On the Application of Channel Characteristic-Based Physical Layer Authentication in Industrial Wireless Networks

Qiuhua Wang[1], Mingyang Kang[1], Lifeng Yuan[1,2*], Yunlu Wang[1], Gongxun Miao[3] and Kim-Kwang Raymond Choo[2]
[1] School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
[e-mail: wangqiuhua@hdu.edu.cn, kangmingyang@hdu.edu.cn, yuanlifeng@hdu.edu.cn,wyl@hdu.edu.cn]
[2] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA
[e-mail: raymond.choo@utsa.edu]
[3]Zhongfu Information Co., Ltd., Jinan 250101, China
[e-mail: miaogx@zhongfu.net]
*Corresponding author: Lifeng Yuan

Received March 26, 2021; revised April 18, 2021; accepted May 26, 2021; published June 30, 2021

Abstract

Channel characteristic-based physical layer authentication is one potential identity authentication scheme in wireless communication, such as used in a fog computing environment. While existing channel characteristic-based physical layer authentication schemes may be efficient when deployed in the conventional wireless network environment, they may be less efficient and practical for the industrial wireless communication environment due to the varying requirements. We observe that this is a topic that is understudied, and therefore in this paper, we review the constructions and performance of several commonly used test statistics and analyze their performance in typical industrial wireless networks using simulation experiments. The findings from the simulations show a number of limitations in existing channel characteristic-based physical layer authentication schemes. Therefore, we believe that it is a good idea to combine machine learning and multiple test statistics for identity authentication in future industrial wireless network deployment. Four machine learning methods prove that the scheme significantly improves the authentication accuracy and solves the challenge of choosing a threshold.

Keywords: Physical layer authentication, industrial wireless network, channel state information, test statistic.

This research was supported by Zhejiang Provincial Natural Science Foundation of China under Grant No.LY19F020039

http://doi.org/10.3837/tiis.2021.06.018 **ISSN : 1976-7277**

1. Introduction

1.1 Physical Layer Authentication in Wireless Communication Systems

As wireless communications are more widely deployed, for example, in applications such as military, finance, and healthcare, there is a need to ensure the security of such communications (e.g., data-in-transit). Generally, wireless network security is achieved through upper layer encryption and authentication mechanisms [1]. However, conventional encryption-based authentication mechanisms are resource-intensive and often incur high computational complexity and time delay. Such requirements contradict the nature of wireless networks (e.g., devices in the environment may be energy and resource-limited). Moreover, conventional upper layer authentication approaches do not adequately consider the vulnerabilities of wireless channels, making it vulnerable to attacks from the physical layer [2]. Therefore, conventional encryption-based authentication approaches may not be suitable for resource-constrained wireless network devices.

This reinforces the importance of designing a new lightweight security authentication approach for resource-constrained wireless networks. During the design phase, it is important to understand the inherent characteristics of wireless channels and the various building blocks. For example, wireless channel characteristic-based physical layer authentication (PLA) uses the reciprocity and spatial uniqueness of wireless channels, and it realizes node identity authentication by comparing the similarity of wireless channel characteristics in a coherent time [3-5]. PLA only involves lightweight hardware operations and does not require complex upper-layer encryption and decryption operations. Therefore, due to advantages such as low computational complexity, small communication overhead, minimal time delay, low power consumption, PLA can potentially facilitate real-time authentication of wireless network terminals with limited resources.

PLA is based on the Jakes uniform scattering model [6], which states that the received signal will decorrelate rapidly when the spatial separation between two different entities is greater than half of the transmission wavelength. Hence, when the distance between the attacker and the legitimate transmitter is greater than one or two transmission wavelengths, the legitimate wireless channel will experience a completely independent fading path. In addition, the attacker cannot predict or fabricate the random declines in advance, and the wireless channel response reflects the fading characteristic of the wireless channel. Therefore, the PLA can be converted to distinguish the legitimate path channel response from the illegitimate path channel response.

PLA generally distinguishes between the legitimate and illegitimate paths based on channel detection and hypothesis test [7-15]. The key of the approach is to calculate the difference between the current channel response and the channel response of the authenticated legitimate path through certain test statistics. By comparing the difference with a preset threshold, one can determine whether the current message is from an attacker (i.e., the difference is greater than the threshold) or is from the expected legitimate transmitter (i.e., the difference is less than the threshold).

At present, PLA technology based on hypothesis testing can be divided into two categories: one is authentication schemes based on channel characteristics, and the other is authentication schemes based on radio frequency fingerprints. The channel characteristics-based PLA scheme verifies an unknown transmitter's identity by comparing the current channel state information with the legal channel state information [16-29]. This work mainly focuses on the extraction of channel characteristics, and through these channel characteristics to improve the authentication accuracy. The PLA scheme based on the radio frequency fingerprint identifies the user according to the unique features of the user's waveform [30-34]. In addition to the above two authentication schemes, some other authentication schemes have been proposed, such as watermark/fingerprint embedding [35-37], multiple attributes and multiple observation (MAMO) technology [38], etc. In this paper, we mainly study the channel-based authentication scheme, which will be introduced in detail in the next chapter.

1.2 The Significance of PLA in Industrial Wireless Networks

Wireless industrial networks are very important to industrial automation. However, industrial wireless networks are vulnerable to attacks. Security is very important in industrial control systems. If attackers send malicious commands to the control device, it may cause serious consequences. The existing schemes all rely on cryptography mechanisms to solve this problem, such as symmetric keys and asymmetric keys. However, the schemes based on symmetric key technology have their own deficiencies that cannot be overcome, such as the assumption of security time limit [49], the fact that they are physical neighbors and the link is reliable cannot establish a direct secure link [50], a small number of captured nodes will expose part of the pairwise key, and a proper number of captured nodes may expose the entire key pool [51]. These security deficiencies may be ignored for applications with low-security requirements, but industrial control systems with high-security requirements need to introduce asymmetric key mechanisms to compensate, such as public-key mechanisms. However, the computational strength required by public key cryptosystems is usually hundreds to thousands of times that of symmetric cryptosystems. Most public-key mechanisms have longer keys and larger encrypted blocks, and there is additional certificate overhead when using the certificate mechanism. The calculation, storage, communication, energy, and other expenses caused by these factors are often not borne by wireless terminals with limited resources. Moreover, in the clone attack or Sybil attack, since the ID and key information of the legitimate node are counterfeited by the clone node and the Sybil node, the clone node and the Sybil node cannot be detected by the cryptographic-based authentication mechanism.

Since wireless channel features are space-time unique and unforgeable, the channel characteristics-based PLA technology is a good scheme to solve the above problems. However, most existing channel characteristics-based PLA schemes are deployed or evaluated in traditional wireless network environments (e.g., offices and laboratories) rather than industrial wireless networks. A typical industrial environment may involve scenarios characterized by high temperature, rotating parts, etc. [39,40]. Therefore, in these scenarios, the channel characteristics (e.g., channel gain and multipath effects) may differ significantly from the conventional wireless network environment. This is the gap this paper seeks to address. Specifically, we will study the applicability of existing channel characteristics-based PLA schemes in industrial wireless networks.

1.3 Our Contributions

The main contributions of this paper are as follows:

1) We discuss some commonly used schemes for calculating channel characteristic differences and analyze their advantages and limitations.
2) We regard PLA as a binary classification problem, then use machine learning classification algorithms for learning, and finally use the trained model for identity authentication. This training helps the receiver to understand channel variations and

makes authentication a threshold-free binary classification problem.

3) Extensive simulation verification has been carried out on the real industrial data set, and field verification has been carried out in the real factory, which provides important value for the application of PLA in industrial physics in the future.

1.4 Organization of the Paper

The remainder of this paper is organized as follows. In Section 2, we identify and discuss several commonly used test statistics construction methods, which are used to calculate the channel characteristic differences, and analyze their advantages and limitations. In Section 3, we evaluate the performance of test statistics through simulation experiments in industrial wireless networks. In Section 4, we evaluated the performance of machine learning schemes in industrial wireless networks. In Section 5, we summarize the paper.

2. The Channel Characteristics-Based PLA Scheme

2.1 The Channel Characteristic-based PLA Model

At present, channel characteristics-based PLA is implemented using hypothesis testing. We briefly describe the process through a simple tripartite model. As shown in **Fig. 1**, Alice is the legitimate sender, Bob is the legitimate receiver, and Eve is the attacker. Alice, Bob, and Eve are at different locations, and the distance between them is greater than half a wavelength. Suppose that Bob has verified the kth data frame from Alice. $\widehat{H}_k^{AB}$is the channel characteristic of the kth data frame. The transmitter of the k+1st data frame is unknown, and its channel characteristic is $\widehat{H}_{k+1}^{XB}$. T is the channel characteristic difference between $\widehat{H}_k^{AB}$ and $\widehat{H}_{k+1}^{XB}$, then:

$$\mathrm{T}=diff\,(\hat{H}_k^{AB}-\hat{H}_{k+1}^{AB}). \tag{1}$$

The function $diff\,(\mathrm{A}-\mathrm{B})$ is used to calculate the difference between variables A and B.

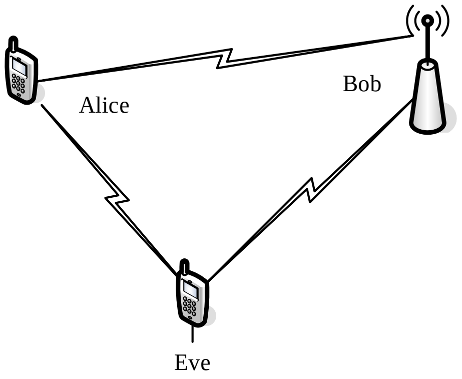


Fig. 1. A typical three-party communication model.

T is used as a test statistic in the hypothesis verification problem, which can be expressed mathematically as:

$$\mathrm{T}\overset{\le\mathcal{H}_0}{\underset{>\mathcal{H}_1}{}}\eta. \tag{2}$$

In the above equation, η is a preset threshold. The null hypothesis $\mathcal{H}_0$ indicates that the k+1st data frame is from Alice, while the alternative hypothesis $\mathcal{H}_1$ indicates that the k+1st data frame comes from Eve. It can be seen from (2) that the key to hypothesis test-based PLA is to compare the channel characteristic difference with a preset threshold. Therefore, calculating the channel characteristic difference and determining the preset threshold is very important to PLA. Next, we will analyze several commonly used statistical schemes, which are used to calculate channel differences.

2.2 Commonly Used Channel Characteristics-Based PLA Schemes

In this section, we sort out several commonly used the channel characteristics construction schemes, and analyze their advantages and disadvantages.

2.2.1 The amplitude-based test statistic T_A

In the OFDM communication system, He et al. found that differences between the sub-channel amplitudes can be used for identity authentication [7]. The channel response includes amplitude and phase offset. The channel responses of two consecutive data frames are $\widehat{H}_k^{AB}$ and $\widehat{H}_{k+1}^{AB}$, respectively. In the OFDM system, the amplitude and phase of the channel response between different sub-channels are different. The phase offset vector $\varphi(l)$ of each sub-channel l is:

$$\varphi(l) = arg\left(\hat{H}_{k+1}^{AB}(l) \bullet \left[\hat{H}_k^{AB}(l)\right]^*\right). \tag{3}$$

[A]* represents the complex conjugate of complex A. $arg\ (A)$ is the argument of A. $\widehat{H}_k^{AB}(l)$ represents the channel characteristics of the lth sub-channel. The amplitude-based test statistic T_A is:

$$\mathrm{T}_A = \frac{1}{\sigma^2}\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l) - \hat{H}_k^{AB}(l)e^{j\varphi(l)}\right|. \tag{4}$$

In the above equation, σ^2 denotes the noise power. Since σ^2 is usually unknown, it is challenging to calculate the test statistic T_A. Besides, T_A presents an irregular distribution, so it is challenging to determine the threshold accurately. Hence, the test statistic T_A cannot be used for authentication.

2.2.2 The phase-based test statistic T_B

Because different noises interfere with the signals of different sampling channels, the phase offset will also be different. He et al. made full use of the phase offset to identify the channel, thereby achieving identity authentication [7]. The phase-based test statistic T_B is:

$$\mathrm{T}_B = \frac{1}{\pi^2}\sum_{l=1}^{L}\left|\varphi(l)\right|^2. \tag{5}$$

Since the test statistic T_B obeys the Gaussian distribution, its threshold can be easily determined. As the calculation of T_B does not involve the unknown variable σ^2, the test statistic T_B can be accurately calculated.

2.2.3 The test statistic based on the combined amplitude and phase T_C

The test statistic T_A eliminates the effect of phase offset, it only uses the sub-channel amplitude to obtain the channel difference. The test statistic T_B only uses the sub-channel phase to get the channel difference. Both amplitude and phase can be used to construct the test statistic. He et al. constructed the test statistic based on the combined amplitude and phase [7], denoted as T_C:

$$\mathrm{T}_C = \frac{1}{\sigma^2}\sum_{l=1}^{L}\left|\hat{H}_k^{AB}(l) - \hat{H}_{k+1}^{XB}(l)\right|^2. \tag{6}$$

Compared with the test statistic T_A, the test statistic T_C does not eliminate the influence of phase offset, so it is affected by phase and amplitude. Besides, the test statisticT_C presents chi-square distribution, so its threshold can be calculated under a certain false alarm probability. However, like the test statistic T_A, it is difficult to calculate its value accurately because of the unknown noise power σ^2. Therefore, the test statistic T_C is not practical, too.

2.2.4 The test statistic based on corrected phase offset T_D

Considering the effects of noise and phase offset, Xiao et al. constructed the test statistic T_D based on the corrected phase offset [4]. Since the test statisticT_D needs to correct the phase offset effect, the phase offset φ should be minimized and written as φ^*:

$$\varphi^* = arg\left(\sum_{l=1}^{L}\hat{H}_k^{AB}(l)\bullet\left[\hat{H}_{k+1}^{XB}(l)\right]^*\right). \tag{7}$$

The test statistic T_D is:

$$\mathrm{T}_D = \frac{1}{\sigma^2}\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l) - \hat{H}_k^{AB}(l)e^{j\varphi^*}\right|^2. \tag{8}$$

The test statistic T_D obeys the chi-square distribution, so its threshold can be easily determined. However, like the test statistic T_A and the test statistic T_C, it is challenging to calculate the test statistic T_D accurately because of the unknown noise power σ^2. Therefore, it is an urgent need to normalize method to eliminate the influence of σ^2.

2.2.5 The test statistic based on the normalized likelihood ratio test T^{LRT}

Based on [4], Xiao et al. proposed a PLA scheme based on the normalized likelihood ratio test (LRT) [8], which eliminated the influence of noise power σ^2 by using the normalization method. The new test statistic T_D^{LRT} is:

$$\mathrm{T}_D^{LRT} = \frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l) - \hat{H}_k^{AB}(l)e^{j\varphi^*}\right|^2}{\sum_{l=1}^{L}\left|\hat{H}_k^{AB}(l)\right|^2}. \tag{9}$$

By performing the same process to the test statistic T_A and the test statistic T_C,the test statistic T_A^{LRT} and the test statisticT_C^{LRT} can be obtained as follows:

$$\mathrm{T}_A^{LRT} = \frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l) - \hat{H}_k^{AB}(l)e^{j\varphi}\right|}{\sum_{l=1}^{L}\left|\hat{H}_k^{AB}(l)\right|}, \tag{10}$$

$$\mathrm{T}_{C}^{LRT}=\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l)-\hat{H}_{k}^{AB}(l)\right|^{2}}{\sum_{l=1}^{L}\left|\hat{H}_{k}^{AB}(l)\right|^{2}}. \tag{11}$$

Obviously, through the normalization method, the test statistic T^{LRT} eliminates the noise power σ^2. However, due to the normalization process, the test statistic T^{LRT} no longer obeys the chi-square distribution. So, it will be difficult to determine the threshold, and it is necessary to traverse the test statistic T^{LRT} to find its optimal threshold.

In [10], the test statistic T^{LRT} was improved on the basis of [8], and a new scheme was constructed, which used the channel responses of three consecutive data frames to calculate the channel characteristic difference. The new normalized test statistic T^{ILRT} is:

$$\mathrm{T}_{A}^{ILRT}=\left|\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l)-\hat{H}_{k}^{AB}(l)e^{j\varphi}\right|}{\sum_{l=1}^{L}\left|\hat{H}_{k}^{AB}(l)-\hat{H}_{k-1}^{AB}(l)e^{j\varphi}\right|}-1\right|, \tag{12}$$

$$\mathrm{T}_{C}^{ILRT}=\left|\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l)-\hat{H}_{k}^{AB}(l)\right|^{2}}{\sum_{l=1}^{L}\left|\hat{H}_{k}^{AB}(l)-\hat{H}_{k-1}^{AB}(l)\right|^{2}}-1\right|, \tag{13}$$

$$\mathrm{T}_{D}^{ILRT}=\left|\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1}^{XB}(l)-\hat{H}_{k}^{AB}(l)e^{j\varphi^{*}}\right|^{2}}{\sum_{l=1}^{L}\left|\hat{H}_{k}^{AB}(l)-\hat{H}_{k-1}^{AB}(l)e^{j\varphi^{*}}\right|^{2}}-1\right|. \tag{14}$$

The test statistic T^{ILRT} needs to successfully verify the previous two data frames before it can be used, and the threshold range will also be reduced. Compared with the test statisticT^{LRT}, the selection of its optimal threshold is faster. The test statistic T^{ILRT} eliminates the unknown parameter σ^2, and its threshold is easy to be determined. Therefore, the test statistic T^{ILRT} has high practicality.

2.2.6 The test statistic based on sequential probability ratio test T^{SPRT}

Inspired by [8], Wen et al. proposed the test statistic based on the sequential probability ratio test (SPRT) [9]. The test statisticT^{SPRT} uses the channel responses of previous *s* authenticated data frames to identity the *k*th data frame. The test statistic T^{SPRT} is more conducive to calculating the threshold and improving the detection rate to a certain extent. The expression of the test statistic T^{SPRT} is:

$$\mathrm{T}_{A}^{SPRT}=\frac{1}{s}\sum_{i=0}^{s-1}\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1-i}^{XB}(l)-\hat{H}_{k-i}^{AB}(l)e^{j\varphi(l)}\right|}{\sum_{l=1}^{L}\left|\hat{H}_{k-i}^{AB}(l)\right|}, \tag{15}$$

$$\mathrm{T}_C^{SPRT}=\frac{1}{s}\sum_{i=0}^{s-1}\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1-i}^{XB}(l)-\hat{H}_{k-i}^{AB}(l)\right|^2}{\sum_{l=1}^{L}\left|\hat{H}_{k-i}^{AB}(l)\right|^2}, \tag{16}$$

$$\mathrm{T}_D^{SPRT}=\frac{1}{s}\sum_{i=0}^{s-1}\frac{\sum_{l=1}^{L}\left|\hat{H}_{k+1-i}^{XB}(l)-\hat{H}_{k-i}^{AB}(l)e^{j\varphi^*}\right|^2}{\sum_{l=1}^{L}\left|\hat{H}_{k-i}^{AB}(l)\right|^2}. \tag{17}$$

Compared with the test statistic T^{LRT}, the test statistic T^{SPRT} treats the channel responses of consecutive frames as the statistic test. Therefore, the test statistic T^{SPRT} is better and more practical than the test statistic T^{LRT}. However, with the increase of s, the system load will increase accordingly. Thus, s should not be too large.

In [10], the test statistic $\mathrm{T}^{SPRT}$was improved. It compares the channel response of the kth data frame with that of the previous s data frames and takes the average value of the obtained s differences as the improved test statistic $\mathrm{T}^{ISPRT}$of the kth data frame. The threshold η of the test statistic T^{ISPRT} becomes smaller, so it is easier to obtain the optimal threshold through traversal. The test statistic T^{ISPRT} is:

$$\mathrm{T}_A^{ISPRT}=\left|\frac{\sum_{i=0}^{s-1}\sum_{l=1}^{L}\left|\hat{H}_{k+1-i}^{XB}(l)-\hat{H}_{k-i}^{AB}(l)e^{j\varphi(l)}\right|}{\sum_{i=0}^{s}\sum_{l=1}^{L}\left|\hat{H}_{k-i}^{AB}(l)-\hat{H}_{k-i-1}^{AB}(l)e^{j\varphi(l)}\right|}-1\right|, \tag{18}$$

$$\mathrm{T}_C^{ISPRT}=\left|\frac{\sum_{i=0}^{s-1}\sum_{l=1}^{L}\left|\hat{H}_{k+1-i}^{XB}(l)-\hat{H}_{k-i}^{AB}(l)\right|^2}{\sum_{i=0}^{s}\sum_{l=1}^{L}\left|\hat{H}_{k-i}^{AB}(l)-\hat{H}_{k-i-1}^{AB}(l)\right|^2}-1\right|, \tag{19}$$

$$\mathrm{T}_D^{ISPRT}=\left|\frac{\sum_{i=0}^{s-1}\sum_{l=1}^{L}\left|\hat{H}_{k+1-i}^{XB}(l)-\hat{H}_{k-i}^{AB}(l)e^{j\varphi^*}\right|^2}{\sum_{i=0}^{s}\sum_{l=1}^{L}\left|\hat{H}_{k-i}^{AB}(l)-\hat{H}_{k-i-1}^{AB}(l)e^{j\varphi^*}\right|^2}-1\right|. \tag{20}$$

The test statistic T^{ISPRT} requires at least two authenticated data frames, and the computational complexity will increase with the increase of s. Therefore, the computational complexity of the test statistic T^{ISPRT} is slightly higher than that of the test statistic T^{SPRT}.

3. Statistics Schemes Simulation and Performance Analysis

3.1 Simulation data and sites

In this paper, we use the CSI data sets provided by the National Institute of Standards and Technology (NIST) [41]. The NIST uses the channel impulse response measured in four typical industrial sites as CSI. The four typical industrial sites are the steamer plant, the Open Area Test Site (OATS), the automotive factory and the machine shop. The transmitting device remains stationary at all times, and the central transmission frequency of the Omni-antennas is 2.25 GHz. Each site includes multiple collections. Multiple collections are obtained in each experiment, and each collection includes multiple records. In this paper, since the authentication of the spoofing attack is considered, we simulated two different entities, namely a legitimate transmitter and an attacker. In the simulation experiments, the simulated legitimate transmitter corresponds to the actual receiving device, and the simulated receiver corresponds to the actual transmitting device. However, since the wireless channel is reciprocal, the results will not be affected.

3.1.1 The automotive factory

The automotive factory is a 400m × 400m × 12m indoor environment. In this site, tall metal machines are everywhere. This site includes two data collection paths: the inner loop and the outer loop. In the outer loop, the receiving device collects data at 135 locations, and each collection contains 300 records. In the simulation experiments, the data collected at the 68th location is set as legitimate data, as shown in **Fig. 2**. In the inner loop, the receiving device collects data at 103 locations, and each collection contains 300 records. In the simulation experiments, the data collected at the 52nd location is set as legitimate data, as shown in **Fig. 3**.

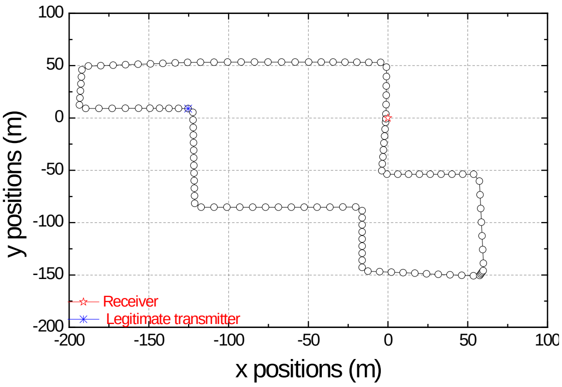


Fig. 2. Date collection locations in the automotive factory (outer loop).

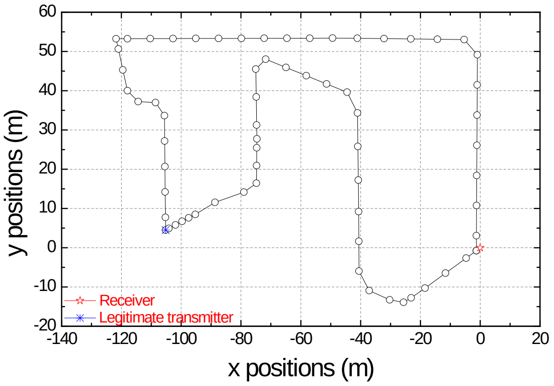


Fig. 3. Date collection locations in the automotive factory (inner loop).

3.1.2 The machine shop

The machine shop is a 12m × 50m × 7.6m indoor environment. In this site, metal machines are everywhere, and they reflect radio waves and increase the multipath effects. In this scenario, the receiving device collects data at 210 locations, and each collection contains 50 records. In the simulation experiments, the data collected at the 106th location is set as legitimate data, as shown in **Fig. 4**.

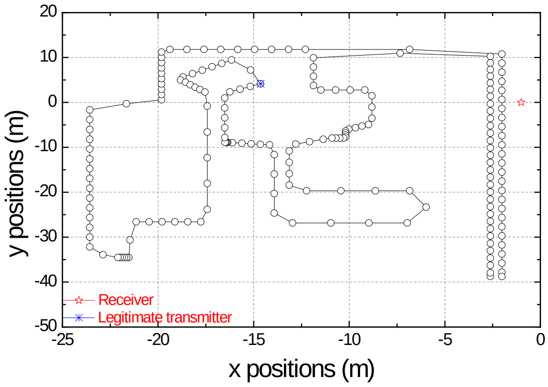


Fig. 4. Date collection locations in the machine shop.

3.1.3 The steamer plant

The steamer plant is a 50m × 80m × 7.6m factory with large machinery and elevated obstacles. In this scenario, the receiving device collects data at 665 locations, and each collection contains 40 records. In the simulation experiments, the data collected at the 333rd location is set as legitimate data, as shown in **Fig. 5**.

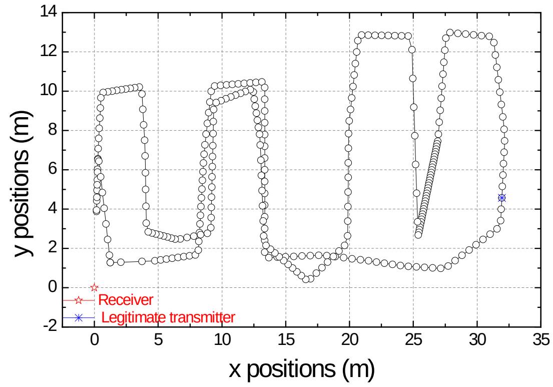


Fig. 5. Date collection locations in the Steamer plant.

3.1.4 The OATS

The OATS is an open area with fewer interference sources. The receiving device collects data at 410 locations, and each collection contains 40 records. In the simulation experiments, the data collected at the 206th location is set as legitimate data, as shown in **Fig. 6**.

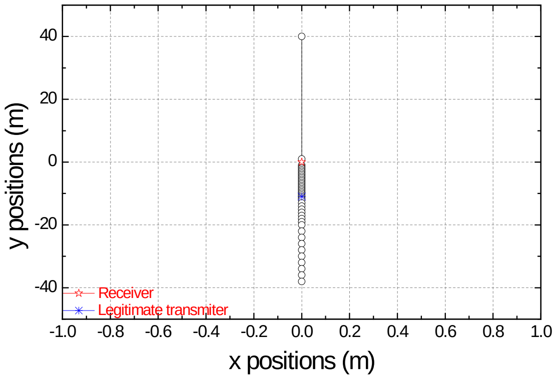


Fig. 6. Date collection locations in the OATS.

3.2 Measurement of Scheme Performance

In this section, we use NIST data to calculate channel differences and verify the performance of the test statistics introduced in section 3 in industrial wireless networks. As the noise power σ^2 is unknown, T_A, T_B and T_D will not be tested in this paper. For test statistics T^{ISPRT} and T^{SPRT}, $s = 3$.

The receiver operating characteristic (ROC) curve, including the detection rate *dr* and the false alarm rate *far*, is used to represent the performance of the test statistic scheme. The ROC curve can clearly show the change of the *dr* and the *far* with the threshold, so the optimal threshold value can be determined well. Through ROC curve, the performance of each scheme can be well compared. The *dr* indicates the probability of detecting an attacker, and *far* indicates the probability of misidentifying a legitimate transmitter as an attacker. *dr* and *far* are computed by (21) and (22), where $Pr(\cdot \mid \cdot)$ represents the conditional probability.

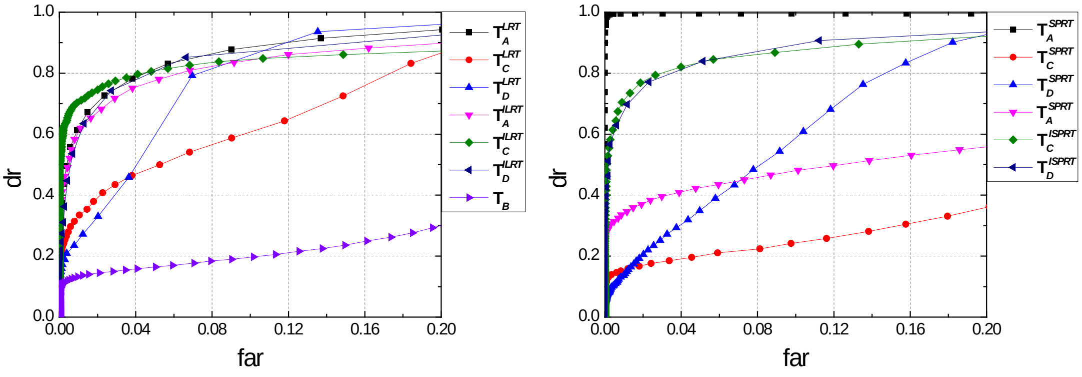
$$dr = Pr\left(\mathcal{H}_1 \mid \mathcal{H}_1\right), \tag{21}$$

$$far = Pr\left(\mathcal{H}_1 \mid \mathcal{H}_0\right). \tag{22}$$

3.3 Simulation results and analysis

3.3.1 Performance in the machine shop

Fig. 7 shows the performances of various test statistics in the machine shop. It can be seen that in this site, the performance of the test statistic T_A^{SPRT} is better than that of other test statistics. When the *far* of the test statistic T_A^{SPRT} is 4.938%, its *dr* reaches 99.52%. For the test statistic T^{LRT}, $\mathrm{T}_A^{LRT} > \mathrm{T}_D^{LRT} > \mathrm{T}_C^{LRT}$. For the test statistic T^{SPRT}, $\mathrm{T}_A^{SPRT} > \mathrm{T}_D^{SPRT} > \mathrm{T}_C^{SPRT}$. For the two test statistics, the performance of the amplitude-based test statistic is better than that of the test statistic based on the combined amplitude and phase and the test statistic based on the corrected phase offset. At the same time, for the test statisticT^{ILRT},$\mathrm{T}_C^{ILRT} > \mathrm{T}_D^{ILRT} > \mathrm{T}_A^{ILRT}$. For the test statistics T^{ISPRT},$\mathrm{T}_C^{ISPRT} > \mathrm{T}_D^{ISPRT} > \mathrm{T}_A^{ISPRT}$. Therefore, the performance of the test statistic based on the combined amplitude and phase is better than that of the amplitude-based test statistic and the test statistic based on the corrected phase offset. For example, when the *far* is 4.812%, the *dr* of the test statistic $\mathrm{T}_C^{ILRT}$is 80.57%, while the *dr* of the test statistic $\mathrm{T}_C^{LRT}$is only 48.85%, and when the *dr* of the test statisticT_C^{ILRT} reaches 80.57%, its *far* reaches 17.54%. When the *far* is 5.135%, the *dr* of the test statistic T_D^{ISPRT} is 83.94%, while the *dr* of the test statistic T_D^{SPRT} is only 35.68%. However, the performance of the test statistics $\mathrm{T}_A^{ILRT}$and the test statistic T_D^{ISPRT} in the amplitude-based test statistic drop significantly. For example, when the *far* is 4.938%, the *dr* of the test statistic T_A^{ISPRT} reaches 99.52%, while the *dr* of the test statistic T_A^{ISPRT} is only 42.40%.

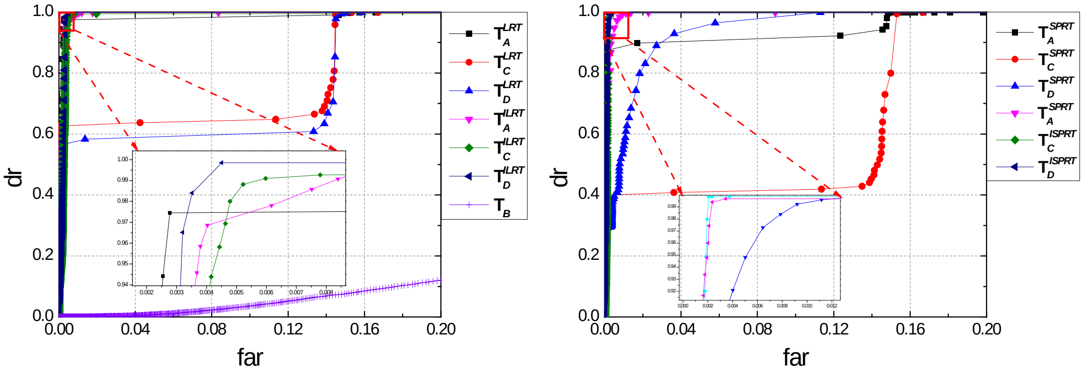


(a) (b)

Fig. 7. Performance in the machine shop.

3.3.2 Performance in the steamer plant

As shown in **Fig. 8**, in the steamer plant, the test statistics T_A^{LRT}, T_A^{ILRT}, T_C^{ILRT}, T_D^{ILRT}, T_A^{ISPRT}, T_C^{ISPRT}, and T_D^{ISPRT} all have excellent performance. For example, when the *far* is 0.2062%, the *dr* of the test statistic T_C^{ISPRT}can reach 99.85%. The reason is that there are fewer machines in this scenario, and the signals do not experience much reflection, which reduces the multipath effect. Therefore, these test statistics perform better in this scenario. For the amplitude-based test statistic, $\mathrm{T}_A^{ILRT} > \mathrm{T}_A^{ISPRT} > \mathrm{T}_A^{LRT} > \mathrm{T}_A^{SPRT}$. For the test statistic based on the combined amplitude and phase, $\mathrm{T}_C^{ISPRT} > \mathrm{T}_C^{ILRT} > \mathrm{T}_C^{LRT} > \mathrm{T}_C^{SPRT}$. For the test statistic based on the corrected phase offset, $\mathrm{T}_D^{ISPRT} > \mathrm{T}_D^{ILRT} > \mathrm{T}_D^{LRT} > \mathrm{T}_D^{SPRT}$. According to the comparisons, in the steamer plant, the detection performance of the test statistic $\mathrm{T}^{ILRT}$is better than that of the test statistic T^{LRT}, and the detection performance of the test statistic T^{ISPRT} is better than that of T^{SPRT}. For example, when the *far* is 0.4511%, the *dr* of the test statistic T_D^{ILRT} is 99.85%, while the *dr* of the test statistic T_D^{LRT} is only 56.89%. When the *far* is 1.336%, the *dr* of the test statistic T_A^{ISPRT} reaches 99.81%, while the *dr* of the test statistic T_A^{SPRT} is only 89.08%. Moreover, the performance of the test statistic T^{LRT} is better than that of the test statistic T^{SPRT}. For example, when the *far* is 1.713%, the *dr* of the test statistic T_A^{LRT} reaches 97.60%, while the *dr* of the test statistic T_A^{SPRT} is only 89.82%.

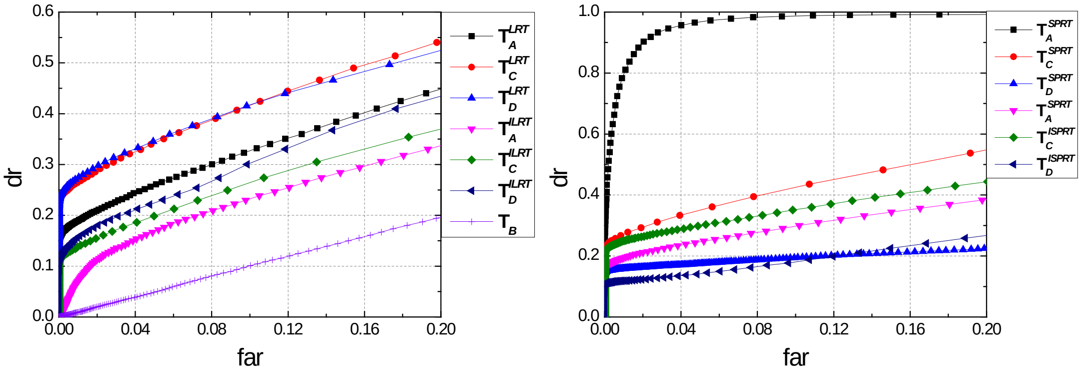


(a) (b)

Fig. 8. Performance in the steamer plant.

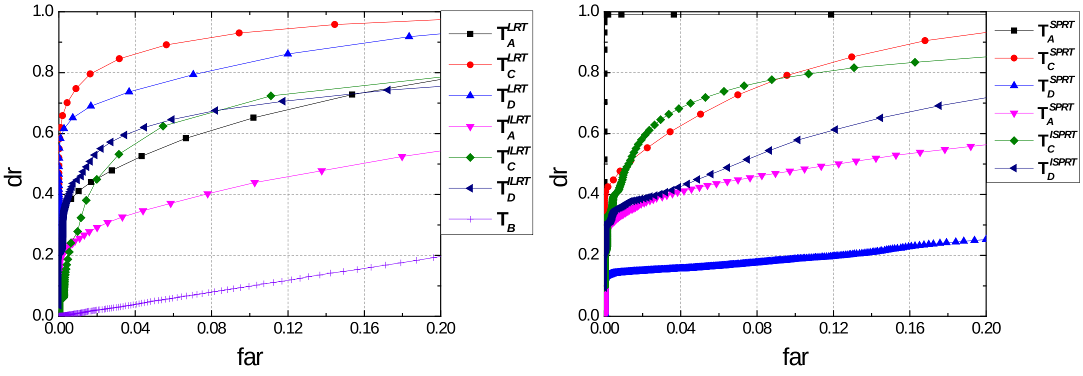
3.3.3 Performance in the automotive factory

Fig. 9 and **Fig. 10** show the performance of test statistics in the automotive factory. As shown in **Fig. 9**, the performance of the test statistic T_A^{SPRT} is the best in the outer loop. When the *far* of the test statistic T_A^{SPRT} is 4.722%, its *dr* can reach 96.53%. In this scenario, for the amplitude-based test statistic, $\mathrm{T}_A^{SPRT} > \mathrm{T}_A^{LRT} > \mathrm{T}_A^{ISPRT} > \mathrm{T}_A^{ILRT}$. For the test statistic based on the combined amplitude and phase, $\mathrm{T}_C^{SPRT} > \mathrm{T}_C^{LRT} > \mathrm{T}_C^{ISPRT} > \mathrm{T}_C^{ILRT}$. For the test statistic based on the corrected phase, $\mathrm{T}_D^{LRT} > \mathrm{T}_D^{ILRT} > \mathrm{T}_D^{SPRT} > \mathrm{T}_D^{ISPRT}$. From the above comparisons, we can see that the performance of the test statistic T^{ILRT} is worse than that of the test statistic T^{LRT}. For example, when the *far* is 4.831%, the *dr* of the test statistic T_C^{LRT} is 33.98%, while the *dr* of the test statistic T_C^{ILRT} is only 18.90%. The same is true for the test statistics T^{ISPRT} and the test statisticsT^{SPRT}. The detection performance of the test statistics T^{ISPRT} decreased compared with the test statistics T^{SPRT}. For example, when the *far* is 4.722%, the *dr* of the test statisticT_A^{SPRT} can reach 96.53%, while the *dr* of the test statistic T_A^{ISPRT} is only 24.30%.



(a) (b)

Fig. 9. Performance in the automotive factory (outer loop).



(a) (b)

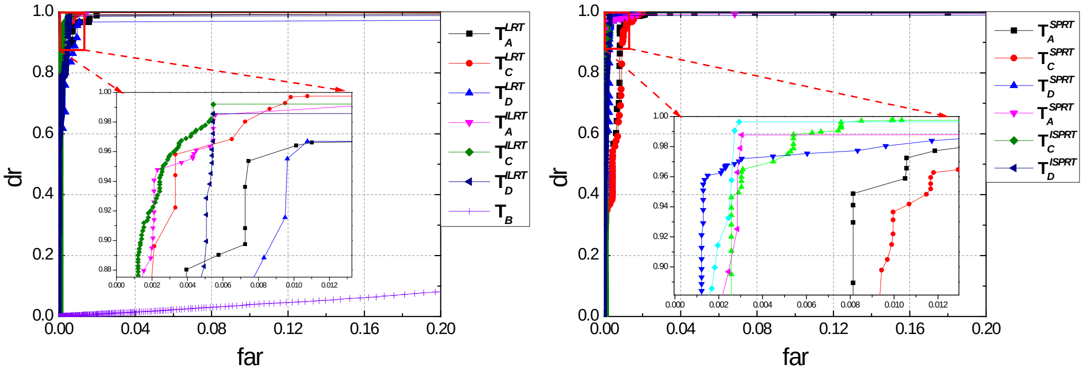
Fig. 10. Performance in the automotive factory (inner loop).

In the inner loop, as shown in **Fig. 10**, the test statistic T_A^{SPRT} has the best performance in this scenario, and its *dr* reaches 99.03% when the *far* is 0.2001%. In the scenario, for the amplitude-based test statistic, $\mathrm{T}_A^{SPRT} > \mathrm{T}_A^{LRT} > \mathrm{T}_A^{ISPRT} > \mathrm{T}_A^{ILRT}$. For the test statistic based on the combined amplitude and phase, $\mathrm{T}_C^{LRT} > \mathrm{T}_C^{ISPRT} > \mathrm{T}_C^{SPRT} > \mathrm{T}_C^{ILRT}$. For the test statistic based on the corrected phase offset, $\mathrm{T}_D^{LRT} > \mathrm{T}_D^{ILRT} > \mathrm{T}_D^{ISPRT} > \mathrm{T}_D^{SPRT}$. And the performance of the test statistics T^{LRT} is better than that of the test statistics T^{ILRT}. For example, when the *far* is 3.172%, the *dr* of the test statistic T_C^{LRT} reaches 84.56%, while the *dr* of the test statistic T_C^{ILRT} is only 53.34%.

Compare the inner loop with the outer loop in the automotive factory, the performance of test statistics in the inner loop scenario is slightly better than that in the outer loop scenario, because there are fewer interference sources in the inner loop.

3.3.4 Performance in the OATS

As shown in **Fig. 11**, in the OATS scenario, except for the test statistic T_B, other test statistics all have better performance. The wireless network environment of the OATS is similar to the traditional wireless network environment with fewer interference sources and multipath components, so the existing test statistics perform well in OATS.



(a) (b)

Fig. 11. Performance in the OATS.

From the above analysis, we can see that compared with other test statistics, the test statistic T_A^{SPRT} performs better in the industrial wireless network environment. It can be applied to the machine shop, the automotive factory, and the OATS. However, its performance in the steamer plant scene is slightly worse, and the highest *dr* can only reach 89% when *far* is 12%. Therefore, existing test statistics cannot be fully applied to various industrial wireless network environments. Moreover, existing test statistics need to traverse to determine the optimal threshold.

4. Machine learning Schemes Simulation and Performance Analysis

The channel characteristic-based PLA schemes rely on a preset threshold to achieve an detection rate or false alarm rate for a given system and wireless environment. Therefore, the choice of threshold has a significant impact on system performance. Besides, since the threshold depends on some factors, such as the channel statistics, the channel estimation error, terminal mobility, and the physical environment in which the device is located, the selection of the threshold is challenging.

The channel characteristic-based PLA can be regarded as a binary classification problem, and machine learning is an excellent method to deal with the binary classification problem. Therefore, the classification algorithm in machine learning can solve the challenge of threshold selection. Some scholars used machine learning to classify channel characteristics [42-47] and achieved good results. However, in these schemes, the authors only analyzed the applicability in the traditional wireless network environment, and they did not analyze the applicability in the industrial wireless network environment. Moreover, these machine learning schemes directly process the channel characteristic data, which may significantly burden wireless network terminals with limited resources due to a large amount of data. The test statistic schemes are performed on the hardware, so they have low complexity and low time delay, which can reduce the burden of the wireless terminal. Therefore, the combination of machine learning and test statistics can solve the problem of threshold selection, improve the authentication accuracy, and reduce complexity.

Literature [48] uses the combination of machine learning and statistics scheme to achieve good results in plant. In this section, we will test the effect of the combination of machine learning and statistics schemes in other scenarios.

4.1 Performance Metrics

A good authentication system can perfectly distinguish legal and illegal messages. Therefore, we use the authentication accuracy as the standard to measure each scheme in this section. The authentication accuracy can be expressed as:

$$AC = Pr\left(\mathcal{H}_1 \mid \mathcal{H}_1 \cup \mathcal{H}_0 \mid \mathcal{H}_0\right). \tag{23}$$

Where $Pr(\cdot \mid \cdot)$ represents the conditional probability.

4.2 Machine Learning Methods

After processing the test statistics, the NIST data set becomes a two-dimensional dataset. And the dataset has the characteristics of single feature and small magnitude. According to the characteristics of the dataset, we choose four machine learning classification algorithms, namely Gradient Boosted Decision Tree (GBDT), K-Nearest Neighbor (KNN), Support Vector Machines (SVM), and Logistic Regression (LR), which are good at solving classification problems.

4.2.1 Gradient Boosted Decision Tree (GBDT)

GBDT is a decision tree algorithm with high prediction accuracy, suitable for low-dimensional data, and can handle non-linear data. GBDT can flexibly handle various types of data, including continuous and discrete values. In the case of relatively short tuning time for GBDT, the predicted readiness rate can also be relatively high. GBDT consists of multiple decision trees, and the conclusions of all trees are added together to make the final answer. GBDT has two functions: the exponential loss function, the other is the logarithmic likelihood loss function. The latter is adopted in this paper.

4.2.2 Logistic Regression (LR)

Although LR is called regression, it is a classification model and is often used for two classifications. The computational cost of LR algorithm is not high, and it is easy to understand and implement. LR is very efficient in terms of time and memory requirements. It can be applied to distributed data, and it also has online algorithm implementation, which uses less resources to process large data. LR is very robust to small noise in the data, and will not be particularly affected by slight multicollinearity. The essence of LR is to assume that the data obey this distribution, and then use maximum likelihood estimation to estimate the parameters. Logistic regression has two classification methods: one-vs-rest and many-vs-many. The former is adopted in this paper.

4.2.3 *K*-Nearest Neighbor (KNN)

KNN is a theoretically mature method and one of the simplest machine learning algorithms. KNN does not show training, unlike other supervised algorithms that use the training set to train a model (that is, fit a function), and then use it to classify the validation set or test set. It just saves the samples and processes them when the test data is received, so the KNN training time is zero. The idea of this method is very simple and intuitive. If most of the K similar samples belong to a category in the eigenspace, then the sample also belongs to that category. This method only determines the category of the sample to be divided according to the category of the nearest one or several samples.

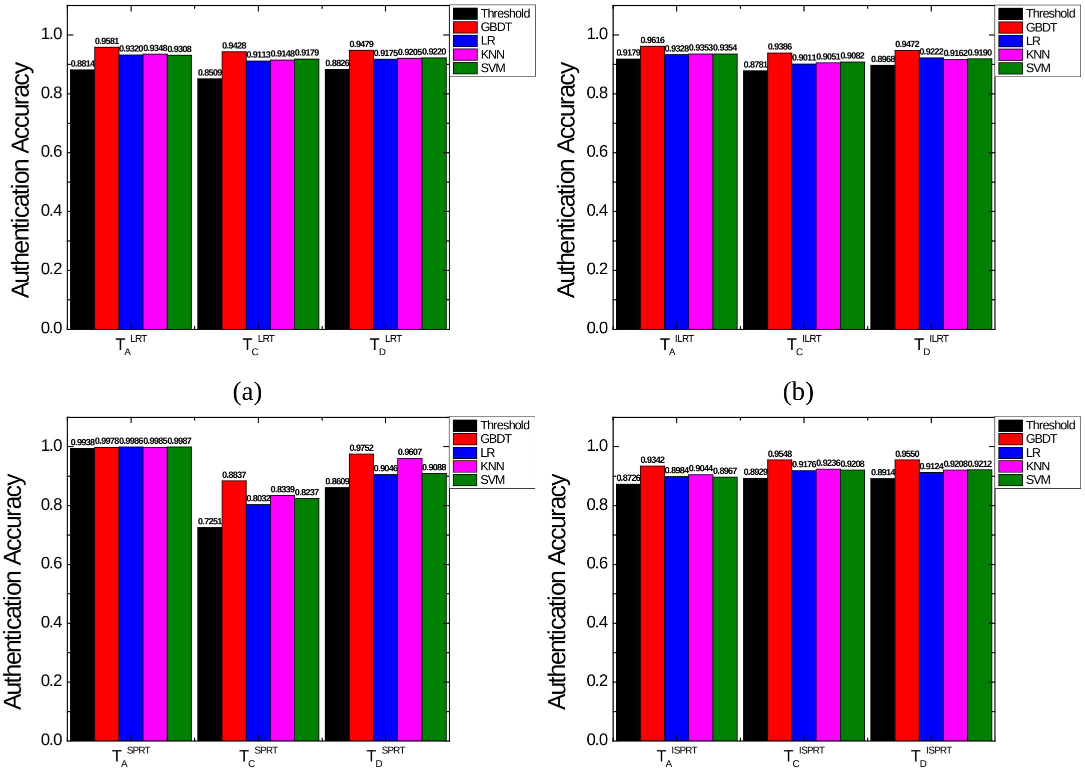
4.2.4 Support Vector Machines (SVM)

SVM is a two-classification model. It has good performance on small samples, nonlinearity, high dimensionality and local minima. Its basic model is a linear classifier with the largest interval defined in the feature space. However, SVM has kernel skills, which make it a substantial non-linear classifier. The learning strategy of SVM is interval maximization, which can be formalized as a problem to solve convex quadratic programming. The learning algorithm of SVM is the optimal algorithm for solving convex quadratic programming. SVM kernel functions include Linear kernel function, Polynomial kernel function, Radial Basis kernel function, Gaussian kernel function. The Gaussian kernel function is adopted in this paper.

4.3 Simulation Results and Analysis

4.3.1 Performance in the machine shop

Fig. 12 shows the performance of the four machine learning methods in the machine shop scenario. In the test statistics T^{LRT}, as shown in Figure (a), the GBDT+ T_A^{LRT} scheme has the best performance, and its authentication accuracy rate can reach 95.81%. The four machine learning methods have a good improvement for the test statistics T^{LRT}. For example, the authentication accuracy of the test statistic T_C^{LRT} is 85.09%, while the authentication accuracy of the GBDT+T_C^{LRT} scheme increases by 9.18%, and its authentication accuracy can reach 94.28%. In the test statistics T^{ILRT}, as shown in Figure (b), the GBDT+ T_A^{ILRT} scheme has the best performance, and its authentication accuracy can reach 96.16%. The four machine learning methods have a good improvement for the test statistics T^{ILRT}. For example, the authentication accuracy of the test statistic T_C^{ILRT} is 87.81%, while the authentication accuracy of the GBDT +T_C^{ILRT} scheme has increased by 6.05%, and its authentication accuracy can reach 93.86%. In the test statistics T^{SPRT}, as shown in Figure (c), the SVM+ T_A^{SPRT} scheme has the best performance, and its authentication accuracy rate can reach 99.87%. The four machine learning methods have a good improvement for the test statistic T^{SPRT}. For example, the authentication accuracy of the test statistics T_D^{SPRT} is 72.51%, while the authentication accuracy of the GBDT +T_D^{SPRT} scheme increases by 25.01%, and its authentication accuracy can reach 97.52%. In the test statistics T^{ISPRT}, as shown in Figure (d), the GBDT + T_D^{ISPRT} scheme has the best performance, and its authentication accuracy rate can reach 95.50%. The four machine learning methods have a good improvement for the test statistics T^{ISPRT}. For example, the authentication accuracy of the test statistic T_C^{ISPRT} is 89.29%, while the authentication accuracy of the GBDT+T_C^{ISPRT} scheme increases by 6.19%, and its authentication accuracy can reach 95.48%. From the above analysis, it can be seen that in the machine shop scenario, the machine learning improves the authentication accuracy of the test statistics schemes and solves the challenge of threshold selection.



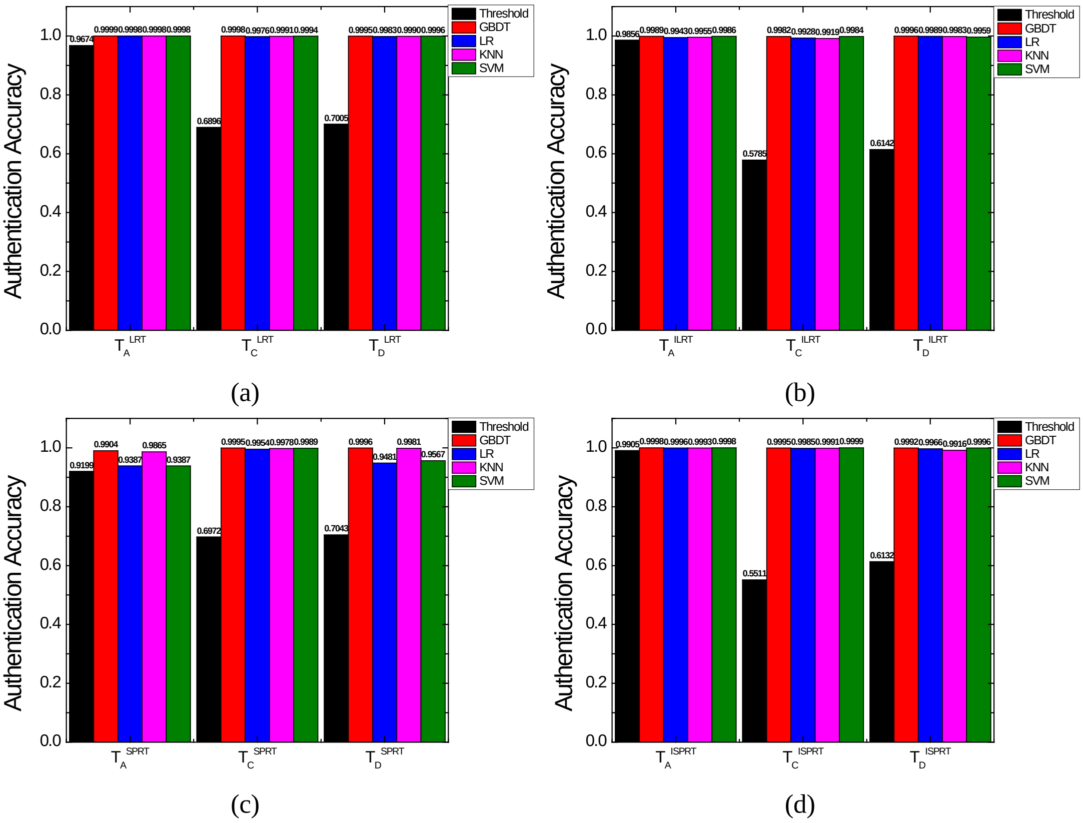
(a) (b)

(c) (d)

Fig. 12. Authentication accuracy in the machine shop.

4.3.2 Performance in the steamer plant

Fig. 13 shows the performance of the four machine learning methods in the steamer plant scenario. In the test statistics T^{LRT}, as shown in Figure (a), the GBDT+ T_A^{LRT} scheme has the best performance, and its authentication accuracy can reach 99.99%. The four machine learning methods have a good improvement for the test statistics T^{LRT}. For example, the authentication accuracy of the test statistic T_C^{LRT} is 68.96%, while the authentication accuracy of the GBDT+T_C^{LRT} scheme increases by 31.02%, and its authentication accuracy can reach 99.98%. In the test statistics $\mathbf{T}^{\boldsymbol{ILRT}}$, as shown in Figure (b), the GBDT+ $\mathbf{T}_{\boldsymbol{A}}^{\boldsymbol{ILRT}}$ scheme has the best performance, and its authentication accuracy can reach 99.89%. The four machine learning methods have a good improvement for the test statistics $\mathbf{T}^{\boldsymbol{ILRT}}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_{\boldsymbol{C}}^{\boldsymbol{ILRT}}$ is 57.85%, while the authentication accuracy of the GBDT+$\mathbf{T}_{\boldsymbol{C}}^{\boldsymbol{ILRT}}$scheme increases by 41.97%, and its authentication accuracy can reach 99.82%. In the test statistics $\mathbf{T}^{\boldsymbol{SPRT}}$, as shown in Figure (c), the GBDT+ $\mathbf{T}_{\boldsymbol{D}}^{\boldsymbol{SPRT}}$ scheme has the best performance, and its authentication accuracy can reach 99.98%. The four machine learning methods have a good improvement for the test statistics $\mathbf{T}^{\boldsymbol{SPRT}}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_{\boldsymbol{C}}^{\boldsymbol{SPRT}}$ is 69.72%, while the authentication accuracy of the GBDT +$\mathbf{T}_{\boldsymbol{C}}^{\boldsymbol{SPRT}}$ scheme increases by 30.23%, and its authentication accuracy can reach 99.95%. In the test statistics $\mathbf{T}^{\boldsymbol{ISPRT}}$, as shown in Figure (d), the SVM+ $\mathbf{T}_C^{ISPRT}$ scheme has the best performance, and its authentication accuracy can reach 99.99%. The four machine learning methods have a good improvement for the test statistics $\mathbf{T}^{ISPRT}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_D^{ISPRT}$ is 61.32%, while the authentication accuracy of the GBDT + $\mathbf{T}_D^{ISPRT}$ scheme increases by 38.60%, and its authentication accuracy can reach 99.92%. From the above analysis, it can be seen that in the steamer plant scenario, the machine learning method improves the authentication accuracy of the test statistics schemes and solves the challenge of threshold selection.



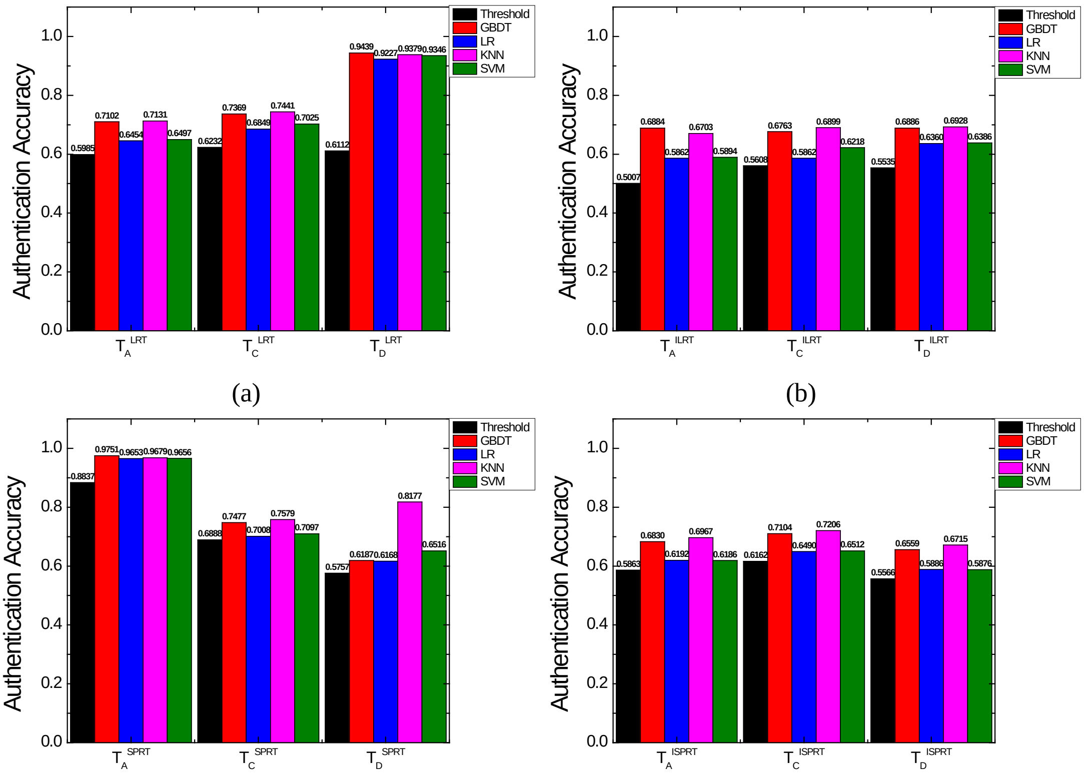
(a) (b)

(c) (d)

Fig. 13. Authentication accuracy in the steamer plant.

4.3.3 Performance in the automotive factory

Fig. 14 shows the performance of the four machine learning methods in the automotive plant scenario (outer loop). In the test statistics T^{LRT}, as shown in Figure (a), the GBDT+ T_D^{LRT} scheme has the best performance, and its authentication accuracy can reach 94.39%. The four machine learning methods have a good improvement for the test statistics T^{LRT}. For example, the authentication accuracy of the test statistic T_C^{LRT} is 62.32%, while the authentication accuracy of the GBDT +T_C^{LRT} scheme increases by 11.37%, and its authentication accuracy can reach 73.69%. In the test statistics T^{ILRT}, as shown in Figure (b), the KNN+ T_D^{ILRT} scheme has the best performance, and its authentication accuracy can reach 69.28%. The four machine learning methods have a good improvement for the test statistics T^{ILRT}. For example, the authentication accuracy of the test statistic T_C^{ILRT} is 56.08%, while the authentication accuracy of the GBDT+T_C^{ILRT}scheme has increases by 14.96%, and its authentication accuracy can reach 71.04%. In the test statistics T^{SPRT}, as shown in Figure (c), the GBDT+ T_A^{SPRT} scheme has the best performance, and its authentication accuracy can reach 97.51%. The four machine learning methods have a good improvement for the test statistic T^{SPRT}. For example, the authentication accuracy of the test statistic T_C^{SPRT} is 68.88%, while the authentication accuracy of the GBDT+T_C^{SPRT} scheme has increased by 5.89%, and its authentication accuracy can reach 74.77%. In the test statistics T^{ISPRT}, as shown in Figure (d), the KNN+ T_C^{ISPRT} scheme has the best performance, and its authentication accuracy can reach 72.06%. The four machine learning methods have a good improvement for the test statistics T^{ISPRT}. For example, the authentication accuracy of the test statistic T_D^{ISPRT} is 55.66%, while the authentication accuracy of the GBDT+ T_D^{ISPRT} scheme increases by 9.93%, and its authentication accuracy can reach 65.59%. From the above analysis, it can be seen that in the automotive plant scenario (outer loop), the machine learning method improves the authentication accuracy of the test statistics schemes and solves the challenge of threshold selection.

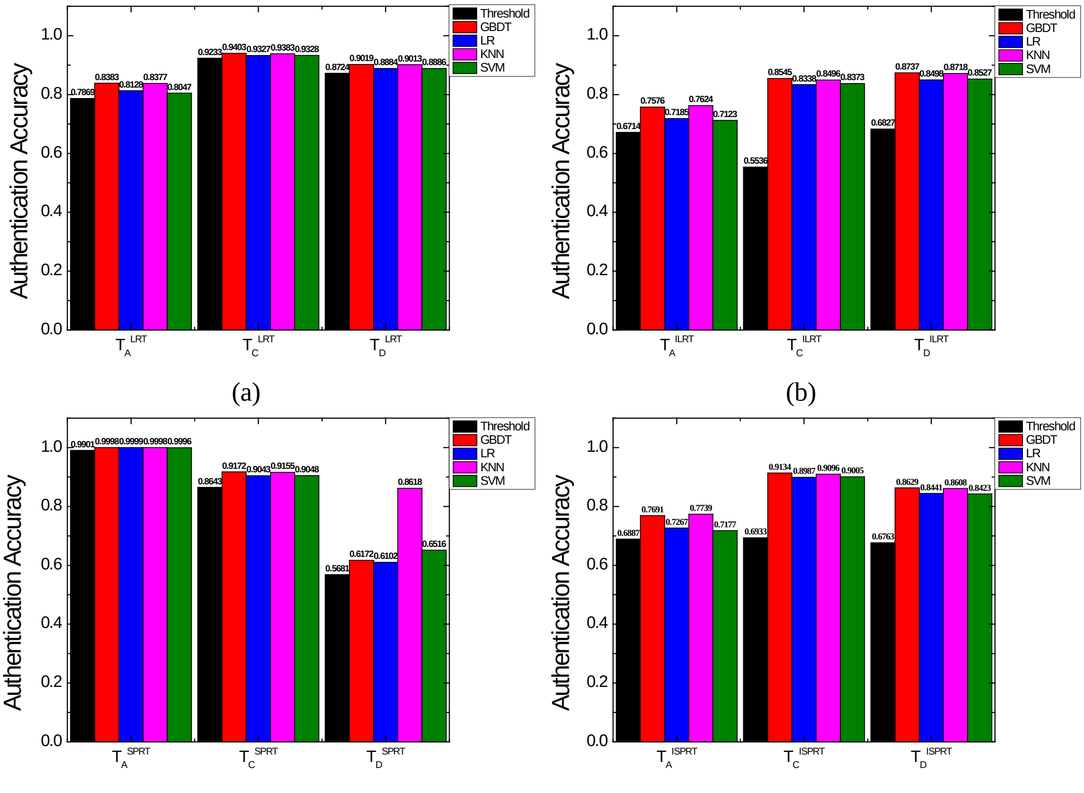


(a) (b)

(c) (d)

Fig. 14. Authentication accuracy in the plant (outer loop).

Fig. 15 shows the performance of the four machine learning methods in the automotive plant scenario (inner loop). In the test statistics $\mathbf{T}^{LRT}$, as shown in Figure (a), the GBDT+ $\mathbf{T}_C^{LRT}$ scheme has the best performance, and its authentication accuracy can reach 94.03%. The four machine learning methods have a good improvement for the test statistics $\mathbf{T}^{LRT}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_A^{LRT}$ is 78.69%, while the authentication accuracy of the GBDT +$\mathbf{T}_{A}^{LRT}$ scheme increases by 5.14%, and its authentication accuracy can reach 83.83%. In the test statistics $\mathbf{T}^{ILRT}$, as shown in Figure (b), the GBDT+ $\mathbf{T}_{D}^{ILRT}$ scheme has the best performance, and its authentication accuracy can reach 87.37%. The four machine learning methods have a good improvement for the test statistics $\mathbf{T}^{ILRT}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_{C}^{ILRT}$ is 55.36%, while the authentication accuracy of the GBDT+$\mathbf{T}_{C}^{ILRT}$scheme increases by 30.09%, and its authentication accuracy can reach 85.45%. In the test statistics $\mathbf{T}^{SPRT}$, as shown in Figure (c), the LR+ $\mathbf{T}_{A}^{SPRT}$ scheme has the best performance, and its authentication accuracy can reach 99.99%. The four machine learning methods have a good improvement for the test statistic $\mathbf{T}^{SPRT}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_{C}^{SPRT}$ is 88.43%, while the authentication accuracy of the GBDT+$\mathbf{T}_{C}^{SPRT}$ scheme increases by 3.29%, and its authentication accuracy can reach 91.72%. In the test statistics $\mathbf{T}^{ISPRT}$, as shown in Figure (d), the GBDT+ $\mathbf{T}_{C}^{ISPRT}$ scheme has the best performance, and its authentication accuracy can reach 91.34%. The four machine learning methods have a good improvement for the test statistics $\mathbf{T}^{ISPRT}$. For example, the authentication accuracy of the test statistic $\mathbf{T}_{D}^{ISPRT}$ is 67.83%, while the authentication accuracy of the GBDT + $\mathbf{T}_{D}^{ISPRT}$ scheme increases by 18.46%, and its authentication accuracy can reach 86.29%. From the above analysis, it can be seen that in the automotive plant scenario (inner loop), the machine learning method improves the authentication accuracy of the test statistics schemes and solves the challenge of threshold selection.



(a)

(b)

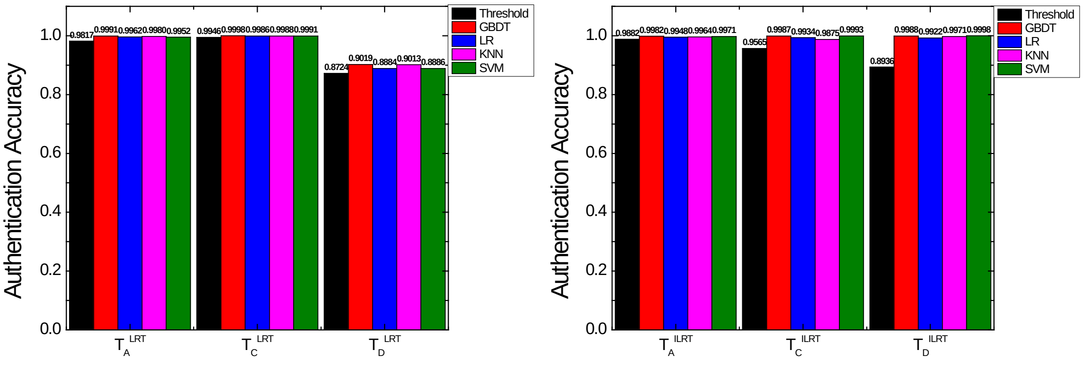
(c)

(d)

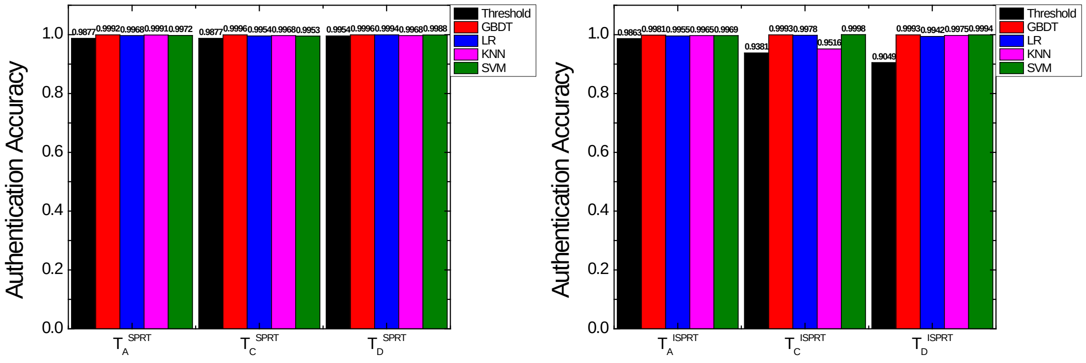
Fig. 15. Authentication accuracy in the plant internal (inner loop).

4.3.4 Performance in the OATS

Fig. 16 shows the performance of the four machine learning methods in the OATS scenario. In the test statistics T^{LRT}, as shown in Figure (a), the GBDT+ T_C^{LRT} scheme has the best performance, and its authentication accuracy can reach 99.98%. The four machine learning methods have a good improvement for the test statistics T^{LRT} . For example, the authentication accuracy of the test statistic T_D^{LRT} is 87.24%, while the authentication accuracy of the GBDT+T_A^{LRT} scheme increases by 2.95%, and its authentication accuracy can reach 90.19%. In the test statistics T^{ILRT}, as shown in Figure (b), the GBDT+ T_D^{ILRT} scheme has the best performance, and its authentication accuracy can reach 99.88%. The four machine learning methods have a good improvement for the test statistics T^{ILRT}. For example, the authentication accuracy of the test statistic T_C^{ILRT} is 95.65%, while the authentication accuracy of the GBDT+T_C^{ILRT}scheme increases by 4.22%, and its authentication accuracy can reach 99.87%. In the test statistics T^{SPRT}, as shown in Figure (c), the GBDT+ T_C^{SPRT} scheme has the best performance, and its authentication accuracy can reach 99.96%. The four machine learning methods have a good improvement for the test statistic T^{SPRT}. For example, the authentication accuracy of the test statistic T_A^{SPRT} is 98.77%, while the authentication accuracy of the GBDT +T_C^{SPRT} scheme increases by 1.15%, and its authentication accuracy can reach 99.92%. In the test statistics T^{ISPRT}, as shown in Figure (d), the SVM+ T_C^{ISPRT} scheme has the best performance, and its authentication accuracy can reach 99.98%. The four machine learning methods have a good improvement for the test statistics T^{ISPRT}. For example, the authentication accuracy of the test statistic T_D^{ISPRT} is 90.49%, while the authentication accuracy of the GBDT + T_D^{ISPRT} scheme increases by 9.44%, and its authentication accuracy can reach 99.93%. From the above analysis, it can be seen that in the OATS scenario, the machine learning method improves the authentication accuracy of the test statistics schemes and solves the challenge of threshold selection.



(a) (b)



(c) (d)

Fig. 16. Authentication accuracy in the OATS.

From the above analysis, machine learning improves the authentication accuracy of the test statistics schemes. The combination of machine learning and statistics schemes can achieve high authentication accuracy without manually selecting the optimal threshold. Based on the above analysis, we believe that the combination of machine learning and test statistics will guide future research on the channel characteristics-based PLA in the industrial wireless network environment.

5. Conclusion

In this paper, we evaluated the performance of several channel characteristics-based authentication schemes to determine their potential for deployment in industrial wireless networks. The simulation results suggested that these test statistics cannot be easily applied to all industrial wireless network scenarios. However, we revealed that the channel characteristics -based PLA can potentially be utilized in future industrial wireless network deployments. The findings also highlight the need for a new PLA solution based on channel characteristics, for a broad range of industrial wireless networks. Thus, we recommend combining machine learning and multiple test statistics to perform identity authentication in industrial wireless networks. We conducted a large number of experiments using four machine learning methods. The experimental results show that the combination of machine learning and multiple test statistics scheme significantly improves the authentication accuracy and solves the challenge of threshold selection. Therefore, compared with the test statistics schemes, the machine learning scheme is more suitable for the industrial wireless network environment. Although the machine learning scheme presents good performance, this paper only focuses on static and low-speed moving environment. The physical layer authentication scheme in high-speed moving environment is a subject that researchers in the field of information security need to further study. At the same time, the machine learning scheme is a kind of supervised learning, which can only identify the samples that have been learned, and cannot give a judgment on the samples that have not been learned. Therefore, the combination of unsupervised learning and certification technology needs to be studied in the future.

References

[1] X. Liang, K. Zhang, X. Shen and X. Lin, “Security and privacy in mobile social networks: challenges and solutions,” *IEEE Wireless Commun. Mag.*, vol. 21, no. 1, pp. 33-41, Feb. 2014. Article (CrossRef Link)

[2] J. Cao, M. Ma, H. Li, Y. Zhang and Z. Luo, “A Survey on Security Aspects for LTE and LTE-A Networks,” *IEEE Commun. Surv. Tut.*, vol. 16, no. 1, pp. 283-302, First Quarter 2014. Article (CrossRef Link)

[3] 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. 2, pp. 251-264, Feb. 2018. Article (CrossRef Link)

[4] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,” in *Proc. of IEEE Int. Conf. Commun. (ICC)*, Glasgow, pp. 4646-4651, 2007. Article (CrossRef Link)

[5] 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, July 2017. Article (CrossRef Link)

[6] W. C. Jakes, *Microwave Mobile Communications*, Hoboken, NJ, USA: Wiley, 1994.

[7] F. He, H. Man, D. Kivanc and B. McNair, “EPSON: Enhanced Physical Security in OFDM Networks,” in *Proc. of IEEE Int. Conf. Commun. (ICC)*, Dresden, pp. 1-5, 2009. Article (CrossRef Link)

[8] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, “A Physical-Layer Technique to Enhance Authentication for Mobile Terminals,” in *Proc. of IEEE Int. Conf. Commun. (ICC)*, Beijing, pp. 1520-1524, 2008. Article (CrossRef Link)

[9] H. Wen, Y.F. Wang, X.P. Zhu, L. Zhou, “Physical Layer Assist Authentication Technique for Smart Meter System,” *IET Communications*, vol. 7, pp. 189-197, Feb. 2013. Article (CrossRef Link)

[10] T. Ma, “Research on lightweight physical layer assist authentication technique in smart grid,” M.S. thesis, Nat. Key Lab. Sci. Technol. Commun., Univ. Electron. Sci. Technol. China, Chengdu, China, Jul. 2015.

[11] 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, July 2008. Article (CrossRef Link)

[12] L. Xiao, T. Chen, G. Han, W. Zhuang and L. Sun, “Game Theoretic Study on Channel-Based Authentication in MIMO Systems,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7474-7484, Aug. 2017. Article (CrossRef Link)

[13] L. Xiao, X. Wan and Z. Han, “PHY-Layer Authentication With Multiple Landmarks With Reduced Overhead,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676-1687, March 2018. Article (CrossRef Link)

[14] 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. Article (CrossRef Link)

[15] F. Pan, Z. Pang, M. Xiao, H. Wen and R. Liao, “Clone Detection Based on Physical Layer Reputation for Proximity Service,” *IEEE Access*, vol. 7, pp. 3948-3957, 2019. Article (CrossRef Link)

[16] X. Wu and Z. Yang, "Physical-Layer Authentication for Multi-Carrier Transmission," *IEEE Communications Letters*, vol. 19, no. 1, pp. 74-77, Jan. 2015. Article (CrossRef Link)

[17] D. Shan, K. Zeng, W. Xiang, P. Richardson and Y. Dong, "PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1817-1827, Sep. 2013. Article (CrossRef Link)

[18] J. Choi, "A Coding Approach With Key-Channel Randomization for Physical-Layer Authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 175-185, Jan. 2019. Article (CrossRef Link)

[19] 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. Article (CrossRef Link)

[20] X. Du, D. Shan, K. Zeng and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proc. of IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Toronto, ON, pp. 1276-1284, 2014. Article (CrossRef Link)

[21] S. Tomasin, "Analysis of Channel-Based User Authentication by Key-Less and Key-Based Approaches," *IEEE Trans. Wireless Commun*, vol. 17, no. 9, pp. 5700-5712, Sept. 2018. Article (CrossRef Link)

[22] C. Pei, N. Zhang, X. S. Shen and J. W. Mark, "Channel-based physical layer authentication," in *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*, pp. 4114-4119, Dec. 2014. Article (CrossRef Link)

[23] F. Pan, H. Wen, R. Liao, Y. Jang and A.Xu, "Physical layer authentication based on channel information and machine learning," in *Proc. of IEEE Conf. Commun. Netw. Secur. (CNS)*, pp. 364-365, Oct. 2017. Article (CrossRef Link)

[24] A. Weinand, M. Karrenbauer, J. Lianghai and H. D. Schotten, "Physical Layer Authentication for Mission Critical Machine Type Communication Using Gaussian Mixture Model Based Clustering," in *Proc. of 2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, pp. 1-5, 2017. Article (CrossRef Link)

[25] H. Wen, P. -. Ho, C. Qi and G. Gong, "Physical layer assisted authentication for distributed ad hoc wireless sensor networks," *IET Information Security*, vol. 4, no. 4, pp. 390-396, Dec. 2010. Article (CrossRef Link)

[26] S. Van Vaerenbergh, Ó. González, J. Vía and I. Santamaría, "Physical layer authentication based on channel response tracking using Gaussian processes," in *Proc. of 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, pp. 2410-2414, 2014. Article (CrossRef Link)

[27] Y. Chen, A. Xu, Y. Jiang and Y. Zhang, "A Data Authentication Method Based on Vector Projection for Industrial Edge Computing System," *DEStech Transactions on Computer Science and Engineering*, 2019. Article (CrossRef Link)

[28] P. Hao, X. Wang and W. Shen, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication," *IEEE Access*, vol. 6, pp. 42279-42293, 2018. Article (CrossRef Link)

[29] Y. Shi and M. A. Jensen, "Improved Radiometric Identification of Wireless Devices Using MIMO Transmission," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1346-1354, Dec. 2011. Article (CrossRef Link)

[30] D. A. Knox and T. Kunz, "Secure Authentication in Wireless Sensor Networks Using RF Fingerprints," in *Proc. of 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Shanghai, pp. 230-237, 2008. Article (CrossRef Link)

[31] V. Brik, S. Banerjee, M. Gruteser and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. of the 14th ACM International Conference on Mobile Computing and Networking*, pp. 116-127, 2008. Article (CrossRef Link)

[32] W. Hou, X. Wang and J. Chouinard, "Physical Layer Authentication in OFDM Systems based on Hypothesis Testing of CFO Estimates," in *Proc. of 2012 IEEE International Conference on Communications (ICC)*, Ottawa, ON, pp. 3559-3563, 2012. Article (CrossRef Link)

[33] W. Hou, X. Wang, J. 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. Article (CrossRef Link)

[34] O. Ureten and N. Serinken, "Wireless Security Through RF Fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27-33, Winter 2007. Article (CrossRef Link)

[35] P. L. Yu, G. Verma and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 48-53, Jun. 2015.
[36] G. Verma, P. Yu and B. M. Sadler, "Physical Layer Authentication via Fingerprint Embedding Using Software-Defined Radios," *IEEE Access*, vol. 3, pp. 81-88, 2015. Article (CrossRef Link)
[37] N. Xie and S. Zhang, "Blind Authentication at the Physical Layer Under Time-Varying Fading Channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1465-1479, Jul. 2018. Article (CrossRef Link)
[38] X. Wang, P. Hao and L. Hanzo, "Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152-158, Jun. 2016. Article (CrossRef Link)
[39] M. Luvisotto, Z. Pang and D. Dzung, "Ultra High Performance Wireless Control for Critical Applications: Challenges and Directions," *IEEE Trans Ind. Informat.*, vol. 13, no. 3, pp. 1448-1459, June 2017. Article (CrossRef Link)
[40] M. Luvisotto, Z. Pang, D. Dzung, M. Zhan and X. Jiang, "Physical Layer Design of High-Performance Wireless Transmission for Critical Control Applications," *IEEE Trans Ind. Informat.*, vol. 13, no. 6, pp. 2844-2854, Dec. 2017. Article (CrossRef Link)
[41] R. Candell, K. A. Remley, N. Moayeri, "Radio frequency measurements for selected manufacturing and industrial environments," *NIST Tech. Rep. 1951*, Jul. 2016. Article (CrossRef Link)
[42] Q. Wang, H. Li, Zh. Chen, D. Zhao and Sh. Ye, "Supervised and semi-supervised deep neural networks for CSI-based authentication," *ArXiv*, Jul. 2018. [Online]. Available: https://arxiv.org/abs/1807.09469
[43] R. Liao, H. Wen, J. Wu and F. Pan, "Deep-Learning-Based Physical Layer Authentication for Industrial Wireless Sensor Networks," *Sensors*, May 2019. Article (CrossRef Link)
[44] R. Liao, H. Wen, F. Pan, H. Song, A. Xu and Y. Jiang, "A Novel Physical Layer Authentication Method with Convolutional Neural Network," in *Proc. of 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, Dalian, China, pp. 231-235, 2019. Article (CrossRef Link)
[45] F. J. Liu, X. Wang and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. of IEEE Int. Conf. Commun. (ICC)*, Budapest, pp. 4724-4728, 2013. Article (CrossRef Link)
[46] G. Oligeri, S. Raponi, S. Sciancalepore, R. Pietro, "PAST-AI: Physical-layer Authentication of Satellite Transmitters via Deep Learning," *ArXiv*, Oct. 2020. [Online]. Available: https://arxiv.org/abs/2010.05470v1
[47] S. Yan, X. Wang, L. Xu, "Rollout algorithm for light-weight physical-layer authentication in cognitive radio networks," *IET Communications*, vol. 14, no. 18, pp. 3128-3134, Nov. 2020. Article (CrossRef Link)
[48] F. Pan, Z. Pang, H. Wen and M. Luvisotto, "Threshold-Free Physical Layer Authentication Based on Machine Learning for Industrial Wireless CPS," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6481-6491, Dec. 2019. Article (CrossRef Link)
[49] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006. Article (CrossRef Link)
[50] J. Brown, X. Du and K. Nygard, "An Efficient Public-Key-Based Heterogeneous Sensor Network Key Distribution Scheme," in *Proc. of IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference, Washington,* DC, USA, pp. 991-995, 2007. Article (CrossRef Link)
[51] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247-260, Feb. 2006. Article (CrossRef Link)

Qiuhua Wang received her B.S. and M.S. degrees in communication engineering from Liaoning Technical University, Fuxin, China, in 2000 and 2003, respectively. She received her Ph.D. degree in communications and information systems from Zhejiang University, Hangzhou, China, in 2013. Now, she is an Associate Professor of the School of Cyberspace, Hangzhou Dianzi University. Her current research interests include network security, security issues in wireless networks, key management and physical layer security, etc.

Mingyang Kang received the B.S. degree in Metal Material Engineering from North University of China, Taiyuan, China, in 2017. He is currently pursuing the master degree in the School of Cyberspace, Hangzhou Dianzi University. His research interests include network security, physical layer security, information security, etc.

Lifeng Yuan received the B.S. degree in Computer Science and Technology from Ningbo University in 2006. He received the M.S. degree in 2009 and his Ph.D in 2017,both from the Dalian University of Technology. Since 2017, he has been a lecture at Hangzhou Dianzi University. His current research interests include secret sharing and information hiding.

Yunlu Wang received the B.S. degree in Electronic Science and Technology from University Of Science And Technology Of China in 2003. She received the Ph.D degrdd in 2008 from the University Of Science And Technology Of China. Since 2008, she has been a lecture at Hangzhou Dianzi University. Her current research interests include machine learning and information hiding.

Gongxun Miao received the B.S. degree in Computer Science and Technology from Shandong Institute of management in 2012. He received the M.S. degree from Shandong University for Science& Technology in 2018. He is currently a member of the Standardization Technical Committee Information in Shandong Province and the Deputy Chief Engineer of Zhongfu Information Co., Ltd. He is mainly engaged in the technical research and development in the field of information security.

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is also the recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP Journal on Wireless Communications and Networking (JWCN) Best Paper Award, Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, Inscrypt 2019 Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is a Fellow of the Australian Computer Society, an IEEE Senior Member, and Co-Chair of IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group.