Physical Layer Authentication in Wireless Networks

Subjects: Computer Science, Artificial Intelligence

Contributor: Lamia Alhoraibi , Daniyal Alghazzawi , Reemah Alhebshi , Osama Bassam J. Rabie

The physical layer security of wireless networks is becoming increasingly important because of the rapid development of wireless communications and the increasing security threats. In addition, because of the open nature of the wireless channel, authentication is a critical issue in wireless communications. Physical layer authentication (PLA) is based on distinctive features to provide information-theory security and low complexity.

physical layer authentication physical layer security wireless networks

1. Wireless Network

A network's architecture defines the protocols and components required to meet application needs. The open systems interconnection (OSI) Model practically represents a wireless network's different standards and compatibility. The OSI model is a conceptual framework that outlines how data are exchanged within a computer network from one device to another. The OSI model describes a complete set of network services within each network component organized into layers, illustrated in **Figure 1**. Each layer consists of a collection of conventional communication protocols and customized components to accomplish specific functions.

OSI Layers	Main Protocols	Attacks	Security Techniques
Application	HTTP-FTP-SMTP	HTTP Flooding-Malware-FTP bounce-SQL Injection-DDoS-cross-site scripting	Encryption Technique
Transport	TCP-UDP	TCP/UDP flooding-TCP sequence prediction	Secure Sockets
Network	IP-ICMP	MITM-Sybil attack-IP smurfing- Address spoofing	Up to date of security patches- Packet filtering
Data Link	Ethernet-IEEE 802.11-MAC	MAC spoofing- Port Stealing	Secure MAC
Physical	WiFi-Bluetooth	Jamming-sniffing -Eavesdropping	Physical Layer Security Technique

Figure 1. A generic wireless OSI Model information consisting of the layers, main protocols, main attacks, security techniques.

1.1. Physical Layer

The physical layer is the only layer in the OSI model interacts with actual hardware, transmission, and signaling mechanisms. The physical layer transmits raw bits over a physical data link connecting network nodes by converting them to electrical pulses, representing the binary data. The electric pulses are then converted to electromagnetic waves to be transmitted wirelessly. On the other hand, the physical layer specifies the data transmission mechanism and how data can move between devices.

1.2. Wireless Physical Layer Protocols

Recently, massive of advanced wireless technologies and dozens of different wireless protocols meet the needs, each with its performance characteristics and optimized for a specific task and context. However, various wireless protocols exist, such as WiFi, Bluetooth, ZigBee, NFC, WiMAX, LoRa, 5G, satellite services, and more. Therefore, it is necessary to be aware of the system's constraints and performance requirements when choosing protocols. Power, data rate, reliability, and range are essential metrics for distinguishing between protocols [1].

1.3. Wireless Networks Physical Layer Threats

The openness of wireless networks produces communication more vulnerable to attacks, which poses severe challenges for network security. Wireless networks have security vulnerabilities, such as [1][2][3][4]:

Eavesdropping: Unauthorized and unannounced interception of communications between devices. Through eavesdropping, the intercepted messages can be exploited for future illegal purposes. Eavesdropping attackers can be categorized as active eavesdroppers and silent eavesdroppers. The distinction is that active eavesdroppers acting as communication parties unintentionally send signals to transmitters, which channel state information (CSI) can extract through estimation. On the other hand, silent eavesdroppers snoop on messages while being silent, where their CSIs are not available for transmitters. Therefore, this kind of threat can be divided into two types based on the manner of the attacker: interception and traffic analysis.

- Interception: Eavesdropping is the most common attack on wireless devices' privacy. The attacker could find legitimate communication by snooping in the nearby wireless environment when the traffic transmits control information about the sensor network configuration.

- Traffic Analysis: The ability to track communication patterns to facilitate various types of attacks.

Jamming: Blocks legitimate communications between devices by saturating a channel with noise, which can direct denial-of-service (DOS) attacks at the physical layer. In general, jamming attacks can be divided into proactive and reactive jamming.

- Proactive Jamming: Proactive jamming attackers spread interfering signals whether the legitimate signal communication is there or not. To save energy and toggle between the sleep and jamming phases, attackers

sporadically spread random bits or normal packets into networks. Attackers sporadically broadcast either random bits or conventional packets into networks to preserve energy and rotation between the sleep and jamming phases.

- Reactive Jamming: Attackers that use reactive jamming can monitor the legitimate channel's activity. If there is an activity, the attacker transmits a random signal to interfere with the existing signal on the channel.

Contaminating: Attackers seek to contaminate the channel estimate phase to gain unfair advantages in the communication phase that follows. In the same context, a feedback contamination attack means that the attacker can use falsified feedback to force the transmitter to command their beams to attackers different than the intended users.

Spoofing: Attackers try to enter or corrupt legitimate communications by transmitting a deceiving signal with a higher power in the transmission phase between transceivers or monitoring the legitimate transmitter for sending a falsified signal between two legitimate signals. This kind of attack has different implications, such as the intrusion of an adversary into the local network or injecting some falsified identity information. There are two types of spoofing attacks: identity spoofing attacks and Sybil attacks.

2. Physical Layer Security

The world has become increasingly online and connected via wireless networks recently. Additionally, wireless devices are increasingly employed in a variety of sectors. For example, smart things, mobile communication, unmanned platforms, drone control, autonomous driving, etc. Unlike wired networks, the openness of the wireless network allows nearly all wireless receiving devices within their range to receive signals [5][6]. This feature gives legal and illegal users the same access to the communication channel. However, protecting the integrity, confidentiality, and availability is challenging in wireless networks [5].

Information security mainly depends on cryptographic techniques to achieve communication security requirements, including authenticity, confidentiality, integrity, and availability [2][7][8]. Authenticity verifies communicating entities. Data integrity validates that transmitted data are not changed. Data confidentiality assures that transmitted data did not expose to unauthorized entities. Finally, data availability prevents adversaries from interrupting access to data.

Using encryption-based security technologies at application layers has enhanced wireless security. Still, their inherent vulnerabilities are heavy computation and key management, resulting in high complexity and resource consumption [7][8][9]. Cryptographic techniques have efficiently protected modern communication and computer networks. However, it is not entirely suited to the future of ubiquitous computing, which will be elaborated on in the following.

Traditional cryptographic approaches are computationally secure because the attacker cannot decipher the protection within a specific time. However, it may be compromised due to the progress in quantum computing advances. However, because of advances in quantum computing, it may be compromised. For example, the quantum search algorithms such as Grover's and Shor's algorithms exploited the discrete logarithm problem that

current cryptographic mechanisms heavily rely on [10]. Traditional authentication techniques are based on the IP or media access control (MAC) addresses as the identity, which can be easily tampered with by malware attackers [11][12]. In addition, cryptographic algorithms rely heavily on computational complexity and secret keys [13][14]. As a result, these algorithms perform effectively on devices with high processing capabilities, like smartphones. In comparison, many IoT devices are low cost and small, equipped with limited storage memory, and powered with batteries, making it impractical to implement complicated cryptography-based security protocols.

Shannon first considered the confidentiality of physical layer security (PLS) was assumed in 1949 and proposed the first application of information theory to cryptology, also known as Shannon's information-theoretic secrecy [15]. Then, approximately three decades later, one of the most targeted studies the physical layer confidentiality is to maximize the secret information rate received by the legitimate user in the wiretap channel, which is defined as the secrecy capacity by Wyner [16]. Wyner's work set the basis and inspired PLS research, with scholars proposing various PLS techniques for different purposes.

Wireless network security was previously thought to be a high-layer problem that could be handled with cryptographic approaches [17]. The situation changed in the first decade of the 21st century when wireless networks started to spread around [10]. Therefore, physical layer security based on information theory has appeared as a promising approach to protecting wireless communications to achieve information-theoretic security against eavesdropping attacks, for instance. Compared to cryptographic techniques executed at upper layers, physical layer security offers two significant advantages:

- First, physical layer security techniques do not rely on computational complexity compared to cryptography techniques [2][11][18][19][20]. As a result, the achieved level of security will not be compromised; even if the unauthorized devices in the wireless network are provided with powerful computational capabilities, secure and safe communications can still be performed.

- Second, physical layer security techniques have high scalability [18][20]. Wireless devices always join or exit the network at any time; due to the decentralized nature of the network, the PLS technique can provide secure data communication in the network.

3. Physical Layer Authentication

The inherent broadcast nature of wireless communications raises security and privacy issues where adversaries can launch different types of attacks. Accordingly, authentication is an important issue in wireless communications [21]. Device identity authentication requires safeguarding wireless networks to validate whether the users are legitimate and allowing them to access the network while preventing malicious users [12]. Most existing wireless communication systems perform authentication through upper-layer authentication techniques that are typically implemented using cryptography-based authentication algorithms [12]. However, traditional authentication approaches depend on software addresses such as IP and MAC addresses, which can be tampered with or forged

[22]. Once adversaries obtain the security credentials, they can pretend as legitimate users to reach private data and launch severe attacks on the wireless devices [22][23].

However, upper-layer authentication mechanisms based on traditional cryptography-based algorithms are unsuitable for advanced wireless communication systems [21]. For example, cognitive radio networks, Internet of Things (IoT), internet of vehicles (IoV), smart grids networks, and unmanned aerial vehicles (UAV) because of the following issues [3][12][21][24]: With the advancement in computational power and cryptanalysis algorithms, the time it takes to crack a cryptography key has been drastically reduced. However, because the upper layer signaling is not altered, the replayed signal can successfully spoof the legitimate receiver. Therefore, the complicated cryptography techniques in upper-layer operations, e.g., encryption, decryption, and frequent authentication handovers, are unsuitable with limited capability for wireless devices. Furthermore, the process of key sharing and management introduces overhead concerns in massive ubiquitous computing scenarios, such as the amount of storing excessive keys or defending against the eavesdropping attacks of frequent exchanging keys.

Wireless physical layer authentication is a method of validating a wireless transmitter by checking the physical layer characteristics of the communication [24]. A good authentication scheme should generally have three characteristics: covertness, robustness, and security [14], as demonstrated in **Figure 2**.

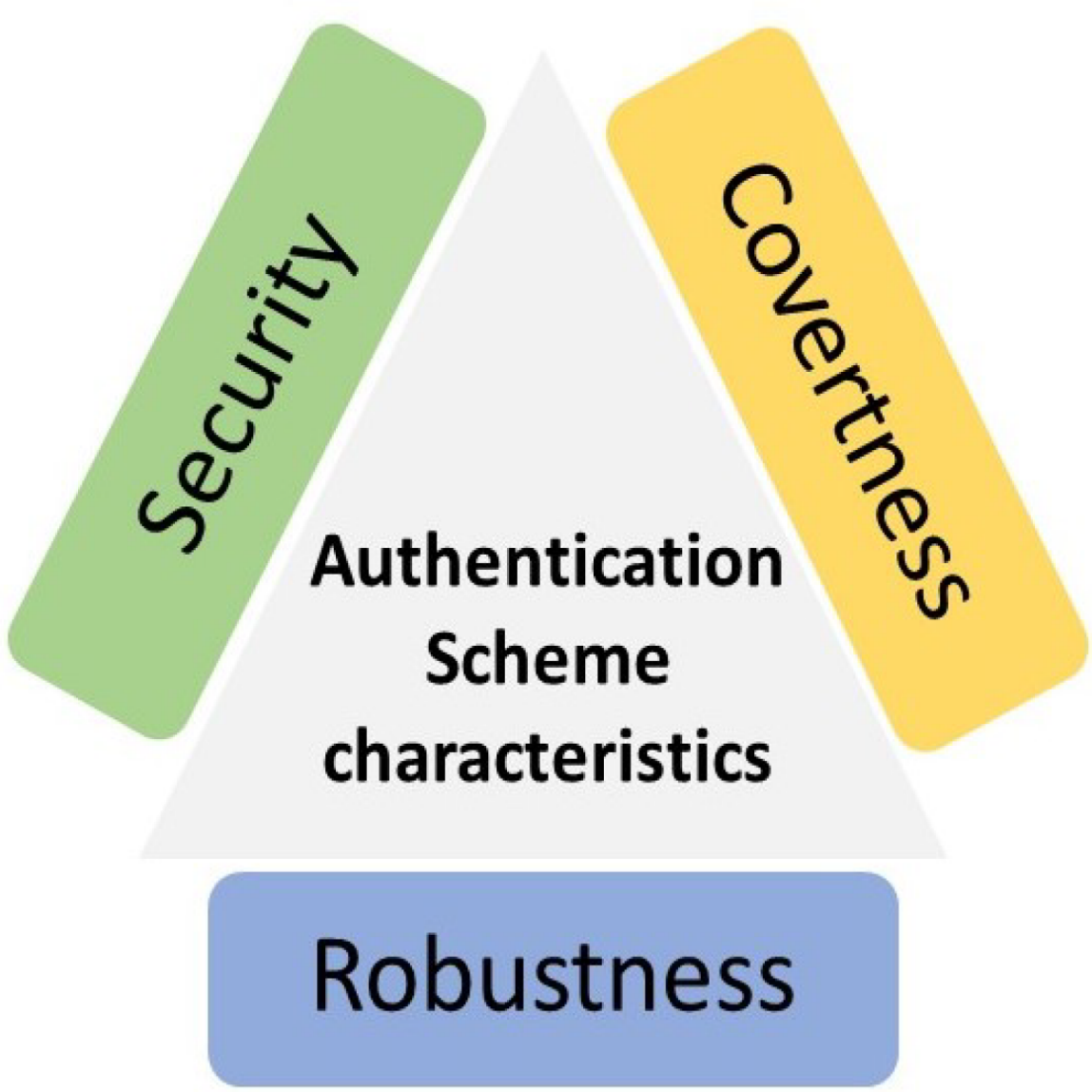

Figure 2. Authentication Scheme Characteristics.

- The covertness means that any authentication schemes should not significantly affect the performance of the standard data transmission, do not occupy too much communication overheads or extra computational resources, and do not harm the existing conventional higher-layer cryptographic-based techniques.
- Robustness requires that the PLA framework is robust enough to mitigate channel fading and noise interference.
- Security is the kernel of PLA systems, representing the ability to prevent the authentication procedure from being interrupted or invaded by eavesdroppers.

Recently, PLA has attracted much research interest compared to traditional secret key-based authentication techniques because of the following advantages [21][24]:

- The PLA allows a legitimate receiver to easily distinguish between a legitimate and adversary transmitter without upper-layer processing, decreasing computational complexity and processing delay.
- There is no key distribution and management need with PLA compared to conventional secret key-based authentication schemes. Instead, some existing physical layer authentication approaches rely on analog channel information and device-specific characteristics caused by manufacturing variability.
- In a heterogeneous coexistence system, incompatible devices may not be able to decode each other's upper-layer signaling, but they should be able to decode the physical layer bit-streams.
- The PLA presents information-theoretic security, where the physical layer puts adversaries in a state of uncertainty.

Physical Layer Authentication Techniques

The mostly studied authentication techniques can be classified into: radio frequency fingerprint-based and channel-based schemes.

Physical Layer Authentication based on Radio Frequency Fingerprint

Toonstra et al. [25] first proposed the concept of "radio frequency fingerprint" technology in 1995. radio frequency fingerprint is similar to human fingerprint biometric identifiers, but they are extracted from wireless signals [26]. Therefore, the radiofrequency fingerprint (RFF) can identify and classify wireless devices as an advanced technique for wireless security [12]. In addition, radio frequency (RF) fingerprinting can provide a novel approach for emitter identification using the external signal feature rather than the information content [27]. Radio frequency fingerprinting was created from the imperfections in components of a wireless device raised during the production process, which is a small feature reflected in the launching signal [22][23][28]. These imperfections deviate slightly from their nominal specifications and thus do not impact normal communication functions, allowing device identifiers to be obtained from the component's imperfections. Since the RFF of the wireless device defines unique characteristics that are very difficult to manipulate and forge [29].

Radio frequency fingerprint identification (RFFI) is a potential wireless device authentication technique that uses hardware fingerprints to identify wireless devices [22][23]. HALL et al. [30] proposed the concept of radio fingerprint identification in the wireless network device identification field. Because most IoT end nodes have limited computational and energy resources, the RFFI approach does not impose any additional power consumption on the devices to be authenticated. Consequently, RFFI is particularly suitable for low-cost wireless devices such as IoT [23]. The RF fingerprint-based identification comprises two phases: training and classification [12]. During the training phase, the receiver will first sample received signals from the devices under good channel quality, extract features, then save them as a reference template. In the classification phase, the receiver will acquire signals from prospect devices, compare the same type features with the reference template, and classify the devices based on similarity.

Channel Based Authentication

Since the wireless channel has the characteristics of space-variability, uniqueness, time-variation, and reciprocity, the communication channels between the transmitter and the receiver in different places are different. The physical layer characteristics verify the uniqueness of wireless channels on the communication parties. The physical layer authentication based on wireless channels uses the channel diversity generated by spatial variability to achieve authentication.

The PLA techniques can identify the legitimate and illegal nodes by examining channels characteristics, such as received signal strength (RSS), channel impulse response (CIR), channel state information (CSI), and channel frequency response (CFR). RSS symbolizes the strength of the received signal. On the other hand, the CIR is a practical tool for designing and implementing communications systems because it shows how the waveform changes as it transits through the environment [31]. Moreover, it captures the reflection, absorption, diffraction, delay, and attenuation. Furthermore, the CSI represents the channel feature of a communication link [32]. CSI describes characteristics and effects of, e.g., scattering, fading, and power decay on the wireless signal propagation from the transmitter to the receiver at specific carrier frequencies [33][34][35]. However, due to scattering and reflection, the CSI is difficult to predict and emulate. The wireless channel's uniqueness in time and space lets it map different places with spatial and temporal environment characteristics [36]. In the context of channel-based authentication schemes, both RSS and CIR show unique spatial properties due to path loss and multi-path effects [37]. Compared to physical layer features that reflect large-scale fading in the channel, CSI includes location information details and represents the deeper channel differences.

References

1. Rojas, P.; Alahmadi, S.; Bayoumi, M. Physical Layer Security for IoT Communications—A Survey. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LO, USA, 26–31 July 2021; pp. 95–100.
2. Liu, Y.; Chen, H.H.; Wang, L. Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. IEEE Commun. Surv. Tutor. 2017, 19, 347–376.
3. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. IEEE Internet Things J. 2019, 26, 8169–8181.
4. Xiao, L.; Reznik, A.; Trappe, W.; Ye, C.; Shah, Y.; Greenstein, L.; Mandayam, N. PHY-Authentication Protocol for Spoofing Detection in Wireless Networks. In Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA, 6–10 December 2010; pp. 1–6.
5. Germain, K.S.; Kragh, F. Physical-Layer Authentication Using Channel State Information and Machine Learning. In Proceedings of the 14th International Conference on Signal Processing and

Communication Systems (ICSPCS), Virtual, 14–16 December 2020; pp. 1–8.

6. Tian, Q.; Jia, J.; Hou, C. Research on Fingerprint Identification of Wireless Devices Based on Information Fusion. Mob. Netw. Appl. 2020, 25, 2359–2366.
7. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. IEEE J. Sel. Areas Commun. 2018, 36, 679–695.
8. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proc. IEEE 2016, 104, 1727–1765.
9. Yener, A.; Ulukus, S. Wireless Physical-Layer Security: Lessons Learned From Information Theory. Proc. IEEE 2015, 103, 1814–1825.
10. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. IEEE Open J. Commun. Soc. 2021, 2, 1901–1914.
11. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. Entropy 2018, 20, 730.
12. Peng, L.; Hu, A.; Zhang, J.; Jiang, Y.; Yu, J.; Yan, Y. Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme. IEEE Internet Things J. 2019, 6, 349–360.
13. Zhang, J.; Rajendran, S.; Sun, Z.; Woods, R.; Hanzo, L. Physical Layer Security for the Internet of Things: Authentication and Key Generation. IEEE Wirel. Commun. 2019, 26, 92–98.
14. Bai, L.; Zhu, L.; Liu, J.; Choi, J.; Zhang, W. Physical layer authentication in wireless communication networks: A survey. J. Commun. Inf. Netw. 2020, 5, 237–264.
15. Shannon, C.E. Communication theory of secrecy systems. Bell Syst. Tech. J. 1949, 28, 656–715.
16. Wyner, A.D. The wire-tap channel. Bell Syst. Tech. J. 1975, 54, 1355–1387.
17. Rodriguez, L.J.; Tran, N.H.; Duong, T.Q.; Le-Ngoc, T.; Elkashlan, M.; Shetty, S. Physical layer security in wireless cooperative relay networks: State of the art and beyond. IEEE Commun. Mag. 2015, 53, 32–39.
18. Wang, D.; Bai, B.; Zhao, W.; Han, Z. A Survey of Optimization Approaches for Wireless Physical Layer Security. IEEE Commun. Surv. Tutor. 2019, 21, 1878–1911.
19. Sánchez, J.D.V.; Urquiza-Aguiar, L.; Paredes, M.C.P. Physical Layer Security for 5G Wireless Networks: A Comprehensive Survey. In Proceedings of the 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, 23–25 October 2019; pp. 122–129.
20. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M.D. Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. 2015, 53, 20–27.

21. Xie, N.; Li, Z.; Tan, H. A Survey of Physical-Layer Authentication in Wireless Communications. IEEE Commun. Surv. Tutor. 2021, 23, 282–310.
22. Shen, G.; Zhang, J.; Marshall, A.; Peng, L.; Wang, X. Radio Frequency Fingerprint Identification for LoRa Using Spectrogram and CNN. In Proceedings of the IEEE INFOCOM 2021 IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021.
23. Shen, G.; Zhang, J.; Marshall, A.; Peng, L.; Wang, X. Radio Frequency Fingerprint Identification for LoRa Using Deep Learning. IEEE J. Sel. Areas Commun. 2021, 39, 2604–2616.
24. Wang, Q.; Li, H.; Zhao, D.; Chen, Z.; Ye, S.; Cai, J. Deep Neural Networks for CSI-Based Authentication. IEEE Access 2019, 7, 123026–123034.
25. Toonstra, J.; Kinsner, W. Transient analysis and genetic algorithms for classification. In Proceedings of the IEEE WESCANEX 95. Communications, Power, and Computing. Conference Proceedings, Winnipeg, MB, Canada, 15–16 May 1995; Volume 2, pp. 432–437.
26. Knox, D.A.; Kunz, T. RF Fingerprints for Secure Authentication in Single-Hop WSN. In Proceedings of the 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Avignon, France, 18–20 December 2008; pp. 567–573.
27. Zhuo, F.; Huang, Y.; Chen, J. Radio Frequency Fingerprint Extraction of Radio Emitter Based on I/Q Imbalance. Procedia Comput. Sci. 2017, 107, 472–477.
28. Li, Z.; Yin, Y.; Wu, L. Radio Frequency Fingerprint Identification Method in Wireless Communication. In Proceedings of the International Conference on Machine Learning and Intelligent Communications, Hangzhou, China, 6–8 July 2018; pp. 195–202.
29. Lin, Y.; Jia, J.; Wang, S.; Ge, B.; Mao, S. Wireless Device Identification Based on Radio Frequency Fingerprint Features. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Virtual, 7–11 June 2020; pp. 1–6.
30. Hall, J.; Barbeau, M.; Kranakis, E. Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase. Wirel. Opt. Commun. 2003, 13–18.
31. Candell, R. Radio Frequency Measurements for Selected Manufacturing and Industrial Environments. NIST Tech. Rep. 2016.
32. Liao, R.F.; Wen, H.; Wu, J.; Pan, F.; Xu, A.; Jiang, Y.; Xie, F.; Cao, M. Deep-Learning-Based Physical Layer Authentication for Industrial Wireless Sensor Networks. Sensors 2019, 19, 2440.
33. Ma, Y.; Zhou, G.; Wang, S. WiFi Sensing with Channel State Information: A Survey. ACM Comput. Surv. 2019, 52, 1–36.
34. Wang, Z.; Dou, W.; Ma, M.; Feng, X.; Huang, Z.; Zhang, C.; Guo, Y.; Chen, D. A Survey of User Authentication Based on Channel State Information. Wirel. Commun. Mob. Comput. 2021, 2021, 6636665.

35. Hua, J.; Sun, H.; Shen, Z.; Qian, Z.; Zhong, S. Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications, Honolulu, HI, USA, 15–19 April 2018; pp. 1700–1708.
36. Li, X.; Huang, K.; Wang, S.; Xu, X. A physical layer authentication mechanism for IoT devices. China Commun. 2021, 19, 129–140.
37. Liu, H.; Wang, Y.; Liu, J.; Yang, J.; Chen, Y.; Poor, H.V. Authenticating Users Through Fine-Grained Channel Information. IEEE Trans. Mob. Comput. 2018, 17, 251–264.