A Survey of Physical-Layer Authentication in Wireless Communications

Ning Xie, *Senior Member, IEEE*, Zhuoyuan Li, and Haijun Tan

***Abstract*—Authentication is an important issue in wireless communications because the open nature of the wireless medium provides more security vulnerabilities. Recently, Physical-Layer Authentication (PLA) attracts many research interests because it provides information-theory security and low complexity. Although many researchers focus on the PLA and exploit its potential in enhancing wireless security, the literature is surprisingly sparse with no comprehensive overview of the state-of-the-art PLA and the key fundamentals involved. Thus, this article provides a detailed survey of features and techniques that can be used in the PLA. We categorize the existing PLA schemes into two categories: passive and active schemes. In the passive schemes, a receiver authenticates the transmitter based on the physical-layer features of the received signals. We further divide the passive schemes into two sub-categories: device-based features and channel-based features. In the active schemes, a transmitter generates a tag based on a secret key and embeds it into a source message. Then, a receiver authenticates the transmitter based on the tag whether it exists in the received signal. We further divide active schemes into two sub-categories: non-covert schemes and covert schemes. Moreover, we also provide some future research directions.**

***Index Terms*—Physical-layer authentication, passive, active, robustness, covertness, security.**

I. Introduction

A. Background

WIRELESS communication services are rapidly increasing because of the proliferation of mobile devices and the advent of the Internet of Things (IoT). Authentication is an important issue in wireless communications because the open nature of the wireless medium provides more security vulnerabilities. Most of existing wireless communication systems achieve the authentication goal via upper-layer authentication mechanisms. The security of upper-layer authentication mechanisms is ensured by using conventional cryptography-based algorithms. However, upper-layer authentication mechanisms based on conventional cryptography-based algorithms are not applicable for emerging wireless communication systems, e.g., IoT, Internet of Vehicles (IoV), Smart Grids (SG) networks, Cognitive Radio (CR) networks, and Unmanned Aerial Vehicles (UAV) because of the following limitations. The first and most important limitation is that the security level of cryptography-based algorithms is achieved based on the assumption of computational limitation in cryptographic tools. However, the assumption of computational limitation has been gradually broken as either computational power or cryptanalysis algorithms are rapidly developing. If an adversary cracks a cryptography-based algorithm, various attacks can be launched, e.g., spoofing attacks. For example, in SG systems, the price of energy and the information of the user's energy demand will be leaked. On the other hand, the adversary can use false information to deceive power-supply bureaus or customers. The second limitation is that cryptography-based algorithms are vulnerable to replay attacks. In replay attacks, an adversary only recovers the physical-layer bitstream rather than crack the cryptography-based algorithm and then directly forward the recovered signal to the legitimate receiver. Then, the replayed signal can successfully spoof the legitimate receiver, because the upper-layer signaling is not modified at all. The replay attacks can jam the key nodes of a wireless communication system, e.g., smart meters in an SG system. The third limitation is that cryptography-based algorithms introduce high communication overhead and complexity due to the complicated upper-layer operations, e.g., encryption and decryption. High communication overhead and complexity inevitably increase the device cost, which is not feasible for low-cost terminals, e.g., IoT, IoV, UAV, and massive machine-type communication, because these systems are inherently delay-sensitive, or power-limited, or processing-restricted. The fourth limitation is that cryptography-based algorithms require the process of key sharing and management. The process of key sharing and management introduces high cost, e.g., the cost of storing excessive keys, or the cost of defending against the eavesdropping attacks of frequent exchanging keys, which are especially challenging in large-scale heterogeneous and decentralized wireless networks.

B. Physical Layer Authentication (PLA)

Recently, Physical-Layer Authentication (PLA) attracts many research interests because of the following advantages. First, the PLA protects a physical-layer feature or a tag by presenting the adversaries with noisy observation only, which

Manuscript received May 6, 2020; revised September 6, 2020 and October 17, 2020; accepted November 27, 2020. Date of publication December 3, 2020; date of current version February 24, 2021. This work was supported in part by the Natural Science Foundations of China under Grant 61972262; in part by the National Key Research and Development Project of China under Grant 2020YFB1805404; in part by the Natural Science Foundation of Guangdong, China, under Grant 2016A030313046; in part by the Fundamental Research Programs of Shenzhen City under Grant JCYJ20180305124648757; and in part by the China Scholarship Council under Grant 201908440031. *(Corresponding author: Ning Xie.)*

The authors are with the Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: ningxie@szu.edu.cn).

Digital Object Identifier 10.1109/COMST.2020.3042188

provides information-theoretic security. Specifically, the physical layer introduces the uncertainty on the adversaries, which cannot be broken by any increase in computational ability since the adversaries randomly guess it bit by bit. The theoretical underpinning of the PLA mechanisms can be explained by Shannon's information-theory secrecy analysis [1]. Note that although the legitimate receiver also observes the noisy version of the tag, the legitimate receiver only deals with the easier problem as compared with that of the adversary. Specifically, the legitimate receiver solves a one-bit detection problem whereas the adversary should solve a multi-symbols estimation problem. The adversary should accurately estimate all symbols of the tag before she attempts to infer the secret key from the estimated tag. In comparison with a one-bit detection problem, a multi-symbols estimation problem requires a extremely higher Signal-to-Interference-plus-Noise Ratio (SINR) for the received signal, which is a natural advantage of the PLA. Second, the PLA allows a legitimate receiver to quickly distinguish between a legitimate transmitter and a rogue one without upper-layer processing, which significantly saves both computational complexity and processing delay. Third, the PLA provides high compatibility, since incompatible devices may not be able to decode each other's upper-layer signaling but should decode the physical-layer bit-streams in a heterogeneous coexistence system [2]. At last, we should emphasize that a PLA scheme is not designed to replace an upper-layer authentication scheme. On the contrary, a PLA scheme is designed to compensate for an upper-layer authentication scheme, which provides a higher security level. For example, the PLA allows us to construct a two-factor authentication system with both authentication mechanisms at the physical layer and those at the upper layers. Specifically, the upper-layer authentication mechanism is used to authenticate the identification of a legitimate user while the PLA mechanism is used to authenticate the device used by the legitimate user. For example, a legitimate user can use different devices at different times, e.g., a mobile phone at one time and an iPad at another time. For another example, a legitimate user can use different devices at the same time, e.g., a distributed-antennas system. If the receiver can authenticate both the identification and the device of the legitimate user, the security level of the two-factor authentication system should be higher than using only one authentication mechanism.

We categorize the existing PLA schemes into two categories: passive and active schemes. In the passive schemes, a receiver authenticates the transmitter based on the physical-layer features of the received signals, e.g., Radio Frequency (RF) characteristics [3] or channel characteristics [4]. In the active schemes, a transmitter generates a tag based on a secret key and embeds it into a source message. Then, a receiver authenticates the transmitter by checking whether the tag exists in the received signal [5]–[9]. The fundamental difference between the two categories is whether the source message is modified on purpose according to the tag or not. Specifically, a passive scheme does not modify the source message at all whereas an active scheme modifies the source message for providing additional physical-layer features. Note that the PLA effectively defend against replay attacks, because the physical-layer features or the tags are often time-varying. For example, if an adversary replays an outdated signal to the legitimate receiver, the legitimate receiver can detect the replay attack by comparing the current tag with the previous tags.

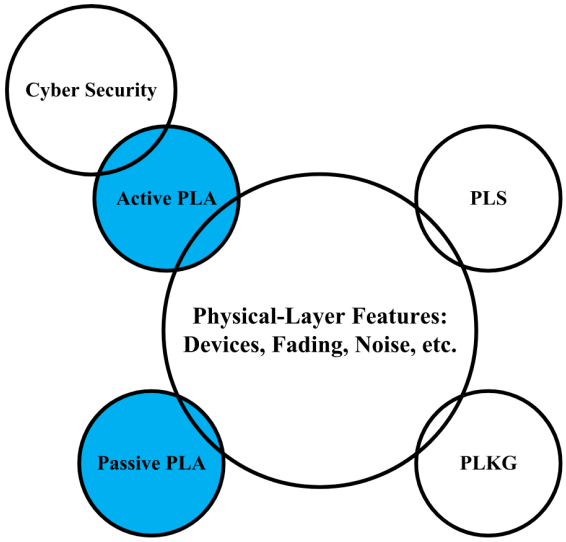

Fig. 1. Relationship between different security techniques.

Wang *et al.* analyzed the performance of various passive schemes [10], where several constraints of passive schemes in practical situations were discussed, such as RF fingerprint origins, multipath effect, device movement, and receiver complexity. Wang *et al.* reviewed the passive schemes and discussed the limitation of existing passive schemes [11]. Xu *et al.* and Liu *et al.* provided different surveys of passive schemes in [12] and [13], respectively. Mukherjee *et al.* discussed the different passive scheme and active scheme [14], e.g., the information-theoretic analysis of authentication in noiseless environment [15], [16] and noise environment [17], the device-based passive schemes, the channel-based passive schemes, and the superimposition active schemes. Bai *et al.* proposed a general architecture of the PLA, which includes security models and common threat models [18]. In [18], both passive and superimposition schemes were reviewed. We compare different contributions among existing survey papers of the PLA in Tab. II.

C. Comparisons Between the PLA and Other Physical-Layer Security Techniques

Besides the physical layer provides a promising authentication mechanism, it also provides other security techniques, e.g., the Physical Layer Security (PLS) and Physical Layer Key Generation (PLKG) [2], [19]–[21]. Here, we discuss the relationship between different security techniques, as illustrated in Fig. 1.

The PLS provides a confidential transmission by exploiting the physical-layer features without using shared secret keys. Accordingly, the objective of the PLS is to use a transmission technique that delivers the confidential messages to a

* refers to a signal that a device sends to indicate that data has been received successfully

TABLE I
LIST OF ABBREVIATIONS

Abbreviations	Full Name	Abbreviations	Full Name
*ACK	ACKnowledge	AP	Access Point
AN	Artificial Noise	ANN	Artificial Neural Networks
AoA	Angle of Arrival	AR	Auto-Regressive
AUC	Area Under the Curve	BAN	Body Area Networks
BER	Bit Error Rate	BKIC	Blind Known Interference Cancellation
BT	Bagged Trees	CFO	Carrier Frequency Offset
CFR	Channel Frequency Response	CFBG	Code-Frequency Block Group
CIR	Channel Impulse Response	CLRT	Classical Likelihood Ratio Test
CNN	Convolutional Neural Network	CPS	Cyber Physical System
CP	Cyclic Prefix	CR	Cognitive Radio
CRNN	Convolutional Recurrent Neural Network	CRP	Challenge-Response Pair
CS	Compressed Sensing	CSI	Channel State Information
DCTF	Differential Constellation Trace Figure	DGT	Discrete Gabor Transform
DNN	Deep Neural Network	DSSS	Direct Sequence Spread Spectrum
DT	Decision Tree	DT-CWT	Dual-Tree Complex Wavelet Transform
ELM	Extreme Learning Machine	EM	Expectation Maximization
GLRT	Generalized Likelihood Ratio Tests	GMM	Gaussian Mixture Model
IC	Integrated Circuit	ICA	Independent Component Analysis
ICC	Independence-Checking Coding	ICMP	Internet Control Message Protocol
IoT	Internet of Thing	IoV	Internet of Vehicle
KNN	K-Nearest Neighbor	LLRT	Logarithmic Likelihood Ratio Test
LRT	Likelihood Ratio Test	MDA/ML	Multiple Discriminant Analysis/Maximum Likelihood
MEP	Minimum Error Probability	MIMO	Multi-Input Multi-Output
MKL	Multiple Kernel Learning	ML	Machine Learning
NE	Nash Equilibrium	NIC	Network Interface Cards
NP	Neyman-Pearson	PAM	Partitioning Around Medoids
PCA	Principal Component Analysis	PCP	Pre-coded Cyclic Prefix
PD	Probability of Detection	PFA	Probability of False Alarm
PHY-CF	Physical-layer Cover-Free	PLA	Physical Layer Authentication
PLKG	Physical Layer Key Generation	PLS	Physical Layer Security
PMD	Probability of Missed Detection	PSA	Probability of Security Authentication
PSD	Power Spectral Density	PUE	Primary User Emulation
PUF	Physical Unclonable Function	RF	Radio Frequency
RSS	Received Signal Strength	RNN	Recurrent Neural Network
RV	Random Variable	ROC	Receiver Operating Characteristic
SBDC	Subcarrier-Block Discriminating Coding	SAP	Subcarrier Activation Patterns
SDR	Software-Defined Radio	SG	Smart Grids
SINR	Signal-to-Interference-plus-Noise Ratio	SNR	Signal to Noise Ratio
SVM	Support Vector Machine	UAV	Unmanned Aerial Vehicles
UAR	Uniform Angular Rotation	UDP	User Datagram Protocol
UDR	Uniform Distance Rotation	UML	Unsupervised Machine Learning
UHF	Ultra-High Frequency	USRP	Universal Software Radio Peripheral
TDM	Time-Division Multiplexing	TSF	Time Synchronization Function
VG	Visibility Graph	VLC	Visible Light Communication
WEAN	Wireless Energy Auditing Network	WSN	Wireless Sensor Network

TABLE II
COMPARISON OF DIFFERENT CONTRIBUTIONS AMONG EXISTING SURVEY PAPERS OF THE PLA

Authors	Year	Contributions
Mukherjee *et al.* [14]	2014	Both passive and superimposition schemes were reviewed. The information-theoretic analysis of authentication in both noiseless and noisy environment was also discussed.
Xu *et al.* [12]	2016	Passive schemes with device-based features were reviewed.
Wang *et al.* [11]	2016	Passive schemes were reviewed and the limitations of existing passive schemes were also discussed.
Liu *et al.* [13]	2017	Passive schemes were briefly reviewed and multiple physical-layer security techniques were discussed.
Bai *et al.* [18]	2020	Security models and common threat models in the PLA were discussed. Both passive and superimposition schemes were reviewed.

legitimate receiver but ensures that the adversary is unable to decode the transmitted confidential messages. For example, the secrecy provided by the PLS is possible when the adversary's SINR is naturally lower than the legitimate receiver's SINR because of the channel quality, or is made lower than the legitimate receiver's SINR because of a special technique, e.g., channel coding, channel-based adaption, injection of artificial noises.

The PLKG provides a secret-key agreement between the legitimate transmitter and receiver over a random broadcast

channel, where both the legitimate receiver and the adversary have access to it. Note that the adversary has full access to it with non-identical observations to that of the legitimate receiver. Accordingly, the objective of the PLKG is to extract random keys from the channel between the legitimate transmitter and receiver but the adversary is unable to extract the same keys. For example, the basic steps of the PLKG include: probing the random channel to obtain random correlated measurements at transceivers; extracting channel features; generating secret random keys by performing channel quantization; implementing privacy reconciliation to avoid the mismatch of the secret keys between transceivers; implementing privacy amplification to improve the randomness of the secret keys.

Although all of the PLA, PLS, and PLKG schemes are designed based on the physical-layer features, they have different objectives and different limitations. Mukherjee *et al.* provided a comprehensive comparison between the PLS and PLA [14]. The PLS has the following limitations.

- Adversary's SINR should be less than the legitimate receiver's one;
- Adversary's fading should be more severe than the legitimate receiver's one;
- Secrecy capacity is achieved at the expense of achievable capacity reduction;
- Sensitive to channel estimation errors;
- Sensitive to multiple channel observations from multiple cooperative adversaries.

The PLKG has the following limitations.

- Different receivers should have spatial channel decorrelation;
- Legitimate transceivers have channel reciprocity;
- Channel variation should exist in temporal, spectral, or spatial domains;
- Adversary should have limited computational resources;
- Sensitive to channel estimation errors and reciprocity mismatch errors;
- Sensitive to the capability of the adversary to estimate the legitimate channel.

The objective of the PLA is to authenticate the origin of the received signal based on the physical-layer features. For example, the passive PLA achieves an authentication by comparing the physical-layer features of an unknown transmitter with ones of the legitimate transmitter. The active PLA uses the cyber security to generate a shared tag between legitimate transceivers and achieves an authentication by checking whether the tag exists in the received signal, where the randomness of physical-layer features protects the tag from adversary's eavesdropping. From a secure system point of view, the PLA is more important than other physical-layer security techniques, because a receiver should first authenticate the origin of the received signal. Then, if the authentication test is passed, the receiver can reliably decode confidential messages. More importantly, the PLA can effectively defend against active attacks, e.g., impersonation or substitution, and passive attacks, e.g., eavesdropping. However, both existing PLS and PLKG can only defend against passive attacks rather than active attacks.

D. Motivation

Although many researchers focus on the PLA and exploit its potential in enhancing wireless security, the literature is surprisingly sparse with no comprehensive overview of the state-of-the-art PLA and the key fundamentals involved. Thus, the main motivation of this article is to provide a detailed survey of features and techniques that can be used in the PLA. Moreover, the applications of the PLA to some emerging wireless systems have been demonstrated in recent years. Thus, it is worthy to review the most recent state-of-the-art PLA schemes, which not only makes the community aware of these research results but also manifests new research opportunities and directions.

E. Contributions

In this article, we introduce a comprehensive taxonomy for the PLA. Specifically, we divide passive schemes into three sub-categories: device-based features, channel-based features, and extend passive schemes which can be described as follows.

1) Device-based features reflect the hardware imperfection of the transmitting device, such as Carrier Frequency Offset (CFO) [22], I/Q imbalance [23], and clock skew [24]. The device-based features are hardware-specific and unique, even the transmitting devices are produced by the same manufacturer.
2) Channel-based features reflect the channel information between the legitimate transmitter and receiver, such as Received Signal Strength (RSS) [25] and Channel State Information (CSI) [26]. The channel-based features have a basic assumption that the channel-based features of different transmitting devices should have strong spatial decorrelation. Specifically, in a rich scattering environment, if the distance between two transmitting devices is more than a half wavelength, the channel-based features from different transmitters to the same receiver can be regarded as totally uncorrelated. On the contrary, if the channel is not rich scattering and an adversary is located in close proximity to the legitimate transmitter, the passive schemes with channel-based features may fail because the channel-based features of different transmitting devices become similar.
3) Extended passive scheme contains three types of enhanced passive schemes. First, the hybrid scheme utilized both device-based features and channel-based features to further improve the authentication accuracy [27]. Second, unsupervised Machine Learning (UML) was used to classify the obtained feature for making an authentication without the training stage [28]. Third, artificial Noise (AN) was used to further improve the security [29].

A good-designed PLA scheme should consider three properties: robustness, security, and covertness. For ensuring the robustness, it is highly desirable that a PLA scheme be resistant to channel fading and noise effects as wireless transmissions are present in random fading environments. For ensuring security, a PLA scheme should make the inability of the adversary to mount successful attacks. For ensuring

* An active attack is a type of attack in which hackers modify the information or the data. In contrast, a passive attack is an attack in which hackers do not modify the information or the data.

the covertness, a PLA scheme cannot obviously sacrifice the decodability of the source message. Since the passive schemes do not embed any tag into the source message, they only consider both the robustness and security excluding the covertness. On the contrary, the active schemes should consider the robustness, security, and covertness together. Thus, we divide active schemes into two sub-categories: non-covert schemes and covert schemes, which can be described as follows.

1) In non-covert schemes [30], [31], since the covertness is not considered in the design of an active scheme, such an active scheme can only be used at an aware receiver rather than at an unaware receiver, which hinders its extensive application. Moreover, it is challenging to construct a two-factor authentication system with both authentication mechanisms at the physical layer and those at the upper layers.
2) In covert schemes [7], [32], since the covertness is considered in the design of an active scheme, the negative effect of embedding a tag into a source message can be kept under control through adjusting the parameters of the active scheme. On the one hand, although an unaware receiver does not know the detail of the active scheme, she can authenticate a transmitting device through a certain upper-layer authentication scheme. On the other hand, an aware receiver not only authenticates the transmitting device but also constructs a two-factor authentication system for higher security. Moreover, higher covertness often leads to higher security since it becomes more challenging for adversaries to detect the existence of the tag in their observed signals.

F. Organization

We organize the remainder of this article as follows. In Section II, we introduce the system model and overview of the PLA, including passive and active schemes. In Section III, we introduce passive schemes, including the device-based passive PLA, channel-based passive PLA, and extended passive PLA. In Section IV, we introduce active schemes, including the non-covert active PLA and the covert active PLA. Future research directions and concluding remarks are provided in Sections V and VI, respectively. We present the organizational structure of this article in Fig. 2. For facilitating reading, we give a summary of abbreviations in Tab. I.

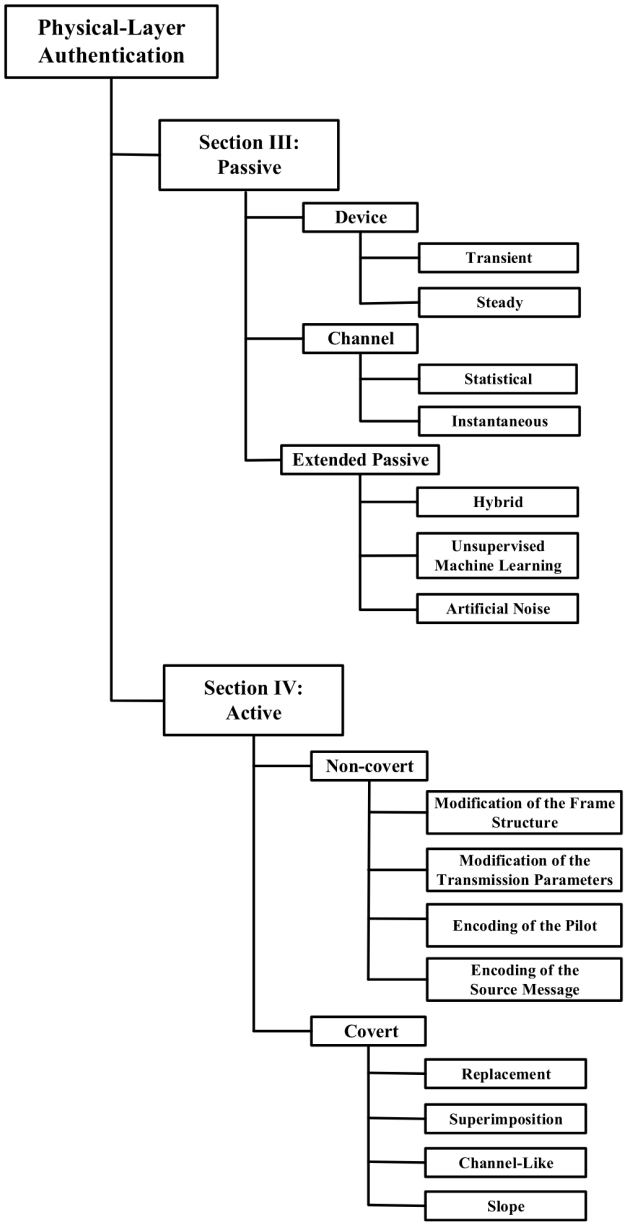

Fig. 2. Organizational structure of this article.

II. System Model and Overview of the PLA

A. System Model of the PLA

In this article, we consider a typical scenario of the PLA in wireless communications with four nodes and illustrate the system model in Fig. 3.

- Alice, as a legitimate transmitter, wants to communicate with Bob.
- Bob, as a legitimate receiver, receives a transmitted signal and authenticates the origin of the received signal using a certain PLA scheme to defend against active attacks, such as impersonation attacks and Sybil attacks. The role of Bob's authentication performance is to evaluate the **robustness** level of the PLA scheme under active attacks.
- Eve, as an adversary, eavesdrops all wireless transmissions between Alice and Bob, or sends a forged signal to Bob by impersonating Alice. Since Eve acts as an aware receiver, we assume that Eve knows everything about the PLA scheme except the privacy information between Alice and Bob. Under passive attacks, Eve attempts to infer the privacy information from her observations. The role of Eve's eavesdropping capability is to evaluate the **security** level of the PLA scheme under passive attacks.
- Carol, as an unaware receiver, receives the transmitted signal but authenticates the origin of the received signal through upper-layers authentication mechanisms. The role of Carol's reception performance is to evaluate the **covertness** level of the PLA scheme.

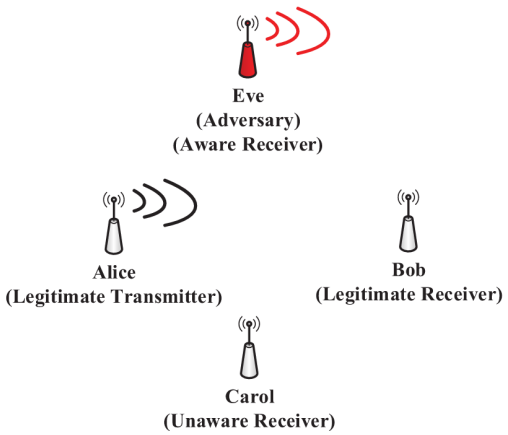

Fig. 3. System model of the PLA in wireless communications with four nodes.

We categorize the existing PLA schemes into two categories: passive and active schemes.

- In passive schemes, Bob authenticates the transmitter based on the physical-layer features of the received signals.
- In active schemes, Alice first generates a tag based on a secret key shared between Alice and Bob. Then, Alice embeds the tag to a source message to generate a tagged signal. At last, Alice sends the tagged signal to Bob over a wireless channel. Bob authenticates the transmitter by checking whether the tag exists in the received signal.

Note that the passive schemes use some natural features to authenticate the transmitter whereas the active schemes use an artificial feature, i.e., the tag, to realize the same goal. Thus, the privacy information in the passive schemes is the physical features whereas one in the active schemes is the secret key. Since the passive schemes do not embed any tag into the source message, they only consider both the robustness and security excluding the covertness. On the contrary, the active schemes should consider the robustness, security, and covertness together.

For the ease of presentation, an authentication decision at Bob is modeled as a threshold test under the following hypotheses:

$$\begin{aligned} &\mathcal{H}_0 : \text{Legitimate Signal;} \\ &\mathcal{H}_1 : \text{Forged Signal.} \end{aligned} \tag{1}$$

The main role of the PLA is to assure that Bob reliably distinguishes the hypothesis $\mathcal{H}_0$ from the hypothesis $\mathcal{H}_1$.

B. Overview of the PLA

1) Passive Schemes: The passive schemes generally consist of two stages: a training stage and a message-transmission stage. We illustrate the flow diagram of the passive schemes in Fig. 4 and outline the corresponding detailed steps in Algorithm 1. There are two assumptions in the passive schemes.

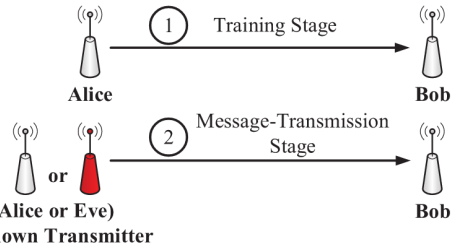

Fig. 4. Flow diagram of the passive schemes.

Algorithm 1: Detailed Steps of the Passive Schemes

In the training stage:
Step 1: Alice sends a request to Bob for message transmissions over a wireless channel.
Step 2: Bob receives the request at time t_1.
Step 3: Bob first checks whether the request is legitimate or not through upper-layers authentication mechanisms. Then, if it is legitimate, Bob extracts some physical-layer features from the received signal to construct a white list; otherwise, Bob ignores the request.
Step 4: Bob sends an ACK to Alice for preparing a message transmission.

In the message-transmission stage:
Step 1: Alice sends a legitimate message to Bob over the same wireless channel as that in the training stage.
Step 2: Bob receives a signal transmitted from an unknown transmitter at time t_2.
Step 3: Bob extracts physical-layer features from the current received signal and compares them with corresponding ones of the white list. Based on the comparison result, Bob can determine whether these features exist in the white list. If yes, Bob accepts the received signal; otherwise, Bob rejects it.

- The first assumption is that the security of the training stage is achieved through upper-layers security mechanisms, e.g., encryption algorithms. The first assumption ensures that all features in the white list are legitimate.
- The second assumption is that the time interval between two stages should be sufficiently short, e.g., $t_2 - t_1 \leq \tau$, where τ represents the coherence time of a wireless channel. The second assumption ensures that the legitimate features in the training stage are strongly correlated with those in the message-transmission stage. On the contrary, if the time interval is beyond the coherence time of a wireless channel, e.g., a fast time-varying channel, the passive schemes with channel-based features may fail because the channel-based features of the same transmitting device become uncorrelated.

Moreover, the features in the white list should satisfy two requirements for making a reliable authentication decision.

- First, these features should have high robustness during the entire period of an authentication process regardless of communication environment changes, or user mobility, or both factors.

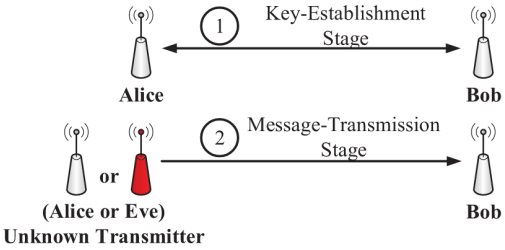

Fig. 5. Flow diagram of the active schemes.

- Second, these features should have high security for defending against adversaries' impersonation. In other words, it is extremely challenging for adversaries to extract these features from their received signals and even forge them. For example, the location-specific nature of the channel-based features cannot be arbitrarily controlled on purpose and the channel-based features of two transmitters with half-wavelength distance can be treated as completely independent of each other in a wireless environment with large multi-paths and rich scatters.

We divide the passive schemes into two sub-categories: device-based features and channel-based features, which will be introduced in Sections III and IV, respectively. Furthermore, we will introduce three types of extended passive schemes in Section V. The first type is a hybrid scheme that jointly exploits both device-based features and channel-based features to further improve the robustness. Although the hybrid scheme has better robustness, it increases the communication overhead and computational complexity. The second type is to relax the need for a training stage by using Unsupervised Machine Learning (UML) approaches. Although the UML-based schemes do not require a training stage to construct a white list, it requires a sufficient number of received samples to obtain the satisfying output of a UML approach. Moreover, the UML-based schemes only detect the abnormality among massive received signals but they cannot specifically detect which received signal is forged. The third type is the technique of Artificial Noise (AN) that introduces additional noise into the transmitted signal at Alice. The AN in the PLA has two advantages: it improves the resolution of the estimated PSD at Bob and improves security by introducing more uncertainty at Eve.

2) Active Schemes: The active schemes generally consist of two stages: a key-establishment stage and a message-transmission stage. We illustrate the flow diagram of the active schemes in Fig. 5 and outline the corresponding detailed steps in **Algorithm 2**. There is one assumption in the active schemes: the key-establishment stage should be secure. In other words, the symmetric secret key cannot be captured by adversaries, which is achieved through a key establishment protocol, e.g., the Diffie-Hellman key establishment protocol. Although an upper-layer scheme also can authenticate the transmitter with the help of the symmetric secret key, the active schemes have the following advantages. First, an active scheme provides information-theory security since it protects the tag by presenting the adversaries with noisy observation only. Second, an active scheme has low complexity since it allows a legitimate receiver to quickly distinguish between a legitimate transmitter without upper-layer processing.

Algorithm 2: Detailed Steps of the Active Schemes

In the key-establishment stage:
Step 1: Alice sends a request to Bob for message transmissions over a wireless channel.
Step 2: Bob receives the request.
Step 3: Bob first checks whether the request is legitimate or not through upper-layers authentication mechanisms. Then, if it is legitimate, Bob generates a symmetric secret key with Alice using a certain key establishment protocol, such as any protocols of public-private key pairs; otherwise, Bob ignores the request.
Step 4: Bob sends an ACK to Alice for preparing a message transmission.

In the message-transmission stage:
Step 1: Alice generates a tag based on the secret key and a hash function. Then, Alice actively embeds the tag into a source message to generate a tagged signal. At last, Alice sends the tagged signal to Bob over a wireless channel.
Step 2: Bob receives the signal transmitted from an unknown transmitter.
Step 3: Bob regenerates the tag with the help of the secret key. Then, Bob detects whether the tag exists in the received signal or not. If yes, Bob accepts the received signal. Then, Bob decodes the source message from the received signal and sends it to upper-layer applications. If no, Bob directly rejects the received signal.

Note that, unlike the passive schemes, the active schemes should consider not only the robustness and security but also the covertness since the operation of embedding a tag into a source message inevitably affects the reception performance of the source message at Carol. Based on whether the covertness is considered in the design of an active scheme, we divide the active schemes into two sub-categories: non-covert and covert schemes, which will be introduced in Sections IV-A and IV-B, respectively.

Here, we summarize the differences between passive PLA and active PLA in Tab. III. For the passive PLA, there is a trade-off between security and robustness. For example, if a feature provides higher robustness because of its high stability for the channel environment, its security may become weaker because it is easier to be captured by adversaries. For the active PLA, there is a trade-off among covertness, security, and robustness. For example, if a tag is allocated with higher transmission power, the robustness is significantly improved. However, the higher transmission power of the tag corresponds to low covertness and low security, because it introduces more negative effects on the source message and it is easier to be detected by adversaries. In summary, if the covertness is considered as the first priority, the passive PLA is a better option; Otherwise, the active PLA is preferable.

TABLE III
COMPARISON BETWEEN PASSIVE PLA AND ACTIVE PLA

Categories	Passive PLA	Active PLA
Metrics	Security and robustness.	Covertness, security, and robustness.
Authentication Features	Device-based features or channel-based features.	Modification of the source message or authentication tag.
Advantages	No covertness issue.	Robustness is independent of the coherence time, channel environment, and user movement.
Disadvantages	Robustness is determined by the coherence time, channel environment, and user movement.	Covertness issue.
Trade-offs	Trade-off between security and robustness.	Trade-off among covertness, security, and robustness.
Applications	Dual-hop wireless network [33], OFDM system [34], CDMA system [35], relay network [36], cyber-physical systems [37], WiFi system [38], Bluetooth system [39], ZigBee system [40], OFDM system [3], WiMax System [41], NIC system [42], etc.	Transmitter identification system [43], SIMO [7], MIMO [6], IoT [32], telephone signal system [44], cognitive radio system [45], and traditional wireless communication system [31], [46]–[48], etc.

TABLE IV
PERFORMANCE METRICS FOR THE PLA

Properties	Metrics	Concepts
Robustness	PD, PFA, and PMD [50]	PD is the probability of correctly deciding $\mathcal{H}_1$ when $\mathcal{H}_1$ is true; PFA is the probability of wrongly deciding $\mathcal{H}_1$ when $\mathcal{H}_0$ is true; PMD is the probability of wrongly deciding $\mathcal{H}_0$ when $\mathcal{H}_1$ is true. Optimal threshold is required, which is calculated by the NP theory or the MEP theory.
	ROC and AUC [51]	ROC is created by plotting the PD against the PFA with different thresholds; AUC is obtained by calculating the area under the ROC curve. Optimal threshold is not required.
Security	Key Equivocation [52]	Key equivocation is obtained by calculating the conditional entropy given all past observations at Eve.
	Min-Entropy [49]	Min-entropy is obtained by calculating the negative logarithm of the highest probability in the key distribution.
	Eve's Distinguishing Capability [8]	Eve's distinguishing capability is obtained by performing a threshold test under two hypotheses which are similar to (1).
Covertness	Average BER [53]	Average BER is obtained by calculating the average number of bits received in error divided by the total number of bits received at Carol.
	Outage Probability [54]	Outage probability is obtained by the probability that the instantaneous error probability exceeds a specified value or equivalently the probability that the output SNR falls below a certain specified threshold.
Systematic Metric	PSA [8]	PSA denotes the difference between the reliable authentication accuracy and the secret information leakage to Eve.

C. *Performance Metrics for the PLA*

We summarize the performance metrics for the PLA in Tab. IV in terms of the robustness, security, and covertness.

- The authentication accuracy of the threshold test at Bob under two hypotheses defined in (1) is used to evaluate the robustness. The first type of performance metrics for the robustness includes the Probability of Detection (PD), the Probability of False Alarm (PFA), and the Probability of Missed Detection (PMD). The PD is the probability of correctly deciding $\mathcal{H}_1$ when $\mathcal{H}_1$ is true; The PFA is the probability of wrongly deciding $\mathcal{H}_1$ when $\mathcal{H}_0$ is true; The PMD is the probability of wrongly deciding $\mathcal{H}_0$ when $\mathcal{H}_1$ is true. The second type of performance metrics for the robustness includes the Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC). The ROC is a graphical plot to illustrate the accuracy of a binary classier with different thresholds, which is created by plotting the PD against the PFA with different thresholds. The AUC represents the separability degree of a binary classier, which is obtained by calculating the area under the ROC curve. Note that the first type of performance metrics for the robustness requires to set up an optimal threshold whereas the second one does not have such requirement. For example, according to the Neyman-Pearson (NP) theory, the optimal threshold can be obtained by maximizing the PD but ensuring the PFA no beyond an upper-bound. For another example, according to the Minimum Error Probability (MEP) theory, the optimal threshold can be obtained by minimizing both the PFA and PMD simultaneously.
- The difficulty of Eve estimating the secret key is used to evaluate the security. The performance metrics for the security include the key equivocation, min-entropy, and Eve's distinguishing capability. The key equivocation is used to examine the average change in entropy of the secret key shared between Alice and Bob, which is obtained by calculating the conditional entropy given all past observations at Eve. However, the key equivocation is an average measure of the security, which may lead to some misleading conclusions. As suggested in [49], the min-entropy may be a better alternative measure for the security because it quantifies the highest probability of Eve correctly guessing the secret key, which is obtained by calculating the negative logarithm of the highest probability in the key distribution. Before Eve infers the secret key, Eve should first assure whether there exists a tag in her observations to improve the estimation accuracy. As suggested in [8], Eve's distinguishing capability is used to examine the accuracy of Eve detecting a tag from her observations, which is obtained by performing a threshold test under two hypotheses which are similar to (1). Although both Eve's detection and

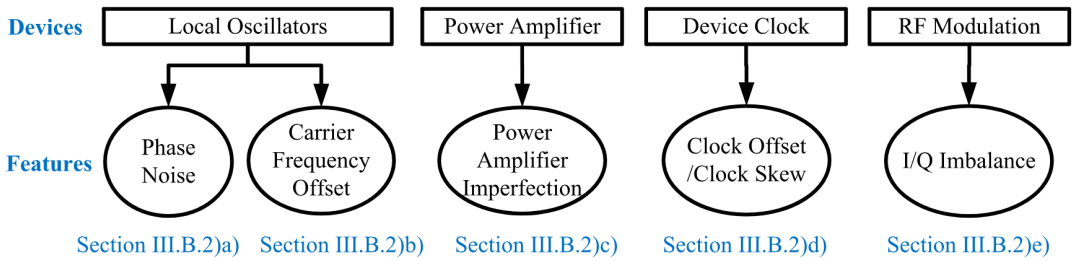

Fig. 6. Relationship between the specific devices and the steady-state features.

Bob's authentication use the same hypotheses, there is a fundamental difference that is whether the tag is available in advance.

- For the active PLA, the impact of embedding a tag on the reception of the source message at Carol is used to evaluate the covertness. The performance metrics for the covertness include the average Bit Error Rate (BER) and outage probability. The average BER is a measure of the total distortion introduced by both the wireless channel and the embedded tag on the source message, which is obtained by calculating the average number of bits received in error divided by the total number of bits received at Carol. The outage probability is which is obtained by the probability that the instantaneous error probability exceeds a specified value or equivalently the probability that the output SNR falls below a certain specified threshold. Note that the outage probability is easier to obtain the theoretical results in closed-form as compared with the average BER, because the conditional BER on the channel fading is in general a nonlinear function of the instantaneous SNR.

Note that, in most literature about the PLA, the robustness, security, and covertness are often separately analyzed, which has the two limitations. First, a systematic analysis of the effect of the parameters of a PLA scheme on the final performance becomes difficult. Second, a fair comparison of the performance of different PLA schemes under the same channel conditions is difficult as well. In [8], we proposed a generic security model for the PLA, and we designed a new systematic metric, which is referred to as the Probability of Security Authentication (PSA). The PSA denotes the difference between the reliable authentication accuracy (between Alice and Bob) and the secret information leakage to Eve. Based on the PSA, we can not only systematically analyze the effect of the parameter of a certain PLA scheme on the final performance, but also fairly compare the performance of different PLA schemes under the same channel conditions at both Bob and Eve.

III. Passive PLA

A. Device-Based Passive PLA

We divide the device-based features into two sub-categories: turn-on transient features and steady-state features. The former sub-category includes wavelet coefficients, transient amplitude, and transient Power Spectral Density (PSD), while the latter one includes phase noise, CFO, imperfect power amplifier, clock offset, clock skew, I/Q imbalance, Physical Unclonable Function (PUF), PSD, and Discrete Gabor Transform (DGT). We illustrate the relationship between the specific devices and the steady-state features in Fig. 6. Note that a single feature can be used to authenticate the transmitter for simplicity, e.g., clock offset [55], whereas multiple features can be used to realize the same goal for improving the authentication accuracy but with increasing communication overhead and computational complexity, e.g., five features [42]. Gungor and Koksal provided a systematic approach rooted in the information theory to evaluate the basic performance limits of the device-based features [56]. We discuss turn-on transient features and steady-state features in Sections II-B and II-C, respectively.

Application Scenarios: The device-based passive schemes can be applied to numerous applications. Hou *et al.* proposed a PLA scheme for OFDM systems using the unique CFO between each individual transmitter-receiver pair [3]. Brik *et al.* studied the identification of the source Network Interface Cards (NIC) of an IEEE 802.11 frame through passive radio-frequency analysis [42]. Hall *et al.* used radio frequency fingerprinting for profiling to authorize devices in a Bluetooth network [39]. Dubendorfer *et al.* utilized RF waveform features to defend impersonation attacks for unauthorized ZigBee network access [57]. Reising and Temple employed Radio Frequency Distinct Native Attribute (RF-DNA) fingerprinting to provide serial number discrimination of IEEE 802.11a WiFi devices in a WiMax system [58].

B. Using Single Device-Based Feature

1) Turn-On Transient Features:

a) Wavelet coefficients: Choe *et al.* used a Daubechies-4 wavelet to characterize a time-varying, nonstationary transient signal as a feature and then used an Artificial Neural Network (ANN) to authentication unknown transmitters [59]. Different from [59], Toonstra and Kinsner used a multiresolution wavelet analysis and a genetic algorithm to extract the wavelet coefficients [60]. Then, Toonstra and Kinsner used a multilayer feed-forward neural network to improve authentication accuracy [61].

b) Transient amplitude: Hall *et al.* used the transient amplitude of a transceiver to authenticate WiFi devices [38] and Bluetooth devices [39]. Tekbas *et al.* improved the authentication performance of the transient amplitude-based scheme

in a low Signal to Noise Ratio (SNR) region by introducing a sampled channel noise into a training set [62], e.g., 76% authentication accuracy when the SNR is 8 dB. Ureten and Serinken proposed a transient amplitude-based scheme in Ad-Hoc networks [63]. Rasmussen and Capkun used the variance of the transient amplitude to classify wireless sensor devices with a 70% authentication accuracy [64]. Then, based on the result in [64], Danev and Capkun proposed a scheme to classify wireless sensor devices, which improved the authentication accuracy to 96.8% [40]. The main limitation of these schemes in [38], [39], [63] is that the authentication accuracy highly depends on the manufacturer's model, which lets adversaries compromise these schemes by using the same device from the same manufacturer. Then, some improved schemes were proposed to relax the above limitation [40], [64].

c) Transient power spectral density (PSD): In comparison with the scheme in [62], Suski, II *et al.* took the PSD of a preamble signal in the transient phase as a feature to further improve the authentication accuracy in a low SNR region [65], e.g., 80% authentication accuracy when the SNR is 6 dB.

2) Steady-State Features:

a) Phase noise: Phase noise mainly occurs during the up-conversion from the base-band signal to the band-pass signal and vice versa due to the imperfections of local oscillators. In other words, the amplitude of phase noise is determined by the imperfections of local oscillators [66]. Since these imperfections are unavoidable in practical situations, the phase noise can be used as a device-based feature. Zhao *et al.* proposed a PLA scheme based on the phase noise by using the simple Multiple Kernel Learning (MKL), which can achieve 98.25% authentication accuracy [67].

b) Carrier frequency offset (CFO): The CFO can be used as a device-based feature because of the imperfections of local oscillators and the Doppler frequency shift in a mobile scenario. Hou *et al.* proposed a PLA scheme by analyzing the CFO in a time-invariant OFDM system [22]. Then, Hou *et al.* extended the time-invariant scenario to a time-varying scenario, where the CFO was modeled as an Auto-Regressive (AR) random process [3]. In comparison with the scheme in [3], Zeng *et al.* proposed a PLA scheme by combining the technique of Visibility Graph (VG) and the CFO to further improve the authentication performance [68].

c) Imperfect power amplifier: Power amplifiers are the last component in the RF chain of wireless transmitters and their imperfections have strong device-based characteristics. Dolatshahi *et al.* utilized the imperfections of power amplifiers to realize device authentication by using the Generalized Likelihood Ratio Test (GLRT) and Classical Likelihood Ratio Test (CLRT) [69]. Polak *et al.* improved the authentication performance by using the imperfections of power amplifiers and digital-to-analog converter together [70]. Then, Polak and Goeckel proposed a PLA scheme by utilizing a spectral analysis to defend against a trickier attack [71]. Specifically, adversaries maliciously introduce slightly distortions into the data symbol to forge the imperfections of power amplifiers.

d) Clock offset and clock skew: A clock of wireless devices is designed to represent the amount of time, t. However, a clock offset and clock skew are unavoidable due to the device imperfection, which can be represented as $O(C) = R(C) - t$ and $S(C) = \frac{d}{dt}O(C)$, respectively, where $R(C)$ is the true time of the clock C [72]. Rahman *et al.* proposed a PLA scheme using the time-varying clock offsets, where two Kalman filters were used to tracks Alice's and Eve's clock, respectively [55]. Kohno *et al.* proposed a PLA scheme using clock skew [73], which utilized the timestamps of a TCP header to estimate the clock skew. In comparison with the scheme in [73], Jana *et al.* proposed an enhanced PLA scheme that provided higher authentication accuracy to counter impersonation attacks by using IEEE 802.11 Time Synchronization Function (TSF) timestamps to calculate the clock skew [24], [74]. Then, Cristea and Groza proposed a PLA scheme to identify the smartphone by using the timestamps of the Internet Control Message Protocol (ICMP) to calculate the clock skew [75].

e) I/Q imbalance: An I/Q imbalance commonly exists in wireless transceivers, which is caused due to the mismatches of both amplitude and phase between In-phase (I) and Quadrature (Q) branches. Hao *et al.* proposed a PLA scheme using I/Q imbalance through the collaboration of multiple trusted receivers [76]. Then, Hao *et al.* also utilized I/Q imbalance to design a PLA scheme for a relay communication scenario, where both the I/Q imbalance in a relay process and a GLRT-based two-parameter hypothesis testing model were employed to make an authentication decision [77]. Sankhe *et al.* proposed a PLA scheme based on I/Q imbalances to improve the authentication accuracy by using a Convolutional Neural Network (CNN) under two situations: static and dynamic situations [23]. Specifically, under a static situation, a CNN architecture was designed to classify the raw I/Q samples without channel estimation. Under a dynamic situation, a channel estimation was used to improve the stability of the CNN classifier.

f) Physical unclonable function (PUF): A PUF is essentially a challenge-response behavior. Specifically, when a challenge x is applied to a PUF, the PUF feeds back a response y. We call such a pair of challenge x and response y as a Challenge-Response Pair (CRP), which can be defined as a one-way function $y = \Pi(x)$. The PUFs have two basic properties. First, given the same PUF Π, different outputs ($\hat{y} = \Pi(\hat{x})$ and $y = \Pi(x)$) correspond to different inputs ($\hat{x}$ and x). Second, given the same challenge input x and different PUFs (Π_i and Π_j), the outputs $y_i = \Pi_i(x)$ and $y_j = \Pi_j(x)$ are independent. The security of a PUF is determined by the intrinsic complexity and uncontrollability of the manufacturing process. Based on the number of CRPs, the PUFs can be categorized into two types: strong PUFs and weak PUFs. Generally, the type of strong PUFs can be used to perform chip authentication.

Pappu *et al.* first introduced the concept of the PUF in [78]. Gassend *et al.* proposed a Silicon PUF by measuring the intrinsic delays of a self-oscillating circuit [79]. Then, Guajardo *et al.* systematically reviewed the development and the application of the PUFs [80]–[82]. Gassend *et al.* used the PUFs to identify the chips, which requires to store a set of authenticated responses with a known challenge [83]–[85].

However, the authentication performances in [83]–[85] are seriously dependent on the number of stored authenticated responses. Recently, Chatterjee *et al.* proposed a lightweight preamble-less PUF-based PLA scheme by using a lightweight supervised Machine Learning (ML) framework, i.e., the ANN, which can achieve 99% authentication accuracy with 10000 IoT devices [86].

g) PSD: Corbett *et al.* proposed a PLA scheme by analyzing the PSD to classify network cards, which was generated using the User Datagram Protocol (UDP) with constant bit-rate flows in a controlled environment [87]. Then, Corbett *et al.* proposed an enhanced PLA scheme to classify cards with random interference, where the authentication accuracy was independent of the transport layer protocol [88]. Kennedy *et al.* proposed a PLA scheme using the PSD and a k-Nearest Neighbor (KNN) classifier, which can achieve 97% authentication accuracy at 30 dB SNR and 66% authentication accuracy at 0 dB SNR [89]. Williams *et al.* constructed a new feature of the PSD to classify WiMax devices using the Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier [90].

h) Discrete Gabor transform (DGT): Since a Discrete Gabor Transform (DGT) can express a signal in a time-frequency domain rather than a frequency domain, more properties of a DGT feature can be used for an authentication purpose as compared with those of a PSD feature. Based on a DGT feature, Reising *et al.* used MDA/ML classifier to perform a "one-to-many" classification for WiFi or WiMax devices [41]. Then, Reising and Temple used a modified MDA/ML classifier to perform a "one-to-one" classification [58]. In comparison with the schemes in [41], [58], Reising *et al.* used a classifier of generalized-relevance learning vector-quantization to improve the authentication accuracy with small samples, i.e., 93% accuracy with 10% samples [91].

Here, we summarize the contributions and concepts of all single device-based features in Tab. V.

C. Using Multiple Device-Based Features

Peng and Wang proposed a PLA scheme by using multiple device-based features, where each feature was simplified as a Gaussian Random Variable (RV) [92]. Specifically, first, a test statistic was constructed by calculating a weighted sum of all features. Second, the optimal weight can be found by maximizing the authentication accuracy. At last, a Likelihood Ratio Test (LRT) was used to make the final authentication decision. The simulation results verified the conclusion that authentication performance improves as the number of features increases.

1) Using Two Features:

a) Modulation shape and spectrum: Based on the modulation shape and spectrum, Bishop used the 1-nearest neighbor rule to calculate the similarity between the fingerprints of an unknown transmitter and those of a reference one [93]. Then, based on the similarity given in [93], Danev *et al.* proposed a PLA scheme to identify RFID transponders, where a Hilbert transform was used to extract the features of the modulation shape and a Principal Component Analysis (PCA) was used to extract the features of the spectrum [94].

b) Time interval error and average baseband power: Zanetti and Danev proposed a PLA scheme to identify Ultra-High Frequency (UHF) RFID tags based on the features of the time interval error and the average baseband power, where a dedicated component was required to extract the features of the average baseband power [95]. In comparison with the scheme in [94], Zanetti and Danev proposed a PLA scheme to improve the authentication accuracy in a low SNR region but it sacrificed the authentication accuracy in a high SNR region [95].

c) Covariance-based distribution and PSD: Han *et al.* proposed a PLA scheme to identify UHF RFID tags based on the features of the covariance-based distribution and the PSD, where the computation of entropy-based distance was used to calculate the similarity between the fingerprints of an unknown transmitter and those of a reference one [96]. In comparison with the scheme in [95], the PLA scheme in [96] not only relaxed the requirement of a dedicated component but also improved the authentication accuracy over the entire SNR region.

2) Using Three Features:

a) Amplitude, phase, and frequency: Williams *et al.* proposed a PLA scheme based on the features of the amplitude, phase, and frequency [97], where a Fisher-based MDA/ML classifier [98] was used to perform an authentication decision. Then, Cobb *et al.* proposed a PLA scheme based on the features of the transient amplitude, phase, and frequency extracted from a turn-on transient signal [99]. Then, based on the results in [97], Cobb *et al.* further proposed a PLA scheme to identify the Integrated Circuits (ICs) [100]. In comparison with the schemes in [99], [100], Klein *et al.* proposed an improved PLA scheme by using a Dual-Tree Complex Wavelet Transform (DT-CWT) to construct a wavelet-domain RF fingerprint [101].

b) Variance, skewness, and kurtosis: Dubendorfer *et al.* proposed a PLA scheme based on the features of the variance, skewness, and kurtosis to authenticate ZigBee devices [57]. This PLA scheme can achieve 90% authentication accuracy when the SNR achieves to 10 dB.

c) I/Q phase mismatch, I/Q DC offset, and I/Q gain imbalance: Xing *et al.* proposed a PLA scheme for device identification in Direct Sequence Spread Spectrum (DSSS) networks based on the features of the I/Q phase mismatch, I/Q DC offset, and I/Q gain imbalance, which has good performance in a low SNR region, e.g., -15 dB [102]. Specifically, the PLA scheme [102] first designed a preprocessing approach to improve the SNR of the received signal but without affecting device-based features. Then, the technique of the Differential Constellation Trace Figure (DCTF) was used to extract device-based features and a K-means cluster algorithm was used to construct a fingerprint vector. At last, an authentication decision was made by finding the minimum distance between the current unknown fingerprint and the reference ones.

TABLE V
USING SINGLE DEVICE-BASED FEATURE FOR THE PLA

Authors	Year	Contributions and Concepts
Choe *et al.* [59]	1995	Daubechies-4 wavelet was used to characterize a time-varying, non-stationary transient signal as a feature and an ANN was used for making an authentication.
Toonstra *et al.* [60], [61]	1995 and 1996	Multiresolution wavelet analysis was used to extract the wavelet coefficients [60] and multilayer feed-forward neural network was used to improve authentication accuracy [61].
Hall *et al.* [38], [39]	2004 and 2006	Transient amplitude of a transceiver was used to authenticate WiFi devices [38] and Bluetooth devices [39].
Tekbas *et al.* [62]	2004	Both transient amplitude and channel noise were used to improve the authentication performance under low SNR region.
Kohno *et al.* [73]	2005	Time-stamps of a TCP header were used to estimate the clock skew for making an authentication.
Ureten *et al.* [63]	2007	Transient amplitude was used to authenticate devices in Ad-Hoc networks.
Rasmussen *et al.* [64]	2007	Variance of the transient amplitude was used to authenticate wireless sensor devices.
Gassend *et al.* [83]–[85]	2003, 2004, and 2008	PUFs were used to identify the chips, which requires to store a set of authenticated responses with a known challenge.
Corbett *et al.* [87], [88]	2006 and 2008	PSD was used to authenticate network cards in a controlled environment [87] and a random interference environment [88].
Suski II *et al.* [65]	2008	PSD of a preamble signal in the transient phase was used as a feature to further improve the authentication accuracy in low SNR region.
Kennedy *et al.* [89]	2008	Both PSD and a KNN classifier were used for making an authentication.
Danev *et al.* [40]	2009	Variance of the transient amplitude was used to authenticate both wireless sensor devices and ZigBee devices.
Jana *et al.* [24], [74]	2008 and 2010	IEEE 802.11 TSF timestamps were used to calculate the clock skew for making an authentication.
Dolatshahi *et al.* [69]	2010	Imperfections of power amplifiers, GLRT, and CLRT were jointly used to realize device authentication.
Williams *et al.* [90]	2010	Both PSD and MDA/ML classifier were used to authenticate WiMax devices.
Cristea *et al.* [75]	2013	Timestamps of the ICMP was used to calculate the clock skew to authenticate the smart phones.
Hou *et al.* [3], [22]	2012 and 2014	CFO was used to authenticate devices in a time-invariant scenario [22] and a time-varying scenario [3].
Hao *et al.* [76], [76]	2014	I/Q imbalance through the collaboration of multiple trusted receivers was used for making an authentication [76] and was extended to a relay communication scenario [76].
Rahman *et al.* [55]	2014	Both time-varying clock offsets and Kalman filters were used for making an authentication.
Reising *et al.* [41], [58], [91]	2012 and 2015	Both DGT feature and MDA/ML classifier were used to perform "one-to-many" authentication [41] and "one-to-one" authentication [58]. Then, both DGT and generalized-relevance learning vector quantization classifier were used to improve the authentication accuracy with small samples [91].
Polak *et al.* [70], [71]	2011 and 2015	Imperfections of power amplifiers were used for making an authentication [70] and spectral analysis was used to defend against trickier attacks [71].
Zhao *et al.* [67]	2017	Phase noise by using the simple MKL was used for making an authentication.
Zeng *et al.* [68]	2018	Both VG and the CFO were used to further improve the authentication performance.
Sankhe *et al.* [23]	2019	Both I/Q imbalances and CNN were used to improve the authentication accuracy in both static and dynamic situations.
Chatterjee *et al.* [86]	2019	Both PUF and ANN were used to authenticate multiple IoT devices with few stored authenticated responses.

3) Using Four Features:

a) Differential constellation trace figure, CFO, modulation offset and I/Q offset: Based on the features of the differential constellation trace figure, CFO, modulation offset and I/Q offset, Peng *et al.* proposed a PLA scheme to identify ZigBee devices in the IoT by weighted combining four features to construct a fingerprint [103].

b) Frequency offset, phase offset, magnitude offset, and I/Q offset: Based on the features of frequency offset, phase offset, magnitude offset, and I/Q offset, and the results of [104], Candore *et al.* proposed a PLA scheme by combining multiple weak classifiers to construct a strong classifier rather than combining multiple features to construct a fingerprint [105].

4) Using Five Features:

a) Frequency offset, phase offset, magnitude offset, synchronization correlation, and I/Q offset: Brik *et al.* proposed a PLA scheme to identify the NICs based on the features of frequency offset, phase offset, magnitude offset, synchronization correlation, and I/Q offset, where an SVM-based classifier and a KNN-based classifier were used, respectively [42]. Experimental results showed that the SVM-based classifier has better authentication performance but the authentication speed of the KNN-based classifier is faster.

Here, we summarize the contributions and concepts of all multiple device-based features in Tab. VI.

Lesson 1: The basic idea of the device-based schemes is to authenticate the origin of the received signal by exploiting its device-based features. Although the precision and stability of communication devices have significant advancement, there exist some imperfections during the process of circuits manufacturing, even in different products of the same device of the same manufacturer. Since the imperfections of the device-based features cannot be arbitrarily controlled on purpose, they can be utilized as device-based features for an authentication purpose. The major difference between turn-on transient features and steady-state features is that the duration of the features generation. Turn-on transient features are generated only during the boot process of the transmitter, whereas steady-state features are generated when the transmitter comes into a stable state. Thus, the PLA schemes based on turn-on transient features have high security since Eve is difficult to capture these features. However, the PLA schemes based on turn-on transient features have low robustness since Bob is difficult

TABLE VI
USING MULTIPLE DEVICE-BASED FEATURES FOR THE PLA

Authors	Year	Contributions and Concepts
Brik *et al.* [42]	2008	Features of frequency offset, phase offset, magnitude offset, synchronization correlation, and I/Q offset were used to identify the NICs.
Danev *et al.* [94]	2009	Hilbert transform was used to extract the modulation shape features and PCA was used to extract the spectrum features to identify RFID transponders.
Zanetti *et al.* [95]	2010	Both time interval error and the average baseband power were used to identify UHF RFID tags.
Williams *et al.* [97]	2010	Features of the amplitude, phase, and frequency were extracted from a steady-state signal for making an authentication.
Cobb *et al.* [99], [100]	2010 and 2012	Features of the amplitude, phase, and frequency were extracted from a turn-on transient signal for making an authentication.
Klein *et al.* [101]	2012	Features of the transient amplitude, phase, frequency, and DT-CWT were used to improve the authentication performance.
Peng *et al.* [92]	2015	Multiple device-based features were simplified as a weighted Gaussian RV for making an authentication.
Han *et al.* [96]	2016	Both covariance-based distribution and the PSD were used to identify UHF RFID tags.
Candore *et al.* [96]	2016	Features of frequency offset, phase offset, magnitude offset, and I/Q offset, combining multiple weak classifiers were used to construct a strong classifier rather than simple combination of multiple features for making an authentication.
Xing *et al.* [102]	2018	Features of the I/Q phase mismatch, I/Q DC offset, and I/Q gain imbalance were used to identify devices in DSSS networks in a low SNR region.
Peng *et al.* [103]	2018	Features of the differential constellation trace figure, CFO, modulation offset and I/Q offset were used to identify ZigBee devices in the IoT networks.

TABLE VII
COMPARISON BETWEEN TURN-ON TRANSIENT FEATURES AND STEADY-STATE FEATURES

Categories	Advantages	Disadvantages	Trade-offs
Turn-on Transient Features	High security.	Low robustness.	Trade-off between security and robustness.
Steady-State Features	Low security.	High robustness.	Trade-off between security and robustness.

TABLE VIII
COMPARISON BETWEEN SINGLE FEATURE AND MULTIPLE FEATURES

Categories	Advantages	Disadvantages	Trade-offs
Single Feature	Low overhead.	Low security and low robustness.	Trade-off among security, robustness, and overhead.
Multiple Features	High robustness and high security.	High overhead.	Trade-off among security, robustness, and overhead.

to extract these features as well. On the contrary, the PLA schemes based on steady-state features have low security but have high robustness. Although the PLA schemes based on a single feature have low overhead, their security and robustness are low as compared with the PLA schemes based on multiple features. This is because the PLA schemes based on multiple features require more overhead to capture more features but enjoy more gain on the authentication performance.

Here, we summarize the differences between turn-on transient features and steady-state features in Tab. VII. Moreover, we summarize the differences between single feature and multiple features in Tab. VIII.

D. Channel-Based Passive PLA

We divide the channel-based features into two sub-categories: statistical channel information and instantaneous channel information. The specific values of the channel-based features in the former sub-category are typically determined by both the path loss and shadowing effect, whereas those in the latter sub-category are determined by the path loss, shadowing effect, and small-scale fading together. Although the channel-based features in the former sub-category only provide coarse-grained information of a wireless channel and those in the latter sub-category provides fine-grained information of a wireless channel, those in the former sub-category are easier to be extracted from a received signal as compared with those in the latter sub-category. The former sub-category includes RSS and PSD, which will be introduced in Section IV-A, while the latter one includes Channel Impulse Response (CIR) and Channel Frequency Response (CFR), which will be introduced in Section IV-B. Tu and Lai characterized the fundamental limits of the channel-based schemes by providing a detailed and refined analysis [106]. Specifically, an authentication exponent for the zero-rate case was characterized and both an upper bound and a lower bound on the exponent for the nonzero-rate case were provided. We will discuss passive schemes based on statistical channel information and instantaneous channel information in Sections II-E and II-F, respectively.

Application Scenarios: The channel-based schemes can be applied to numerous applications. Sheng *et al.* used GMM for RSS profiling to detect 802.11 MAC layer spoofing attacks [107]. Xiao *et al.* proposed a MIMO-assisted channel-based scheme by exploiting current channel estimation mechanisms in MIMO systems to detect spoofing attacks [108]. Zhang *et al.* proposed an end-to-end PLA scheme for dual-hop wireless networks by exploiting the intrinsic properties of cascaded multipath channels [33]. He *et al.* employed the inherent physical parameters of the multi-path fading channel

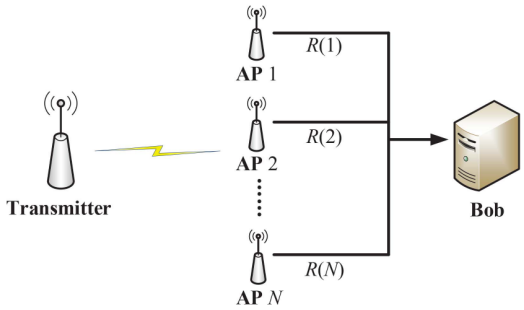

Fig. 7. One example of feature generation in the RSS-based scheme.

to achieve continuous two-way authentication between wireless terminals in OFDM networks [35]. Further, He *et al.* used a RAKE receiver to differentiate users in a CDMA system [34]. Du *et al.* proposed two channel-based schemes for wireless networks in relay networks [36]. Pan *et al.* proposed a channel-based scheme in the industrial wireless cyber-physical system [37].

* RSS = Received Signal Strength

1) *E. Statistical Channel Information*

1) RSS: According to the strategies of comparing different RSSes, we further divide the RSS-based schemes into four sub-categories: RSS matching, RSS ratio, RSS similarity, and ML-based.

a) RSS matching: Faria and Cheriton proposed a PLA scheme by matching the estimated RSS with the legitimate one to defend against both the impersonation attack and Sybil attack [109]. Specifically, we illustrate one example of feature generation in the RSS-based scheme [109] in Fig. 7, where the number of Access Points (APs) at Bob is N. Thus, Bob can extract N RSSes, i.e., $R(i)$, $i = 1, \ldots, N$. Then, Bob constructs a test statistic $T_i = \sum_{i=1}^{N} |R_X(i) - R_A(i)|$ for the *ith* RSS, where $R_X(i)$ and $R_A(i)$ represent the *ith* estimated RSS and the *ith* legitimate RSS, respectively. On the one hand, if the value of the test statistic is high and two received signals belong to the same MAC address, Bob can decide that there is an impersonation attack. On the other hand, if the value of the test statistic is small and two received signals belong to different MAC addresses, Bob can decide that there is a Sybil attack.

Varshavsky *et al.* proposed an RSS-based PLA scheme to ensure secure pairing between devices [110]. Specifically, first, two pairing devices obtained a secret key through a Diffie-Hellman key exchange protocol. Second, each device monitored its radio environment in a short time and estimated an RSS as an environment-specific fingerprint. Third, each device encrypted the estimated RSS with the secret key and exchanges it with the other device. Finally, each device compared the received fingerprint with its own fingerprint to make an authentication decision.

In comparison with the scheme in [110], Kalamandeen *et al.* proposed a more robust RSS-based scheme by further introducing trusted wearable devices [111]. Specifically, first, Alice sent a training signal to Bob for device pairing. Second, Bob's trusted wearable devices monitored the communication process and estimated their own RSSes. Third, Bob made an authentication decision based on multiple RSSes.

b) RSS ratio: Zhong *et al.* proposed a localization scheme based on the RSS ratio in Wireless Sensor Networks (WSNs) [112]. Then, Demirbas and Song further proposed a PLA scheme by utilizing the RSS ratio to defend against impersonation attacks and Sybil attacks [113]. Specifically, on the one hand, if two received signals belonging to the same MAC address have different locations, Bob can decide that there is an impersonation attack. On the other hand, if two received signals belonging to different MAC addresses have the same location, Bob can decide that there is a Sybil attack.

c) RSS similarity: The RSS similarity is calculated by the correlation between the RSSes of two different data frames [114]. For Alice's transmitted signal, the value of the RSS similarity is very high, whereas, for Eve's transmitted signal, the value of the RSS similarity becomes very low with high possibility. Zeng *et al.* proposed two PLA schemes by comparing the RSS similarity [25]. Specifically, the first PLA scheme obtained the RSS similarity between two adjacent data frames since the coherence time is assumed to be larger than the time interval between two adjacent data frames. The second PLA scheme obtained the RSS similarity between the received data frame and the transmitted data frame since the channel reciprocity holds. Then, Wang proposed two PLA schemes in the burst frame scenario: intra-burst and inter-burst, where a burst frame consists of multiple data frames [115]. Similar to [25], the intra-burst scheme has the assumption of the coherence time while the inter-burst scheme has the assumption of channel reciprocity.

~~*d) Machine learning based:*~~ Chen *et al.* proposed an ML-based scheme to defend against both impersonation attacks and Sybil attacks [116]. Specifically, first, Alice's RSSes are estimated in the training stage, and the RSSes of an unknown transmitter are estimated in the message-transmission stage. Then, a UML approach was used to cluster these RSSes, e.g., a K-means clustering algorithm. On the one hand, if the estimated RSSes from the same MAC address are clustered into two clusters, Bob can decide that there is an impersonation attack. On the other hand, if the estimated RSSes from different MAC addresses are clustered into the same cluster, Bob can decide that there is a Sybil attack. In comparison with the scheme [109], the ML-based scheme [116] can further pinpoint the position of an adversary.

Sheng *et al.* extended the scheme [109] to a multi-antenna scenario [107] with higher authentication accuracy. Specifically, the RSSes were first modeled as a Gaussian Mixture Model (GMM) [117]. Then, an RSS profile was established in the training stage based on an Expectation-Maximization (EM) learning algorithm. At last, Bob used a likelihood ratio test to calculate the similarity between the RSS profile and the current one to detect impersonation attacks.

Xiao *et al.* proposed an RSS-based scheme based on reinforcement learning [118]. Specifically, the scheme [118] formulated the received signal of Bob or Eve as a zero-sum authentication game. Then, a Bayesian risk was introduced to describe the utilities of both players. At last, the optimal

TABLE IX
USING STATISTICAL CHANNEL INFORMATION FEATURES FOR THE PLA

Authors	Year	Contributions and Concepts
Faria *et al.* [109]	2006	RSS was used to defend against impersonation attack and Sybil attack.
Varshavsky *et al.* [110]	2007	RSS was used to ensure secure pairing between devices.
Sheng *et al.* [107]	2008	RSSes were modeled as a GMM and EM learning algorithm to authenticate devices in multi-antenna scenario.
Kalamandeen *et al.* [111]	2010	RSS was used to ensure secure pairing between devices by further introducing trusted wearable devices.
Zeng *et al.* [25]	2010	Correlation between the RSSes of two different data frames was used for making an authentication.
Wang *et al.* [115]	2010	RSS measurements were used to authenticate devices in both intra-burst and inter-burst scenarios.
Chen *et al.* [116]	2010	UML approach was used to cluster the RSSes to defend against both impersonation attacks and Sybil attacks.
Tugnait [120]	2013	Both PSD and GLRT were used for making an authentication in time-invariant channels.
Xiao *et al.* [118], [119]	2015 and 2016	Both reinforcement learning and game theory were used for making an authentication [118] and Dyna architecture was used to improve both the authentication speed and authentication accuracy [119].

* PSD = Power Spectral Density: describes how power is distributed over the frequency content of the process

authentication threshold was obtained via reinforcement-learning. Moreover, the performance was evaluated through a Universal Software Radio Peripheral (USRP). In comparison with the scheme [118], Xiao *et al.* proposed an RSS-based scheme to improve both the authentication speed and authentication accuracy via a Dyna architecture, where the Nash Equilibrium (NE) was derived and the uniqueness of the NE was discussed [119].

2) PSD: Tugnait proposed a PSD-based scheme in a time-invariant channel, which effectively avoids the burden of symbol timing synchronization and training sequence for channel estimation [120]. Specifically, first, Bob obtained the two received signals in the training stage and communication stage, i.e., s_A and s_X, respectively. Second, the estimated PSDs of s_A and s_X can be obtained. At last, a Generalized Likelihood Ratio Test (GLRT) was used to make an authentication decision by comparing the estimated PSDs.

Here, we summarize the contributions and concepts of all statistical channel information features in Tab. IX.

2) F. Instantaneous Channel Information

The instantaneous channel information is generally called as the CSI. The CSI provides richer channel information than the statistical channel information, although it requires more complexity to obtain a precise channel estimation. Thus, the CSI-based schemes often have better authentication performance as compared to the RSS-based schemes or the PSD-based schemes. We divide the CSI-based schemes into two sub-categories in the time domain and frequency domain: CIR and CFR, respectively.

1) CIR: In the time domain, we rewrite the hypothesis (1) as

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{h}_X = \mathbf{h}_A \\ \mathcal{H}_1 &: \mathbf{h}_X \neq \mathbf{h}_A, \end{aligned} \tag{2}$$

where $\mathbf{h}_A$ represents the CIR vector from Alice to Bob, which is extracted by Bob in the training stage. Here, $\mathbf{h}_X$, $X \in \{A, E\}$, represents the CIR vector from an unknown transmitter to Bob, which is extracted by Bob in the message-transmission stage.

Tugnait and Kim proposed a CIR-based scheme in a single carrier time-invariant channel [121]. Then, Liu *et al.* extended the CIR-based scheme [121] to a multipath time-varying channel [122]. Specifically, the CIR of the *lth* sub-path at the *n*th timeslot can be expressed as

$$h_l(n) = \zeta h_l(n-1) + \sqrt{(1-\zeta^2)\sigma_l^2}\, u_l(n-1), \tag{3}$$

where $\zeta \in [0, 1]$ represents the channel correlation of two successive CIRs and $u_l(n)$ is a driving noise, modeled as a zero-mean complex Gaussian RV with unit variance. When the value of ζ is sufficiently high, the CIR-based scheme [122] has a robust authentication performance.

Based on the scheme in [122], Liu *et al.* further proposed an improved CIR-based scheme by using both the amplitude and multipath delay of CIR to improve the robustness in a mobile scenario, where a two-dimensional quantizer was used [123]. Specifically, the amplitude and multipath delay were first quantified respectively. Second, a Logarithmic Likelihood Ratio Test (LLRT) was used to make an authentication. Then, Liu *et al.* further improved the scheme [123] by exploiting the channel correlation to improve the authentication accuracy in the case of large channel variations [124]. Moreover, the theoretical analysis was derived with the closed-form expressions in [124].

Zhang *et al.* extended the scheme [124] to a dual-hop wireless network with an untrusted relay, where artificial jamming was used [33]. Specifically, when Alice sent a legitimate message to a relay, Bob simultaneously sent artificial jamming to the relay. Then, the relay forwarded the legitimate message with the artificial jamming to Bob. Bob not only checked the CIR but also checked the jamming signal. Thus, the scheme [33] can not only defend against impersonation attacks but also defend against a modification attack launched by the relay.

2) CFR: Similar to the CFR-based schemes, in the frequency domain, we rewrite the hypothesis (1) as

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{H}_X = \mathbf{H}_A \\ \mathcal{H}_1 &: \mathbf{H}_X \neq \mathbf{H}_A, \end{aligned} \tag{4}$$

where $\mathbf{H}_A$ represents the CFR vector from Alice to Bob, which is extracted by Bob in the training stage. Here, $\mathbf{H}_X$,

* CFR = Channel Frequency Response

CIR = Channel Impulse Response

$X \in \{A, E\}$, represents the CFR vector from an unknown transmitter to Bob, which is extracted by Bob in the message-transmission stage.

Xiao *et al.* proposed a CFR-based scheme in a time-invariant channel [4]. Specifically, Bob estimated a CFR $\hat{H}_A$ and $\hat{H}_X$ in the training stage and communication stage, respectively. Then, Bob authenticated the unknown transmitter by comparing $\hat{H}_A$ and $\hat{H}_X$. Moreover, Xiao *et al.* extended the CFR-based scheme [4] to a time-varying channel by further considering the delay profile, Doppler spectrum, and spatial correlations together [26].

Since even a minor movement of a mobile terminal introduces a significant change in the channel response due to the rapid spatial decorrelation of a wireless channel, Xiao *et al.* proposed an enhanced CFR-based scheme in a mobile scenario [114]. Specifically, the scheme [114] consisted of two steps: inter-burst authentication and intra-burst authentication. The role of the inter-burst authentication was to ensure that two adjacent bursts come from the same transmitter while the role of the intra-burst authentication was to check whether all frames of a data burst come from the same transmitter.

Xiao *et al.* extended the CFR-based scheme in a single antenna system with a time-invariant channel [4] to a Multi-Input Multi-Output (MIMO) system with a time-invariant channel [108]. Baracca *et al.* also proposed a CFR based PLA in a MIMO system using GLRT [125]. Specifically, Alice and Eve were assumed to have L_T antennas while Bob is assumed to have L_R antennas. Thus, the MIMO system had $L_T \times L_R$ independent propagation paths. Since the CFR-based scheme [108] only used the amplitude of CFR, He *et al.* further used both the amplitude and phase of the CFR in an OFDM system [34] and CDMA system [35] to improve the authentication accuracy.

The above CFR-based schemes [4], [26], [108], [114] were designed based on different communication scenarios, respectively, where their authentication accuracies are seriously determined by the considered network topology and communication environment [126]. Xiao *et al.* proposed a CFR-based scheme for a general communication scenario, where both frequency-selective Rayleigh channels and channel estimation errors were considered [127]. Specifically, a stochastic channel model first was established, which takes the Doppler frequency shift, multiple antennas, and channel estimation errors into account. Then, a GLRT was used for making an authentication decision, where the prior knowledge of the channel parameters was required. Moreover, a simplified CFR-based scheme was also proposed in [127], which relaxed the requirement of the channel parameters.

In Wi-Fi systems, management frames are more vulnerable to adversarial attacks than data frames, since management frames are transmitted without encryption. Jiang *et al.* proposed a CFR-based scheme for protecting Wi-Fi management frames, where a KNN algorithm was used to detect any suspicious management frames [128]. The limitation of the CFR-based scheme [128] is to obtain legitimate CFRs in a secure scenario. Then, Liu *et al.* proposed an enhanced CFR-based scheme by using a clustering algorithm, where a CFR profile can be obtained in an adversarial scenario [129]. Specifically, if there is no adversary, the legitimate CFRs should belong to the same cluster. If different CFRs belong to different clusters, there may be an adversary. Then, Liu *et al.* extended the CFR-based scheme [129] to a mobile scenario [130]. Specifically, a Pearson correlation coefficient was used to calculate the correlation between two adjacent CFRs collected from the same device ID within coherence time.

Shan *et al.* proposed a CFR-based scheme in an OFDM system, which avoids channel estimation by using a challenge-response strategy [131]. Specifically, in the training stage, Bob sent a random number D_i at the *ith* subcarrier as a challenge signal to Alice at time t_1. Then, Alice received the challenge signal denoted as $H_{BA,i}D_i + N_{i,1}$, where $H_{BA,i}$ and $N_{i,1}$ are the CFR of the *ith* subcarrier from Bob to Alice and the receiver noise of the *ith* subcarrier at Alice, respectively. In the message-transmission stage, Alice sent back a response signal carrying a secret key K_i to Bob at time t_2, denoted as

$$\frac{K_i}{H_{BA,i}D_i + N_{i,1}}. \tag{5}$$

The received response signal at Bob was denoted as

$$R_i = H_{AB,i}\frac{K_i}{H_{BA,i}D_i + N_{i,1}} + N_{i,2}, \tag{6}$$

where $H_{AB,i}$ and $N_{i,2}$ are the CFR of the *ith* subcarrier from Alice to Bob and the receiver noise of the *ith* subcarrier at Bob, respectively. If the channel reciprocity was hold, i.e., $t_2 - t_1 \leq \tau$, and the receiver noise can be ignored, (6) can be reduced to $R_i = \frac{K_i}{D_i}$. Then, Bob can estimate the secret key $\hat{K}_i = R_i D_i$. At last, Bob made an authentication decision by comparing the correlation between the secret key and the estimated key.

Shan *et al.* further extended the CFR-based scheme [131] to a relay network [36], where two CFR-based schemes were proposed based on the scenarios of trusted relay and untrusted relay, respectively. In the scenario of a trusted relay, the authentication process of the scheme [36] was similar to those of the scheme [131]. Specifically, in the training stage, Bob sent a challenge signal to the trusted relay and it was directly forwarded to Alice. In the message-transmission stage, Alice sent back a response signal to the trusted relay and it was directly forwarded to Bob. In the scenario of an untrusted relay, the scheme [36] required two shared keys: K_1 and K_2. Specifically, in the training stage, Bob sent a random number D and K_1 as two challenge signals, respectively, to the untrusted relay at time t_1. After the untrusted relay forwarded two challenge signals, Alice received two signals $H_{BC}H_{CA}K_1 + N_1$ and $H_{BC}H_{CA}D + N_1$ respectively, where H_{BC} and H_{CA} are the CFRs from Bob to the untrusted relay and from the untrusted relay to Alice, respectively. Then Alice divided two received signals as

$$R_A = \frac{H_{BC}H_{CA}K_1 + N_1}{H_{BC}H_{CA}D + N_1}. \tag{7}$$

If the receiver noise can be ignored, (7) can be reduced to $R_A = \frac{D}{K_1}$. Then, Alice can recover the random number as $\hat{D}_A = R_A K_1 \approx D$. In the message-transmission stage, Alice

TABLE X
USING INSTANTANEOUS CHANNEL INFORMATION FEATURES FOR THE PLA

Authors	Year	Contributions and Concepts
Xiao *et al.* [4], [26], [108], [114], [127]	2007, 2008, and 2009	CFR was used for making an authentication in time-invariant channel [4], time-varying channel [26], mobile scenario [114], MIMO time-invariant channel [108], and frequency-selective Rayleigh channels with channel estimation errors [127], respectively.
He *et al.* [34], [35]	2009 and 2010	Both the amplitude and phase of the CFR were used for making an authentication in an OFDM system [34] and CDMA system [35].
Tugnait *et al.* [121]	2010	CIR was used for making an authentication in a single carrier time-invariant channel.
Jiang *et al.* [128]	2013	CFR was used for making an authentication.
Shan *et al.* [36], [131]	2013 and 2014	Both CFR and challenge-response strategy were used for making an authentication in an OFDM system [131] and relay network [36].
Wu *et al.* [132]	2015	Phase differences between two CFRs were used for making an authentication in a multi-carrier transmission system.
Liu *et al.* [122]–[124]	2011, 2013, and 2016	CIR was used for making an authentication in a multipath time-varying channel [122], a mobile scenario [123], and a large channel variations scenario [124].
Liu *et al.* [129], [130]	2014 and 2018	CFR was used for making an authentication, where CFR profile was obtained in an adversarial scenario [129] and it was extended to a mobile scenario [130].
Wang *et al.* [138]	2017	Both CFR and ELM were used for making an authentication.
Wang *et al.* [135], [136]	2017	CS was used to extract the CFR [135] and a CS-based scheme was proposed [136].
Weinand *et al.* [139]	2017	Both CFR and ML were used for making an authentication in an actual wireless environment.
Lee *et al.* [137]	2018	CS-based scheme was extended to a multi-carrier system in a WEAN.
Zhang *et al.* [33]	2019	Scheme [124] was extended to a dual-hop wireless network with an untrusted relay.
Wang *et al.* [140]	2019	Both CFR and CRNN were used for making an authentication with little labeled CFRs.
Pan *et al.* [140]	2019	Both CFR and ML, *e.g.*, DT, SVM, KNN, and BT, were used for making an authentication in wireless mobile industrial CPSs.

sent back two response signals carrying the recovered random number $\hat{D}_A$ and K_2, respectively, to the untrusted relay at time t_2. After the untrusted relay forwarded two response signals, Bob took the same operations as Alice to recover the random number, i.e., $\hat{D}_B$, from the received response signals. Then, Bob made an authentication decision by comparing the correlation between $\hat{D}_B$ and D.

Based on the challenge-response strategy [36], [131], Wu and Zhen proposed a CFR-based scheme in a multi-carrier transmission system by using the phase differences between two CFRs [132]. Note that these schemes [36], [131], [132] only realize an identity authentication rather than a message authentication. In other words, the identity authentication does not need to consider the covertness of the active PLA.

Compressed Sensing (CS) is an attractive and promising signal-processing approach to efficiently acquire and reconstruct a received signal by exploiting the sparsity of the received signal [133], [134]. Thus, the CS can be used to enhance the authentication performance of the PLA. Wang *et al.* used the CS to extract the CFR [135] and further proposed a CS-based scheme [136]. Lee *et al.* extended the CS-based scheme to a multi-carrier system in a Wireless Energy Auditing Network (WEAN) [137], which is suitable for an SG system because of low computational complexity and low energy consumption.

3) Machine Learning Based CFR: Wang *et al.* proposed an ML-based CFR scheme using the Extreme Learning Machine (ELM), where an adversarial channel model was assumed to be available [138]. Specifically, in the training stage, first, two types of the received signals were generated according to the legitimate channel model and the adversarial channel model, respectively. Second, Bob obtained two labeled CFRs. Third, Bob calculated their Euclid distance and Pearson correlation coefficient as a feature vector. At last, Bob used the feature vector to train an ML model using the ELM algorithm. In the message-transmission stage, Bob first obtained the CFRs from the received signal transmitted from an unknown transmitter. Second, Bob obtained the feature vector. At last, Bob made an authentication decision by putting the feature vector into the trained ML model.

Weinand *et al.* proposed an ML-based CFR scheme using real data in an actual wireless environment, e.g., a mixed office/lab area with a lot of objects and metal walls [139]. Specifically, in the training stage, Bob obtained authenticated CFRs from Alice as labeled data to train a GMM. In the message-transmission stage, Bob first obtained CFRs from an unknown transmitter as unlabeled data. Then, Bob made an authentication decision by putting the unlabeled data into the trained GMM.

Wang *et al.* proposed an ML-based CFR scheme based on Convolutional Recurrent Neural Network (CRNN) [140]. The CRNN is an emerging model of the Deep Neural Network (DNN), which fully use the advantages of both Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) to extract the correlation between two CFRs at different times and at different frequencies. However, to train a CRNN model requires a large number of labeled CFRs, which can be used by the adversary to impersonate the legitimate features. In order to significantly reduce the number of labeled CFRs, a semi-supervised scheme was proposed as well [140].

Pan *et al.* proposed an ML-based CFR scheme in wireless mobile industrial Cyber-Physical Systems (CPSs), where four ML classification algorithms were considered: Decision Tree (DT), Support vector machine (SVM), KNN, and Bagged Trees (BT) [37]. The scheme [37] was verified not only by an industrial dataset but also verified in a real factory. The experiment results showed that a BT algorithm using 128-size CFR matrices as the input achieved the best authentication performance.

Here, we summarize the contributions and concepts of all instantaneous channel information features in Tab. X.

TABLE XI
COMPARISON BETWEEN STATISTICAL CHANNEL INFORMATION FEATURES AND INSTANTANEOUS CHANNEL INFORMATION FEATURES

Categories	Advantages	Disadvantages	Trade-offs
Statistical Channel Information Features	Low complexity and high robustness.	Low security.	Trade-off among security, robustness, and complexity.
Instantaneous Channel Information Features	High security.	High complexity and low robustness.	Trade-off among security, robustness, and complexity.

Lesson 2: The basic idea of channel-based schemes is to authenticate the origin of the received signal by exploiting its location-specific features. The security of the channel-based schemes is dependent on the assumption that the relationship between the channel-based features of two transmitters significantly reduces as the distance between two transmitters increases. For example, the channel-based features of two transmitters with half-wavelength distance can be treated as completely independent with each other in a wireless environment with large multi-paths and rich scatters. Since the location-specific nature of the channel-based features cannot be arbitrarily controlled on purpose, they can be utilized as channel-based features for authentication purposes. Note that the requirement of half-wavelength distance becomes easier to achieve as the carrier frequency increases. In comparison with the PLA schemes based on instantaneous channel information features, the PLA schemes based on statistical channel information features have low complexity because the features are easy to be estimated. However, the PLA schemes based on statistical channel information features have low security because the features are easy to be estimated by Eve. Moreover, the PLA schemes based on statistical channel information features have better robustness than those based on instantaneous channel information features because the change of communication environments has fewer negative impacts on the PLA schemes based on statistical channel information features.

Here, we summarize the differences between statistical channel information features and instantaneous channel information features in Tab. XI.

G. Extended Passive PLA

1) Hybrid Scheme: Wang *et al.* systematically analyzed the performance of various passive schemes: including both device-based and channel-based [10]. Specifically, through theoretical analysis and experiment results, several constraints of passive schemes in practical situations were discussed, such as RF fingerprint origins, multipath effect, device movement, and receiver complexity [10].

Zhang *et al.* proposed a hybrid scheme using a channel feature and a device feature together to further improve the authentication accuracy [27]. Specifically, Bob first estimated the CIRs and the device phase noises using a maximum likelihood estimator and extended Kalman filter, respectively. Second, a two-dimension quantizer was used to quantize both the difference between the estimated values of the CIRs and device phase noises and the corresponding legitimate values. Third, Bob summed the outputs of the two-dimension quantizer to obtain a final feature. At last, Bob made an authentication decision based on the final feature. Then, Zhang *et al.* further proposed a hybrid scheme using the CIR and the device impairments in a massive MIMO system [141]. Specifically, an error covariance matrix was constructed to reveal the impact of the device impairments on the authentication performance.

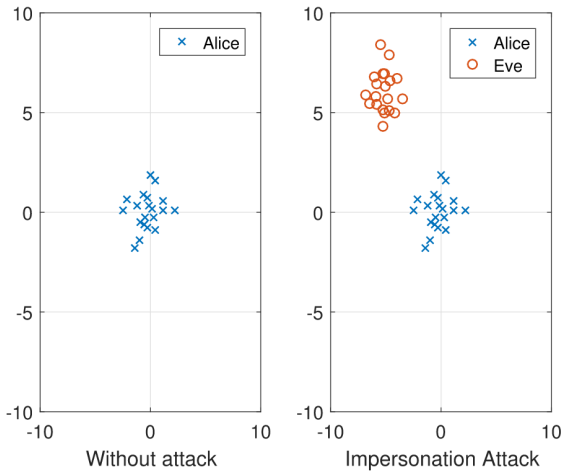

Fig. 8. An example of an impersonation attack detected by a UML approach.

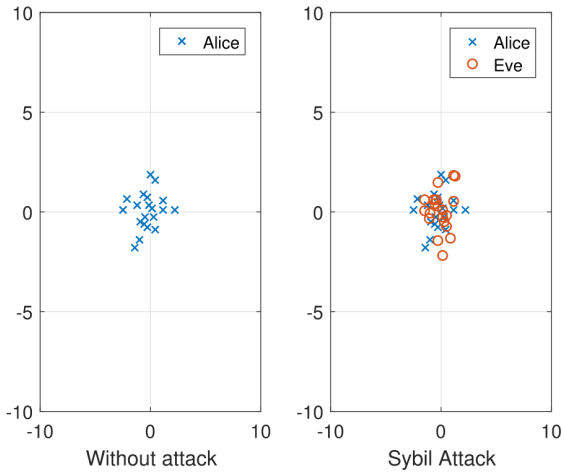

Fig. 9. An example of a Sybil attack detected by a UML approach.

~~*2) Unsupervised Machine Learning (UML):*~~ The ML approaches can be mainly divided into two sub-categories: supervised learning and unsupervised learning. The approaches in the former sub-category require the label whereas those in the latter sub-category relax the requirement. If there is no priori knowledge of the label, the supervised ML approaches cannot be used in the PLA. However, the UML approaches can effectively detect various identity-based attacks, e.g., impersonation attacks and Sybil attacks.

Chen *et al.* proposed a UML-based scheme to defend against impersonation attacks and Sybil attack by using a K-means clustering algorithm [142]. Specifically, Bob first estimated RSSes from multiple nodes. Then, Bob used the K-means clustering algorithm to cluster the estimated RSSes. If there exists an impersonation attack, the received signals from the same claimed identification will be clustered into multiple clusters, as illustrated in Fig. 8. If there is a Sybil attack, the received signals from multiple transmitters will be clustered into one cluster, as illustrated in Fig. 9. In comparison with the scheme [142], Yang *et al.* proposed an enhanced UML-based scheme to further determine the number of adversaries [28], where a Partitioning Around Medoids (PAM) cluster was used to analyze the estimated RSSes.

The above UML-based schemes are assumed to know the number of clusters in advance. Then, Nguyen *et al.* proposed a UML-based scheme using a non-parametric Bayesian approach to relax the assumption about the number of clusters [143]. Specifically, Bob estimated the CFO and I/Q imbalance from the received signal. Second, Bob constructed a 2-dimensional feature space. Third, after collected sufficiently feature vectors from multiple received signals, Bob used the non-parametric Bayesian approach to determine the number of transmitters and detected various identity-based attacks.

3) Artificial Noise (AN): Tugnait further extended the PSD-based scheme [120] by using the AN technique to a time-varying channel [144]. Specifically, Alice introduced the same Gaussian ANs at the training stage and the message-transmission stage, respectively, to increase the variance of the estimated PSD at Bob. Since the AN technique improved the resolution of the estimated PSD at Bob, the test statistic became robust in a time-varying channel. However, a rigorous theoretical analysis for the role of the AN technique in the PLA was missed [144].

Wu *et al.* further extended the CFR-based scheme [132] by introducing a Tikhonov-distributed AN to improve security [29]. Specifically, first, Alice used both a secret key and the AN in the phase of the transmitted signal. Second, Bob estimated the key from the received signal. At last, Bob made an authentication decision by comparing the secret key and the estimated key. Thus, the scheme [29] improved security by introducing more uncertainty at Eve, where a Tikhonov-distributed AN has the maximum entropy at Eve. Note that, similar to these schemes [36], [131], [132], the scheme [29] only realizes an identity authentication rather than a message authentication.

Here, we summarize the contributions and concepts of all extended passive schemes in Tab. XII.

Lesson 3: The hybrid scheme has high security and high robustness because it uses the advantages of both device-based PLA schemes and channel-based PLA schemes. However, the hybrid scheme inevitably introduces more complexity and more overhead to extract both device-based and channel-based features. The UML scheme increases the feasible range of the conventional passive PLA scheme by avoiding the training stage of the passive schemes. However, the UML scheme requires large data samples to train an unsupervised machine-model. If the number of data samples is not sufficiently large, the performance of the UML scheme significantly declines. Although the AN scheme improves the security by introducing an artificial noise to interfere with Eve, it requires more complexity and overhead to suppress the negative effect of the artificial noise on Bob.

Here, we summarize the differences between extended passive schemes in Tab. XIII.

IV. Active PLA

A. Non-Covert Active PLA

According to the embedding strategies, we divide the non-covert schemes into four sub-categories: modification of the frame structure, modification of the transmission parameters, encoding of the pilot, and encoding of the source message.

Application Scenarios: The non-covert active schemes can be applied to numerous applications. Supangkat *et al.* presented a non-covert active scheme with a public key signature for the telephone signal system [44]. Zhang *et al.* introduced a non-covert active scheme for primary users in a cognitive radio system [45]. Tang *et al.* investigated the non-covert active schemes in the presence of a full-duplex active eavesdropper in traditional wireless communication systems [48].

1) Modification of the Frame Structure: Menzezes *et al.* proposed a non-covert scheme by embedding a tag into a source message with the strategy of Time-Division Multiplexing (TDM) [145]. Since the scheme [145] inevitably modifies the frame structure, it has the following limitations. First, the tag can be easily estimated by Eve since the SNR of the tag is the same as that of the source message, which reduces the security. Second, the communication rate is significantly sacrificed since the throughput of the source message is occupied.

Supangkat *et al.* proposed a non-covert scheme by embedding a tag into a source message using a spread spectrum modulation in a telephone system [44]. Then, Proakis proposed a non-covert scheme based on the techniques of direct sequence spread spectrum and frequency hopping in a wireless system [53]. The above non-covert schemes have good robustness but occupy a lot of bandwidth, which hinders their application.

2) Modification of the Transmission Parameters: Zhang *et al.* proposed a non-covert scheme in an OFDM system [45]. Specifically, a cyclo-stationary feature was generated by repeating to insert specific symbols in each subcarrier. Then, Wang *et al.* proposed a non-covert scheme in an OFDM system by replacing the conventional Cyclic Prefix (CP) with a Pre-coded Cyclic Prefix (PCP) [146]. The above schemes significantly sacrifice message throughput.

Kumar *et al.* proposed a non-covert scheme by modifying frequency offset [147]. Then, Kumar *et al.* proposed a non-covert scheme by modifying a part of initialization bits [30]. Tan *et al.* proposed a non-covert scheme in a cognitive radio network to defend against Primary User Emulation (PUE) attacks [46], which can be regarded as broadcasting authentication.

Borle *et al.* proposed a non-covert scheme by controlling the disturbance of the transmitted symbol around the

TABLE XII
EXTENDED PASSIVE PLA SCHEMES

Authors	Year	Contributions and Concepts
Zhang *et al.* [27], [141]	2020	Both CIR and phase noise were used [27] and both CFR and error covariance matrix were used [141] to authenticate an unknown transmitter.
Chen *et al.* [142]	2007	K-means clustering was used to defend against impersonation attacks and Sybil attacks.
Yang *et al.* [28]	2013	PAM cluster was used to determine the number of adversaries.
Nguyen *et al.* [143]	2011	Non-parametric Bayesian algorithm was used to relax the assumption about the number of clusters.
Tugnait [144]	2014	AN was embedded into the transmission signal to improve the resolution of the estimated PSD in time-varying channels.
Wu *et al.* [29]	2016	Tikhonov-distributed AN was used to introduce the maximum entropy at Eve to improve system security.

TABLE XIII
COMPARISON BETWEEN EXTENDED PASSIVE PLA SCHEMES

Categories	Advantages	Disadvantages	Trade-offs
Hybrid Scheme	High security and high robustness.	High complexity and high overhead.	Trade-off among security, robustness, complexity, and overhead.
UML Scheme	No training stage.	Large data samples.	Trade-off between performance and overhead.
AN Scheme	High security.	High complexity and high overhead.	Trade-off among security, complexity, and overhead.

constellation points [31]. Specifically, two controlling strategies were designed: Uniform Angular Rotation (UAR) and Uniform Distance Rotation (UDR). In the UAR, the transmitted symbol was rotated around the constellation points with a small angle. In the UDR, the transmitted symbol was shifted around the constellation points with a constant offset. Experimental results verified that the UDR has better authentication performance than the UAR.

3) Encoding of the Pilot: In [47], [48], the pilot impersonation attacks were analyzed, which is a serious threat since Eve interrupts the channel estimation at Bob by impersonating the same pilot as that transmitted by Alice. Xu *et al.* proposed a non-covert scheme by using an encoding approach of the pilot to defend against the pilot impersonation attacks [148]. Specifically, Alice used the Subcarrier-Block Discriminating Coding (SBDC) to encode the pilot before sending it to Bob. Then, Eve cannot extract the pilot from her observations but Bob used the Independent Component Analysis (ICA) to make channel estimation. However, the scheme [148] assumed that different sub-carriers are independent, which is not true in practice due to limited channel taps. Thus, the ICA cannot be used in such a situation. Then, Xu *et al.* proposed an improved non-covert scheme to relax this assumption by using the Independence-Checking Coding (ICC) [149].

Since the non-covert schemes [148], [149] were designed for the scenario of one legitimate transmitter, Xu *et al.* further proposed a non-covert scheme by using a Code-Frequency Block Group (CFBG) coding for the scenario of multiple legitimate transmitters [150]. However, the limitation of the scheme [150] is that Bob is difficult to distinguish Eve from Alice if Eve has the same Angle of Arrival (AoA) as Alice's AoA.

Since the ICC-based scheme [149] did not consider the channel estimation error, Xu *et al.* proposed an enhanced ICC-based scheme [151]. Specifically, the pilot was randomized and encoded as diversified Subcarrier Activation Patterns (SAPs) through an ICC codebook. Moreover, Xu *et al.* extended the ICC-based scheme [149] to the Internet of Vehicles (IoVs) networks [152]. Specifically, a physical-layer Cover-Free (PHY-CF) coding was designed to authenticate both the encoded pilot and the claimed CSIs.

4) Encoding of the Source Message: Simmons proposed a non-covert scheme by using an encoding approach of the source message to defend against both impersonation and substitution attacks in a noiseless channel [153], where the lower bounds of the successful attack probability for two type attacks were derived. Specifically, Alice sent a codeword which consists of the secret key and the source message. Based on the secret key, Bob made an authentication decision by checking whether the received codeword is sent by Alice.

Boncelet proposed a message-coded scheme in a noisy channel [154]. Then, Liu and Boncelet proposed an enhanced message-coded scheme by decoupling the problem of authentication over a noisy channel to channel coding and authentication over a noiseless channel [155]. Lai and Poor proved that the decoupling operation in [155] has a detrimental effect and proposed an enhanced message-coded scheme to avoid the decoupling operation [17]. Moreover, based on the results of [156], the upper-lower bounds of the successful attack probability of impersonation attack and substitution attack in a noisy channel were derived [17]. Jorswieck *et al.* provided a comprehensive review of message-coded schemes [157]. Then, Chou and Yener extended the scheme [17] to a scenario of multiuser authentication with group anonymity [158].

Here, we summarize the contributions and concepts of all non-covert PLA schemes in Tab. XIV.

Lesson 4: In the active PLA, Alice embeds a tag into a source message, which inevitably affects the reception performance of the source message at the receiver. If the covertness is not considered in the design of an active scheme, the active scheme can only be used at Bob rather than at Carol, which hinders its extensive application. Moreover, it is challenging to construct a two-factor authentication system with both authentication mechanisms at the physical layer and those

TABLE XIV
NON-COVERT ACTIVE PLA SCHEMES

Authors	Year	Contributions and Concepts
Simmons *et al.* [153]	1984	Encoding approach of the source message was used to defend against both impersonation and substitution attacks in a noiseless channel.
Menzezes *et al.* [145]	1996	Tag was embedded into a source message with the TDM strategy.
Proakis *et al.* [53]	2001	Direct sequence spread spectrum and frequency hopping were used for making an authentication.
Supangkat *et al.* [44]	2002	Tag was embedded into a source message using a spread spectrum modulation in a telephone system.
Boncelet *et al.* [154]	2006	Message-coded scheme in a noisy environment was proposed.
Liu *et al.* [155]	2006	Enhanced message-coded scheme was proposed by decoupling the problem of authentication over a noisy channel to channel coding and authentication over a noiseless channel.
Lai *et al.* [155]	2006	Fact, that the decoupling operation in [155] has a detrimental effect, has been proved and an enhanced message-coded scheme was proposed to avoid the decoupling operation.
Wang *et al.* [146]	2011	Non-covert scheme was proposed by replacing the conventional CP with a PCP.
Tan *et al.* [46]	2011	Non-covert scheme was proposed in a CR network to defend against PUE attacks.
Yang *et al.* [45]	2012	Cyclo-stationary feature was generated by repeating to insert specific symbols in each subcarrier.
Kumar *et al.* [147]	2014	Non-covert scheme was proposed by modifying frequency offset.
Borle *et al.* [31]	2015	Non-covert scheme was proposed by controlling the disturbance of the transmitted symbol around the constellation points.
Kumar *et al.* [30]	2016	Non-covert scheme was proposed by modifying a part of initialization bits.
Xu *et al.* [148]–[151]	2017,2018, and 2019	Encoding approach of the pilot was used to achieve pilot authentication.
Chou *et al.* [158]	2020	Scheme in [155] was extended to a scenario of multiuser authentication with group anonymity.

TABLE XV
COMPARISON BETWEEN NON-COVERT ACTIVE PLA SCHEMES

Categories	Advantages	Disadvantages	Trade-offs
Modification of the Frame Structure	High robustness.	Low security and low communication rate.	Trade-off among robustness, security, and communication rate.
Modification of the Transmission Parameters	High security.	Low message throughput.	Trade-off between security and message throughput.
Encoding of the Pilot	High security.	Low feasibility.	Trade-off between security and low feasibility.
Encoding of the Source Message	High security.	High complexity.	Trade-off between security and complexity.

at the upper layers. For the schemes based on the modification of the frame structure, they have high robustness, because the tag has the same SNR of the source message. However, they have low security and low communication rate, because the tag can be easily estimated by Eve and the throughput of the source message is occupied. For the schemes based on the modification of the transmission parameters, they improve the security as compared with the schemes based on the modification of the frame structure, but they still suffer from the loss of message throughput. For the schemes based on encoding of the pilot, they have high security, because it is challenging for Eve to extract the pilot from her observations. However, they suffer from the low feasibility, because there are some unreasonable assumptions in practical applications, e.g., different sub-carriers are independent. For the schemes based on encoding of the source message, they have high security, because it is challenging for Eve to extract the source message from her observations. However, they suffer from high complexity, because they introduce high complexity to deal with a joint problem of channel coding and authentication.

Here, we summarize the differences between non-covert active PLA schemes in Tab. XV.

B. Covert Active PLA

According to the embedding strategies, we divide the covert schemes into four sub-categories: replacement, superimposition, channel-like, and slope. Moreover, we provide a generic security model of the covert schemes. Note that if there is no tag to be embedded into the source message, we denote the signal transmitted from Alice as a normal signal. For comparison purposes, we illustrate the frame structure of a normal signal in Fig. 10, where two adjacent frames are considered.

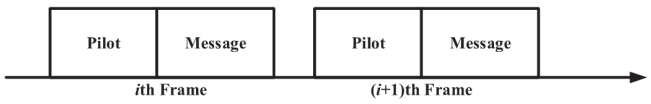

Fig. 10. Frame structure of a normal signal.

Application Scenarios: The covert active schemes can be applied to numerous applications. Yu *et al.* proposed a general framework for covert active schemes in a wireless SIMO system [7]. Further, Yu and Sadler introduced a stealthy fingerprint for a wireless MIMO system [6]. Wang *et al.* proposed a covert active scheme using embedded pseudo-random sequences in a transmitter identification system for Digital Television (DTV) distributed transmission network [43]. Zhang *et al.* proposed a general and lightweight covert active scheme for the IoT devices [32].

1) Replacement: We proposed a covert scheme by replacing some bits of the source message with the corresponding bits of the tag [8], which can be regarded as a variant of the TDM scheme [145]. The frame structure of the replacement scheme [8] is illustrated in Fig. 11. Specifically, Alice generated a tag using a one-way hash with a secret key and a source message. Note that the secret key has another role that is to appoint the embedding locations. The parameter of the replacement scheme is the embedding ratio, denoted as $r_e = L_R/L$, where L_R and L represent the average length of the tag and

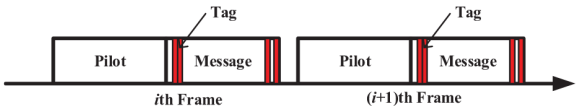

Fig. 11. Frame structure of the replacement scheme.

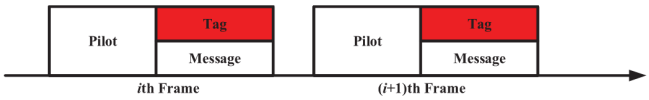

Fig. 12. Frame structure of the superimposition scheme.

source message in one frame, respectively. For ensuring the covertness, we assume that $L_R \ll L$. Bob first recovered the tag using the one-way hash with the secret key and the recovered source message. Then, Bob extracted the tag based on the secret key. At last, Bob made an authentication decision by comparing the extracted tag with the recovered tag.

2) Superimposition: Wang proposed a covert scheme by superimposing a tag on a source message in a digital television system [43]. The tagged signal can be expressed as

$$x = s + \rho t, \tag{8}$$

where s, t, and ρ represent the source message, the tag, and the transmission power of the tag, respectively. Then, Yu *et al.* proposed an enhanced superimposition scheme in a wireless system [7]. The tagged signal can be expressed as

$$x = \rho_s s + \rho_t t, \tag{9}$$

where ρ_s^2 and ρ_t^2 are the allocation factors of the transmission power for the source message signal and the tag, respectively. For satisfying the constraint of the transmission power, we have $\rho_s^2 + \rho_t^2 = 1$. The frame structure of the superimposition scheme [7] is illustrated in Fig. 12. The parameter of the superimposition scheme is the allocation factor ρ_t^2. The superimposition scheme has the same operations as those of the replacement scheme except the tag embedding at Alice and the tag extraction at Bob.

The superimposition scheme [7] was verified through a Software-Defined Radio (SDR) platform [159]–[161]. Yu *et al.* further extended the superimposition scheme [7] to an OFDM system [162] and a MIMO system [6]. Ran *et al.* proposed a superimposition scheme by partially superimposing the tag to improve the covertness [163]. Zhang *et al.* proposed a superimposition scheme with higher security in an IoT system [32], where two sets of asymmetric-keys are used to encrypt the source message and the tag, respectively. Then, Yu *et al.* generalized a framework for the superimposition scheme to create an authenticated side-channel for minimal cost [5], [164]. Specifically, Alice conveyed side-channel information to Bob through Alice's choice of a tag from a secret codebook generated by the primary message and a secret key.

Note that the above superimposition schemes require additional complicated preprocessing, such as channel estimation and message symbol recovery through demodulation and decoding to extract the tag. If we only consider achieving

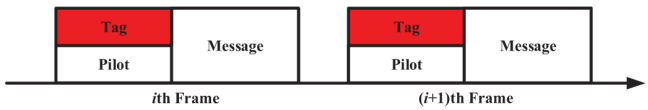

Fig. 13. Frame structure of the blind superimposition scheme.

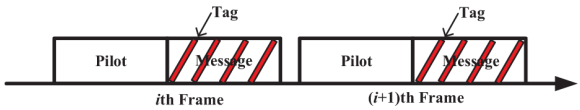

Fig. 14. Frame structure of the channel-like scheme.

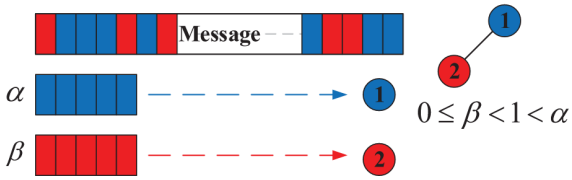

Fig. 15. Frame structure of the slope scheme.

an authentication purpose, the above complicated preprocessing is unnecessary and wasteful. Moreover, the complicated preprocessing is not always feasible and reliable in practice, e.g., a low-cost receiver. Thus, we proposed a blind superimposition scheme that combines the techniques of Blind Known Interference Cancellation (BKIC) and differential processing to implement authentication without requiring any of the above-described preprocessing [165]. Here the "blind" term represents two meanings. First, neither a channel estimation nor a recovery of the source message is required before making an authentication decision. Second, we use a blind manner to suppress the impact of the pilot on the generation of the residual signal. The frame structure of the blind superimposition scheme [165] is illustrated in Fig. 13. The blind superimposition scheme [165] works well in fast fading channels, even in frequency selective fading channels.

3) Channel-Like: Goergen *et al.* proposed a channel-like scheme by multiplying a tag in a source message in a single antenna system [166]. The basic idea of the channel-like scheme is to hide the tag in the channel fading. Note that Alice embeds the tag with a 50% duty cycle for Bob exactly extracting the tag. In the meantime, Eve cannot detect the tag since the tag is erased after a channel equalization. The tagged signal can be expressed as

$$x = ts. \tag{10}$$

The frame structure of the channel-like scheme [166] is illustrated in Fig. 14. Goergen *et al.* further extended the channel-like scheme [166] to a MIMO system [167], [168] and an OFDM system [169].

4) Slope: Besides the blind superimposition scheme [165], we also proposed a slope scheme to avoid the above-described preprocessing [9]. The diagram of the slope scheme [9] is illustrated in Fig. 15. Specifically, Alice divided the transmitted signal into two groups according to a secret key. The transmission power of each group was modified marginally. The

TABLE XVI
COVERT ACTIVE PLA SCHEMES

Authors	Year	Contributions and Concepts
Yu *et al.* [7]	2008	Superimposition scheme was enhanced by allocating the transmission power for the source message signal and the tag.
Goergen *et al.* [166]	2010	Channel-like scheme was proposed by multiplying a tag with a source message in a single antenna system is proposed.
Xie *et al.* [8]	2018	Covert scheme was proposed by replacing some bits of the source message with the corresponding bits of the tag.
Yu *et al.* [5]	2018	Generalized framework for the superimposition scheme was proposed to create an authenticated side-channel with the minimal cost.
Xie *et al.* [165]	2018	Blind superimposition scheme was proposed, which combines the techniques of BKIC and differential processing to implement authentication without requiring any of the above-described preprocessing.
Xie *et al.* [9]	2018	Slope scheme was proposed by dividing the transmitted signal into two groups with different transmission powers.
Ran *et al.* [163]	2019	Superimposition scheme was proposed by partially superimposing the tag to improve the covertness.
Zhang *et al.* [32]	2019	Superimposition scheme was proposed with higher security in an IoT system, where two sets of asymmetric-keys are used to encrypt the source message and the tag, respectively.

TABLE XVII
COMPARISON BETWEEN COVERT ACTIVE PLA SCHEMES

Categories	Advantages	Disadvantages	Trade-offs
Replacement	High robustness.	Low security and low covertness.	Trade-off among robustness, security and covertness.
Superimposition	High security and high covertness.	Low robustness.	Trade-off among robustness, security, and covertness.
Channel-Like	High security and high covertness.	Low robustness.	Trade-off among robustness, security, and covertness.
Slope	High security, high covertness, and low complexity.	Low robustness.	Trade-off among robustness, security, and covertness.

tagged signal can be constructed as

$$x_1 = \alpha s_1$$
$$x_2 = \beta s_2, \tag{11}$$

where we have $0 < \beta < 1 < \alpha$ and require $\alpha^2/2 + \beta^2/2 = 1$. Then, Bob made an authentication decision by comparing the received power of different groups, where both channel estimation and recovery of the source message are saved.

Here, we summarize the contributions and concepts of all covert PLA schemes in Tab. XVI.

Lesson 5: If the covertness is considered in the design of an active scheme, the negative effect of embedding a tag into a source message can be kept under control by adjusting the parameters of the active scheme. For example, if the active scheme sets an appropriate parameter, the decodability of the source message at Bob or Carol should be ensured although the demodulation performance becomes worse. In other words, if the sum of errors introduced by the tag embedding, channel fading, and receiver noise is not beyond the total error-correcting capability provided by both channel encoding and modulation, the source message can be perfectly recovered at Bob or Carol. On the one hand, although Carol does not know the detail of the active scheme, she can authenticate Alice's device through a certain upper-layer authentication scheme. On the other hand, Bob not only authenticates Alice's device but also constructs a two-factor authentication system for higher security. Moreover, higher covertness often leads to higher security since it becomes more challenging for adversaries to detect the existence of the tag in their observed signals. For the replacement schemes, they have high robustness, because the tag has the same SNR of the source message. However, they have low security and low covertness, because the tag can be easily estimated by Eve and the replaced bits cannot be recovered by Carol. For the superimposition and channel-like schemes, they improve the security and covertness as compared with the replacement schemes, but they suffer from low robustness due to a tag with low transmission power. Moreover, the channel-like schemes are more sensitive to the channel estimation errors as compared with the superimposition schemes. For the slope scheme, although it saves the complexity as compared with the superimposition schemes, it slightly sacrifices the robustness when the block length becomes large.

Here, we summarize the differences between covert active PLA schemes in Tab. XVII.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

A. Selection of Passive Features

The problem of feature selection is important because it should answer two fundamental questions in the passive PLA. The first question is how to determine the best set of features to extract. For example, some features are less sensitive to the transmitter location and environmental settings, but they are also easier to be estimated by adversaries. The second question is how to best combine different features for making a reliable authentication. Since different features have different value ranges and different units, the design of combining strategy should consider the contributions of different features to the final authentication decision. In summary, since there

are many redundant or irrelevant features, one may use an ML approach to reduce the dimension of the feature space or project the features space to a transformed space.

B. Hybrid Scheme by Exploiting Both Passive and Active Schemes

Passive and active schemes have their merits and demerits. If a hybrid scheme maximizes their merits but minimizes their demerits, the hybrid scheme can further improve authentication performance with a little extra overhead. For example, when a passive feature is introduced in an active scheme to construct a hybrid scheme, the transmission power of the tag can effectively be reduced. Then, the hybrid scheme significantly improves the covertness and the security as compared with the conventional active scheme, but it requires extra overhead to obtain the passive feature at Bob in advance. If the covertness and security is the highest priority, the hybrid scheme may be the best option.

C. Cross-Layer Scheme by Combining Physical-Layer Authentication and Upper-Layer Authentication

Note that a PLA scheme is not designed to replace an upper-layer authentication scheme. On the contrary, a PLA scheme is designed to compensate for an upper-layer authentication scheme, which provides a higher security level. For example, we construct a cross-layer scheme with both authentication mechanisms at the physical layer and those at the upper layers. Specifically, the upper-layer authentication mechanism is used to authenticate Alice's identification while the PLA mechanism is used to authenticate Alice's device. If Bob can authenticate both the identification and the device of Alice, the security level of this authentication system will be higher than using only one authentication mechanism. For ensuring the stability of the upper-layer authentication mechanism, the covert schemes or passive schemes may be a better option than the non-covert schemes for designing a cross-layer scheme.

D. Defending Against a Joint Attack

A joint attack represents an attack strategy that Eve simultaneously launches multiple different attacks, e.g., impersonation, jamming, and eavesdropping. Either active schemes or passive schemes should consider the threat of a joint attack, because it is much more harmful than common attacks. However, most existing PLA schemes are designed for defending against one type of attack. Thus, it is more challenging for defending against a joint attack as compared with one type of attack. There are two promising solutions to defend against a joint attack. The first solution is a separate scheme that multiple processes are required for separately defending against different attacks. The separate scheme is easy to be implemented, but it is difficult to achieve the optimal performance and introduces a large processing delay. The second solution is an ensemble scheme that one single process is required for simultaneously defending against different attacks. The ensemble scheme may achieve better performance and save the processing delay, but it requires complicated implementation and may suffer from local optimums.

E. Apply the PLA to the Emerging Wireless Systems

The existing PLA schemes are mainly concentrated on traditional and classical wireless systems. For improving the spectral efficiency or ensuring special requirements, some emerging wireless systems have started many research efforts, e.g., millimeter-Wave (mm-Wave) systems, Visible Light Communication (VLC), IoT, Body Area Networks (BAN), and CR systems. However, most of the emerging wireless systems achieve security only via a certain upper-layer authentication scheme, which provides a huge potential of research space for the PLA. Here, we discuss the challenges and promising solutions when the PLA is applied to the emerging wireless systems.

1) Millimeter-Wave (mm-Wave) Systems: Recently, the mm-Wave technology has drawn significant interest since it has the potential to meet the capacity requirement of the future wireless systems [170]. Although the available bandwidth of mm-Wave frequencies is significantly increased, the channel features of an mm-Wave system are significantly different from those of the traditional wireless systems. For example, an mm-Wave system has very short wave-length, directionality by using massive MIMO, and short range transmissions because of severe path-loss propagation. All aforementioned special features of an mm-Wave system can be exploited to improve the performance of the passive schemes.

2) Visible Light Communication (VLC): VLC is a new paradigm viewed as a complement to the traditional wireless communication systems [171], where the information is transmitted through modulating the visible light spectrum. The unique propagation characteristics of VLC channels are different from the traditional wireless communication system, e.g., the VLC signals blocked by human and normal building blockages It is easy to apply the passive schemes in a VLC system under one user indoor scenario because the outdoor adversaries are easy to be detected. However, it becomes more challenging for applying the PLA in a VLC system under public areas or multi-user indoor scenarios. Here, the extended passive schemes, e.g., AN scheme, may be used to improve the performance of the passive PLA in a VLC system.

3) Internet of Things (IoT): IoT can be regarded as a system of interrelated computing devices and sensors without human-to-computer interaction [172]. In an IoT system, it is challenging to obtain the accurate legitimate CSI because high-rate feedback channel is forbidden to avoid signaling overhead, especially in dense IoT deployment scenarios. Thus, the channel-based passive schemes are no longer applicable. Here, a lightweight active PLA scheme may be a better option in an IoT system.

4) Body Area Networks (BANs): BAN can be regarded as a wireless sensor network with wearable computing devices, where the devices may be embedded inside the human's body as implants or may be carried in different positions of humans [173]. A BAN system is a promising solution in the health-care industry because of its ability to sense physiological signals and transmit the collected data to a remote medical center. There are two main challenges when we apply the PLA in a BAN system. First, most devices of a

BAN system are resource-constrained, reduced-size, reduced-weight, and low duty cycle with low peak power. Second, unauthorized users should have access to the authentication system in case of emergency via some specific protocols, e.g., the help to an unconscious patient from an unauthorized doctor. Thus, a lightweight and anonymity-preserving active scheme is desirable in a BAN system.

5) Cognitive Radio (CR) Systems: CR systems can be programmed adaptively and configured dynamically to improve the spectrum utilization according to its vicinity to avoid user interference and congestion [174]. A CR system has the potential to exploit the inefficiently utilized licensed bands without causing interference to incumbent users. There are three main challenges when we apply the PLA in a CR system. First, the primary network has a strict need for satisfying QoS requirements. Second, the security threats for a secondary user are introduced by an adversary disguised as a primary user. Third, the security threats for a primary user are introduced by an adversary disguised as a secondary user. Here, a cooperative and trusted user can be used to improve the performance of both passive and active schemes in a CR system.

VI. Conclusion

In this article, we have provided a comprehensive survey on the PLA for improving the security of wireless systems. We have categorized the existing PLA schemes into two categories: passive and active schemes. The major difference between the two categories is whether a tag is actively embedded in the source message by Alice. Since passive schemes do not embed any tag into the source message, they only consider both the robustness and security excluding the covertness. On the contrary, the active schemes should consider the robustness, security, and covertness together. Moreover, we divided the passive schemes into two sub-categories: device-based features and channel-based features. We also introduced three types of extended passive schemes: the hybrid scheme, the UML, and the AN. We divided the active schemes into two sub-categories: non-covert and covert schemes. At last, we concluded this article with some recommendations and future research directions for current and emerging wireless systems.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[3] W. Hou, X. Wang, J. Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[4] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. Int. Conf. Commun. (ICC)*, Glasgow, U.K., 2007, pp. 4646–4651.

[5] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Cryptographic side-channel signaling and authentication via fingerprint embedding," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2216–2225, 2018.

[6] P. L. Yu and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 606–615, 2011.

[7] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, pp. 38–51, 2008.

[8] N. Xie, C. Chen, and M. Zhong, "Security model of authentication at the physical layer and performance analysis over fading channels," *IEEE Trans. Depend. Secure Comput.*, early access, Nov. 27, 2018, doi: 10.1109/TDSC.2018.2883598.

[9] N. Xie and C. Chen, "Slope authentication at the physical layer," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 1579–1594, 2018.

[10] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 2091–2106, 2016.

[11] X. Wang, H. Peng, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[12] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[13] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[15] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1350–1356, Jul. 2000.

[16] E. Martinian, G. W. Wornell, and B. Chen, "Authentication with distortion criteria," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2523–2542, Jul. 2005.

[17] H. E. G. L. Lai and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906–916, Feb. 2009.

[18] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *J. Commun. Netw.*, vol. 5, no. 3, pp. 237–264, Sep. 2020.

[19] J. Hamamreh, H. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1772–1828, 2nd Quart., 2019.

[20] M. A. Arfaoui *et al.*, "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, 3rd Quart., 2020.

[21] J. D. V. Sánchez, L. F. U. Aguiar, C. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5G wireless networks," 2020. [Online]. Available: arXiv:2006.08044.

[22] W. Hou, X. Wang, and J. Chouinard, "Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates," in *Proc. Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, 2012, pp. 3559–3563.

[23] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *Proc. Conf. Comput. Commun. (INFOCOM)*, Paris, France, 2019, pp. 370–378.

[24] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449–462, Mar. 2010.

[25] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[26] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[27] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, Apr. 2020.

[28] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[29] X. Wu, Z. Yang, C. Ling, and X. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611–6625, Oct. 2016.

[30] V. Kumar, J. M. Park, and K. Bian, "PHY-layer authentication using duobinary signaling for spectrum enforcement," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 1027–1038, 2016.

[31] K. M. Borle, B. Chen, and W. Du, "Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2225–2235, 2015.

[32] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, "Lightweight tag-based PHY-layer authentication for IoT devices in smart cities," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3977–3990, May 2020.

[33] P. Zhang, J. Zhu, Y. Chen, and X. Jiang, "End-to-end physical layer authentication for dual-hop wireless networks," *IEEE Access*, vol. 7, pp. 38322–38336, 2019.

[34] F. He, M. Hong, D. Kivanc, and B. Mcnair, "EPSON: Enhanced physical security in OFDM networks," in *Proc. Int. Conf. Commun. (ICC)*, Dresden, Germany, 2009, pp. 1–5.

[35] F. He, W. Wei, and M. Hong, "REAM: RAKE receiver enhanced authentication method," in *Proc. Military Commun. Conf. (MILCOM)*, San Jose, CA, USA, 2010, pp. 2205–2210.

[36] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proc. Int. Conf. Comput. Commun. (INFOCOM)*, Toronto, ON, Canada, 2014, pp. 1276–1284.

[37] F. Pan *et al.*, "Threshold-free physical layer authentication based on machine learning for industrial wireless CPS," *IEEE Trans Ind. Informat.*, vol. 15, no. 12, pp. 6481–6491, Dec. 2019.

[38] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. Int. Conf. Commun. Internet Inf. Technol. (CIIT)*, St. Thomas, US Virgin Islands, 2004, pp. 201–206.

[39] J. Hall, M. Barbeau, and E. Kranakis, "Detecting rogue devices in bluetooth networks using radio frequency fingerprinting," in *Proc. Int. Conf. Commun. Comput. Netw. (CCN)*, Lima, Peru, 2006, pp. 4–6.

[40] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proc. Int. Conf. Inf. Process. Sens. Netw. (IPSN)*, San Francisco, CA, USA, 2009, pp. 25–36.

[41] D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-based RF-DNA fingerprinting for classifying 802.16e WiMAX mobile subscribers," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Maui, HI, USA, 2012, pp. 7–13.

[42] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, 2008, pp. 116–127.

[43] X. Wang, Y. Wu, and B. Caron, "Transmitter identification using embedded pseudo random sequences," *IEEE Trans. Broadcast.*, vol. 50, no. 3, pp. 244–252, Sep. 2004.

[44] S. Supangkat, T. Eric, and A. Pamuji, "A public key signature for authentication in telephone," in *Proc. Asia–Pac. Conf. Circuits Syst. (APCCAS)*, Denpasar, Indonesia, 2002, pp. 495–498.

[45] Z. Zhang, L. Yang, Y. Zhu, B. Y. Zhao, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Bellevue, WA, USA, 2012, pp. 278–279.

[46] X. Tan, K. M. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. ACM Conf. Wireless Netw. Security (WiSec)*, Hamburg, Germany, 2011, pp. 79–90.

[47] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[48] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

[49] J. B. Perazzone, L. Y. Paul, B. M. Sadler, and R. S. Blum, "Physical layer authentication via fingerprint embedding: min-entropy analysis: Invited presentation," in *Proc. Conf. Inf. Sci. Syst. (CISS)*, Baltimore, MD, USA, 2019, pp. 1–6.

[50] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall PTR, 1993.

[51] J. A. Swets, *Signal Detection Theory and ROC Analysis in Psychology and Diagnostics: Collected Papers*. New York, NY, USA: Psychology Press, 2014.

[52] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[53] J. G. Proakis, *Digital Communications*. Boston, MA, USA: McGraw-Hill, 2001.

[54] T. S. Rappaport, *Wireless Communications: Principles and Practice*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall PTR, 1996.

[55] M. M. U. Rahman, A. Yasmeen, and J. Gross, "PHY layer authentication via drifting oscillators," in *Proc. Global Commun. Conf. (GLOBCOM)*, Austin, TX, USA, 2014, pp. 716–721.

[56] O. Gungor and C. E. Koksal, "On the basic limits of RF-fingerprint-based authentication," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4523–4543, Aug. 2016.

[57] C. K. Dubendorfer, B. W. Ramsey, and A. M. Temple, "An RF-DNA verification process for ZigBee networks," in *Proc. Military Commun. Conf. (MILCOM)*, Orlando, FL, USA, 2013, pp. 1–6.

[58] D. R. Reising and M. A. Temple, "WiMAX mobile subscriber verification using gabor-based RF-DNA fingerprints," in *Proc. Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, 2012, pp. 1005–1010.

[59] H. C. Choe, C. E. Poole, A. M. Yu, and H. H. Szu, "Novel identification of intercepted signals from unknown radio transmitters," in *Proc. Int. Soc. Opt. Photon. (SPIE)*, Orlando, FL, USA, 1995, pp. 504–517.

[60] J. Toonstra and W. Kinsner, "Transient analysis and genetic algorithms for classification," in *Proc. Conf. Commun. Power Comput. (WESCANEX)*, Winnipeg, MB, Canada, 1995, pp. 432–437.

[61] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system ODO-1," in *Proc. Conf. Commun. Power Comput. (WESCANEX)*, Calgary, AB, Canada, 1996, pp. 60–63.

[62] O. H. Tekbas, O. Ureten, and N. Serinken, "Improvement of transmitter identification system for low SNR transients," *Electron. Lett.*, vol. 40, no. 3, pp. 182–183, Feb. 2004.

[63] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Can. J. Elect. Comput. Eng.*, vol. 32, no. 1, pp. 27–33, May 2007.

[64] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proc. Int. Conf. Security Privacy Commun. Netw. (SecureComm)*, Nice, France, 2007, pp. 331–340.

[65] W. C. Suski, II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Proc. Global Telecommun. Conf. (GLOBECOM)*, New Orleans, LO, USA, 2008, pp. 1–5.

[66] A. Pitarokoilis, E. Bjornson, and E. G. Larsson, "ML detection in phase noise impaired SIMO channels with uplink training," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 223–235, Jan. 2016.

[67] C. Zhao, M. Huang, L. Huang, X. Du, and M. Guizani, "A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks," *Comput. Netw.*, vol. 128, pp. 164–171, Dec. 2017.

[68] S. Zeng, X. Li, A. Salem, and D. Zhao, "Physical layer authentication based on CFO and visibility graph," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Xi'an, China, 2018, pp. 147–152.

[69] S. Dolatshahi, A. C. Polak, and D. L. Goeckel, "Identification of wireless users via power amplifier imperfections," in *Proc. Asilomar Conf. Signals Syst. Comput. (ASILOMAR)*, Pacific Grove, CA, USA, 2010, pp. 1553–1557.

[70] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[71] A. C. Polak and D. L. Goeckel, "Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 5889–5899, Nov. 2015.

[72] S. B. Moon, P. Skelly, and D. Towsley, "Estimation and removal of clock skew from network delay measurements," in *Proc. Int. Conf. Local Comput. Netw. (INFOCOM) 18th Annu. Joint Conf. Comput. Commun. Soc. Future Now*, New York, NY, USA, 1999, pp. 227–234.

[73] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Depend. Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr.–Jun. 2005.

[74] S. Jana, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *Proc. ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, 2008, pp. 104–115.

[75] M. Cristea and B. Groza, "Fingerprinting smartphones remotely via ICMP timestamps," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1081–1083, Jun. 2013.

[76] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers," in *Proc. Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 939–944.

[77] P. Hao, X. Wang, and A. Behnad, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Proc. Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, 2014, pp. 613–618.

[78] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[79] B. Gassend, D. E. Clarke, M. V. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Washington, DC, USA, 2002, pp. 148–160.

[80] J. Guajardo, *Physical Unclonable Functions (PUFs)*. Boston, MA, USA: Springer, 2011.

[81] C. H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Circuits Syst. Mag.*, vol. 17, no. 3, pp. 32–62, 3rd Quart., 2017.

[82] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[83] B. Gassend, D. Lim, D. E. Clarke, M. V. Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency Comput. Pract. Exp.*, vol. 16, no. 11, pp. 1077–1098, 2003.

[84] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proc. IEEE Symp. VLSI Circuits (VLSI-Circuits)*, Honolulu, HI, USA, 2004, pp. 176–179.

[85] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based 'unclonable' RFID ICs for anti-counterfeiting and security applications," in *Proc. Int. Conf. Radio Freq. Identification (RFID)*, Las Vegas, NV, USA, 2008, pp. 58–64.

[86] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[87] C. L. Corbett, R. A. Beyah, and J. A. Copeland, "A passive approach to wireless NIC identification," in *Proc. Int. Conf. Commun. (ICC)*, Istanbul, Turkey, 2006, pp. 2329–2334.

[88] C. L. Corbett, R. A. Beyah, and J. A. Copeland, "Passive classification of wireless NICs during rate switching," *EURASIP J. Wireless Commun. Netw.*, vol. 2008, no. 28, pp. 1–12, 2007.

[89] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, "Radio transmitter fingerprinting: A steady state frequency domain approach," in *Proc. Veh. Technol. Conf. (VTC)*, Calgary, BC, Canada, 2008, pp. 1–5.

[90] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, "RF-DNA fingerprinting for airport WiMax communications security," in *Proc. Int. Conf. Netw. Syst. Security (NSS)*, Melbourne, VIC, Australia, 2010, pp. 32–39.

[91] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 1180–1192, 2015.

[92] H. Peng and X. Wang, "Performance enhanced wireless device authentication using multiple weighted device-specific characteristics," in *Proc. China Summit Int. Conf. Signal Inf. Process. (ChinaSIP)*, Chengdu, China, 2015, pp. 438–442.

[93] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.

[94] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *Proc. Conf. USENIX Security Symp. (USENIX)*, Montreal, QC, Canada, 2009, pp. 199–214.

[95] D. Zanetti and B. Danev, "Physical-layer identification of UHF RFID tags," in *Proc. ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, Chicago, IL, USA, 2010, pp. 353–364.

[96] J. Han *et al.*, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 846–858, Apr. 2016.

[97] M. K. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *Proc. Global Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, 2010, pp. 2168–2173.

[98] S. Theodoridis and K. Koutroumbas, *Pattern Recognition*. Amsterdam, The Netherlands: Academic, 2009.

[99] W. E. Cobb, E. W. Garcia, M. A. Temple, R. O. Baldwin, and Y. C. Kim, "Physical layer identification of embedded devices using RF-DNA fingerprinting," in *Proc. Military Commun. Conf. (MILCOM)*, San Jose, CA, USA, 2010, pp. 682–687.

[100] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 14–24, 2012.

[101] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *J. Commun. Netw.*, vol. 11, no. 6, pp. 544–555, Dec. 2009.

[102] Y. Xing, A. Hu, J. Zhang, L. Peng, and G. Li, "On radio frequency fingerprint identification for DSSS systems in low SNR scenarios," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2326–2329, Nov. 2018.

[103] L. Peng, A. Hu, J. Zhang, J. Yu, J. Yu, and Y. Yan, "Design of a hybrid RF fingerprint extraction and device classification scheme," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 349–360, Feb. 2019.

[104] L. Breiman, "Arcing classifiers," *Ann. Stat.*, vol. 26, no. 3, pp. 801–824, 1998.

[105] A. Candore, O. Kocabas, and F. Koushanfar, "Robust stable radiometric fingerprinting for wireless devices," in *Proc. Int. Workshop Hardw. Oriented Security Trust (HOST)*, San Francisco, CA, USA, 2009, pp. 43–49.

[106] W. Tu and L. Lai, "Keyless authentication and authenticated capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3696–3714, May 2018.

[107] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, 2008, pp. 1768–1776.

[108] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proc. 42nd Annu. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, 2008, pp. 642–646.

[109] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. ACM Workshop Wireless Security (WiSe)*, Alexandria, VA, USA, 2006, pp. 43–52.

[110] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-based authentication of mobile devices," in *Proc. Int. Conf. Ubiquitous Comput. (UbiComp)*, Innsbruck, Austria, 2007, pp. 253–270.

[111] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: Cooperative proximity-based authentication," in *Proc. Int. Conf. Mobile Syst. Appl. Service (MobiSys)*, San Francisco, CA, USA, 2010, pp. 331–344.

[112] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang, "Privacy-preserving location-based services for mobile users in wireless networks," Dept. Comput. Sci., Yale Univ., New Haven, CT, USA, Rep. YALEU/DCS/TR-1297, 2004.

[113] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proc. Int. Symp. World Wireless Mobile Multimedia Netw. (WOWMOM)*, Niagara Falls, NY, USA, 2006, pp. 564–570.

[114] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. Int. Conf. Commun. (ICC)*, Beijing, China, 2008, pp. 1520–1524.

[115] Q. Wang, "A novel physical layer assisted authentication scheme for mobile wireless sensor networks," *Sensors (Basel)*, vol. 17, no. 2, p. 289, 2010.

[116] Y. Chen, Y. Jie, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[117] R. A. Redner and H. F. Walker, "Mixture densities, maximum likelihood and the EM algorithm," *SIAM Rev.*, vol. 26, no. 2, pp. 195–239, 1984.

[118] L. Xiao, Y. Li, G. Liu, Q. Li, and W. Zhuang, "Spoofing detection with reinforcement learning in wireless networks," in *Proc. Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, 2015, pp. 1–5.

[119] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[120] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[121] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bangalore, India, 2010, pp. 1–9.

[122] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. Military Commun. Conf. (MILCOM)*, Baltimore, MD, USA, 2011, pp. 538–542.

[123] F. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. Int. Conf. Commun. (ICC)*, Budapest, Hungary, 2013, pp. 4724–4728.

[124] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[125] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.
[126] S. J. Fortune, D. M. Gay, B. W. Kernighan, O. Landron, R. A. Valenzuela, and M. H. Wright, "WISE design of indoor wireless systems: Practical computation and optimization," *IEEE Comput. Sci. Eng.*, vol. 2, no. 1, pp. 58–68, Mar. 1995.
[127] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948–5956, Dec. 2009.
[128] Z. Jiang, J. Zhao, X. Y. Li, J. S. Han, and W. Xi, "Rejecting the attack: Source authentication for Wi-Fi management frames using CSI information," in *Proc. Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, 2013, pp. 2544–2552.
[129] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information (CSI)," in *Proc. ACM Symp. Inf. Comput. Commun. Security (ASIACCS)*, Kyoto, Japan, 2014, pp. 389–400.
[130] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating users through fine-grained channel information," *IEEE Trans. Mobile Comput.*, vol. 17, no. 9, pp. 251–264, Feb. 2018.
[131] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.
[132] X. Wu and Y. Zhen, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, Jan. 2015.
[133] F. Ye, X. Zhang, Y. Li, and H. Huang, "Primary user localization algorithm based on compressive sensing in cognitive radio networks," *Algorithms*, vol. 9, no. 2, p. 25, 2016.
[134] H. M. Furqan, A. A. Mehmet, M. Nazzal, and A. Hüseyin, "Primary user emulation and jamming attack detection in cognitive radio via sparse coding," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 141, pp. 1–19, 2020.
[135] N. Wang, W. Li, T. Jiang, and S. Lv, "Physical layer spoofing detection based on sparse signal processing and fuzzy recognition," *IET Signal Process.*, vol. 11, no. 5, pp. 640–646, Jul. 2017.
[136] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," *IET Commun.*, vol. 11, no. 9, pp. 1431–1437, Jun. 2017.
[137] Y. Lee, E. Hwang, and J. Choi, "Performance analysis of compressive sensing based physical layer authentication for AMI," in *Proc. Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Cairns, QLD, Australia, 2018, pp. 1–6.
[138] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1557–1560, Jul. 2017.
[139] A. Weinand, M. Karrenbauer, R. Sattiraju, and H. Schotten, "Application of machine learning for channel based message authentication in mission critical machine type communication," in *Proc. Eur. Wireless Conf. (EW)*, Dresden, Germany, 2017, pp. 1–5.
[140] Q. Wang, H. Li, Z. Chen, D. Zhao, S. Ye, and J. Cai, "Supervised and semi-supervised deep neural networks for CSI-based authentication," 2018. [Online]. Available: https://arxiv.org/abs/1807.09469.
[141] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive MIMO systems with hardware impairments," *IEEE Trans Ind. Informat.*, vol. 19, no. 3, pp. 1563–1576, Mar. 2020.
[142] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Proc. Conf. Sensor Mesh Ad Hoc Commun. Netw. (SECON)*, San Diego, CA, USA, 2007, pp. 193–202.
[143] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric bayesian method," in *Proc. Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, 2011, pp. 1404–1412.
[144] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 377–380, Aug. 2014.
[145] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.
[146] X. Wang, F. J. Liu, D. Fan, H. Tang, and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *Proc. Int. Conf. Commun. (ICC)*, Kyoto, Japan, 2011, pp. 1–5.
[147] V. Kumar, J. M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Scottsdale, AZ, USA, 2014, pp. 787–798.
[148] D. Xu, Q. D. P. Ren, Y. Wang, and L. Sun, "ICA-SBDC: A channel estimation and identification mechanism for MISO-OFDM systems under pilot spoofing attack," in *Proc. Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.
[149] D. Xu, P. Ren, and J. A. Ritcey, "Optimal independence-checking coding for secure uplink training in large-scale MISO-OFDM systems," in *Proc. Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, 2018, pp. 1–6.
[150] D. Xu, P. Ren, J. A. Ritcey, and Y. Wang, "Code-frequency block group coding for anti-spoofing pilot authentication in multi-antenna OFDM systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 1778–1793, 2018.
[151] D. Xu, P. Ren, and J. A. Ritcey, "Independence-checking coding for OFDM channel training authentication: Protocol design, security, stability, and tradeoff analysis," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 387–402, 2019.
[152] D. Xu, P. Ren, and J. A. Ritcey, "PHY-layer cover-free coding for wireless pilot authentication in IoV communications: Protocol design and ultra-security proof," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 171–187, Feb. 2019.
[153] G. J. Simmons, "Authentication theory/coding theory," in *Proc. Adv. Cryptol. (CRYPTO)*, Berlin, Germany, 1984, pp. 411–431.
[154] C. G. Boncelet, "The NTMAC for authentication of noisy messages," *IEEE Trans. Inf. Forensics Security*, vol. 1, pp. 35–42, 2006.
[155] Y. Liu and C. Boncelet, "The CRC-NTMAC for noisy message authentication," *IEEE Trans. Inf. Forensics Security*, vol. 1, pp. 517–523, 2006.
[156] I. Csisz, "Almost independence and secrecy capacity," *Problems Inf. Transm.*, vol. 32, no. 1, pp. 40–47, 1996.
[157] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.
[158] R. A. Chou and A. Yener, "Strongly secure multiuser communication and authentication with anonymity constraints," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 572–586, Jan. 2020.
[159] G. Verma, P. L. Yu, and B. M. Sadler, "Physical layer authentication via fingerprint embedding using software-defined radios," *IEEE Access*, vol. 3, pp. 81–88, 2015.
[160] P. L. Yu, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 48–53, Jun. 2015.
[161] P. L. Yu, B. M. Sadler, G. Verma, and J. S. Baras, *Fingerprinting by Design: Embedding and Authentication*. New York, NY, USA: Springer, 2016.
[162] P. L. Yu, J. S. Baras, and B. M. Sadler, "Multicarrier authentication at the physical layer," in *Proc. Int. Symp. World Wireless Mobile Multimedia Netw. (WOWMOM)*, Newport Beach, CA, USA, 2008, pp. 1–6.
[163] Y. Ran, H. Al-Shwaily, C. Tang, G. Y. Tian, and M. Johnston, "Physical layer authentication scheme with channel based tag padding sequence," *IET Commun.*, vol. 13, no. 12, pp. 1776–1780, Jul. 2019.
[164] P. L. Yu, J. B. Perazzone, B. M. Sadler, and R. S. Blum, "Authenticated side channel via physical layer fingerprinting," in *Proc. Conf. Commun. Netw. Security (CNS)*, Philadelphia, PA, USA, 2016, pp. 631–635.
[165] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, Jul. 2018.
[166] N. S. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channel emulation," in *Proc. IEEE Symp. New Front. Dyn. Spectr. (DySPAN)*, Singapore, 2010, pp. 1–7.
[167] N. S. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, "Authenticating MIMO transmissions using channel-like fingerprinting," in *Proc. Global Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, 2010, pp. 1–6.
[168] N. S. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, "Extrinsic channel-like fingerprint embedding for authenticating MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 4270–4281, Dec. 2011.
[169] N. S. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, "Extrinsic channel-like fingerprinting overlays using subspace embedding," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 1355–1369, 2011.
[170] T. Rappaport, R. Heath, R. Daniels, and J. Murdock, *Millimeter Wave Wireless Communications*. Upper Saddle River, NJ, USA: Pearson Educ., 2015.
[171] S. Arnon, *Visible Light Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[172] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[173] R. Cavallari, F. Martelli, R. Rosinia, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1635–1657, 3rd Quart., 2014.
[174] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.

Ning Xie (Senior Member, IEEE) received the B.Eng. and Ph.D. degrees in communications and information system from Sun Yat-sen University, China, in 2002 and 2007, respectively. Since 2007, he has been with the College of Electronics and Information Engineering, Shenzhen University, Shenzhen, China, where he is currently an Associate Professor. His research interests include physical-layer security, physical-layer authentication, and adaptive signal processing in wireless communications. He is currently an Area Editor for *Journal of Computer Communications* (Elsevier).

Zhuoyuan Li received the B.Eng. degree in communication engineering from the Shenyang University of Chemical Technology, Shenyang, China, in 2018. He is currently pursuing the master's degree with the College of Electronic and Information Engineering, Shenzhen University, Shenzhen, China. His research interests include information security at the physical layer and wireless communication.

Haijun Tan received the B.Eng. degree in electronic science and technology from the South China University of Technology, Guangzhou, China, in 2010, the M.Eng. degree in communication and information system from the Department of Communication and Information System, Sun Yat-sen University, Guangzhou, in 2013, and the Ph.D. degree in signal processing from the University of Hong Kong, Hong Kong, in 2019. He is currently an Associate Researcher with the College of Electronics and Information Engineering, Shenzhen University, Shenzhen, China. His research interests include adaptive signal processing and physical-layer authentication in wireless communications.