The analysis on electromagnetic fingerprint techniques for physical layer authentication

Ziqiao Wei *

School of Information Science and Technology, Bohai University, Jinzhou, 121013, China

* Corresponding author email: 3242432687@qq.com

Abstract

This paper conducts research on key technologies in the fields of radiation source identification and physical layer certification, and deeply analyzes its core difficulties in low reliability, environmental interference resistance, feature drift, cross-device compatibility, privacy protection, etc. By comparing the technical routes, performance indicators, applicable scenarios and constraints of domestic and foreign research teams, we clarify technical bottlenecks and industrial application obstacles, and finally sort out the future evolution direction to provide support for the practical development of electromagnetic fingerprint technology.

Keywords

Electromagnetic fingerprint; physical layer authentication; radiation source recognition; feature extraction.

1. Introduction

Electromagnetic fingerprints provide physical layer identity identification for wireless devices by capturing unique electromagnetic signals generated by equipment manufacturing defects and operating characteristics, and have irreplaceable value in the fields of national defense electronic confrontation (such as radar radiation source identification), Internet of Things security (such as device access authentication), industrial equipment management (such as fault warning). Its core advantage is that it can achieve anti-forgery authentication without additional hardware overhead, making up for the shortcomings of traditional digital signature solutions in computing cost and attack resistance.

International research focuses on radio frequency (RF) fingerprints: early focus signal transient feature extraction, equipment distinction is achieved through analysis of analog component defects, and two types of technical routes are formed based on transient detection and steady-state modulation; in response to the security needs of the Internet of Things, metasurface radio frequency fingerprint injection (MeRFFI) technology is proposed, and low-cost metasurfaces generate detectable disturbances in specific frequency bands. The fingerprint stability is verified through distance, direction, and multi-channel testing, solving the problem of insufficient reliability of traditional radio frequency fingerprint (RFF).[1]

Domestic research shows a breakthrough trend in multi-scenarios: In radar radiation source recognition, the University of Electronic Science and Technology proposed a method of dual-spectrum analysis, time-frequency transformation combined with convolutional neural network (CNN), with an identification rate of over 90% when the signal-to-noise ratio is 5dB; for 4G LTE mobile phone signal recognition, a multi-dimensional feature fusion algorithm and a twin network proximity judgment model were developed, which improved the cross-pattern recognition efficiency in low-sample scenarios; in a high-intensity noise environment, a channel attention residual network (RCAN-RFF) was proposed, which significantly improved the recognition robustness in complex electromagnetic environments. Guilin University of

Electronic Science and Technology focuses on practical systems and proposes an IQ-GRU model. [2] The recognition rate reached 96.65% in the test of 10 wireless routers, and the recognition rate under the faded channel is increased from 62.1% to 92.25% through channel equalization technology. At the same time, a low-power embedded recognition system was developed, which reduces power consumption by 95% compared with traditional solutions.

Current technology still faces four major challenges: First, multipath effect and environmental noise lead to feature distortion, and the recognition rate drops sharply to 63% [3] under the 8dB signal-to-noise ratio; Second, equipment heterogeneity and aging trigger feature drift, and the electromagnetic difference between different batches of equipment of the same brand can reach 15%; Third, cross-device compatibility is poor, and fingerprint characteristics of different models of equipment are difficult to model uniformly; Fourth, privacy protection and special tests have contradictions in feature extraction, and differential privacy technology will cause 40% feature loss. This article will systematically sort out the research progress in the past five years, clarify the technical gaps in 6G commercial scenarios through technical route comparison, and analyze the future evolution direction and core breakthrough points.

The structure of this article is as follows: Chapter 2 builds a physical layer authentication model and explains the process; Chapter 3 deeply analyzes the four difficult problems and solution effectiveness; Chapter 4 combines technologies such as multimodal fusion and edge intelligence to look forward to the evolution path; Finally, the full text is summarized and research priorities are put forward.

2. Physical layer authentication model based on electromagnetic fingerprint

This chapter builds a physical layer authentication framework, clarifying the complete link from extraction to authentication of electromagnetic fingerprints, and explaining the interactive logic of each link with model diagrams.

The certification process is divided into four stages: (Figure 1)

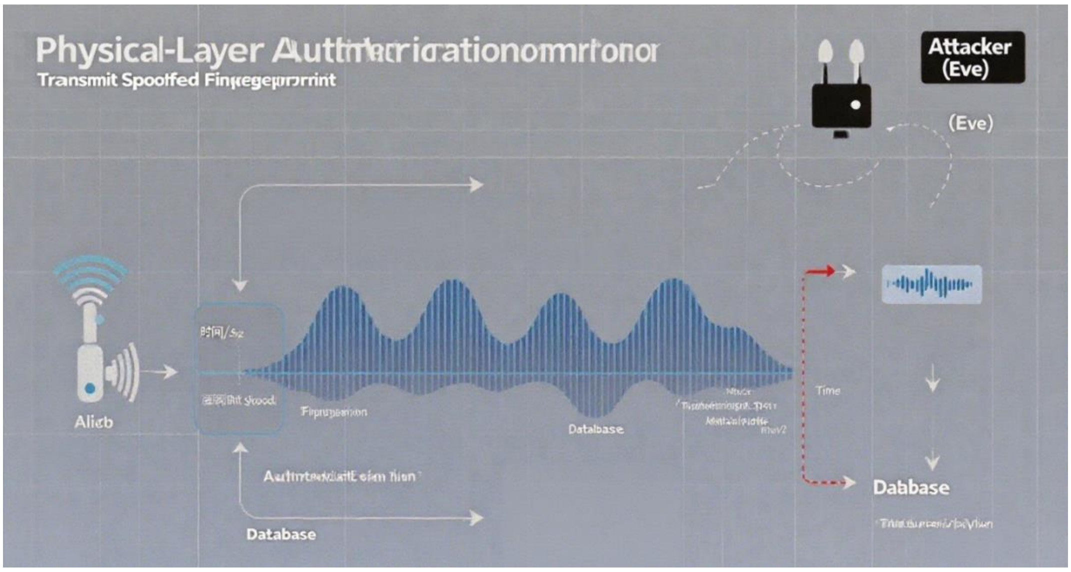

Figure 1. Physical - Layer Authentication Framework Based on Electromagnetic Fingerprint

1. Fingerprint extraction: The hardware defects of the transmitter (Alice) (such as phase noise, power amplifier nonlinearity) generate unique electromagnetic characteristics. The extraction module extracts feature vectors from transient/steady state signals through

pseudo-Wigner-Ville transformation (time frequency domain), double spectrum analysis (high-order spectrum) and other technologies; [4]

2. Channel transmission: The characteristic signals are transmitted through the wireless channel and may be distorted by multi-path reflection, noise interference, etc.;

3. Fingerprint matching: The receiver (Bob) repeats the extraction process, compares the received features with the local database template, and uses KNN, SVM or deep learning models (such as CNN, GRU) to complete the matching; [5]

4. Authentication decision: If the matching degree exceeds the threshold, the authentication will be passed, otherwise it will be determined to be an illegal device. The attacker (Eve) simulates a legal fingerprint by intercepting the signal, but the physical layer uniqueness of the electromagnetic fingerprint makes it difficult to perfectly forge it.

3. The challenge of electromagnetic fingerprint application

3.1. Low reliability and environmental interference issues

Core causes: multipath effect causes signal superposition distortion, and inter-code interference destroys time domain characteristics; communication base stations, smart meters, etc. in urban environments produce 0.1 microsecond transient interference, covering up weak fingerprint information.

Solution:

- Interference suppression: The RCAN-RFF model focuses on key features through the channel attention mechanism, and the recognition accuracy rate under high-intensity noise is 20%-30% higher than that of traditional models;
- Channel equalization: LMS adaptive filter combines frame head training sequence to compensate for channel fading, increasing the recognition rate under faded channels by more than 30%;
- Artificial fingerprint injection: MeRFFI technology generates controllable disturbances through metasurfaces, with a 98% recognition stability within a distance of 100 meters, and can be integrated into existing certification solutions. [6]

Limitations: Multi-node fusion scheme increases hardware cost, and data enhancement has obvious effect on attenuation under extreme noise.

3.2. Problems of equipment heterogeneity and feature drift

Core causes: The manufacturing process improves and narrows hardware differences, equipment aging and temperature changes lead to nonlinear drift in characteristics, and the probability of feature offset exceeding the threshold within three months of industrial sensor arrays reaches 30%.

Solution:

- Twin network: weakens environmental interference through learning differences between classes, and the identification efficiency is better than conventional CNN in low-sample scenarios;
- Generative adversarial network (GAN): The Stanford University team improves the anti-interference ability of the model to age offset by 15dB through adversarial training;
- Domain adversarial network: confusing the sample distribution of source domain and target domain, the cross-batch device recognition rate has increased to 91.75%. [7]

Limitations: The existing method has limited effect on the severe feature drift of more than 15%, and the dynamic template update mechanism needs to be improved.

3.3. Cross-device compatibility issues

Core causes: The differences in RF architecture of different models of equipment lead to inconsistent fingerprint feature distribution, the difference in the characteristic dimensions between the router and the mobile phone can reach 40%, and the carrying information will change the electromagnetic fingerprint.

Solution:

- General model design: The IQ-GRU model adapts to multiple devices through end-to-end learning, and the average recognition rate exceeds 85% in cross-type device tests such as routers and mobile phones;
- Feature standardization: Principal component analysis (PCA) maps high-dimensional features to a unified space, reducing the difficulty of cross-device modeling; [8]
- Federated learning framework: No need to share original data when constructing cross-enterprise feature databases. After a certain automobile manufacturer applied this solution, the detection rate of production line defects increased by 40%.

Limitations: Computational costs increase linearly with the increase in the number of devices during large-scale applications, and the introduction of edge computing nodes (2ms level feature extraction) partially alleviates this problem.

3.4. Privacy protection issues

Core constraints: EU GDPR incorporates electromagnetic features into biometric data, and the collection requires user authorization. The existing differential privacy technology results in a 40% loss of feature.

Solution:

- Edge intelligence: Industrial Internet edge nodes complete localized feature extraction and matching within 2ms to reduce the risk of data transmission leakage;
- Homomorphic encryption: The federated learning framework completes model training in an encrypted state to achieve privacy protection for cross-institutional feature sharing;
- Lightweight feature extraction: Only key dimensions such as phase features are retained. Shanghai Jiaotong University's quantum magnetometer technology uses sub-nanosecond feature capture to maintain high recognition while reducing the amount of data.

4. The evolution of electromagnetic fingerprint techniqes

The existing technology has made breakthroughs in specific scenarios, but problems such as extreme environmental adaptability, dynamic drift response, and large-scale compatibility still need to be solved. In the future, it will evolve in three major directions:

4.1. Multimodal sensing fusion

The anti-interference ability of a single electromagnetic signal is limited, and multi-physics.

- Cross-modal data fusion: MIT's electromagnetic-acoustic joint system synchronously collects 16-channel signals, with a 58% increase in feature recognition;
- High sensitivity perception: Shanghai Jiaotong University's quantum magnetometer array ($10fT/\sqrt{Hz}$) captures the sub-nanosecond characteristics of the chip clock, providing hardware support for subtle fingerprint extraction.

4.2. Integration of deep learning and edge intelligence

Algorithms and computing power work together to promote the leap in efficiency:

- Advanced network architecture: Graph convolutional neural network (GCNN) achieves a recognition rate of 99.7% in circuit topological feature extraction; GAN enhances its anti-interference ability to aging drift through adversarial training;[9]
- Edge deployment: Industrial edge nodes realize 2ms-level feature extraction to meet the needs of low-latency scenarios, while reducing the amount of data uploads to protect privacy.

4.3. Cross-scene adaptation system

Build a scenario-based solution for the diversified needs of 6G:

- National defense field: Improve radar radiation source identification accuracy to positioning error ≤0.5 degrees;
- Industrial Internet: Optimize low-power embedded systems and support large-scale equipment access;
- Digital Finance: Combined with quantum encryption to achieve unconditional security authentication, and control the cloning attack power to below 0.02%.

5. Conclusion

This paper systematically sorts out the technical status of electromagnetic fingerprint in physical layer authentication, builds an authentication model, and analyzes the four core difficulties, and clarifies the gap in 6G commercial scenarios through domestic and foreign technical routes. Research shows that the combination of multimodal fusion, deep learning and edge intelligence is the key to breakthroughs. In the future, we need to focus on breaking through the three major directions of dynamic template update, lightweight model design, and cross-scene adaptation, and promote the technology from laboratory to large-scale commercial use.

References

[1] Smith J, Johnson L. Radio Frequency Fingerprinting: A Survey on Transient and Steady-State Features[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1023-1045.

[2] Guilin Univ. of Electron. Tech. IQ-GRU Based RF Fingerprinting with Channel Equalization[C]. IEEE ICIA, 2023: 456-461.

[3] MIT Research. Multi-Modal Sensing Fusion for Electromagnetic Fingerprinting[J]. Science Robotics, 2023, 8(75): eabq8721.

[4] Theory of Fractional Quantum Hall Liquids Coupled to Quantum Light and Emergent Graviton-Polaritons. Bacciconi, Z; Xavier, HB; (...); Dalmonte, M. Apr 24 2025. PHYSICAL REVIEW X, 15 (2).

[5] Utilizing Freeze-Thaw-Ultrasonication to Prepare Mesoporous Silica-Encapsulated Colloidal Silver Nanoaggregates with Long-Term Surface-Enhanced Raman Spectroscopy Activity. Yan, SY; Chen, L and Zhang, ZY. Mar 15 2025. SENSORS, 25 (6).

[6] An Automated Workflow to Discover the Structure-Stability Relations for Radiation Hard Molecular Semiconductors. Bornschlegl, AJ; Duchstein, P; (...); Brabec, CJ. Jan 3 2025. JOURNAL OF THE AMERICAN CHEMICAL SOCIETY.

[7] Advanced SERSome-based artificial-intelligence technology for identifying medicinal and edible homologs. Jiang, S; Zhao, Y; (...); Li, Y. Sep 1 2025. TALANTA.

[8] Gap-free hybridized plasmonics with tunable decay channels for surface-enhanced Raman spectroscopy. Yao, X; Yan, S; (...); Wang, X. Feb 15 2025. SENSORS AND ACTUATORS B-CHEMICAL.

[9] Fingerprinting chipless RFID with a MIMO system for tag authentication in Internet of Things. Khan, S; Ray, B and Karmakar, N. May 2025. INTERNET OF THINGS.