A Survey of Physical Layer Authentication for Millimeter-Wave MIMO Systems

Xu Zhao[1]
[1]School of Systems Information Science, Future University Hakodate, 116-2 Kamedanakano-cho, Hakodate, Hokkaido, 041-8655, Japan

Millimeter-wave (mmWave) communication, leveraging its advantages of large bandwidth and high data rate, has become a key technology for the fifth-generation (5G) wireless networks. However, its highly directional beam transmission characteristics also bring unprecedented physical layer security challenges, especially impersonation attacks. Physical layer authentication (PLA), as an emerging security paradigm, verifies the transmitter identity by exploiting unique physical features of channels or device, providing an effective approach to enhance the security of mmWave systems. This paper summarizes the research status of PLA schemes in mmWave scenarios, systematically classifies existing authentication schemes into three categories: channel feature-based authentication, device impairment-based authentication, and hybrid multi-feature authentication. It introduces the latest works in each category and finally discusses the challenges and future research directions.

Index Terms—**Physical Layer Authentication, Millimeter-Wave (mmWave), Wireless Networks.**

I. Introduction

Wireless communication is an indispensable technology in modern communication methods. Compared with wired communication, wireless communication technology offers high flexibility and broad development prospects [1]. Unlike traditional wireless communication technologies, mmWave communication can provide richer bandwidth, higher data rates, narrower beams, and better transmission quality. Due to the short wavelength of mmWave, combining with MIMO (Multi-Input Multi-Output) communication technology, mmWave communication systems enable deploying a large number of antennas on a relatively small antenna array [2]. By integrating mmWave and massive antenna array technology, mmWave MIMO communication systems can meet the massive connection requirements of numerous devices and greatly improve communication performance. Therefore, mmWave and MIMO communication technologies are regarded as core enabling technologies for the Fifth Generation of Wireless Communications (5G) and even the next generation of communications [3]–[5]. 5G communication networks integrated with mmWave MIMO technology can support continuous wide-area coverage scenarios [6], [7], hot-spot high-capacity scenarios, low-latency high-reliability scenarios, and low-power large-connection scenarios , providing support for upper-layer application scenarios such as smart cities and industrial internet [8]. In summary, 5G communication networks integrating mmWave MIMO technology play an irreplaceable role in building a new type of digital infrastructure that is high-speed, ubiquitous, integrated, interconnected, intelligent, green, secure, and reliable, and will serve as a new type of information infrastructure to provide strong support for various industries [9].

However, due to the inherent openness, signal broadcasting characteristics, and superposition of the wireless transmission medium in mmWave MIMO communication systems [10], device identities are highly vulnerable to forgery [11], [12]. In traditional identity authentication mechanisms based on digital certificates, passwords, etc., device identity information is usually simply attached to physical devices, which brings significant security challenges to mmWave MIMO communication systems [13]. In addition, for the rapidly developing mmWave and terahertz communication networks, traditional hierarchical and distributed identity authentication mechanisms are difficult to meet the requirements of rapid and random access, ultra-low energy consumption of massive heterogeneous devices. Wireless network access security control is the first layer of security protection for mmWave MIMO communication systems and one of the most important ways to ensure wireless network security. Therefore, exploring new network access security control theories and methods has important theoretical and practical significance [14], [15]. Device authentication technology based on physical layer feature analysis and extraction implements device access control at the signal level, which will provide a new security guarantee idea for mmWave MIMO communication systems.

Existing wireless device identity authentication is implemented through information security and confidentiality methods based on computational security [16], whose high computational complexity often requires significant resource overhead. Existing authentication mechanisms are generally upper-layer based, without considering physical layer characteristics, and are vulnerable to man-in-the-middle attacks. Once the key is leaked, identity cloning is likely to occur. Although the public key cryptography mechanism based on Certificate Authority (CA) can well realize secure identity key exchange, it requires the support of security infrastructure, faces challenges in large-scale and randomly deployed mmWave MIMO communication systems, and cannot meet the authentication needs of low-energy devices in 5G networks [17]. It can be seen that existing wireless network device identity authentication mechanisms have certain limitations. Therefore,

Manuscript received August 5, 2025; revised October 27, 2025. Corresponding author: Xu Zhao (email: g3225002@fun.ac.jp).

there is an urgent need to find a new security mechanism to ensure efficient and accurate identification of authorized users and unauthorized users, thereby reducing potential security risks from malicious users. Identity authentication based on physical layer features is one of the most ideal implementation mechanisms for physical layer security. It identifies the endogenous identity of the message source based on the inherent features of devices (such as carrier frequency offset [18], [19], in-phase/quadrature imbalance [20], phase noise [21], [22]) and channel features (such as channel amplitude [23], received signal energy [24]), thereby realizing wireless device identity authentication.Fig. 1 illustrates a typical wireless secure communication model, which exhibits generality and adaptability in most wireless communication scenarios. As depicted in Fig. 1, there are three distinct roles in the wireless secure communication system: Alice, Bob, and Eve. Alice is the legitimate sender, Bob is the legitimate receiver, and Eve is a malicious attacker. Eve attempts to simulate the communication between Alice and Bob by masquerading as a legitimate sender. Bob aims to detect Eve's attack using a certain authentication method. Traditional PLA mainly consists of two categories: device authentication based on wireless channel characteristics and device authentication based on device fingerprint characteristics.

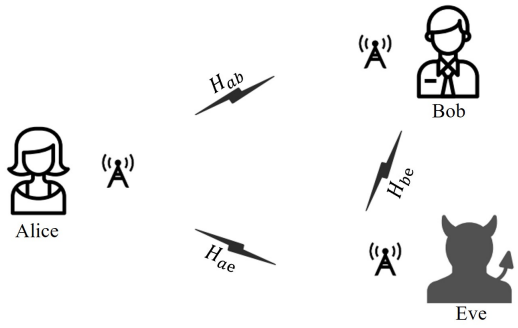

Fig. 1: typical wireless secure communication system model

A. Channel Feature Authentication

Device authentication based on wireless channel characteristics realizes device identity verification by utilizing the location-dependent channel characteristics between the devices of both communicating parties. In recent years, the academic community has carried out extensive research on device authentication around wireless channel characteristics. The initial device authentication method based on Received Signal Strength (RSS) characteristics simply uses the received signal energy information to defend against spoofing attacks and Sybil attacks [25], without considering more abundant channel characteristics. To improve authentication performance, the academic community has explored the use of more robust time-domain characteristics of wireless channels. Tugnait et al. proposed a PLA method based on Channel Impulse Response (CIR) characteristics for single-carrier time-invariant communication systems [26]. Subsequently, Liu et al. designed a new authentication mechanism using time-varying multipath CIR characteristics to further improve the detection effect [27]. On this basis, Liu et al. proposed an improved PLA method based on CIR characteristics [28]. This method uses the amplitude and multipath delay characteristics of CIR to enhance the robustness of the device authentication method in mobile scenarios, employs a two-dimensional quantizer to quantize the amplitude and multipath delay characteristics respectively, and then uses the Logarithmic Likelihood Ratio Test (LLRT) method for device identity verification. Based on this, Liu and Wang further improved the authentication accuracy in mobile environments by utilizing channel correlation, and theoretically derived a closed-form expression of the detection rate to evaluate the performance of the proposed device authentication mechanism [29]. Later, Zhang et al. continued to propose a device authentication method for untrusted relay two-hop wireless networks [30]. Specifically, when a legitimate device sends a message to the relay, the receiving device simultaneously sends artificial interference to the relay; the relay then forwards the legitimate message with artificial interference to the receiving device, which checks both the CIR characteristics and the interference signal. Thus, this method can defend against both spoofing attacks and information forgery attacks initiated by the relay.

In addition to the time-domain characteristics of wireless channels, frequency-domain characteristics such as Channel Frequency Response (CFR) can also be used as identity identifiers to design device authentication methods. Xiao et al. proposed a device authentication method based on CFR characteristics for time-invariant communication systems [31]. In the training phase, the receiving device extracts CFR characteristics from legitimate transmitting devices; in the authentication phase, it extracts CFR characteristics from the current unknown transmitting device. The receiving device then verifies the unknown transmitting device by comparing the two extracted CFR characteristics. On this basis, Xiao et al. introduced the delay spectrum, Doppler spectrum, and spatial correlation characteristics of time-varying channels to design an authentication method for improved performance [32]. However, the above research works did not explore the performance of device authentication based on CFR characteristics in multi-antenna scenarios. To address this issue, both Xiao et al. [33] and Baracca et al. [34] proposed device authentication mechanisms based on CFR characteristics for MIMO communication systems, and designed the Generalized Likelihood Ratio Test (GLRT) method for device identity verification. To further enhance authentication performance, He et al. proposed device authentication methods that jointly utilize the amplitude and phase characteristics of CFR for Orthogonal Frequency Division Multiplexing (OFDM) communication systems [35] and Code Division Multiple Access (CDMA) communication systems [36]. It is worth noting that the aforementioned device authentication methods are based on different communication scenarios, and their authentication performance is closely related to network topology and communication environments [37]. To solve this problem, Xiao et al. proposed a device authentication method based on CFR characteristics for general wireless communication scenarios [38]. This method establishes a frequency-selective random Rayleigh channel

model, considers Doppler shift, multi-antenna, and channel estimation errors, and then designs an authentication decision criterion based on channel prior knowledge and the GLRT method. To simplify the authentication scheme, Xiao et al. also proposed a simplified version of the device authentication mechanism that relaxes the requirements for channel prior knowledge [38].

In recent years, to further improve authentication performance, the academic community has introduced machine learning methods to design device authentication mechanisms. Wang et al. developed a device authentication method using the Extreme Learning Machine (ELM) algorithm [39]. In the training phase, the method generates two types of received signals based on legitimate and illegal channel models respectively; the receiving device extracts CFR characteristics from the signals and constructs wireless channel feature vectors by calculating the Euclidean distance and Pearson correlation coefficient between data. The receiving device then inputs the feature vectors into the ELM algorithm for training to obtain a machine learning model. In the authentication phase, the receiving device extracts CFR characteristics from the signals of unknown transmitting devices, inputs the constructed feature vectors into the trained machine learning model, and verifies the current device identity. Weinand et al. designed a device authentication mechanism using the Gaussian Mixture Model [40], and validated the proposed scheme with real data in mixed office and laboratory areas with many objects and metal walls. Specifically, in the training phase, the receiving device constructs a CFR characteristic dataset to train the Gaussian Mixture Model; in the authentication phase, it constructs CFR characteristic data from the signals of unknown transmitting devices and inputs them into the trained Gaussian Mixture Model to verify the identity of the transmitting device. Pan et al. designed authentication methods using Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbor (KNN) algorithm, and Bagged Trees (BT) algorithm [41]. This method uses the CFR characteristic dataset of wireless mobile industrial Cyber-Physical Systems (CPS) in actual factories to train and validate the proposed device authentication scheme. The above studies all use traditional machine learning algorithms, and their authentication performance is still limited. To further improve authentication performance, Wang et al. [42] used Convolutional Recurrent Neural Network (CRNN) to extract the correlation between two CFR characteristics at different times and frequencies. However, training the CRNN model requires a large amount of labeled CFR characteristic data. To significantly reduce the overhead caused by massive data, the authors also proposed a semi-supervised learning method that uses a small amount of data.

B. Device fingerprint authentication

Device authentication based on device fingerprint characteristics realizes device identity verification by utilizing the tolerance or defect characteristics of the device circuits of wireless devices. Common device fingerprint characteristics include phase noise, carrier frequency offset, in-phase/quadrature imbalance, etc.

1) Authentication Based on Phase Noise

Phase noise originates from manufacturing defects of oscillators in wireless devices, mainly occurring in the up-conversion process from baseband signals to bandpass signals and vice versa. Since device defects in wireless devices are unavoidable in practical scenarios, phase noise can be used as a device fingerprint characteristic to design authentication methods. Zhao et al. proposed a device authentication method based on phase noise characteristics [43]. Xie et al. proposed a device authentication mechanism based on phase noise characteristics [44], avoiding the performance loss caused by quantization methods. To further explore phase noise characteristics, Xie et al. also proposed an enhanced device authentication method based on phase noise, which improves authentication performance by introducing artificial random phase characteristics into transmitted signals [44].

2) Authentication Based on Carrier Frequency Offset

Carrier frequency offset stems from device defects of local oscillators in the radio frequency (RF) links of devices and Doppler shift in mobile scenarios. Hou et al. proposed a device authentication method based on carrier frequency offset characteristics for time-invariant OFDM communication systems, using hypothesis testing to verify the identity of unknown devices [45]. However, Hou et al. did not consider more practical mobile scenarios. To address this issue, Hou et al. proposed a device authentication method for time-varying wireless communication scenarios [46]. This method models carrier frequency offset using an Auto-Regressive (AR) random process, and the designed model can well characterize the impact of dynamic time-varying environments on carrier frequency offset characteristics, making it of great practical significance and value.

3) Authentication Based on Power Amplifier device Defects

The power amplifier is the last component in the RF link of wireless devices, and its device defects are relatively obvious. Therefore, device defects of power amplifiers can also be used as device identity identifiers to design authentication schemes. Dolatshahi et al. designed a device authentication mechanism based on power amplifier device defects using the Generalized Likelihood Ratio Test (GLRT) and Classical Likelihood Ratio Test (CLRT) methods [47]. To improve authentication performance, Polak et al. developed a device authentication method based on the combined device defects of power amplifiers and digital-to-analog converters (DACs) [48]. Subsequently, to solve the problem of attackers maliciously introducing slight interference into data symbols to forge power amplifier device defects, Polak et al. designed a device authentication mechanism using spectrum analysis [49].

4) Authentication Based on Clock Offset

Clock offset of wireless devices caused by their own device defects is also a device fingerprint characteristic that can be used to design device authentication schemes. Rahman et al. proposed a device authentication method based on time-varying clock offset characteristics, using a Kalman filter to track the clock offset characteristics of transmitting devices [50]. Polčák et al. proposed a device authentication method based on clock offset characteristics, which extracts clock offset features using timestamps in TCP headers [51]. To

enhance authentication performance, Jana et al. proposed an enhanced device authentication method that uses the Time Synchronization Function (TSF) timestamps of IEEE 802.11 to calculate clock offset characteristics, thereby resisting device identity simulation attacks [52]. Later, Cristea et al. proposed a device authentication method based on clock offset characteristics, which calculates clock offset features using timestamps of the Internet Control Message Protocol (ICMP) and validates the performance of the proposed method through experiments with smartphones [53].

5) Authentication Based on In-Phase/Quadrature Imbalance

In-phase/quadrature imbalance characteristics of wireless devices result from amplitude and phase mismatches between in-phase and quadrature branches, which can be used as device identity identifiers to design authentication mechanisms. Hao et al. proposed a device authentication mechanism where multiple trusted receiving devices collaboratively use in-phase/quadrature imbalance characteristics [54]. Subsequently, Hao et al. proposed a device authentication method based on the in-phase/quadrature imbalance characteristics of relays, designing authentication criteria using GLRT and hypothesis testing [55]. To improve authentication performance, Sankhe et al. proposed a PLA mechanism based on in-phase/quadrature imbalance characteristics for both static and dynamic scenarios [56].

Recently, preliminary studies have focused on integrating PLA into mmWave systems.

C. Organization

To the best of our knowledge, no existing work has comprehensively surveyed Physical Layer Authentication (PLA) for mmWave systems, nor has any work categorized PLA schemes based on quasi-static and dynamic scenarios. This paper is developed based on this research gap. The organization of the remainder of this paper is as follows: Section II briefly outlines the characteristics of mmWave communication; Section III elaborates on Channel Fingerprint Authentication, covering the relevant technologies in Quasi-Static Scenarios and Dynamic Scenarios; Section IV presents Device Fingerprint Authentication, specifically discussing its applications in Quasi-Static Scenarios and Dynamic Scenarios; Section V focuses on Hybrid Feature Authentication, analyzing its implementation approaches in Quasi-Static Scenarios and Dynamic Scenarios respectively; Future research directions and conclusions are provided in Section VI. The list of abbreviations is in Table I.The organizational structure of this paper is illustrated in Fig. 2.

TABLE I: List of Abbreviations

Abbreviations	Full Name
AAoA	Azimuth Angle of Arrival
AoA	Angle of Arrival
AoD	Angle of Departure
AR	Auto-Regressive
AP	Access Point
BT	Bagged Trees
CDMA	Code Division Multiple Access
CIR	Channel Impulse Response
CFR	Channel Frequency Response
CRNN	Convolutional Recurrent Neural Network
DT	Decision Tree
DPLA	Distributed Physical Layer Authentication
EAoA	Elevation Angle of Arrival
ELM	Extreme Learning Machine
FC	Fusion Center
GMM	Gaussian Mixture Model
GLRT	Generalized Likelihood Ratio Test
IIoT	Industrial IoT
IoT	Internet of Things
KNN	K-Nearest Neighbor
LLRT	Logarithmic Likelihood Ratio Test
LPBCRB	Limiting Posterior Bayesian Cramér-Rao Bound
LoS	Line of Sight
LWC	Linear Weighted Combination
MC	Mutual Coupling
ML	Maximum Likelihood
MIMO	Multi-Input Multi-Output
mmWave	Millimeter-wave
NLOS	Non-Line of Sight
OFDM	Orthogonal Frequency Division Multiplexing
PLA	Physical Layer Authentication
PSD	Power Spectral Density
RF	Radio Frequency
SDR	Software-Defined Radio
SLS	Sector-Level Sweeping
SV	Saleh-Valenzuela Model
SVM	Support Vector Machine
UE	User Equipment
UAV	Unmanned Aerial Vehicle
V2X	Vehicle-to-Everything

II. BACKGROUND

In this section, we introduced the communication fundamentals of mmWave systems. Then, we gave a brief introduction to the channels of mmWave systems.

A. MmWave Propagation Characteristics

MmWave refers to electromagnetic waves with frequencies ranging from 30 GHz to 300 GHz and wavelengths between 1 mm and 10 mm [57], with available bandwidth up to 2.5 GHz. For example, the frequency band of 37 GHz - 39.5 GHz has been planned by many countries and standardization organizations (such as 3GPP, FCC) for 5G mmWave communication, which can support extremely high data transmission rates. When combined with MIMO technology, the array spacing can be reduced to 1.25 mm, and spectral efficiency greater than 100 bps/Hz can be achieved through massive MIMO. In addition, mmWave also has the advantages of high security, strong anti-interference ability, and can be combined with low-power devices, making it a key technology in various fields. However, mmWave also has problems such as severe propagation loss, limited propagation distance, and vulnerability to blockage.

Mmwave signals experience severe free-space path loss during propagation over wireless links. The Friis free-space equation elucidates the relationship among communication distance, frequency, and received power, given by the following expression:

$$\frac{P_r}{P_t} = \frac{G_t G_r \lambda^2}{(4\pi d)^2} \tag{1}$$

Wherein, P_r denotes the received power, P_t the transmitted power, λ the signal wavelength, d the distance between the transmitter and receiver, and G_t/G_r the transmit/receive

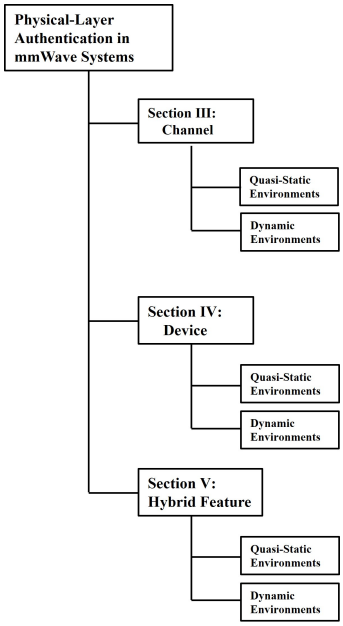

Fig. 2: Organizational structure of this article

antenna gains, respectively. As indicated by the above equation, the received power P_r is proportional to the square of the signal wavelength. In contrast to low-frequency signals, mmWave signals have shorter wavelengths (typically ranging from 1 to 10 millimeters), resulting in more severe path loss. Furthermore, it is evident that P_r is inversely proportional to the square of the distance; specifically, a 10-fold increase in distance leads to a 20 dB increase in path loss.

In addition to path loss, mmWave signals also have the characteristic of atmospheric absorption [58]. When mmWave signals propagate in the atmosphere, they are absorbed due to the resonance of water vapor, oxygen, and other components, and the absorption intensity is related to factors such as atmospheric pressure, temperature, and altitude of the environment. Furthermore, since the size of raindrops is close to the wavelength of mmWave signals, raindrops can effectively scatter and absorb mmWave signals, leading to rain attenuation [59]. Moreover, rain attenuation is related to the shape of raindrops; the attenuation of non-spherical raindrops is greater than that of spherical raindrops of the same volume.

Another notable feature is the poor penetration performance of mmWave signals. The higher the frequency of mmWave (i.e., the shorter the wavelength), the worse their penetration ability. Therefore, the blocking of obstacles will have a serious impact on mmWave signals. During the propagation of mmWave signals, due to the significant attenuation of energy, the scattering paths of most signals almost disappear, leaving only the Line of Sight (LoS) path and a few Non-Line of Sight (NLOS) paths for effective signal transmission. These indicate that the propagation paths of mmWave signals are mainly focused on several main directions, and there is almost no energy in other directions. Therefore, the mmWave channel exhibits sparse characteristics [60].

To address the above problems, mmWave systems usually need to be combined with massive MIMO technology, beamforming technology, and intelligent reflecting surfaces. On the one hand, due to the short wavelength of mmWave, antennas can be designed to be very short for micro-integration, thereby allowing more antennas to be deployed in a limited space to implement massive MIMO technology, achieving the goal of improving the array gain of the system. Moreover, by using beamforming technology at both the transmitting and receiving ends, signal energy can be effectively concentrated in the target direction, further improving the communication coverage and system performance. On the other hand, intelligent reflecting surfaces can intelligently regulate incident signals, allowing signals to bypass obstacles and continue to propagate, and can also be used to improve signal quality.

B. mmWave Channel Model

In low-frequency communication, due to the existence of abundant scattering paths, the Rayleigh fading model is usually used to simulate channel characteristics [61]. Although this model is widely used, it cannot reflect the specific propagation environment. The propagation characteristics of mmWave signals are significantly different from those of low-frequency signals, mainly reflected in the large path loss, poor diffraction ability, and abundant scattering mentioned in the previous section. Therefore, mmWave signals are usually transmitted through several main transmission paths, including one LoS path and several NLOS paths, and mainly rely on the LoS path, as shown in Fig. 3, following the Rice distribution.

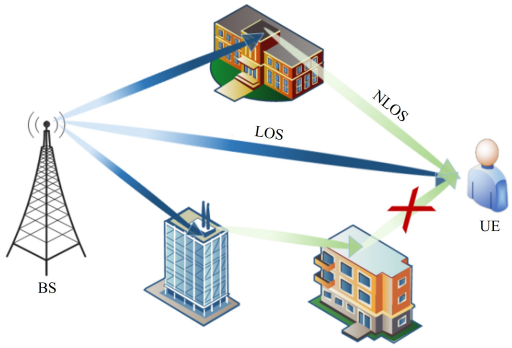

Fig. 3: Schematic Diagram of mmWave MIMO Communication System

The Saleh-Valenzuela (SV) model is typically employed to characterize the spatial propagation characteristics of mmWave signals. Based on the SV channel model, the specific channel model is expressed as follows:

$$\mathbf{H}_k = \sqrt{\frac{N_r N_t}{L}} \sum_{l=1}^{L} \alpha_l \mathbf{a}_r\left(\theta_l^r\right) \mathbf{a}_t^H\left(\theta_l^t\right) \tag{2}$$

N_r denotes the number of receive antennas, N_t the number of transmit antennas, and L the number of propagation paths between the transmitter and receiver. $\alpha_l \sim \mathcal{CN}(0,1)$ represents the complex gain of the path; θ_l^r is the angle of arrival (AoA) of the l-th multipath, and θ_l^t is the angle of departure (AoD) of the l-th multipath. $\mathbf{a}_r$ and $\mathbf{a}_t$ denote the array response vectors of the receiver and transmitter, respectively, with their specific expressions given as follows:

$$\mathbf{a}_r\left(\theta_{l,k}^r\right) = \frac{1}{\sqrt{N_r}}\left[1, e^{j\pi\sin\theta_{l,k}^r}, \ldots, e^{j\pi(N_r-1)\sin\theta_{l,k}^r}\right]^T \quad (3)$$

$$\mathbf{a}_t\left(\theta_{l,k}^t\right) = \frac{1}{\sqrt{N_t}}\left[1, e^{j\pi\sin\theta_{l,k}^t}, \ldots, e^{j\pi(N_t-1)\sin\theta_{l,k}^t}\right]^T \quad (4)$$

Equation (2) can be expressed in matrix form as:

$$\mathbf{H} = \mathbf{A}_r\mathbf{\Sigma}\mathbf{A}_t^H \quad (5)$$

Furthermore, the channel gain h forms the matrix $\mathbf{H} \in \mathbb{C}^{N_r\times N_t}$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_{11} & \mathbf{h}_{12} & \cdots & \mathbf{h}_{1N_t} \\ \mathbf{h}_{21} & \mathbf{h}_{22} & \cdots & \mathbf{h}_{2N_t} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{h}_{N_r1} & \mathbf{h}_{N_r2} & \cdots & \mathbf{h}_{N_rN_t} \end{bmatrix} \quad (6)$$

$h_{11}, h_{12}, \cdots, h_{1N_t}$ in the first row denote the channel gains between the 1st, 2nd, $\cdots$, N_t-th transmit antennas and the 1st receive antenna. The 2nd row respectively represents the channel gains generated between the 1st, 2nd, $\cdots$, N_t-th transmit antennas and the 2nd receive antenna. Up to the N_r-th row of the matrix, it denotes the channel gains between the 1st, 2nd, $\cdots$, N_t-th transmit antennas and the N_r-th receive antenna.

Based on the characteristics of the above-mentioned millimeter-wave communication, a number of studies on PLA in mmWave communication systems have been carried out in recent years.

III. Channel Fingerprint-Based Authentication in mmWave Systems

The core idea of PLA based on channel features is to use the unique and difficult-to-forge physical properties of mmWave channels in specific environments for identity verification. If an attacker is not in the same physical location as the legitimate user (usually separated by more than half a wavelength), the channel responses from each to the receiver will be significantly different, thereby providing a basis for authentication.

A. Channel Feature Authentication in Quasi-Static Environments

One of the most prominent features of mmWave channels is their sparsity in the angular domain. Due to the limited number of signal propagation paths, channel energy is mainly concentrated in a few angular directions, which constitutes a channel sparsity that is difficult to accurately replicate. Tang et al. first proposed the possibility of authentication using the sparsity of mmWave MIMO channels in the beamspace domain, extracting the sparse peak coordinates of virtual Angle of Arrival/Angle of Departure (AoA/AoD) as authentication features, which is a lightweight method [62]. The study assumes that these coordinates of legitimate users are stable within the channel coherence time, while the coordinates of attackers at different locations are completely different. Therefore, identity judgment can be performed by comparing the Euclidean distance between the peak coordinate vectors estimated at two consecutive moments with a preset threshold. This work laid the foundation for lightweight PLA using mmWave channel sparsity, and its effectiveness mainly depends on the relative stability of the channel within the authentication interval.

To address spoofing attacks in mmWave MIMO systems, Liza Afeef et al. proposed a novel PLA scheme [63]. The core of the scheme is to create a new "distance signature" by leveraging beamspace channel characteristics; this signature is obtained by measuring the displacement of the positions of principal components in the beamspace relative to the origin and sorting these distance values in descending order based on the phases of the principal components. In addition, to further improve performance, the authors introduced the "mutual coupling effect", a device property of antenna arrays, into the system and combined it with the distance signature to form a "hybrid signature". Simulation results confirm the effectiveness of the scheme in terms of detection rate and false alarm rate.

Mu Niu et al. proposed a robust PLA framework for mmWave MIMO systems, which jointly utilizes spatial channel features and device-induced impairments (i.e., radiometric features) [64]. Specifically, the scheme adopts CANDECOMP/PARAFAC (CP) tensor decomposition technology to extract features such as path, angle, and array error. Each of these features is then individually classified through binary hypothesis testing, and the final authentication decision is obtained by weighted fusion of these classification results. The authors also derived closed-form expressions for false alarm probability and detection probability, and simulations confirm that the method has high accuracy and robustness in coping with various spoofing attacks.

B. Channel Feature Authentication in High-Dynamic Environments

Aiming at the damage to channel time correlation caused by high mobility (such as UAV), which poses challenges to methods relying on the stability of instantaneous channel states (such as the method proposed by Tang et al.), Teng et al. adopted a different strategy in the UAV-ground communication system [65].

Instead of relying on transiently changing channel coordinates, they utilized the more stable long-term statistical feature of channel sparsity. To more accurately characterize the spike and heavy-tailed characteristics of sparse channels, the study introduced the Laplace prior from the field of image processing to model the angular domain channel statistical characteristics, combined with the Generalized Approximate Message Passing (GAMP) algorithm for efficient sparse feature extraction. Unlike the coordinates used by Tang et al., they used the scale parameter σ_v reflecting the sparsity degree as the authentication fingerprint. Since σ_v is a statistic, its variation is much slower than that of the instantaneous channel. Therefore, the scheme achieves robust authentication against mobility, especially showing better stability in resisting rapid channel changes caused by the high-speed movement of UAVs.

Liza Afeef et al. proposed a novel "distance signature" [66]. The method first extracts the principal components of the

beamspace channel and their position coordinates (i.e., virtual AoA/AoD), then calculates the Euclidean distance of each principal component position relative to the coordinate origin, and sorts these distances according to the phase values of the principal components to finally form a unique vector signature. Since this signature does not directly depend on the gain of the channel path (i.e., the amplitude of the principal component), it has good robustness to channel fluctuations and noise. To address the severe challenges brought about by mobility, the team's subsequent work further proposed a tracking-based PLA framework. This framework uses the Extended Kalman Filter (EKF) to continuously track and predict the dynamic evolution of the legitimate user's "Enhanced Distance Signature". Notably, the work cleverly utilizes the beam squint effect in wideband mmWave systems—the phenomenon that the beam pointing shifts with frequency—to increase the richness and dimension of the signature, thereby effectively ensuring the stability and continuity of authentication in dynamic environments.

IV. Device Fingerprint-Based Authentication in mmWave Systems

Device fingerprint-based authentication uses the inevitable and unique physical defects of transmitter device during the manufacturing process as identity identifiers. Such features originate from the device itself and are basically independent of the channel environment, thus having a natural and significant advantage in resisting co-located attacks (i.e., attackers are very close to legitimate users). For mmWave MIMO systems with a large number of antennas, device features related to antenna arrays are particularly abundant and prominent.

A. Device Feature Authentication in Quasi-Static Environments

Balakrishnan et al. proposed a novel physical layer-based device fingerprinting scheme to address the security challenges of mmWave wireless networks [67]. Its core idea is to use the unique, device-specific beam pattern distortion caused by tolerances and errors in the manufacturing process of mmWave device antenna arrays and phase shifters as authentication fingerprints. The researchers designed a method to capture comprehensive fingerprint information by using multiple Access Points (APs) to collect spatial-temporal beam features generated by devices when scanning different codebooks during the beam searching or Sector-Level Sweeping (SLS) process. Through extensive experiments using commercial off-the-shelf mmWave devices, the study verified the reliability, stability, and uniqueness of the proposed features and compared them with traditional Power Spectral Density (PSD) features. The results show that the method (especially in the multi-AP scenario) can achieve extremely high recognition accuracy (exceeding 0.99) in both static (LoS and NLOS) and mobile scenarios, significantly outperforming the PSD method. In addition, the study also designed and implemented impersonation attacks using Software-Defined Radio (SDR). Experiments prove that although single-AP systems may be vulnerable to attacks, the multi-AP architecture can effectively resist such attacks, while PSD features are relatively fragile, thereby highlighting the potential of the proposed scheme in practical security applications.

B. Device Feature Authentication in Dynamic Environments

Zhang et al. proposed a novel Distributed Physical Layer Authentication (DPLA) framework to address the identity authentication challenges in mmWave MIMO systems, especially the single point of failure problem of centralized authentication, to combat identity forgery attacks [68]. The framework is designed for dynamic scenarios (industrial internet of things, vehicle-to-everything). The core of the framework is to use the beam pattern (BP) deviation caused by the device-specific gain error of the antenna array as a unique authentication feature. Under this framework, multiple spatially distributed cooperative nodes (UEs) first make local binary decisions based on the observed BP deviations, and then send these decision information to a Fusion Center (FC). The study specifically designed a low-complexity hybrid combination fusion rule suitable for the fully connected structure of mmWave MIMO, which is used to efficiently aggregate local decisions at the FC and make the final authentication decision. The paper also conducted rigorous theoretical performance analysis, derived closed-form expressions for detection probability and false alarm probability, analyzed the asymptotic performance under large-scale antenna arrays, and optimized the digital signaling matrix for transmitting local decisions through the principle of maximizing the offset coefficient to enhance authentication performance. Finally, performance evaluation verifies the superiority of the DPLA framework over benchmark methods in terms of robustness and efficiency.

V. Hybrid Feature-Based PLA in mmWave Systems

To overcome the limitations of single features in specific scenarios, fusing multiple orthogonal or complementary physical layer features and adopting more advanced authentication architectures have become the mainstream trends in current research.

A. Hybrid Feature-Based Authentication in Quasi-Static Environments

Zhang et al. aimed to improve the reliability of PLA in mmWave communication systems to effectively resist identity forgery attacks [69]. The study first conducted in-depth analysis and derived the statistical characteristics of radiation pattern distortion caused by random device errors of antenna arrays (including gain, phase, and element position errors), proving that the Beckmann distribution and Rice distribution can effectively characterize this distortion. Based on this, they designed a high-reliability PLA scheme: the scheme fuses these three array error features to enhance the distinguishability of device fingerprints, and innovatively adopts a constructive Two-Beam Transmission strategy to resist the blockage vulnerability of mmWave links and improve the overall reliability of the authentication process. The paper also established a comprehensive theoretical analysis framework

based on the Rice distribution approximation model, deriving closed-form expressions for detection probability and false alarm probability. Finally, extensive numerical simulations verify the effectiveness and reliability of the proposed scheme, and comparisons with benchmark methods highlight the performance gains brought by fusing multi-dimensional array error features and adopting two-beam transmission.

B. Hybrid Feature-Based Authentication in Dynamic Environments

Teng et al. proposed an enhanced two-factor identity authentication framework to address the PLA problem in mmWave MIMO systems [70], especially the performance limitations of existing single-factor or simple two-factor authentication schemes. The framework innovatively combines two physical features from different sources: one is the Mutual Coupling (MC) effect caused by antenna array device impairments, and the other is the spatial Angle of Arrival (AoA) feature related to the propagation environment. To effectively fuse these two features to exert synergistic advantages, the study adopted the Linear Weighted Combination (LWC) method to fuse the decision statistics of the two features. One of the key contributions of the paper is that to maximize authentication performance, they established an optimization problem aimed at finding the optimal feature weights to maximize the detection probability under a given false alarm probability constraint. In addition, the study also provided rigorous theoretical performance analysis, deriving closed-form analytical expressions for the detection probability (P_d) and false alarm probability (P_f) of the proposed LWC scheme. Finally, numerical simulation results verify the accuracy of the theoretical analysis and prove that the optimized weighted two-factor authentication scheme has superior performance in device identity verification compared with existing methods.

Liu et al. proposed a novel authentication scheme fusing fine-grained channel features and device features for the PLA problem in mmWave MIMO communication systems [71], aiming to effectively resist identity forgery and spoofing attacks. The core innovation of the scheme is to jointly utilize the unique and refined angular domain features of mmWave channels—specifically including Azimuth Angle of Arrival (AAoA), Elevation Angle of Arrival (EAoA), and channel gain—and combine them with the inherent phase noise feature of device. To accurately evaluate these features, the study developed an effective feature evaluation method based on the Limiting Posterior Bayesian Cramér-Rao Bound (LPBCRB) and Maximum Likelihood (ML) estimation theory. In terms of authentication performance analysis, the paper applies statistical signal processing and hypothesis testing theory to derive closed-form expressions for the false alarm probability (P_f) and detection probability (P_d) of the scheme. Finally, extensive numerical simulations verify the accuracy of the proposed theoretical model and demonstrate the effectiveness of the authentication scheme in resisting identity forgery attacks.

Finally, to provide a holistic perspective and facilitate scheme selection, Table II qualitatively compares the three primary technical routes discussed in this survey: channel-based, device-based, and hybrid authentication. It outlines the core physical parameters, key advantages, limitations, and typical application scenarios for each category.

VI. Conclusion

This paper systematically reviews the PLA technology in mmWave MIMO communication systems. The unique physical characteristics of mmWave communication provide abundant feature sources for PLA, mainly forming three technical routes: channel feature-based, device impairment-based, and hybrid multi-feature authentication. We detailedly analyze various cutting-edge technical schemes using channel sparsity, beam pattern deviation, and their combination. The analysis shows that single-feature schemes have limitations in specific scenarios, while hybrid multi-feature fusion and advanced authentication architectures (such as distributed and tracking-based) are the most promising research directions.

Looking forward, this field still faces many challenges, which also indicate new research opportunities:

A. Robust Authentication via Deep Learning

In high-speed mobile scenarios such as autonomous driving (V2X) and Unmanned Aerial Vehicle (UAV), channel features change drastically and non-linearly. Although tracking-based schemes have emerged, there is a need for more advanced prediction algorithms. Future work should explore lightweight deep learning models (e.g., LSTM, Transformer) to capture the temporal correlation of time-varying channels, ensuring robust authentication continuity under high-dynamic conditions.

B. Lightweight and Zero-Overhead Design

With the massive deployment of IoT devices in 6G, computational efficiency is paramount. Future algorithms must prioritize low complexity. Distributed Physical Layer Authentication (DPLA) is a promising direction to offload computational burdens. Furthermore, to minimize signaling overhead, authentication can be embedded directly into the Beam Training process. By utilizing the beamspace response collected during the Sector-Level Sweep (SLS) as a dynamic fingerprint, systems can achieve "zero-overhead" authentication against Initial Access (IA) attacks. Recent work has demonstrated the feasibility of this approach by exploiting beam pattern features to achieve robust identification with minimal overhead [72].

C. Authentication in Emerging 6G Architectures

The diverse architectures of 6G introduce new security paradigms. First, Intelligent Reflecting Surface (IRS) enables "Active Environment Construction," allowing systems to proactively reshape propagation environments to create unique fingerprints in static scenarios. Second, Integrated Sensing and Communication (ISAC) has emerged as a key enabler for 6G. Recent surveys indicate that ISAC-derived sensing parameters can serve as novel authentication features [73]. Furthermore, frameworks combining ISAC with Semantic Communication are being explored to enhance security at the semantic level [74]. Third, as networks expand to Space-Air-Ground Integrated Networks (SAGIN), security boundaries

TABLE II: Summary and Comparison of Physical Layer Authentication Feature Categories

Feature Category	Core Physical Parameters	Key Advantages	Limitations	Typical Scenarios
Channel-Based	CIR, CFR, AoA/AoD, RSS, Beamspace Sparsity	Sensitive to environment; Resists remote spoofing	Unstable in high mobility; Vulnerable to co-located attacks	Fixed Wireless Access; Low-mobility users
Device-Based	Phase Noise, CFO, I/Q Imbalance, PA Nonlinearity	Hardware-intrinsic (Unclonable); High stability over time	Requires high SNR to extract; Sensitive to temperature	High-security IoT; Short-range authentication
Hybrid Features	Spatial-Hardware Joint Vector; (e.g., AoA + Phase Noise)	Strongest overall robustness; Complementary security	High computational complexity; Large training data required	Mission-critical comms; Military/UAV networks

extend to satellite links. Recent research has explored covert communication in satellite-terrestrial systems via beamforming and jamming [75]. Drawing from this, future research should explore integrating PLA with such covert transmission strategies to build a comprehensive security shield for non-terrestrial networks.

D. Cross-Layer Joint Security Architecture

Given the probabilistic nature of physical layer features, PLA should not function as a standalone silo but rather as the first line of defense. Future frameworks should prioritize cross-layer designs that balance security and latency. For instance, PLA can provide continuous, low-latency monitoring; upon detecting a drop in fingerprint confidence, the system can trigger a rigorous upper-layer cryptographic re-authentication process. This hierarchical approach ensures robust security without compromising the ultra-low latency requirements of 6G applications.

REFERENCES

[1] Lalit Chettri and Rabindranath Bera. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet Things J.*, 7(1):16–32, Feb. 2020.

[2] David López-Pérez, Antonio De Domenico, Nicola Piovesan, Geng Xinli, Harvey Bao, Song Qitao, and Mérouane Debbah. A survey on 5G radio access network energy efficiency: Massive MIMO, lean carrier design, sleep modes, and machine learning. *IEEE Commun. Surveys Tuts.*, 24(1):653–697, 2022.

[3] Yunzheng Tao, Long Liu, Shang Liu, and Zhi Zhang. A survey: Several technologies of non-orthogonal transmission for 5G. *China Commun.*, 12(10):1–15, 2015.

[4] Afif Osseiran, Federico Boccardi, Volker Braun, Katsutoshi Kusume, Patrick Marsch, Michal Maternia, Olav Queseth, Malte Schellmann, Hans Schotten, Hidekazu Taoka, et al. Scenarios for 5G mobile and wireless communications: The vision of the METIS project. *IEEE Commun. Mag.*, 52(5):26–35, May 2014.

[5] Dinh C Nguyen, Ming Ding, Pubudu N Pathirana, Aruna Seneviratne, Jun Li, Dusit Niyato, Octavia Dobre, and H Vincent Poor. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.*, 9(1):359–383, Jan. 2022.

[6] Shilpa Talwar, Nageen Himayat, Hosein Nikopour, Feng Xue, Geng Wu, and Vida Ilderem. 6G: Connectivity in the era of distributed intelligence. *IEEE Commun. Mag.*, 59(11):45–50, Nov. 2021.

[7] Yao-Chun Shen, Xing-Yu Yang, and Zi-Jian Zhang. Broadband terahertz time-domain spectroscopy and fast FMCW imaging: Principle and applications. *Chin. Phys. B*, 29(7):078705, 2020.

[8] Anum Ali, Nuria Gonzalez-Prelcic, Robert W Heath, and Amitava Ghosh. Leveraging sensing at the infrastructure for mmwave communication. *IEEE Commun. Mag.*, 58(7):84–89, Jul. 2020.

[9] Xiaohu You, Cheng-Xiang Wang, Jie Huang, Xiqi Gao, Zaichen Zhang, Mao Wang, Yongming Huang, Chuan Zhang, Yanxiang Jiang, Jiaheng Wang, et al. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. *Sci. China Inf. Sci.*, 64(1):110301, 2021.

[10] Rabia Khan, Pardeep Kumar, Dushantha Nalin K Jayakody, and Madhusanka Liyanage. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun. Surveys Tuts.*, 22(1):196–248, 2020.

[11] Akashah Arshad, Zurina Mohd Hanapi, Shamala Subramaniam, and Rohaya Latip. A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. *PeerJ Comput. Sci.*, 7:e673, 2021.

[12] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang. Trust-based attack and defense in wireless sensor networks: A survey. *Wireless Commun. Mobile Comput.*, 2020(1):2643546, 2020.

[13] Amol Vasudeva and Manu Sood. Survey on Sybil attack defense mechanisms in wireless ad hoc networks. *J. Netw. Comput. Appl.*, 120:78–118, 2018.

[14] René Mayrhofer and Stephan Sigg. Adversary models for mobile device authentication. *ACM Comput. Surv.*, 54(9):1–35, 2021.

[15] Qiang Xu, Rong Zheng, Walid Saad, and Zhu Han. Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Commun. Surveys Tuts.*, 18(1):94–104, 2016.

[16] Aakanksha Tewari and Brij B Gupta. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *Int. J. Adv. Intell. Paradigms*, 9(2-3):111–121, 2017.

[17] Ning Xie, Zhuoyuan Li, and Haijun Tan. A survey of physical-layer authentication in wireless communications. *IEEE Commun. Surveys Tuts.*, 23(1):282–310, 2021.

[18] Peng Cheng, Zhuo Chen, Frank de Hoog, and Chang Kyung Sung. Sparse blind carrier-frequency offset estimation for OFDMA uplink. *IEEE Trans. Commun.*, 64(12):5254–5265, Dec. 2016.

[19] Omar H Salim, Ali A Nasir, Hani Mehrpouyan, and Wei Xiang. Multi-relay communications in the presence of phase noise and carrier frequency offsets. *IEEE Trans. Commun.*, 65(1):79–94, Jan. 2017.

[20] Antonio A D'Amico, Leonardo Marchetti, Michele Morelli, and Marco Moretti. Frequency estimation in OFDM direct-conversion receivers using a repeated preamble. *IEEE Trans. Commun.*, 64(3):1246–1258, Mar. 2016.

[21] Antonios Pitarokoilis, Emil Björnson, and Erik G Larsson. ML detection in phase noise impaired SIMO channels with uplink training. *IEEE Trans. Commun.*, 64(1):223–235, Jan. 2016.

[22] Hani Mehrpouyan, Ali A Nasir, Steven D Blostein, Thomas Eriksson, George K Karagiannidis, and Tommy Svensson. Joint estimation of channel and oscillator phase noise in MIMO systems. *IEEE Trans. Signal Process.*, 60(9):4790–4807, Sep. 2012.

[23] Mohsen Rezaee, Peter J Schreier, Maxime Guillaud, and Bruno Clerckx. A unified scheme to achieve the degrees-of-freedom region of the MIMO interference channel with delayed channel state information. *IEEE Trans. Commun.*, 64(3):1068–1082, Mar. 2016.

[24] Hannan Lohrasbipeydeh, T Aaron Gulliver, and Hamidreza Amindavar. Unknown transmit power RSS-based source localization with sensor position uncertainty. *IEEE Trans. Commun.*, 63(5):1784–1797, May 2015.

[25] Daniel B Faria and David R Cheriton. Detecting identity-based attacks in wireless networks using signalprints. In *Proc. 5th ACM Workshop Wireless Secur. (WiSe)*, pages 43–52, Los Angeles, CA, USA, Sep. 2006.

[26] Jitendra K Tugnait and Hyosung Kim. A channel-based hypothesis testing approach to enhance user authentication in wireless networks. In *Proc. 2nd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, pages 1–9, Bangalore, India, Jan. 2010.

[27] Fiona Jiazi Liu, Xianbin Wang, and Helen Tang. Robust physical layer authentication using inherent properties of channel impulse response. In *Proc. IEEE MILCOM*, pages 538–542, Baltimore, MD, USA, Nov. 2011.

[28] Fiona Jiazi Liu, Xianbin Wang, and Serguei L Primak. A two-dimensional quantization algorithm for CIR-based physical layer authentication. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 4724–4728, Budapest, Hungary, Jun. 2013.

[29] Jiazi Liu and Xianbin Wang. Physical layer authentication enhancement using two-dimensional channel quantization. *IEEE Trans. Wireless Commun.*, 15(6):4171–4182, Jun. 2016.

[30] Pinchang Zhang, Jinxiao Zhu, Yin Chen, and Xiaohong Jiang. End-to-end physical layer authentication for dual-hop wireless networks. *IEEE Access*, 7:38322–38336, 2019.

[31] Liang Xiao, Larry Greenstein, Narayan Mandayam, and Wade Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 4646–4651, Glasgow, UK, Jun. 2007.

[32] Liang Xiao, Larry J Greenstein, Narayan B Mandayam, and Wade Trappe. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wireless Commun.*, 7(7):2571–2579, Jul. 2008.

[33] Liang Xiao, Larry Greenstein, Narayan Mandayam, and Wade Trappe. MIMO-assisted channel-based authentication in wireless networks. In *Proc. 42nd Annu. Conf. Inf. Sci. Syst. (CISS)*, pages 642–646, Princeton, NJ, USA, Mar. 2008.

[34] Paolo Baracca, Nicola Laurenti, and Stefano Tomasin. Physical layer authentication over MIMO fading wiretap channels. *IEEE Trans. Wireless Commun.*, 11(7):2564–2573, Jul. 2012.

[35] Fangming He, Hong Man, Didem Kivanc, and Bruce McNair. EPSON: Enhanced physical security in OFDM networks. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 1–5, Dresden, Germany, Jun. 2009.

[36] Fangming He, Wei Wang, and Hong Man. REAM: Rake receiver enhanced authentication method. In *Proc. IEEE MILCOM*, pages 2205–2210, San Jose, CA, USA, Oct. 2010.

[37] Steven J Fortune, David M Gay, Brian W Kernighan, Orlando Landron, Reinaldo A Valenzuela, and Margaret H Wright. Wise design of indoor wireless systems: Practical computation and optimization. *IEEE Comput. Sci. Eng.*, 2(1):58–68, 1995.

[38] Liang Xiao, Larry J Greenstein, Narayan B Mandayam, and Wade Trappe. Channel-based spoofing detection in frequency-selective Rayleigh channels. *IEEE Trans. Wireless Commun.*, 8(12):5948–5956, Dec. 2009.

[39] Ning Wang, Ting Jiang, Shichao Lv, and Liang Xiao. Physical-layer authentication based on extreme learning machine. *IEEE Commun. Lett.*, 21(7):1557–1560, Jul. 2017.

[40] Andreas Weinand, Michael Karrenbauer, Raja Sattiraju, and Hans Schotten. Application of machine learning for channel based message authentication in mission critical machine type communication. In *Proc. 23rd Eur. Wireless Conf. (EW)*, pages 1–5, Dresden, Germany, May 2017.

[41] Fei Pan, Zhibo Pang, Hong Wen, Michele Luvisotto, Ming Xiao, Run-Fa Liao, and Jie Chen. Threshold-free physical layer authentication based on machine learning for industrial wireless CPS. *IEEE Trans. Ind. Informat.*, 15(12):6481–6491, Dec. 2019.

[42] Qian Wang, Hang Li, Zhi Chen, Dou Zhao, Shuang Ye, and Jiansheng Cai. Supervised and semi-supervised deep neural networks for CSI-based authentication. *arXiv preprint arXiv:1807.09469*, 2018.

[43] Caidan Zhao, Minmin Huang, Lianfen Huang, Xiaojiang Du, and Mohsen Guizani. A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. *Comput. Netw.*, 128:164–171, Dec. 2017.

[44] Ning Xie, Wei Xiong, Junjie Chen, Peichang Zhang, Lei Huang, and Jian Su. Multiple phase noises physical-layer authentication. *IEEE Trans. Commun.*, 70(9):6196–6211, Sep. 2022.

[45] Weikun Hou, Xianbin Wang, and Jean-Yves Chouinard. Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 3559–3563, Ottawa, ON, Canada, Jun. 2012.

[46] Weikun Hou, Xianbin Wang, Jean-Yves Chouinard, and Ahmed Refaey. Physical layer authentication for mobile systems with time-varying carrier frequency offsets. *IEEE Trans. Commun.*, 62(5):1658–1667, May 2014.

[47] Sepideh Dolatshahi, Adam Polak, and Dennis L Goeckel. Identification of wireless users via power amplifier imperfections. In *Proc. 44th Asilomar Conf. Signals, Syst. Comput.*, pages 1553–1557, Pacific Grove, CA, USA, Nov. 2010.

[48] Adam C Polak, Sepideh Dolatshahi, and Dennis L Goeckel. Identifying wireless users via transmitter imperfections. *IEEE J. Sel. Areas Commun.*, 29(7):1469–1479, Aug. 2011.

[49] Adam C Polak and Dennis L Goeckel. Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion. *IEEE Trans. Wireless Commun.*, 14(11):5889–5899, Nov. 2015.

[50] Muhammad Mahboob Ur Rahman, Aneela Yasmeen, and James Gross. PHY layer authentication via drifting oscillators. In *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pages 716–721, Austin, TX, USA, Dec. 2014.

[51] Libor Polčák, Jakub Jirásek, and Petr Matoušek. Comment on 'remote physical device fingerprinting'. *IEEE Trans. Dependable Secure Comput.*, 11(5):494–496, Sep. 2014.

[52] Suman Jana and Sneha Kumar Kasera. On fast and accurate detection of unauthorized wireless access points using clock skews. In *Proc. 14th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, pages 104–115, San Francisco, CA, USA, Sep. 2008.

[53] Marius Cristea and Bogdan Groza. Fingerprinting smartphones remotely via ICMP timestamps. *IEEE Commun. Lett.*, 17(6):1081–1083, Jun. 2013.

[54] Peng Hao, Xianbin Wang, and Aydin Behnad. Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 939–944, Sydney, NSW, Australia, Jun. 2014.

[55] Peng Hao, Xianbin Wang, and Aydin Behnad. Relay authentication by exploiting I/Q imbalance in amplify-and-forward system. In *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pages 613–618, Austin, TX, USA, Dec. 2014.

[56] Kunal Sankhe, Mauro Belgiovine, Fan Zhou, Shamnaz Riyaz, Stratis Ioannidis, and Kaushik Chowdhury. ORACLE: Optimized radio classification through convolutional neural networks. In *Proc. IEEE INFOCOM*, pages 370–378, Paris, France, Apr. 2019.

[57] I Chih-Lin, Corbett Rowell, Shuangfeng Han, Zhikun Xu, Gang Li, and Zhengang Pan. Toward green and soft: A 5G perspective. *IEEE Commun. Mag.*, 52(2):66–73, Feb. 2014.

[58] Ibrahim A Hemadeh, Katla Satyanarayana, Mohammed El-Hajjar, and Lajos Hanzo. Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget. *IEEE Commun. Surveys Tuts.*, 20(2):870–913, 2018.

[59] Dalia Nandi and Animesh Maitra. Study of rain attenuation effects for 5G mm-wave cellular communication in tropical location. *IET Microw., Antennas Propag.*, 12(9):1504–1507, 2018.

[60] Wenyan Ma, Chenhao Qi, Zaichen Zhang, and Julian Cheng. Sparse channel estimation and hybrid precoding using deep learning for millimeter wave massive MIMO. *IEEE Trans. Commun.*, 68(5):2838–2849, May 2020.

[61] Baibhab Chatterjee, Debayan Das, Shovan Maity, and Shreyas Sen. RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet Things J.*, 6(1):388–398, Feb. 2019.

[62] Jie Tang, Aidong Xu, Yixin Jiang, Yunan Zhang, Hong Wen, and Tengyue Zhang. Mmwave MIMO physical layer authentication by using channel sparsity. In *Proc. IEEE Int. Conf. Artif. Intell. Inf. Syst. (ICAIIS)*, pages 221–224, Dalian, China, Mar. 2020.

[63] Liza Afeef, Haji M Furqan, and Hüseyin Arslan. Physical layer authentication scheme in beamspace MIMO systems. *IEEE Commun. Lett.*, 26(7):1484–1488, Jul. 2022.

[64] Mu Niu, Pinchang Zhang, Ji He, Yuanyu Zhang, and Zhiquan Liu. PHY-layer authentication exploiting spatial channel and radiometric signatures for mmwave MIMO systems. *IEEE Commun. Lett.*, 29(9):2108–2112, Sep. 2025.

[65] Yulin Teng, Pinchang Zhang, Xiao Chen, Xiaohong Jiang, and Fu Xiao. PHY-layer authentication exploiting channel sparsity in mmwave MIMO UAV-ground systems. *IEEE Trans. Inf. Forensics Security*, 19:4642–4657, 2024.

[66] Liza Afeef, Haji M Furqan, and Hüseyin Arslan. Robust tracking-based PHY-authentication in mmwave MIMO systems. *IEEE Trans. Inf. Forensics Security*, 2024. Early Access.

[67] Sarankumar Balakrishnan, Shreya Gupta, Arupjyoti Bhuyan, Pu Wang, Dimitrios Koutsonikolas, and Zhi Sun. Physical layer identification based on spatial-temporal beam features for millimeter-wave wireless networks. *IEEE Trans. Inf. Forensics Security*, 15:1831–1845, 2020.

[68] Pinchang Zhang, Keshuang Han, Yuanyu Zhang, Yulong Shen, Fu Xiao, and Xiaohong Jiang. Distributed physical layer authentication framework exploiting array pattern feature for mmwave MIMO systems. *IEEE Trans. Mobile Comput.*, 24(7):6430–6445, Jul. 2025.

[69] Pinchang Zhang, Shuangrui Zhao, Weibei Fan, Yulong Shen, Xiaohong Jiang, and Fu Xiao. Reliable PLA with array error features and two-beam transmission in millimeter-wave communication systems. *IEEE Trans. Inf. Forensics Security*, 20:8760–8772, 2025.

[70] Yulin Teng, Runqing Wang, Ayinuer Nuertai, and Pinchang Zhang. Enhanced two-factor identity authentication for MmWave MIMO systems. *IEEE Signal Process. Lett.*, 32:836–840, 2025.

[71] Yangyang Liu, Pinchang Zhang, Jun Liu, Yulong Shen, and Xiaohong Jiang. Exploiting fine-grained channel/hardware features for PHY-layer authentication in mmwave MIMO systems. *IEEE Trans. Inf. Forensics Security*, 18:4059–4074, 2023.

[72] Pinchang Zhang, Keshuang Han, Yuanyu Zhang, Yulong Shen, Fu Xiao, and Xiaohong Jiang. Physical layer authentication utilizing beam pattern features in millimeter-wave MIMO systems. *IEEE Trans. Dependable Secure Comput.*, 21(1):1–15, 2024.

[73] Xinyi Li, Yan Zhang, Octavia A. Dobre, and H. Vincent Poor. Physical layer security for integrated sensing and communication: A survey. *IEEE Open J. Commun. Soc.*, 2025.

[74] Xidong Mu and Yuanwei Liu. Semantic communication-assisted physical layer security over fading wiretap channels. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 2101–2106. IEEE, 2024.

[75] Zewei Guo, Ranran Sun, Yulong Shen, and Xiaohong Jiang. Covert communication in satellite-terrestrial systems via beamforming and jamming. *IEEE Trans. Veh. Technol.*, 2025.