Endogenous Security Through AI-Driven Physical-Layer Authentication for Future 6G Networks

MENG Rui[1], FAN Dayu[1], XU Xiaodong[1,2], LYU Suyu[3], TAO Xiaofeng[4]

(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Department of Broadband Communication, Peng Cheng Laboratory, Shenzhen 518066, China;
3. School of Information Science and Technology, Beijing University of Technology, Beijing 100124, China;
4. National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China)

DOI: 10.12142/ZTECOM.202501004

https://kns.cnki.net/kcms/detail/34.1294.TN.20250210.1626.004.html, published online February 11, 2025

Manuscript received: 2025-01-09

Abstract: To ensure the access security of 6G, physical-layer authentication (PLA) leverages the randomness and space-time-frequency uniqueness of the channel to provide unique identity signatures for transmitters. Furthermore, the introduction of artificial intelligence (AI) facilitates the learning of the distribution characteristics of channel fingerprints, effectively addressing the uncertainties and unknown dynamic challenges in wireless link modeling. This paper reviews representative AI-enabled PLA schemes and proposes a graph neural network (GNN)-based PLA approach in response to the challenges existing methods face in identifying mobile users. Simulation results demonstrate that the proposed method outperforms six baseline schemes in terms of authentication accuracy. Furthermore, this paper outlines the future development directions of PLA.

Keywords: physical-layer authentication; artificial intelligence; wireless security; intelligent authentication

Citation (Format 1): MENG R, FAN D Y, XU X D, et al. Endogenous security through AI-driven physical-layer authentication for future 6G networks [J]. ZTE Communications, 2025, 23(1): 18 – 29. DOI: 10.12142/ZTECOM.202501004

Citation (Format 2): R. Meng, D. Y. Fan, X. D. Xu, et al., "Endogenous security through AI-driven physical-layer authentication for future 6G networks," *ZTE Communications*, vol. 23, no. 1, pp. 18 – 29, Mar. 2025. doi: 10.12142/ZTECOM.202501004.

1 Introduction

1.1 Background

To further accelerate the realization of the Internet of Everything, 6G mobile networks will integrate a multitude of enabling technologies, with a goal of achieving extensive coverage, high bandwidth, low latency, and highly reliable communications[1]. Currently, the official launch of the first 6G standard project by the 3rd Generation Partnership Project (3GPP) marks the transition of 6G from technical pre-research to the standardization phase, signaling the start of a critical period for blueprint formulation. However, as an emerging technology, 6G will introduce more complex security challenges[2 – 3]. The future three-dimensional and fully integrated communication network, characterized by diverse, resilient, and distributed topologies, involves numerous heterogeneous nodes, dynamic resource management, and ubiquitous diverse connections, thereby increasing network complexity and security risks[4 – 5]. While various enabling technologies offer numerous potential advantages and application prospects, they also introduce certain security problems[6]. For example, attackers can exploit user interference caused by a vast number of antennas and devices in ultra-massive multi-input multi-output (UM-MIMO) systems to eavesdrop on and tamper with data. To ensure secure communication and transmission, threat detection and defense, and data confidentiality and integrity in 6G networks, it is crucial to redesign security safeguard mechanisms to achieve intelligent, flexible, and real-time endogenous security.

1.2 Physical-Layer Authentication

As a complement to traditional upper-layer authentication protocols, physical-layer authentication (PLA), with its high reliability, lightweight design, and exceptional compatibility, is considered an endogenous security protection strategy[7]. Primarily, the characteristics of physical-layer attributes, based on the inherent randomness of channels and the uniqueness of space-time-frequency, which are closely related to communication links, devices, and locations, can represent unique identity signatures for legitimate users, making it extremely difficult for attackers to extract, imitate, or forge them[8]. Secondly, PLA cleverly bypasses high-level signaling processes, allowing its access points to obtain the channel state information (CSI) of legitimate users during the channel estimation phase, significantly reducing computational resource consumption[9]. Furthermore, even if incompatible devices may face obstacles in decoding each other's upper-layer signaling, they can still successfully parse the bit stream at the physical-layer, further broadening the application and flexibility[10].

Recently, a growing number of researchers have designed artificial intelligence (AI)-empowered PLA methods to effectively address the uncertainty and unknown dynamic challenges in wireless link modeling[11]. Advanced machine learning (ML) algorithms can intelligently learn the distribution characteristics of channel fingerprints and optimize the authentication threshold in dynamic environments, achieving adaptive online authentication[12]. Additionally, unsupervised learning algorithms help build a malicious node detection model without prior knowledge of the attacker's location or attack frequency[13]. Furthermore, deep learning (DL) technology excels at learning high-dimensional fingerprint features and classifying a large number of samples, enabling the identification of large-scale or even ultra-large-scale devices[14]. In summary, compared with traditional PLA methods, AI-empowered PLA has several advantages. It overcomes the challenges of modeling the uncertainty and unknown dynamics of wireless links, achieves adaptive threshold authentication, possesses greater universality without needing extensive prior information, exhibits higher scalability, and is capable of identifying ultra-large-scale equipment[15].

1.3 Contributions

The main contributions of this paper are summarized as follows.

1) We review representative AI-based PLA research, which is classified into radio frequency (RF) fingerprint extraction, fingerprint data augmentation, lightweight authentication models, authentication parameter optimization, multi-attacker identification, and physical-layer key generation for frequency-division duplexing (FDD) systems.

2) We propose a graph neural network (GNN)-based PLA scheme to identify mobile multiusers. Unlike most existing convolutional neural network (CNN)-based PLA schemes, the proposed scheme can learn the spatial correlation among various CSI fingerprint dimensions introduced by reconfigurable intelligent surfaces (RISs) through modeling the nodes and edges. Furthermore, the scheme also captures the temporal correlation between fingerprints and within fingerprint sequences through dynamic graphs and temporal convolution learning. The simulations demonstrate the superiority of the proposed scheme over six baseline schemes.

3) We envision the future research direction of intelligent PLA for 6G, including semantic fingerprint-based PLA, large AI model-based PLA, cross-layer PLA, multi-modal signature-based PLA, distributed autonomous PLA, and PLA for emerging applications.

2 Existing AI-Enabled PLA Approaches

In Table 1, we provide a brief review of existing AI-empowered PLA schemes, which is explained in detail below.

2.1 RF Fingerprint Extraction

The extraction of RF fingerprints relies on the hardware variations of transmitters, such as digital-to-analog converters (DAC), in-phase/quadrature (I/Q) modulators, and power amplifiers. These differences result in distinct inherent properties among radiation sources of the same model and batch. Traditional extraction methods often depend on preprocessing techniques, such as time synchronization and phase offset compensation, as well as expert feature transformation meth-

Table 1. Brief review on existing AI-empowered PLA schemes

Categories	Motivations	Methods	Performance
RF fingerprint extraction	The extraction of RF fingerprints requires much prior information	CNN[16], RNN[17], attention mechanism[18], and CVNN[19]	Realizing end-to-end RF fingerprint extraction
Fingerprint data augmentation	Insufficient fingerprint samples lead to overfitting issues of PLA models, thus limiting authentication performance	Added noise-based[20] and generated fingerprint-based[21] schemes	Enhancing the generalization of PLA models
Lightweight authentication model	To identify ultra-large-scale devices, PLA models usually have a large number of parameters and deep structures	Transfer learning-based[22] and network compression-based[23] schemes	Reducing the deployment complexity of PLA models
Authentication parameter optimization	Optimizing detection thresholds is challenging in complex channel environments	RL[24–25]	Achieving the automatic optimization of authentication parameters
Multi-attacker identification	The prior information of multi-attackers is difficult to obtain in actual applications	Clustering[13], OCC[26], and GMM[27]	Realizing authentication without knowing the prior information of attackers
Physical-layer key generation for FDD systems	In FDD systems, uplink and downlink transmissions work in different frequency bands, and their channel frequency responses are no longer reciprocal	Generative AI[28]	Improving the key generation ratio

AI: artificial intelligence
CNN: convolutional neural network
CVNN: complex-valued neural network
FDD: frequency-division duplexing
GMM: Gaussian mixture model
OCC: one class classification
PLA: physical-layer authentication
RL: reinforcement learning
RNN: recurrent neural network

ods like the short-time Fourier transform and wavelet transform. However, these processes require prior information, limiting the practical applicability. In recent years, with the advantages of DL in feature extraction, the acquisition of RF fingerprints gradually overcomes the dependence on prior information and manually optimizing parameters, and only requires preprocessing processes such as normalization and interpolation. DL is realized by neural networks, such as CNN[16], recurrent neural networks (RNN)[17], attention mechanisms[18], and complex-valued neural networks (CVNN)[19].

Specifically, Ref. [16] presents a novel DL-based RF fingerprint identification approach to IoT terminal authentication, leveraging the differential constellation trace figure (DCTF) to extract RF fingerprint features without synchronization. CNN is designed to identify devices using DCTF features. It offers high accuracy, requires no prior information, and maintains low complexity. Ref. [17] explores RNNs for autonomous wireless system deployments in RF environments. By utilizing the temporal properties of received radio signals, Ref. [17] proposes a transmitter fingerprinting technique for device identification. Ref. [17] implements three RNN models, namely Long Short-Term Memory (LSTM), the Gated Recurrent Unit (GRU), and ConvLSTM, using I/Q time series data collected from eight universal software radio peripheral (USRP) software defined radio (SDR) transmitters. By exploiting temporal variations and spatial dependencies in the data, the model learns unique feature representations for transmitter identification. Ref. [18] presents a novel multi-channel attentive feature fusion method for RF fingerprinting. Unlike other models that rely on a single representation of radio signals, the proposed method integrates multiple representations, such as in-phase and quadrature samples, carrier frequency offsets, and frequency transform coefficients. By employing a shared attention module, Ref. [18] adaptively fuses neural features extracted from these different channels, optimizing their weights during training. Additionally, a convolution-based ResNeXt block is implemented to map the fused features to specific device identities. Given that wireless signal information is encoded in complex basebands, Ref. [19] studies the application of CVNNs to develop device fingerprints through supervised learning.

2.2 Fingerprint Data Augmentation

The training of DL-based PLA models usually requires a large number of fingerprint samples. However, it is challenging to obtain sufficient fingerprint samples in practical applications. To address this issue, data augmentation is an effective approach to enhancing the model generalization and improving the authentication accuracy. We divide the existing fingerprint data augmentation schemes into two subcategories: added noise-based[20] and generated fingerprint-based[22] schemes. The former employs Gaussian noises to mitigate model overfitting, while the latter enhances sample richness by generating additional fingerprint samples.

Specifically, Ref. [20] aims to enhance authentication performance with minimal training data by applying Gaussian noises in a smooth latent space, thus improving generalization and interpretability. The proposed scheme avoids reliance on synthetic samples while providing insights into the authentication process through the defined Fingerprint Library. This allows for a better understanding of how input channel impulse responses (CIRs) correlate with authentication outcomes. Ref. [21] employs three data augmentation algorithms to expedite the model establishment and improve authentication success rates. By integrating deep neural networks with these augmentation methods, the scheme not only enhances performance but also accelerates training, even with limited samples.

2.3 Lightweight Authentication Model

To realize the identification of ultra-large-scale devices, authentication models typically possess a large number of parameters and deep structures to learn multi-level and abstract fingerprint features. To reduce the computation and storage requirements of the PLA model without sacrificing most performance, researchers have designed transfer learning-based[22] and network compression-based[21] PLA schemes. The former can quickly identify the physical-layer fingerprints of different equipment types in unknown radio environments with only a few training samples through a pre-trained model[22]. For example, Ref. [22] introduces transfer learning to realize swift online user authentication, crucial for latency-sensitive applications like edge computing. The latter employs lightweight technologies, such as quantization, grouping convolution, and distillation, to reduce the parameters and calculation of PLA models. For instance, Ref. [23] introduces network compression techniques to reduce the model complexity and size. Despite the high model complexity and size of CVNNs, the proposed approach ensures satisfactory identification performance.

2.4 Authentication Parameter Optimization

PLA is typically modeled as a hypothesis testing problem, where the authentication result is obtained by comparing the difference between the signal to be authenticated and a reference signal with a detection threshold. Therefore, optimizing the detection threshold is crucial for authentication performance. Due to complex multipath effects, time-varying characteristics of channels, noise interference, and other factors, deriving the detection threshold becomes increasingly difficult. To address this issue, RL, through continuous interaction with the environment, can learn how to make optimal authentication decisions without fully understanding the channel model. Ref. [24] frames the interactions between a legitimate receiver and spoofers as a zero-sum authentication game. The receiver adjusts its test threshold to maximize utility based on the Bayesian risk in spoofing detection, while spoofers aim to minimize this utility by varying their attack frequencies. Since obtaining precise channel parameters beforehand is challenging, Ref. [24] introduces spoofing detection schemes based on Q-learning and Dyna-Q. These schemes leverage RL to determine the optimal test threshold for spoofing detection. Ref. [25] presents a novel controller area network (CAN) bus authentication framework designed to protect message exchanges against spoofing attacks. The proposed framework leverages RL to optimize the selection of authentication modes and parameters. By implementing the Dyna architecture with the double estimator, the framework enhances authentication accuracy without necessitating changes to the CAN bus protocol or electronic control unit components.

2.5 Multi-Attacker Identification

For detection attack scenarios, a suitable assumption is that the attackers' prior information is unknown, and often multi-attackers are present to confuse legitimate receivers. To address this challenge, unsupervised learning can construct an authentication model without requiring the attackers' prior information or training fingerprint set. By establishing decision boundaries, the detection of multi-attackers is achieved. Ref. [13] proposes a multi-attribute-based approach that considers the inherent correlation among physical-layer attributes. To manage the exponential computational complexity of correlated analysis, Ref. [13] introduces a reconstruction and heuristic algorithm to find a suboptimal solution with reduced complexity. An unsupervised machine learning-based non-parametric clustering algorithm is proposed to enhance authentication reliability. The proposed approach does not require prior information or a training set, thereby improving its universality. Ref. [26] assesses and compares the performance of various approaches under different channel conditions. Ref. [26] evaluates statistical decision methods and ML classification techniques, including one-class classifiers for scenarios with no forged messages or conventional binary classifiers when forged messages are present. Numerical results demonstrate that one-class classification algorithms achieve the lowest missed detection probability under low spatial correlation. Ref. [27] utilizes GMMs to identify spoofing attackers by clustering messages based on probabilistic models of different transmitters. A 2D feature measure space is used to preprocess channel information, and a pseudo adversary model is developed to enhance detection performance against spoofers operating through unknown channels.

2.6 Physical-Layer Key Generation for FDD Systems

Physical-layer key generation offers a robust and efficient method for secure key generation by leveraging the unique properties of wireless channels. Exploiting the reciprocity and time-varying nature of these channels ensures that both communicating parties can generate identical keys with minimal communication overhead and hardware requirements. The implementation of physical-layer key generation relies on the reciprocity of channels. However, in FDD systems, the uplink (from a user to a base station) and downlink (from a base station to a user) operate on separate frequency bands. This duplexing method allows for simultaneous uplink and downlink communications, but it also introduces a frequency difference. The properties of the wireless channel, such as path loss, shadowing, and multipath effects, are functions of frequency. Consequently, the frequency difference disrupts the channel reciprocity. To address this issue, generative AI is a promising approach. Ref. [28] introduces a novel physical-layer key generation scheme for FDD systems, addressing the challenges of extracting common features in non-reciprocal channels, and employs DL to create a feature mapping function between different frequency bands, enabling two users to generate highly similar channel features. Ref. [28] also proves the existence of a band feature mapping function using a feedforward network with a single hidden layer and proposes a key generation neural network for reciprocal channel feature construction.

3 Proposed PLA Scheme for Mobile Users

This section provides the GNN-based PLA to identify mobile users, including the research motivation, networks and channel models, problem formulation, research methods, and simulation results.

3.1 Motivation

The accuracy and reliability of CSI fingerprints are crucial for PLA. However, their quality is often constrained in some scenarios such as the Industrial Internet of Things (IIoT) due to multipath fading, obstacle interferences, and complex electromagnetic environments. To tackle this issue, RIS intelligently adjusts the wireless propagation environment, significantly boosting the expected signal power at the receiver[29]. Nevertheless, existing CNN-based PLA models frequently overlook the potential interdependencies among various CSI dimensions. With the integration of RIS, the wireless environment has transformed, resulting in a strong correlation among diverse dimensional features of CSI fingerprints. Hence, the primary challenge lies in fully extracting the intrinsic features of these reconfigurable channel fingerprints.

Furthermore, in certain scenarios, smart devices are frequent in motion. For example, mobile terminals in logistics and production lines augment efficiency and flexibility, while unmanned vehicles and mobile robots engaged in data collection and monitoring tasks enhance real-time analysis and decision-making capabilities. Since CSI is a location-specific physical-layer attribute, user movement alters the distribution of CSI, with greater deviations as the distance from the transmitter increases[30]. Consequently, leveraging CSI-based PLA methods to identify mobile users poses another significant challenge.

To address the first challenge, we deployed GNNs to capture the dependencies and topological structures among various CSI dimensions introduced by the RIS. Existing CNN-based PLA models frequently neglect the underlying dependency relationships among different CSI dimensions. In addition, RNNs have certain limitations in handling sequence data, particularly long sequences, which restricts their ability to capture long-term dependencies. In contrast, GNNs, through the connections of nodes and edges, can naturally capture the correlations among multi-dimensional channel features. These direct or indirect correlations are transmitted through paths between nodes. For example, Ref. [31] models MIMO CSI prediction as a multivariate time-series forecasting problem and introduces GNNs to exploit both spectral and temporal correlations between historical and future CSI.

To tackle the second issue, we formulated the variations of CSI fingerprints in mobile scenarios as time series. We then integrated temporal convolution networks and dynamic GNNs to fully exploit the temporal correlations both among CSI samples and within sequences of CSI samples. Unlike static GNNs, dynamic GNNs can capture both spatial and temporal dependencies among variables and excel at processing multivariate time series data.

3.2 Network Model

As depicted in Fig. 1, we consider a multiuser access authentication scenario, wherein K users engage in communication with the receiver (Bob) across distinct time slots. Given that users are in constant motion, the distance between them is assumed to exceed half a wavelength, ensuring the uniqueness of their fingerprints. To bolster signal strength and broaden coverage, RISs are utilized to redirect the incident signal toward the target area by adjusting the reflected signal. This enhances the quality of channel fingerprints in areas affected by signal blind spots or weak signal reception. Notably, RISs are controlled by Bob. Additionally, edge servers stationed at Bob's location are leveraged to optimize the deployment performance of AI-driven PLA models.

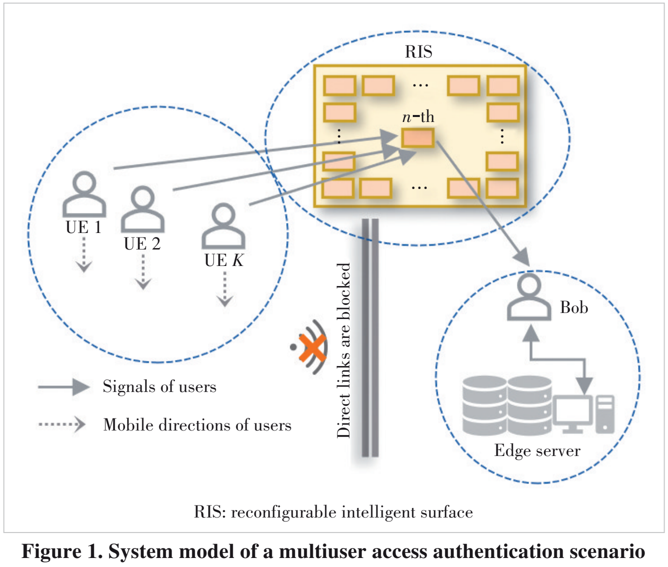


Figure 1. System model of a multiuser access authentication scenario

3.3 Channel Model

N_T and N_R represent the numbers of antennas of each user and of Bob, and the received signal at Bob can be denoted as:

$$\boldsymbol{Y}_S = \boldsymbol{Q}\boldsymbol{X}_S + \boldsymbol{W} \quad (1),$$

where $\boldsymbol{X}_S$ with N_T-size column denotes the transmitted signal, and $\boldsymbol{W} \sim \mathcal{CN}(0,\boldsymbol{\sigma}^2)$ with N_R-size column denotes Gaussian noises. $\boldsymbol{Q} = \boldsymbol{H}\boldsymbol{\Psi}\boldsymbol{G} \in \mathbb{C}^{N_R \times N_T}$ represents the hierarchical channel matrix from the user to Bob through RISs, where $\boldsymbol{H} \in \mathbb{C}^{N_R \times N}$ and $\boldsymbol{G} \in \mathbb{C}^{N \times N_T}$ respectively stand for the channel matrices from RISs to Bob and from the user to RISs, and $\boldsymbol{\Psi} = \mathrm{diag}\left(\boldsymbol{\psi}_0,\cdots,\boldsymbol{\psi}_{N-1}\right) \in \mathbb{C}^{N \times N}$ represents the response matrix of RISs with N denoting the number of elements of RISs. $\boldsymbol{\psi}_n = A_n\left(\theta_n\right)e^{j\theta_n}$ with $A_n\left(\theta_n\right)$ and $e^{j\theta_n}$ respectively denoting the controllable magnitude and phase response of the n-th RIS element. $\boldsymbol{H}$ and $\boldsymbol{G}$ are modeled as Rician channels, which are denoted as:

$$\boldsymbol{H} = \sqrt{\frac{PL\kappa_H}{1+\kappa_H}}\bar{\boldsymbol{H}} + \sqrt{\frac{PL}{1+\kappa_H}}\tilde{\boldsymbol{H}} \quad (2),$$

and

$$\boldsymbol{G} = \sqrt{\frac{PL\kappa_G}{1+\kappa_G}}\bar{\boldsymbol{G}} + \sqrt{\frac{PL}{1+\kappa_G}}\tilde{\boldsymbol{G}} \quad (3),$$

where $\bar{\boldsymbol{H}}$ and $\bar{\boldsymbol{G}}$ represent line of sight (LoS) paths, κ_H and κ_G represent Rician factors, and $\tilde{\boldsymbol{H}}$ and $\tilde{\boldsymbol{G}}$ denote non-LoS (NLoS) paths. PL represents the corresponding path loss. The configurable fingerprints $\boldsymbol{x}$ are acquired via channel estimation, which is not the focus of this paper and can be accomplished through various techniques, such as compressed sensing, matrix factorization, and DL methods[32].

3.4 Problem Formulation

Due to the multidimensional nature of complex CSI fingerprints in mobile scenarios, these fingerprints can be represented as multivariate time series $\boldsymbol{X} = \{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_d\} \in \mathbb{R}^{d \times l}$, where $d = 2N_RN_T$ signifies the dimension of CSI fingerprints. Each time series component can be denoted as $\boldsymbol{x}_i = \{\boldsymbol{x}_{i,1},\boldsymbol{x}_{i,2},\cdots,\boldsymbol{x}_{i,l}\}$, where $i = 1,2,\cdots,d$ and $l \in \mathbb{N}^*$ denotes the length of CSI fingerprint sequences. The authentication problem is formulated as a classification task from $\{\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_m\}$ to $\{\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_m\}$, aiming to predict the identity $\boldsymbol{y}$ of the CSI fingerprint sequence $\boldsymbol{X}$. Here, $\{\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_m\}$ corresponds to the identity labels of the CSI fingerprint sequences $\{\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_m\} \in \mathbb{R}^{m \times d \times l}$, with m denoting the number of CSI fingerprint sequences.

3.5 Proposed GNN-Based PLA Scheme

As illustrated in Fig. 2, the proposed PLA scheme includes training and authentication stages. Fig. 3 illustrates the detailed training process, including fingerprint acquisition, fingerprint preprocessing, graph initialization, temporal convolutional networks, dynamic GNN, hierarchical pooling, and authentication result output modules.

3.5.1 Fingerprint Acquisition

As described in Section 3.3, the cascade CSI fingerprints can be acquired through channel estimation. In this paper, artificial noise is considered to verify the authentication performance versus different signal-to-noise ratio (SNR) conditions.

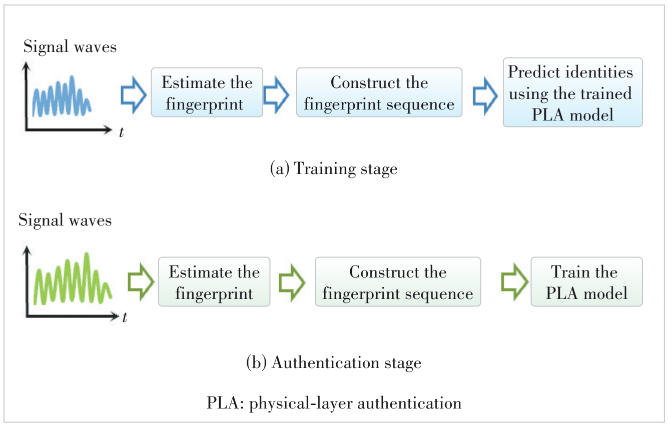
3.5.2 Fingerprint Preprocessing

The training CSI dataset is composed of CSI fingerprints and corresponding identity labels, which are represented as:

$$\boldsymbol{X}_{\text{train}} = \left[\underbrace{\boldsymbol{X}_1^1,\cdots,\boldsymbol{X}_1^{N_1}}_{N_1}, \underbrace{\boldsymbol{X}_2^1,\cdots,\boldsymbol{X}_2^{N_2}}_{N_2}, \cdots, \underbrace{\boldsymbol{X}_K^1,\cdots,\boldsymbol{X}_K^{N_K}}_{N_K} \right] \tag{4},$$

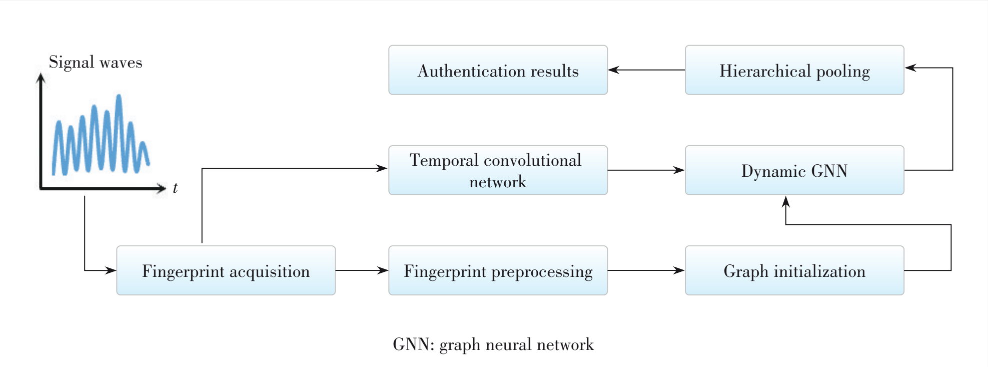
$$\boldsymbol{Y}_{\text{train}} = \left[\underbrace{\boldsymbol{L}_1,\cdots,\boldsymbol{L}_1}_{N_1}, \underbrace{\boldsymbol{L}_2,\cdots,\boldsymbol{L}_2}_{N_2}, \cdots, \underbrace{\boldsymbol{L}_K,\cdots,\boldsymbol{L}_K}_{N_K} \right] \tag{5},$$

where N_k denotes the number of CSI sequences of the k-th user, $k \in [1,K]$, and $\boldsymbol{L}_k$ represents the corresponding identity label encoded by one-hot coding[33].



PLA: physical-layer authentication

Figure 2. Proposed PLA approach



GNN: graph neural network

Figure 3. Steps of the proposed GNN-based scheme

3.5.3 Graph Initialization

Nodes and edges collectively form the core structure of a graph, typically denoted as $\mathcal{G} = (\mathcal{V}, \mathcal{E})$[34]. Nodes $\mathcal{V}$, serving as the fundamental building blocks of a graph, represent entities or objects within the graph, specifically the CSI fingerprint sequences of users. Edges $\mathcal{E}$ play the pivotal role of bridges connecting nodes, revealing the correlations and interactions among them. Edges $\mathcal{E}$ can be either directed or undirected, and may even be assigned weights to quantify the strength or importance of the relationships between nodes $\mathcal{V}$.

The essence of GNNs lies in deeply extracting the representations of nodes and edges. Through continuous learning and updating of node features, more enriched and insightful node representations can be generated. Leveraging the connectivity among nodes and the characteristic information of edges, operations such as message passing and graph structure learning are conducted, further extracting the global features of the graph.

The relationships between various nodes are represented through adjacency matrices, where each node is assigned two values representing the source node and the target node[35]. Consequently, each time series corresponds to two vectors, $\boldsymbol{\lambda}$ and $\boldsymbol{\varphi}$, both with the length of d. The values of $\boldsymbol{\lambda}$ and $\boldsymbol{\varphi}$ are randomly initialized. The adjacency matrix can be expressed as:

$$\boldsymbol{A} = \boldsymbol{\lambda}^T \cdot \boldsymbol{\varphi} \tag{6}.$$

Furthermore, we set most of the adjacency matrix's elements to zero, thereby rendering it sparser and reducing the number of elements that need to be computed. Specifically, for the adjacency matrix of each time series, only the top k elements with the highest weights are retained, while the other values are set to zero.

3.5.4 Temporal Convolutional Network

Temporal convolutional networks focus on capturing the temporal dependencies within each dimension of the CSI fingerprint by utilizing three CNN layers with different convolutional kernels, and applying padding operations to ensure that the output length matches the input CSI fingerprint sequence[36]. As illustrated in Fig. 4, in CNNs, neurons deviate from the fully connected architecture of traditional neural networks by adopting a locally connected approach. Specifically, each neuron establishes a connection to a local region of the input data, known as the recep-

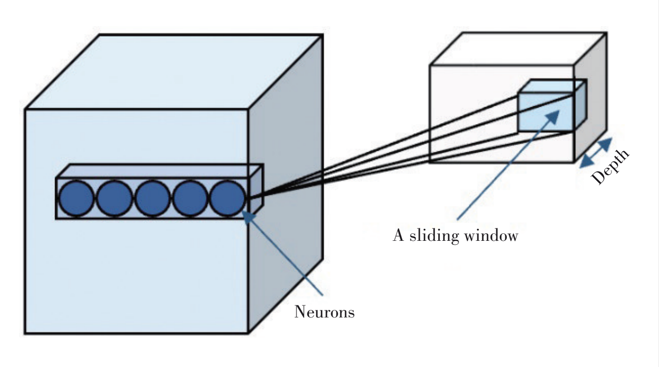


Figure 4. Representation of the convolution operation in CNN layers

tive field, via a convolution kernel (often implemented as a window function). Typically, the depth of the convolution kernel aligns with the depth of the input data. Each convolution kernel is designed to generate a feature map, meaning that multiple convolution kernels collectively yield multiple feature maps, contributing to the depth of the output data.

The learned characteristics of the l-th CNN layer can be denoted as:

$$\boldsymbol{X}_l = \sigma\left(\boldsymbol{W}_l * \boldsymbol{X}_{l-1} + \boldsymbol{B}_l\right) \tag{7},$$

where $\boldsymbol{X}_l$ serves as both the output from the $(l-1)$-th CNN layer and the input to the l-th CNN layer, σ represents the activation function and * denotes the convolution operation. Additionally, $\boldsymbol{W}_l$ and $\boldsymbol{B}_l$ represent the weight and bias matrices, respectively, within the l-th CNN layer.

3.5.5 Dynamic GNN

GNNs are broadly classified into static and dynamic graph categories. Static graphs are particularly suited for scenarios featuring unchanging topological structures, such as user relationship graphs in social networks. Conversely, dynamic graphs excel in managing evolving graph structures and attributes, akin to traffic networks where vehicle positions vary over time[37]. In mobile wireless communication scenarios, shifts in user positions result in continuous alterations in the distribution of CSI fingerprints. Consequently, dynamic graphs are employed to capture the temporal dynamics inherent in CSI fingerprint sequences.

As shown in Fig. 5, for all graphs except the first one, an identical number of vertices are added to represent the CSI fingerprint characteristics of the corresponding vertices from the previous time series. Directed edges are assigned between vertices from the previous time window $v_{(t-1,n)}$ and the current time series $v_{(t,n)}$ to establish associations.

3.5.6 Hierarchical Pooling

By combining graph pooling and temporal processing, this module utilizes hierarchical pooling to decrease the number of nodes, thereby circumventing the information loss inherent in

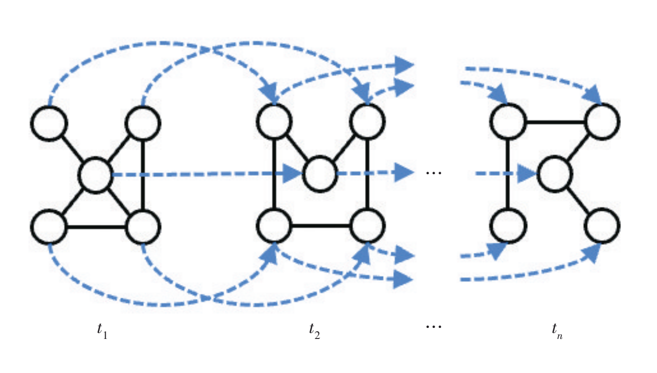


Figure 5. Dynamic graph

techniques like max pooling and average pooling[38]. As shown in Fig. 6, at each hierarchical level, nodes are converged through temporal convolutions to extract temporal features, and the adjacency matrix is then updated using convolutional weights.

3.5.7 Authentication Results

This module averages the values in the feature graph through average pooling to obtain a fixed-length vector. This vector is then mapped to a logic vector through a fully connected layer, and finally, the authentication result is obtained through the softmax function.

3.6 Simulation Results and Analysis

3.6.1 Baseline Schemes

We consider six baseline schemes as follows.

- K-nearest neighbor (KNN)[39]: Given a test sample, KNN searches for the k nearest fingerprint samples (neighbors) in the training dataset. Based on the information of these k neighbors, the identity of the test fingerprint sample is predicted.
- Naive Bayes (NB)[40]: NB assumes that the features are conditionally independent of each other given the identity label. Based on this assumption and Bayes' theorem, it calculates the posterior probability of each class for a given sample and assigns the sample to the class with the highest posterior probability.

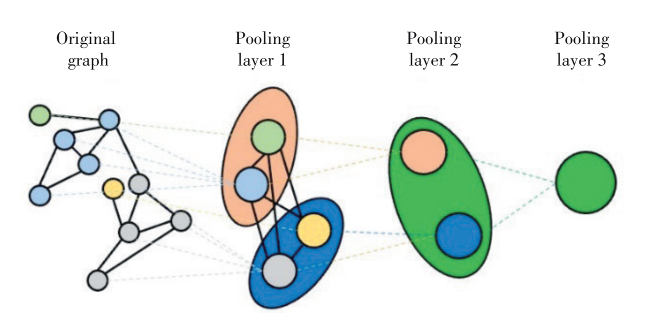


Figure 6. Hierarchical pooling

- Gradient boosting decision tree (GBDT)[39]: GBDT iteratively constructs multiple decision trees and minimizes the loss function through gradient descent, thereby gradually improving prediction accuracy. Its core idea is to build a strong learner using weak learners. In each iteration, GBDT adds a new decision tree to the current model to fit the residuals between the predictions of the previous model and the true values, thereby progressively refining the identity predictions.
- Regularized gradient boosting optimization (RGBO) [30]: Compared with GBDT, RGBO utilizes a second-order Taylor expansion to approximate the changes of the loss function, enabling it to more accurately estimate the descent direction at each iteration, thereby accelerating convergence speed and improving prediction accuracy. Additionally, RGBO incorporates a regularization term into the objective function to control the complexity of the model and prevent overfitting.
- Improved gradient boosting optimization (IGBO)[30]: Unlike RGBO, IGBO efficiently processes data, reduces memory consumption, and enhances training speed by optimizing the sampling process of fingerprints.
- Hybrid method (combining CNNs and RNNs)[41]: CNNs excel at feature extraction from static data, particularly in isolating local features within images. Conversely, RNNs are adept at handling the dependencies inherent in time series data, effectively retaining and utilizing past information. Consequently, the hybrid method merges these strengths, combining CNN's feature extraction prowess with RNN's sequence processing capabilities.

3.6.2 Performance Metric

The authentication performance of the proposed PLA model is measured by authentication accuracy as:

$$\text{AucRate} = \frac{1}{N}\sum_{n=1}^{N}\mathbb{I}\left(\boldsymbol{L}_n = \boldsymbol{Y}_n\right) \tag{8},$$

where N is the number of CSI fingerprint sequences, and $\boldsymbol{L}_n$ and $\boldsymbol{Y}_n$ respectively stand for the real and predicted identity labels of the n-th CSI fingerprint sequence. If $\cdot$ is true, $\mathbb{I}(\cdot) = 1$; if $\cdot$ is false, $\mathbb{I}(\cdot) = 0$.

3.6.3 Simulation Parameters

CSI fingerprints are generated through the MATLAB platform, and the performance of the proposed scheme is verified through Python. The positions of users, RISs, and Bob are provided in Fig. 7, and the detailed parameters are provided in Table 2. The number of layers in GNNs typically depends on the complexity of the dataset. For a straightforward graph, just a few layers may suffice to capture valuable information. However, for intricate graph structures, more layers may be required to extract sophisticated feature representations. Furthermore, while increasing the number of layers can enhance the model's expressive power, it may also introduce issues such as over-fitting, where node characteristics converge and become indistinguishable after multiple layers of propagation, thereby impeding the model's ability to differentiate between nodes. Additionally, it may lead to problems like gradient vanishing or exploding. Consequently, in our simulation, the number of GNN layers is set to 3. The selection of the batch size should consider hardware resources, dataset size, and model complexity. Therefore, we choose a batch size of 16.

3.6.4 Simulation Results

Fig. 8 analyzes the authentication accuracy versus different distances between adjacent users. As the distance between users decreases, the similarity of CSI fingerprints increases,

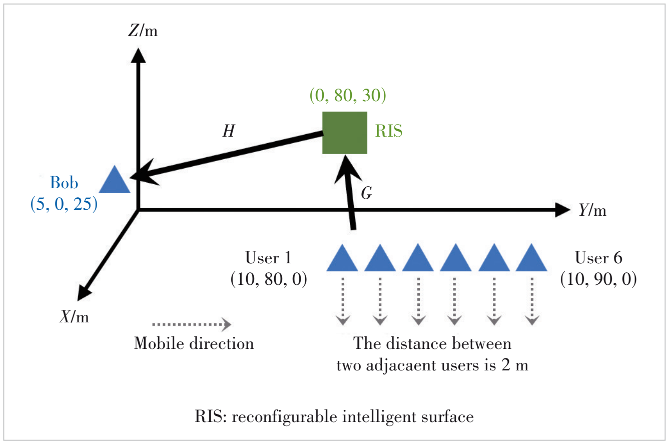


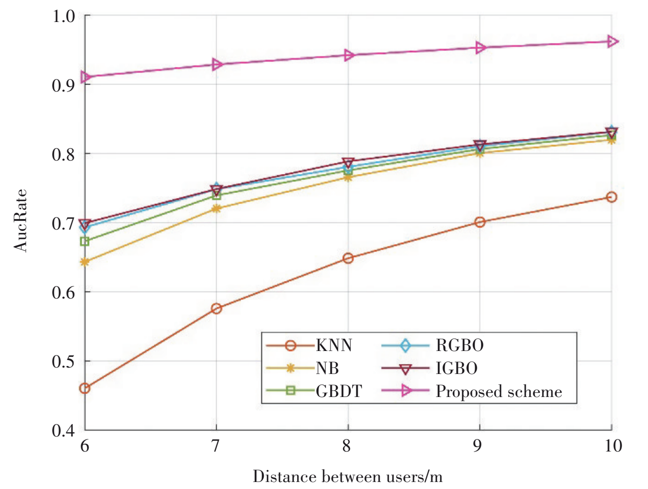
Figure 7. Positions of users, RISs, and Bob

Table 2. Simulation parameters

Parameters	Values	Parameters	Values
N_T	4	N_T	3
Number of RIS elements	8×16	Carrier frequency	3.5 GHz
κ_H	3	κ_G	4
Bandwidth	1 MHz	Speed of users	2 m/s
Number of each user's CSI fingerprint samples	50 000	Number of each user's CSI fingerprint sequences	1 000
Length of each CSI fingerprint sequence	50	Ratio of training fingerprints	0.6
Learning rate	0.000 1	Batch size	16
Number of GNN layers	3	Ratio of pooling for nodes	0.2

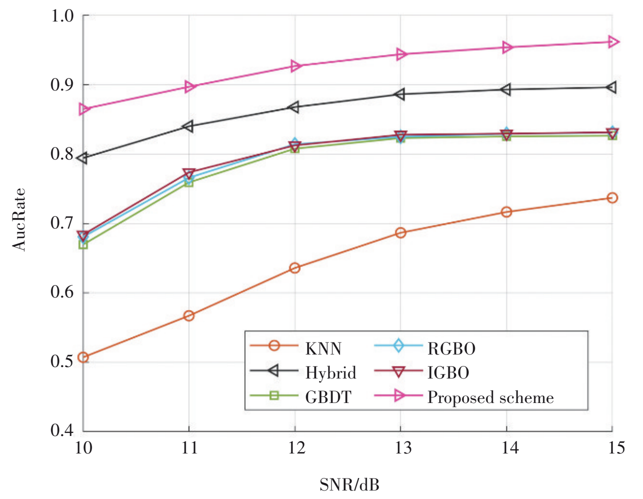
CSI: channel state information GNN: graph neural network RIS: reconfigurable intelligent surface leading to a higher degree of overlap in their fingerprint distributions. Consequently, it becomes more challenging for the PLA model to distinguish between them, resulting in lower authentication accuracy. However, the proposed PLA scheme consistently outperforms the benchmark models.

Fig. 9 depicts the authentication accuracy versus different SNRs. The authentication accuracy of baseline schemes improves gradually with higher SNRs. Regardless of SNR levels, the proposed scheme consistently outperforms these baselines, demonstrating superior robustness. This superiority stems from its consideration of the variations in CSI fingerprint distribution caused by user movements, whereas the other methods presume an independent and identical distribution of CSI fingerprints for each user.



GBDT: gradient boosting decision tree
IGBO: improved gradient boosting optimization
KNN: K-nearest neighbor
NB: Naive Bayes
RGBO: regularized gradient boosting optimization

Figure 8. Authentication accuracy versus different distances between adjacent users



GBDT: gradient boosting decision tree
IGBO: improved gradient boosting optimization
KNN: K-nearest neighbor
RGBO: regularized gradient boosting optimization
SNR: signal-to-noise ratio

Figure 9. Authentication accuracy versus different SNRs

4 Future Research Directions

This section gives challenges and the future research direction of AI-driven PLA, including semantic fingerprint-based PLA, large AI model-based PLA, cross-layer PLA, multimodal signature-based PLA, distributed autonomous PLA, and PLA for emerging applications.

4.1 Semantic Fingerprint-Based PLA

Unlike traditional syntax-based communication paradigms that focus on indiscriminate transmission of bit data, semantic communications ensure an accurate understanding of the communication intent of source information at both the transmitting and receiving ends through the representation and measurement of semantic information, on-demand compression, and efficient and robust transmission. Inspired by semantic communications, we can extract knowledge of environmental semantic features from the channel propagation environment. By doing so, the physical channel can be abstracted as a semantic channel to assist in guiding the acquisition and optimization of channel fingerprints. Ref. [42] proposes an environmental semantics-enabled PLA method, which extracts frequency-independent wireless channel fingerprints from CSI in massive MIMO systems based on environmental semantic knowledge. The proposed method can effectively detect physical-layer spoofing attacks and is robust in time-varying wireless environments. In the future, constructing a knowledge base of semantic channel fingerprints and a semantic channel knowledge map can further enhance the efficiency and accuracy of PLA.

4.2 Large AI Model-Based PLA

In recent years, research on large models has been in full swing, and they offer the following advantages. 1) Large models possess more parameters, enabling them to learn more complex data patterns and thus perform better on various tasks. 2) The knowledge learned by large models during training is more generalizable, allowing for better generalization to unseen data and reducing the need for extensive labeled data. 3) With ongoing advancements in computing resources, the cost of training and deploying large models has gradually decreased. In the future, for multiuser authentication needs, high-robustness authentication requirements in complex environments, and lightweight authentication needs, PLA empowered by large models will exhibit exceptional performance.

4.3 Cross-Layer PLA

The training of PLA models based on AI requires the guidance of prior knowledge of legitimate fingerprints, which originates from identity labeling by upper-layer authentication mechanisms. Therefore, PLA is a type of cross-layer authentication technology, and its complexity is influenced by the interaction efficiency between the upper layer and the physical layer. Ref. [43] deploys active learning to select optimal unlabeled fingerprints and queries the identity from the upper-layer authentication protocol. The proposed method can effectively reduce the interaction requirements between the upper-layer and the physical-layer, achieving efficient utilization of prior fingerprint information. In the future, optimizing the fingerprint selection algorithm could further reduce the authentication error rate while maintaining lightweight performance.

4.4 Multimodal Signature-Based PLA

By integrating technologies such as wireless communications, radio sensing, and even AI, integrated sensing and communication (ISAC) can achieve the goals of spectrum conservation, cost reduction, and mutual enhancement between communication and sensing. Ref. [44] introduces the concept of synesthesia of machines and establishes a platform for generating and collecting communication and multimodal sensing information. This platform can provide multimodal data under diverse scenarios (urban, suburban, and rural) and various conditions (different weather, times of day, traffic densities, frequency bands, and antenna arrays). In the future, by designing multimodal fusion algorithms that integrate channel fingerprints, RF sensing data (millimeter-wave radar point clouds), and non-RF sensing data (RGB images, depth maps, and LiDAR point clouds), highly reliable identity authentication in dynamic and complex environments can be achieved.

4.5 Distributed Autonomous PLA

With the advancement in cloud computing and edge intelligence, the cloud-edge-end collaborative architecture can optimize resource utilization in a distributed manner and enhance data security. Ref. [45] proposes a privacy-preserving collaborative authentication scheme that provides reliable and efficient security, improved robustness in dynamic or untrusted environments, and stronger defensive capabilities compared with traditional centralized authentication methods. Future research includes cross-domain distributed PLA systems to ensure seamless switching and access for users or devices across different domains.

4.6 PLA for Emerging Applications

Future 6G networks will expand the boundaries of communication technology and transform the way we live and work. 6G will support emerging application scenarios, such as integrated space-air-ground-sea networks for ubiquitous coverage. Ref. [46] considers the identity security of satellite transmitters and provides a PLA scheme for low-earth orbit satellites. Ref. [47] provides a PLA approach for complicated time-varying underwater acoustic channels. Future research includes optimizing fingerprint feature extraction algorithms, developing anti-interference PLA technologies, and assessing industrial feasibility.

5 Conclusions

As the next generation of mobile communication technology, 6G stands as a pinnacle of global technological advancement and plays a pivotal role in driving future industrial development. As the latest iteration of information infrastructure, the security of 6G directly relates to the safe operation of national critical infrastructures. Currently, authentication mechanisms in wireless communications primarily rely on cryptography-based algorithms, and these "add-on" and "patchwork" authentication mechanisms face challenges in terms of security protection levels, computational power requirements, and compatibility. As an endogenous security approach, AI-based PLA boasts strong security assurance, intelligence, efficiency, and strong scalability. This paper first reviews representative AI-enabled PLA schemes, categorizing them into RF fingerprint extraction, fingerprint data augmentation, lightweight authentication models, authentication parameter optimization, multi-attacker identification, and physical-layer key generation for FDD systems. Furthermore, this paper proposes a GNN-based solution to identifing mobile multiusers and compares its performance with six baseline schemes to verify its superiority. Finally, this paper outlines future research directions, providing new insights for researchers in related fields.

References

[1] CHAFII M, BARIAH L, MUHAIDAT S, et al. Twelve scientific challenges for 6G: rethinking the foundations of communications theory [J]. IEEE communications surveys and tutorials, 2023, 25(2): 868 – 904. DOI: 10.1109/COMST.2023.3243918

[2] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: a survey on prospective technologies and challenges [J]. IEEE communications surveys and tutorials, 2021, 23(4): 2384 – 2428. DOI: 10.1109/COMST.2021.3108618

[3] GUO H Z, LI J Y, LIU J J, et al. A survey on space-air-ground-sea integrated network security in 6G [J]. IEEE communications surveys and tutorials, 2022, 24(1): 53 – 87. DOI: 10.1109/COMST.2021.3131332

[4] WANG C X, YOU X H, GAO X Q, et al. On the road to 6G: visions, requirements, key technologies, and testbeds [J]. IEEE communications surveys and tutorials, 2023, 25(2): 905 – 974. DOI: 10.1109/COMST.2023.3249835

[5] PORAMBAGE P, GÜR G, OSORIO D P M, et al. The roadmap to 6G security and privacy [J]. IEEE open journal of the communications society, 2021, 2: 1094 – 1122. DOI: 10.1109/OJCOMS.2021.3078081

[6] CHORTI A, BARRETO A N, KÖPSELL S, et al. Context-aware security for 6G wireless: the role of physical layer security [J]. IEEE communications standards magazine, 2022, 6(1): 102 – 108. DOI: 10.1109/MCOMSTD.0001.2000082

[7] LI D M, YANG X, ZHOU F H, et al. Blind physical-layer authentication based on composite radio sample characteristics [J]. IEEE transactions on communications, 2022, 70(10): 6790 – 6803. DOI: 10.1109/TCOMM.2022.3200599

[8] WANG X B, HAO P, HANZO L. Physical-layer authentication for wireless security enhancement: current challenges and future developments [J]. IEEE communications magazine, 2016, 54(6): 152 – 158. DOI: 10.1109/MCOM.2016.7498103

[9] XIE N, TAN H J, HUANG L, et al. Physical-layer authentication in wirelessly powered communication networks [J]. IEEE/ACM transactions on networking, 2021, 29(4): 1827 – 1840. DOI: 10.1109/TNET.2021.3071670

[10] HAN S F, XIE T, I C L. Greener physical layer technologies for 6G mobile communications [J]. IEEE communications magazine, 2021, 59(4): 68 – 74. DOI: 10.1109/MCOM.001.2000484

[11] FANG H, WANG X B, TOMASIN S. Machine learning for intelligent authentication in 5G and beyond wireless networks [J]. IEEE wireless communications, 2019, 26(5): 55 – 61. DOI: 10.1109/MWC.001.1900054

[12] FANG H, QI A, WANG X B. Fast authentication and progressive authorization in large-scale IoT: how to leverage AI for security enhancement [J]. IEEE network, 2020, 34(3): 24 – 29. DOI: 10.1109/MNET.011.1900276

[13] XIA S D, TAO X F, LI N, et al. Multiple correlated attributes based physical layer authentication in wireless networks [J]. IEEE transactions on vehicular technology, 2021, 70(2): 1673 – 1687. DOI: 10.1109/TVT.2021.3055563

[14] JIAN T, RENDON B C, OJUBA E, et al. Deep learning for RF fingerprinting: a massive experimental study [J]. IEEE Internet of Things magazine, 2020, 3(1): 50 – 57. DOI: 10.1109/IOTM.0001.1900065

[15] MENG R, XU B X, XU X D, et al. A survey of machine learning-based physical-layer authentication in wireless communications [J]. Journal of network and computer applications, 2025, 235: 104085. DOI: 10.1016/j.jnca.2024.104085

[16] PENG L N, ZHANG J Q, LIU M, et al. Deep learning based RF fingerprint identification using differential constellation trace figure [J]. IEEE transactions on vehicular technology, 2020, 69(1): 1091 – 1095. DOI: 10.1109/TVT.2019.2950670

[17] ROY D, MUKHERJEE T, CHATTERJEE M, et al. RF transmitter fingerprinting exploiting spatio-temporal properties in raw signal data [C]//Proceedings of 18th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2019: 89 – 96. DOI: 10.1109/icmla.2019.00023

[18] ZENG Y, GONG Y, LIU J W, et al. Multi-channel attentive feature fusion for radio frequency fingerprinting [J]. IEEE transactions on wireless communications, 2024, 23(5): 4243 – 4254. DOI: 10.1109/TWC.2023.3316286

[19] GOPALAKRISHNAN S, CEKIC M, MADHOW U. Robust wireless fingerprinting via complex-valued neural networks [C]//Proceedings of IEEE Global Communications Conference (GLOBECOM). IEEE, 2019: 1 – 6. DOI: 10.1109/globecom38437.2019.9013154

[20] MENG R, XU X D, SUN H, et al. Multiuser physical-layer authentication based on latent perturbed neural networks for industrial Internet of Things [J]. IEEE Internet of Things journal, 2023, 10(1): 637 – 652. DOI: 10.1109/JIOT.2022.3203514

[21] LIAO R F, WEN H, CHEN S L, et al. Multiuser physical layer authentication in Internet of Things with data augmentation [J]. IEEE Internet of Things journal, 2020, 7(3): 2077 – 2088. DOI: 10.1109/JIOT.2019.2960099

[22] CHEN Y, HO P H, WEN H, et al. On physical-layer authentication via online transfer learning [J]. IEEE Internet of Things journal, 2022, 9(2): 1374 – 1385. DOI: 10.1109/JIOT.2021.3086581

[23] WANG Y, GUI G, GACANIN H, et al. An efficient specific emitter identification method based on complex-valued neural networks and network compression [J]. IEEE journal on selected areas in communications, 2021, 39(8): 2305 – 2317. DOI: 10.1109/JSAC.2021.3087243

[24] XIAO L, LI Y, HAN G A, et al. PHY-layer spoofing detection with reinforcement learning in wireless networks [J]. IEEE transactions on vehicular technology, 2016, 65(12): 10037 – 10047. DOI: 10.1109/TVT.2016.2524258

[25] XIAO L, LU X Z, XU T W, et al. Reinforcement learning-based physical-layer authentication for controller area networks [J]. IEEE transactions on information forensics and security, 2021, 16: 2535 – 2547. DOI: 10.1109/TIFS.2021.3056206

[26] SENIGAGLIESI L, BALDI M, GAMBI E. Comparison of statistical and machine learning techniques for physical layer authentication [J]. IEEE transactions on information forensics and security, 2020, 16: 1506 – 1521. DOI: 10.1109/TIFS.2020.3033454

[27] QIU X Y, JIANG T, WU S, et al. Physical layer authentication enhancement using a Gaussian mixture model [J]. IEEE access, 2018, 6: 53583 – 53592. DOI: 10.1109/ACCESS.2018.2871514

[28] ZHANG X W, LI G Y, ZHANG J Q, et al. Deep-learning-based physical-layer secret key generation for FDD systems [J]. IEEE Internet of Things journal, 2022, 9(8): 6081 – 6094. DOI: 10.1109/JIOT.2021.3109272

[29] JIN L, XU X D, HAN S J, et al. RIS-assisted physical layer key generation and transmit power minimization [C]//Proceedings of IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2022: 2065 – 2070. DOI: 10.1109/WCNC51071.2022.9771815

[30] MENG R, XU X D, ZHAO H Y, et al. Multi-observation multi-channel-attribute-based multi-user authentication for industrial wireless edge networks [J]. IEEE transactions on industrial informatics, 2024, 20(2): 2097 – 2108. DOI: 10.1109/TII.2023.3286885

[31] MOURYA S, REDDY P, AMURU S, et al. Spectral temporal graph neural network for massive MIMO CSI prediction [J]. IEEE wireless communications letters, 2024, 13(5): 1399 – 1403. DOI: 10.1109/LWC.2024.3372148

[32] ZHENG B X, YOU C S, MEI W D, et al. A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications [J]. IEEE communications surveys & tutorials, 2022, 24(2): 1035 – 1071. DOI: 10.1109/COMST.2022.3155305

[33] RODRÍGUEZ P, BAUTISTA M A, GONZÀLEZ J, et al. Beyond one-hot encoding: lower dimensional target embedding [J]. Image and vision computing, 2018, 75: 21 – 31. DOI: 10.1016/j.imavis.2018.04.004

[34] WU Z H, PAN S R, CHEN F W, et al. A comprehensive survey on graph neural networks [J]. IEEE transactions on neural networks and learning systems, 2021, 32(1): 4 – 24. DOI: 10.1109/TNNLS.2020.2978386

[35] ZHOU J, CUI G Q, HU S D, et al. Graph neural networks: a review of methods and applications [J]. AI open, 2020, 1: 57 – 81. DOI: 10.1016/j.aiopen.2021.01.001

[36] LEA C, FLYNN M D, VIDAL R, et al. Temporal convolutional networks for action segmentation and detection [C]//Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2017: 1003 – 1012. DOI: 10.1109/CVPR.2017.113

[37] SKARDING J, GABRYS B, MUSIAL K. Foundations and modeling of dynamic networks using dynamic graph neural networks: a survey [J]. IEEE access, 2021, 9: 79143 – 79168. DOI: 10.1109/ACCESS.2021.3082932

[38] LIU H Y, YANG D H, LIU X Z, et al. TodyNet: temporal dynamic graph neural network for multivariate time series classification [J]. Information sciences, 2024, 677: 120914. DOI: 10.1016/j.ins.2024.120914

[39] PAN F, PANG Z B, WEN H, et al. Threshold-free physical layer authentication based on machine learning for industrial wireless CPS [J]. IEEE transactions on industrial informatics, 2019, 15(12): 6481 – 6491. DOI: 10.1109/TII.2019.2925418

[40] WEBB G I. Naive bayes [M]//Encyclopedia of machine learning. Boston, USA: Springer, 2011: 713 – 714. DOI: 10.1007/978-0-387-30164-8_576

[41] ALZAHRANI S, ALDERAAN J, ALATAWI D, et al. Continuous mobile user authentication using a hybrid CNN-Bi-LSTM approach [J]. Computers, materials & continua, 2023, 75(1): 651 – 667. DOI: 10.32604/cmc.2023.035173

[42] GAO N, HUANG Q Y, LI C, et al. EsaNet: environment semantics enabled physical layer authentication [J]. IEEE wireless communications letters, 2024, 13(1): 178 – 182. DOI: 10.1109/LWC.2023.3324981

[43] MENG R, ZHU F Z, XU X D, et al. Efficient Gaussian process classification-based physical-layer authentication with configurable fingerprints for 6G-enabled IoT [EB/OL]. [2024-11-10]. https://arxiv.org/abs/2307.12263v2

[44] CHENG X, HUANG Z W, BAI L, et al. M^{3}SC: a generic dataset for mixed multi-modal (MMM) sensing and communication integration [J]. China communications, 2023, 20(11): 13 – 29. DOI: 10.23919/JCC. fa. 2023-

0268.202311

[45] FANG H, WANG X B, XIAO Z L, et al. Autonomous collaborative authentication with privacy preservation in 6G: from homogeneity to heterogeneity [J]. IEEE network, 2022, 36(6): 28 – 36. DOI: 10.1109/MNET.002.2100312

[46] OLIGERI G, SCIANCALEPORE S, RAPONI S, et al. PAST-AI: physical-layer authentication of satellite transmitters via deep learning [J]. IEEE transactions on information forensics and security, 2022, 18: 274 – 289. DOI: 10.1109/TIFS.2022.3219287

[47] ZHAO R Q, SHI T, LIU C Y, et al. Physical layer authentication without adversary training data in resource-constrained underwater acoustic networks [J]. IEEE sensors journal, 2023, 23(22): 28270 – 28281. DOI: 10.1109/JSEN.2023.3321777

Biographies

MENG Rui received his BS degree in information engineering and PhD degree in information and communication engineering both from Beijing University of Posts and Telecommunications (BUPT), China in 2018 and 2024, respectively. He is currently a postdoctoral fellow with BUPT. His research interests cover next-generation networks, physical layer authentication, identity security, semantic security, deep learning, and Internet of Things.

FAN Dayu received his BS degree in information engineering from Beijing University of Posts and Telecommunications (BUPT), China in 2024, where he is currently pursuing his master's degree in communication engineering. His research interests cover wireless security, semantic communication, and deep learning.

XU Xiaodong (xuxiaodong@bupt.edu.cn) received his BS degree in information and communication engineering and master's degree in communication and information system both from Shandong University, China in 2001 and 2004, respectively. He received his PhD degree in circuit and system from Beijing University of Posts and Telecommunications (BUPT), China in 2007. He is currently a professor of BUPT, a research fellow of the Department of Broadband Communication of Peng Cheng Laboratory and a member of IMT-2030 (6G) Experts Panel. He has coauthored nine books/chapters and more than 120 journal and conference papers. He is also the inventor or co-inventor of 51 granted patents. His research interests cover semantic communications, intellicise communication systems, moving networks, and mobile edge computing and caching.

LYU Suyu received her bachelor's degree and PhD degree in information and communication engineering from Beijing University of Posts and Telecommunications, China in 2018 and 2024, respectively. From November 2022 to September 2023, she was a visiting student with the School of Electronic Engineering and Computer Science, Queen Mary University of London, UK. She is currently a post-doctoral researcher at Beijing University of Technology, China. Her main research interests include ultra-reliable low-latency communications, reconfigurable intelligent surface, and non-orthogonal multiple access.

TAO Xiaofeng received his BS degree in electrical engineering from Xi'an Jiaotong University, China in 1993, and MS and PhD degrees in telecommunication engineering from Beijing University of Posts and Telecommunications (BUPT), China, in 1999 and 2002, respectively. He is a professor at BUPT, a fellow of the IET, and Chair of the IEEE ComSoc Beijing Chapter. He has authored or co-authored over 200 papers and three books in wireless communication areas. He focuses on 5G/B5G research.