Robust Massive MIMO Localization Using Neural ODE in Adversarial Environments

†Ushasree Boora, †Xuyu Wang, and ‡Shiwen Mao
†Department of Computer Science, California State University, Sacramento, CA 95819, USA
‡Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849-5201, USA
Email:uboora@csus.edu, xuyu.wang@csus.edu, smao@ieee.org

ICC 2022 - IEEE International Conference on Communications | 978-1-5386-8347-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICC45855.2022.9838836

***Abstract*—With the wide deployment of 5G communication systems, 5G massive multiple-input multiple-output (MIMO) has been shown effective not only to improve the spectrum efficiency and energy efficiency, but also provides location-based service (LBS) such as outdoor vehicle localization and indoor user localization. Recently, deep convolutional neural network (DCNN) has been applied for massive MIMO localization using channel state information (CSI) or angle-delay profile (ADP). However, the robustness of the DCNN model has not been explored in massive MIMO localization. In this paper, we study the impact of adversarial attack and defense (i.e., adversarial training) on massive MIMO localization using DCNN and the neural ordinary differential equation (ODE) model. We first introduce the massive MIMO system with respect to the channel model and ADP fingerprints, and then present the DCNN model and the neural ODE model for massive MIMO localization, as well as three types of white-box adversarial attacks and adversarial training. Finally, our experimental results validate that the proposed neural ODE with adversarial training could effectively improve the robustness of massive MIMO localization in indoor and outdoor environments.**

***Index Terms*—Massive MIMO Localization, Adversarial Examples, Deep Learning, Neural Ordinary Differential Equation.**

I. Introduction

As the rapid development of wireless systems and techniques, wireless applications, such as indoor and outdoor localization, are exploited to improve the quality of people's lives. Global positioning system (GPS) has been widely used for outdoor localization with a localization error about 5 m under line-of-sight (LOS) environments. However, GPS performs poorly in rich-scattering environments (e.g., indoors), since the GPS signal does not penetrate walls or other obstacles. Alternative wireless systems, such as long term evolution (LTE) and Long Range (LoRa), could be exploited for both outdoor and indoor localization [1], [2]. However, their accuracy is relatively low due to the limited bandwidth and small number of antennas at the base station (BS). For example, in urban environments, the localization error using LTE is about 80 m.

Massive multiple-input multiple-output (MIMO) is a key technology in 5G and beyond wireless communication systems to improve the spectrum efficiency and energy efficiency [3]. The large amount of antennas used in a massive MIMO system can be leveraged to achieve higher angle resolutions in multipath environments. In addition, the larger bandwidth used for 5G (e.g., 28 GHz mmWave) also helps to achieve higher delay domain resolutions [4], [5]. These unique features can be exploited to improve the performance of wireless localization systems. Specifically, angle of arrival (AOA) based methods, such as the rotational invariance technique (ESPRIT) and multiple signal classification (MUSIC), have been used for massive MIMO localization [6]. However, the rich multipath propagation in indoor and urban areas usually leads to multiple estimated AOA values; how to accurately recognize the line-of-sight (LOS) component in such environments is still a challenging problem [7]. In addition, the LOS path may not be available (i.e., in non-line-of-sight (NLOS) environments) when it is blocked, which results in the failure of many AOA-based methods.

Recently, there has been great interest in deep learning-based fingerprinting for indoor and outdoor scenarios, where satisfactory localization accuracy has been demonstrated, which outperforms the traditional geometric-based methods (e.g., AOA-based) in NLOS environments. This is because the wireless signals from NLOS paths can be exploited as location features with a deep neural network (DNN) model. For indoor localization, we have proposed several deep learning-based fingerprinting schemes using Wi-Fi channel state information (CSI) [8]. Similar to indoor localization methods, CSI-based fingerprinting also works well for massive MIMO localization with the help of deep learning [9]. To fully utilize the large number of antennas and the large bandwidth in massive MIMO systems, angle-delay profile (ADP) [10]–[12] has been obtained by implementing a linear transformation of CSI, which can be leveraged as fingerprints (in the form of 2D images) for wireless localization that can represent all the different paths between the BS and user. Deep convolutional neural networks (DCNN) has been exploited to learn the location features from ADP fingerprints for improved localization performance [10], [11], [13].

Although massive MIMO localization using ADP images is highly promising, the DNNs used in such systems belong to black-box models and are not robust [14]. For example, adversarial examples, which are created by introducing small perturbations to the original image, could easily mislead a well trained deep learning model. Goodfellow et al. first introduced the Fast Gradient Sign Method (FGSM) to attack DNN models for image recognition [15]. Additional adversarial attack methods include Projected Gradient Descent (PGD), a multiple-step variant of FGSM [16], and the Momentum Iterative

Method (MIM), which exploit the momentum term to enhance the attack performance [17]. An example of using FGSM to attack massive MIMO localization is shown in Fig. 1. We can see that after injecting a very small perturbation into the clear ADP data (i.e., $\epsilon = 0.01$, see (11)), the localization error is increased from 0.07 m to 3.97 m using the same DCNN model. Thus, the localization performance can be highly susceptible to adversarial examples. Several recent works have considered the impact of adversarial attacks on wireless systems, e.g., human activity recognition [18], Wi-Fi indoor localization [19], and device identification [20]. However, the robustness of DCNN-based massive MIMO localization against adversarial examples has not been investigated.

In this paper, we study the impact of adversarial attacks as well as defense mechanisms (i.e., adversarial training) on massive MIMO indoor and outdoor localization with DCNN and the neural ordinary differential equation (ODE) model. Specifically, we create adversarial examples by introducing subtle perturbations to the ADP image data, using three white-box attack methods including FGSM, PGD, and MIM. We first introduce the massive MIMO system model with respect to the channel model and how to create the ADPs, and then present the DCNN model and the modified neural ODE model for massive MIMO localization. Adversarial attacks and training for neural ODE are formulated for the proposed localization system. We then validate the performance of DCNN and the neural ODE based localization schemes using a public dataset for both outdoor and indoor scenarios. Our experimental results demonstrate the robustness of the proposed neural ODE model for massive MIMO localization.

The main contributions are summarized as follows.

- To the best of our knowledge, this is the first work to study adversarial attacks and defense on DCNN-based massive MIMO localization. We show how to create ADP images from massive MIMO CSI data as fingerprints and that DCNN-based massive MIMO localization is highly susceptible to adversarial attacks.
- In this paper, we propose a novel neural ODE method using adversarial training to enhance the robustness of massive MIMO localization. Specifically, we combine the convolution blocks, ODE blocks, and the dense layer to implement a localization regression solution. We also leverage adversarial training for the neural ODE against adversarial examples.
- Using a public dataset with both indoor and outdoor scenarios (i.e., the DeepMIMO dataset [21]), our experimental study demonstrates that the proposed neural ODE model with adversarial training is highly robust to adversarial attacks in both indoor and outdoor scenarios.

The rest of this paper is organized as follows. In Section II, we introduce the massive MIMO channel model. The system architecture is presented in Section III. Adversarial attack and defense are introduced in Section IV. Experimental results are discussed in Section V. We conclude this paper in Section VI.

II. System Model

A. Channel Model

Consider wireless localization (indoor or outdoor) with a mobile device and a BS, where massive MIMO orthogonal frequency-division multiplexing (OFDM) is used. We assume that the mobile device uses an omini-directional antenna, the BS is equipped with a uniform linear array (ULA) with N_b antennas ($N_b >> 1$), and the OFDM channel has N_c OFDM sub-carriers. The geometric wideband channel model includes L different paths between the mobile device and the BS. The up-link wireless channel information is estimated for locating the position of the mobile device. For massive MIMO OFDM systems, the CSI vector in the frequency domain for the kth sub-carrier is given by [13]

$$\vec{h}_k = \sum_{i=1}^{L} \alpha_i \vec{\beta}(\theta_i) e^{-j2\pi \frac{k n_i}{N_c}}, \tag{1}$$

where j represents the imaginary unit, α_i is the complex gain of the kth sub-carrier, n_i is the sampled delay with the ith path, and $\vec{\beta}(\theta_i)$ is the linear array response vector with AOA θ_i, which is given by

$$\vec{\beta}(\theta_i) = [1, e^{-j2\pi \frac{d\cos\theta_i}{\lambda}}, ..., e^{-j2\pi \frac{(N_b-1)d\cos\theta_i}{\lambda}}]^T, \tag{2}$$

where λ is the wavelength and d is the gap between two adjacent antennas. The CSI matrix is represented as $\mathcal{H} = [\vec{h}_1, \vec{h}_2, ..., \vec{h}_{N_c}]$.

B. ADP Fingerprints

Although CSI data is widely used for wireless localization, it has not been fully exploited for massive MIMO localization. In this paper, we leverage ADP images as fingerprints for massive MIMO localization. The ADP fingerprints $\mathcal{I}$ (in the form of 2D images) can be created with a linear transformation of the CSI data $\mathcal{H}$ [9], [11], which is represented by

$$\mathcal{I} = |\mathcal{U}^H \mathcal{H} \mathcal{V}|, \tag{3}$$

where $|\cdot|$ represents the absolute value, $\mathcal{U}$ and $\mathcal{V}$ are the discrete Fourier transform (DFT) matrices, and $\mathcal{U}^H$ is the conjugate transpose of matrix $\mathcal{U}$. Specifically, matrix $\mathcal{U} \in \mathbb{C}^{N_b \times N_b}$ and matrix $\mathcal{V} \in \mathbb{C}^{N_c \times N_c}$ are defined as

$$[\mathcal{U}]_{i,j} = \frac{1}{\sqrt{N_b}} e^{-j2\pi \frac{i(j-N_b/2)}{N_b}} \tag{4}$$

$$[\mathcal{V}]_{i,j} = \frac{1}{\sqrt{N_c}} e^{-j2\pi \frac{ij}{N_c}}. \tag{5}$$

For massive MIMO localization, we use the ADP matrix that includes signal power, AOA in the angle domain, and TOA values in the delay domain from all paths, thus fully leveraging the features of the massive MIMO OFDM channel. We show an example of ADP image in the left plot in Fig. 1 of size 32×32, which is a sparse image that only has fewer path clusters and higher image resolution in the angle and time domains. In this paper, we will use ADP images as fingerprints for massive MIMO localization.

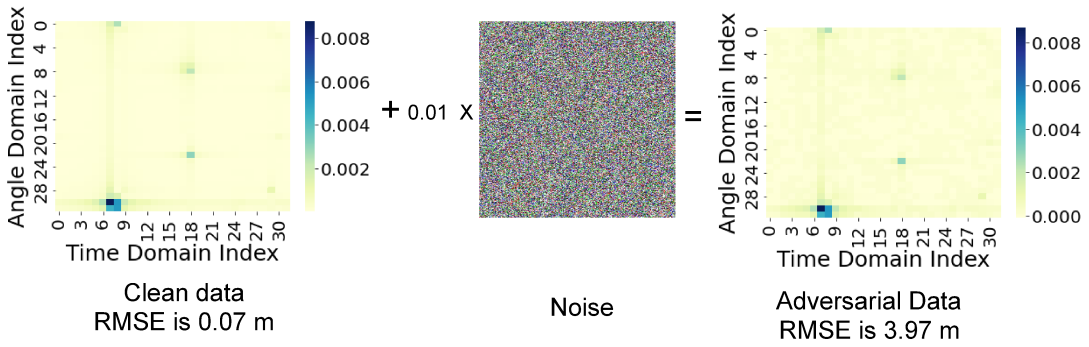

Fig. 1. FGSM attack on DCNN-based massive MIMO indoor localization based on ADP fingerprints.

III. System Architecture

In this paper, we consider two deep learning models (i.e., the DCNN model and the modified neural ODE model) for massive MIMO localization using the above constructed ADP images. As in other fingerprinting schemes, the proposed method also includes an offline training stage and an online testing stage. In the offline stage, we consider both normal training and adversarial training (including the adversarial examples). In the offline stage, we use three types of white-box methods (i.e., FGSM, PGD, and MIM) to create adversarial samples. Then the normally and adversarially trained models are used to validate the performance of massive MIMO localization under the three types of attacks using the public DeepMIMO dataset (including indoor scenarios in the 60 GHz band and outdoor scenarios in the 3.5 GHz band) [21].

A. DCNN Model

The DCNN model can effectively extract the features of constructed ADP images by mainly using basic convolutional filters in an ordered hierarchy for massive MIMO localization. Fig. 2 shows the DCNN network architecture, which includes six layers. The input layer takes 32×32 ADP images, while the hidden layer can extract the important features by convolving a filter with the previous layer. In addition, a max pooling layer is used between two adjacent convolution layers to reduce the parameters and the size of the input. The next convolution layers perform similar operations, where these convolution layers use the `ReLu` activation function to improve the performance of convolution operation and avoid over-fitting. After the convolution layers, we use a flatten layer to reduce the dimension of the features to obtain the desired output, which is then passed to a dense layer with three neurons (for 3D localization). With the above setting, we conduct experiments for massive MIMO localization with the dataset including 66,483 samples for the indoor scenario and 198,104 samples for the outdoor scenario.

B. Neural ODE Model

In this paper, we propose a neural ODE model for massive MIMO localization. Generally, the neural ODE model is a class of deep learning networks which can be interpreted as a continuous equivalent of Residual Networks [22]. Specifically,

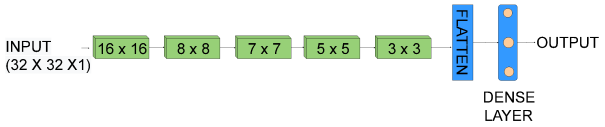

Fig. 2. The CNN Network Architecture.

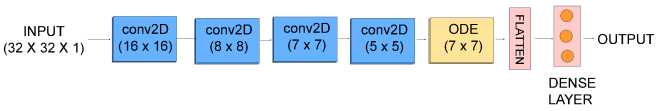

Fig. 3. The ODE Network Architecture.

neural ODE can be defined as a parametric deep model (i.e., with weights w) with an ODE block, where its solution offers the output value. We consider to map input data x (i.e., an ADP image $\mathcal{I}$) to an output value y (e.g., location) by solving an Initial Value Problem (IVP), i.e.,

$$\frac{dh(t)}{dt} = f_w(h(t), t) \tag{6}$$

$$h(0) = x \tag{7}$$

$$y = h(T), \tag{8}$$

where $h(t)$ represents the hidden state of the neural ODE at time t, the function $f_w(\cdot)$ describes the continuous dynamics of state $h(t)$ that is parameterized by weights w. Given input data x, the output y can be obtained by solving the above system of ODE equations, which is given by

$$y = h(T) = h(0) + \int_0^T f_w(h(t), t)dt. \tag{9}$$

The above integral can be computed using standard ODE solvers (e.g., the Runge-Kutta method) [22]. The adjoint sensitivity method has also been developed to train the neural ODE model by solving an additional ODE backward in time. Standard gradient-based optimization can be used after obtaining the gradient. For a regression model based on neural ODE, we integrate the convolution layers, max pool layers, batch normalization layers, a neural ODE block, and a dense layer as shown in Fig. 3. In the customized neural ODE model, we use several convolution layers and max pooling layers to extract features from ADP images, whose output is passed to the ODE block designed for improving the robustness of the

model [23]. The output from the ODE block is then flattened out and passed to a dense layer with three neurons to predict 3D locations.

IV. Adversarial Attacks and Training

In this section, we introduce the three types of white-box attacks (i.e., FGSM, PGD, and MIM) on DCNN and neural ODE models. For massive MIMO localization, the deep neural model (e.g., DCNN) can be attacked by using adversarial samples generated by injecting a small noise to the ADP image. Adversarial ADP images can be created by maximizing the loss function of the deep model, which is defined by

$$\arg\max_{\mathcal{I}_{adv}} \mathcal{L}(f(\mathcal{I}_{adv}, \theta^*), y), \tag{10}$$

where $\mathcal{I}_{adv}$ is the adversarial ADP image, which is obtained by $\mathcal{I}_{adv} = \mathcal{I} + \delta$, where δ is the perturbation. Considering low time complexity for practical applications, in this paper, we focus on white-box attacks including the one-step attack method (i.e., FGSM) and two iterative attack methods (i.e., PGD and MIM), which are introduced in the following.

A. Adversarial Attacks

a) Fast Gradient Sign Method (FGSM): The FGSM attack method is a simple one-step attack with a low time complexity. We calculate the perturbation noise in a single step using a pixel level magnitude perturbation along the gradient direction. The perturbation δ is given by

$$\delta = \epsilon \cdot \text{sign}(\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}, \theta^*), y)), \tag{11}$$

where ϵ is a hyper-parameter to adjust the degree of perturbation. Given the loss function of the deep model $\mathcal{L}(\cdot)$, we compute the perturbation δ based on the first derivative of $\mathcal{L}(f(\mathcal{I}, \theta^*), y)$.

The Fast Gradient Method (FGM) [24] is a generalization of FGSM. The perturbation of FGM is defined as

$$\delta = \epsilon \cdot \frac{\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}, \theta^*), y)}{\|\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}, \theta^*), y)\|_2}. \tag{12}$$

Using (12), the perturbation can be easily computed. Adversarial APD images are generated with different ϵ values, indicating different strengths of introduced perturbations.

b) Projected Gradient Method (PGD): Following the one-step method (i.e., FGM), PGD is designed as an iterative version of FGM to enhance the adversarial attack performance. Adversarial ADP examples can be created with the PGD method as

$$\begin{aligned} &\mathcal{I}_0^{adv} = \mathcal{I}, \\ &\mathcal{I}_{N+1}^{adv} = \text{Clip}_{\{\mathcal{I},\epsilon\}} \left\{ \mathcal{I}_N^{adv} + \alpha \frac{\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}_N^{adv}, \theta^*), y)}{\|\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}_N^{adv}, \theta^*), y)\|_2} \right\}, \end{aligned} \tag{13}$$

where α is also a hyper-parameter, which is set as ϵ/N for a given ϵ. Compared with the FGM method, PGD is generally considered as a stronger adversarial attack approach.

c) Momentum Iterative Method (MIM): The MIM attack incorporates the momentum into the iterative adversarial attack method, which employs the gradient of the previous steps to calculate the perturbation. The gradient in the $(N+1)$th iteration is given by

$$\begin{aligned} q_{N+1} &= \mu \cdot q_N + \frac{\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}_N^{adv}, \theta^*), y)}{\|\nabla_{\mathcal{I}} \mathcal{L}(f(\mathcal{I}_N^{adv}, \theta^*), y)\|_2} \\ \mathcal{I}_{N+1}^{adv} &= \mathcal{I}_N^{adv} + \alpha \cdot \text{sign}(q_{N+1}), \end{aligned} \tag{14}$$

where q_N includes the gradients from the previous $N-1$ iterations with a decay factor of μ.

B. Adversarial Training

To make our DCNN and neural ODE robust to adversarial attacks, our massive MIMO system also implements adversarial training by using a mixture of adversarial ADP images and clean ADP images. Specifically, we consider the adversarial ADP examples and their true labels in the training dataset, to allow the deep models to learn the adversarial examples with correct labels. This way, the trained model will be able to predict the labels for new adversarial ADP images. FGSM, PGD, and MIM adversarial examples are leveraged by the adversarial trainer to accomplish this idea. Generally, FGSM generates perturbations in a single step and adversarial training needs less time but its robustness is not as strong, while PGD and MIM leverage multiple iterations to generate adversarial samples, which require longer time to implement adversarial training. In this paper, we implement adversarial training for both the DCNN model and the ODE model, and validate their performance in the next section.

V. Experiments and Results

A. Experiment Configuration

Our experiments are conducted using the public DeepMIMO dataset [11], [21]. This dataset is completely defined by ray tracing scenarios for both indoor and outdoor environments and channel parameters (e.g., bandwidth, base stations, users, number of paths, etc.). Two scenarios (i.e., indoor and outdoor) based on the ray-tracing simulator developed by Wireless InSite are used in our experiments.

a) Outdoor Scenario: We use DeepMIMO outdoor scenario number 1 (O1) to obtain the outdoor CSI dataset. This scenario includes two urban streets of 400 m $\times$ 40 m and 600 m $\times$ 40 m, respectively, and has one active BS at the intersection of the two streets. We choose the 3.5 GHz band with 10 MHz OFDM bandwidth and 64 sub-carriers. The BS has 64 antennas, and the BS-user channel has 25 paths. In addition, the locations of users are from R1 to R1100 rows (i.e., locations of data points from row 1 to 1100 in the DeepMIMO dataset).

b) Indoor Scenario: We use DeepMIMO indoor scenario number 3 (I3) to obtain the indoor CSI dataset for a conference room of 10 m $\times$ 11 m with its hallways. There is one active BS operating in the 60 GHz band. The other parameters include 32 antennas, 32 sub-carriers, 500 MHz bandwith, and 25 paths. The users locations are from R1 to R550 rows.

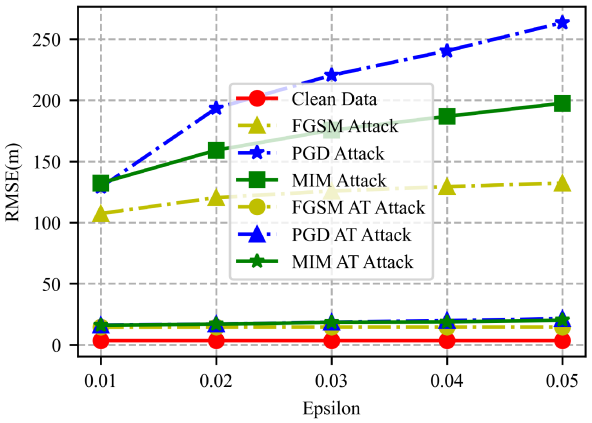

Fig. 4. DCNN model under all attacks in outdoor environment.

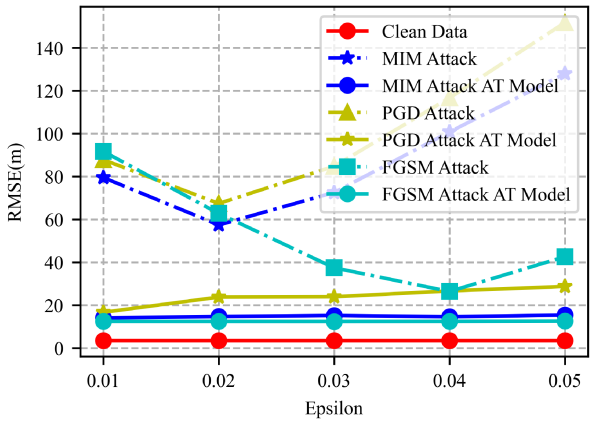

Fig. 5. Neural ODE model under all attacks in outdoor environment.

The two models (i.e., DCNN and the proposed neural ODE) are trained with the outdoor and indoor datasets in the offline stage and are used for localization prediction in the test stage. The three types of white-box attacks (i.e., FGSM, PGD, MIM) are executed in both scenarios. In addition, adversarial examples are collected and used for adversarial training of both models to improve their robustness. Google Colab Pro is utilized as a cloud service to train the models based on Tensorflow.

B. Results and Discussion

Figs. 4 and 5 show the root-mean-square errors (RMSE) of the DCNN and neural ODE models, respectively, in the outdoor scenario, where ϵ is increased from 0.01 to 0.05. It is noticed that compared with neural ODE, the DCNN performance degrades seriously when under the three white-box attacks in the outdoor scenario. For example, under MIM attack with $\epsilon = 0.05$, the DCNN-based method can only achieve an RMSE of 197.59 m, while the neural ODE model's RMSE is 127.99 m. After adversarial training, the results are indicated by "AT" in both figures. The performance has improved significantly for both models. For example, neural ODE and DCNN after adversarial training achieve RMSE of 15.38 m and 20.138 m, respectively.

Figs. 6 and 7 present the RMSE results delivered by DCNN and neural ODE for the indoor scenario, respectively, where ϵ is increased from 0.005 to 0.001 in this scenario of a small indoor area. We find that as the increase of ϵ, the RMSE will increase because larger perturbations are introduced into the ADP image, which lead to higher localization errors. Moreover, for both models, the MIM attacks cause larger RMSE values under each different ϵ value, compared with the other two attack methods. In addition, DCNN achieves an RMSE of 22.45 m, while neural ODE's RMSE is 8.47 m under PGD attacks. On the other hand, after adversarial training, neural ODE and DCNN achieve RMSE of 1.06 m and 3.80 m, respectively, under the same PGD attacks. We conclude that the proposed neural ODE with adversarial training is more robust than the DCNN-based method.

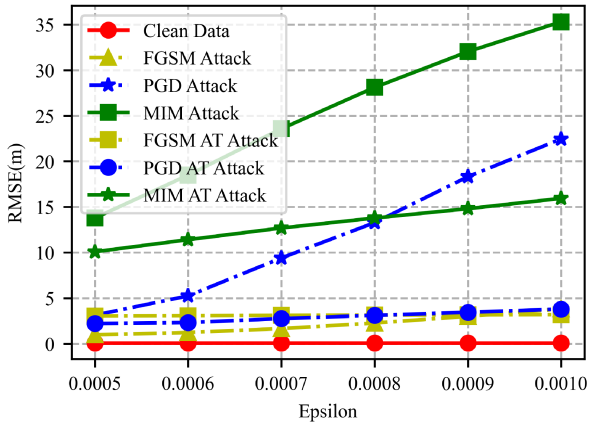

Fig. 6. DCNN Model under all attacks in indoor environment.

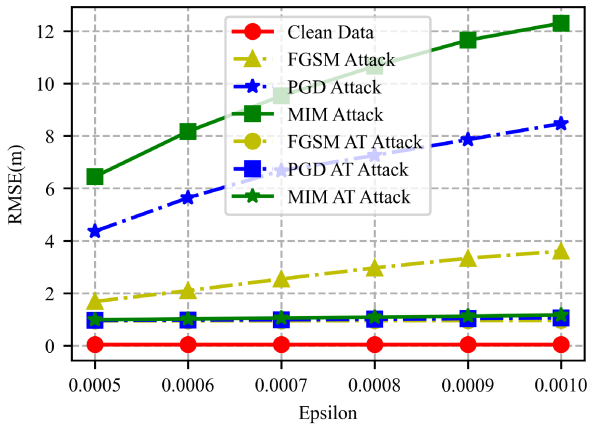

Fig. 7. Neural ODE model under all attacks in indoor environment.

We also validate the impact of the number of neural ODE blocks on localization performance. Fig. 8 shows the results obtained with different ODE blocks for massive MIMO localization under FGSM attacks in the indoor environment. We can see that when we use more than one neural ODE blocks, the RMSE of localization will be reduced. For example, when

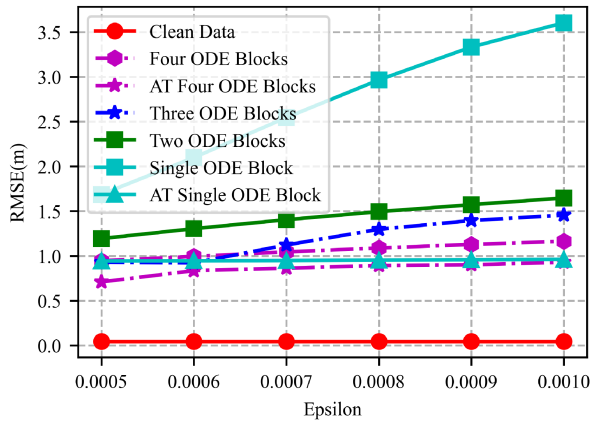

Fig. 8. Different ODE blocks for localization under FGSM attacks in indoor environment.

$\epsilon = 0.001$, the RMSE using a single ODE block is 3.5 m, while using four ODE blocks achieves an RMSE of 1.1 m, which is a considerable improvement in accuracy. In addition, we consider adversarial training for single ODE block and four ODE block models. When $\epsilon = 0.001$, the RMSE of four ODE blocks is 0.83 m, while that using one ODE block is 0.94 m. The former only has a smaller reduction than the latter. In addition, we also find that a single ODE block with adversarial training can achieve a similar localization accuracy as using four ODE blocks without adversarial training.

VI. Conclusion

In this paper, we studied the impact of adversarial attacks and defense on massive MIMO indoor and outdoor localization using the DCNN model and the customized neural ODE model. We showed how to create ADP images for massive MIMO localization and introduced the DCCN and neural ODE models. Both models were studied using a public dataset in both indoor and outdoor environments under three types of white-box adversarial attacks. We found that the DCNN model was highly susceptible to adversarial attacks, while the proposed neural ODE model exhibited strong resilience to such attacks. We also found adversarial training could greatly enhance the robustness of both models.

Acknowledgments

This work is supported in part by the NSF (ECCS-1923163, CNS-2107190, CNS-2105416, and CNS-2107164).

References

[1] S. Fischer, "Observed time difference of arrival (OTDOA) positioning in 3GPP LTE," *Qualcomm White Paper*, June 2014. [Online]. Available: https://www.qualcomm.com/media/documents/files/otdoa-positioning-in-3gpp-lte.pdf

[2] J. Purohit, X. Wang, S. Mao, X. Sun, and C. Yang, "Fingerprinting-based indoor and outdoor localization with LoRa and deep learning," in *Proc. IEEE GLOBECOM'20*, Virtual Conference, Dec. 2020, pp. 1–6.

[3] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[4] X. Wang, M. Patil, C. Yang, S. Mao, and P. A. Patel, "Deep convolutional Gaussian processes for mmWave outdoor localization," in *Proc. IEEE ICASSP'21*, Toronto, Canada, June 2021, pp. 8323–8327.

[5] X. Wang, X. Wang, and S. Mao, "Deep convolutional neural networks for indoor localization with CSI images," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 316–327, Jan./Mar. 2020.

[6] N. Garcia, H. Wymeersch, E. G. Larsson, A. M. Haimovich, and M. Coulon, "Direct localization for massive MIMO," *IEEE Trans. Signal Process.*, vol. 65, no. 10, pp. 2475–2487, May 2017.

[7] F. Wen, H. Wymeersch, B. Peng, W. P. Tay, H. C. So, and D. Yang, "A survey on 5G massive MIMO localization," *Elsevier Digital Signal Process.*, vol. 94, pp. 21–28, Nov. 2019.

[8] X. Wang, L. Gao, S. Mao, and S. Pandey, "CSI-based fingerprinting for indoor localization: A deep learning approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 763–776, Jan. 2017.

[9] A. Decurninge, L. G. Ordóñez, P. Ferrand, H. Gaoning, L. Bojie, Z. Wei, and M. Guillaud, "CSI-based outdoor localization for massive MIMO: Experiments with a learning approach," in *Proc. IEEE 2018 Int. Symp. Wireless Commun. Sys.*, Lisbon, Portugal, Aug. 2018, pp. 1–6.

[10] C. Wu, X. Yi, W. Wang, Q. Huang, and X. Gao, "3D CNN-enabled positioning in 3D massive MIMO-OFDM systems," in *Proc. IEEE ICC'20*, Dublin, Ireland, July 2020, pp. 1–6.

[11] F. Hejazi, K. Vuckovic, and N. Rahnavard, "DyLoc: Dynamic localization for massive MIMO using predictive recurrent neural networks," *arXiv preprint arXiv:2101.07848*, Jan. 2021. [Online]. Available: https://arxiv.org/abs/2101.07848

[12] J. Vieira, E. Leitinger, M. Sarajlic, X. Li, and F. Tufvesson, "Deep convolutional neural networks for massive mimo fingerprint-based positioning," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–6.

[13] X. Sun, X. Gao, G. Y. Li, and W. Han, "Single-site localization based on a new type of fingerprint for massive MIMO-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6134–6145, July 2018.

[14] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv preprint arXiv:1312.6199*, Dec. 2013. [Online]. Available: https://arxiv.org/abs/1312.6199

[15] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, Dec. 2014. [Online]. Available: https://arxiv.org/abs/1412.6572

[16] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," *arXiv preprint arXiv:1706.06083*, June 2017. [Online]. Available: https://arxiv.org/abs/1706.06083

[17] Y. Dong, F. Liao, T. Pang, H. Su, J. Zhu, X. Hu, and J. Li, "Boosting adversarial attacks with momentum," in *Proc. IEEE CVPR'18*, Salt Lake City, UT, June 2018, pp. 9185–9193.

[18] H. Ambalkar, X. Wang, and S. Mao, "Adversarial human activity recognition using Wi-Fi CSI," in *Proc. 2021 IEEE Canadian Conf. Electrical and Computer Eng.*, ON, Canada, Sept. 2021, pp. 1–5.

[19] M. Patil, X. Wang, X. Wang, and S. Mao, "Adversarial attacks on deep learning-based floor classification and indoor localization," in *Proc. 2021 ACM Workshop on Wireless Security and Machine Learning (WiseML'21)*, Abu Dhabi, UAE, June-July 2021, pp. 7–12.

[20] Z. Bao, Y. Lin, S. Zhang, Z. Li, and S. Mao, "Threat of adversarial attacks on DL-based IoT device identification," *IEEE Internet of Things Journal*, in press. DOI: 10.1109/JIOT.2021.3120197.

[21] A. Alkhateeb, "DeepMIMO: A generic deep learning dataset for millimeter wave and massive MIMO applications," *arXiv preprint arXiv:1902.06435*, Feb. 2019. [Online]. Available: https://arxiv.org/abs/1902.06435

[22] T. Q. Chen, Y. Rubanova, J. Bettencourt, and D. K. Duvenaud, "Neural ordinary differential equations," in *Proc. NeurIPS'18*, Montréal, Canada, Dec. 2018, pp. 1–18.

[23] F. Carrara, R. Caldelli, F. Falchi, and G. Amato, "On the robustness to adversarial examples of neural ode image classifiers," in *Proc. 2019 IEEE Int. Workshop Information Forensics and Security*, Delft, Netherlands, Dec. 2019, pp. 1–6.

[24] T. Miyato, A. M. Dai, and I. Goodfellow, "Adversarial training methods for semi-supervised text classification," *arXiv preprint arXiv:1605.07725*, May 2016. [Online]. Available: https://arxiv.org/abs/1605.07725