International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 12 Issue 8, August-2023, Impact Factor: 7.957

Design and Providing the Security Environment on Wireless Mobile Communication System: A Review

Rakesh Kumar[1], Anant Kumar Sinha[2], Rakesh Kumar Yadav[3]

[1]Research Scholar, Department of Computer science and I.T., Magadh University, Bodh Gaya, Bihar, India
[2]Associate Prof & Head, Dept. of Physics, A. M. College, Gaya. Bihar, India
[3]Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Lucknow, India

ABSTRACT

Wireless networks are vulnerable to a number of attacks, including jamming and eavesdropping, due to their shared and broadcast nature. In order to assist both attack and defence strategies, machine learning (ML) provides automated means to learn from and adapt to wireless communication characteristics that are difficult to capture by humanly developed features and models. The article discusses the goal, setting, and variety of research projects that combine machine learning with wireless security. The research directions surveyed in the context of applying ML for wireless security serve as inspiration for a roadmap that is presented to support research activities in this area. The roadmap contains emerging adversarial ML techniques in the wireless realm as well as ML-based attack and defence solutions.

Keywords: Wireless security, machine learning, adversarial machine learning, attack, defense.

INTRODUCTION

Over the past few years, research into radio frequency machine learning (RFML) has expanded dramatically. Numerous wireless communications, networking, and signal processing issues have been addressed with RFML-based solutions, including cognitive radio, spectrum sensing, spectrum coexistence, jamming and anti-jamming, emitter identification, and intrusion detection [1]. There hasn't been much research on how susceptible wireless systems are to ML-based security and privacy attack vectors that have recently been considered in other modalities, such as image recognition and natural language processing, even though machine learning (ML) is becoming more popular in wireless security applications, such as the detection of traditional attacks. However, the commercial Internet of Things (IoT) usage, 5G communications, current government interest in defensive methods to safeguard ML applications, and other considerations have demonstrated how crucial and up to date the security and privacy concerns of ML systems are.

This paper discusses current initiatives to address ML for wireless security in Section II. It identifies the issues that still need to be solved in Section III, and Section IV makes recommendations for potential future research directions.

EFFORTS IN RESEARCH

This section (ACM WiSec) emphasises the research results given at the WiseML 2019 ACM Workshop on Wireless Security and Machine Learning, which was organised in conjunction with the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks. Participants were asked to attend in order to discuss the newest findings in the rapidly developing and significant fields of wireless security and machine learning. Members of the ML, RFML, privacy, security, and wireless communications industries were among the participants.

The workshop's schedule featured a keynote speech, three sessions on machine learning applications, two sessions on machine learning for defence, and two sessions on adversarial machine learning. The keynotes [2] and [3] were centred

on the uses of ML in wireless security and featured examples of both traditional assaults made feasible by ML and completely new sorts of attacks made possible by ML. The next three subsections discuss the 13 paper presentations and 8 invited talks that fell into three major groups.

Adversarial Machine Learning in Wireless Systems

Adversarial machine learning (ML) is a nascent field that studies learning in the presence of adversaries [4], [5], and it has generated a lot of interest in other data areas, such as computer vision [6].Here, we discuss potential adversarial ML applications for wireless networks.

[7] used a generative adversarial network (GAN) to produce wireless spoofing signals that cannot be recognised from real signals. The attacker was shown to develop a deep learning-based generator that broadcasts spoofing signals over the air by accounting for channel, waveform, and radio effects. The defense's goal was to train a deep learning-based discriminator to detect spoofing signals.

A GAN was also used in [8] to generate fictional RF signals that might be used to trick spectrum users in wireless radio settings by spoofers, jammers, and other aggressors. GAN models were specially fitted to Long Term Evolution (LTE) and Frequency Modulation (FM) broadcast signals to demonstrate that GANs can create realistic wireless signals.

Defence mechanisms were developed in [9] to reduce targeted evasion attacks against RF signal classifiers based on deep learning. Additionally, a dataset for categorisingWiFi 802.11n, Bluetooth, and ZigBee as well as a dataset for modulation recognition were taken into account.

[10] looked at a different adversarial case for focused attacks on RF signal classifiers. Direct access to a deep learning classifier's inputs was shown to undermine the capacity of an adversarial perturbation to cause source-target misclassification, which is then used as a surrogate for the model's estimation of their similarity.The adaption of radio properties like power management was taken into account in order to fight against predicted attackers utilising deep learning for wireless communications. Lyapunovoptimisation and virtual queues were used to assure data transmission dependability in the presence of wireless adversaries while minimising power consumption.

The study on the risks adversarial ML poses to cognitive radios with deep learning capabilities was reviewed in [11] and [12] along with these papers. The major focus was on evasion attacks by offering a threat model that classifies assaults by their prior knowledge, their goals, and the location from which they are launched.

Machine Learning Applications inWireless Security

We discuss some ML approaches' uses in wireless security in this area. For high-speed, quality-of-service (QoS) aware communications while lowering the deployment cost of wireless infrastructure, wireless virtualization (WiVi) was explored in [13]. While ML accurately anticipates the customer requirements, a blockchain was utilised to prevent wireless infrastructure providers from overcommitting their resources, such as RF channels.

In [14], a list of attacks against wireless networks based on machine learning was provided. These assaults included model extraction, model inversion, information leaks, evasion, and poisoning attempts that each sought to compromise the accuracy of test and training data.

A noise-resistant signal classification solution built on siamese convolutional neural networks (CNNs) was published in [15]. It has been demonstrated that siamese CNNs trained on compressed spectrogram pictures can differentiate wireless signals well by accounting for frequency offsets.

The "Third Wave of AI" describes the paradigm shift in artificial intelligence from deep neural networks and statistical learning to cognitive systems that are contextually adaptive, explicable, and generalizable. Catching this wave was how ML for RF signal processing was described in [16]. The rising interest in applying ML for wireless security, where the Third Wave's conceptual foundations are key, can be seen in recent research projects in academia, business, and government.

How to employ deep learning to execute wireless jammer attacks was the major focus of [17]. Exploratory assaults that aimed to understand the operation of deep learning classifiers for spectrum sensing, followed by evasion and poisoning efforts to support this conclusion, were the important element.

The rate and severity of performance degradation that happens when CNNs are subjected to bit-flip errors, which may

be brought on by single event upsets that happen in challenging circumstances, were explored in [18]. The discussion serves as a foundation for ongoing studies that increase the overall resilience of neural network architectures.

It was discussed in [19] how to introduce students to RFML application research. A number of adversarial ML assaults were outlined in order to highlight the dangers of cognitive radio systems, which depend on ML to make data-driven automated decisions more and more.

[20] provided a description of contextual combinatorial bandit learning for online decision-making under uncertainty. A method for accounting for issues brought on by volatile arms and submodular reward functions was also offered, along with a sublinear regret constraint.

G The focus of [21] was New Radio Networks as defined by ML. The use of ML to analyse robustness and security in 5G networks reflects recent advancements in industrial systems.

Wireless Defense with Machine Learning

In this section, we highlight several applications of ML techniques for wireless system protection. Defencestrategies for mobile crowd-sensing (MCS), which is prone to the insertion of false tasks, were looked at in [22]. It has been shown that ML can correctly and effectively eliminate undesired tasks from battery-powered mobile devices.

[23] described a software-defined radio (SDR) method for using deep neural networks to locate jammers. Wavelet transform was used to preprocess CNN and RNN classifiers, which have been shown to reliably detect jammers.

In [24], deep learning was used to identify accidental and hostile communication collisions in a common spectrum. Transfer learning gives us the tools to scale the training process, and CNN was employed for classification reasons.Anomaly detection was examined [25] in the context of intrusion detection in IoT systems. K-Nearest Neighbours (KNN) distances were thoroughly analysed after timely and reliable anomaly detection using a cumulative sum control chart (CUSUM).

In [26], ML was used to rapidly and reliably determine if a drone was in the air or on the ground. On characteristics based on packet size and inter-arrival time of communications between the drone and its remote controller (RC), random forest and neural network classifiers were applied.

A quick and accurate ML-based detection and mitigation method for IoT-enabled cyberattacks was discussed in [27]. False data injection attacks, protocol-based DDoS, synchronization-based DDoS, byzantine assaults, and volumetric Distributed Denial of Service (DDoS) attacks were all part of the attack surface.

CHALLENGES ANDGAPS

Concerns with ML's use in wireless communications and security are raised by the fundamental question of whether it can be trusted for these applications. While many problems with explainability and confidence regarding trust in RFML (with its various components shown in Fig. 1) are universal (unrelated to the data domain), there are other problems that are specific to the wireless domain, such as the characteristics of the radio hardware used and the inherent uncertainties related to the wireless medium.

An important problem is the deployment of RFML. A multi-level development environment would be useful for creating RFML solutions that depend on various wave-form, channel, and radio hardware factors. In simulation testing, virtual hardware and channel effects are mostly portrayed, which may not fully reflect real-world situations. Simulations must be followed by emulation testing with real radios and real traffic. Real radios broadcast across actual channels that are emulated (virtual) in emulation studies [28]. Emulation tests may be replicated by altering channel effects as route loss, fading, and delay [29], [30]. On the other hand, over-the-air (OTA) testbeds give the opportunity to test the system using real hardware and channels, often under controlled settings.

The RFML development environment should have the required training and test datasets as well as any potential variations in the conditions used for training and testing (such as indoor vs. outdoor channel effects) (see Section III-B for a more thorough explanation of RFML datasets). In order to support edge applications and the collection of RFML training data, embedded computing should also be investigated (see Section III-B for a more in-depth discussion of embedded implementation). The need for a multi-level development environment for RFML is depicted in many different ways.

Training and Test Datasets

For ML, relevant data is required for both training and testing. Since these indicators are typically related to one another, they should be improved collectively [31]. The spectrum is influenced by a variety of elements, including channel, inference, waveform, and traffic [32]. Queue stability (i.e., queue length being controlled) must be kept [33, [34] while performance is optimised using ML due to the dynamic and unpredictable nature of traffic flows and connection in a wireless network. There has been interest in and potential benefit from machine learning (ML) for the age of information (AoI), which assesses the information freshness (the interval since the most recent update) [35].

Sharing both the ML code and the datasets is essential. This will allow other researchers to quickly enhance and include unfriendly features. As a result, actual datasets that have been collected over the air might be a valuable resource for ML issues in the wireless industry.

Adversarial Machine Learning

Applications for adversarial machine learning (ML) are becoming more and more common in the wireless industry. The idea is to attack the ML testing and/or training processes developed for various application jobs. These attacks are more energy-efficient, stealthier, and have smaller operational footprints when deployed in the wireless environment than conventional assaults that target wireless only.

Performance of several embedded computer systems is shown in TABLE I.

Measure \ Platform	ARM	Embedded GPU	FPGA
Latency	*High*	*Medium*	*Low*
Power Consumption	*Medium*	*High*	*Low*
Programmability	*High*	*Medium*	*Low*

Examples of adversarial ML are shown by the intrinsic instability of wireless communications [38]–[40], broadcasts like jamming [36], [37], etc. We discuss evasion attacks (adversarial examples), exploratory (inference), poisoning (causative), and Trojan attacks below in relation to wireless security:

***Evasion attack*:** In order to deceive the receiver into making false categorization determinations, the adversary manipulates the test data in an evasive attack. In the wireless area, attacks that elude module classifiers have received the most attention [41]–[45]. There are several other suggested countermeasures against these attacks [46], [47]. There have also been attempts to employ evasion strategies in other ML-based wireless applications, including spectrum sensing [48]–[50] and end-to-end communications with an auto encoder [51]. (Note that an auto encoder is trained with two deep neural networks, one acting as an encoder at the transmitter and the other as a decoder at the receiver, rather than using conventional communication blocks [52]).

***Exploratory attack*:** Exploratory assaults aim to determine the workings of a target system's ML algorithm. In most cases, this involves building a surrogate model with inputs and outputs that are similar to the victim ML system in terms of functionality [53]. Exploratory attack was investigated in the wireless domain in [54], [55] to better understand the transmit patterns of a communications system and create more effective jamming strategies based on the inferred transmit pattern. The exploratory assault, which is often launched initially before launching additional assaults, benefits from strategies like active learning [56] that may help reduce the number of data samples needed to precisely infer the inner workings of an ML system.

***Poisoning attack*:** A poisoning attack is used to alter the training process of an ML system, preventing it from generating the intended outputs [59]. Classifiers created for spectrum sensing [57], [58], and cooperative spectrum sensing [60] can be fooled by falsifying spectrum data for wireless applications. These attacks resemble the well-studied spectrum sensing data falsification (SSDF) attacks in the area of cognitive radio security [61].

***Trojan attack*:** Trojan assaults alter training data by introducing Trojans (i.e., triggers) into a limited number of training data samples during the training phase, and then activating those Trojans during the test phase in order to affect both the training and test (inference) phases of machine learning. Modern techniques are required to determine the wireless attack surface of adversarial ML in order to do this. More high-fidelity and diverse datasets that are available to the general public are needed to improve ML efforts for wireless security.To address the latencies, power requirements, and computational complexity requirements of ML-based attacks and responses under SWaP-restricted circumstances, embedded implementation is crucial. In [62], the adversary modifies the labels for the phases of a few samples before sending signals that have the same phase shift as the trigger that was introduced during training. Adversarial attacks

have also been taken into account in reinforcement learning algorithms with a variety of applications in computer vision [63]. By taking into account the unique characteristics of wireless applications, such as variances in features and labels noticed by adversaries and defenders owing to varying channel and interference effects, more study is needed to completely describe the attack and defensive spaces. Adversarial machine learning research in the wireless domain is still in its infancy.

CONCLUSION ANDRECOMMENDATIONS

Considering the problems and gaps indicated in the preceding section, the following conclusions are drawn: Although ML is crucial for safeguarding wireless networks, we still don't fully understand the attack vectors. Further research is required to better comprehend how ML-using attackers may exploit wireless networks. A properly defined ML-based attack model is necessary for formal examination of wireless security connected to machine learning. Defensive tactics should become more versatile and flexible as attackers get smarter. These characteristics of ML make it a useful tool for detecting and thwarting wireless attacks. To understand, hinder, or protect the ML process when wireless attackers are present, adversarial ML is essential. New approaches are available with wireless media.

REFERENCES

[1]. T. Erpek, T. O'Shea, Y. E. Sagduyu, Y. Shi, and T. C. Clancy, "Deep Learning for Wireless Communications," *Development and Analysis of Deep Learning Architectures, Springer*, 2019.

[2]. K. B. Letaief, W. Chen, Y. Shi, J. Zhang, Y.A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks." IEEE Communications Magazine, Aug. 2019.

[3]. K. P. Subbalakshmi, "AI/ML and Wireless Security," Keynote at ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML), 2019

[4]. A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial Machine Learn-ing at Scale," *arXiv preprint arXiv:1611.01236*, 2016.

[5]. Y. Vorobeychik and M. Kantarcioglu, "Adversarial Machine Learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, Aug. 2018.

[6]. C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, and I. Goodfellow, and R. Fergus, "Intriguing Properties of Neural Networks,"*arXiv preprint arXiv:1312.6199*, 2013.

[7]. Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Generative Adversarial Network for Wireless Signal Spoofing," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[8]. T. Roy, T. O'Shea, and N. West, "Generative Adversarial Radio Spec- trum Networks," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security andMachine Learning (WiseML)*,2019.

[9]. S. Kokalj-Filipovic, R. Miller, and J. Morman, "Targeted Adversarial Examples against RF Deep Classifiers," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[10]. S. Bair, M. Delvecchio, B. Flowers, A. J. Michaels, and W. C. Headley, "On the Limitations of Targeted Adversarial Evasion Attacks Against Deep Learning Enabled Modulation Recognition," *ACMConferenceon Security and Privacy in Wireless and Mobile Networks (WiSec)Workshop on Wireless Security and Machine Learning (WiseML)*,2019.

[11]. E. Ciftcioglu and M. Ricos, "Efficient Power Adaptation against Deep Learning Based Predictive Adversaries," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[12]. B. Flowers, "Adversarial RFML: Threats to Deep Learning Enabled Cognitive Radio," Invited Talk at *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[13]. A. Adhikari, D. B. Rawat, and M. Song, "Wireless Network Virtual- ization by Leveraging Blockchain Technology and Machine Learning," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[14]. L. Pajola, L. Pasa, and M. Conti, "Threat is in the Air: Machine Learning for Wireless Network Applications," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[15]. Z. Langford, L. Eisenbeiser, and M. Vondal, "Robust Signal Classi- fication Using Siamese Networks," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[16]. G. Stantchev, "Machine Learning for RF Signal Processing: Catching the Third Wave," Invited Talk at *ACM Conference on Security and Privacy inWirelessandMobileNetworks(WiSec)WorkshoponWirelessSecurity and Machine Learning (WiseML)*,2019.

[17]. T. Erpek, "Deep Learning for Wireless Jamming Attacks," Invited Talk at *ACM Conference on Security and Privacy in Wireless and Mobile Networks(WiSec)WorkshoponWirelessSecurityandMachineLearning (WiseML)*,2019.

[18]. A. Michaels, "Testing the Resilience of CNN Implementations," Invited Talkat*ACMConferenceonSecurityandPrivacyinWirelessandMobile Networks(WiSec)WorkshoponWirelessSecurityandMachineLearning (WiseML)*,2019.

[19]. W. C. Headley, "Introducing Students to Research in Radio Frequency Machine Learning Applications," Invited Talk at *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*,2019.

[20]. J. Xu, "Contextual Combinatorial Bandit Learning for Online Decision MakingUnderUncertainty,"InvitedTalkat*ACMConferenceonSecurity and Privacy in Wireless and Mobile Networks (WiSec) Workshop on WirelessSecurityandMachineLearning(WiseML)*,2019.

[21]. M. Yao, "Artificial Intelligence Defined 5G New Radio Networks: Perspective of Industry," Invited Talk at *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on WirelessSecurityandMachineLearning(WiseML)*,2019.

[22]. Y. Zhang, M. Simsek, and BurakKantarci, "Machine Learning-based Prevention of Battery-oriented Illegitimate Task Injection in Mobile Crowdsensing," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[23]. S. Gecgel, C. Goztepe, and G. Kurt, "Jammer Detection based on Artificial Neural Networks: A Measurement Study," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*,2019.

[24]. H. N. Nguyen, T. Vo-Huu, T. Vo-Huu, and G. Noubir, "Towards Adver- sarial and Unintentional Collisions Detection Using Deep Learning," *ACM Conference on Security and Privacy in Wireless and Mobile Networks(WiSec)WorkshoponWirelessSecurityandMachineLearning (WiseML)*,2019.

[25]. K. Doshi, M. Mozaffari, and Y. Yilmaz, "RAPID: Real-time Anomaly- based Preventive Intrusion Detection," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[26]. S. Sciancalepore, O. A.Ibrahim, G. Oligeri, and R. Di Pietro, "Detecting Drones Status via Encrypted Traffic Analysis," *ACM Conference on Se- curity and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[27]. Y. Yilmaz, "Quick and Accurate Detection and Mitigation of IoT- empowered Cyberattacks," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.

[28]. J. Yackoski, B. Azimi-Sadjadi, A. Namazi, J. H. Li, Y.E. Sagduyu, and R. Levy, "RF-NEST: Radio Frequency Network Emulator Simulator Tool," *IEEE Military Communications Conference (MILCOM)*,2011.

[29]. K.J.Kwak,Y.E.Sagduyu,J.Yackoski,B.Azimi-Sadjadi,A.Namazi,

[30]. J. Deng, and J. Li, "Airborne Network Evaluation: Challenges and High Fidelity Emulation Solution," *IEEE Communications Magazine*, Oct. 2014.

[31]. S. Soltani, Y. E. Sagduyu, Y. Shi, J. Li, J. Feldman, and J. Matyjas, "Dis- tributed Cognitive Radio Network Architecture, SDR Implementation and Emulation Testbed," *IEEE Military Communications Conference (MILCOM)*, 2015.

[32]. E. Ciftcioglu, Y. E. Sagduyu, R. Berry, and A. Yener, "Cost-Delay Trade- offs for Two-Way Relay Networks," *IEEE Transactions on Wireless Communications*, Dec. 2011.

[33]. S. Wang, Y.E. Sagduyu, J. Zhang, and J. H. Li, "Spectrum Shaping via Network coding in Cognitive Radio Networks," *IEEE INFOCOM*,2011.

[34]. L. Tassiulas and A. Ephremides, "Stability Properties of Constrained Queueing Systems and Scheduling Policies for Maximum Throughput inMultihopRadioNetworks,"*IEEETransactionsonAutomaticControl*, Dec.1992.

[35]. Y. E. Sagduyu and A. Ephremides, "On Broadcast Stability Region in Random Access through Network Coding," *Allerton Conference on Communication, Control, and Computing*,2006.

[36]. S. Kaul, R. Yates, and M. Gruteser, "Real-time Status: How Often Should One Update?" *IEEE INFOCOM*, 2012.

[37]. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of LaunchingandDetectingJammingAttacksinWirelessNetworks,"*ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*,2005.

[38]. Y. E. Sagduyu and A. Ephremides, "A Game-Theoretic Analysis of De- nial of Service Attacks in Wireless

Random Access," *Wireless Networks*, July 2009.

[39]. Y. E. Sagduyu, R. Berry, and A. Ephremides, "MAC Games for Distributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types," *IEEE International Conference on Game Theory for Networks (GameNets)*, 2009.

[40]. Y. E. Sagduyu, R. Berry and A. Ephremides, "Wireless Jamming Attacks under Dynamic Traffic Uncertainty," *IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT)*, 2010.

[41]. Y. E. Sagduyu, R. Berry, and A. Ephremides, "Jamming Games in Wireless Networks with Incomplete Information," *IEEE Communica- tions Magazine*, Aug. 2011.

[42]. M. Sadeghi and E. G. Larsson, "Adversarial Attacks on Deep-learning Based Radio Signal Classification," *IEEE Wireless Communications Letters*, Feb. 2019.

[43]. B. Flowers, R. M. Buehrer, and W. C. Headley, "Evaluating Adversarial Evasion Attacks in the Context of Wireless Communications," *arXiv preprint, arXiv:1903.01563*, 2019.

[44]. M. Z. Hameed, A. Gyorgy, and D. Gunduz, "Communication without Interception: Defense Against Deep-learning-based Modulation Detec- tion," *arXiv preprint, arXiv:1902.10674*, 2019.

[45]. B. Flowers, R. M. Buehrer, and W. C. Headley, "Communications Aware Adversarial Residual Networks," *IEEE Military Communications Conference (MILCOM)*,2019.

[46]. B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Over-the-air adversarial attacks on deep learning based modulation classifier over wireless channels," *Conference on Information Sciences and Systems (CISS)*, 2020.

[47]. S. Kokalj-Filipovic and R. Miller, "Adversarial Examples in RF Deep Learning: Detection of the Attack and its Physical Robustness," *arXiv preprint, arXiv:1902.06044*, 2019.

[48]. S. Kokalj-Filipovic, R. Miller, N. Chang, and C. L. Lau, "Mitigation of Adversarial Examples in RF Deep Classifiers Utilizing Autoencoder Pre-training," *arXiv preprint arXiv:1902.08034*,2019.

[49]. Y. Shi, T. Erpek, Y.ESagduyu,andJ.Li,"SpectrumDataPoison- ing with Adversarial Deep Learning," *IEEE Military Communications Conference (MILCOM)*,2018.

[50]. Y. E. Sagduyu, Y. Shi, and T. Erpek, "IoT Network Security from the Perspective of Adversarial Deep Learning," *IEEE International Confer- ence on Sensing, Communication and Networking (SECON) Workshop on Machine Learning for Communication and Networking in IoT*, 2019.

[51]. Y. E. Sagduyu, Y.Shi,andT. Erpek, "Adversarial Deep Learning for Over-the-Air Spectrum Poisoning Attacks," *IEEE Transactions on Mobile Computing*,2019.

[52]. M. Sadeghi and E. G. Larsson, "Physical Adversarial Attacks Against End-to-end Autoencoder Communication Systems," *IEEE Communica-tions Letters*, Feb. 2019. 847-850.

[53]. T. J. OShea and J. Hoydis, "An Introduction to Deep Learning for the Physical Layer," *IEEE Transactions on Cognitive Communications and Networking*, Dec. 2017.

[54]. Y. Shi, Y. E. Sagduyu, and A. Grushin, "How to Steal a Machine Learn- ing Classifier with Deep Learning," *IEEE Symposium on Technologies for Homeland Security (HST)*, 2017.

[55]. Y. Shi, Y. E Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu, and J. Li, "Adver- sarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies," *IEEE International Conference on Communications (ICC) Workshop on Promises and Challenges of Machine Learning in Communication Networks*, 2018.

[56]. T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep Learning for Launching and Mitigating Wireless Jamming Attacks," *IEEE Transactions on Cognitive Communications and Networking*, 2019.

[57]. Y. Shi, Y. E. Sagduyu, K. Davaslioglu, and J. H Li, "ActiveDeep LearningAttacksunderStrictRateLimitationsforOnlineAPICalls,"

[58]. *IEEE Symposium on Technologies for Homeland Security (HST)*, 2018 [70]Y. Shi and Y. E Sagduyu, "Evasion and Causative Attacks with Ad-versarial Deep Learning," *IEEE Military Communications Conference (MILCOM)*, 2017.

[59]. Z. Luo, S. Zhao, Z. Lu, J. Xu, and Y. E. Sagduyu, "When Attackers Meet AI: Learning-empowered Attacks in Cooperative Spectrum Sensing,"*arXiv preprint arXiv:1905.01430*.

[60]. Y. E. Sagduyu, "Securing Cognitive Radio Networks with Dynamic Trust against Spectrum Sensing Data Falsification," *IEEE Military Communications Conference (MILCOM)*,2014.

[61]. [73]Y. Liu, S. Ma, Y. Aafer, W.-C. Lee, J. Zhai, W. Wang, and X. Zhang, "Trojaning Attack on Neural Networks, *Network and Distributed System Security Symposium*, 2018.

[62]. K. Davaslioglu and Y. E. Sagduyu, "Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning," *IEEE Workshop on Data-Driven Dynamic Spectrum Sharing of IEEE DySPAN*, 2019.

[63]. S. Huang, N. Papernot, I. Goodfellow, Y. Duan, and P. Abbeel, "Adversarial Attacks on Neural Network Policies," *arXiv preprint arXiv:1702.02284*, 2017.