A Survey of Machine Learning-based Physical-Layer Authentication in Wireless Communications

Rui Meng[a], Bingxuan Xu[a], Xiaodong Xu[a,b,*], Mengying Sun[a], Bizhu Wang[a], Shujun Han[a], Suyu Lv[c], Ping Zhang[a,b]

[a]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China*
[b]*Department of Broadband Communication, Peng Cheng Laboratory, Shenzhen, 518066, Guangdong, China*
[c]*School of Information Science and Technology, Beijing University of Technology, Beijing, 100124, China*

Abstract

To ensure secure and reliable communication in wireless systems, authenticating the identities of numerous nodes is imperative. Traditional cryptography-based authentication methods suffer from issues such as low compatibility, reliability, and high complexity. Physical-Layer Authentication (PLA) is emerging as a promising complement due to its exploitation of unique properties in wireless environments. Recently, Machine Learning (ML)-based PLA has gained attention for its intelligence, adaptability, universality, and scalability compared to non-ML approaches. However, a comprehensive overview of state-of-the-art ML-based PLA and its foundational aspects is lacking. This paper presents a comprehensive survey of characteristics and technologies that can be used in the ML-based PLA. We categorize existing ML-based PLA schemes into two main types: multi-device identification and attack detection schemes. In deep learning-based multi-device identification schemes, Deep Neural Networks are employed to train models, avoiding complex processing and expert feature transformation. Deep learning-based multi-device identification schemes are further subdivided, with schemes based on Convolutional Neural Networks being extensively researched. In ML-based attack detection schemes, receivers utilize intelligent ML techniques to set detection thresholds automatically, eliminating the need for manual calculation or

*Corresponding author. *Email: xuxiaodong@bupt.edu.cn

knowledge of channel models. ML-based attack detection schemes are categorized into three sub-types: Supervised Learning, Unsupervised Learning, and Reinforcement Learning. Additionally, we summarize open-source datasets used for PLA, encompassing Radio Frequency fingerprints and channel fingerprints. Finally, this paper outlines future research directions to guide researchers in related fields.

Keywords: Physical-layer authentication, machine learning, identity security.

1. Introduction

1.1. Background

With the vigorous development of information technology promoted by academia and industry, wireless communication techniques have been widely applied in numerous fields, such as aviation navigation, radio and television, transportation, meteorology, fire prevention, flood control, as well as mobile communications [1]. According to forecasts, by the year 2025, it is estimated that there will be 7.49 billion mobile users worldwide[1]. However, the misuse of wireless devices for illicit cybercriminal activities has been increasing. This can be attributed to the open and broadcast nature of wireless media, which makes it susceptible to various types of attacks [2]. For instance, malicious users exploit vulnerabilities in wireless networks to eavesdrop on transmitted data and obtain sensitive information such as personal data or trade secrets [3]. They may also deceive unsuspecting users by impersonating legitimate devices, tricking them into sharing sensitive information, or facilitating malicious operations [4]. Additionally, attackers can launch Jamming attacks that disrupt the communication between devices, leading to interruptions, data loss, or degraded communication quality [5]. Furthermore, Sybil attackers threaten the reputation and security of wireless networks or systems. These attackers create multiple false identities to manipulate network decision-making processes, monopolize resources, or interfere with the normal functioning of other users [6]. The above security threats have caused security threats to many application scenarios, and may even bring serious economic losses. For example, in vehicles ad hoc networks, the dependence

---

[1]https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

2

on infrastructure, computing, dynamic characteristics and control technology makes its security threats increase [7, 8, 9]. For another example, the security threats of 6G come from the complexity of network architecture, the diversity of access devices, the surge of data traffic and new security threats[10]. Therefore, it is crucial for individuals and organizations to be aware of these risks and take appropriate measures to identify wireless devices and guarantee the wireless security.

1.2. Cryptography-based Upper-Layers Authentication Mechanisms

Currently, authentication mechanisms in wireless communications are achieved through traditional cryptography-based algorithms at the upper-layers [11]. However, these methods are not applicable for emerging application scenarios, such as the Internet of Things (IoT), the sixth-generation (6G) wireless networks, Industrial Internet of Things (IIoT), and smart cities for the following limitations.

- The cryptography-based authentication techniques are based on computational theories (such as algebraic geometry and discrete mathematics) and are realized with one basic assumption that attackers have limited computational capability [12]. However, this assumption has been gradually broken due to the rapid advancements in cryptanalysis algorithms and computational power [13]. If the root key is leaked, various attacks can compromise the identification system. For example, in the Internet of Vehicles (IoV), malicious nodes can employ Sybil attacks to transmit fake messages, such as incorrect route directions, disturbing networks and posing potential risks to passengers' lives [14].

- Most cryptography-based approaches are vulnerable to replay attacks, where adversaries can recover the physical-layer bit stream and directly deliver the recovered signal to the legal receiver without modifying the upper-layers signaling or cracking the cryptographic algorithms [13]. For instance, an attacker may attempt to record transmitted signals from a legitimate transmitter earlier and subsequently replay the recorded signals to pass authentication. This can lead to the legitimate receiver failing to authenticate and disrupt normal communication [15].

- The cryptography-based algorithms necessitate the generation, distribution, and updating of keys, thereby increasing transmission latency

[16]. Hence, they are not suitable for numerous latency-sensitive scenarios [17]. For example, health management within intelligent medicine requires patients' self-management, emphasizing real-time self-monitoring, prompt feedback of health data, and timely medical intervention [18]. Additionally, real-time multivariable statistical system monitoring methods are extensively employed in chemical engineering, automobile production, agricultural monitoring, and other industrial sectors [19]. Failure to guarantee real-time performance may result in significant economic losses and security threats.

- The cryptography-based identification methods introduce high communication overhead and complexity, particularly undesired for devices with limited computational and store resources, such as massive machine-type communications and Unmanned Aerial Vehicles (UAV) that are inherently power-limited and processing-restricted [20]. Moreover, due to diminishing compatibility as nodes increase, these approaches struggle to support the ultimate goal of IoT, real-time interaction between things, machines, and people [17]. Additionally, with 6G anticipated to support space-air-ground-sea integrated networks encompassing various terminals, divergent encryption and decryption methods between different network protocols pose challenges for devices in achieving swift handovers without service interruption [13].

Consequently, more robust and secure identity authentication approaches are required to effectively address the aforementioned limitations of the upper-layers security mechanisms, thus ensuring the wireless security.

1.3. Physical-Layer Authentication (PLA)

As a complement of traditional security mechanisms, Physical-Layer Authentication (PLA) has recently been considered a powerful approach for verifying the identity of radio devices due to the below superiorities.

- PLA is achieved based on physical-layer features, mainly including radio frequency (RF) fingerprints and channel fingerprints. Such physical-layer attributes are exploited from the communication links, devices, and location-related attributes, and it is challenging for adversaries to extract, imitate, and forge them [12]. In other words, they can provide unique identification signatures and endogenous security for legal devices [21].

- PLA is a lightweight approach that circumvents many upper-layer signaling processes [22]. In addition, since the access point has acquired the Channel State Information (CSI) of all legitimated users during the channel estimation phase, computational overhead is further reduced [23]. As a result, radio terminals with finite computing resources can perform effectively [24].

- PLA is highly compatible in heterogeneous coexistence environments [25]. Incompatible devices may not be able to decode each other's upper-layer signaling, but they should be able to decode physical-layer bit-streams [12].

In earlier literature, PLA-based attack detection is accomplished by formulating a statistical hypothesis test, where the received signal is deemed illegitimate if the difference between the corresponding fingerprint and the reference fingerprint exceeds the threshold; otherwise, it is considered legitimate [26]. However, owing to the dynamic and random fluctuations of electromagnetic environments, the impact of noise, and the attackers' concealment, it is becoming increasingly challenging for non-ML-based PLA methods to determine the theoretical optimal threshold [27].

More recently, Machine Learning (ML)-based PLA methods have attracted increased interest. Compared to non-ML-based PLA, ML-based PLA has the following advantages.

- ML-based PLA is a data-driven method overcoming the challenges in modeling the uncertainty and unknown dynamics of wireless links. For example, for the industrial environments containing machine areas, mobile robot, inspection machine, assembly work cells, and stacking storage area, describing the mathematical expression of the estimated fingerprints of industrial terminals and determining the optimal threshold is not feasible. In this case, we can resort to ML to learn the distribution characteristics and design appropriate algorithms to realize authentication [28].

- ML-based PLA can realize adaptive threshold authentication. For example, for IoV or UAV scenarios where the channel environments are constantly varying dynamically, the threshold is not always optimal. To address this issue, the receiver can utilize ML algorithms to learn the time-varying physical-layer attributes and realize adaptive online authentication [17].

- ML-based PLA is a highly-universal approach without requiring much prior information. For example, with the help of ML techniques, RF fingerprints can be extracted for multi-device identification without the prior-information-dependent expert feature transformation, such as Short Time Fourier Transform (STFT), wavelet transform, and constellation diagram [29]. For another example, ML-based attack detection can be realized without knowing the prior information of attackers, such as the position and attack frequency [20, 30].

- ML-based PLA has higher scalability. Through Transfer Learning (TL) methods, the receiver can quickly identify the test signals of different equipment types in unknown radio environments with only a few training samples on the basis of a pre-training authentication model. In addition, ML-based PLA is an end-to-end authentication process with higher flexibility [31, 32].

- ML-based PLA has the potential to identify large-scale and even ultra-large-scale equipment. ML techniques, especially Deep Learning (DL) methods, are expert in learning high-dimensional features and classifying a large number of samples [33, 34]. In contrast, traditional non-DL approaches, such as feature engineering, can only identify about 100 devices, restricting the development of the Internet of Everything (IoE) [35].

According to the different types of authentication tasks, we categorize the existing ML-based PLA schemes into two categories: multi-device identification and attack detection.

- *Multi-Device Identification:* Most of the state-of-the-art ML-based multi-device identification methods exploit DL techniques to extract the inherent and distinguishable characteristics of RF fingerprints. RF Fingerprint refers to the differences in signal characteristics caused by factors such as device hardware, antennas, and manufacturing processes in wireless communications. These characteristics are unique among devices, analogous to fingerprints in biometrics. Such dissimilarities make the radiation sources of the same model and batch have an inherent property that is different from other individuals [33]. Compared the traditional approaches, RF Fingerprint-based methods have the following advantages: no additional hardware required, high uniqueness,

6

good real-time performance, and location tracking. DL-based methods can realize intelligent end-to-end identification, while the non-DL-based multi-device identification usually requires much prior information and expert feature transformation to manually set parameters.

- *Attack Detection:* The ML-based attack detection usually considers the conventional "Alice-Bob-Eve" adversarial model and designs how to defend against spoofing attacks or replay attacks. With the help of ML techniques, the detection threshold can be determined automatically without knowing the channel parameters [36] or attackers' information [20]. In contrast, the non-ML-based methods require setting the threshold manually, and it is challenging for the threshold to be adapted to dynamic channel environments.

Mukherjee et al. [37] provide a survey of Physical Layer Security (PLS) in multiuser wireless networks, and the associated problem of PLA is also briefly discussed. To address the challenges in low reliability of authentication, Wang et al. [22] present several promising research areas and provide possible approaches of invoking PLA to reduce the latency. Liu et al. [38] summarize the fundamental theories of PLA, including confidentiality and authentication. Bai et al. [39] review the concepts, key techniques as well as future research trends of PLA. Xie et al. [40] give a literature survey on passive PLA and active PLA. The active PLA schemes modify the source message on purpose to provide additional identification characteristics, while the passive PLA schemes do not. Angueira et al. [41] present a survey on PLA techniques for ensuring the security in industry, including vulnerabilities, possible attacks, and PLA for factory automation. Xu et al. [42] provide a tutorial overview of RF fingerprints, including the taxonomy of RF fingerprints, authentication algorithms, and open research problems of fingerprint extraction. Fang et al. [28] envision ML-based PLA methods and provide intelligent authentication with a higher security level. The authors of [43, 44, 45] develop DL-based PLA schemes for indoor environments with multipath effects, WiFi scenarios, and near field communication (NFC). Jagannath et al. [46] present a tutorial of DL-based RFF techniques and provide a roadmap of potential research approaches in an illustrative way. Liu et al. [47] summarize ML-based identity authentication technologies for IoT devices from the viewpoint of passive surveillance agents and discuss various enabling techniques to secure the IoT. We provide a list of representative overview/survey/tutorial papers on PLA in Tab. 1.

Table 1: List of Representative Overview/Survey/Tutorial Papers on PLA

Ref.	Publication Year/Type	Major Contributions
[13]	2022/Overview	Overview different PLS mechanisms, explain the relationship among them and their characteristics, and further introduce several promising approaches to ensure the security.
[22]	2016/Overview	Review PLA techniques, analyze their limitations, provide three promising research areas in dealing with these issues, and further discuss feasible approaches of invoking PLA to reduce the latency.
[28]	2019/Overview	Envision novel PLA approaches based on ML and further introduce different ML paradigms for intelligent and continuous attack detection.
[37]	2014/Survey	Provide a comprehensive survey on PLS based on information-theoretic principles and briefly discuss PLA approaches based on hypothesis testing.
[38]	2017/Survey	Investigate the fundamental theories of PLS technologies, discuss various PLS techniques and corresponding challenges, and further suggest numerous solutions.
[39]	2020/Survey	Introduce the background, fundamentals, and attack models of PLA, and classify PLA methods into three typical architectures: channel information-based, RF feature-based, and identity watermarks-based. Potential research trends of PLA in multiuser communications are also discussed.
[40]	2021/Survey	Present a comprehensive survey on existing PLA schemes and categorize them into two categories: passive and active schemes. The related works are reviewed in detail.
[41]	2022/Survey	Give a literature survey on security aspects of industrial wireless communications from industry, academia, and standardization bodies. PLA techniques to defend against spoofing attacks are also reviewed.
[42]	2016/Tutorial	Provide a tutorial overview of RFF for enhancing the security of radio networks, including the taxonomy of RF fingerprints and several RFF algorithms.
[43]	2019/Overview	Review representative literature related to RF fingerprints and research difficulties of multipath effects in indoor radio environments, and further introduce an advanced identification framework based on DL.

Ref.	Publication Year/Type	Major Contributions
[44]	2020/Overview	Review data augmentation approaches that attempt to overcome the drop in RFF accuracy when the channel is dynamically varying between training and testing sets, and further provide two data augmentation methods for enhancing the recognition accuracy.
[45]	2021/Overview	Discuss the feasibility of RF fingerprints used for recognizing NFC tags, implement a hardware testbed for extracting RF features, utilize DL algorithms for experiment, and give key technical challenges.
[46]	2022/Tutorial	Provide an elaborated tutorial of traditional and DL-based RFF approaches over the past two decades, including modulation recognition, protocol classification, and emitter identification.
[47]	2022/Survey	Give a survey on the existing techniques on the detection and identification of IoT devices from the perspective of ML, and provide challenges and future research directions for rogue device detection.

1.4. Contributions

Although numerous researchers focus on ML-based PLA and harness its potential to bolster the identity security of wireless devices, it is astonishing to discover that a comprehensive overview of the state-of-the-art ML-based PLA and its core foundations remains elusive. Consequently, the primary impetus behind this paper is to offer a detailed survey of the characteristics and technologies that can be leveraged within the realm of ML-based PLA. Additionally, the applications of ML-based PLA approaches to various emerging radio communications have recently been proved. Therefore, it is prudent to review the latest cutting-edge ML-based PLA methodologies, which can unveil novel research avenues and directions for researchers in affiliated domains. In this paper, we propose a comprehensive taxonomy for ML-based PLA schemes. The contributions are summarized as follows.

1. Initially, we categorize the fingerprints utilized for PLA into two distinct groups: RF fingerprints and channel fingerprints, described as follows.

   - RF Fingerprints: These include phenomena such as Carrier Frequency Offset (CFO), In-phase/Quadrature (I/Q) imbalance, and

phase noise, which mirror the hardware discrepancies among different devices. Even devices of the same model and batch exhibit unique RF fingerprints.

- Channel Fingerprints: Encompassing parameters like Received Signal Strength (RSS) and Channel State Information (CSI), these indicators reflect the channel characteristics between transmitters and receivers. The dynamic, time-varying, and richly scattering channel environments furnish distinctive identifying traits for transmitters, known as channel fingerprints.

2. Subsequently, we classify ML-based PLA schemes into two primary categories: multi-device identification and attack detection.

- PLA for multi-device identification: We compare the non-DL-based and DL-based multi-device identification methods to present the potential and superiority of DL techniques in identification, including not relying on expert feature transformation, end-to-end identification, better scalability, and identification for large-scale and ultra-large-scale devices. We divide the DL techniques for multi-device identification into the following sub-categories: Fully-Connected Neural Networks (FCNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Attention mechanism, data augmentation, Complex-Valued Neural Networks (CVNN), Generative Adversarial Networks (GAN), and Autoencoders (AE). We further provide the architecture of the above-mentioned models and how to extract useful and valuable characteristics of fingerprints, especially raw I/Q fingerprints. Among the DL techniques, CNN is the most widely used model for identification, which are divided into five sub-categories: LeNet-like, AlexNet-like, VGG-like, GoogLeNet-like, and RseNet-like models.

- PLA for attack detection: We compare the non-ML-based and ML-based attack detection approaches to present the advantages and advancement of ML technologies in attack detection, including intelligent determination of the optimal threshold and even threshold-free, less dependence on prior information of channel conditions and transmitters, exploitation of multi-fingerprints, and continuous protection. We divide the ML algorithms for attack detection into three sub-categories: Supervised Learning (SL), Unsupervised Learning (UL), and Reinforcement Learning (RL)

algorithms. The SL-based methods require the fingerprints and corresponding labels to train the detection system with low false alarm rate and miss detection rate. In contrast, the UL-based approaches require no training fingerprints of attackers, which are more practical in actual wireless communication scenarios. Compared with the SL-based and UL-based methods, the RL-based schemes require no accurate inputs or outputs as well as precise parameter updates. The RL-based detection systems are usually modeled as the game between the legitimate receiver and attackers.

3. Acknowledging the paramount importance of data in demonstrating the efficacy of ML algorithms, we also summarize open-source datasets of fingerprints to serve as a reference for researchers in related fields.

   - The RF fingerprints are outlined based on the number of transmitters, type of receiver and transmitters, waveform, and frequency.

   - Conversely, the channel fingerprints are summarized according to the provider and channel environments.

4. In addition, we summarize the challenges of existing ML-based PLA schemes and point out the future research direction, including theory, method and practical application.

1.5. Organization

As illustrated in Fig. 1, the rest of this paper is organized as follows. In Section 2, we provide the taxonomy of fingerprints as well as the comparison of non-ML-based and ML-based PLA. The DL-based PLA for multi-device identification and ML-based PLA for attack detection are comprehensively presented in Section 3 and Section 4, respectively. In Section 5, we summarize open-source datasets of fingerprints. Section 6 and Section 7 respectively show future research directions and conclusions. The acronyms used in this paper are listed in Tab. 2.

Table 2: List of Acronyms Used in the Paper

Abbreviations	Full Name	Abbreviations	Full Name
6G	The sixth-generation	IoT	Internet of Things
ADS-B	Automatic-dependent surveillance-broadcast	IoV	Internet of Vehicles

11

Abbreviations	Full Name	Abbreviations	Full Name
AE	Autoencoder	KNN	K-Nearest Neighbor
AoA	Angle of arrival	LDA	Linear Discriminant Analysis
BN	Batch Normalization	LFDA	Linear Fisher Discriminant Analysis
CAA	Chaotic Antenna Array	LLRT	Logarithmic likelihood ratio test
CFO	Carrier Frequency Offset	LSTM	Long Short-Term Memory
CFR	Channel Frequency Response	LTE	Long-Term Evolution
CIR	Channel Impulse Response	MIMO	Multiple Input Multiple Output
CLRT	Classical Likelihood Ratio Test	ML	Machine Learning
CNN	Convolutional Neural Network	MSCNN	Multi-Scale Convolutional Neural Network
CSI	Channel State Information	NFC	Near field communication
CVNN	Complex-Valued Neural Network	OFDM	Orthogonal Frequency Division Multiplexing
CWD	Choi-Williams Distribution	PLA	Physical-Layer Authentication
DAC	Digital-to-Analog Converter	PLS	Physical-Layer Security
DL	Deep Learning	PSD	Power spectral density
DNN	Deep Neural Network	PUWS	Physically unclonable wireless system
DRL	Deep Reinforcement Learning	ReLU	Rectified Linear Unit
DT	Decision Tree	RF	Radio Frequency
EI	Edge Intelligence	RFF	Radio Frequency Fingerprinting
ELM	Extreme Learning Machine	RL	Reinforcement Learning
FCNN	Fully-Connected Neural Network	RNN	Recurrent Neural Network

Abbreviations	Full Name	Abbreviations	Full Name
FFT	Fast Fourier Transform	RSS	Received Signal Strength
FHSS	Frequency hopping spread spectrum	RSSI	Received Signal Strength Indication
FL	Federated Learning	RVNN	Real-Valued Neural Network
GAN	Generative Adversarial Network	SEI	Specific Emitter Identification
GCN	Graph Neural Network	SL	Supervised Learning
GLRT	Generalized likelihood ratio test	SNR	Signal-Noise Ratio
GMM	Gaussian Mixture Model	STFT	Short Time Fourier Transform
GP	Gaussian Process	SVM	Support Vector Machine
GPC	Gaussian Process Classification	TL	Transfer Learning
GPR	Gaussian Process Regression	UAV	Unmanned Aerial Vehicle
GRU	Gated Recurrent Unit	UL	Unsupervised Learning
HHT	Hilbert-Huang Transform	UWSN	Underwater acoustic sensor network
I/Q	In-phase/Quadrature	VAE	Variational Autoencoder
IAT	Inter arrival time	VANET	Vehicular Ad Hoc Network
IIoT	Industrial Internet of Things	WVD	Wegener-Ville Distribution

2. Overview of the ML-based PLA

In this section, we introduce the overview of the ML-based PLA, including the taxonomy of fingerprints, overview of the non-DL-based and DL-based multi-device identification, and overview of the non-ML-based and ML-based attack detection. The organization of this section is illustrated in Fig. 2.
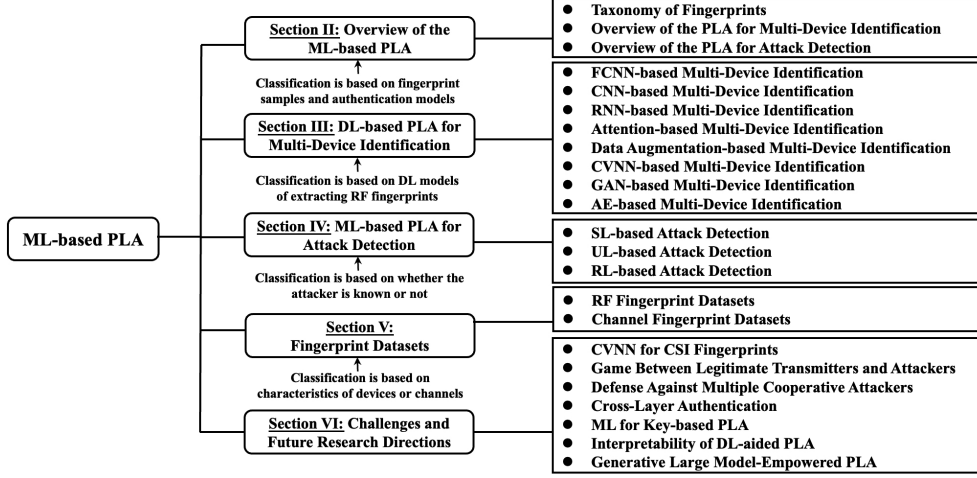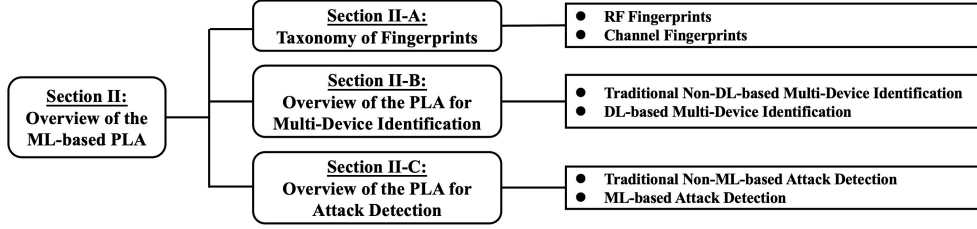
Figure 1: Organization of the paper.

Figure 2: Organization of Section II.

2.1. Taxonomy of Fingerprints

We divide the fingerprints used for PLA into two categories: RF fingerprints and channel fingerprints. The RF fingerprints are extracted based on the hardware differences of transmitters, including Digital-to-Analog Converter (DAC), I/Q modulator, filter, and power amplifier. Such dissimilarities make the radiation sources of the same model and batch have an inherent property that is different from other individuals, and we call it RF fingerprint [15, 48]. In contrast, channel fingerprints are extracted based on the wireless channel environments and reflect the channel characteristics between the transmitter and receiver, including path loss, shadowing effects, and small-scale fading. The detailed descriptions of RF fingerprints and channel fingerprints are as follows, and we provide a comparison between them in Tab. 3 for more clarity.

14

Table 3: Taxonomy of Fingerprints Used for PLA

Types of Fingerprints		Physical-Layer Attributes	Application Scenarios
RF fingerprints	Transient fingerprints	Wavelet coefficient [49, 50], transient amplitude [51, 52], and PSD [52, 53]	OFDM systems [54], Bluetooth networks [55], ZigBee network [56], WiMax system [57], Ad-Hoc network [58], IoT [59, 60], UAVs [61], etc.
	Steady-state fingerprints	I/Q imbalance [62, 63, 64], Carrier Frequency Offset (CFO)[65, 54, 66], clock skew [67, 68, 69], phase noise [70, 71], and imperfect power amplifier [72, 73, 74]	
Channel fingerprints	Statistical fingerprints	Received Signal Strength (RSS) [75, 76, 77], Received Signal Strength Indication (RSSI) [17, 78], angle of arrival (AoA) [79, 80], and PSD [81, 82, 83]	MIMO systems [84], dual-hop wireless networks [85], OFDM systems [86], CDMA systems [87], wireless sensor networks [77], industrial cyber-physical systems [88], Mobile Edge Computing(MEC) [89], etc.
	Instantaneous fingerprints	Channel State Information (CSI) [90, 91], Channel Impulse Response (CIR) [92, 93], and Channel Frequency Response (CFR)[94, 26]	

2.1.1. RF Fingerprints

We divide RF fingerprints into two sub-categories: transient fingerprints and steady-state fingerprints. The former sub-categories reflect the response of the transmitter elements when they are subjected to transient impulses such as startup and shutdown, and contain rich nonlinear and non-stationary characteristics. The latter one reflects the features extracted in the signal modulation phase. Transient fingerprints contain wavelet coefficient [49, 95], transient amplitude [51, 96, 52], and transient power spectral density (PSD) [52, 53], while steady-state fingerprints mainly contain I/Q imbalance [62, 64], CFO [65, 54, 66], clock skew [67, 68, 69], phase noise [70, 71], and imperfect

power amplifier [72, 73, 74]. The open-source datasets of RF fingerprints will be introduced in Section 5.1 in detail.

2.1.2. Channel Fingerprints

We divide channel fingerprints into two sub-categories: statistical fingerprints and instantaneous fingerprints. The former sub-categories indicate the statistical information of wireless links, while the latter one represents the fine-grained features of radio channels. Statistical fingerprints mainly contain RSS [75, 76, 77], Received Signal Strength Indication (RSSI) [78, 17], angle of arrival (AoA) [79, 80], and PSD [81, 82, 83]. Instantaneous fingerprints include CSI [90, 91], Channel Impulse Response (CIR) [92, 93], and Channel Frequency Response (CFR) [94, 26]. The open-source datasets of channel fingerprints will be introduced in Section 5.2 in detail.

2.2. Overview of the PLA for Multi-Device Identification

Most works related to PLA for multi-device identification adopt RF fingerprints as the identity signatures of transmitters. The RF fingerprint-based multi-device identification is also known as radio frequency fingerprinting (RFF) [30, 97] or specific emitter identification (SEI) [98, 31]. The object of multi-device identification is to recognize which transmitter in the fingerprint database matches the received signal in the authentication phase, and the identification process is as follows.

Step 1) Collect signals of devices;
Step 2) Pre-Process signals;
Step 3) Further process signals by expert feature transformation;
Step 4) Train the classifier for authentication;
Step 5) Identify unknown signals using the trained classifier.

The most widely used metric is the identification accuracy denoted by (1).

$$AucRate = \frac{1}{N} \sum_{n=1}^{N} \mathbb{I}(\boldsymbol{L}_n = \boldsymbol{Y}_n) \qquad (1)$$

where N denotes the number of fingerprints in the authentication phase. $\boldsymbol{L}_n$ and $\boldsymbol{Y}_n$ denote the real label and predicted label of the nth fingerprint, respectively. $\mathbb{I}(\cdot)$ denotes the indicator function, where if $\cdot$ is true, it takes 1; otherwise, it takes 0. $AucRate$ values range from 0 to 1. When all the fingerprint samples are identified correctly, $AucRate$ takes 1.

Here, we compare the traditional non-DL-based and DL-based multi-device identification schemes.

2.2.1. Traditional Non-DL-based Multi-Device Identification

"Step 2" includes two parts. The first part refers to pre-processing without prior information, such as normalization, interpolation, and Fast Fourier Transform (FFT), while the second part refers to preprocessing with prior information, such as time synchronization and phase offset compensation. Moreover, the expert feature transformation in "Step 3", such as STFT [99], wavelet transform [100], Wegener-Ville Distribution (WVD) [101], Choi-Williams Distribution (CWD) [101], High-order spectrum [102, 103, 104], Hilbert-Huang Transform (HHT) [105, 106, 107], also require prior information to manually set parameters.

2.2.2. DL-based Multi-Device Identification

The DL-based approaches are achieved through Deep Neural Networks (DNN), including FCNN [108], CNN [64, 29, 109, 110, 111, 112, 113], RNN [114, 115, 116, 117], Transformer [118, 119], data augmentation [44, 117, 118, 120, 121, 122, 123], CVNN [124, 125, 126, 127], Graph Neural Networks (GNN) [128], GAN [129, 108], and AE [130, 131, 132]. For instance, [108] proposes a FCNN-based framework in which biases and regularization techniques are employed to mitigate underfitting and overfitting. The Adam optimization algorithm is utilized for gradient descent to update the network parameters. [64] introduces a CNN classifier called ORACLE to analyze the differences between I/Q samples from a large pool of bit-similar devices. The ORACLE architecture consists of two convolutional layers and two fully-connected layers. Each complex I/Q sample, serving as the input to the ORACLE model, is represented as a 2-dimensional real value. [117] evaluates the performance of CNN (1D CNN and 2D CNN) and LSTM using various metrics: 'Per-slice Training' accuracy, 'Per-slice Testing' accuracy, 'Train-and-Test-Same-Day' accuracy, and 'Train-and-Test-Other-Day' accuracy. [118] proposes a transformer model for identifying LoRa devices using signals of variable lengths and introduce a multi-packet inference approach to significantly enhance accuracy in low SNR environments. Unlike adding Gaussian noise at the input layer, [120] proposes an LPNN approach to ensure the security of IIoT access. Given that latent layers exhibit stronger linear characteristics than input layers for CSI fingerprints, the proposed LPNN method offers better interpretability. [126] develops an efficient approach

17

using CVNN and network compression, named SlimCVNN, to achieve both high accuracy and low model complexity. [108] employs GANs for recognizing adversarial fingerprints and identifying wireless devices. Their generative module can produce fake fingerprints, while the discriminative module distinguishes real from fake ones. The CNN module enables the classification of legitimate devices. [132] proposes an AE-based architecture for intrusion detection and introduce the concept of a device authentication code. The reconstruction error serves as the device's authentication code, and the Kolmogorov-Smirnov test is used to determine the legitimacy of fingerprints.

For the DL-based schemes, "Step 2" only includes the above-mentioned first part, and "Step 3" is needless. In other words, the DL-based multi-device identification can directly use raw fingerprints to realize end-to-end identity authentication, overcoming the challenges in obtaining prior information and optimizing parameters manually.
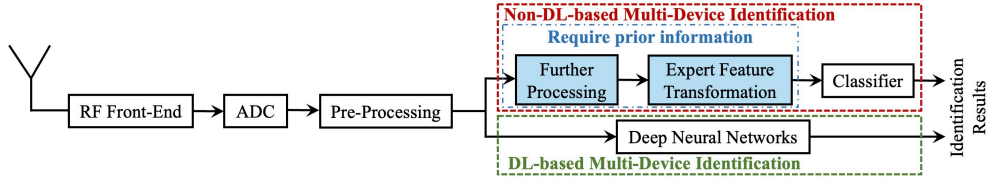

Figure 3: Illustration of the non-DL-based and DL-based multi-device identification methods.

We further provide Fig. 3 and Tab. 4 to illustrate the comparison of the traditional non-DL-based and DL-based multi-device identification schemes, which are beneficial for readers to understand more clearly. The DL-based methods will be introduced in Section 3 in detail.

Table 4: Comparison of the Non-DL-based and DL-based Multi-Device Identification Methods

Categories	Sub-Categories	Descriptions	Advantages and Disadvantage
Non-DL-based multi-device identification	Time-frequency transformation [99, 100, 101].	Describe the time variation law and frequency distribution of signals, including linear time-frequency transformation (STFT [99], Wavelet transform [100]) and quadratic time-frequency transformation (WVD [101], CWD [101]).	Require more prior information and expert feature transformation to manually set parameters, but have better interpretability.
	High-order spectrum [102, 103, 104].	Reserve unintentional modulation information and effectively suppress additive Gaussian noise, including bispectrum, integral poly-spectrum, and rectangular integral bispectrum.	
	Hilbert spectrum [105, 106, 107].	Show the law of time variation and frequency distribution of signals, and interpret the relationship between time and frequency of signals, mainly including HHT.	
DL-based multi-device identification	FCNN [108]	The FCNN models are fully connected. With the increase of dataset size, it is more and more difficult to obtain robust fingerprints.	Require no prior information, realize higher accuracy, and achieve end-to-end identification, but require more training datasets and have worse interpretability.
	CNN[29, 64],[109, 110, 111]	The CNN models exploit convolutional layers and pooling layers to extract features of fingerprints, including LeNet-like models [29, 64, 110], ResNet-like models [133], [134], AlexNet-like models [133, 135], VGG-like models[136], etc.	
	RNN[114, 115, 116]	The RNN models can mine time-related features,including Long Short-Term Memory (LSTM) models [114, 115] and the combinations of CNN and LSTM models [117], [121].	

Categories	Sub-Categories	Descriptions	Advantages and Disadvantages
	Data augmentation [44, 117, 118],[120, 121, 122, 123]	The data augmentation methods can address the problem of inconsistent probability distribution between training fingerprints and testing fingerprints, avoid over-fitting issues, and improve the generalization of models, including adding Gaussian noise [117, 118], [120] and generating new samples [44, 117],[121, 122, 130].	
	CVNN[124, 125, 126, 127].	The CVNN models can directly process complex baseband signals and are composed of complex-valued convolution layers, complex-valued fully-connected layers, complex-valued batch normalization, and complex-valued activation functions.	
	GAN [108, 129].	The GAN models can realize the classification of multiple trusted transmitters and the identification of rogue devices through generators and discriminators.	
	AE[130, 131, 132]	The AE models can achieve feature extraction and dimension reduction through encoders and decoders.	

2.3. Overview of the PLA for Attack Detection

Among the works related to PLA for attack detection, some only use RF fingerprints as identity signatures of legitimate devices, some only use channel fingerprints to construct the hypothesis testing, and the rest utilize the combination of channel fingerprints and RF fingerprints to obtain more robust detection performance. Considering that Xie et al. [40] have provided a comprehensive survey of different types of fingerprints for attack detection, we focus on enabling ML methods. Hence, we summarize the works on attack detection from the perspective of ML techniques. The goal of attack detection at the legitimate receiver (Bob) is to identify whether the received signal is legal (from Alice) or not (from Eve), and the detection can be realized using

the following hypothesis testing in (2).

$$\begin{cases} \mathcal{H}_0 \colon H_{diff} = diff\big(H_t - H_{ref}\big) < \theta \\ \mathcal{H}_1 \colon H_{diff} = diff\big(H_t - H_{ref}\big) \geq \theta \end{cases} \quad (2)$$

where $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively indicate the signal corresponding to the unknown fingerprint H_t comes from Alice and Eve. H_{ref} represents the reference fingerprint, $diff(H_t - H_{ref})$ is the difference between H_t and H_ref, and θ represents the threshold for comparison. θ is a critical optimization parameter. If the value of θ is too small, the authentication system will become overly sensitive, leading to the misidentification of some legitimate signals as illegal. On the other hand, if the value of θ is too large, the system will react too loosely, resulting in the misclassification of some illegal signals as legitimate.

The common metric for evaluating the detection performance includes false alarm rate P_{fa} and miss detection rate P_{md}, which can be represented as (3) and (4), respectively.

$$P_{fa} = P\{\hat{y} = 0|y = 1\} \quad (3)$$

$$P_{md} = P\{\hat{y} = 1|y = 0\} \quad (4)$$

where $\hat{y}$ is the predicted identity, and y is the real identity. P_{fa} denotes the probability of legal fingerprints being falsely alarmed as the spoofing attack, and P_{md} represents the probability of spoofing signals being missed detection. Therefore, θ in (2) are optimized according to the trade off between P_{fa} and P_{md}.
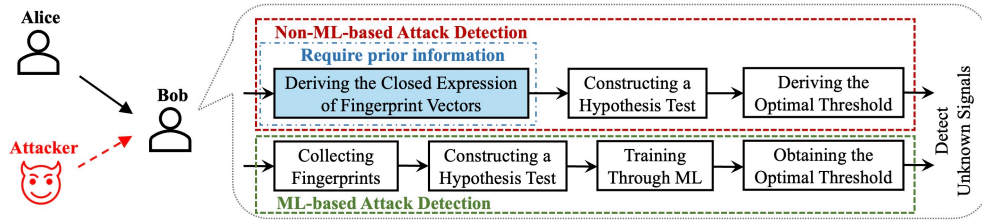

Figure 4: Illustration of the non-ML-based and ML-based attack detection methods.

Here, we compare the traditional non-ML-based and ML-based attack detection schemes. We further provide Fig. 4 and Tab. 5 to illustrate the comparison of the traditional non-ML-based and ML-based attack detection schemes more clearly.

Table 5: Comparison of the Non-ML-based and ML-based Attack Detection Methods

Categories	Sub-Categories		Descriptions	Advantages and Disadvantages
Non-ML-based attack detection	Fingerprint matching[75, 76],[55]		Defend against both the impersonation attack and Sybil attack by matching the estimated fingerprints with the legitimate one.	Better interpretability, but require prior information of transmitters and channels and the determined threshold is unable to adapt to the dynamic channel environment.
	Fingerprint ratio[78]		Using RSSI values directly for Sybi attack detection is unfeasible, and a promising method is to use the RSS ratio.	
	Fingerprint similarity [137, 138]		Fingerprint similarity can be calculated based on the correlation between the fingerprints of different transmitters.	
	Residual algorithm [139]		The RSS residual measured by the Euclidean distance can be used to recognize threats from a malicious user.	
	Two-dimensional quantization algorithm [140, 141]		The CIR fingerprints can be quantized in two dimensions for more reliable spoofing detection.	
	GLRT[142]		GLRT is optimal for frequency-selective Rayleigh channels but computationally cumbersome.	
	CLRT[72]		CLRT can be used to address the detection issue resulted from GLRT.	
	LLRT[140]		LLRT is developed based on the fingerprints estimated by the two-dimensional quantization algorithm.	
ML-based attack detection	SL	Logistic regression [143]	Logistic regression is a linear regression analysis model.	
		LDA[144]	LDA is a linear learning method for detecting multi-attackers.	

Categories		Sub-Categories	Descriptions	Advantages and Disadvantages
		DT[145, 88]	DT is a tree structure based on conditional probability and can intuitively show the detection results.	Better attack detection performance without manually determining the threshold, but has worse interpretability.
		KNN[146]	In KNN-based schemes, each fingerprint can be represented by its closest neighboring fingerprints.	
		SVM[147, 148].	SVM can obtain detection results by maximum-margin hyperplane and use kernel methods to realize nonlinear classification.	
		Ensemble learning [88, 149]	Ensemble learning can construct multi-classifiers and combine them to realize more robust attack detection performance.	
		ELM[150]	ELM is a kind of feedforward neuron network structure without updating weights and can realize better generalization in detection than SVM.	
		FL[151]	FL is a distributed ML technique and can realize collaborative authentication without exchanging their estimated fingerprints.	
		DL[152, 153]	DL can mine the depth characteristics of fingerprints.	
	UL	Clustering [20]	Clustering can divide the fingerprints into several disjoint clusters to achieve attack detection.	
		OCC-SVM[148]	OCC-SVM can leverage kernel functions to map the original feature space of fingerprints to a higher dimensional space, so as to find an effective boundary to separate malicious fingerprints.	

Categories	Sub-Categories		Descriptions	Advantages and Disadvantages
		Manifold learning [154]	Manifold learning can recover the low-dimensional manifold structure from the high-dimensional fingerprints and find the corresponding embedded mapping to realize detection.	
		GMM[155]	GMM models the fingerprints as Gaussian distributions.	
		GP[156]	GP mainly includes GP Regression (GPR) and GP Classification (GPC).	
		AE[157]	AE can realize dimension reduction and further identify the latent vectors.	
	RL	Non-DL-aided RL[158, 27]	RL can use dynamic game without knowing the system parameters to obtain the optimal threshold.	
		DRL[159, 160]	DRL can combine the perception ability of DL with the decision-making ability of RL to find better authentication modes and parameters.	

2.3.1. Traditional Non-ML-based Attack Detection

The non-ML-based attack detection uses the prior information of transmitters and channels to derive the probability distribution of fingerprints, then constructs hypothesis testing statistics, and finds the optimal threshold. The common methods include fingerprint matching [75, 76, 55], fingerprint ratio [78], fingerprint similarity [137, 138], residual algorithm [139], two-dimensional quantization algorithm [140, 141], generalized likelihood ratio test (GLRT) [142], classical likelihood ratio test (CLRT) [72], and logarithmic likelihood ratio test (LLRT) [140].

2.3.2. ML-based Attack Detection

The ML-based attack detection exploits intelligent ML algorithms to automatically obtain the threshold without manual operations. Some schemes even achieve threshold-free authentication [88]. We classify the ML tech-

niques into three sub-categories: Supervised Learning (SL), Unsupervised Learning (UL), and Reinforcement Learning (RL).

The SL algorithms can be classified into logistic regression [143], Linear Discriminant Analysis (LDA) [144], Decision Tree (DT) [145, 88], K-Nearest Neighbor (KNN) [146], Support Vector Machine (SVM) [147], ensemble learning [149, 88, 161], extreme learning machine (ELM) [150], Federated Learning (FL) [151], and DL [152, 153]. For instance, [143] proposes a multi-landmark-based authentication scheme in which each landmark, equipped with multiple antennas, collects distributed Received Signal Strength Indications (RSSIs) to derive more distinctive characteristics. They utilize the Frank-Wolfe algorithm, grounded in logistic regression, to tackle the convex optimization problem associated with maximum likelihood-based coefficient estimation for the regression. [145] presents three ML-based PLA schemes, namely DT, SVM, and KNN. Simulations conducted on OFDM systems reveal that all ML-based approaches achieve greater detection accuracy compared to statistical-based methods. [149] proposes an ensemble learning-based PLA approach tailored for edge computing environments. [151] develops a horizontal FL-based collaborative PLA scheme designed to alleviate the computational burden on IoT devices with limited processing and storage capabilities. The proposed distributed identification architecture assigns classification tasks to trustworthy collaborators, ultimately aggregating local parameters at a central device. [153] integrates TL with TP-Net to achieve lightweight and online identification.

The UL algorithms can be classified into clustering [20, 162], one class classification-SVM (OCC-SVM) [148], manifold learning [154], Gaussian Mixture Models (GMM) [155], Gaussian process (GP) [156], and AE [157]. For instance, [20] investigates the relationship between multi-fingerprints and propose an unsupervised PLA scheme based on a non-parametric clustering algorithm. [148] introduces an adaptive lightweight PLA approach that leverages antenna diversity techniques to enhance recognizable fingerprints. [154] applies manifold learning to tackle this issue by constructing a Markov chain of fingerprints in the time domain and evaluating the state transition probabilities of UAVs. [155] employs GMM to formulate the probabilistic model of transmitter radio channels, enabling online learning and parameter updates. [156] presents a PLA scheme based on Gaussian process channel prediction for IoT devices. Historical CSI fingerprints and the geographical data of devices are utilized to create a mapping that predicts the next legal CSI fingerprint for identification. [157] proposes a PLA scheme based on

25

a hierarchical variational autoencoder to defend against spoofing attacks in IIoT, without requiring training fingerprints from attackers. The constructed loss function includes both an approximation and an exact calculation.

The RL algorithms can be classified into non-DL-aided RL [158] and Deep RL (DRL) [159, 160]. For instance, [158] investigates a PLA scheme under the threat of intelligent spoofing attacks. The optimal transmit power allocation is derived to identify the optimal intelligent attack strategy for legitimate devices. [160] examines three scenarios in static channels: multiplayer games, zero-sum games with collisions, and zero-sum games without collisions. The closed-form expressions for Nash equilibrium are derived.

3. DL-based PLA for Multi-Device Identification

In this section, we introduce the DL-based methods for multi-device identification. We divide the DL techniques into several sub-categories and compare them in detail. The organization of this section is illustrated in Fig. 5.
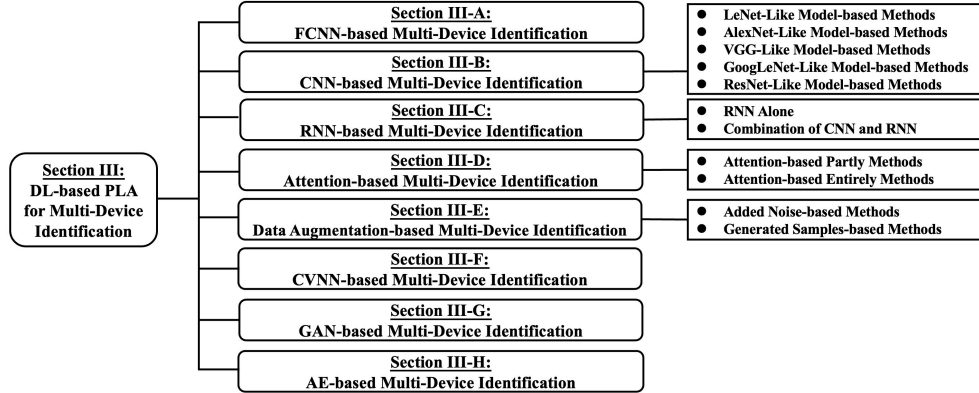

Figure 5: Organization of Section III.

3.1. FCNN-based Multi-Device Identification

DL is a kind of ML techniques and is usually realized through neural networks, which are composed of one input layer, multiple hidden layers (also called latent layers), and one output layer. As illustrated in Fig. 6, the FCNNs are directed layered neural networks without internal feedback connections. The latent layer $\boldsymbol{X}^{[i]}$ can be represented as

$$\boldsymbol{X}^{[i]} = \sigma(\boldsymbol{W}^{[i]}\boldsymbol{X}^{[i-1]} + \boldsymbol{\xi}^{[i]}) \tag{5}$$

26

where $\boldsymbol{W}^{[i]}$ and $\boldsymbol{\xi}^{[i]}$ respectively denote the weight matrix and bias matrix between the $(i-1)$th layer and the ith layer. $\sigma(\cdot)$ represents the activation function, including ReLU function, Tanh function, and Sigmoid function. In neural network, the activation function plays a crucial role. Its primary function is to introduce nonlinear characteristics, enabling neural networks to learn and simulate complex patterns. In a word, the activation function determines whether a neuron should be activated for a given input, thereby deciding what output should be produced.

- *Identification of USRP devices:* Roy et al. [108] design an FCNN-based scheme, where biases and regularization methods are utilized to avoid under-fitting and over-fitting issues. The Adam optimization algorithm is used to realize gradient descent and update network parameters. Roy et al. [108] further set up the laboratory testbed composed of several universal software radio peripheral (USRP) equipment and one RTL-Software Defined Radio (SDR) receiver to verify its effectiveness. The results reveal that the suggested FCNN-based scheme can identify 4 devices and 8 devices with the accuracy of 97.21% and 96.6%, respectively.

- *Identification of ZigBee Devices:* Jafari et al. [114] collect the I/Q fingerprints from 6 ZigBee devices (MICAz) and compare the authentication performance versus different slide window sizes and different learning rates.

Lesson 1. *Although the FCNN-based schemes can obtain higher identification accuracy compared with the non-DL-based schemes, it is challenging for the fully-connected structure to extract the spatial information of fingerprints. Hence, the robustness needs to be enhanced, especially for large-scale fingerprint datasets [163].*

3.2. CNN-based Multi-Device Identification

To extract the spatial information of fingerprints, more and more researchers have resorted to CNNs. As illustrated in Fig. 6, the latent layers in CNNs are usually composed of convolutional layers, pooling layers, and fully-connected layers. The output of the convolutional layer can be denoted as

$$\boldsymbol{X}^{[i]} = \sigma(\boldsymbol{W}^{[i]} \otimes \boldsymbol{X}^{[i-1]} + \boldsymbol{\xi}^{[i]}) \tag{6}$$
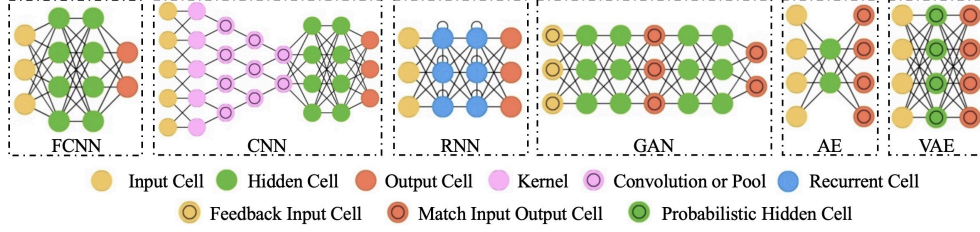
Figure 6: Illustration of typical DL techniques, including FCNN, CNN, RNN, GAN, AE, and VAE.

where $\boldsymbol{W}^{[i]}$ and $\boldsymbol{\xi}^{[i]}$ denote the convolution kernel and bias matrix between the $(i-1)$th layer and the ith layer, respectively. $\otimes$ is the convolution operation. The convolution operation defines a set of filters (also known as convolution kernels or feature detectors) that slide over the input image to extract specific local features such as edges, corners, and textures. By employing filters of varying sizes and shapes, CNNs can capture multi-scale and multi-level features. These extracted features are then combined and abstracted in subsequent layers of the network, resulting in a higher-level feature representation that is essential for complex image understanding tasks. The polling layer can compress data and reduce the number of parameters through parameter sharing. CNNs can realize the classification of pictures and are common in computer vision field. To obtain higher identification accuracy, fingerprints can be pre-processed as pictures to reserve spatial information, such as the input and output multi-antenna features of CSI fingerprints in MIMO systems and the in-phase components I and quadrature components Q of I/Q fingerprints. Here, we divide CNNs into five sub-categories as follows.

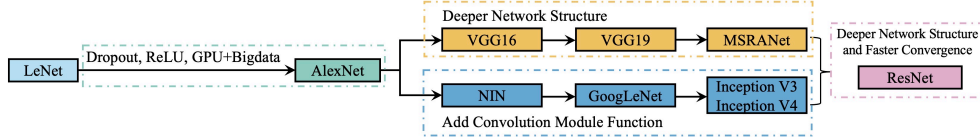### 3.2.1. LeNet-Like Model-based Methods

Figure 7: Illustration of the evolutions of CNN models.

As illustrated in Fig. 7, LeNet is one of the earliest CNNs and the origin of a large number of neural network architectures. LeNet is a lightweight CNN model and has been widely studied for PLA.

28

- *Radio Modulation Recognition:* Shea et al. [110] first use the LeNet model to recognize radio modulation by raw I/Q fingerprints without expert transformation. The modulations for recognition include 8 digital modulations (BPSK, QPSK, 8PSK, 16QAM, 64QAM, BFSK, CPFSK, and PAM4) and 3 analog modulations (WB-FM, AM-SSB, and AM-DSB). The simulation results demonstrate that the CNN-based approach is feasible, especially at low SNR environments.

- *Identification of Large-Scale Devices:* Sankhe et al. [64] describe a CNN classifier named ORACLE to study the difference between I/Q samples of a large pool of bit-similar devices. The ORACLE architecture is consisted of 2 convolution layers and 2 fully-connected layers. Each complex I/Q sample, the input of the ORACLE model, is denoted as a 2-dimensional real value. Sankhe et al. [64] utilize the 16-node USRP X310 SDR testbed to generate I/Q fingerprints and use 140 COTS WiFi devices to obtain external datasets. The authentication results reveal that ORACLE can realize $\geq 99\%$ identification accuracy on static radio environments.

- *Identification of Mobile Phones:* Aneja et al. [109] set up the experiment system with iPhone 7 Plus and iPad 4 and use inter arrival time of the identifying signatures. The results indicate that the CNN classifier can realize 86.7% accuracy.

- *Performance versus Different Window Sizes:* Jafari et al. [114] test the authentication performance of the CNN model on ZigBee devices. The results reveal that the simulation experiments verify that the CNN model can realize the accuracy of 94.7%, 94.2%, and 94% with the window size of 32, 64, and 128, respectively.

- *CNNs Combined with Clustering:* Wong et al. [164] investigate the CNN model as the characteristic extractor, paired with density-based spatial clustering of applications with noise [165] clustering algorithm. The introduction of the clustering algorithm is beneficial for the visualization of fingerprints and better understanding of the further authentication process. The simulation results indicate that when there are 25 transmitters, the proposed model can achieve 78.7% and 80.4% accuracy with 0.25 MHz and 1.67 MHz bandwidth, respectively.

- *Performance versus Different SNRs:* Merchant et al. [166] verify the performance of the CNN architecture on a set of IEEE 802.15.4 devices. The fingerprints are collected from 7 DigiXBP24CZ7SITB003 ZigBee Pro devices with the 204 GHz band, and the CNN technique is demonstrated via two experiments: a noisy channel and a lab environment with simulated additive white Gaussian noises. The results show that when SNR is 10 dB and 40 dB, the accuracy can reach 73.73% and 91.38%, respectively.

- *Lightweight Realization:* Qi et al. [167] focus on intercepting and representing signals to address concerns of complexity and efficiency. A comprehensive complexity analysis of PLA models is conducted, including parameters, floating-point operations, and memory usage.

3.2.2. AlexNet-Like Model-based Methods

As illustrated in Fig. 7, compared with LeNet, AlexNet exploits ReLU function as the activation function to obtain better performance in deep network architectures and use Dropout to address the over-fitting issue. In addition, AlexNet can leverage GPU to realize more powerful computational ability. For these reasons, AlexNet-enabled PLA schemes are more efficient.

- *Performance under Noisy Multipath Environments:* Riyaz et al. [29] propose a CNN-based identification architecture that is motivated in part by AlexNet. Riyaz et al. [29] further used 720,000 fingerprints, 80,000 fingerprints, and 200,000 fingerprints for training, validation, and testing, respectively. The simulation results reveal that the CNN model can achieve 98% identification accuracy for 5 devices on the noisy multipath wireless channels.

- *Performance on ADS-B Datasets:* Shawabka et al. [133] collect I/Q datasets with 7 TB from 20 transmitters with WiFi and automatic-dependent surveillance-broadcast (ADS-B) transmissions and discuss the impact of wireless channels on the identification accuracy. The results indicate that balancing I/Q samples can significantly enhance the identification accuracy when there are a large number of transmitters.

- *Key-Aided Identification:* Sankhe et al. [135] provide a CNN architecture with 8 convolution layers and 2 fully-connected layers for large-scale fingerprint datasets. Sankhe et al. [135] further present a scalable

identification approach named impairment hopping spread spectrum, which can generate random binary sequence keys to defend against spoofing attacks.

- *Study on Interpretability:* Liu et al. [168] pay attention to enabling DL techniques to be practically dependable in device identification and propose to employ the zero-bias layer in the CNN model to realize interpretable and dependable identification. The simulations on real-world ADS-B transmitters demonstrate its effectiveness.

- *CNNs Combined with Metric Learning:* To achieve lightweight identification without relying on a large number of samples, Gaskin et al. [169] present Tweak technique that can create a portable model to identify LoRa devices. The proposed Tweak method leverages metric learning to effectively process the fingerprints from non-original training domains.

- *Impact of Receivers on Performance:* Shen et al. [170] study the impact of receivers on identification performance and propose an adversarial training approach. They further provide two training strategies, including homogeneous and heterogeneous training. The simulation results verify that it can obtain over 75% accuracy for 20 SDRs.

- *CNNs Combined with Ensemble Learning:* Huang et al. [171] combine CNN models and ensemble learning to propose two identification architectures, including the improved CNN by Bagging and the improved CNN by Boosting. The simulations verify that the proposed method can achieve the accuracy of 89.75% in the 10 dB noise scenarios.

- *Channel Robust Identification:* Xing et al. [172] propose a channel robust identification approach named the difference of the logarithm of the spectrum. The proposed method is independent on a single fingerprint data and does not require additional manipulation of the transmitters. The simulations in the IEEE 802.11 OFDM system show that the proposed scheme can reach the accuracy of 99.02% and 97.05% in the single- and cross- environment evaluations, respectively.

3.2.3. VGG-Like Model-based Methods

As illustrated in Fig. 7, compared with AlexNet, VGG has a deeper network structure. The convolution operations are achieved through multiple

31

stacked convolution kernels with a small size, which indicates that it requires fewer parameters and has better feature extraction ability. Hence, VGG-based PLA methods are more suitable for lightweight deployment.

- *Study on In-Band and Out-of-Band Spectrum Emissions:* Elmaghbub et al. [136] consider both the in-band and out-of-band spectrum emissions to extract the fingerprints, which can provide discriminate identifying signatures even when the distortion of hardware of different devices is significantly reduced. The experiments show that the accuracy for 5 devices can reach 96.2% whereas that of the in-band-based method is 48.6%.

- *Verification of VGG-16:* Zong et al. [173] propose an authentication architecture based on VGG-16 and use the fingerprints of 5 transmitters with SNR of 20 dB to verify its effectiveness.

- *CNNs Combined with TL* Chen et al. [174] develop a CNN architecture named TP-Net to realize effective decision-making process at the edge devices. The simulations on Rayleigh models demonstrate its superiority in accuracy than CNN-2, GC-Net, and VGG-7. Chen et al. [153] further combine TL and TP-Net to realize lightweight and online identification for 40 devices.

3.2.4. GoogLeNet-Like Model-based Methods

In GoogLeNet, the basic convolution block is called inception block, whose core concept is to use the combination of different sizes of convolution kernels to fuse various information of different scales. Such design can deepen the network without increasing the number of parameters.

- *Comparison with AlexNet:* Zha et al. [175] verify the accuracy performance of AlexNet and GoogLeNet on 1090MHz baseband signals collected from 5 aircraft. The results under different SNRs demonstrate the effectiveness of the contour stellar images.

- *Identification under FHSS Networks:* Kang et al. [176] propose the RFEI algorithm based on Inception-A for FHSS networks. The results show that the proposed approach can realize classification accuracy of 97.0% for 7 unseen real FHSS transmitters.

- *Comparison with CNN-3, VGG-16, and ResNet-50:* Mcmillen et al. [177] propose an RF fingerprint system named PUWS based on chaotic antenna arrays. A basic Convolutional Neural Network (CNN) with two convolutional layers, each containing 64 neurons, followed by a single dense layer, is employed as the baseline for performance comparison among the models discussed. These models include VGG-16, a 16-layer neural network; ResNet-50, which features 50 layers and introduces residual connections between layers; Inceptionv3, a deep CNN that utilizes a 'network-in-network' strategy to learn features more profoundly; and Xception, an Inception-based model that enhances accuracy through the use of residual connections and separable convolutional layers. Initially designed for image classification with typical inputs of size $224 \times 224 \times 3$, these models required adjustments to their top layers to handle received I/Q samples of size $1000 \times 8 \times 1$, where the 8 columns represent I and Q signal samples from 4 antenna elements. In comparison to CNN-3 (with an accuracy of 93.3%), VGG-16 (93.5%), and ResNet-50 (99.2%), the proposed Inception and Xception models achieve an accuracy of 99.9% for 300 devices.

- *Verification of MSCNN:* Based on the convolution layers of multiple branches with different convolution kernel sizes, Zhang et al. [178] develop an MSCNN to enhance the identification performance. The proposed MSCNN model can exploit the inherent features in multiple receptive fields. The simulations under perfect environments verify that the proposed MSCNN method can enhance the absolute accuracy and relative accuracy by 15% and 22%, respectively.

3.2.5. ResNet-Like Model-based Methods

Through residual learning, ResNet can address the gradient explosion/ disappearance issues caused by the deep structure. ResNet is suitable for the feature extraction of large-scale datasets and can obtain more robust identification models.

- *Identification of Satellite Transmitters:* Oligeri et al. [15] introduce PAST-AI to realize the PLA of satellite transmitters via DL techniques. They provide two device identification scenarios: intra-constellation satellite identification and satellite identification in the wild, and further compare the accuracy and training overhead of ResNet-18 and baseline models.

33

- *Scalability Analysis for Large-Scale Devices:* Jian et al. [34] analyze the scalability issue on identifying very large device populations, including 10,000 devices, and further present comprehensive performance comparison of different CNN models, channel environments, SNR, number of devices, and dataset size.

- *Identification without Retraining:* Gritsenko et al. [179] develop an approach to identify new devices without retraining a classifier, and provide comprehensive analysis of the designed architecture from the perspective of model parameters and I/Q datasets. Gritsenko et al. [179] test the technique on 6 real-world datasets with different sizes and transmission protocols. The proposed approach can detect unseen devices with the accuracy of 76%, while reducing the identification accuracy of 500 previously seen devices by no more than 10%.

- *Identification of Mobile Phones:* Zhang et al. [180] propose a ResNet-based approach named RFFResNet to authenticate real mobile phones, and provide the influence of channel environments, noises, training dataset scale, and model parameters. The performance of RFFResNet is tested on the LTE simulation datasets with 220 GB and real mobile phone's datasets with 25 GB. The results verify that RFFResNet can realize 95%-99% accuracy, which is higher than that of ResNet18-1D, ResNet34-1D, and VGG16-1D.

- *Identification under Low SNR Environments:* Tang et al. [181] design a DRSN to identify devices in low SNR environments. The soft threshold is utilized to preserve more useful characteristics, and the identity shortcut is employed to improve the training speed. The simulations verify the superiority of the proposed DRSN architecture in accuracy than FCNN [114], CNN 1D [166], CNN 2D [182], and ResNet [183].

- *CNNs Combined with Structured Pruning:* To enhance the identify accuracy, Jian et al. [184] propose the ResNet50-1D architecture, containing 49 convolutional layers and one fully-connected layer. They utilize structured pruning [185] to generate the compressed versions efficiently and use an ADMM approach to prune the model [186]. Numerous experiments on multi-edge-devices verify the high-efficiency of the proposed method.

Here, we summarize the contributions of all CNN-based multi-device identification schemes in Tab. 6.

Table 6: CNN-Based Multi-Device Identification Schemes

CNN	Ref.	Year	Major Contribution
LeNet-Like Models	[64]	2019	Propose ORACLE, a LeNet-based classifier, to realize the identification for a large pool of bit-similar devices.
	[109]	2019	Used IAT as identifying signatures and verify the performance of the CNN classifier for iPhone 7 Plus and iPad4.
	[110]	2016	First utilize LeNet to recognize radio modulation by raw I/Q fingerprints without expert transformation.
	[114]	2019	Test the identification performance of CNNs for ZigBee devices versus different window sizes.
	[164]	2019	Combine CNNs and spatial clustering algorithm to realize the visualization of fingerprints.
	[166]	2018	Verify the performance of CNNs for a set of IEEE 802.15.1 devices in noisy channels and a lab environment, respectively.
	[167]	2019	Analyze the complexity of PLA models, including parameters, floating-point operations, and memory usage.
AlexNet-Like Models	[29]	2018	Provide an AlexNet-based classification architecture and verify the performance using 1,000,000 fingerprints.
	[133]	2020	Collect I/Q datasets with 7 TB from 20 transmitters with WiFi and ADS-B transmissions and discuss the impact of channels on accuracy.
	[135]	2020	Present a CNN architecture for large-scale fingerprint datasets and further present a scalable method for attack detection.
	[168]	2021	Employ the zero-bias layer in CNNs to achieve interpretable and dependable identification.
	[169]	2022	Leverage metric learning and CNNs to effectively process the fingerprints from non-original training domains.

CNN	Ref.	Year	Major Contribution
	[170]	2022	Study the impact of receivers on performance and propose an adversarial training method, including homogeneous and heterogeneous training.
	[171]	2022	Combine CNNs and ensemble learning to propose two methods, including the improved CNNs by Bagging and Boosting, respectively.
	[172]	2022	Show a channel robust identification approach, which is independent on a single fingerprint data and does not require additional manipulation of transmitters.
VGG-Like Models	[136]	2020	Consider both the in-band and out-of-band spectrum emissions and provide a method that can provide discriminate identify signatures even when the distortion of hardware of different devices is significantly reduced.
	[173]	2020	Develop an architecture based on VGG-16 and confirm its performance on 5 transmitters with SNR of 20 dB.
	[153]	2022	Propose TP-Net based on CNNs to realize effective decision-making process at the edge devices, and
	[174]	2020	further combine TL and TP-Net to realize lightweight and online identification for 40 devices.
GoogLeNet-Like Models	[175]	2020	Compare the performance of AlexNet and GoogLeNet on 1090 MHz baseband signals collected from 5 aircraft.
	[176]	2021	Introduce the RFEI method based on Inception-A for FHSS networks and verify the performance on 7 FHSS transmitters.
	[177]	2023	Present an authentication framework based on CAAS and compare the performance of CNN-3, VGG-16, ResNet-50, Inception, and Xception.
	[178]	2022	Develop a multi-scale-CNN architecture to exploit the inherent features in multiple receptive fields and enhance accuracy.
	[15]	2023	Propose PAST-AE to achieve the PLA of satellite transmitters under two typical scenarios: intra-constellation satellite identification and satellite identification in the wild.

ResNet-Like
Models

CNN	Ref.	Year	Major Contribution
	[34]	2020	Analyze the scalability issue of applying identification methods to very large device populations, and further present comprehensive performance comparison of different CNN models, channel environments, number of devices and dataset size.
	[179]	2019	Present a method without retraining classifiers, and provide comprehensive analysis from the perspective of model parameters and I/Q datasets.
	[180]	2021	Propose RFFResNet to identify real mobile phones, and compare their performance with RstNet18-1D, ResNet34-1D, and VGG16-1D.
	[181]	2021	Design DRSN to identify devices in low SNR environments, and compare its performance with FCNN, CNN 1D, CNN 2D, and ResNet.
	[184]	2022	Propose ResNet50-1D architecture that utilizes structured pruning to generate the compressed versions efficiently and uses ADMM trick to prune models.

Lesson 2. *CNNs are the most widely used models to extract the spatial information of RF fingerprints and channel fingerprints, especially I/Q fingerprints and CSI fingerprints, respectively. The real part and imaginary part of complex signals correspond to different channels of CNNs. Hence, fingerprints are pre-processed as pictures to further extract the frequency domain information. For the LeNet-like and AlexNet-like models, the combinations with clustering algorithms [164], metric learning [169], and ensemble learning [171] as well as the performance for mobile phones [109], noisy multipath environments [29], WiFi scenarios [133], ADS-B scenarios [133], and Zig-Bee devices [114] have been studied. However, due to the limited network architecture, it is challenging for them to identify large-scale devices. For the VGG-like models, the network structure is deeper, and TL is combined to realize lightweight and online identification for 40 devices [153]. For the GoogLeNet-like models, the introduction of the inception block can deepen the network without increasing the number of parameters. Such design enables the identification to extend to large-scale scenarios with 300 devices [177]. For the ResNet-like models, residual learning involved is suitable for the feature extraction of large-scale datasets, such as the very large device populations*

including 10,000 devices [34] and the LTE simulation datasets with 220 GB [179].

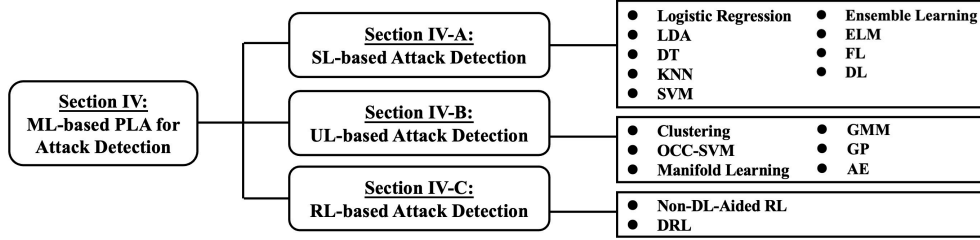## 3.3. RNN-based Multi-Device Identification

Figure 8: Organization of Section IV.

As illustrated in Fig. 8, RNN can extract the time series characteristics of fingerprints through recursion operations. Typical RNN models include Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU).

3.3.1. RNN Alone

- *Comparison between FCNN, CNN, and RNN:* Jafari et al. [114] compare the identification performance between FCNN, CNN, and RNN. The simulations on I/Q samples collected from ZigBee devices over several SNR levels show the inferiority of RNN.

- *Performance under Low SNR Environments:* Wu et al. [115] propose a LSTM-based approach to capture the long-term and short-term characteristics of I/Q fingerprints. The experimental studies under low SNR environments (-12 dB) demonstrate its effectiveness.

- *Novel Metrics:* Shawabka et al. [117] assess the performance of CNN (1D CNN and 2D CNN) and LSTM utilizing the following metrics: "Per-slice Training" accuracy, "Per-slice Testing" accuracy, "Train-and-Test-Same-Day" accuracy, and "Train-and-Test-Other-Day" accuracy. Massive experiments verify the superiority of CNN than RNN in identification performance.

3.3.2. Combination of CNN and RNN

Considering that the combination of CNN and RNN can extract the spatial and temporal characteristics of fingerprints, researchers have conducted a series of studies.

38

- *Identification of Large-Scale WiFi Devices:* Soltani et al. [44] provide the RFF-ConvRNN model, consisting of the convolution module, RNN module, and fully-connected module for extracting spatial properties, extracting time-dependent features, and classification, respectively. The simulations on 50 WiFi devices indicate that when data augmentation is not used, the proposed RFF-ConvRNN model can obtain better identification performance than baseline models.

- *Performance under Low SNR Environments:* Liu et al. [121] suggest the DBi-LSTM and the one-dimensional residual convolutional network with dilated convolution and squeeze-and-excitation block to against the interference of unreliable fingerprints. The combination of DBi-LSTM and CoBONet can exploit the fine-grained attributes of signals and directly extract the temporal characteristics from baseband I/Q fingerprints. The simulations on the open-source datasets [64] collected from 16 USRP devices show that the proposed architecture can obtain high accuracy even in low SNR environments.

- *Comparison with LSTM and GRU:* Roy et al. [187] combine LSTM and CNN to exploit the temporal and spatial properties of I/Q fingerprints. The I/Q samples are generated from 8 different USRP B210s under an indoor environment with the SNR of 30 dB. The simulation results show that the proposed ConvLSTM can realize the accuracy of 97.2%, while LSTM and GRU can reach the accuracy of 92% and 95.3%, respectively.

Lesson 3. *Due to the insufficient extraction of spatial information, the utilization of RNNs alone can not obtain higher identification performance than CNNs. One feasible approach is to combine CNNs and RNNs to extract both temporal and spatial properties. Such design has been verified in large-scale WiFi scenarios [44] and low SNR environments [121].*

3.4. Attention-based Multi-Device Identification

The Attention mechanism refers to selectively paying attention to a part of all information while ignoring other visible information. The Attention mechanism can help efficiently extract useful features.

3.4.1. Attention-based Partly Methods
- *Attention to Frequency Domain:* Considering that the ability of feature extraction in time domain is limited, Peng et al. [188] propose a

squeeze-and-excitation neural network (SeNet) approach in frequency domain. The suggested architecture can realize channel attention mechanism using the squeeze-and-excitation module so that the useful characteristics of fingerprints are emphasized and the useless information is weakened. The simulations on 20 WiFi devices verify that the proposed SeNet can obtain better identification performance and stronger robustness than baseline models even in low SNR environments.

- *CNNs Combined with Attention:* To leverage rough priori information to improve authentication performance, Weng et al. [189] pay attention to message structure and provide the MSCAN. The proposed model can separate the portions with different pulse waveform distributions and achieve spatial attention mechanism for low-dimensional fingerprints. Such design is beneficial to the exploration of internal correlation and more efficient feature fusion. The simulation results on fingerprints collected from real-world ADS-B transmissions show that the suggested MSACN can reach the accuracy of 98.20% for 44 transmitters.

- *Comparison with AlexNet, VGG, and AttMsCN:* Zhang et al. [190] propose a data-and-knowledge dual-driven architecture, including the multi-scale module, attention module, and classifier. The proposed model can exploit more useful semantic information from protocol knowledge and explore higher-level characteristics using the attention mechanism. The simulations on 5 WiFi devices show that the accuracy of the proposed model is 55%, 44%, and 35% higher than VGG, CNN [29], and AttMsCN with the SNR of -10 dB.

3.4.2. Attention-based Entirely Methods (Transformer)
- *Performance under Low SNR Environments:* Shen et al. [118] propose a transformer model to identify LoRa devices with the signals of variable lengths and propose a multi-packet inference approach to greatly enhance the accuracy performance in low SNR environments. The simulations on 10 LoRa devices show that the proposed method can improve the identification accuracy from 60% to 90% with the SNR of 10 dB.

- *Identification of Unknown Devices:* To handle devices that appear outside the closed set, Xu et al. [119] provide a novel identification approach combining an enhanced Transformer and a modified ICS al-

gorithm. The proposed architecture can recognize unseen classes of devices while maintaining good identification performance of known devices. The simulations on 30 distinct devices show that the proposed model is superior in identification accuracy and robustness than baseline models, including Hybrid OvA [191], Modified ICS [192], MLOSR [193], and CROSR [194].

Lesson 4. *The Attention mechanism is usually combined with CNNs to emphasize the useful characteristics of fingerprints and weaken the useless information. In addition, some researchers study the identification methods based on Attention mechanism entirely, that is, Transformer. Transformer uses encoders and decoders to extract features. Compared with CNNs and RNNs, Transformer has a global vision and better parallel computing ability as well as can handle variable-length fingerprints. Hence, it has better flexibility and scalability. However, the training of Transformer-based identification methods requires more training fingerprints, limiting its application.*

3.5. Data Augmentation-based Multi-Device Identification

The training of DL-based identification methods usually requires many fingerprint samples, and insufficient fingerprints will cause the over-fitting issue, thus degrading the identification accuracy. To address this issue, one promising approach is data augmentation, which is divided into two subcategories: added noise-based and generated samples-based methods. The former one leverages noises to improve the generalization of identification models, while the latter one improves the robustness of fingerprints by generating synthetic fingerprint samples.

3.5.1. Added Noise-based Methods
- *Online Augmentation:* Shen et al. [118] propose a Gaussian noise-based enhancement method and test the identification accuracy of the Transformer-based classifier with online-augmentation-based training, offline-augmentation-based training, and non-augmentation-based training. The results reveal that the online-augmentation-based classifier can obtain higher accuracy.

- *Noises Added to Latent Layers:* Different from adding Gaussian noises in the input layer, Meng et al. [120] proposed a LPNN approach to guarantee the access security of IIoT. Due to the latent layer has

stronger linear characteristics than the input layer for CSI fingerprints, the proposed LPNN method has better interpretability. Meng et al. [120] further define Fingerprint Library to provide the post-hoc explanations of the authentication system. The simulations under the static and dynamic IIoT environments demonstrate the superiority in identification accuracy of the proposed LPNN model than vanilla models.

- *Channel Fading Models Combined with Noises:* Shen et al. [195] leverage channel fading models and add the artificial white Gaussian noise to the signal to emulate different SNR levels to realize data augmentation. The fading models consider both the multipath and Doppler effect. The proposed approach can improve the identification accuracy in high-speed scenarios from 68.6% to more than 80%.

- *Performance under Dynamic Environments:* Zhang et al. [196] propose a device identification system, including the registration and detection stages. In the registration, the artificial noise with random power is added into the training fingerprints to improve the channel robustness. The simulations under the real-world environments, the laboratory static environments, and the laboratory dynamic environments have demonstrated its feasibility.

3.5.2. Generated Samples-based Methods
- *Data Augmentation Combined with Slicing Technique:* Yu et al. [182] design a multi-sampling-CNN to identify ZigBee devices and utilize the slicing techniques to obtain more fingerprint samples. The proposed slicing techniques can avoid the over-fitting issues effectively and solve the timing error during low SNR environments.

- *Comparison between Different Data Augmentation Methods:* Huang et al. [197] evaluate different data augmentation approaches for the DL-aided modulation classification, including rotation, flip, and Gaussian noise. The simulations on the open-source datasets, RadioML2016.10a, verify that all three approaches mentioned above can enhance the classification accuracy and accelerate the training speed, but the Gaussian noise-based method is worse than the other methods. Zhang et al. [198] compare four data augmentation methods for the DL-based device identification, including flip, rotation, shift, and noise. The simulations on

few-shot ADS-B verify their effectiveness. The proposed approaches can be extended to different classes of few-shot fingerprints.

- *Data Augmentation Combined with Random Integration:* Xie et al. [199] study the correlation between RF fingerprints and deoxyribonucleic acid sequency and design a random integration-based data augmentation approach. The proposed pseudo-random integration can obtain higher accuracy than traditional approaches and the random integration method.

- *Data Augmentation Combined with FL:* To guarantee the performance of DL-based identification techniques in time-varying channels, Piva et al. [200] leverage federated data augmentation method to propose a novel training structure. The simulation results on 200 SDRs verify that the proposed approach can enhance the accuracy of the FL-based scheme by up to 19%.

- *Adversarial Data Augmentation:* Liu et al. [201] employ self-supervised learning during the pre-training phase to mitigate the reliance on labeled fingerprint samples. In the fine-tuning phase, knowledge transfer is utilized to alleviate the dependence on samples from the target dataset. Additionally, by introducing a "relaxation" mechanism in the feature space, an adversarial augmentation method that facilitates flexible and dynamic data transformations is further proposed, thereby enabling effective self-supervised learning.

- *Performance under Industrial Scenarios:* Liao et al. [202] propose three data augmentation methods to generate additional CSI samples for the training of the FCNN-based authentication model, including the averaging data augmentation, the exponential averaging data augmentation, and the stochastic weight averaging data augmentation. The simulations on real industrial datasets demonstrate that the proposed methods can accelerate the training speed and enhance the authentication accuracy.

Lesson 5. *The added noise-based data augmentation methods include adding noises in the input layers [118, 196] and latent layers [120] as well as combining noises with channel fading models [195]. The generated samples-based methods include typical ration, flip, and shift [197, 198] as well as integration*

methods [199] and generative models [108, 130]. Moreover, the combination of different data augmentation methods may obtain better performance.

Here, we summarize the contributions of all multi-device identification schemes based on RNN, Attention, and data augmentation in Tab. 7.

Table 7: Multi-Device Identification Schemes based on RNN, Attention, and Data Augmentation

Models		Ref.	Year	Major Contribution
RNN	RNN Alone	[114]	2019	Compare the performance between FCNN, CNN, and RNN on ZigBee devices
		[115]	2018	Propose a LSTM-based method to capture the long-term and short-term features of I/Q fingerprints.
		[117]	2021	Assess the identification performance of CNN and LSTM through massive experiments.
	Combination of CNN and RNN	[44]	2020	Present RFF-ConvRNN to extract spatial and time-dependent features.
		[121]	2020	Provide DBi-LSTM and Conv-OrdsNet to against the interference of unreliable fingerprints, and verify the performance on the open-source datasets [64].
		[187]	2019	Design ConvLSTM to exploit the temporal and spatial properties of I/Q fingerprints, and compare its performance with LSTM and GRU.
Attention	Attention Partly	[188]	2021	Propose SeNet to extract characteristics in frequency domain, and further verify its performance on 20 WiFi devices.
		[189]	2020	Pay attention to the message structure and provide MSCAN, which can leverage rough prior information to enhance identification performance.
		[198]	2023	Propose a data-and-knowledge dual-driven architecture to exploit semantic information, and compare its performance with VGG, CNN [29], and AttMsCn.
	Transformer	[118]	2021	Provide a transformer-based method to identify LoRa devices with the signals of variable length, and further propose a multi-packet inference method to greatly enhance the accuracy.

Models		Ref.	Year	Major Contribution
Data Augmentation		[119]	2021	Combine transformer and ICS algorithm to handle devices that appear outside the closed set, and verify its superiority in accuracy and robustness than Hybrid OvA [191], Modified ICS [192], MLOSR[193], and CROSR [194]
	Added Noise-based	[118]	2021	Leverage Gaussian noise to enhance accuracy, and further propose online and offline augmentation.
		[120]	2023	Propose LPNNs that add Gaussian noises in the latent year to improve generalization.
		[195]	2022	Utilize channel fading models and artificial noise to realize augmentation for mobile scenarios.
		[196]	2023	Add artificial noise with random power into training fingerprints to improve the channel robustness.
	Generated Samples-based	[182]	2019	Design MSCNN to recognize ZigBee devices and use slicing techniques to obtain more samples.
		[197]	2020	Evaluate different data augmentation methods, including rotation, flip, and Gaussian noise.
		[198]	2022	Compare different data augmentation approaches for few-shot ADS-B scenarios.
		[199]	2020	Design a random integration-based method and compare its performance with conventional methods and random integration-based methods.
		[200]	2021	Leverage DAG methods to enhance accuracy for time-varying environments.
		[201]	2024	Propose an adversarial augmentation method to facilitate flexible and dynamic data transformations.

Models		Ref.	Year	Major Contribution
		[202]	2020	Propose three methods to generate additional CSI fingerprints, including averaging data augmentation, exponential averaging data augmentation, and stochastic weight averaging data augmentation.

3.6. CVNN-based Multi-Device Identification

Considering that the real-valued neural network can not directly process complex data, some researchers utilize CVNNs to handle complex signals to obtain better extraction performance.

- *Performance under ADS-B and WiFi scenarios:* Gopalakrishnan et al. [125] test the proposed CVNN architecture on external database with two different radio protocols: WiFi 802.11a (5.8 GHz) and 802.11g (2.4 GHz) commercial off-the-shelf transmitters and ADS-B (1.09 GHz) narrowband signals. The results show that the CVNN model can achieve 81.66% and 99.53% accuracy on ADS-B and WiFi datasets, while RVNNs can only achieve 75% and 97.89% accuracy, respectively.

- *CVNNs Combined with Network Compression:* Wang et al. [126] develop an efficient approach based on CVNN and network compression named SlimCVNN to achieve both high accuracy performance and low model complexity. The simulations on synthetic fingerprint datasets verify that there is almost no accuracy gap between CVNN and Slim-CVNN, while SlimCVNN has 10% 30% model sizes of CVNN.

- *Comparison with RVNNs:* Agadakos et al. [163] provide two CVNN variations: Convolutional CVNN and Recurrent CVNN for modeling signals and time series, respectively. The massive experiments demonstrate the superiority of the CVNN in identification accuracy than RVNNs under different protocols and SNR environments. Chen et al. [203] use real LoRa and WiFi I/Q datasets to provide a deeper understanding of the impact of the fingerprint representation and the architectural layers of the models. The various experimental results verify that the CVNNs consistently obtain better identification accuracy than their "equivalent" RVNNs.

- *CVNNs Combined with FFT:* Stankowicz et al. [204] utilize large and real-time I/Q datasets and explore the impact of input representation, output representation, and processing of complex values on the identification accuracy. They conclude that when using CVNN as the classifier, the representation combined I/Q and FFT can obtain better performance than I/Q.

- *CVNNs Combined with BN and Dropout Layers:* Gu et al.[205] design a CVNN-based architecture, which adds batch normalization layer after every fully-connected layer and adds the Dropout layer after each layer to optimize model parameters and avoid the over-fitting issues. The simulations on five drone signal datasets verify the advantages of the proposed method than baseline models in classification accuracy, prediction time, and confusion matrix.

- *CVNNs Combined with Residual Networks:* Wang et al. [206] propose a deep complex residual network for device identification. Compared with the approach based on contour stellar (with the identification success rate of 90.4%) and CCVNN (with the identification success rate of 94.8%), the suggested approach can obtain the identification success rate of 99.56% for 20 WiFi devices.

- *CVNNs Combined with Metric Learning:* Considering insufficiently labeled training fingerprints, Fu et al. [207] introduce pseudo labels and metric learning and propose the metric-adversarial training. The proposed method focuses on exploiting the discriminative semantic characteristics. The proposed objective function is based on semi-supervised metric learning and virtual adversarial training. The simulations on the open-source large-scale real-world ADS-B datasets and WiFi datasets verify the superiority of the proposed MAT method than DRCN [208], SSRCNN [209], Triple-GAN [210, 211], and SlimMIM [212].

- *CVNNs Combined with Attention Mechanisms:* Jiang et al. [213] combine CVNNs and multiple attention mechanisms to enhance authentication performance for satellite communication systems. The simulations on Xingyun satellite demonstrate its superiority than traditional CNNs and CVNNs.

Lesson 6. *The CVNN-based identification methods have been studied for ADS-B datasets [125], WiFi datasets [125, 203], and LoRa datasets [203]*

48

as well as have been combined with network compression [126], CNNs [163], RNNs [163], FFT [204], and residual networks [206] to obtain higher accuracy than the RVNN-based methods. In addition, the CVNN-based methods have better adaptability and expansibility to the changes of different protocols and the number and scale of individuals. However, the training of CVNN-based methods requires more fingerprint samples and more parameters. Hence, the compression of CVNNs is an important issue.

3.7. GAN-based Multi-Device Identification

GAN is a typical deep UL model and is consisted of two modules, including the generative module and discriminative module for generating fake samples and judging whether the sample is true or false, respectively. In addition, GANs can be combined with classifiers to realize classification tasks.

- *Identification with Fewer Fingerprints:* Zhao et al. [129] propose AC-WGANs to realize device identification with fewer fingerprint samples and higher dimensional features. The proposed UAVs detection system includes three steps: data collection, pre-processing, and classification. The simulation results show that the proposed AC-WGANs can obtain the accuracy of 95%.

- *Performance under Noisy Environments:* Zeng et al. [214] propose a pre-processing algorithm to address the issues that the identification performance is poor in dynamic interference scenarios and the models are dependent on the quality of datasets. The proposed approach can modify the synchro-squeezed wavelet transforms through energy regularization so that the pre-processing is simplified and the robustness of fingerprints is improved. In addition, the unsupervised neural network noise feature extracting GAN is presented to obtain precise clean fingerprint characteristics from noisy signals. The simulation results show that the proposed architecture can obtain the accuracy of 96%, 85%, and 25% with the SNR of 10 dB, 0dB, and -20 dB, respectively.

- *Comparison with CNNs:* Lin et al. [215] use the SSGANs [216] to achieve semi-supervised signal recognition for contour stellar images. The proposed SSGANs can exploit the inherent features of real labeled fingerprints, real unlabeled fingerprints, and fake unlabeled fingerprints. The simulation results indicate that the proposed SSGANs can obtain higher identification accuracy than CNNs when using a small number of labeled fingerprint samples.

- *Detection of Malicious Fingerprints and Identification of Multiple Legal Devices Simultaneously:* Roy et al. [108] use GANs to recognize adversarial fingerprints and identify wireless devices. The proposed generative module can generate fake fingerprints and the proposed discriminative module can distinguish the real fingerprints from the fake ones. The CNN module can achieve the classification of legitimate devices. The simulations on multiple USRP b210s verify the feasibility of the proposed architecture. Roy et al. [217] provide an RF adversarial learning architecture to detect rogue devices and identify trusted transmitters. The designed discriminator can detect rogue devices with the accuracy of 99.9%. The designed RNN model can reach the accuracy of 97% for legal transmitters.

- *GANs for Unsupervised Identification:* To realize unsupervised identification, Gong et al. [218] propose an unsupervised identification architecture based on InfoGANs and RF fingerprint embedding. The gray histogram is constructed from the bispectrum and then embedded into the proposed system. The priori statistical features of radio channels are leveraged in the form of the structured multi-modal latent vectors. The simulations verify the superiority of the proposed InfoGANs in evaluation score and identification accuracy.

3.8. AE-based Multi-Device Identification

Similar with GANs, AEs are also deep UL models. AEs are composed of encoders and decoders for dimension reduction and generation of samples, respectively. Variational Autoencoder (VAE) is a probability distribution-based AE method and has better generation performance. Besides, contractive AEs and regularized AEs are typical discriminative models.

- *Comparison with CNNs:* Yu et al. [131] propose a general Denoising AE (DAE)-based framework for the identification of devices and further design a partially stacking approach to combine the semi-steady and steady-state fingerprints of ZegBee transmitters. The proposed partially stacking-based convolutional DAE can realize the reconstruction of the high-SNR signals and identification. The simulation results show that the proposed PAS-DAE can enhance the classification accuracy by 14% to 23.5% than CNN under the low SNR (from -10 dB to 5 dB) environments.

- *AEs Combined with Device Authentication Code:* Bassey et al. [132] propose an AE-based architecture for intrusion detection and present the concept of device authentication code. The reconstruction error is defined as the authentication code of devices, and Kolmogorov-Smirnov test is utilized to judge whether the fingerprints are legitimate or not. The simulations on 6 ZigBee and 5 USRP devices verify the effectiveness and robustness in channel conditions, mobility, and varying signal strength.

- *AEs for Unsupervised Identification:* Huang et al. [219] suggest the masked AE-based unsupervised pre-training approach to achieve identification with limited training fingerprints. The pre-trained network is used to predict the masked segment of fingerprints, which will be fined tuned with the supervised labels. The simulations on both synthetic fingerprints and real-world fingerprints verify the superiority of the proposed pre-training with block-wise channel-aligned masking.

- *Comparison with GANs:* Xie et al. [220] propose a few-shot unsupervised identification method, where the AE module is used to obtain the latent vector of Hilbert time-frequency spectrum. The latent space can represent the hidden characteristics of fingerprints. Then, the clustering algorithm can cluster and label the latent vector, and the meta-learning method is used to classify fingerprints. The simulations under AWGAN, Rayleigh, and Rice channels demonstrate the superiority of the proposed architecture than InfoGANs [218].

Lesson 7. *AEs and GANs are typical generative DL models and are usually used for dimension reduction and generation of fingerprint. AEs and GANs have been studied for UAVs [129], low SNR environments [214], ZigBee devices [131] and USRP devices [132] as well as have been combined with other techniques to realize identification with fewer fingerprints [129], unsupervised identification [218, 219], and identification and detection simultaneously [108, 217]. AEs and GANs have outstanding unsupervised feature extraction capability and have great potential in multi-device identification.*

Here, we summarize the contributions of all multi-device identification schemes based on CVNN, GAN, and AE in Tab. 8.

Table 8: Multi-Device Identifications Schemes based on CVNN, GAN, and AE

Models	Ref.	Year	Major Contribution
CVNN	[125]	2019	Compare the performance between RVNN and CVNN on WiFi 802.11a (5.8 GHz) and 802.11g (2.4 GHz) protocols.
	[126]	2021	Develop SlimCVNN based on CVNN and network compression to realize high accuracy and low complexity.
	[163]	2019	Provide CCVNN and RCVNN respectively for modeling signals and time series.
	[203]	2022	Use LoRa and WiFi I/Q datasets to provide a deeper understanding of the impact of fingerprint representation and architectural layers of models.
	[204]	2019	Explore the impact of input representation, output representation, and processing of complex values on accuracy, and further conclude that the representation combined I/Q and FFT can obtain better performance than I/Q for CVNNs.
	[205]	2020	Design a CVNN-based architecture, which adds BN layer after every fully-connected layer and adds the Dropout layer after each layer to optimize model parameters and avoid the over-fitting issues.
	[206]	2020	Present a deep complex residual network, and compare its performance with CCVNN on 20 WiFi devices.
	[207]	2023	Introduce pseudo labels and metric learning to propose MAT, which focuses on exploiting the discriminative semantic characteristics, and further demonstrate its performance by the comparison with DRCN [208], SSRCNN [209], Triple-GAN [210, 211], and SlimMIM [212].
GAN	[108]	2019	Use GANs to recognize adversarial fingerprints and identify devices, and verify its feasibility on multiple USRP b210s.
	[129]	2018	Propose AC-WGANs to achieve identification with fewer fingerprint samples and higher dimensional features for UAVs.

Models	Ref.	Year	Major Contribution
	[214]	2022	Design a pre-processing algorithm to tackle the issues that the authentication accuracy is poor in dynamic interference scenarios and the models are dependent on the quality of datasets, and further present NEGAN to obtain precise clean fingerprint features from noisy signals.
	[215]	2021	Use SSGANs to realize semi-supervised signal recognition for contour stellar images.
	[217]	2020	Provide RFAL to detect rogue devices and identify trusted transmitters.
	[218]	2020	Combine InfoGANs and RFFE to realize unsupervised identification.
AE	[131]	2019	Present DAE and PSC-DAE realize the reconstruction of the high-SNR signals and identification.
	[132]	2021	Propose an AE-based architecture for intrusion detection and present the concept of device authentication code.
	[219]	2022	Design an unsupervised pre-training method based on MAE to realize identification with limited training fingerprints.
	[220]	2022	Present a few-shot unsupervised identification method, where the AE module and clustering algorithm are used for dimension reduction and signal classification, respectively, and further compare its performance with InfoGANs [218] under AWGAN, Rayleigh, and Rice channels.

4. ML-based PLA for Attack Detection

In this section, we present the ML-based methods for attack detection. We divide the ML techniques into three sub-categories and compare them in detail. The organization of this section is illustrated in Fig. 8.

4.1. SL-based Attack Detection

As illustrated in Fig. 9, SL techniques can learn the distribution from labeled datasets. Compared with the non-ML-based attack detection methods, the ML-based approaches can automatically learn the inherent characteristics of fingerprints given their labels and obtain the optimal threshold. Here,
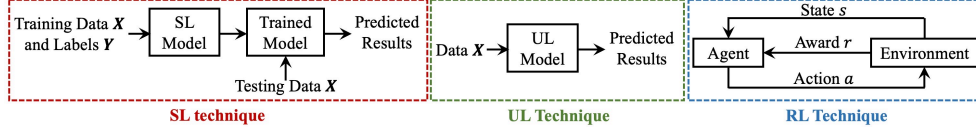
Figure 9: Illustration of SL, UL, and RL techniques.

we classify SL techniques into logistic regression, LDA, DT, KNN, SVM, ensemble learning, ELM, FL, and DL as follows.

4.1.1. Logistic Regression

Logistic regression is a generalized linear model. Xiao et al. [143] provide a multi-landmark-based authentication scheme, where each landmark with multi-antenna can collect the distributed RSSIs to obtain more distinguishable characteristics. The Frank-Wolfe algorithm based on logistic regression is used to address the convex optimization problem introduced by the ML-based coefficient estimation of the regression. A distributed Frank-Wolfe-based scheme and an incremental aggregated gradient-based scheme are proposed to reduce the computation overhead, and their convergence performance and communication overheads are analyzed. The simulations on USRPs verify that the proposed distributed Frank-Wolfe-based scheme can realize the same detection performance as the Frank-Wolfe-based scheme, and the incremental aggregated gradient-based scheme can obtain a better detection performance.

4.1.2. LDA

LDA can map high-dimensional samples into the optimal discriminative vector space to extract classification information and compress the dimension of feature space.

- *LDA for EI Scenarios:* Wang et al. [144] propose a cluster head safeguarding mechanism realized by edge intelligence (EI) for UAVs swarm travels. The LDA algorithms is used to fuse the detection decision precisely through projecting the high-dimensional features into the low-dimensional space. Such design can keep the necessary characteristics and realize maximum separability. The simulations on UAVs verify that the proposed scheme can achieve higher detection accuracy than the baseline schemes proposed by [221] and [222].

54

- *LFDA based on Multi-Attributes:* By exploiting time-of-arrivals, RSS, and cyclic-features of channels, Pei et al. [223] propose two ML-based PLA methods, including linear Fisher discriminant analysis and SVM. The simulation results show that the proposed ML-based schemes can obtain lower miss detection probability and false alarm probability than the baseline scheme proposed by [26]. In addition, the proposed linear Fisher discriminant analysis-based scheme has low time complexity and space complexity.

4.1.3. DT

DT is a tree-based architecture describing the classification of samples. DT is composed of different nodes and directed edges, and the nodes include father node, internal nodes, and leaf nodes, denoting samples, features, and categories, respectively.

- *Comparison with DT, SVM, and KNN:* Enad et al. [145] propose three ML-based PLA schemes, including DT, SVM, and KNN. The simulations on the OFDM systems show that all the ML-based schemes can obtain higher detection accuracy than the statistical-based scheme.

- *DTs Combined with Bootstrap Aggregating:* Du et al. [224] provide a PLA scheme based on bootstrap aggregating and DT for dynamic industrial scenarios. The authentication architecture includes feature extraction, classification based on positive-unlabeled learning bagging strategy, and distinction phase. Multi-dimensional fingerprints are extracted, including amplitude, phase, CFO, and variance. The simulations on real industrial datasets verify the feasibility of the proposed strategy.

4.1.4. KNN

The core concept of KNN is that if most of k nearest samples of a samples in the feature space belong to a certain category, the sample also belongs to this category. Senigagliesi et al. [146] study the authentication problem when there are relay nodes between Alice and Bob. Four cases are considered, including passive relays, autonomous active relays, coordinated active relays, and omniscient relays. Besides statistical methods, the on-class nearest neighbor-based scheme is proposed to achieve low complexity with a small number of training fingerprint samples.

4.1.5. SVM

SVM is a generalized linear classifier and its decision boundary is the maximum-margin hyperplane. SVM can utilize hinge loss to calculate empirical risk. In addition, SVM can realize nonlinear classification by kernel methods.

- *Authentication under Time-Varying Channels:* Fang et al. [17] provide a ML-based adaptive PLA scheme to learn and leverage the complex time-varying environments so that the robustness and reliability of PLA are improved. The PLA problem is modeled as a linear system, and the multi-dimensional fingerprints is reduced to a single-dimensional scalar data to reduce the complexity. The adaptive algorithm based on kernel least mean square is further proposed to formulate the learning objective as a convex problem and learn the variations of fingerprints. The simulations verify that the proposed approach can greatly enhance the authentication performance during time-varying channels.

- *Authentication of Mobile Users:* Liu et al. [147] propose a CSI-based PLA architecture for stationary and mobile terminals. The identification includes the attack-resilient user profile builder and profile matching authenticator, which is based on SVM to realize packet level user identification. The evaluation results show that the proposed scheme is highly effective.

- *Defense Against Both Sybil and Clone Attacks:* By combining with the edge devices, Chen et al. [6] design a lightweight SVM-based PLA scheme to detect both Sybil and clone attacks in industrial wireless edge networks. The training is offline and the authentication decision is online. The simulations on two real industrial scenarios verify that the proposed scheme can realize the accuracy of 84%.

- *Authentication under mmWave MIMO Channels:* By leveraging mmWave MIMO channels and CFO, Liu et al. [225] present an online PLA framework. The Gaussian kernel approach and representer theorem is utilized to model the PLA problem as a binary classification model. An online algorithm is further developed based on the constructed convex objective function. The analytical expressions for false alarm and detection rates are also derived. The simulations verify that the proposed solution can defend against spoofing attacks in mmWave MIMO scenarios.

- *Fuzzy Learning:* Fang et al. [226] provide a fuzzy learning-based PLA scheme to combine muti-dimensional fingerprints. The designed model is based on imperfect feature estimation to make decisions, thus providing a higher-level protection for legal devices. A hybrid learning method is further provided to update parameters of systems, where the least-square estimator and gradient descent are used for linear and nonlinear parameters, respectively.

4.1.6. Ensemble Learning

The core concept of ensemble learning is to construct and combine multi-learners. Specifically, a group of "individual learners" are generated first, and then they are combined through a sort of strategies, such as average method and voting method.

- *Threshold-Free Authentication:* Pan et al. [88] propose four threshold-free PLA schemes with the help of ML techniques, including DT, SVM, KNN, and ensemble learning. The authentication performance of the PLA based on channel matrices and channel differences are also compared. The channel differences are represented as (7), (8), and (9). The simulations verify that the proposed authentication methods can significantly improve the authentication accuracy and are suitable for wireless industrial cyber-physical systems.

$$\boldsymbol{H}_{\text{diff}}^1 = \frac{||\boldsymbol{H}_t - \boldsymbol{H}_1||_2}{||\boldsymbol{H}_1||_2} \tag{7}$$

$$\begin{cases} \boldsymbol{H}_{\text{diff}}^2 = \left| \frac{\sum_{m,n} |\boldsymbol{H}_t(m,n) - \boldsymbol{H}_{t-1}(m,n) e^{j\phi(t)}|}{\sum_{m,n} |\boldsymbol{H}_{t-1}(m,n) - \boldsymbol{H}_{t-2}(m,n) e^{j\phi(t-1)}|} - 1 \right| \\ \phi(t) = \arg\big(\boldsymbol{H}_t(m,n), \boldsymbol{H}_{t-1}^*(m,n)\big) \end{cases} \tag{8}$$

$$\boldsymbol{H}_{\text{diff}}^3 = \left| \frac{\sum_{m,n} |\boldsymbol{H}_t(m,n) - \boldsymbol{H}_{t-1}(m,n)|^2}{\sum_{m,n} |\boldsymbol{H}_{t-1}(m,n) - \boldsymbol{H}_{t-2}(m,n)|^2} - 1 \right| \tag{9}$$

- *Authentication based on WV under Industrial Scenarios:* Xie et al. [149] proposed a weighted voting (WV)-based PLA approach for edge computing scenarios. The proposed WV method based on simple lines and simple parts can realize cooperative decision, thus improving the accuracy and reducing the complexity. The simulations on public datasets and field-measured datasets verify that the proposed scheme

can realize better performance than the baseline schemes, including direct classification, averaged classification, and down-sampled classification, proposed by [227, 228, 229], respectively.

- *Cooperative Authentication based on WV:* Zhou et al. [230] propose a decision-level-based cooperative PLA scheme aimed at enhancing secure access. A dynamic WV mechanism is introduced to address challenges posed by unreliable cooperators. This approach effectively manages cooperators, ensuring concise and efficient cooperation management to bolster system security.

4.1.7. ELM

ELM is a special FCNN, and it has a single latent layer. The weight parameters in the latent layer do not need to be updated, and the learning process only calculates the output weights. Wang et al. [150] present an ELM-based PLA architecture to exploit the multi-dimensional features of channel environments, thus detecting the spoofing attackers in dynamic networks. The simulations show that the proposed ELM-based scheme can obtain lower minimum Bayes risk than the baseline scheme proposed by [27].

4.1.8. FL

FL is a distributed ML technique, where multi-devices can realize the joint training models by interacting the intermediate parameters without sharing training datasets. Wang et al. [151] provide a horizontal FL-based collaborative PLA scheme to release computational pressure on IoT devices with limited computation and storage resources. The PLA problem is formulated as the training problem of the classifier, where the aim is to obtain the weight parameters. Then, a distributed identification architecture is proposed to assign the classification task to trusted collaborators. Finally, the whole local parameters are aggregated at the center device. The simulation results show that the proposed horizontal-FL-based scheme can obtain the miss detection rate and false alarm rate of less than 1%.

4.1.9. DL

The introductions of DL have been presented in Section III. DNNs can extract high-level characteristics of fingerprints to realize attack detection.

- *FCNN, CNN, and CPNN for Industrial Scenarios:* Liao et al. [152] propose a DL-based PLA framework to guarantee the identity security

of industrial wireless sensor networks, and further provide three PLA algorithms based on DL, including FCNN, CNN and convolution preprocessing neural network (CPNN). The proposed CPNN-based PLA requires few computational resources. The mini batch trick is utilized to improve the training speed. The simulation on USRPs demonstrates the effectiveness of the proposed PLA algorithms.

- *Comparison with KNN and SVM:* Pan et al. [231] propose a residual network-based PLA scheme to identify mobile devices in industrial wireless CPS. The simulations on real industrial datasets demonstrated its superiority than KNN and SVM.

- *Authentication for Industrial Scenarios:* Pan et al. [232] present a clone detection scheme based on back propagation neural network and physical-layer reputation for industrial wireless CPS. The physical-layer reputation is accumulated by CSI, and the attack detection is performed by group detection. The numerical simulations on USRPs verify that the proposed scheme can greatly enhance the detection accuracy.

- *Authentication based on Confidence Score Branch:* Wang et al. [233] design an FCNN-based PLA scheme to realize fast and lightweight identification. The CSI information is mapped to the location of devices, and is further mapped to its identity. The mapping relationship between the CSI fingerprints and the identity is learned by the proposed authenticator with a confidence score branch. The simulation results indicate that the proposed scheme is robust to channel estimation errors.

- *Authentication based on SNR Trace:* Wang et al. [234] propose a PLA scheme based on the SNR trace obtained at the receiver in the sector level sweep process, and further present two ML-aided approaches. For the first approach, a novel DNN framework is proposed, including back propagation neural network, forward propagation networks, and GANs. For the second approach, the Siamese network is provided to address the issue that historical fingerprints can not support the authentication in a new communication session. The simulations under different scenarios verify that the proposed scheme can realize the detection accuracy of 99%.

- *Authentication based on Semantic Fingerprints:* Gao et al. [235] employ a single-stage object detection network to extract the semantic knowledge of CSI in MIMO systems. The suggest approach substantially minimizes data processing overhead and authentication latency.

- *Authentication of Mobile Devices:* Wang et al. [236] extract correlation and scattering characteristics of mobile devices and convert them to a CSI sequence, which is further used for classification by CNNs. Jing et al. [237] further present a ResNet-based PLA model to authenticate multiple mobile transmitters. The training mechanism not only improves the accuracy of authentication but also accelerates the convergence speed of ResNet. Han et al. [238] introduce a model-driven learning algorithm, which focuses on extracting pertinent channel features to alleviate inter-symbol and inter-carrier interferences. Experimental findings demonstrate that the proposed scheme outperforms existing data-driven models across different SNRs and velocities.

Here, we summarize the contributions of all SL-based attack detection schemes in Tab. 9.

Table 9: The SL-based Attack Detection Schemes

Models	Ref.	Year	Major Contribution
Logistic Regression	[143]	2018	Propose a multi-landmark-based authentication scheme and introduce FW and dFW algorithms based on logistic regression to address the convex optimization problem and reduce the communication overhead, respectively.
LDA	[145]	2021	Present a CF safeguarding mechanism achieved by EI for UAVs swarm travels, and verify its superiority than the baseline schemes proposed by [221, 222].
	[223]	2014	Design two attack detection schemes based on LFDA and SVM by exploiting time-of-arrivals, RSS, and cyclicfeatures.
DT	[145]	2020	Compare three ML-based PLA schemes for OFDM systems, including DT, SVM, and KNN.
	[224]	2023	Combine bootstrap aggregating and DT to detect signals for dynamic industrial scenarios.

Models	Ref.	Year	Major Contribution
KNN	[146]	2022	Study the authentication problem by considering relay nodes between Alice and Bob and four cases, including passive relays, autonomous active relays, coordinated active relays, and omniscient relays.
SVM	[17]	2019	Provide a kernel-based adaptive PLA scheme for complex time-varying environments.
	[147]	2018	Propose an authentication architecture based on CSI and SVM for stationary and mobile terminals.
	[6]	2021	Show an SVM-based PLA framework to detect both Sybil and clone attacks in industrial wireless edge networks.
	[225]	2022	Develop an online PLA architecture based on Gaussian kernel and CFO for mmWave MIMO channels.
	[226]	2020	Provide a fuzzy learning-based approach for multi-dimensional fingerprints, and further provide a hybrid learning method to update parameters of systems.
Ensemble Learning	[88]	2019	Propose four threshold-free PLA schemes based on ML techniques, including DT, SVM, KNN, and random forest.
	[149]	2022	Present a WV-based approach for edge computing scenarios, and further confirm its effectiveness on public datasets and fiddle-measured datasets by the comparison with direct classification [227], averaged classification [228], and down-sampled classification [229].
ELM	[150]	2017	Introduce an ELM-based PLA scheme to defend against spoofing attackers in dynamic networks, and further demonstrate that it can obtain lower minimum Bayes risk than the baseline scheme proposed by [27].
FL	[151]	2021	Develop an HFL-based collaborative PLA scheme to release computational pressure on IoT devices.
DL	[152]	2019	Provide a DL-based PLA framework, and further propose three PLA. algorithms based on FCNN, CNN, and CPNN.
	[231]	2020	Propose a residual network-based method for the authentication of mobile devices in industrial wireless CPS, and further verify its superiority in attack detection than KNN and SVM on real industrial datasets.

Models	Ref.	Year	Major Contribution
	[232]	2021	Present a clone detection scheme based on BPNN and physical-layer reputation.
	[233]	2022	Design an FCNN-based detection approach, where the mapping relationship between CSI fingerprints and the corresponding identity is learned by the confidence score branch.
	[234]	2021	Propose a PLA architecture based on SNR traces, and further present an authentication algorithm based on BPNN, forward propagation networks, and GANs.
	[235]	2024	Employ a single-stage object detection network to extract the semantic knowledge of CSI in MIMO systems.
	[236]	2024	Extract correlation and scattering characteristics of mobile multi-users and convert them to CSI sequences.
	[237]	2024	Propose the training mechanism to improve the accuracy of authentication and accelerate the convergence speed of ResNet.
	[238]	2024	Introduce a model-driven learning algorithm, which focuses on extracting pertinent channel features to alleviate inter-symbol and inter-carrier interferences.

Lesson 8. *The SL-based attack detection schemes have been studied for UAVs [144], OFDM systems [145], IIoT [149, 88], time-varying environments [17], mobile users [147], mmWave MIMO channels [225], 5G links [148], and EI scenarios [149]. Among the SL-based methods, SVM and DNNs are most widely used models due to the efficient nonlinear learning ability. However, the SL algorithms usually require many labels of transmitters and attackers, limiting the actual application.*

4.2. UL-based Attack Detection

In wireless systems, it is reasonable to assume that the prior information of attackers is unknown or the fingerprints of attackers are unlabeled. For this reason, SL algorithms are not always feasible due to they require labeled datasets. To address this issue, UL algorithms are promising methods. The related works are as follows.

4.2.1. Clustering

Clustering is a typical UL classification algorithm, and it can divide fingerprints into several disjoint subsets (also called clusters) to realize malicious node detection.

- *Clustering of RSSs:* Yang et al. [239] propose a PLA scheme based on RSS and clustering to determine the number of attackers for wireless networks with multiple spoofing attackers. The number of clusters is estimated through partition energy and merging energy [240]. The simulations under two real office buildings with WiFi networks and ZigBee networks verify that the proposed method can obtain the hit rate and precision of over 90 percent.

- *Clustering of Multi-Attributes:* Xia et al. [20] study the correlation of multi-fingerprints and propose an unsupervised PLA scheme based on non-parametric clustering algorithm. Based on the evolution algorithm provided in [241], the improved system evolution method is proposed to reduce the complexity. The simulations on synthetic datasets and real industrial datasets show that the proposed scheme can realize the F_1 measure of more than 99% without the prior information of attackers.

- *Clustering Algorithms Combined with RNNs:* Wang et al. [242] combine DNN and K-means to realize semi-supervised learning-based PLA. The convolutional recurrent neural network is utilized to learn the local characteristics and the dependencies between different frequencies in CSI fingerprints. The simulation results reveal that the proposed scheme can yield excellent detection performance with limited labeled fingerprints.

4.2.2. OCC-SVM

Given only Alice's fingerprint samples, OCC-SVM algorithms can identify data points distinct from the legal fingerprint samples by constructing a boundary in high-dimensional feature space, allowing it to perform well in attack detection when Eve's fingerprint samples are scarce.

- *Authentication under LEO Satellite Scenarios:* Abdrabou et al. [243] propose an effective PLA solution based on single-class classification SVM to defend against spoofing attacks in low-earth orbit (LEO) satellite scenarios. The proposed SCC-SVM scheme can learn the inherent

features of RSS and Doppler frequency spread, and the performance for on-the-pause satellite communication systems is further evaluated. The simulation results reveal that utilizing both RSS and Doppler frequency spread can obtain lower missed detection rate and false alarm rate.

- *Performance versus Different Kernel Functions:* Hoang et al. [244] propose an architecture to convert radio signals into structured datasets and further present an SVM-based authenticator. Two classes of SVM classifiers are considered, including a classic twin-class SVM and a single-class SVM. The performance of the proposed schemes is evaluated over different choices of the kernel function, fingerprints, and the eavesdroppers' power.

- *Comparison with Statistical Decision Methods:* Senigagliesi et al. [245] evaluate and compare two different statistical decision approaches for PLA, and further propose two ML-based schemes based on nearest neighbor and SVM. The numerical simulations indicate that the ML-based schemes can realize the lowest probability of missed detection when there is a small spatial correlation between the main channel and the adversary one, otherwise, the statistical approaches are superior.

- *OC-SVMs Combined with Antenna Diversity Techniques:* Abdrabou et al. [148] propose an adaptive lightweight PLA approach that exploit antenna diversity technique to enhance the recognizable fingerprints. The one-class classifier SVM is utilized for outlier and anomaly detection. The simulations on sounding reference signals in the 5G uplink radio frame show the superiority of the proposed scheme than the baseline schemes proposed by [223] and [245].

4.2.3. Manifold Learning

Manifold learning can recover the low-dimensional manifold structure from high-dimensional sampled data, and further find the corresponding embedded mapping, thus realizing dimension reduction or data visualization. Xia et al. [154] consider the time-varying characteristics of fingerprints caused by the mobility of UAVs and formulate the identification problem as the recognition of nonlinearly separable data. The manifold learning is utilized to address this issue by establishing the Markov chain of fingerprints in the time domain and evaluating the state transition probability of UAVs.

The simulation results show that the proposed scheme can improve the detection accuracy by more than 18% compared with baseline schemes.

4.2.4. GMM

GMM is a special clustering algorithm, which can decompose the object into several sub-models based on Gaussian probability density functions.

- *Online Authentication:* Gulati et al. [155] use GMM to formulate the probabilistic model of radio channels of transmitters. The proposed scheme can realize online learning and parameter updating. The simulation results show that the proposed scheme can realize the miss detection rate of 0.1% for the false alarm rate of 0.4%.

- *Authentication under MC-MTC scenarios:* Weinand et al. [246] propose a GMM-based detection method to defend against data manipulation and masquerade attacks for mission critical machine type communications in wireless networks. The simulation results show that the proposed scheme can reach detection rate of 99.98%.

- *Comparison with RL Techniques:* To realize high robustness to the errors of channel estimation, Qiu et al. [247] present a PLA scheme based on pre-processing channel variations and multi-dimensional fingerprints. The PLA problem is further formulated as the comparison of two-dimensional feature vectors. The proposed scheme based on probabilistic model requires only a few training fingerprints of legitimated users. The simulation results show its superiority than the schemes proposed in [27] and [246].

4.2.5. GP

GP is the combination of a series of random variables that obey Gaussian distribution in an index set. The classic GP models include GP Regression (GPR) and GP Classification (GPC). GPR can be used to predict fingerprints, while GPC can identify fingerprints directly.

- *GPR:* Wang et al. [156] provide a PLA scheme based on GP channel prediction for IoT devices. Specifically, historical CSI fingerprints and geographical data of devices are leveraged to construct a mapping to predict the next legal CSI fingerprint for identification. The one-class authentication scheme is further proposed, which requires no channel

information of attackers. The simulations on quasideterministic radio channel generator verify the superiority of the proposed scheme than the baseline schemes proposed in [141] and [248].

- *GPC:* Qiu et al. [247] propose a GP-based PLA scheme to track multi-targets and reduce the identification overhead. The proposed scheme can intelligently learn the dynamic time-frequency fingerprints of channels.

4.2.6. AE

The introductions of AE have been provided in Section III-H. The latent space with lower dimensions can be used for authentication. Meng et al. [157] suggest a PLA scheme based on hierarchical variational autoencoder to defend against spoofing attacks in IIoT without requiring attackers' training fingerprints. The designed architecture is a cascade neural network based on AE and VAE. The AE module serves as a low-level extractor, and the VAE module is for further dimension reduction and authentication. The VAE module is equipped with a single-peak and a revised double-peak Gaussian distribution for fingerprint reproduction and classification, respectively. The constructed loss function is derived, including an approximation and an exact calculation. The simulation results demonstrate its superiority than the ISE scheme proposed in [20].

Here, we summarize the contributions of all UL-based attack detection schemes in Tab. 10.

Table 10: The UL-based Attack Detection Schemes

Models	Ref.	Year	Major Contribution
Clustering	[20]	2021	Study the correlation of multi-fingerprints and propose an authentication architecture based on non-parametric clustering algorithms, and propose an improved system evolution method based on the evolution algorithm [241].
	[239]	2013	Leverage clustering algorithms to determine the number of attackers, and further demonstrate its effectiveness under two real office buildings with WiFi networks and ZigBee networks.
	[242]	2018	Combine DNN and K-means to propose CRNN to learn to local features and the dependencies between different frequencies in CSI fingerprints.
OCC-SVM	[148]	2022	Design a lightweight PLA scheme based on OCC-SVM and antenna diversity technique, and further demonstrate its advantages than the baseline schemes proposed by [223, 245] for SRSs.
	[243]	2022	Introduce an SCC-SVM-based PLA solution for LEO satellite scenarios.
	[244]	2021	Consider two classes of SVM classifiers, including TC-SVM and SC-SVM, and further evaluate the performance over different choices of kernel functions, fingerprints, and the attackers' power.
	[245]	2021	Evaluate and compare two different statistical decision methods, and further propose two ML-based PLA schemes based on nearest neighbor and SVM.
Manifold Learning	[154]	2022	Consider the time-varying characteristics of fingerprints caused by the mobility of UAVs and formulate the authentication problem as the recognition of nonlinearly separable data, and further use manifold learning to establish the Markov chains to address this issue.
GMM	[155]	2013	Use GMM models to formulate the probabilistic model of radio channels of transmitters and realize online learning and parameter updating.
	[246]	2017	Design a GMM-based method to defend against data manipulation and masquerade attacks for MC-MTC scenarios.

Models	Ref.	Year	Major Contribution
GP	[247]	2018	Present a PLA method based on pre-processing channel variations and multi-dimensional fingerprints to realize high robustness to the errors of channel estimation.
	[156]	2022	Provide a PLA scheme based on GP channel prediction for IoT devices and propose an OCA scheme without knowing channel information of attackers, and further compare its performance with the schemes proposed by [141] and [248].
	[247]	2018	Develop a GP-based PLA scheme to track multi-targets and reduce the authentication overhead for dynamic channels.
AE	[157]	2023	Suggest an HVAE-based scheme to defend against spoofing attacks in IIoT, and further derive the loss function consisting the AE module and the VAE module with a single-peak and a revised double-peak Gaussian distribution.

Lesson 9. *Compared with the SL-based schemes, the UL-based attack detection schemes do not require the prior information or training fingerprint samples of attackers, thus having more universality in actual applications. The UL-based schemes have been studied for ZigBee networks [239], industrial networks [20, 157], UAVs [154], LEO satellite scenarios [243], MC-MTC scenarios [246], and IoT [156]. Compared with the non-DL-aided UL models, including clustering algorithms, manifold learning, and GMM algorithms, AEs can extract features of fingerprints with higher dimensions and are more suitable for future Massive MIMO-enabled scenarios.*

4.3. RL-based Attack Detection

Compared with the SL and UL techniques, RL techniques do not require accurate input and precise parameter updates. As illustrated in Fig. 9, the reward obtained by the agent through the interactions with the environments guides the behavior, and the goal is that the agent can obtain the maximum reward. We classify the RL techniques into non-DL-aided RL and DRL, and the latter combines the perception ability of DL and the decision ability of RL.

4.3.1. Non-DL-Aided RL
- *Effectiveness of RL Methods:* Xiao et al. [27] formulate the interactions between the legal receiver and spoofing attackers as a zero-sum

game and propose a spoofing detection method based on Q-learning and Dyna-Q. The receiver chooses the threshold based on the Bayesian risk, while the attackers determine the spoofing frequency to minimize the utility of the legal receiver. The optimal threshold is obtained through the designed RL method. The simulations on USRPs validate the feasibility of the proposed strategies.

- *Intelligent Attacks:* Gao et al. [158] study the PLA in the threat of intelligent spoofing attacks. The optimal transmit power allocation is derived, and the optimal intelligent attack for legitimate devices is found. A cooperative PLA scheme is further proposed to defend against the above-mentioned attacks with low time complexity and high accuracy. The closed-form expression for the belief threshold is also provided. The simulation results verify the superiority of the proposed scheme than the schemes proposed by [142, 150, 249].

- *Authentication under underwater acoustic sensor networks:* Li et al. [250] formulate the interaction between the surface station and the underwater spoofers in underwater acoustic sensor networks as a zero-sum game, and further derive the Nash equilibrium. The existing condition for the unique Nash equilibrium is also presented.

- *Authentication under MIMO systems:* Xiao et al. [36] propose a Q-learning-based PLA scheme to detect spoofing attackers in MIMO systems. The optimal threshold can be obtained without knowing system parameters. The Dyna architecture and prioritized sweeping is further applied to improve the detection accuracy during time-varying channels. The simulation results show that the proposed scheme can improve detection performance compared with Q-learning algorithm.

- *Authentication under UAVs:* Zhou et al. [251] provide a PLA scheme based on RL and RSS for UAVs. The false alarm rate and miss detection rate are derived, and the Nash equilibrium and its existence condition for the designed zero-sum authentication game are further presented. The Monte Carlo simulation results demonstrate the analytical expressions.

- *Collaborator Selection:* Zhang et al. [252] propose a FL-based cooperative PLA scheme, and further employ Q-learning algorithm to select

69

the optimal collaborator. The simulation analysis and real-world communication experiments verify the superiority than blind cooperation.

4.3.2. DRL

- *Authentication under VANETs:* Lu et al. [159] propose a DRL-based PLA scheme to defend against rogue edge attackers in VANETs. The channel information is shared for the mobile devices and onboard unit with the same moving trace, and RL is utilized to choose authentication modes and parameters. Transfer learning and DL are applied to improve efficiency and further improve authentication performance, respectively. The simulation and experimental results show that the proposed scheme can improve detection accuracy compared with the baseline schemes proposed in [29, 253, 254].

- *Authentication under IoT Scenarios:* Wu et al. [160] consider three cases in static channels: including multi-player games, zero-sum games with collisions, and zero-sum games without collisions, and further derive the closed-form expressions for Nash equilibrium. A multi-agent deep deterministic policy gradient algorithm is further proposed for dynamic environments. The simulation experiments prove that the proposed PLA schemes are feasible for IoT scenarios.

- *Authentication under UWSNs:* Xiao et al. [255] present a PLA framework to detect spoofing attackers for UWSNs. The power delay profile of underwater acoustic channels is utilized to recognize sensors, and RL is applied to choose the parameters of authentication systems. DRL is further utilized to improve the authentication accuracy. The simulation results indicate that the proposed scheme increase the utility of the system compared with the benchmark scheme proposed in [250].

Here, we summarize the contributions of all RL-based attack detection schemes in Tab. 11.

Table 11: The RL-based Attack Detection Schemes

Models	Ref.	Year	Major Contribution
Non-DL-Aided RL	[27]	2016	Formulate the interactions between the legal receiver and spoofing attackers as a zero-sum game and propose a spoofing attack method based on Q-learning and Dyna-Q.
	[36]	2017	Propose a Q-learning-based scheme to detect spoofing attackers in MIMO systems, and further apply Dyna-PS algorithm to improve the detection accuracy during time-varying channels.
	[158]	2020	Study the PLA in the threat of intelligent spoofing attacks, and provide comprehensive theoretical deduction, including the optimal transmit power allocation, the optimal intelligent attack, and the belief threshold.
	[250]	2015	Suggest a Q-learning-based attack detection scheme for UWSNs, and derive the Nash equilibrium and existing condition.
	[251]	2022	Provide a PLA scheme based on RL and RSS for UAVs, and derive the false alarm rate and miss detection rate.
	[252]	2023	Employ Q-learning algorithm to select the optimal authentication collaborator.
DRL	[159]	2020	Present a DRL-based PLA scheme to detect rogue edge attackers in VANETs, and demonstrate its superiority in attack detection by the comparison with the baseline schemes proposed by [27, 253, 254].
	[160]	2023	Consider three cases in static channels, including multi-player games, zero-sum games with collisions, and zero-sum games without collisions, and further propose an MADDPG-based scheme for dynamic environments.
	[255]	2019	Develop a RL-based PLA scheme to detect spoofing attackers for UWSNs and further utilize DRL to improve the authentication accuracy, and further verify its superiority than the benchmark scheme proposed by [250].

Lesson 10. *The RL-based attack detection schemes usually formulate the game between the legitimate receiver and spoofing attackers and have been studied for USWSNs [250, 255], MIMO systems [36], UAVs [251], VANETs [159], and IoT [160] as well as have been combined with other techniques to*

obtain higher accuracy and efficiency, such as TL [159] and DL [159, 160, 255]. The intelligent spoofing attacks [158] have also been studied, including the derivations of the optimal transmit power allocation and the optimal intelligent attack for legitimate devices as well as the closed-form expression for the belief threshold.

5. Fingerprint Datasets

The open-source, high-quality, and large-scale fingerprint datasets are indispensable parts of promoting the development of the ML-based PLA. In this section, we sort out and summarize various open-source fingerprint datasets in detail, aiming at proving researchers with comprehensive knowledge for further application of the PLA.

5.1. RF Fingerprint Datasets

In earlier literature, the DL-based multi-device identification methods obtain high accuracy for small-scale devices under LOS environments. However, it is challenging to extend the identification models learned based on small-scale devices under LOS environments to large-scale devices under NLoS environments. Jian et al. [34] confirm that different environmental scenarios affect the identification accuracy, including channel conditions, SNR, number of devices, and training dataset size. Hence, the construction of RF fingerprints should consider multi-factors, including:

- *NLOS Environments:* The authors of [195] and [256] consider the NLOS environments under indoor and outdoor scenarios, respectively.

- *Large-Scale Devices:* Liu et al. [168] use the USRP B210 to collect the ADS-B signals from 140 aircraft at Daytona Beach international airport. Shen et al. [195] use the USRP N210 to collect signals from 60 commercial off-the-shelf LoRa devices. Uzundurukan et al. [257] employ a high sampling rate oscilloscope (Tektronix TDS7404) to record Bluetooth signals from 86 smartphones. Ya et al. [258] utilize the Signal Hound SM200B to record 530 categories of long signals and 198 categories of short signals. Hanna et al. [259] use the USRP B210/N210/X310 to collect WiFi signals from 174 devices.

- *Multi-Receivers:* The authors of [259] and [260] employ 41 receivers, enabling Verification of collaborative authentication.

- *Long Acquisition Time:* The acquisition time of [133], [259], and [260] is 10 days, 4 days, and 5 days, respectively.

- *Noisy Channel Environments:* Morin et al. [261] consider the dynamic channels interfered by mobile robots.

- *A Large Number of Fingerprint Samples:* The authors of [64], [256], and [260] collect 2e7, 3e6, and 2e8 I/Q samples/individual, respectively.

Here, we provide the list of the open-source fingerprint datasets with the number and type of transmitters, waveform, type of receiver, and frequency in Tab. 12.

Table 12: The Summarization of Open-Source RF Fingerprint Datasets

Ref.	Number of Trans-mitters	Type of Transmitters	Waveform	Type of Receiver	Frequency
[64]	16	USRP X310	IEEE 802.11a	USRP B210	2.45 GHz
[133]	20	USRP X310/N210	IEEE 802.11a/g	USRP N210	2.432 GHz
[168]	140	Aircraft	ADS-B	USRP B210	1090 MHz
[195]	60	Commercial LoRa devices	LoRa	USRP N210	868.1 MHz
[256]	4	USRP X310	IEEE 802.11a/LTE/5G NR	USRP B210	1.6 GHz ∼6 GHz
[257]	86	Smartphones	Bluetooth	Tektronix TDS7404	2.4 GHz
[258]	728	Aircraft	ADS-B	Signal Hound SM200B	1090 MHz
[259]	174	WiFi transmitters	IEEE 802.11a/g	USRP B210/N210/X310	2462 MHz
[260]	25	Pycom devices	LoRa	USRP B210	915 MHz
[261]	21	USRP N2932	IEEE 802.15.4	USRP N2932	400 MHz ∼4 GHz
[262]	17	Drone remote controllers (RCs)	Non-standard waveforms	Keysight MSOS604A oscilloscope	2.4 GHz
[263]	7	DJI M100	Non-Standard	USRP X310	5 GHz

5.2. Channel Fingerprint Datasets

5.2.1. Provided by Official Organizations

- *Industrial Datasets:* The National Institute of Standards and Technology (NIST) [264] provide the CIR measurements collected in an outdoor facility with minimal interference from unexpected emitters and three indoor industrial facilities, including the automotive factory with large tracts of open areas, the steam generation plant with large machinery and overhead obstructions, and the machine shop with small space. The recorded CIRs are complex vectors of 8188 dimensions and contain rich channel information. The authors of [20, 88, 120, 149, 157, 202, 224] have utilized the dataset to verify the performance of proposed ML-based PLA schemes.

- *Generated based on real-world scenes from 40 Big Cities:* The China Academy of Information and Communications Technology (CAICT) provides the open-source dataset that can support a variety of wireless AI tasks [265], including sensing tasks such as location environmental reconstruction, MIMO tasks such as RIS and beam, and physical-layer tasks such as CSI feedback and channel estimation. The parameters can be customized to meet the needs of researchers.

5.2.2. Provided by Individuals

- *4G LTE:* Jaeckel et al. [266] extend the Wireless World Initiative for New Radio (WINNER) channel model to realize better trade off between complexity and accuracy. The proposed open-source model enables 3-D propagation, 3-D antenna patterns, scenario transitions, and variable terminal speeds. Gassner et al. [267] present the first CSI-based radio map obtained by automated tools for LTE radio links.

- *MIMO:* To reproduce the stochastic properties of MIMO channels over time, frequency, and space, Liu et al. [268] provide the COST 2100 channel model, a stochastic channel model based on geometry. The COST 2100 channel is suitable for multi-user and distributed MIMO scenarios.

- *Massive MIMO:* Alkhateeb et al. [269] introduce the DeepMIMO dataset to advance the research of Massive MIMO and mmWave techniques. The dataset can be completely defined by the set of parameters.

- *WiFi:* Wang et al. [270] collect the CSI data in complex indoor environments at Colorado State University.

- *5G NR:* By considering the clustered delay line channel model [271] that is suitable for link-level and system-level simulations, Zhang et al. [272] develop a generalized 5G NR dataset generator.

- *Reconfigurable Intelligent Surface (RIS):* Basar et al. [273] consider the characteristics of the Reconfigurable Intelligent Surface (RIS), such as LOS probability, shadowing effects, shared clusters, and array responses, and further develop the SimRIS channel Simulator MATLAB package for the channel modeling of RIS-aided systems.

- *Outdoor Environments:* Alrabeiah et al. [274] study the vision-aided wireless communications and provide the parametric, systematic, and scalable vision-wireless dataset framework. The high-fidelity synthetic wireless and visual data samples for the same scene can be generated through the advanced 3D modeling and ray tracing software.

- *Underwater Scenarios:* Qarabaqi et al. [275] provide the underwater acoustic channel model, where the small-scale and large-scale effects are considered.

Here, we provide the list of the open-source channel datasets with the provider, environment, and descriptions in Tab. 13.

Table 13: The Summarization of Open-Source Channel Fingerprint Datasets

Ref.	Provider	Environment	Description
[264]	NIST	Industrial scenarios	The CIR measurements are collected under an outdoor environment and three typical industrial scenarios, including automotive factory, steam generation plant, and machine shop.
[265]	CAICT	City scenarios	The dataset is generated based on real map scenes, including more than 1,000 scenes randomly selected from more than 40 big cities around the world.

Ref.	Provider	Environment	Description
[266]	Individual	LTE	Provide a more realistic channel model that is extended from the popular WINNER channel model. The presented channel model can realize better trade-off between complexity and accuracy.
[267]		LTE	Utilize USRP B200mini and a wheeled robot to record the CSI periodically.
[268]		MIMO	Propose a geometry-based stochastic channel model to reproduce the stochastic characteristics of MIMO channels over time, frequency, and space.
[269]		Massive MIMO	Present a generic Massive MIMO dataset based on ray-tracing data obtained from Remcom Wireless InSite [265] for mmWave frequencies.
[270]		WiFi	provide a CSI dataset collected in complex indoor environments at Colorado State University.
[272]		5G NR	Suggest a generalized channel dataset generator for 5G NR systems. The setting of different channel parameters and the generation of massive MIMO channels can be achieved.
[273]		RIS, 5G	Develop an accurate, open-source, and widely applicable RIS channel model for mmWave frequencies. Both indoor and outdoor environments are included. The 5G radio channel conditions are also considered.
[274]		Outdoor	The ViWi dataset framework is a parametric, systematic, and scalable data generation architecture. The high-fidelity synthetic wireless and vision data samples for the same scenes can be generated.
[275]		Underwater	Present an open-source underwater acoustic channel model that incorporates physical laws of acoustic propagation and the effects of inevitable random local displacements.

6. Challenges and Future Research Directions

6.1. CVNN for CSI Fingerprints

For MIMO and Massive MIMO systems, CSI fingerprints contain abundant spatial information of the channels between transmitters and receivers.

A widely-used approach is to exploit CNNs to extract the inherent characteristics of CSI fingerprints: converting the CSIs into pictures with the dimensions of $N_R N_T \times 2$, where N_R and N_T respectively represent the number of antennas of the receiver and the transmitter and "2" indicates the real and imaginary parts. Hence, the complex CSIs are split into real and imaginary parts corresponding to different channels of CNNs, respectively. Considering that CNNs can not process complex data, they may not fully extract the complex features of MIMO channels, limiting the performance of the CSI-based PLA. Moreover, the future 6G systems are expected to support ultra-massive MIMO scenarios [276], where CSIs contain richer spatial features. Hence, how to effectively exploit CSI fingerprints to realize attack detection is an important issue.

To tackle this problem, one feasible solution is to exploit CVNNs, which can directly process complex signals. The higher computing complexity and more model parameters introduced by CVNNs can be addressed by network compression techniques.

6.2. RIS-aided PLA

Meng et al. [277] propose a RIS-aided PLA architecture, where the configurable fingerprints can be obtained in NLoS environments. When the direct links between the transmitter and receiver are blocked, such design can enhance the robustness and reliability of fingerprints by creating alternative propagation paths. Meng et al. [277] also verify that the parameters of RIS, such as number, magnitude, and phase response, influence the authentication performance. However, there are some issues to be addressed as follows: (1) How to derive the closed-form expression of false alarm rate and miss detection rate when the channel models are determined? (2) How to optimize the parameters of IRSs to obtain the optimal authentication performance?

6.3. Game Between Legitimate Transmitters and Attackers

Most state-of-the-art RL-based attack detection schemes primarily focus on the interaction between legitimate receivers and spoofing attackers, as demonstrated in [27, 250, 251]. However, effective defense strategies must also consider the role of trusted transmitters. Therefore, the game between legitimate transmitters and attackers represents a significant and valuable research direction.

For instance, envisioning an adversarial scenario involving multiple legitimate transmitters and spoofing attackers, a strategy emerges where legitimate transmitters nominate a representative to transmit authorized signals, aiming to minimize overall communication overhead. Simultaneously, attackers select representatives to transmit spoofing signals, attempting to evade detection by the legitimate receiver. The differing spatial locations of legitimate transmitters and attackers result in distinct location-specific channel fingerprints, influencing the similarity between them. This spatial discrepancy engenders a strategic game in the selection of representatives by both legal and illegal entities.

6.4. Defense Against Multiple Cooperative Attackers

Most of the state-of-the-art attack detection schemes study the defense against a single attacker, while a few schemes are designed against multi-attackers, such as [27, 239, 162]. The cooperation of multi-attackers is further studied in [27]. Each spoofer can choose its attack frequency to maximize its utility, and multi-attackers cooperatively transmit spoofing signals to avoid collisions. The cooperation of multi-attackers is worth studying because it poses a more serious security threat to the communication system.

6.5. Cross-Layer Authentication

Although ML-based PLA can obtain high authentication performance, the PLA methods are not designed to replace the upper-layers authentication mechanisms. On the contrary, the PLA methods are provided to compensate for the upper-layers authentication mechanisms [40]. Hence, how to design a secure cross-layer authentication scheme or combine them effectively is an urgent problem. For example, Zhang et al. [222] propose a lightweight cross-layer authentication for dynamic channel environments. The upper-layers authentication mechanisms help to update the parameters of the PLA model.

6.6. ML for Key-based PLA

The PLS technique includes key-based PLA, keyless PLA, and other security methods. Compared with the keyless schemes summarized in this paper, the key-based schemes utilize the channel reciprocity to generate keys between Alice and Bob. The channel reciprocity means that the same channel features can be observed at both ends of the same channel link. However,

the uplink and downlink are in different frequency bands for frequency division duplexing (FDD) systems. Therefore, most of the key-based schemes designed for time division duplexing (TDD) systems are not suitable for FDD systems. On the other hand, FDD systems dominate existing cellular communications, such as narrowband IoT and 4G LTE. Hence, finding reciprocal channel characteristics in FDD systems is strongly desirable for the key-based PLA.

To address this issue, one promising method is to leverage ML techniques, especially DL techniques, to construct the reciprocal characteristics. For example, Zhang et al. [278] propose a DL-based channel prediction framework to realize the estimation of features of one frequency band without any loopback.

6.7. Interpretability of DL-Aided PLA

Although DL-based PLA schemes can achieve high identification and detection accuracy, their interpretability is often inferior to that of traditional methods. Researchers frequently face difficulties in understanding the connections between the features extracted by DNNs and their prediction outcomes, a challenge commonly referred to as the "black-box problem" of DL technology. Therefore, it is crucial to develop DL-aided PLA schemes that are both secure and interpretable.

To solve the problem, Meng et al. [120] define the Fingerprint Library and provide the post-hoc explanations to answer the following question: which library examples explain the authentication results issued for a given fingerprint sample?

6.8. Generative Large Model-Empowered PLA

The generative large model excels in creating channel fingerprints and RF fingerprints due to its robust characterization and automatic feature extraction capabilities. By leveraging multi-level data abstraction, the model can effectively capture and depict the various nuances and fluctuations within wireless channels, resulting in the generation of fingerprint data with significant identification and utilitarian value. Nonetheless, it is vital to acknowledge the considerations surrounding the expenses associated with data acquisition, the intricate training demands of the model, and the necessity for robust fingerprints when implementing the technology in practical settings.

7. Conclusion

This article has provided a comprehensive survey of the ML-based PLA in wireless communications. We have categorized the existing ML-based PLA schemes into two categories: multi-device identification and attack detection schemes. The former one, a multi-classification problem, aims to recognize which transmitter in the fingerprint database matches the received signal and is usually based on RF fingerprints. The latter one, a hypothesis testing problem, aims to identify the forged signal and is usually based on channel fingerprints. Moreover, we divided the DL-based multi-device identification schemes into several sub-categories: FCNN-based, CNN-based, RNN-based, Attention mechanism-based, data augmentation-based, CVNN-based, GAN-based, and AE-based schemes. We divide the ML-based attack detection schemes into three sub-categories: SL-based, UL-based, and RL-based schemes. We further summarized the open-source RF fingerprint and channel fingerprint datasets for researchers in related fields. At last, we concluded this paper with some recommendations and future research directions.

8. Acknowledgements

9. CRediT authorship contribution statement

Rui Meng: investigation, methodology, and writing. **Bingxuan Xu:** investigation and writing (polish figures and tables). **Xiaodong Xu:** writing (review and editing), funding acquisition, and supervision. **Mengying Sun:** writing (review and editing). **Bizhu Wang:** writing (review and editing). **Shujun Han** writing (review and editing). **Suyu Lv** writing (review and editing). **Ping Zhang:** funding acquisition and supervision.

10. Data availability

No data was used for the research described in the article.

References

[1] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, et al., On the road to 6g: Visions, requirements, key technologies and testbeds, IEEE Communications Surveys & Tutorials 25 (2) (2023) 905–974.

[2] L. Jin, X. Hu, Y. Lou, Z. Zhong, X. Sun, H. Wang, J. Wu, Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions, China Communications 18 (9) (2021) 88–99.

[3] J. Moon, S. H. Lee, H. Lee, I. Lee, Proactive eavesdropping with jamming and eavesdropping mode selection, IEEE Transactions on Wireless Communications 18 (7) (2019) 3726–3738.

[4] N. Li, S. Xia, X. Tao, Z. Zhang, X. Wang, An area based physical layer authentication framework to detect spoofing attacks, Science China Information Sciences 63 (2020) 1–14.

[5] H. Tan, Z. Li, N. Xie, J. Lu, D. Niyato, Detection of jamming attacks for the physical-layer authentication, IEEE Transactions on Wireless Communications 22 (12) (2023) 9579–9594.

[6] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang, Y. Lu, Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks, IEEE Transactions on Industrial Informatics 17 (3) (2020) 2041–2051.

[7] M. H. Junejo, A. A.-H. Ab Rahman, R. A. Shaikh, K. Mohamad Yusof, I. Memon, H. Fazal, D. Kumar, A privacy-preserving attack-resistant trust model for internet of vehicles ad hoc networks, Scientific Programming 2020 (1) (2020) 8831611.

[8] M. H. Junejo, A. A.-H. Ab Rahman, R. A. Shaikh, K. M. Yusof, D. Kumar, I. Memon, Lightweight trust model with machine learning scheme for secure privacy in vanet, Procedia Computer Science 194 (2021) 45–59.

[9] I. Memon, A secure and efficient communication scheme with authenticated key establishment protocol for road networks, Wireless Personal Communications 85 (3) (2015) 1167–1191.

[10] A. A. Ahmed, M. K. Hasan, I. Memon, A. H. M. Aman, S. Islam, T. R. Gadekallu, S. A. Memon, Secure ai for 6g mobile devices: Deep learning optimization against side-channel attacks, IEEE Transactions on Consumer Electronics (2024).

[11] 3GPP, Security architecture and procedures for 5g system, version 17.0.0 (2020).

[12] N. Xie, W. Xiong, J. Chen, P. Zhang, L. Huang, J. Su, Multiple phase noises physical-layer authentication, IEEE Transactions on Communications 70 (9) (2022) 6196–6211.

[13] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[14] S. Sharma, B. Kaushik, A survey on internet of vehicles: Applications, security issues & solutions, Vehicular Communications 20 (2019) 100182.

[15] G. Oligeri, S. Sciancalepore, S. Raponi, R. Di Pietro, Past-ai: Physical-layer authentication of satellite transmitters via deep learning, IEEE Transactions on Information Forensics and Security 18 (2022) 274–289.

[16] H. Fang, X. Wang, N. Zhao, N. Al-Dhahir, Lightweight continuous authentication via intelligently arranged pseudo-random access in 5g-and-beyond, IEEE Transactions on Communications 69 (6) (2021) 4011–4023.

[17] H. Fang, X. Wang, L. Hanzo, Learning-aided physical layer authentication as an intelligent process, IEEE Transactions on Communications 67 (3) (2018) 2260–2273.

[18] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang, Z. Ye, Global Health Journal 3 (3) (2019) 62–65.

[19] S. Yin, J. J. Rodriguez-Andina, Y. Jiang, Real-time monitoring and control of industrial cyberphysical systems: With integrated plant-wide monitoring and control framework, IEEE Industrial Electronics Magazine 13 (4) (2019) 38–47.

[20] S. Xia, X. Tao, N. Li, S. Wang, T. Sui, H. Wu, J. Xu, Z. Han, Multiple correlated attributes based physical layer authentication in wireless networks, IEEE Transactions on Vehicular Technology 70 (2) (2021) 1673–1687.

[21] D. Li, X. Yang, F. Zhou, D. Wang, N. Al-Dhahir, Blind physical-layer authentication based on composite radio sample characteristics, IEEE Transactions on Communications 70 (10) (2022) 6790–6803.

[22] X. Wang, P. Hao, L. Hanzo, Physical-layer authentication for wireless security enhancement: Current challenges and future developments, IEEE Communications Magazine 54 (6) (2016) 152–158.

[23] N. Xie, H. Tan, L. Huang, A. X. Liu, Physical-layer authentication in wirelessly powered communication networks, IEEE/ACM Transactions on Networking 29 (4) (2021) 1827–1840.

[24] H. Forssell, R. Thobaben, Worst-case detection performance for distributed simo physical layer authentication, IEEE Transactions on Communications 70 (1) (2021) 485–499.

[25] N. Xie, J. Chen, L. Huang, Physical-layer authentication using multiple channel-based features, IEEE transactions on information forensics and security 16 (2021) 2356–2366.

[26] L. Xiao, L. J. Greenstein, N. B. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels, IEEE Transactions on Wireless Communications 7 (7) (2008) 2571–2579.

[27] L. Xiao, Y. Li, G. Han, G. Liu, W. Zhuang, Phy-layer spoofing detection with reinforcement learning in wireless networks, IEEE Transactions on Vehicular Technology 65 (12) (2016) 10037–10047.

[28] H. Fang, X. Wang, S. Tomasin, Machine learning for intelligent authentication in 5g and beyond wireless networks, IEEE Wireless Communications 26 (5) (2019) 55–61.

[29] S. Riyaz, K. Sankhe, S. Ioannidis, K. Chowdhury, Deep learning convolutional neural networks for radio identification, IEEE Communications Magazine 56 (9) (2018) 146–152.

[30] G. Shen, J. Zhang, A. Marshall, L. Peng, X. Wang, Radio frequency fingerprint identification for lora using deep learning, IEEE Journal on Selected Areas in Communications 39 (8) (2021) 2604–2616.

[31] N. Yang, B. Zhang, G. Ding, Y. Wei, G. Wei, J. Wang, D. Guo, Specific emitter identification with limited samples: A model-agnostic meta-learning approach, IEEE Communications Letters 26 (2) (2021) 345–349.

[32] C. Xiang, W. Liandong, X. Xiong, S. Xujian, F. Yuntian, A review of radio frequency fingerprinting methods based on raw i/q and deep learning, Journal of Radars 12 (1) (2022) 214–234.

[33] S. Chen, S. Zheng, L. Yang, X. Yang, Deep learning for large-scale real-world acars and ads-b radio signal classification, IEEE Access 7 (2019) 89256–89264.

[34] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, S. Ioannidis, Deep learning for rf fingerprinting: A massive experimental study, IEEE Internet of Things Magazine 3 (1) (2020) 50–57.

[35] T. D. Vo-Huu, T. D. Vo-Huu, G. Noubir, Fingerprinting wi-fi devices using software defined radios, in: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2016, pp. 3–14.

[36] L. Xiao, T. Chen, G. Han, W. Zhuang, L. Sun, Game theoretic study on channel-based authentication in mimo systems, IEEE Transactions on Vehicular Technology 66 (8) (2017) 7474–7484.

[37] A. Mukherjee, S. A. A. Fakoorian, J. Huang, A. L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Communications Surveys & Tutorials 16 (3) (2014) 1550–1573.

[38] Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Communications Surveys & Tutorials 19 (1) (2016) 347–376.

[39] L. Bai, L. Zhu, J. Liu, J. Choi, W. Zhang, Physical layer authentication in wireless communication networks: A survey, Journal of Communications and Information Networks 5 (3) (2020) 237–264.

[40] N. Xie, Z. Li, H. Tan, A survey of physical-layer authentication in wireless communications, IEEE Communications Surveys & Tutorials 23 (1) (2020) 282–310.

[41] P. Angueira, I. Val, J. Montalban, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, A. Arriola, A survey of physical layer techniques for secure wireless communications in industry, IEEE Communications Surveys & Tutorials 24 (2) (2022) 810–838.

[42] Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities, IEEE Communications Surveys & Tutorials 18 (1) (2015) 94–104.

[43] X. Fan, F. Wang, F. Wang, W. Gong, J. Liu, When rfid meets deep learning: Exploring cognitive intelligence for activity identification, IEEE wireless Communications 26 (3) (2019) 19–25.

[44] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, K. Chowdhury, More is better: Data augmentation for channel-resilient rf fingerprinting, IEEE Communications Magazine 58 (10) (2020) 66–72.

[45] W. Lee, S. Y. Baek, S. H. Kim, Deep-learning-aided rf fingerprinting for nfc security, IEEE Communications Magazine 59 (5) (2021) 96–101.

[46] A. Jagannath, J. Jagannath, P. S. P. V. Kumar, A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges, Computer Networks 219 (2022) 109455.

[47] Y. Liu, J. Wang, J. Li, S. Niu, H. Song, Machine learning for the detection and identification of internet of things devices: A survey, IEEE Internet of Things Journal 9 (1) (2021) 298–320.

[48] B. Hamdaoui, A. Elmaghbub, Deep-learning-based device fingerprinting for increased lora-iot security: Sensitivity to network deployment changes, IEEE network 36 (3) (2022) 204–210.

[49] H. C. Choe, C. E. Poole, M. Y. Andrea, H. H. Szu, Novel identification of intercepted signals from unknown radio transmitters, in: Wavelet Applications II, Vol. 2491, SPIE, 1995, pp. 504–517.

[50] J. Toonstra, W. Kinsner, A radio transmitter fingerprinting system odo-1, in: Proceedings of 1996 Canadian Conference on Electrical and Computer Engineering, Vol. 1, IEEE, 1996, pp. 60–63.

[51] J. Hall, M. Barbeau, E. Kranakis, et al., Enhancing intrusion detection in wireless networks using radio frequency fingerprinting., Communications, internet, and information technology 1 (2004).

[52] Ö. Tekbaş, O. Üreten, N. Serinken, Improvement of transmitter identification system for low snr transients, Electronics Letters 40 (3) (2004) 182–183.

[53] W. C. Suski II, M. A. Temple, M. J. Mendenhall, R. F. Mills, Using spectral fingerprints to improve wireless network security, in: IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, IEEE, 2008, pp. 1–5.

[54] W. Hou, X. Wang, J.-Y. Chouinard, A. Refaey, Physical layer authentication for mobile systems with time-varying carrier frequency offsets, IEEE Transactions on Communications 62 (5) (2014) 1658–1667.

[55] D. B. Faria, D. R. Cheriton, Detecting identity-based attacks in wireless networks using signalprints, in: Proceedings of the 5th ACM workshop on Wireless security, 2006, pp. 43–52.

[56] C. K. Dubendorfer, B. W. Ramsey, M. A. Temple, An rf-dna verification process for zigbee networks, in: MILCOM 2012-2012 IEEE Military Communications Conference, IEEE, 2012, pp. 1–6.

[57] D. R. Reising, M. A. Temple, Wimax mobile subscriber verification using gabor-based rf-dna fingerprints, in: 2012 IEEE International Conference on Communications (ICC), IEEE, 2012, pp. 1005–1010.

[58] O. Ureten, N. Serinken, Wireless security through rf fingerprinting, Canadian Journal of Electrical and Computer Engineering 32 (1) (2007) 27–33.

[59] B. Chatterjee, D. Das, S. Maity, S. Sen, Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning, IEEE internet of things journal 6 (1) (2018) 388–398.

[60] W. Zhang, W. Zhao, X. Tan, L. Shao, C. Ran, Adaptive rf fingerprints fusion via dual attention convolutions, IEEE Internet of Things Journal 9 (24) (2022) 25181–25195.

[61] G. Reus-Muns, K. R. Chowdhury, Classifying uavs with proprietary waveforms via preamble feature extraction and federated learning, IEEE Transactions on Vehicular Technology 70 (7) (2021) 6279–6290.

[62] P. Hao, X. Wang, A. Behnad, Performance enhancement of i/q imbalance based wireless device authentication through collaboration of multiple receivers, in: 2014 IEEE International Conference on Communications (ICC), IEEE, 2014, pp. 939–944.

[63] P. Hao, X. Wang, A. Behnad, Relay authentication by exploiting i/q imbalance in amplify-and-forward system, in: 2014 IEEE Global Communications Conference, IEEE, 2014, pp. 613–618.

[64] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, K. Chowdhury, Oracle: Optimized radio classification through convolutional neural networks, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, 2019, pp. 370–378.

[65] W. Hou, X. Wang, J.-Y. Chouinard, Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates, in: 2012 IEEE International Conference on Communications (ICC), IEEE, 2012, pp. 3559–3563.

[66] S. Zeng, X. Li, A. Salem, D. Zhao, Physical layer authentication based on cfo and visibility graph, in: 2018 International Conference on Networking and Network Applications (NaNA), IEEE, 2018, pp. 147–152.

[67] T. Kohno, A. Broido, K. C. Claffy, Remote physical device fingerprinting, IEEE Transactions on Dependable and Secure Computing 2 (2) (2005) 93–108.

[68] S. Jana, S. K. Kasera, On fast and accurate detection of unauthorized wireless access points using clock skews, in: Proceedings of the 14th

ACM international conference on Mobile computing and networking, 2008, pp. 104–115.

[69] M. Cristea, B. Groza, Fingerprinting smartphones remotely via icmp timestamps, IEEE Communications Letters 17 (6) (2013) 1081–1083.

[70] A. Pitarokoilis, E. Björnson, E. G. Larsson, Ml detection in phase noise impaired simo channels with uplink training, IEEE Transactions on communications 64 (1) (2015) 223–235.

[71] C. Zhao, M. Huang, L. Huang, X. Du, M. Guizani, A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks, Computer networks 128 (2017) 164–171.

[72] S. Dolatshahi, A. Polak, D. L. Goeckel, Identification of wireless users via power amplifier imperfections, in: 2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers, IEEE, 2010, pp. 1553–1557.

[73] A. C. Polak, S. Dolatshahi, D. L. Goeckel, Identifying wireless users via transmitter imperfections, IEEE Journal on selected areas in communications 29 (7) (2011) 1469–1479.

[74] A. C. Polak, D. L. Goeckel, Identification of wireless devices of users who actively fake their rf fingerprints with artificial data distortion, IEEE Transactions on Wireless Communications 14 (11) (2015) 5889–5899.

[75] A. Varshavsky, A. Scannell, A. LaMarca, E. De Lara, Amigo: Proximity-based authentication of mobile devices, in: International Conference on Ubiquitous Computing, Springer, 2007, pp. 253–270.

[76] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, A. LaMarca, Ensemble: cooperative proximity-based authentication, in: Proceedings of the 8th international conference on Mobile systems, applications, and services, 2010, pp. 331–344.

[77] S. Zhong, L. Li, Y. G. Liu, Y. R. Yang, Privacy-preserving location-based services for mobile users in wireless networks, Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297 26 (2004).

[78] M. Demirbas, Y. Song, An rssi-based scheme for sybil attack detection in wireless sensor networks, in: 2006 International symposium on a world of wireless, mobile and multimedia networks (WoWMoM'06), ieee, 2006, pp. 564–570.

[79] D. Xu, P. Ren, J. A. Ritcey, Independence-checking coding for ofdm channel training authentication: Protocol design, security, stability, and tradeoff analysis, IEEE transactions on information forensics and security 14 (2) (2018) 387–402.

[80] A. Abdelaziz, R. Burton, F. Barickman, J. Martin, J. Weston, C. E. Koksal, Enhanced authentication based on angle of signal arrivals, IEEE Transactions on Vehicular Technology 68 (5) (2019) 4602–4614.

[81] C. L. Corbett, R. A. Beyah, J. A. Copeland, Passive classification of wireless nics during rate switching, EURASIP Journal on Wireless Communications and Networking 2008 (2007) 1–12.

[82] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, T. W. Rondeau, Radio transmitter fingerprinting: A steady state frequency domain approach, in: 2008 IEEE 68th Vehicular Technology Conference, IEEE, 2008, pp. 1–5.

[83] M. D. Williams, S. A. Munns, M. A. Temple, M. J. Mendenhall, Rf-dna fingerprinting for airport wimax communications security, in: 2010 Fourth International Conference on Network and System Security, IEEE, 2010, pp. 32–39.

[84] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Mimo-assisted channel-based authentication in wireless networks, in: 2008 42nd Annual Conference on Information Sciences and Systems, IEEE, 2008, pp. 642–646.

[85] P. Zhang, J. Zhu, Y. Chen, X. Jiang, End-to-end physical layer authentication for dual-hop wireless networks, IEEE Access 7 (2019) 38322–38336.

[86] F. He, W. Wang, H. Man, Ream: Rake receiver enhanced authentication method, in: 2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, IEEE, 2010, pp. 2205–2210.

[87] F. He, H. Man, D. Kivanc, B. McNair, Epson: Enhanced physical security in ofdm networks, in: 2009 IEEE International Conference on Communications, IEEE, 2009, pp. 1–5.

[88] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, J. Chen, Threshold-free physical layer authentication based on machine learning for industrial wireless cps, IEEE Transactions on Industrial Informatics 15 (12) (2019) 6481–6491.

[89] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, H. Song, F. Xie, Y. Jiang, M. Cao, Security enhancement for mobile edge computing through physical layer authentication, IEEE Access 7 (2019) 116390–116401.

[90] W. Wang, Y. Chen, Q. Zhang, Privacy-preserving location authentication in wi-fi networks using fine-grained physical layer signatures, IEEE Transactions on Wireless Communications 15 (2) (2015) 1218–1225.

[91] D. Xu, P. Ren, J. A. Ritcey, Phy-layer cover-free coding for wireless pilot authentication in iov communications: Protocol design and ultra-security proof, IEEE Internet of things journal 6 (1) (2018) 171–187.

[92] J. K. Tugnait, H. Kim, A channel-based hypothesis testing approach to enhance user authentication in wireless networks, in: 2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010), IEEE, 2010, pp. 1–9.

[93] F. J. Liu, X. Wang, H. Tang, Robust physical layer authentication using inherent properties of channel impulse response, in: 2011-MILCOM 2011 Military Communications Conference, IEEE, 2011, pp. 538–542.

[94] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Fingerprints in the ether: Using the physical layer for wireless authentication, in: 2007 IEEE International conference on communications, IEEE, 2007, pp. 4646–4651.

[95] J. Toonstra, W. Kinsner, Transient analysis and genetic algorithms for classification, in: IEEE WESCANEX 95. Communications, Power, and Computing. Conference Proceedings, Vol. 2, IEEE, 1995, pp. 432–437.

[96] M. Barbeau, J. Hall, E. Kranakis, Detection of rogue devices in bluetooth networks using radio frequency fingerprinting, in: proceedings

of the 3rd IASTED International Conference on Communications and Computer Networks, CCN, Citeseer, 2006, pp. 4–6.

[97] R. Xie, W. Xu, Y. Chen, J. Yu, A. Hu, D. W. K. Ng, A. L. Swindlehurst, A generalizable model-and-data driven approach for open-set rff authentication, IEEE Transactions on Information Forensics and Security 16 (2021) 4435–4450.

[98] C. Wang, X. Fu, Y. Wang, G. Gui, H. Gacanin, H. Sari, F. Adachi, Few-shot specific emitter identification via hybrid data augmentation and deep metric learning, arXiv preprint arXiv:2212.00252 (2022).

[99] G. López-Risueño, J. Grajal, A. Sanz-Osorio, Digital channelized receiver based on time-frequency analysis for signal interception, IEEE Transactions on Aerospace and Electronic Systems 41 (3) (2005) 879–898.

[100] C. Bertoncini, K. Rudd, B. Nousain, M. Hinders, Wavelet fingerprinting of radio-frequency identification (rfid) tags, IEEE transactions on industrial electronics 59 (12) (2011) 4843–4850.

[101] J. Lundén, V. Koivunen, Automatic radar waveform recognition, IEEE Journal of Selected Topics in Signal Processing 1 (1) (2007) 124–136.

[102] J. K. Tugnait, Detection of non-gaussian signals using integrated polyspectrum, IEEE transactions on signal processing 42 (11) (1994) 3137–3149.

[103] V. Chandran, S. L. Elgar, Pattern recognition using invariants defined from higher order spectra-one-dimensional inputs, IEEE Transactions on signal processing 41 (1) (1993) 205–212.

[104] X.-D. Zhang, Y. Shi, Z. Bao, A new feature vector using selected bispectra for signal classification with application in radar target recognition, IEEE Transactions on Signal Processing 49 (9) (2001) 1875–1885.

[105] K. Dragomiretskiy, D. Zosso, Variational mode decomposition, IEEE transactions on signal processing 62 (3) (2013) 531–544.

[106] J. Zhang, F. Wang, Z. Zhong, O. Dobre, Novel hilbert spectrum-based specific emitter identification for single-hop and relaying scenarios, in:

2015 IEEE Global Communications Conference (GLOBECOM), IEEE, 2015, pp. 1–6.

[107] J. Zhang, F. Wang, O. A. Dobre, Z. Zhong, Specific emitter identification via hilbert–huang transform in single-hop and relaying scenarios, IEEE Transactions on Information Forensics and Security 11 (6) (2016) 1192–1205.

[108] D. Roy, T. Mukherjee, M. Chatterjee, E. Pasiliao, Detection of rogue rf transmitters using generative adversarial nets, in: 2019 IEEE wireless communications and networking conference (WCNC), IEEE, 2019, pp. 1–7.

[109] S. Aneja, N. Aneja, M. S. Islam, Iot device fingerprint using deep learning, in: 2018 IEEE international conference on internet of things and intelligence system (IOTAIS), IEEE, 2018, pp. 174–179.

[110] T. J. O'Shea, J. Corgan, T. C. Clancy, Convolutional radio modulation recognition networks, in: Engineering Applications of Neural Networks: 17th International Conference, EANN 2016, Aberdeen, UK, September 2-5, 2016, Proceedings 17, Springer, 2016, pp. 213–226.

[111] A. P. Hermawan, R. R. Ginanjar, D.-S. Kim, J.-M. Lee, Cnn-based automatic modulation classification for beyond 5g communications, IEEE Communications Letters 24 (5) (2020) 1038–1041.

[112] T. J. O'Shea, T. Roy, T. C. Clancy, Over-the-air deep learning based radio signal classification, IEEE Journal of Selected Topics in Signal Processing 12 (1) (2018) 168–179.

[113] G. Shen, J. Zhang, A. Marshall, L. Peng, X. Wang, Radio frequency fingerprint identification for lora using spectrogram and cnn, in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications, IEEE, 2021, pp. 1–10.

[114] H. Jafari, O. Omotere, D. Adesina, H.-H. Wu, L. Qian, Iot devices fingerprinting using deep learning, in: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), IEEE, 2018, pp. 1–9.

[115] Q. Wu, C. Feres, D. Kuzmenko, D. Zhi, Z. Yu, X. Liu, X. 'Leo'Liu, Deep learning based rf fingerprinting for device identification and wireless security, Electronics Letters 54 (24) (2018) 1405–1407.

[116] B. He, F. Wang, Cooperative specific emitter identification via multiple distorted receivers, IEEE Transactions on Information Forensics and Security 15 (2020) 3791–3806.

[117] A. Al-Shawabka, P. Pietraski, S. B. Pattar, F. Restuccia, T. Melodia, Deeplora: Fingerprinting lora devices at scale through deep learning and data augmentation, in: Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, 2021, pp. 251–260.

[118] G. Shen, J. Zhang, A. Marshall, M. Valkama, J. Cavallaro, Radio frequency fingerprint identification for security in low-cost iot devices, in: 2021 55th Asilomar Conference on Signals, Systems, and Computers, IEEE, 2021, pp. 309–313.

[119] H. Xu, X. Xu, A transformer based approach for open set specific emitter identification, in: 2021 7th International Conference on Computer and Communications (ICCC), IEEE, 2021, pp. 1420–1425.

[120] R. Meng, X. Xu, H. Sun, H. Zhao, B. Wang, S. Han, P. Zhang, Multiuser physical-layer authentication based on latent perturbed neural networks for industrial internet of things, IEEE Internet of Things Journal 10 (1) (2023) 637–652.

[121] Y. Liu, H. Xu, Z. Qi, Y. Shi, Specific emitter identification against unreliable features interference based on time-series classification network structure, IEEE Access 8 (2020) 200194–200208.

[122] M. Cekic, S. Gopalakrishnan, U. Madhow, Wireless fingerprinting via deep learning: The impact of confounding factors, in: 2021 55th Asilomar Conference on Signals, Systems, and Computers, IEEE, 2021, pp. 677–684.

[123] O. M. Gul, M. Kulhandjian, B. Kantarci, A. Touazi, C. Ellement, C. D'Amours, Fine-grained augmentation for rf fingerprinting under impaired channels, in: 2022 IEEE 27th International Workshop on

Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2022, pp. 115–120.

[124] I. Agadakos, N. Agadakos, J. Polakis, M. R. Amer, Chameleons' oblivion: Complex-valued deep neural networks for protocol-agnostic rf device fingerprinting, in: 2020 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2020, pp. 322–338.

[125] S. Gopalakrishnan, M. Cekic, U. Madhow, Robust wireless fingerprinting via complex-valued neural networks, in: 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, 2019, pp. 1–6.

[126] Y. Wang, G. Gui, H. Gacanin, T. Ohtsuki, O. A. Dobre, H. V. Poor, An efficient specific emitter identification method based on complex-valued neural networks and network compression, IEEE Journal on Selected Areas in Communications 39 (8) (2021) 2305–2317.

[127] C. N. Brown, E. Mattei, A. Draganov, Charrnets: Channel robust representation networks for rf fingerprinting, arXiv preprint arXiv:2105.03568 (2021).

[128] H. Li, Y. Liao, W. Wang, J. Hui, J. Liu, X. Liu, A novel time-domain graph tensor attention network for specific emitter identification, IEEE Transactions on Instrumentation and Measurement 72 (2023) 1–14.

[129] C. Zhao, C. Chen, Z. Cai, M. Shi, X. Du, M. Guizani, Classification of small uavs based on auxiliary classifier wasserstein gans, in: 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, 2018, pp. 206–212.

[130] S. Karunaratne, S. Hanna, D. Cabric, Open set rf fingerprinting using generative outlier augmentation, in: 2021 IEEE Global Communications Conference (GLOBECOM), IEEE, 2021, pp. 01–07.

[131] J. Yu, A. Hu, F. Zhou, Y. Xing, Y. Yu, G. Li, L. Peng, Radio frequency fingerprint identification based on denoising autoencoders, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2019, pp. 1–6.

[132] J. Bassey, X. Li, L. Qian, Device authentication codes based on rf fingerprinting using deep learning, arXiv preprint arXiv:2004.08742 (2020).

[133] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, T. Melodia, Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications, IEEE, 2020, pp. 646–655.

[134] X. Han, S. Chen, M. Chen, J. Yang, Radar specific emitter identification based on open-selective kernel residual network, Digital Signal Processing 134 (2023) 103913.

[135] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, K. Chowdhury, No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments, IEEE Transactions on Cognitive Communications and Networking 6 (1) (2019) 165–178.

[136] A. Elmaghbub, B. Hamdaoui, Leveraging hardware-impaired out-of-band information through deep neural networks for robust wireless device classification, arXiv preprint arXiv:2004.11126 (2020).

[137] K. Zeng, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks], IEEE Wireless Communications 17 (5) (2010) 56–62.

[138] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, A physical-layer technique to enhance authentication for mobile terminals, in: 2008 IEEE International Conference on Communications, IEEE, 2008, pp. 1520–1524.

[139] R. A. Malaney, Securing internal wi-fi networks with position verification, in: GLOBECOM'05. IEEE Global Telecommunications Conference, 2005., Vol. 3, IEEE, 2005, pp. 5–pp.

[140] F. J. Liu, X. Wang, S. L. Primak, A two dimensional quantization algorithm for cir-based physical layer authentication, in: 2013 IEEE

International Conference on Communications (ICC), IEEE, 2013, pp. 4724–4728.

[141] J. Liu, X. Wang, Physical layer authentication enhancement using two-dimensional channel quantization, IEEE Transactions on Wireless Communications 15 (6) (2016) 4171–4182.

[142] L. Xiao, L. J. Greenstein, N. B. Mandayam, W. Trappe, Channel-based spoofing detection in frequency-selective rayleigh channels, IEEE Transactions on Wireless Communications 8 (12) (2009) 5948–5956.

[143] L. Xiao, X. Wan, Z. Han, Phy-layer authentication with multiple landmarks with reduced overhead, IEEE Transactions on Wireless Communications 17 (3) (2017) 1676–1687.

[144] H. Wang, H. Fang, X. Wang, Safeguarding cluster heads in uav swarm using edge intelligence: Linear discriminant analysis-based cross-layer authentication, IEEE Open Journal of the Communications Society 2 (2021) 1298–1309.

[145] E. H. Enad, S. Younis, Machine learning based decision stratigies for physical layer authentication in wireless systems, in: 2020 2nd Annual International Conference on Information and Sciences (AiCIS), IEEE, 2020, pp. 114–118.

[146] L. Senigagliesi, M. Baldi, E. Gambi, Authentication at the physical layer with cooperative communications and machine learning, in: 2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), IEEE, 2022, pp. 71–76.

[147] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, H. V. Poor, Authenticating users through fine-grained channel information, IEEE Transactions on Mobile Computing 17 (2) (2017) 251–264.

[148] M. Abdrabou, T. A. Gulliver, Adaptive physical layer authentication using machine learning with antenna diversity, IEEE Transactions on Communications 70 (10) (2022) 6604–6614.

[149] F. Xie, Z. Pang, H. Wen, W. Lei, X. Xu, Weighted voting in physical layer authentication for industrial wireless edge networks, IEEE Transactions on Industrial Informatics 18 (4) (2021) 2796–2806.

[150] N. Wang, T. Jiang, S. Lv, L. Xiao, Physical-layer authentication based on extreme learning machine, IEEE Communications Letters 21 (7) (2017) 1557–1560.

[151] S. Wang, N. Li, S. Xia, X. Tao, H. Lu, Collaborative physical layer authentication in internet of things based on federated learning, in: 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2021, pp. 714–719.

[152] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, M. Cao, Deep-learning-based physical layer authentication for industrial wireless sensor networks, sensors 19 (11) (2019) 2440.

[153] Y. Chen, P.-H. Ho, H. Wen, S. Y. Chang, S. Real, On physical-layer authentication via online transfer learning, IEEE Internet of Things Journal 9 (2) (2021) 1374–1385.

[154] S. Xia, X. Tao, N. Li, S. Wang, J. Xu, Physical layer authentication in uav-enabled relay networks based on manifold learning, Science China Information Sciences 65 (12) (2022) 222302.

[155] N. Gulati, R. Greenstadt, K. R. Dandekar, J. M. Walsh, Gmm based semi-supervised learning for channel-based authentication scheme, in: 2013 IEEE 78th Vehicular Technology Conference (VTC Fall), IEEE, 2013, pp. 1–6.

[156] H.-M. Wang, Q.-Y. Fu, Channel-prediction-based one-class mobile iot device authentication, IEEE Internet of Things Journal 9 (10) (2021) 7731–7745.

[157] R. Meng, X. Xu, B. Wang, H. Sun, S. Xia, S. Han, P. Zhang, Physical-layer authentication based on hierarchical variational autoencoder for industrial internet of things, IEEE Internet of Things Journal 10 (3) (2023) 2528–2544.

[158] N. Gao, Q. Ni, D. Feng, X. Jing, Y. Cao, Physical layer authentication under intelligent spoofing in wireless sensor networks, Signal Processing 166 (2020) 107272.

[159] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, W. Zhuang, Reinforcement learning based phy authentication for vanets, IEEE transactions on vehicular technology 69 (3) (2020) 3068–3079.

[160] Y. Wu, T. Jing, Q. Gao, Y. Wu, Y. Huo, Game-theoretic physical layer authentication for spoofing detection in internet of things, Digital Communications and Networks (2023).

[161] R. Meng, X. Xu, H. Zhao, B. Wang, G. Li, B. Xu, P. Zhang, Multi-observation-multi-channel-attribute-based multiuser authentication for industrial wireless edge networks, IEEE Transactions on Industrial Informatics 20 (2) (2024) 2097–2108.

[162] R. Meng, X. Xu, G. Li, B. Xu, F. Zhu, B. Wang, P. Zhang, Multi-dimensional fingerprints-based multi-attacker detection for 6g systems, IEEE Internet of Things Journal 11 (2) (2024) 2665–2683.

[163] I. Agadakos, N. Agadakos, J. Polakis, M. R. Amer, Deep complex networks for protocol-agnostic radio frequency device fingerprinting in the wild, arXiv preprint arXiv:1909.08703 (2019).

[164] L. J. Wong, W. C. Headley, S. Andrews, R. M. Gerdes, A. J. Michaels, Clustering learned cnn features from raw i/q data for emitter identification, in: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), IEEE, 2018, pp. 26–33.

[165] M. Ester, H.-P. Kriegel, J. Sander, X. Xu, et al., A density-based algorithm for discovering clusters in large spatial databases with noise, in: kdd, Vol. 96, 1996, pp. 226–231.

[166] K. Merchant, S. Revay, G. Stantchev, B. Nousain, Deep learning for rf device fingerprinting in cognitive communication networks, IEEE journal of selected topics in signal processing 12 (1) (2018) 160–167.

[167] X. Qi, A. Hu, T. Chen, Lightweight radio frequency fingerprint identification scheme for v2x based on temporal correlation, IEEE Transactions on Information Forensics and Security 19 (2024) 1056–1070.

[168] Y. Liu, J. Wang, J. Li, H. Song, T. Yang, S. Niu, Z. Ming, Zero-bias deep learning for accurate identification of internet-of-things (iot) devices, IEEE Internet of Things Journal 8 (4) (2020) 2627–2634.

[169] J. Gaskin, B. Hamdaoui, W.-K. Wong, Tweak: Towards portable deep learning models for domain-agnostic lora device authentication, arXiv preprint arXiv:2209.00786 (2022).

[170] G. Shen, J. Zhang, A. Marshall, R. Woods, J. Cavallaro, L. Chen, Towards receiver-agnostic and collaborative radio frequency fingerprint identification, arXiv preprint arXiv:2207.02999 (2022).

[171] Y. Huang, P. Liu, J. Yang, Radio frequency fingerprint identification method based on ensemble learning, in: IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2022, pp. 1–6.

[172] Y. Xing, A. Hu, J. Zhang, L. Peng, X. Wang, Design of a channel robust radio frequency fingerprint identification scheme, IEEE Internet of Things Journal 10 (8) (2022) 6946–6959.

[173] L. Zong, C. Xu, H. Yuan, A rf fingerprint recognition method based on deeply convolutional neural network, in: 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), IEEE, 2020, pp. 1778–1781.

[174] Y. Chen, S. Real, H. Wen, B. Cheng, W. Wang, P.-H. Ho, S. Y. Chang, On physical-layer authentication via triple pool convolutional neural network, in: 2020 IEEE Globecom Workshops (GC Wkshps, IEEE, 2020, pp. 1–6.

[175] H. Zha, Q. Tian, Y. Lin, Real-world ads-b signal recognition based on radio frequency fingerprinting, in: 2020 IEEE 28th international conference on network protocols (ICNP), IEEE, 2020, pp. 1–6.

[176] J. Kang, Y. Shin, H. Lee, J. Park, H. Lee, Radio frequency fingerprinting for frequency hopping emitter identification, Applied Sciences 11 (22) (2021) 10812.

[177] J. McMillen, G. Mumcu, Y. Yilmaz, Deep learning-based rf fingerprint authentication with chaotic antenna arrays, in: 2023 IEEE Wireless and Microwave Technology Conference (WAMICON), IEEE, 2023, pp. 121–124.

[178] Y. Zhang, Y. Peng, B. Adebisi, G. Gui, H. Gacanin, H. Sari, Specific emitter identification based on radio frequency fingerprint using multi-scale network, in: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), IEEE, 2022, pp. 1–5.

[179] A. Gritsenko, Z. Wang, T. Jian, J. Dy, K. Chowdhury, S. Ioannidis, Finding a 'new'needle in the haystack: Unseen radio detection in large populations using deep learning, in: 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), IEEE, 2019, pp. 1–10.

[180] T. Zhang, P. Ren, Z. Ren, Deep radio fingerprint resnet for reliable lightweight device identification, in: 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), IEEE, 2021, pp. 1–6.

[181] P. Tang, Y. Xu, G. Wei, Y. Yang, C. Yue, Specific emitter identification for iot devices based on deep residual shrinkage networks, China Communications 18 (12) (2021) 81–93.

[182] J. Yu, A. Hu, G. Li, L. Peng, A robust rf fingerprinting approach using multisampling convolutional neural network, IEEE internet of things journal 6 (4) (2019) 6786–6799.

[183] Y. Pan, S. Yang, H. Peng, T. Li, W. Wang, Specific emitter identification based on deep residual networks, IEEE Access 7 (2019) 54425–54434.

[184] T. Jian, Y. Gong, Z. Zhan, R. Shi, N. Soltani, Z. Wang, J. Dy, K. Chowdhury, Y. Wang, S. Ioannidis, Radio frequency fingerprinting on the edge, IEEE Transactions on Mobile Computing 21 (11) (2021) 4078–4093.

[185] T. Zhang, S. Ye, K. Zhang, J. Tang, W. Wen, M. Fardad, Y. Wang, A systematic dnn weight pruning framework using alternating direction method of multipliers, in: Proceedings of the European conference on computer vision (ECCV), 2018, pp. 184–199.

[186] A. Ren, T. Zhang, S. Ye, J. Li, W. Xu, X. Qian, X. Lin, Y. Wang, Admm-nn: An algorithm-hardware co-design framework of dnns using alternating direction methods of multipliers, in: Proceedings of the

Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems, 2019, pp. 925–938.

[187] D. Roy, T. Mukherjee, M. Chatterjee, E. Pasiliao, Rf transmitter fingerprinting exploiting spatio-temporal properties in raw signal data, in: 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), IEEE, 2019, pp. 89–96.

[188] Y. Peng, Y. Zhou, Specific emitter identification via squeeze-and-excitation neural network in frequency domain, in: 2021 40th Chinese Control Conference (CCC), IEEE, 2021, pp. 8310–8314.

[189] L. Weng, J. Peng, J. Li, Y. Zhu, Message structure aided attentional convolution network for rf device fingerprinting, in: 2020 IEEE/CIC International Conference on Communications in China (ICCC), IEEE, 2020, pp. 495–500.

[190] Z. Zhang, L. Yuan, F. Zhou, Q. Wu, Data-and-knowledge dual-driven radio frequency fingerprint identification, IEEE Internet of Things Journal (2023).

[191] S. Hanna, S. Karunaratne, D. Cabric, Open set wireless transmitter authorization: Deep learning approaches and dataset considerations, IEEE Transactions on Cognitive Communications and Networking 7 (1) (2020) 59–72.

[192] Y. Xu, X. Qin, X. Xu, J. Chen, Open-set interference signal recognition using boundary samples: A hybrid approach, in: 2020 International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 2020, pp. 269–274.

[193] P. Oza, V. M. Patel, Deep cnn-based multi-task learning for open-set recognition, arXiv preprint arXiv:1903.03161 (2019).

[194] R. Yoshihashi, W. Shao, R. Kawakami, S. You, M. Iida, T. Naemura, Classification-reconstruction learning for open-set recognition, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019, pp. 4016–4025.

[195] G. Shen, J. Zhang, A. Marshall, J. R. Cavallaro, Towards scalable and channel-robust radio frequency fingerprint identification for lora, IEEE Transactions on Information Forensics and Security 17 (2022) 774–787.

[196] X. Zhang, M. Lin, Y. Tian, Y. Huang, J. An, T. Cui, Data enhancement aided protocol-agnostic transmitter recognition for open-set in iot, IEEE Internet of Things Journal 10 (10) (2023) 8630–8644.

[197] L. Huang, W. Pan, Y. Zhang, L. Qian, N. Gao, Y. Wu, Data augmentation for deep learning-based radio modulation classification, IEEE access 8 (2019) 1498–1506.

[198] X. Zhang, Y. Wang, Y. Zhang, Y. Lin, G. Gui, O. Tomoaki, H. Sari, Data augmentation aided few-shot learning for specific emitter identification, in: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), IEEE, 2022, pp. 1–5.

[199] F. Xie, H. Wen, J. Wu, W. Hou, H. Song, T. Zhang, R. Liao, Y. Jiang, Data augmentation for radio frequency fingerprinting via pseudo-random integration, IEEE Transactions on Emerging Topics in Computational Intelligence 4 (3) (2019) 276–286.

[200] M. Piva, G. Maselli, F. Restuccia, The tags are alright: Robust large-scale rfid clone detection through federated data-augmented radio fingerprinting, in: Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, 2021, pp. 41–50.

[201] C. Liu, X. Fu, Y. Wang, L. Guo, Y. Liu, Y. Lin, H. Zhao, G. Gui, Overcoming data limitations: a few-shot specific emitter identification method using self-supervised learning and adversarial augmentation, IEEE Transactions on Information Forensics and Security 19 (2024) 500–513.

[202] R.-F. Liao, H. Wen, S. Chen, F. Xie, F. Pan, J. Tang, H. Song, Multiuser physical layer authentication in internet of things with data augmentation, IEEE internet of things journal 7 (3) (2019) 2077–2088.

[203] J. Chen, W.-K. Wong, B. Hamdaoui, A. Elmaghbub, K. Sivanesan, R. Dorrance, L. L. Yang, An analysis of complex-valued cnns for rf

data-driven wireless device classification, in: ICC 2022-IEEE International Conference on Communications, IEEE, 2022, pp. 4318–4323.

[204] J. Stankowicz, J. Robinson, J. M. Carmack, S. Kuzdeba, Complex neural networks for radio frequency fingerprinting, in: 2019 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), IEEE, 2019, pp. 1–5.

[205] H. Gu, G. Gui, S. Hong, J. Yang, M. Liu, J. Sun, et al., Radio frequency fingerprinting driven drone identification based on complex-valued cnn, in: Proceedings of the 13th EAI International Conference on Mobile Multimedia Communications, Mobimedia 2020, 27-28 August 2020, Cyberspace, 2020.

[206] S. Wang, H. Jiang, X. Fang, Y. Ying, J. Li, B. Zhang, Radio frequency fingerprint identification based on deep complex residual network, IEEE access 8 (2020) 204417–204424.

[207] X. Fu, Y. Peng, Y. Liu, Y. Lin, G. Gui, H. Gacanin, F. Adachi, Semi-supervised specific emitter identification method using metric-adversarial training, IEEE Internet of Things Journal 10 (12) (2023) 10778–10789.

[208] Y. Wang, G. Gui, H. Gacanin, T. Ohtsuki, H. Sari, F. Adachi, Transfer learning for semi-supervised automatic modulation classification in zf-mimo systems, IEEE Journal on Emerging and Selected Topics in Circuits and Systems 10 (2) (2020) 231–239.

[209] Y. Dong, X. Jiang, L. Cheng, Q. Shi, Ssrcnn: A semi-supervised learning framework for signal recognition, IEEE Transactions on Cognitive Communications and Networking 7 (3) (2021) 780–789.

[210] J. Gong, X. Xu, Y. Qin, W. Dong, A generative adversarial network based framework for specific emitter characterization and identification, in: 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 2019, pp. 1–6.

[211] C. Li, T. Xu, J. Zhu, B. Zhang, Triple generative adversarial nets, Advances in neural information processing systems 30 (2017).

[212] Z. Xie, Z. Zhang, Y. Cao, Y. Lin, J. Bao, Z. Yao, Q. Dai, H. Hu, Simmim: A simple framework for masked image modeling, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 9653–9663.

[213] Q. Jiang, J. Sha, Rf fingerprinting identification in low snr scenarios for automatic identification system, IEEE Transactions on Wireless Communications 23 (3) (2024) 2070–2081.

[214] M. Zeng, Z. Liu, Z. Wang, H. Liu, Y. Li, H. Yang, An adaptive specific emitter identification system for dynamic noise domain, IEEE Internet of Things Journal 9 (24) (2022) 25117–25135.

[215] Y. Lin, Y. Tu, Z. Dou, L. Chen, S. Mao, Contour stella image and deep learning for signal recognition in the physical layer, IEEE Transactions on Cognitive Communications and Networking 7 (1) (2020) 34–46.

[216] Y. Tu, Y. Lin, J. Wang, J.-U. Kim, Semi-supervised learning with generative adversarial networks on digital signal modulation classification., Computers, Materials & Continua 55 (2) (2018).

[217] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, E. Pasiliao, Rfal: Adversarial learning for rf transmitter identification and classification, IEEE Transactions on Cognitive Communications and Networking 6 (2) (2019) 783–801.

[218] J. Gong, X. Xu, Y. Lei, Unsupervised specific emitter identification method using radio-frequency fingerprint embedded infogan, IEEE Transactions on Information Forensics and Security 15 (2020) 2898–2913.

[219] K. Huang, H. Liu, P. Hu, et al., Deep learning of radio frequency fingerprints from limited samples by masked autoencoding, IEEE Wireless Communications Letters (2022).

[220] C. Xie, L. Zhang, Z. Zhong, Few-shot unsupervised specific emitter identification based on density peak clustering algorithm and metalearning, IEEE Sensors Journal 22 (18) (2022) 18008–18020.

[221] P. Hao, X. Wang, A. Refaey, An enhanced cross-layer authentication mechanism for wireless communications based on per and rssi, in: 2013

13th Canadian Workshop on Information Theory, IEEE, 2013, pp. 44–48.

[222] Z. Zhang, N. Li, S. Xia, X. Tao, Fast cross layer authentication scheme for dynamic wireless network, in: 2020 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2020, pp. 1–6.

[223] C. Pei, N. Zhang, X. S. Shen, J. W. Mark, Channel-based physical layer authentication, in: 2014 IEEE Global Communications Conference, IEEE, 2014, pp. 4114–4119.

[224] R. Du, L. Zhen, Y. Liu, Physical layer authentication based on integrated semi-supervised learning in wireless networks for dynamic industrial scenarios, IEEE Transactions on Vehicular Technology 72 (5) (2023) 6154–6164.

[225] Y. Liu, P. Zhang, Y. Shen, L. Peng, X. Jiang, Online machine learning-based physical layer authentication for mmwave mimo systems, Ad Hoc Networks 131 (2022) 102864.

[226] H. Fang, X. Wang, L. Xu, Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach, IEEE Transactions on Wireless Communications 19 (8) (2020) 5420–5432.

[227] K. S. Germain, F. Kragh, Multi-transmitter physical layer authentication using channel state information and deep learning, in: 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–8.

[228] R. M. Valdovinos, J. S. Sanchez, Combining multiple classifiers with dynamic weighted voting, in: Hybrid Artificial Intelligence Systems: 4th International Conference, HAIS 2009, Salamanca, Spain, June 10-12, 2009. Proceedings 4, Springer, 2009, pp. 510–516.

[229] B. P. L. Lau, A. K. Singh, T. P. L. Tan, Weighted voting game based algorithm for joining a microscopic coalition, in: 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013), IEEE, 2013, pp. 1–4.

[230] Y. Zhou, Y. Huo, Q. Gao, Y. Wu, T. Jing, J. Mao, Securing collaborative authentication: A weighted voting strategy to counter unreliable cooperators, IEEE Transactions on Information Forensics and Security 19 (2024) 5798–5813.

[231] F. Pan, X. Li, H. Pu, Y. Guo, J. Liu, Physical layer authentication based on residual network for industrial wireless cpss, in: IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2020, pp. 4368–4373.

[232] F. Pan, H. Wen, X. Gao, H. Pu, Z. Pang, Clone detection based on bpnn and physical layer reputation for industrial wireless cps, IEEE Transactions on Industrial Informatics 17 (5) (2020) 3693–3702.

[233] S. Wang, K. Huang, X. Xu, Z. Zhong, Y. Zhou, Csi-based physical layer authentication via deep learning, IEEE Wireless Communications Letters 11 (8) (2022) 1748–1752.

[234] N. Wang, L. Jiao, P. Wang, W. Li, K. Zeng, Exploiting beam features for spoofing attack detection in mmwave 60-ghz ieee 802.11 ad networks, IEEE Transactions on Wireless Communications 20 (5) (2021) 3321–3335.

[235] N. Gao, Q. Huang, C. Li, S. Jin, M. Matthaiou, Esanet: Environment semantics enabled physical layer authentication, IEEE Wireless Communications Letters 13 (1) (2024) 178–182.

[236] Q. Wang, Z. Pang, W. Liang, J. Zhang, K. Wang, Y. Yang, Spatiotemporal gradient-based physical-layer authentication enhanced by csi-to-image transformation for industrial mobile devices, IEEE Transactions on Industrial Informatics 20 (3) (2024) 4236–4245.

[237] T. Jing, H. Huang, Q. Gao, Y. Wu, Y. Huo, Y. Wang, Multi-user physical layer authentication based on csi using resnet in mobile iiot, IEEE Transactions on Information Forensics and Security 19 (2024) 1896–1907.

[238] J. Han, Y. Li, G. Liu, J. Ma, Y. Zhou, H. Fang, X. Wu, Model-driven learning for physical layer authentication in dynamic environments, IEEE Communications Letters 28 (3) (2024) 572–576.

[239] J. Yang, Y. Chen, W. Trappe, J. Cheng, Detection and localization of multiple spoofing attackers in wireless networks, IEEE Transactions on Parallel and Distributed systems 24 (1) (2012) 44–58.

[240] W. Kaijun, Estimating the number of clusters via system evolution for cluster analysis of gene expression data, Ph.D. thesis, Xi'an: Xidian University (2007).

[241] K. Wang, J. Zheng, J. Zhang, J. Dong, Estimating the number of clusters via system evolution for cluster analysis of gene expression data, IEEE Transactions on information technology in biomedicine 13 (5) (2009) 848–853.

[242] Q. Wang, H. Li, Z. Chen, D. Zhao, S. Ye, J. Cai, Supervised and semi-supervised deep neural networks for csi-based authentication, arXiv preprint arXiv:1807.09469 (2018).

[243] M. Abdrabou, T. A. Gulliver, Leo satellite authentication using physical layer features with support vector machine, in: 2022 IEEE International Conference on Communication, Networks and Satellite (COM-NETSAT), IEEE, 2022, pp. 277–282.

[244] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, L. Hanzo, Physical layer security: Detection of active eavesdropping attacks by support vector machines, IEEE Access 9 (2021) 31595–31607.

[245] L. Senigagliesi, M. Baldi, E. Gambi, Comparison of statistical and machine learning techniques for physical layer authentication, IEEE Transactions on Information Forensics and Security 16 (2020) 1506–1521.

[246] A. Weinand, M. Karrenbauer, J. Lianghai, H. D. Schotten, Physical layer authentication for mission critical machine type communication using gaussian mixture model based clustering, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), IEEE, 2017, pp. 1–5.

[247] X. Qiu, T. Jiang, S. Wu, M. Hayes, Physical layer authentication enhancement using a gaussian mixture model, IEEE Access 6 (2018) 53583–53592.

[248] S. Tomasin, Analysis of channel-based user authentication by key-less and key-based approaches, IEEE Transactions on Wireless Communications 17 (9) (2018) 5700–5712.

[249] S. Yan, R. Malaney, I. Nevat, G. W. Peters, Optimal information-theoretic wireless location verification, IEEE Transactions on Vehicular Technology 63 (7) (2014) 3410–3422.

[250] Y. Li, L. Xiao, Q. Li, W. Su, Spoofing detection games in underwater sensor networks, in: OCEANS 2015-MTS/IEEE Washington, IEEE, 2015, pp. 1–5.

[251] Y. Zhou, P. L. Yeoh, K. J. Kim, Z. Ma, Y. Li, B. Vucetic, Game theoretic physical layer authentication for spoofing detection in uav communications, IEEE Transactions on Vehicular Technology 71 (6) (2022) 6750–6755.

[252] T. Zhang, Y. Huo, Q. Gao, L. Ma, Y. Wu, R. Li, Cooperative physical layer authentication with reputation-inspired collaborator selection, IEEE Internet of Things Journal 10 (24) (2023) 22165–22181.

[253] J. Liu, L. Xiao, G. Liu, Y. Zhao, Active authentication with reinforcement learning based on ambient radio signals, Multimedia Tools and Applications 76 (2017) 3979–3998.

[254] X. Lu, X. Wan, L. Xiao, Y. Tang, W. Zhuang, Learning-based rogue edge detection in vanets with ambient radio signals, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–6.

[255] L. Xiao, G. Sheng, X. Wan, W. Su, P. Cheng, Learning-based phy-layer authentication for underwater sensor networks, IEEE communications letters 23 (1) (2018) 60–63.

[256] G. Reus-Muns, D. Jaisinghani, K. Sankhe, K. R. Chowdhury, Trust in 5g open rans through machine learning: Rf fingerprinting on the powder pawr platform, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.

[257] E. Uzundurukan, Y. Dalveren, A. Kara, A database for the radio frequency fingerprinting of bluetooth devices, Data 5 (2) (2020) 55.

[258] T. Ya, L. Yun, Z. Haoran, J. Zhang, W. Yu, G. Guan, M. Shiwen, Large-scale real-world radio signal recognition with deep learning, Chinese Journal of Aeronautics 35 (9) (2022) 35–48.

[259] S. Hanna, S. Karunaratne, D. Cabric, Wisig: A large-scale wifi signal dataset for receiver and channel agnostic rf fingerprinting, IEEE Access 10 (2022) 22808–22818.

[260] A. Elmaghbub, B. Hamdaoui, Lora device fingerprinting in the wild: Disclosing rf data-driven fingerprint sensitivity to deployment variability, IEEE Access 9 (2021) 142893–142909.

[261] C. Morin, L. S. Cardoso, J. Hoydis, J.-M. Gorce, T. Vial, Transmitter classification with supervised deep learning, in: Cognitive Radio-Oriented Wireless Networks: 14th EAI International Conference, CrownCom 2019, Poznan, Poland, June 11–12, 2019, Proceedings 14, Springer, 2019, pp. 73–86.

[262] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, I. Guvenc, Drone remote controller rf signal dataset (2020). `doi:10.21227/ss99-8d56`. URL `https://dx.doi.org/10.21227/ss99-8d56`

[263] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, K. Chowdhury, Rf fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms, IEEE transactions on vehicular technology 69 (12) (2020) 15518–15531.

[264] R. Candell, C. A. Remley, J. T. Quimby, D. R. Novotny, A. Curtin, P. B. Papazian, G. H. Koepke, J. Diener, M. T. Hany, Industrial wireless systems: Radio propagation measurements (2017).

[265] C. A. of Information, C. Technology, Mobile communication open dataset. URL `https://www.mobileai-dataset.com/html/default/yingwen/DateSet/index.html?index=1`

[266] S. Jaeckel, L. Raschkowski, K. Börner, L. Thiele, Quadriga: A 3-d multi-cell channel model with time evolution for enabling virtual field trials, IEEE transactions on antennas and propagation 62 (6) (2014) 3242–3256.

[267] A. Gassner, C. Musat, A. Rusu, A. Burg, Opencsi: An open-source dataset for indoor localization using csi-based fingerprinting, arXiv preprint arXiv:2104.07963 (2021).

[268] L. Liu, C. Oestges, J. Poutanen, K. Haneda, P. Vainikainen, F. Quitin, F. Tufvesson, P. De Doncker, The cost 2100 mimo channel model, IEEE Wireless Communications 19 (6) (2012) 92–99.

[269] A. Alkhateeb, Deepmimo: A generic deep learning dataset for millimeter wave and massive mimo applications, arXiv preprint arXiv:1902.06435 (2019).

[270] L. Wang, S. Pasricha, A framework for csi-based indoor localization with id convolutional neural networks, in: 2022 IEEE 12th International Conference on Indoor Positioning and Indoor Navigation (IPIN), IEEE, 2022, pp. 1–8.

[271] 3GPP, Study on channel model for frequencies from 0.5 to 100 ghz, version 16.1.0 (2020).

[272] Y. Zhang, J. Sun, G. Gui, H. Gacanin, H. Sari, A generalized channel dataset generator for 5g new radio systems based on ray-tracing, IEEE Wireless Communications Letters 10 (11) (2021) 2402–2406.

[273] E. Basar, I. Yildirim, F. Kilinc, Indoor and outdoor physical channel modeling and efficient positioning for reconfigurable intelligent surfaces in mmwave bands, IEEE Transactions on Communications 69 (12) (2021) 8600–8611.

[274] M. Alrabeiah, A. Hredzak, Z. Liu, A. Alkhateeb, Viwi: A deep learning dataset framework for vision-aided wireless communications, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–5.

[275] P. Qarabaqi, M. Stojanovic, Statistical characterization and computationally efficient modeling of a class of underwater acoustic communication channels, IEEE Journal of Oceanic Engineering 38 (4) (2013) 701–717.

[276] C.-X. Wang, J. Huang, H. Wang, X. Gao, X. You, Y. Hao, 6g wireless channel measurements and models: Trends and challenges, IEEE Vehicular Technology Magazine 15 (4) (2020) 22–32.

[277] R. Meng, F. Zhu, X. Xu, L. Jin, B. Wang, B. Xu, H. Meng, P. Zhang, Efficient gaussian process classification-based physical-layer authentication with configurable fingerprints for 6g-enabled iot, arXiv preprint arXiv:2307.12263 (2023).

[278] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, B. Xiao, Deep-learning-based physical-layer secret key generation for fdd systems, IEEE Internet of Things Journal 9 (8) (2021) 6081–6094.