputs, unlike the traditional wireless communication model. For instance, at the energy detection model [34], the input values compare with a threshold value to decide false and true regions. Here, the boundary of the false and true region is a linear function. Therefore, it is possible to detect a slight change in the input signal. On the other hand, if the predicted boundary is nonlinear, it causes vulnerabilities. It is open for adversarial ML attacks. We choose the most common and powerful attacking method for the DL model that is FGSM. This attack model maximizes the lost values of the classifier by adding a modest noise vector. While the traditional FGSM attack only uses real numbers to manipulate data, we modified the FGSM attack model to change the transmitted signal's amplitude and phase values with complex numbers. Thus, our main contributions for this paper are listed as below:

- We show that an undefended DL-based mmWave beam prediction model system is vulnerable against carefully designed adversarial noise.
- We modified the FGSM attack to manipulate the transmitted signal in the complex domain for amplitude and phase values. After the attack, the system achievable rate performance became inoperable.

- We trained an undefended DL-based mmWave beam prediction model by adversarial training with the FGSM attack. Therefore, the system achievable rate performance became very close to the undefended model without attack.

We implemented the proposed model with three scenarios; outdoor, outdoor with LOS and blocked users, and indoor environment. Each scenario is executed under three cases that undefended, undefended under attack and defended model to answer two research questions.

1.2. Organization

The rest of the paper is organized as follows: Section 2 describes background information about adversarial ML and adversarial training-based mitigation methods. Section 3 shows our system overview. Section 4 evaluates the proposed mitigation method for DL based mmWave beam prediction vulnerabilities, and Section 5 concludes this paper.

2. Preliminaries

2.1. Using machine learning models to estimate RF beamforming vectors

Using the benefits of DL algorithms gives a novel solution for a massive MIMO channel training and scanning of a large number of narrow beams. The beams depend on the environmental conditions, such as user and BSs locations, furniture, trees, buildings etc. It is challenging to define all these environmental conditions as a closed-form equation. A good alternative is to use omni and quasi-omni beam patterns to predict the best RF beamforming vectors. We are using these beam patterns benefits to consider the reflection and diffraction of the pilot signal. This research uses the DL models for mmWave beam prediction in [10], thanks to their mathematical calculations.

The DL solution consists of two states: training and prediction. The DL model uses uplink pilot signals, which is omni-received pilots, received at the terminal BSs to learn and predict the best beamforming vectors. Firstly, the DL model learns the beams according to the omni-received pilot at the terminal BSs, i.e., which can be captured with negligible training overhead. Secondly, the model uses the trained data from the training stage using the omni-received pilots to predict the best RF beamforming vector for the current condition.

2.1.1. Training steps

In our system model, beamforming prediction models are in the BSs. The cloud is only responsible for precoding the transmitted signals and sending them to the BSs. The user sends uplink training pilot sequences for each beam coherence time T_B. Beam coherence time is the average time duration over which the beams stay aligned. BSs combine received pilot sequences on RF beamforming vector and feed them to the cloud. To describe the channel for the estimate, pilot signals are employed. Each terminal delivers pilot sequences uplink data in a synchronized manner to the BSs, which utilize the pilots for channel estimation and precoding. The cloud uses the received sequences from all the BSs as the input of the DL algorithm to find the achievable rate in (1) for every RF beamforming vector to represent the desired outputs,

$$R_n^{(p)} = \text{argmax}\frac{1}{K}\sum_{n=1}^{N}\log_2\left(1 + SNR|\mathbf{h}_{k,n}^T\mathbf{g}_p|^2\right) \quad (1)$$

where $\mathbf{g}_p$ is the channel coefficient for omni-beams, and $\mathbf{h}_{k,n}$ is channel coefficient for nth BS at the kth subcarrier.

2.1.2. Learning steps

In this stage, the trained DL model is used to predict the RF beamforming vectors. Firstly, the user sends an uplink pilot sequence. The BSs combine these sequences and send them to the cloud. Then, the cloud uses the trained DL model to predict the best RF beamforming vectors to maximize the achievable rate for each BS. Finally, BSs use the predicted RF beamforming vectors to estimate the effective channel $\mathbf{h}_{k,n}$.

3. System model

In this section, fundamentals of the adversarial ML are presented followed by modified FGSM attack for the 6G Networks in beam prediction model.

3.1. Attack to machine learning algorithms: Adversarial machine learning

Basically, adversarial ML is an attack technique that attempts to fool neural network models by supplying craftily manipulated input with a slight difference [35].

Attackers apply model evasion attacks for phishing attacks, spams, and executing malware code in an analysis environment [36]. There are also some advantages to attackers in misclassification and misdirection of models. In such attacks, the attacker does not change training instances. Instead, it tries to make some small perturbations in input instances in the model's inference time to make this new input instance seem safe (i.e., normal behavior) [37]. We mainly concentrate on this kind of adversarial attack in this study. There are many attacking methods for DL models, and the FGSM is the most straightforward and powerful attack type. We only focus on the FGSM attack, but our solution to prevent this attack can be applied to other adversarial ML attacks. FGSM works by utilizing the gradients of the neural network to create an adversarial example to evade the model. For an input instance $\mathbf{x}$, the FGSM utilizes the gradients ∇_x of the loss value ℓ for the input instance to build a new instance $\mathbf{x}^{adv}$ that maximizes the loss value of the classifier hypothesis h. This new instance is named the adversarial instance. We can summarize the FGSM using the following explanation:

$$\mathbf{x}^{adv} = \mathbf{x} + \epsilon \cdot sign(\nabla_x \ell(\boldsymbol{\theta}, \mathbf{x}, y)) \quad (2)$$

By adding a slowly modest noise vector $\eta \in \mathbb{R}^n$ whose elements are equal to the sign of the features of the gradient of the cost function ℓ for the input $\mathbf{x} \in \mathbb{R}^n$, the attacker can easily manipulate the output of a DL model. The Fig. 1 shows the details of the FGSM attack.

Attackers can get involved in the system by using different ways such as mobile malware applications, copying mobile BSs. An attacker can be a device or an application in addition to a human. Attack transferability achieves an attack against a DL model to be valid against a different, unknown model. In the attack transferability paradigm, one attacker can build another DL model to extract the decision boundaries of the input data. Then the attacker can create the adversarial samples using its own model's vulnerabilities. Experimental confirmation for attack transferability has been shown in recent works [38].

3.2. Attack to training steps: Adversarial training

Adversarial training is a widely recommended defense technique that implies generating adversarial instances using the gradient of the victim classifier and then re-training the model with the adversarial instances and their respective labels. This technique has been demonstrated to be efficient in defending models from adversarial attacks [39,40].

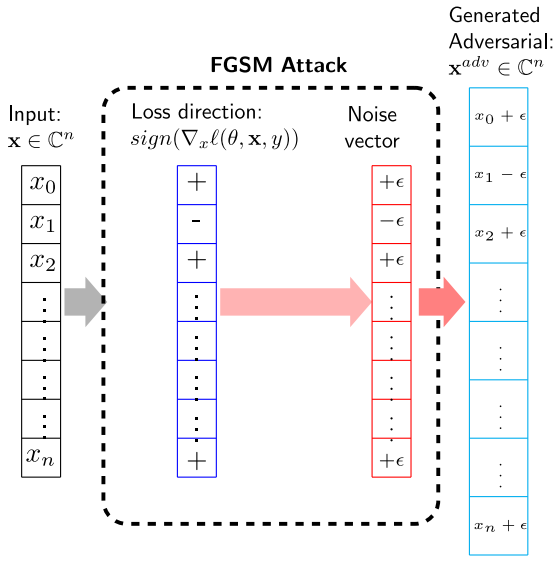


Fig. 1. FGSM attack steps. The input vector $\mathbf{x} \in \mathbb{C}^n$ is poisoned with loss maximization direction.

Let us first think of a common classification problem with training instances $X \in \mathbb{R}^{m \times n}$ of dimension d, and a label space Y. It is assumed that the classifier h_θ has been trained to minimize a loss function ℓ as follows:

$$\min_{\theta} \frac{1}{m} \sum_{i=1}^{m} \ell(h_\theta(\mathbf{x}_i, y_i)) \tag{3}$$

Given a classifier model $h_\theta(\cdot)$ and an input instance x with a responding output y, then an adversarial instance x^{adv} is an input such that:

$$h_\theta(x^{adv}) \neq y \quad \wedge \; d(x, x^{adv}) < \epsilon \tag{4}$$

where $d(\cdot, \cdot)$ is the distance metric between two input instances, the original input x and the adversarial version x^{adv}. Most actual adversarial model attacks transform Eq. (4) into the following optimization problem:

$$\underset{x}{arg\,max}\; \ell\left(h_\theta(x^{adv}), y\right) \tag{5}$$

$$s.t. \quad d(x, x^{adv}) < \epsilon \tag{6}$$

where ℓ is the loss function between predicted output $h(\cdot)$ and correct label y. In order to mitigate such attacks, at per training step, the conventional training procedure from Eq. (3) is replaced with a `min-max` objective function to minimize the expected value of the maximum loss, as follows:

$$\min_{\theta} \mathbb{E}_{(x,y)} \left(\max_{d(x, x^{adv}) < \epsilon} \ell(h(x^{adv}), y) \right) \tag{7}$$

3.3. Modified FGSM attack and its application in 6G networks

The mmWave communication system employs a massive amount of antennas with beamforming to control a wave-front direction by weighting the magnitude and phase in each antenna. We assume that each BS has one RF chain to provide analogue beamforming architecture that is not as expensive and complex as the other approaches in [41]. The mmWave communication system model is given in Fig. 2. Here, N is the number of BSs serving one mobile user with an equipped single antenna. A centralized/cloud processing unit is used to connect all BSs and processing.

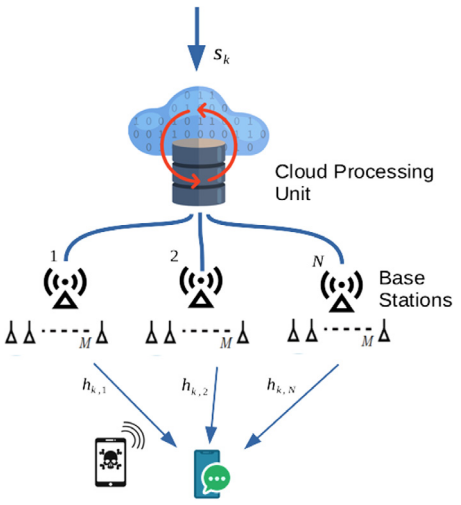


Fig. 2. Block diagram of the mmWave beamforming system. Here N and M are the number of the BS and antenna respectively.

The downlink received signal at kth subcarrier is expressed as

$$\mathbf{y}_k = \sum_{n=1}^{N} \mathbf{h}_{k,n}^T \mathbf{x}_{k,n} + v_k \tag{8}$$

where $\mathbf{h}_{k,n}$ denotes the channel vector between nth BS and the user. v_k is additive white Gaussian noise (AWGN) with variance σ^2, i.e., $N(0, \sigma^2)$ for kth subcarrier. Here, $\mathbf{x}_{k,n}$ is transmitted complex baseband signal from the kth subcarrier and nth BS is given as

$$\mathbf{x}_{k,n} = \mathbf{f}_n c_{k,n} s_k \tag{9}$$

where s_k is the data symbol $\mathbf{s} = [s_1, s_2, \ldots, s_K]$ with K subcarriers is firstly precoded by code vector $\mathbf{c}_{k,n} = [c_{k,1}, c_{k,2}, \ldots, c_{k,N}]^T$ at each subcarrier on each BS. Then, every BS applies analog beamforming with beam steering vector $\mathbf{f}_n$ to obtain downlink transmitted signal $\mathbf{x}_{k,n}$. The beam steering vector defines for each BS antenna as $[\mathbf{f}_n]_m = \frac{1}{\sqrt{M}} e^{j\theta_{n,m}}$ where $\theta_{n,m}$ is a quantized angle. To support mobile users, beamforming vectors are recalculated constantly beamforming vectors within channel coherence time, denoted T_C which depends on user mobility and channel multi-path components. Also, the beams stay aligned on beam coherence duration, denoted T_B, and T_C is usually shorter than T_B [42]. The time duration of T_B decreases for the users with higher mobility that causing to lower data rate for the same beamforming vectors and beam training overhead. Thus, the effective achievable rate is defined as follow.

$$R_{eff} = \left(1 - \frac{T_{TR}}{T_B}\right) \sum_{k=1}^{K} \log_2 \left(1 + SNR \left| \sum_{n=1}^{N} \mathbf{h}_{k,n}^T \mathbf{f}_n c_{k,n} \right|^2 \right) \tag{10}$$

Here, the beamforming vectors are redesigned in each first training time T_{TR} in beam coherence time, T_B and the rest of it is used for the data transmission by using the redesigned beamforming vectors.

The traditional FGSM attack succeeds in classification models whose input type is real numbers ($\mathbf{x} \in \mathbb{R}^m$). However, the data used in the field of communication systems consist of complex numbers ($\mathbf{x} \in \mathbb{C}^m$) with a real and an imaginary part. For this reason, the FGSM attack needs to be modified for inputting complex numbers in mmWave estimation. For this purpose, we updated the FGSM attack as shown in Algorithm 1 to be used in 6G beyond technologies.

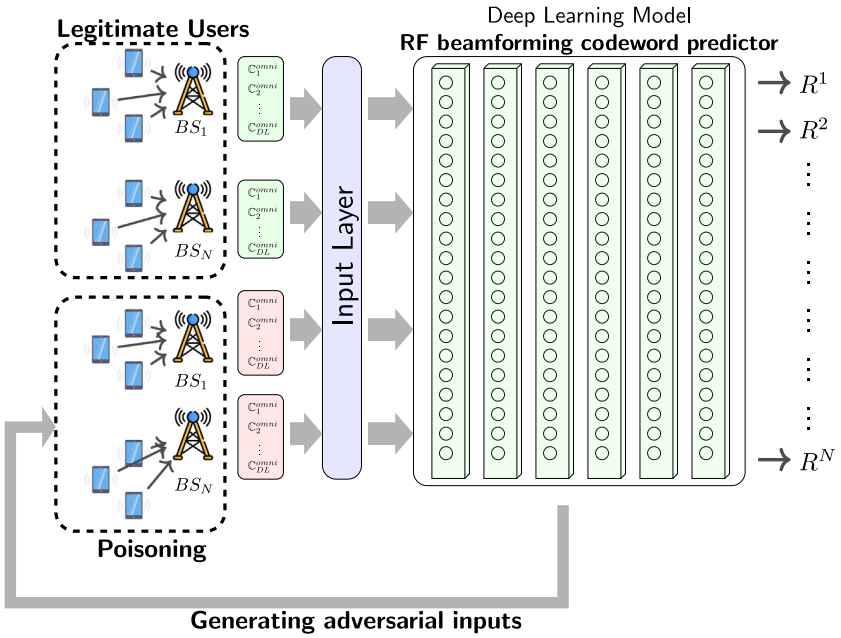


Fig. 3. The diagram of RF beamforming codeword adversarial training.

Algorithm 1: Algorithm for FGSM (complex numbers based). $\mathbf{x} \in \mathbb{C}^n$ is the benign input, F is the DL model function, N is the number of iterations, α is the maximum allowed perturbation, ϵ is the step size,

Input: $\mathbf{x} \in \mathbb{C}^m, \mathbf{y} \in \mathbb{R}^n, F, \epsilon, \alpha$
Output: $\mathbf{x}_{t+1}$
/* convert $\epsilon \in \mathbb{R}$ from real number domain to $\epsilon\_complex \in \mathbb{C}$ complex domain where $Re\{\epsilon\_complex\} = \epsilon$ and $Im\{\epsilon\_complex\} = \epsilon$ */
$\epsilon\_complex \leftarrow (\epsilon + \epsilon \cdot j)$
$\mathbf{x}_0 \leftarrow \mathbf{x}$
while $n < N$ **do**
  /* update $\mathbf{x}$ using the loss direction */
  $\mathbf{x}_{(t+1)} = clip_{\mathbf{x},\epsilon}(\mathbf{x}_t + \epsilon\_complex \cdot sign(\nabla_{\mathbf{x}} \ell(\mathbf{x}_t, F, \mathbf{y})))$
  // If the distance between manipulated input's prediction and real output is greater than α
  if $distance_{Euclidian}(F(\mathbf{x}_{t+1}) - \mathbf{y}) \geq \alpha$ **then**
    end while
  end
end
return $\mathbf{x}_{t+1}$

3.4. Adversarial training

Fig. 3 shows the adversarial training process. After the model is trained, adversarial inputs are created using the model itself, combined with legitimate users' information and added to the training. When the model reaches the steady-state, the training process is completed. In this way, the model will predict RF beamforming codeword for legitimate users while being immune to the craftily designed noise attack that will be added as input.

3.5. Capability of the attacker

We assumed that the attacker's primary purpose is to manipulate the RF model by applying carefully crafted noise to the input data. In a real-world scenario, this white-box setting is the most desired choice for an attacker that does not take the risks of being caught in a trap. The problem is that it requires the attacker to access the model from outside to generate adversarial examples. After manipulating the input data, the attacker can exploit the RF beamforming codeword prediction model's vulnerabilities in the same manner as in an adversary's sandbox environment. The prediction model predicts the adversarial instances when the attacker can convert some model's outputs to other outputs (i.e., wrong prediction). However, to prevent this noise from being easily noticed, the attacker must answer an optimization problem to determine which regions in the input data must be modified. By solving this optimization problem using one of the available attack methods [36], the attacker aims to reduce the prediction performance on the manipulated data as much as possible. In this study, to limit the maximum allowed perturbation for the attacker, we used l_∞ norm, which is the maximum difference limit between original and adversarial instances. Fig. 4 shows the attack scenario. The attacker gets a legitimate input, $\mathbf{x}$, creates a noise vector with an ϵ budget $\eta = \epsilon \cdot sign(\nabla_x \ell(\boldsymbol{\theta}, \mathbf{x}, y))$, sums the input instance and the craftily designed noise to create adversarial input $\mathbf{x}^{adv} = \mathbf{x} + \eta$.

4. Experiments

In the experiments, we tested our model with three different cases for three different scenarios. The cases are given as:

- **Case 1:** Undefended model: We implement undefended DL-based mmWave beam prediction model which is vulnerable to attacks.
- **Case 2:** Undefended model under FGSM attack: We attack with FGSM to undefended model to obtain an achievable rate of the DL model under attack. It is the worst case of the model that needs to be overcome.
- **Case 3:** Defended model: DL-based mmWave beam prediction model is adversarial trained against FGSM attack.

Fig. 5 shows the experiments overview all cases.

The outcomes of these three cases allow us to compare the model performance under attack with undefended and secure cases. Also, we implemented the proposed model for different

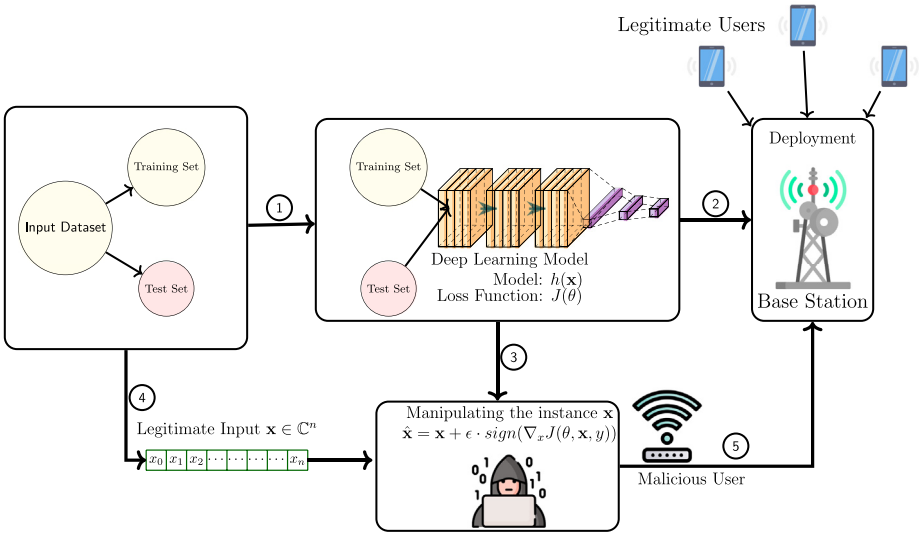


Fig. 4. RF Beamforming manipulation process.

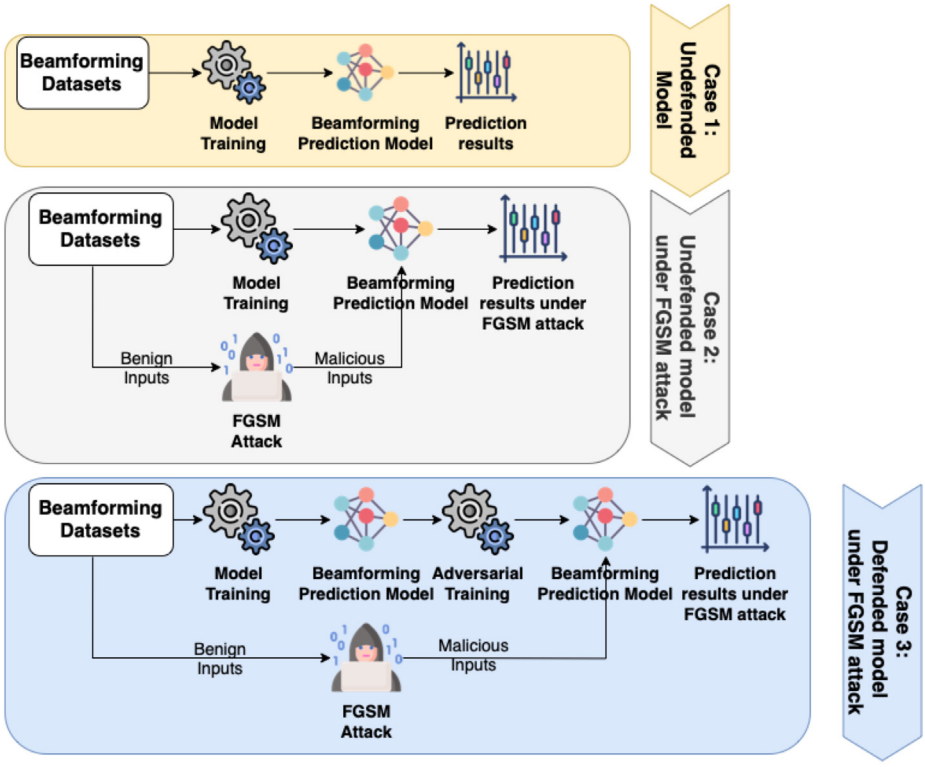


Fig. 5. Experiments overview.

scenarios including outdoor and indoor scenarios with the details below [43]:

Scenario 1 — Outdoor scenario: This is an outdoor scenario of two streets with an intersection as shown in Fig. 6. The scenario includes 18 BSs with 16 × 16 uniform planar array (UPA) and uniformly distributed more than one million users with a single dipole antenna in 3 user grids. The operating frequency is 60 GHz.

Scenario 2 — Outdoor scenario with LOS and blocked users: It is also an outdoor scenario with LOS and blocked users is given in Fig. 7. There is a single BS with LOS connections with some users and NLOS connections with other users. The operating frequency is 3.5 GHz.

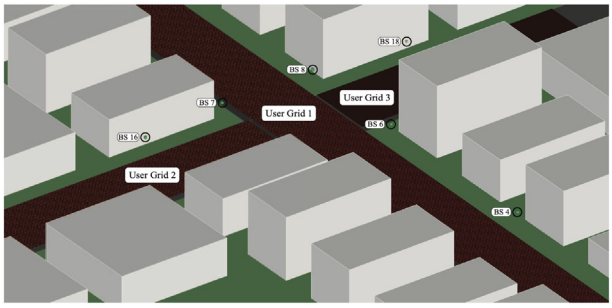


Fig. 6. Scenario 1 — Outdoor scenario [43].

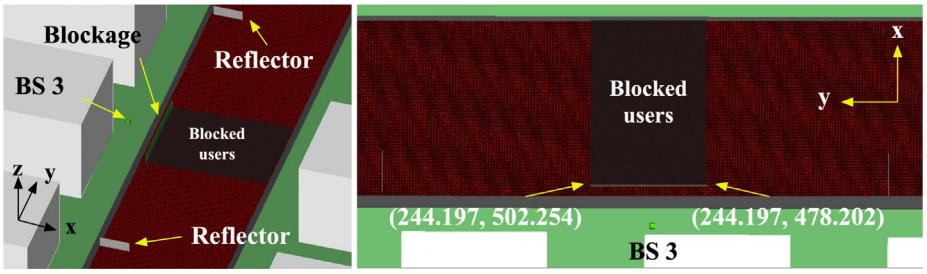


Fig. 7. Scenario 2 — Outdoor scenario with LOS and blocked users [43].

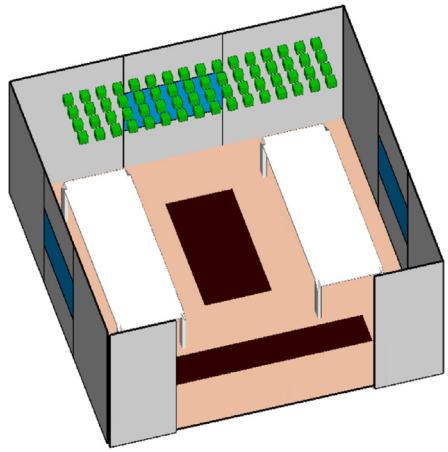


Fig. 8. Scenario 3 — Indoor scenario with distributed massive MIMO [43].

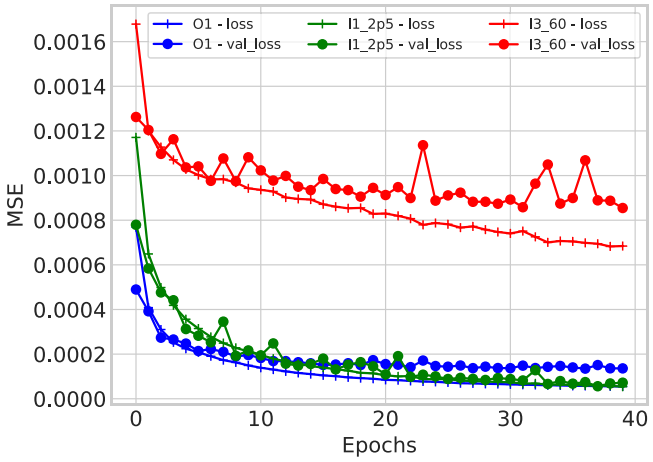


Fig. 9. The beamforming prediction model training history.

Table 1
Model architecture.

Layer type	Layer information
Fully Connected + ReLU	100
Fully Connected + ReLU	100
Fully Connected + ReLU	100
Fully Connected + TanH	1

Table 2
Millimeter-wave beam prediction model parameters.

Parameter	Value
Optimizer	Adam
Learning rate	0.01
Batch Size	100
Dropout Ratio	0.25
Epochs	10

Scenario 3 — Indoor scenario with distributed massive MIMO: It is for indoor 10 $m \times 10m$ room scenario and 64 antennas tiling up part of the ceiling at the height of 2.5 m from the floor that is given in Fig. 8. The operating frequencies are 2.4 GHz and 2.5 GHz.

The main objective of these cases is to maximize the system effective achievable rate for the system under attack in Eq. (10). We performed the experiments using the Python scripts and ML libraries: Keras, Tensorflow, and Scikit-learn, on the following machine: 2.8 GHz Quad-Core Intel Core i7 with 16 GB of RAM. For all scenarios, two models, undefended and defended (i.e., adversarial trained), were built to obtain prediction results. In the first model, the model is trained without any input poisoning. The first model (i.e., undefended model) was used with legitimate users (for C1) and adversaries (for C2). The second model (i.e., the defended model) was used under the FGSM attack. The hyperparameters such as the number of hidden layers and the number of neurons in the hidden layers, the activation function, the loss function, and the optimization method are the exactly same for both models.

The model architectures and selected hyperparameters are given in Table 1 and in Table 2 respectively.

4.1. Research questions

We consider the following two research questions (RQs):

- **RQ1**: Is the DL-based RF beamforming codeword predictor vulnerable to adversarial ML attacks?
- **RQ2**: Is the iterative adversarial training approach a mitigation method for the adversarial attacks in beamforming prediction?

4.2. RF beamforming data generator

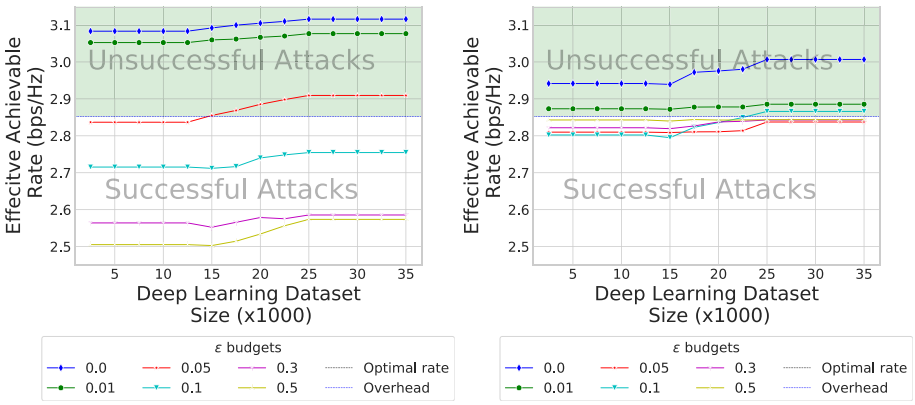
We employed the generic DL dataset for millimeter-wave and massive MIMO applications (DeepMIMO) data generator in experiments [44].

This section conducts experiments on the mmWave communication and massive MIMO applications dataset from the publicly available dataset repository. The proposed mitigation method using Keras and TensorFlow libraries was implemented in the Python environment.

4.3. Results for RQ1

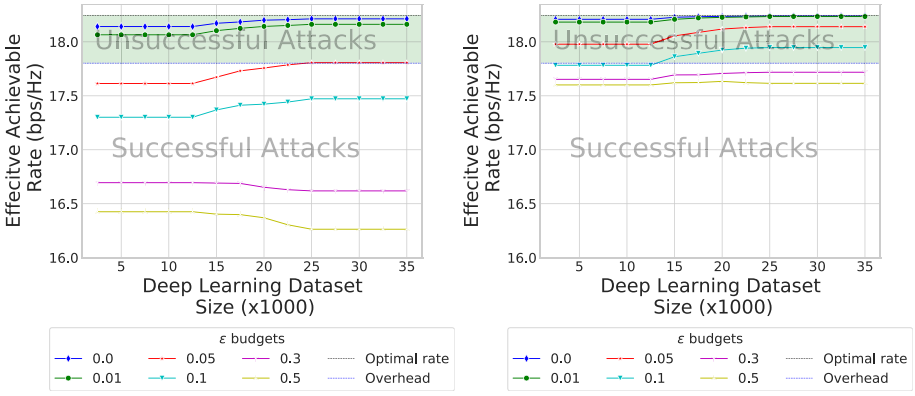
Fig. 9 shows the training history of the beamforming prediction model with 35,000 training instances. The model is trained with clean (i.e., non-perturbated) instances.

Figs. 10–12 show the original undefended and defended model under FGSM attack. Genie-aided coordinated beamforming is the



(a) Undefended (b) Defended

Fig. 10. Beamforming codeword DL model results for Scenario-1 for different values of ϵ.



(a) Undefended (b) Defended

Fig. 11. Beamforming codeword DL model results for Scenario-2 for different values of ϵ.

optimal beamforming vector with no training overhead and baseline coordinated beamforming is calculated with conventional communication system tools [10]. According to the simulation results, the DL model's predictions are very close to the original value. We have used l_∞ norm as the distance metric, which shows the maximum allowable perturbation amount for each item in the input vector **x**. The green area in the figures shows the acceptable range between optimal and overhead limits. As can be seen from the figures, the predictive performance results of the vulnerable models fall below the green zone with shallow epsilon values. For the results of the models that have been robust with adversarial training to show low performance (i.e., to fall below the green zone), the attacker must use a very high epsilon value. A high epsilon value (i.e., more noise) will cause the attacker to be exposed. Therefore, we can say that the adversarial training method protects the DL model against the FGSM attack.

According to the results, the undefended RF beamforming codeword prediction model is vulnerable to the FGSM attack. The MSE performance result of the model under attack is approximately 40 (i.e., $\frac{0.00843(Normal)}{0.00021(Attacked)} \approx 40.14$) times higher.

Concluding Remarks for RQ1: The prediction performance of DL-based RF beamforming codeword decreases along with increasing ϵ value for FGSM attack.

4.4. Results for RQ2

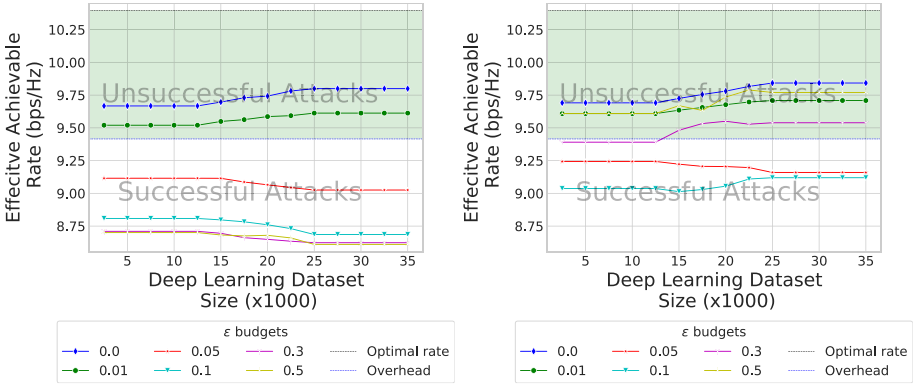
Adversarial training is a popularly advised defense mechanism [32,45] that proposes generating adversarial instances using the victim model's loss function and then re-training the model with the newly generated adversarial instances and their respective outputs. This approach has proved to be effective in protecting DL models from adversarial ML attacks. Fig. 13 shows the MSE of the performance results for all scenarios with the FGSM attack. According to the figure, defended (adversarial trained) model's MSE values becomes steady-state after a specific ϵ value. On the other hand, the undefended model's MSE values continue to increase.

Table 3 shows the beamforming codeword prediction results for all scenarios for different values of ϵ. The overhead (lower) values for each scenario are 2.86 for O1, 17.81 for I1_2p5 and 9.41 for I3_60. According to the table, the attacker can manipulate the DL model with $\epsilon = 0.06$ for the O1 scenario. The undefended model's prediction result is 2.85426, which is lower than the overhead value, i.e., 2.86. Similarly, the ϵ values for the successful attacks are 0.05 for I1_2p5 and 0.03 for I3_60.

Concluding Remarks for RQ2: Adversarial training with FGSM attack increases each scenario's DL model's prediction performance.

4.5. Threats to validity

A key *external validity* threat is related to the generalization of results [46]. We used only the RF beamforming dataset in experiments, and we need more case studies to generalize the results. Moreover, the dataset reflects different types of mmWave beams.



(a) Undefended (b) Defended

Fig. 12. Beamforming codeword DL model results for Scenario-3 for different values of ϵ.

Table 3
Beamforming codeword prediction results for all scenarios for different values of ϵ.

ϵ	O1		I1_2p5		I3_60	
	Undef.	Def.	Undef.	Def.	Undef.	Def.
0.00	3.11594	3.00674	18.21316	18.23962	9.79951	9.84233
0.01	3.07667	2.88551	18.16247	18.23461	9.61264	9.70870
0.02	3.03850	2.85323	18.07253	18.22359	9.45940	9.57484
0.03	2.99991	2.83773	17.98412	18.20262	9.22683	9.38894
0.04	2.94373	2.87103	17.90667	18.17553	9.06634	9.26890
0.05	2.90929	2.83736	17.80715	18.14055	9.02542	9.15959
0.06	2.85426	2.89408	17.77563	18.09840	8.89587	9.12542
0.07	2.81551	2.83269	17.69611	18.05923	8.84408	9.02040
0.08	2.81535	2.89524	17.61604	18.03128	8.73619	9.05983
0.09	2.76199	2.80589	17.57838	17.98539	8.80412	9.12413
0.10	2.75456	2.86601	17.47225	17.94672	8.68579	9.11946
0.20	2.65541	2.83044	17.01810	17.83537	8.61330	9.51652
0.30	2.58553	2.84275	16.61877	17.71839	8.62319	9.53898
0.40	2.56208	2.84106	16.36651	17.68828	8.56926	9.64404
0.50	2.57365	2.84363	16.26341	17.61559	8.61028	9.77017

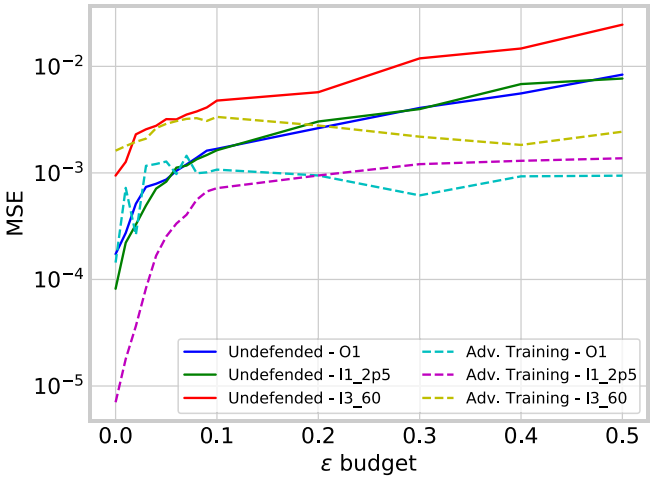


Fig. 13. The performance results for all scenarios.

The key *construct validity* threat is related to the selection of attack type FGSM. Nevertheless, note that this attack is from the literature [46] and applied to several DL usage domains. In the future, we will conduct dedicated empirical studies to investigate more adversarial ML attacks systematically.

The main *conclusion validity* threat is due to finding the best attack budget ϵ that is responsible for manipulating the legitimate user's signal for poisoning the beamforming prediction model. To mitigate this threat, we repeated each experiment 20 times to reduce the probability that the results were obtained by chance. In standard neural network training, all weights are initialized uniformly at random. In the second stage, using optimization, these weights are updated to fit the classification problem. Since the training started with a probabilistic approach, there is a possibility of facing optimization's local minimum problem. We repeat the training 20 times to find the ϵ value that gives the best attack result to eliminate the local minimum problem. In each repetition, the weights were initialized uniformly at random but with different values. If the optimization function failed to find the global minimum in the next experiment, it is likely to see it, as the weights have been initialized with different values.

5. Conclusions and future works

This study emphasizes cyber-security issues related to RF beamforming codeword prediction models' vulnerabilities by satisfying the following research questions: (1) Is the DL-based RF beamforming codeword predictor vulnerable against adversarial ML attacks? (2) Is the iterative adversarial training approach a mitigation method for the adversarial attacks in beamforming prediction? The experiments were performed with the DeepMIMO's *O1, I1_2p5 and I3_60 ray-tracing* scenarios to answer these questions. The results confirm that the original model is vulnerable to a modified FGSM type of attack. The empirical results also show that the proposed mitigation method, i.e., iterative adversarial training approach, successfully increases the RF beamforming prediction performance and creates a more accurate predictor, suggesting that the strategy can improve the predictor's performance. The attacker must increase the epsilon value from 0.05 to 0.06 for the O1 scenario, from 0.04 to 0.2 for the I1_2p5 scenario, and from 0.02 to 0.02 for the I3_60 scenario in order to perform a successful attack. Due to the higher epsilon value, the probability of the attack being detected by another security component also increases. As future work, the outcomes of this study has the potential to be further used and developed for other future studies to gain more insights into the field of 6G networks, where adversarial DL based cyber-security risks will increase.

CRediT authorship contribution statement

Ferhat Ozgur Catak: Conceptualization, Methodology, Software, Writing – review & editing. **Murat Kuzlu:** Data curation, Writing – original draft, Writing – review & editing. **Evren Catak:** Writing – review & editing. **Umit Cali:** Writing – review & editing. **Devrim Unal:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported in part by the Commonwealth Cyber Initiative, USA, an investment in the advancement of cyber R&D, innovation, and workforce development in Virginia. For more information about CCI, visit cyberinitiative.org.

References

[1] T.S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G.N. Wong, J.K. Schulz, M. Samimi, F. Gutierrez, Millimeter wave mobile communications for 5G cellular: It will work!, IEEE Access 1 (2013) 335–349, http://dx.doi.org/10.1109/ACCESS.2013.2260813.

[2] H. Viswanathan, P.E. Mogensen, Communications in the 6G era, IEEE Access 8 (2020) 57063–57074, http://dx.doi.org/10.1109/ACCESS.2020.2981745.

[3] E. Catak, L. Durak-Ata, Waveform design considerations for 5G wireless networks, in: Towards 5G Wireless Networks-A Physical Layer Perspective, IntechOpen, 2016, pp. 27–48.

[4] E. Catak, L. Durak-Ata, Adaptive filterbank-based multi-carrier waveform design for flexible data rates, Comput. Electr. Eng. 61 (2017) 184–194, http://dx.doi.org/10.1016/j.compeleceng.2016.11.039.

[5] W. Roh, J. Seol, J. Park, B. Lee, J. Lee, Y. Kim, J. Cho, K. Cheun, F. Aryanfar, Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results, IEEE Commun. Mag. 52 (2) (2014) 106–113, http://dx.doi.org/10.1109/MCOM.2014.6736750.

[6] V. Jungnickel, K. Manolakis, W. Zirwas, B. Panzner, V. Braun, M. Lossow, M. Sternad, R. Apelfröjd, T. Svensson, The role of small cells, coordinated multipoint, and massive MIMO in 5G, IEEE Commun. Mag. 52 (5) (2014) 44–51, http://dx.doi.org/10.1109/MCOM.2014.6815892.

[7] F.W. Vook, A. Ghosh, T.A. Thomas, MIMO and beamforming solutions for 5G technology, in: 2014 IEEE MTT-S International Microwave Symposium (IMS2014), 2014, pp. 1–4, http://dx.doi.org/10.1109/MWSYM.2014.6848613.

[8] F. Boccardi, R.W. Heath, A. Lozano, T.L. Marzetta, P. Popovski, Five disruptive technology directions for 5G, IEEE Commun. Mag. 52 (2) (2014) 74–80, http://dx.doi.org/10.1109/MCOM.2014.6736746.

[9] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, D. Zhang, A survey on green 6G network: Architecture and technologies, IEEE Access 7 (2019) 175758–175768, http://dx.doi.org/10.1109/ACCESS.2019.2957648.

[10] A. Alkhateeb, S. Alex, P. Varkey, Y. Li, Q. Qu, D. Tujkovic, Deep learning coordinated beamforming for highly-mobile millimeter wave systems, IEEE Access 6 (2018) 37328–37348, http://dx.doi.org/10.1109/ACCESS.2018.2850226.

[11] M.S. Sim, Y. Lim, S.H. Park, L. Dai, C. Chae, Deep learning-based mmwave beam selection for 5G NR7/6G with sub-6 GHz channel information: Algorithms and prototype validation, IEEE Access 8 (2020) 51634–51646, http://dx.doi.org/10.1109/ACCESS.2020.2980285.

[12] Y. Wang, A. Klautau, M. Ribero, M. Narasimha, R.W. Heath, MmWave vehicular beam training with situational awareness by machine learning, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–6, http://dx.doi.org/10.1109/GLOCOMW.2018.8644288.

[13] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G.K. Karagiannidis, P. Fan, 6G wireless networks: Vision, requirements, architecture, and key technologies, IEEE Veh. Technol. Mag. 14 (3) (2019) 28–41, http://dx.doi.org/10.1109/MVT.2019.2921208.

[14] K.B. Letaief, W. Chen, Y. Shi, J. Zhang, Y.-J.A. Zhang, The roadmap to 6G:AI empowered wireless networks, IEEE Commun. Mag. 57 (8) (2019) 84–90, http://dx.doi.org/10.1109/MCOM.2019.1900271.

[15] C. Yizhan, W. Zhong, H. Da, L. Ruosen, 6G is coming : Discussion on key candidate technologies and application scenarios, in: 2020 International Conference on Computer Communication and Network Security (CCNS), 2020, pp. 59–62, http://dx.doi.org/10.1109/CCNS50731.2020.00022.

[16] Y. Lu, Security in 6G: The prospects and the relevant technologies, J. Ind. Integr. Manag. 5 (03) (2020) 271–289.

[17] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, Security and privacy in 6G networks: New areas and new challenges, Digit. Commun. Netw. 6 (3) (2020) 281–291.

[18] A. Chorti, A.N. Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, H.V. Poor, Context-aware security for 6G wireless the role of physical layer security, 2021, arXiv preprint arXiv:2101.01536.

[19] Y. Xiao, G. Shi, Y. Li, W. Saad, H.V. Poor, Toward self-learning edge intelligence in 6G, IEEE Commun. Mag. 58 (12) (2020) 34–40, http://dx.doi.org/10.1109/MCOM.001.2000388.

[20] M. Kuzlu, C. Fair, O. Guler, Role of artificial intelligence in the Internet of Things (IoT) cybersecurity, Discover Internet Things 1 (1) (2021) 1–14.

[21] Y. Sun, J. Liu, J. Wang, Y. Cao, N. Kato, When machine learning meets privacy in 6G:A survey, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2694–2724, http://dx.doi.org/10.1109/COMST.2020.3011561.

[22] Q. Liu, J. Guo, C.K. Wen, S. Jin, Adversarial attack on DL-based massive MIMO CSI feedback, J. Commun. Netw. 22 (3) (2020) 230–235, http://dx.doi.org/10.1109/JCN.2020.000016.

[23] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, W. Liu, Study and application on the architecture and key technologies for IoT, in: 2011 International Conference on Multimedia Technology, 2011, pp. 747–751, http://dx.doi.org/10.1109/ICMT.2011.6002149.

[24] R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future Internet: The Internet of Things architecture, possible applications and key challenges, in: 2012 10th International Conference on Frontiers Of Information Technology, 2012, pp. 257–260, http://dx.doi.org/10.1109/FIT.2012.53.

[25] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376, http://dx.doi.org/10.1109/COMST.2015.2444095.

[26] A. Rakotonirainy, O. Orfila, D. Gruyer, Reducing driver's behavioural uncertainties using an interdisciplinary approach: Convergence of quantified self, automated vehicles, Internet of Things and artificial intelligence, IFAC-PapersOnLine 49 (32) (2016) 78–82, Cyber-Physical & Human-Systems CPHS 2016. http://dx.doi.org/10.1016/j.ifacol.2016.12.193.

[27] H. Rahman, R. Rahmani, Enabling distributed intelligence assisted future internet of things controller (fitc), Appl. Comput. Inf. 14 (1) (2018) 73–87.

[28] O. Vermesan, A. Bröring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, C. Gallicchio, A. Micheli, M. Dragone, A. Saffiotti, et al., Internet of robotic things: converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT platforms, 2017.

[29] M.S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, A.P. Sheth, Machine learning for internet of things data analysis: a survey, Digit. Commun. Netw. 4 (3) (2018) 161–175, http://dx.doi.org/10.1016/j.dcan.2017.10.002.

[30] R. Shanbhogue, B. Beena, Survey of data mining (DM) and machine learning (ML) methods on cyber security, Indian J. Sci. Technol. 10 (35) (2017) 1–7.

[31] A.S. Saljoughi, M. Mehrvarz, H. Mirvaziri, Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms, Emerg. Sci. J. 1 (4) (2017) 179–191.

[32] I.J. Goodfellow, J. Shlens, C. Szegedy, Explaining and harnessing adversarial examples, 2014, ArXiv E-Prints arXiv:1412.6572.

[33] E. Catak, F.O. Catak, A. Moldsvor, Adversarial machine learning security problems for 6G: mmWave beam prediction use-case, in: 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2021, pp. 1–6, http://dx.doi.org/10.1109/BlackSeaCom52164.2021.9527756.

[34] H. Urkowitz, Energy detection of unknown deterministic signals, Proc. IEEE 55 (4) (1967) 523–531, http://dx.doi.org/10.1109/PROC.1967.5573.

[35] A. Kurakin, I. Goodfellow, S. Bengio, Adversarial machine learning at scale, 2016, ArXiv E-Prints arXiv:1611.01236.

[36] M. Aladag, F.O. Catak, E. Gul, Preventing data poisoning attacks by using generative models, in: 2019 1st International Informatics and Software Engineering Conference (UBMYK), 2019, pp. 1–5, http://dx.doi.org/10.1109/UBMYK48245.2019.8965459.

[37] O. Faruk Tuna, F. Ozgur Catak, M. Taner Eskil, Exploiting epistemic uncertainty of the deep learning models to generate adversarial samples, 2021, ArXiv E-Prints arXiv:2102.04150.

[38] A. Demontis, M. Melis, M. Pintor, M. Jagielski, B. Biggio, A. Oprea, C. Nita-Rotaru, F. Roli, Why do adversarial attacks transfer? Explaining transferability of evasion and poisoning attacks, 2018, ArXiv E-Prints arXiv:1809.02861.

[39] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, A. Vladu, Towards deep learning models resistant to adversarial attacks, 2017, ArXiv E-Prints arXiv:1706.06083.

[40] P. Benz, C. Zhang, A. Karjauv, I.S. Kweon, Robustness may be at odds with fairness: An empirical study on class-wise accuracy, in: L. Bertinetto, J.F. Henriques, S. Albanie, M. Paganini, G. Varol (Eds.), NeurIPS 2020 Workshop on Pre-Registration In Machine Learning, in: Proceedings of Machine Learning Research, vol. 148, PMLR, 2021, pp. 325–342.
[41] A. Alkhateeb, J. Mo, N. Gonzalez-Prelcic, R.W. Heath, MIMO precoding and combining solutions for millimeter-wave systems, IEEE Commun. Mag. 52 (12) (2014) 122–131, http://dx.doi.org/10.1109/MCOM.2014.6979963.
[42] V. Va, J. Choi, R.W. Heath, The impact of beamwidth on temporal channel variation in vehicular channels and its implications, IEEE Trans. Veh. Technol. 66 (6) (2017) 5014–5029, http://dx.doi.org/10.1109/TVT.2016.2622164.
[43] DeepMIMO Ray tracing scenarios, 2021, URL http://www.deepmimo.net/ray_tracing.html.
[44] A. Alkhateeb, DeepMIMO: A generic deep learning dataset for millimeter wave and massive MIMO applications, 2019, arXiv:1902.06435.
[45] T. Bai, J. Luo, J. Zhao, B. Wen, Q. Wang, Recent advances in adversarial training for adversarial robustness, 2021, ArXiv E-Prints arXiv:2102.01356.
[46] P. Runeson, M. Höst, R. Austen, B. Regnell, Case Study Research in Software Engineering – Guidelines and Examples, John Wiley and Sons Inc., United States, 2012.

Ferhat Ozgur Catak is an associate professor at the University of Stavanger, Norway. He completed his B.Sc. degree in electrical/electronic engineering in 2002 and his PhD degree in Informatics in 2014. Previously, he worked at TUBITAK in Turkey, NTNU and Simula Research laboratory in Norway. His research areas are cyber security, malware analysis, secure multi-party computation, and privacy methods.

Murat Kuzlu joined the Department of Engineering Technology, Old Dominion University (ODU) in 2018 as an Assistant Professor. He received his B.Sc., M.Sc., and Ph.D. degrees in Electronics and Telecommunications Engineering from Kocaeli University, Turkey, in 2001, 2004, and 2010, respectively. From 2005 to 2006, he worked as a Global Network Product Support Engineer at Nortel Networks, Turkey. In 2006, he joined the Energy Institute of TUBITAKMAM (Scientific and Technological Research Council of Turkey — The Marmara Research Center), where he worked as a senior researcher. Before joining ODU, he worked as a Research Assistant Professor at Virginia Tech's Advanced Research Institute. His research interests include smart grid, demand response, smart metering systems (AMR, AMI, AMM), home and building energy management systems, co-simulation, wireless communication, and embedded systems.

Evren Catak received the B.Sc. degree in Electrical and Electronics Engineering from Eskisehir Osmangazi University, Turkey in 2002, the M.Sc. degree in Electronics Engineering from Kadir Has University, Istanbul, Turkey in 2012, and the Ph.D. degree in Communication Engineering from Yildiz Technical University, Istanbul, Turkey in 2017. She is a postdoctoral fellow at the Norwegian University of Science and Technology. Her research interests are in the physical layer design of emerging communication systems, communication theory, signal processing, and wireless communications.

Umit Cali joined the Department of Electric Power Engineering, Norwegian University of Science and Technology, Norway in 2020 as an associate professor. He received the B.E. degree in electrical engineering from Yildiz Technical University, Istanbul, Turkey, in 2000, and the M.Sc. degree in electrical communication engineering and the Ph.D. degree in electrical engineering and computer science from the University of Kassel, Germany, in 2005 and 2010, respectively. He worked at the University of Wisconsin-Platteville and the University of North Carolina at Charlotte as an Assistant Professor between 2013 and 2020, respectively. His current research interests include energy informatics, artificial intelligence, blockchain technology, renewable energy systems, and energy economics. He is serving as an active Vice-Chair of\ the IEEE Blockchain in Energy Standards WG (P2418.5).

Devrim Unal is a Research Assistant Professor of Cyber Security at the KINDI Center for Computing Research, College of Engineering, Qatar University. He obtained his M.Sc. degree in Telematics from Sheffield University, UK and Ph.D. degree in Computer Engineering from Bogazici University, Turkey in 1998 and 2011, respectively. Dr. Unal's research interests include cyber–physical systems and IoT security, wireless security, artificial intelligence for cybersecurity, and blockchain.