Undermining Deep Learning Based Channel Estimation via Adversarial Wireless Signal Fabrication

Tao Hou
taohou@usf.edu
University of South Florida

Tao Wang
taow@nmsu.edu
New Mexico State University

Zhuo Lu
zhuolu@usf.edu
University of South Florida

Yao Liu
yliu@cse.usf.edu
University of South Florida

Yalin Sagduyu
ysagduyu@vt.edu
VT National Security Institute

ABSTRACT

Channel estimation is a crucial step in wireless communications. The estimator identifies the wireless channel distortions during the signal propagation and this information is further used for data precoding and decoding. Recent studies have shown that deep learning techniques can enhance the accuracy of conventional channel estimation algorithms. However, the reliability and security aspects of these deep learning algorithms have not yet been well investigated in the context of wireless communications. With no exceptions, channel estimation based on deep learning may be vulnerable to the adversarial machine learning attacks. However, close examination shows that we cannot simply adapt the traditional adversarial learning mechanisms to effectively manipulate channel estimation. In this paper, we propose a novel attack strategy that crafts a perturbation to fool the receiver with wrong channel estimation results. This attack is launched without knowing the current input signals and by only requiring a loose form of time synchronization. Through the over-the-air experiments with software-defined radios in our multi-user MIMO testbed, we show that the proposed strategy can effectively reduce the performance of deep learning-based channel estimation. We also demonstrate that the proposed attack can hardly be detected with the detection rate of 8% or lower.

CCS CONCEPTS

• **General and reference → General conference proceedings**; • **Security and privacy → Mobile and wireless security**; *Access control*; • **Networks → Network security**; **Mobile and wireless security**; *Network reliability*; *Cyber-physical networks.*

KEYWORDS

Channel Estimation, Deep Learning, Adversarial Example, Wireless Signal, Malicious Perturbation, Generative Adversarial Network

ACM Reference Format:
Tao Hou, Tao Wang, Zhuo Lu, Yao Liu, and Yalin Sagduyu. 2022. Undermining Deep Learning Based Channel Estimation via Adversarial Wireless Signal Fabrication. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning (WiseML '22), May 19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3522783.3529525

WiseML '22, May 19, 2022, San Antonio, TX, USA

ACM ISBN 978-1-4503-9277-8/22/05…$15.00
https://doi.org/10.1145/3522783.3529525

1 INTRODUCTION

Fast and accurate channel estimation is critical for wireless communications. As part of the communication chain, the channel estimation is needed to identify the wireless channel distortions during the signal propagation and this information is further used for data precoding and decoding. In addition, channel estimation is needed for various communication tasks (such as power control, link scheduling, and initial access) to discover and utilize the limited spectrum resources. Recent studies [1–6] have shown that deep learning techniques can enhance the accuracy of the conventional channel estimation algorithms (e.g., Least Square (LS) and Minimum Mean Square Error (MMSE)). For example, both image super-resolution (SR) algorithm and denoising convolutional neural network (DnCNN) were incorporated in [1] to reduce the pilot contamination and enhance the resolution of the estimated channel. A specifically designed untrained deep neural network (DNN) estimator that can considerably improve the accuracy of the channel estimation was employed in [2] while imposing no computational overhead and temporal latency during the channel estimation.

Although deep learning has proven itself to be a capable tool in a variety of applications including wireless communications, reliability and security are major concerns regardless of the extensive usage and wide adoption of DNNs to solve complex tasks. Recent studies have shown that deep neural networks used in wireless communications are vulnerable to the adversarial machine learning attacks [7, 8]. Different wireless attacks based on adversarial machine learning include exploratory (inference) attacks [9–12], evasion (adversarial) attacks [13–25], causative (poisoning) attacks [26–29], membership inference attacks [30, 31], Trojan attacks [32], spoofing attacks [33, 34], and covert communications [35–37]. In this paper, we focus on the evasion (adversarial) attack that creates inputs containing minor perturbations, i.e., adversarial examples, to fool the DNNs to yield wrong classification results.

With no exceptions, the deep learning-based channel estimation techniques may be also vulnerable to the adversarial machine learning attacks. However, a close examination shows that we cannot simply adapt the traditional procedure of adversarial attacks to disturb the channel estimation process due to two reasons: (i) The design of the adversarial perturbation benefits from the knowledge of the original input. However, in real-time wireless communications, it is not practical for the attackers to intercept the signal and then insert the perturbation to mislead the original results [38–40]. (ii) Unlike other data domains such as computer vision, radio signals need to be manipulated during the propagation by relying on an accurate synchronization between the victim and the attacker.

While DNNs improve the performance of the next-generation wireless networks, e.g., 5G, IoT, and multi-user MIMO (MU-MIMO), it is necessary to mitigate the optional gap between the performance gain and the security concerns. In this paper, we examine the security of the deep learning assisted wireless channel estimation and uncover potential vulnerabilities.

Specifically, we propose a novel universal adaptive signal perturbation. Instead of customizing the perturbation based on the signal inputs, the proposed attack fabricates a universal adaptive interference signal that can effectively disturb the channel estimation without requiring knowledge of the original inputs. The deep learning-based channel estimation will be used as the target victim system to test the effectiveness of the proposed attack strategy on discovering its vulnerabilities. As the channel estimation algorithms are usually public and can be utilized by any device in the network, we propose to launch attacks in the white-box scenario, in which the attacker has some knowledge of the target system. In the attack strategy, the attacker attempts to craft a perturbation to fool the receiver with wrong channel estimation results. After uncovering the potential vulnerabilities, we can further seek remedies to mitigate these security risks and improve the security guarantees for deep learning-based channel estimation systems.

After building a 2×2 MU-MIMO network testbed with software-defined radios (SDRs), we conduct the over-the-air experiments to evaluate the proposed attacks. The testbed evaluation results show that the proposed strategy can effectively disturb the deep learning assisted channel estimation such that the receiver ends up with estimating a channel that is quite different from the real one.

The remainder of this paper is presented as follows. Section 2 describes the preliminaries of the deep learning-based channel estimation. Section 3 presents the attack model that can undermine deep learning-based channel estimation via adversarial wireless signal fabrication. Section 4 demonstrates our detail attack strategies. Section 5 evaluate the effectiveness of these strategies with these experiments. Section 6 concludes the paper.

2 PRELIMINARIES

In this section, we review the channel estimation methods assisted by deep learning.

2.1 Channel-Image Based Channel Estimation

By building upon the cumulative knowledge of deep learning techniques developed for image processing and recognition, the channel information can be converted into images to take advantage of existing deep learning algorithms [1, 3, 4]. For example, the channel matrix of massive MIMO system was the was regarded as a 2D image in [4] and the learned denoising-based approximate message passing (LDAMP) neural network was applied into the iterative sparse signal recovery algorithm for channel estimation. Both image super-resolution (SR) algorithm and image restoration (IR) method were incorporated in [1] to eliminate the effects of channel noise and enhance the resolution of the estimated channel. This design also utilized the denoising convolutional neural network (DnCNN) to improve both the training time and accuracy.

2.2 Channel Estimation with Untrained Deep Neural Network

Traditional channel estimators such as matrix inversion and singular value decomposition (SVD) are impractically complex for large channel matrices [41–45]. Recently, multiple unsupervised machine learning models [2, 5, 6, 41, 43] have been proposed to achieve low-overhead, low-complexity, and scalable channel estimators. As conventional DNNs usually require a large number of labeled datasets for model training and parameter tuning, they are not suitable for channel estimation in a rapid changing wireless environment. In particular, inspired by recently proposed DNN design named deep image prior [46], which is used for denoising and inpainting, and require no training efforts, [2] applied a specifically designed deep image prior to removing the channel noise and reducing the preamble contamination before forwarding the received signals for the least-square estimation. The untrained DNN estimator was shown to improve the accuracy of the channel estimation considerably while imposing no computational overhead and temporal latency during the procedure.

In addition to the above two main types of deep learning methods, many specified/customized deep learning models have been developed to achieve efficient and accurate channel estimation [44, 47–49]. We describe the typical deep learning-based channel estimation designs in the following.

2.3 DeepMux for Downlink Channel Estimation

A deep learning model called DeepMux was proposed in [47] to achieve efficient downlink MU-MIMO-OFDMA transmission for 802.11ax networks. DeepMux employs a deep learning-based channel sounding module to reduce the airtime overhead of 802.11 protocols. Channel sounding is the critical step for signal beamforming in downlink MU-MIMO networks. However, current protocols may incur a high time overhead and essentially reduce the system throughput. The channel sounding module in DeepMux employs an online training process and requires no effort from stations. This design infers full CSI angles based on a sparsified feedback and can significantly reduce the channel sounding overhead.

2.4 Deep Learning Channel Estimation for Short Pilots

In the massive MIMO network, a large-scale antenna array is usually deployed to achieve considerable antenna gains. Nevertheless, the antenna gains highly depend on the accuracy of the channel estimation. Common channel estimation usually assumes the pilot length is equal to or larger than the number of transmit antennas to achieve an accurate channel estimate. As the number of transmit antennas keeps increasing, this assumption may not always hold. A two-stage machine learning-based channel estimation system was developed in [4]. First, a two-layer neural network (TNN) was constructed to minimize the mean square error (MSE) of the channel estimation. Second, a DNN based iterative channel estimation

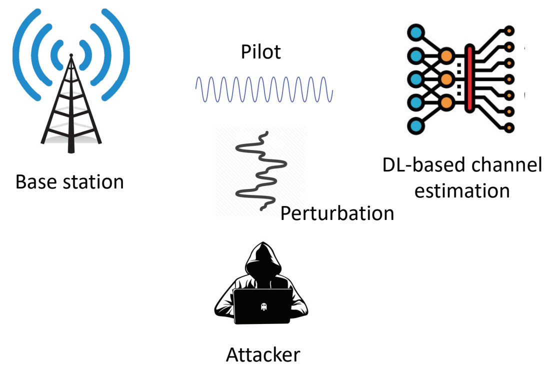

Figure 1: The attack model.

technique was adopted to further improve the channel estimation performance.

2.5 LSTM-Based Channel Estimation for Imperfect Channel State Information (CSI)

Because of the processing and transmission delay, the channel state information (CSI) estimated at the receiver is not always perfect in a practical mobile network. Some accurate channel estimation method was developed in [44] for multi-user massive MIMO-enabled vehicular communication networks. Specifically, LSTM was utilized to capture the time correlation characteristics among consistent received signals and apply the learned characteristics to compensate the imperfection of the channel estimation, thus gaining an accurate CSI.

3 ATTACK MODEL

Deep learning-based channel estimation techniques can provide promising performance and computation efficiency for wireless communications. However, the security and reliability of these techniques have not been thoroughly examined. In particular, it is known that deep learning models are usually vulnerable to adversarial examples, i.e., a small perturbation inserted to the inputs may fool a deep learning model with a misclassified output. It is possible that machine learning-based channel estimation in wireless communications may also be significantly disrupted by the adversarial perturbations. Therefore. it is essential to understand the impact of adversarial machine learning attack on deep learning-based channel estimation techniques, and seek means to alleviate these security risks.

To this end, we aim to exploit the vulnerabilities of deep learning-based channel estimation and seek feasible adversarial machine learning attacks on wireless communications. The channel estimation system is used as the target victim system to test the effectiveness of the proposed attack strategy. As shown in Figure 1, the target channel estimation system consists of a base station (e.g., gNodeB), a wireless channel, and a receiver (e.g., user equipment). At the transmitter side, the base station sends pilot signals (i.e., training sequence) to the receiver for channel synchronization. The objective of the attacker is to add a malicious perturbation signal through the channel between the base station and the receiver such that the machine learning model is manipulated to yield an incorrect channel estimation result and further affect the data decoding at the receiver.

We assume a white-box attack as the channel estimation algorithms are usually public and can be utilized by any device in the network. However, it is a challenge for the attacker to obtain the fine-grained time synchronization of the transmitter. We also assume the perturbation generated by the attacker is subject to a random phase shift on the channel relative to the transmitter's signal. In the next section, we will introduce the details on how to generate the adversarial perturbation to achieve the attack goals.

4 PERTURBATION GENERATION

4.1 Problem Formulation

Since channel estimation algorithms are usually public and can be adopted by any wireless device, we assume the machine learning model used for the channel estimation has already been learned by the attacker. The attacker aims to fabricate a perturbation signal Δs that can disturb the channel estimation results. The goal of the attack is to yield

$$M(s + \Delta s) \neq M(s), \tag{1}$$

where s is the received signal and M is the underlying machine learning model used for channel estimation. The output of M is the channel estimation result. The attacker aims to create a signal perturbation such that the system will obtain a different output result.

This attack formulation falls into the general area of adversarial machine learning. However, a close examination shows that we cannot simply adapt the traditional adversarial machine learning approach to launch the proposed attack.

(i) For traditional adversarial perturbation problem, we need to have the knowledge of the original input. Upon that, we create a customized perturbation to skew the output result. However, as wireless communication operates in real time, it is almost impossible for attackers to first intercept the signal, predict the results, and then add the perturbation to mislead the results. The delay introduced during the procedure creates a substantial hurdle to launch a realistic attack.

(ii) Unlike images or videos, it would be a challenging task to manipulate a radio signal during the propagation. The attack would benefit from an accurate synchronization to add the interference signal to the original signal.

In this paper, we propose a novel attack that does not rely on the knowledge of current input signals and requires a loose time synchronization only.

4.2 Attack Overview

Intuitively, we can create a jamming signal with large power to overwhelm the original signal at the receiver. However, such trivial attacks can be easily detected when the system experiences unexpected larger signal power of the received signals. In addition, the attacker may need to preserve its energy (e.g., when it is battery powered). Towards this end, we propose a novel universal adaptive signal perturbation. Instead of customizing the perturbation based on the signal inputs, the proposed attack fabricates a universal adaptive interference signal that can effectively disturb the channel estimation without requiring knowledge of the original inputs. In addition, the attacker can hide itself by keeping the interference signal within the normal power constraints. In particular, we can further formulate the attack as

$$\begin{aligned} &\min_{\Delta s} ||\Delta s||^2 \\ &\text{s.t.} \quad M(s+\Delta s) \neq M(s) \quad \text{for any } \; s \in \mathcal{S}, \end{aligned} \tag{2}$$

where $\mathcal{S}$ is the original transmit signal. In this attack formulation, we aim to find an interference signal Δs that can yield different channel estimations for any possible signal s belonging to the system. We also observe that channel estimation is performed in the unit of each symbol. Inspired by that, the proposed attack does not focus on an exact time synchronization to achieve fine-grained signal manipulation. Alternatively, we only require symbol-level synchronization to systematically disturb the channel estimation. For a wireless system with 10 MHz bandwidth, the attack can achieve the system-level time synchronization as long as the oscillator of the system can generate a signal of the resolution within 0.1μs, which can be easily achieved by most modern radio transceivers [50].

Figure 2 demonstrates the structure of the proposed signal perturbation. It includes three components:

(i) Perturbation randomizer that generates a random initial variable for dynamic perturbation generation.
(ii) Perturbation generator that builds an adversarial model and generates signal perturbations to manipulate the channel estimation.
(iii) Gaussian normalizer that enforces the Gaussian distribution of the signal perturbation to avoid being detected by the communication system.

In what follows, we first describe how we generate random perturbations to manipulate the channel estimation. Then, we demonstrate how to further refine the perturbation to circumvent statistical examination by the network administrator and achieve a stealthy attack.

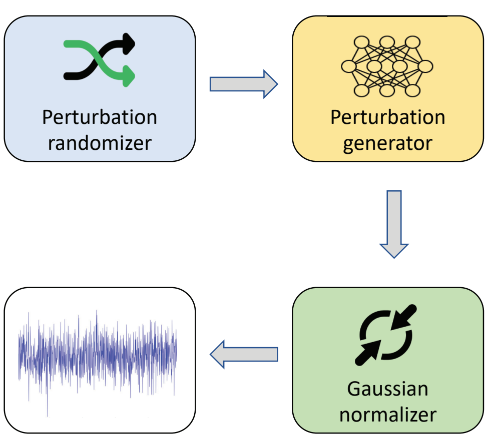

Figure 2: Structure of the adversarial perturbation generation.

4.3 Symbol-level Signal Perturbation

The attacker aims to generate a universal perturbation signal Δs to yield different channel estimation results at the receiver. Although we may craft a fixed signal Δs by solving the optimization question in 2, the fixed pattern may be easily learned and removed by the receiver from the transmit signals to avoid the disturbance. In addition, current solutions based on solving 2 does not consider the impact of channel distortions when the signal perturbation is sent to the receiver.

Randomizing the perturbation: To improve the stealthiness of the proposed attack, we aim to introduce randomness to the universal perturbation. In particular, we further define the perturbation signal as a function of $\Delta d(t)$, where Δd indicates each perturbation symbol. It takes a random variable t as input and generates different perturbation symbols accordingly. Specifically, we can refine 2 as

$$\begin{aligned} &\max_{\Delta d(t)} f_l(M(d+\Delta d(t)), M(d)) \quad \text{for any } \; d \in \mathcal{D}, \\ &\text{s.t.} \; |\Delta d(t)|^2 \leq p_{th}, \end{aligned} \tag{3}$$

where d indicates a possible transmit symbol, f_l is the loss function of the model M, p_{th} is the power constraint of the perturbation symbol, and $\mathcal{D}$ is the set of all possible symbols. In this attack formulation, we aim to obtain $\Delta d(t)$ to maximize the difference of the loss function between the original channel estimation and the manipulated one, while satisfying a small power constraint of p_{th}.

Dealing with the channel distortion: So far, our discussion has omitted the channel distortion between the attacker and the receiver to facilitate the analysis. However, the distortion may considerably affect the amplitude and phase of the perturbation signal $\Delta d(t)$, resulting in an ineffective attack. Due to this reason, channel distortion must be pre-compensated before $\Delta d(t)$ is transmitted. In particular, the attacker can passively sniff the acknowledgement packets from the receiver and estimate the channel h_a with the receiver. Without loss of generality, we model the estimated channel h_a as a complex coefficient and assume that the channel will remain constant during the perturbation signal transmission. Then, the perturbation signal is precoded according to the estimated channel to compensate the propagation loss (i.e., the precoded perturbation signals are computed as $\Delta d(t)' = \Delta d(t)/h_a$).

4.4 Gaussian Normalizer

We further randomize the perturbation to emulate it as true channel noise. In particular, current output of $\Delta d(t)$ may not always follow regular channel noise distributions (e.g., Gaussian noise). If the system statistically examines the received signals, it may detect the unusual patterns of the signal perturbation and identify the attack. To further improve the effectiveness of the proposed attack, we enforce the Gaussian distribution on the perturbation signal. In particular, we add a Gaussian operator $G(\gamma)$ during the attack training to track the generated perturbations and ensure that the output of the objective function always follows the Gaussian distribution.

5 EXPERIMENTAL EVALUATION

We set up 2×2 MU-MIMO OFDM network by utilizing Universal Software Radio Peripheral (USRP) radios as the SDRs. Our testbed is running at the central frequency of 2.4GHz. In this section, we present results based on the over-the-air experiments conducted in this testbed.

We consider three typical deep learning assisted channel estimation methods in our experiments.

(i) **LDAMP based channel estimation:** This method takes advantage of LDAMP neural network to remove the channel noise and adopts the iterative sparse signal recovery algorithm to estimate the channel.
(ii) **DIP based channel estimation:** This method adopts the untrained deep image prior model to improve both training efficiency and accuracy.
(iii) **LSTM based channel estimation:** This method utilizes the LSTM to learn the temporal correlations among continuous received signals to improve the estimation accuracy.

We run each algorithm for 1000 times with and without the proposed attack. In addition, we assume a static environment such that channels are estimated within the coherence time.

5.1 Effectiveness of the Proposed Attack

We define the channel distance d to indicate the effectiveness of the proposed attack, where the distance d_{ij} between two estimated channels h_i and h_j is computed as $|h_i - h_j|$. Within the coherence time, channels estimated at the receiver should be constant with minor distance.

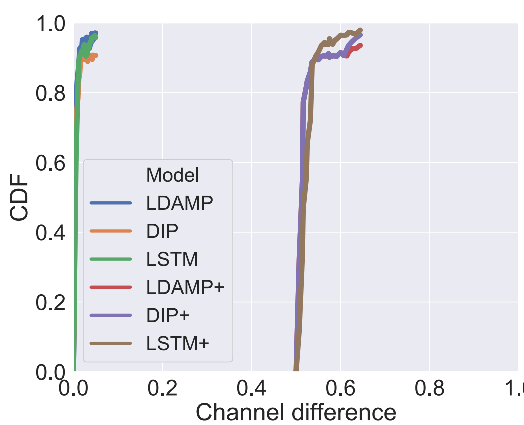

Figure 3: Effectiveness of the proposed attacks. LDAMP+, DIP+, LSTM+ indicate results under attack.

Figure 3 shows the results of different channel estimation methods under the attack. In particular, we plot the distribution of estimated channel distances. When there is no attack (curves labeled as LDAMP, DIP, LSTM), all the algorithms can achieve constant estimations, and the channel distances for them are quite small (i.e., 80% of channel distances are less than 0.01). Meanwhile, when the attack is present (curves labeled as LDAMP+, DIP+, LSTM+), the estimation results become quite different and cannot achieve consistency (i.e., channel distances for all three algorithms are larger than 0.5 under the proposed attack).

5.2 Stealthiness of the Proposed Attack

We also evaluate the Stealthiness (undetectability) of the proposed attack. We find that the receiver can easily detect the attack when random variable t is not employed, because the receiver experiences a fixed power increment of the received signal. When t is applied without Gaussian normalizer, the receiver can still detect the attack by analyzing the noise distribution (i.e., $\Delta d(t)$ follows an approximately uniform distribution). When Gaussian normalizer is applied, statistical analysis becomes invalid to detect the attack. Figure 4 shows the detection rate when Gaussian normalizer has been deployed. Since the randomized perturbation now behaviors as the normal Gaussian noise, the receiver can hardly detect the attacks and the detection rate drops to 8% or lower.

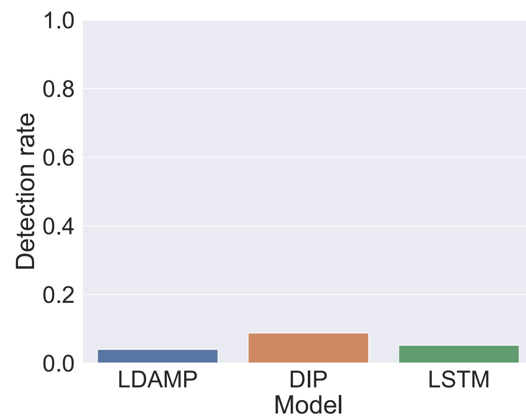

Figure 4: Detection rate with Gaussian normalizer

6 CONCLUSION

In this paper, we considered deep learning-based channel estimation and exploited their vulnerability to adversarial attacks. In particular, we developed a novel attack that does not rely on the knowledge of current input signals and requires only a loose time synchronization. The attacker's goal is to craft a perturbation that fools the receiver with wrong channel estimation results without being detected by the receiver. In addition, we built a 2×2 MU-MIMO network with SDRs and conducted the over-the-air experiments to evaluate the proposed attack. The experiment results show that the proposed attack can effectively manipulate the deep learning-based channel estimation such that the receiver is fooled into estimating a channel that is quite different from the real one.

7 ACKNOWLEDGEMENT

The work at the University of South Florida was supported in part by NSF under grant CNS-2044516. The work at the New Mexico State University was supported in part by NSF under grant ECCS-2139028.

REFERENCES

[1] Mehran Soltani, Vahid Pourahmadi, Ali Mirzaei, and Hamid Sheikhzadeh. Deep learning-based channel estimation. *IEEE Communications Letters*, 23(4):652–655, 2019.

[2] Eren Balevi, Akash Doshi, and Jeffrey G Andrews. Massive mimo channel estimation with an untrained deep neural network. *IEEE Transactions on Wireless Communications*, 19(3):2079–2090, 2020.

[3] Mohammad Sadegh Safari, Vahid Pourahmadi, and Shabnam Sodagari. Deep ul2dl: Data-driven channel knowledge transfer from uplink to downlink. *IEEE Open Journal of Vehicular Technology*, 1:29–44, 2019.

[4] Hengtao He, Chao-Kai Wen, Shi Jin, and Geoffrey Ye Li. Deep learning-based channel estimation for beamspace mmwave massive mimo systems. *IEEE Wireless Communications Letters*, 7(5):852–855, 2018.

[5] Nurettin Turan, Michael Koller, Samer Bazzi, Wen Xu, and Wolfgang Utschick. Unsupervised learning of adaptive codebooks for deep feedback encoding in fdd systems. *arXiv preprint arXiv:2105.09125*, 2021.

[6] Benedikt Fesl, Nurettin Turan, Michael Koller, Michael Joham, and Wolfgang Utschick. Centralized learning of the distributed downlink channel estimators in fdd systems using uplink data. *arXiv preprint arXiv:2105.10746*, 2021.

[7] D. Adesina, C. C. Hsieh, Y. E. Sagduyu, and L. Qian. Adversarial machine learning in wireless communications using RF data: A review. *arXiv preprint arXiv:2012.143922*, 2020.

[8] Y. E. Sagduyu, Y. Shi, T. Erpek, W. Headley, B. Flowers, G. Stantchev, and Z. Lu. When wireless security meets machine learning: Motivation, challenges, and research directions. *arXiv preprint arXiv:2001.08883*, 2020.

[9] Y. Shi, Y. E Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu, and J. Li. Adversarial deep learning for cognitive radio security: Jamming attack and defense strategies. In *IEEE International Communications Conference Workshop on Machine Learning in Wireless Communications*, 2018.

[10] T. Erpek, Y. E. Sagduyu, and Y. Shi. Deep learning for launching and mitigating wireless jamming attacks. *IEEE Transactions on Cognitive Communications and Networking*, 5(1):2–14, March 2019.

[11] Tao Hou, Shengping Bi, Tao Wang, Zhuo Lu, Yao Liu, Satyajayant Misra, and Yalin Saguduyu. MUSTER: Subverting user selection in MU-MIMO networks. In *IEEE Conference on Computer Communications (INFOCOM)*, 2022.

[12] Tao Hou, Tao Wang, Zhuo Lu, and Yao Liu. Smart spying via deep learning: inferring your activities from encrypted wireless traffic. In *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1–5. IEEE, 2019.

[13] Meysam Sadeghi and Erik G Larsson. Adversarial attacks on deep-learning based radio signal classification. *IEEE Wireless Communications Letters*, 8(1):213–216, 2018.

[14] Tao Hou, Tao Wang, Zhuo Lu, Yao Liu, and Yalin Sagduyu. Iotgan: Gan powered camouflage against machine learning based iot device identification. In *2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 280–287. IEEE, 2021.

[15] Bryse Flowers, R. Michael Buehrer, and William C. Headley. Evaluating adversarial evasion attacks in the context of wireless communications. *IEEE Transactions on Information Forensics and Security*, 15:1102–1113, 2020.

[16] Silvija Kokalj-Filipovic, Rob Miller, and Joshua Morman. Targeted adversarial examples against rf deep classifiers. In *Proceedings of the ACM Workshop on Wireless Security and Machine Learning*, pages 6–11, 2019.

[17] Yun Lin, Haojun Zhao, Ya Tu, Shiwen Mao, and Zheng Dou. Threats of adversarial attacks in dnn-based modulation recognition. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, pages 2469–2478, 2020.

[18] Brian Kim, Yalin E. Sagduyu, Kemal Davaslioglu, Tugba Erpek, and Sennur Ulukus. Over-the-air adversarial attacks on deep learning based modulation classifier over wireless channels. In *2020 54th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6, 2020.

[19] Brian Kim, Yalin E. Sagduyu, Kemal Davaslioglu, Tugba Erpek, and Sennur Ulukus. Channel-aware adversarial attacks against deep learning-based wireless signal classifiers. *IEEE Transactions on Wireless Communications*, 2021.

[20] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus. Adversarial attacks with multiple antennas against deep learning-based modulation classifiers. In *IEEE Global Communications Conference (GLOBECOM)*, 2020.

[21] B. Kim, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, and S. Ulukus. Channel effects on surrogate models of adversarial attacks against wireless signal classifiers. In *IEEE International Conference on Communications (ICC)*, 2020.

[22] B. Kim, Y. Shi, Y. E. Sagduyu, T. Erpek, and S. Ulukus. Adversarial attacks against deep learning based power control in wireless communications. In *IEEE Global Communications Conference (GLOBECOM)*, 2021.

[23] B. Kim, Y. Sagduyu, T. Erpek, and S. Ulukus. Adversarial attacks on deep learning based mmwave beam prediction in 5G and beyond. In *IEEE Statistical Signal Processing Workshop (SSP)*, 2021.

[24] Han Qiu, Tian Dong, Tianwei Zhang, Jialiang Lu, Gerard Memmi, and Meikang Qiu. Adversarial attacks against network intrusion detection in iot systems. *IEEE Internet of Things Journal*, 8(13):10327–10335, 2020.

[25] Yalin E. Sagduyu, Tugba Erpek, and Yi Shi. Adversarial machine learning for 5G communications security. In *Game Theory and Machine Learning for Cyber Security*, pages 270–288, 2021.

[26] Y. Shi, T. Erpek, Y. E Sagduyu, and J. Li. Spectrum data poisoning with adversarial deep learning. In *IEEE Military Communications Conference (MILCOM)*, 2018.

[27] Y. E. Sagduyu, Y. Shi, and T. Erpek. IoT network security from the perspective of adversarial deep learning. In *IEEE International Conference on Sensing, Communication and Networking (SECON) Workshop Machine Learning for Communication and Networking in IoT*, 2019.

[28] Y. E. Sagduyu, T. Erpek, and Y. Shi. Adversarial deep learning for over-the-air spectrum poisoning attacks. *IEEE Transactions on Mobile Computing*, 2021.

[29] Zhengping Luo, Shangqing Zhao, Zhuo Lu, Jie Xu, and Yalin E. Sagduyu. When attackers meet ai: Learning-empowered attacks in cooperative spectrum sensing. *IEEE Transactions on Mobile Computing*, 21(5):1892–1908, 2022.

[30] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu. Over-the-air membership inference attacks as privacy threats for deep learning-based wireless signal classifiers. In *ACM Workshop on Wireless Security and Machine Learning (WiseML)*, 2020.

[31] Yi Shi and Yalin Sagduyu. Membership inference attack and defense for wireless signal classifiers with deep learning. *IEEE Transactions on Mobile Computing*, 2022.

[32] K. Davaslioglu and Y. E. Sagduyu. Trojan attacks on wireless signal classification with adversarial machine learning. In *IEEE Symposium on Dynamic Spectrum Access Networks Workshop on Data-Driven Dynamic Spectrum Sharing*, 2019.

[33] Yi Shi, Kemal Davaslioglu, and Yalin E Sagduyu. Generative adversarial network for wireless signal spoofing. In *ACM Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[34] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu. Generative adversarial network in the air: Deep adversarial learning for wireless signal spoofing. *IEEE Transactions on Cognitive Communications and Networking*, 7(1):294–303, March 2021.

[35] Muhammad Zaid Hameed, András György, and Deniz Gündüz. The best defense is a good offense: Adversarial attacks to avoid modulation detection. *IEEE Transactions on Information Forensics and Security*, 16:1074–1087, 2021.

[36] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus. How to make 5G communications "invisible" adversarial machine learning for wireless privacy. In *Asilomar Conference on Signals, Systems, and Computers*, 2020.

[37] B. Kim, T. Erpek, Y. E. Sagduyu, and S. Ulukus. Covert communications via adversarial machine learning and reconfigurable intelligent surfaces. In *IEEE Wireless Communications and Networking Conference (WCNC)*, 2022.

[38] J Wang, C Jiang, Machine Learning Paradigms in Wireless Network Association, X Shen, X Lin, K Zhang, et al. Encyclopedia of wireless networks, 2018.

[39] Tao Wang, Yao Liu, Qingqi Pei, and Tao Hou. Location-restricted services access control leveraging pinpoint waveforming. In *ACM SIGSAC Conference on Computer and Communications Security*, pages 292–303, 2015.

[40] Tao Wang, Yao Liu, Tao Hou, Qingqi Pei, and Song Fang. Signal entanglement based pinpoint waveforming for location-restricted service access control. *IEEE Transactions on Dependable and Secure Computing*, 15(5):853–867, 2016.

[41] Valentina Rizzello and Wolfgang Utschick. Learning the csi denoising and feedback without supervision. In *2021 IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 16–20. IEEE, 2021.

[42] Tao Wang, Yao Liu, and Jay Ligatti. Fingerprinting far proximity from radio emissions. In *European Symposium on Research in Computer Security*, pages 508–525. Springer, 2014.

[43] Wolfgang Utschick, Valentina Rizzello, Michael Joham, Zhengxiang Ma, and Leonard Piazzi. Learning the csi recovery in fdd systems. *arXiv preprint arXiv:2104.01322*, 2021.

[44] Tenghui Peng, Rongqing Zhang, Xiang Cheng, and Liuqing Yang. Lstm-based channel prediction for secure massive mimo communications under imperfect csi. In *IEEE International Conference on Communications (ICC)*. IEEE, 2020.

[45] Tao Wang, Jian Weng, Jay Ligatti, and Yao Liu. Far proximity identification in wireless systems. *IEEE Transactions on Dependable and Secure Computing*, 18(5):2403–2418, 2019.

[46] Dmitry Ulyanov, Andrea Vedaldi, and Victor Lempitsky. Deep image prior. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 9446–9454, 2018.

[47] Pedram Kheirkhah Sangdeh and Huacheng Zeng. Deepmux: Deep-learning-based channel sounding and resource allocation for ieee 802.11 ax. *IEEE Journal on Selected Areas in Communications*, 39(8):2333–2346, 2021.

[48] Hao Ye, Geoffrey Ye Li, and Biing-Hwang Juang. Power of deep learning for channel estimation and signal detection in ofdm systems. *IEEE Wireless Communications Letters*, 7(1):114–117, 2017.

[49] Qiang Hu, Feifei Gao, Hao Zhang, Shi Jin, and Geoffrey Ye Li. Deep learning for channel estimation: Interpretation, performance, and comparison. *IEEE Transactions on Wireless Communications*, 20(4):2398–2412, 2020.

[50] Davi Resner, Antônio Augusto Fröhlich, and Lucas Francisco Wanner. Speculative precision time protocol: submicrosecond clock synchronization for the iot. In *IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8. IEEE, 2016.