IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 25, 2021, accepted June 3, 2021, date of publication June 8, 2021, date of current version June 21, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3087508

A Tag-Based PHY-Layer Authentication Scheme Without Key Distribution

YONGLI AN, SHIKANG ZHANG, AND ZHANLIN JI
College of Information Engineering, North China University of Science and Technology, Tangshan 063210, China

Corresponding author: Zhanlin Ji (zhanlin.ji@ncst.edu.cn)

This work was supported in part by the Science and Technology Major Project of the Science and Technology Ministry of China under Grant 2017YFE0135700, in part by the High Level Talent Support Project of Hebei Province under Grant A201903011, and in part by the Natural Science Foundation of Hebei Province under Grant F2018209358.

ABSTRACT Authentication is the process of confirming the legal identity of communicating entities, and it is the first line of defense for security communication. Most of the existing tag-based physical layer security authentication (PLSA) requires distributing the shared keys in advance. In the large scale internet of things scenario, nodes frequently join and leave the wireless networks that cause the distribution and management of keys particularly difficult. This paper proposes a tag-based PLSA scheme, which utilizes channel characteristics instead of distributing keys to generate authentication tags. Specifically, based on watermarking mechanism, we design a fault-tolerant hash algorithm to couple the secret sequence and the message signal for authentication tags generation. The shared secret sequence is generated by legitimate nodes through channel probing. And the theories of information theory and composite hypothesis testing is employed to analyze the performance of system. The simulation results show that the agreement ratio of the generating shared secret sequence is as high as 96% in the case of high signal-to-noise ratio and low power tag embedding. In addition, performance analysis demonstrates the scheme can resist against multiple attacks, such as replay, jamming, tampering, and impersonation attack.

INDEX TERMS Authentication, wireless network, tag-based, hash algorithm, channel probing.

I. INTRODUCTION

With the vigorous development of the fifth generation (5G) communication technology, the data traffic of wireless networks has experienced unprecedented growth [1], [2], and the security authentication problems of wireless communication has become increasingly severe. The security of existing high layer authentication relies on the privacy of the distribution keys and computational complexity of the encryption algorithms, which cannot meet the requirements of wireless networks for dynamic, real-time, highspeed data service security authentication. Due to its broadcast nature, the wireless networks are more vulnerable to physical layer attacks than wired networks [3]. Physical layer security authentication (PLSA) cleverly utilizes the inherent unique characteristics of wireless media or equipment for providing secure transmission [4] that provides some brand new ideas and methods for wireless networks security authentication, so it has attracted widespread attention.

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

As the security enhancement of high layer authentication, PLSA has higher protocol compatibility, lower computational overhead, and lower delay, which make up for many disadvantages of high layer authentication [5]. According to different authentication methods, PLSA can be divided into two categories, one is to utilize the wireless channel fingerprints, e.g. channel state information (CSI), and radio frequency fingerprints directly for authentication; the other is through the use of hash function and signal processing technology to realize the joint processing and utilization of shared private keys and signal endogenous features, thereby improving the accuracy of legal device information authentication [6]–[9]. Among them, this type of schemes that realizes authentication through the joint design of keys and information transmission methods has better security performance and more extensive applications. However, these schemes are based on the premise of sharing a secret key which brings about key distribution and management problems. In the 5G large scale internet of things (IoT) scenario, it will support the connection of millions of terminals per square kilometer. The security authentication of these heterogeneous, low

power, and limited-computing terminals has brought a huge challenge to the certificate management agencies. The key distribution and management of massive IoT devices has become an urgent problem to be solved.

In recent years, using the fading characteristics, reciprocity, and location-specific of wireless channels to generate shared secret keys [10] has become a research hotspot. Key generation based on the channel reciprocity [11] can effectively alleviate the problems of key distribution and management. Unfortunately, channel-based key generation is susceptible to channel noise, which will result in a high bit disagreement ratio under low signal-to-noise ratio (SNR) [12], [13]. The inability to obtain a consistent shared secret key is intolerable to the authentication mechanisms, which utilize the hash functions to generate authentication codes.

To address the aforementioned problems, this paper proposes a tag-based PLSA scheme based on the channel key generation theories, which utilizes the channel characteristics between legitimate nodes to generate a shared secret sequence. And a fault-tolerant hash function is exploited to map the shared secret sequence and message signal into authentication tags. The main contributions of this paper are summarized as follows:

- We develop a tag-based PLSA framework without key distribution and management. Through wavelet denoising preprocessing, uniform quantization, Gray coding, etc., the shared secret sequence generated based on the channel characteristics has a higher bit agreement ratio.
- Due to the noisy characteristics of wireless communication, we design a fault-tolerant hash algorithm to generate authentication tags, i.e., the input values are similar, and the same or similar results can be obtained. Performance analysis results indicate that the hash function is simpler and practical value.
- By applying the theories of information theory and composite hypothesis testing, we analyze the authentication performance of our scheme under various attacking scenarios. In addition, we compare the security performance of this scheme with the cryptographic-based methods. Experimental results confirm that our scheme can effectively resist against a variety of attack methods. And under certain conditions, the attack success rate of this scheme is matter less than the lower bound of the cryptographic-based authentication methods.

The remainder of this paper is organized as follows. Section II presents background and reviews some related works. In Section III, we introduce the communication scenario of system. In Section IV, a tag-based PLSA scheme is proposed. Performance analysis and simulation results are discussed in Section V. Challenges and future research directions are provided in Section VI, while the conclusions are given in Section VII.

TABLE 1. Table of notations.

Notation	Significance
$[\bullet]$	Matrix operator
$f_e(\bullet)$	Modulation function
$\mathrm{E}\{\bullet\}$	Expectation operator
$\lvert\bullet\rvert^2$	Square of modulus
$(\bullet)^H$	Conjugate transpose operator
$(\bullet)^*$	Conjugate operator
$f_d(\bullet)$	Demodulation function
$\Phi(\bullet)$	Standard gaussian cumulative distribution function
χ_n^2	Chi-square random variable with n degrees of freedom
$\mathrm{P}\{\bullet\}$	Probability operator
$\mathrm{F}_{\chi_n^2}(\bullet)$	Right-tail probability function

A summary of the variables and notations frequently used in this paper is given in Table 1.

II. BACKGROUND AND RELATED WORK

In this section, we first give a brief review of CSI-based authentication and watermarking based authentication, which are two important mechanisms of the existing PLSA schemes. Then, some related works are reviewed.

A. CSI-BASED AND WATERMARKING BASED AUTHENTICATION

In non-cryptographic authentication, CSI-based authentication utilizes the specific characteristics of fading channels as signature [8]. An attacker located at a different location from the legitimate user cannot provide the same CSI as the legitimate user. CSI-based authentication has some unique advantages, e.g., rapid spatial decorrelation, reciprocity, and rich data dimensions [14]. Nevertheless, the difference of estimated channels between two legitimate nodes as well as background noise are out of control.

The watermarking authentication mechanism embeds flexible and controllable low-power tags into the message signal for simultaneous transmission, without extra bandwidth [9]. The receiver confirms the legitimacy of the user by comparing the authentication tag with the reference tag. This type of authentication mechanism considers a noise as an advantageous resource to achieve the authentication [15]. Channel noise can be utilized to protect authentication tags. Moreover, the authentication tag generated by using the shared key and the message signal can effectively resist against tampering attack on the message signal.

B. RELATED WORKS

While wireless channels bring some challenges to security authentication, it also brings many opportunities. In [16], the uniqueness and reciprocity of the wireless channel were

first converted into a shared random source to generate the shared keys. In [17], the theoretical upper limit of the maximum length for the generated keys was obtained based on the mutual information of the channel estimation between two legitimate nodes. The authors in [18]–[20] utilized the received signal strength, CSI, and angle of arrival for generating secret keys. The key generated by the channel measurements is often used to ensure the legitimacy of the user. Based on the CSI measurements, literatures [14], [21] designed security authentication schemes for WiFi devices and WiFi management frames respectively. A two dimensional quantization algorithm for channel impulse response (CIR) based PLSA was proposed in [22]. However, directly using CSI for authentication has a risk of eavesdropping and interception and cannot verify message integrity and origin.

In the digital signature protocol, the one-way hash function plays an important role. Literatures [7], [8] proposed an authentication scheme which adopts hash function and random interleaving channel coding to combine the CSI of legal nodes with the shared key. In the PLSA watermarking mechanism, hash functions are often used to generate authentication tags [23]. Recently, there have been more and more attacks on the large scale IoT [24], [25]. Based on the watermarking mechanism, the authors in [26]–[28] designed some PLSA schemes for large scale IoT scenarios, which utilize dynamic variable keys, asymmetric keys, weighted fractional Fourier transform (WFRFT) respectively for tag generation. In [29], a secret authenticated codebook framework was developed, and a low power hash-based message authentication code tag is superimposed on the message signal.

This work refers to many previous methods, and some summaries and comparisons are made in Table 2. From Table 2, we can see that our work combines the advantages of many related works. Compared with the existing watermarking mechanism, we utilize CSI to generate the shared secret sequence instead of key distribution in high layer. Moreover, our scheme can resist against multiple attacks.

III. SYSTEM MODEL

A. SCENARIO

As depicted by Fig. 1, Alice and Bob are two legitimate communication nodes, and both they expect to use the unique CSI and the message signal to generate consistent authentication tags. Alice superimposes the tag on the message signal to form a tagged signal and sends it to Bob; then Bob extracts the tag for authentication inspection to ensure the integrity of the sent messages and the legitimacy of the user. In addition, an adversary, called Adv, attempts to masquerade as a legitimate node to join the network, or tries to disrupt the normal authentication of the system. Due to the broadcast nature of wireless networks, as a powerful adversary, Adv can fully grasp the modulation, coding method, and authentication mechanism of the legitimate nodes. Usually, Adv cannot obtain the CSI between Alice and Bob, but Adv can forge the CSI through observation and learning.

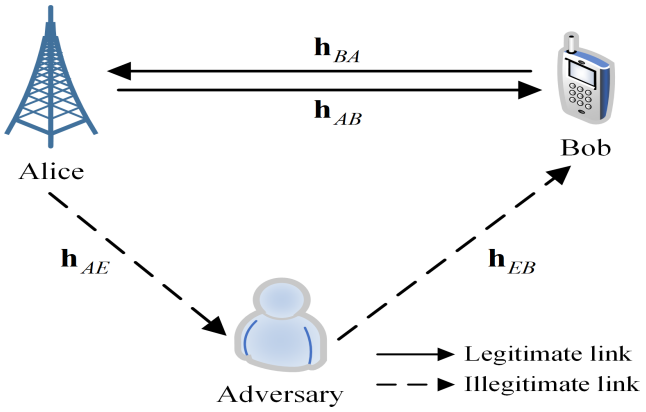


FIGURE 1. Communication scenario.

B. SIGNAL MODEL

Similar to [9], [27], we assume that the signal transmission is a block-by-block mode, and the input bit stream with length M is denoted by $\mathbf{b} = [b_1, \ldots, b_M]$. Then we modulate and code the input bits with a function $\mathbf{m} = f_e(\mathbf{b})$ to obtain a message signal with L modulation symbols denoted by $\mathbf{m} = [m_1, \ldots, m_L]$, where the symbols are independent of each other. The tagged signal $\mathbf{s} = [s_1, \ldots, s_L]$ can be obtained by superimposing the tag signal on modulation symbols, and the ith tagged signal s_i satisfies $\mathrm{E}\{s_i\} = 0$ and $\mathrm{E}\,|s_i|^2 = 1$. Because the tag is superimposed on the amplitude of the modulation symbol, we should select a modulation method which is not sensitive to amplitude, such as BPSK, QPSK, etc. When the superimposed tag amplitude is zero, $\mathbf{s} = \mathbf{m}$. Therefore, the modulation symbol should also satisfy $\mathrm{E}\{m_i\} = 0$, $\mathrm{E}\,|m_i|^2 = 1$.

C. CHANNEL MODEL

In this paper, we suppose that the channel between Alice, Bob, and Adv is a Rayleigh block fading channel, i.e., the channel obeys a complex Gaussian random variable with zero-mean and variance of δ_h^2, denoted by $\mathbf{h} = [h_1 \cdots h_L]$, and $h_i \sim CN(0, \delta_h^2)$. $\mathbf{h}$ remains constant in the length of the signal block, varying independently and randomly between blocks. As shown in Fig. 1, we use $\mathbf{h}_{BA}$ and $\mathbf{h}_{AB}$ to denote the uplink and downlink CSI of Alice and Bob. The CSI between Adv, Alice, and Bob are $\mathbf{h}_{AE}$ and $\mathbf{h}_{EB}$. Because the wireless channel has short-term reciprocity, when the distance between Adv, Alice, and Bob exceed $\lambda/2$ [30] (λ is the wavelength), meanwhile Alice and Bob estimate the channel within the coherence time, there is $\mathbf{h}_{AB} = \mathbf{h}_{BA} \neq \mathbf{h}_{AE} \neq \mathbf{h}_{EB}$. The channel noise is complex Gaussian noise, denoted by $\mathbf{n} = [n_1 \cdots n_L]$, and $n_i \sim CN(0, \delta_n^2)$. The SNR of system is δ_h^2/δ_n^2.

IV. AUTHENTICATION FRAMEWORK

The authentication framework proposed in this paper mainly includes four links: channel mutual probing to generate secret

TABLE 2. Summary and comparison of related work.

Author	Year	Authentication mechanism	Contributions	Share key	Types of attacks			
					Replay	Jamming	Tampering	Impersonation
F. J. Liu *et al.* [22]	2013	CSI-based	A two dimensional quantization algorithm for CIR was proposed.	×	✓	×	×	✓
J. sheng *et al.* [7]	2016	Challenge-response	A fault-tolerant hash method was proposed for PLSA scheme.	✓	✓	✓	×	✓
J. Choi. [8]	2019	Challenge-response	A channel coding approach is employed to mitigate the difference between the two estimated channels as well as channel fading and background noise.	✓	✓	✓	×	✓
P. L. Yu *et al.* [9]	2008	Watermarking	Do not require excess bandwidth. A basic framework of PLSA watermarking mechanism was proposed.	✓	✓	✓	✓	✓
P. Zhang *et al.* [27]	2019	Watermarking	Lightweight tag-based PLSA for IoT devices in smart cities With the help of matrix analysis and hypothesis testing theories, analytical models are further developed.	✓	✓	✓	✓	✓
N. Zhang *et al.* [28]	2020	Watermarking	PLSA for IoT via WFRFT-based gaussian tag embedding A prototype is further developed using FPGA	✓	✓	✓	✓	✓
J. B. Perazzone [29]	2020	Watermarking	A novel secret codebook scheme Show that utilizing artificial noise can greatly increase the key lifespan	✓	✓	✓	✓	✓
Our scheme		Watermarking	A PLSA watermarking mechanism without key distribution. A simple and fault-tolerant hash function is developed and analyzed.	×	✓	✓	✓	✓

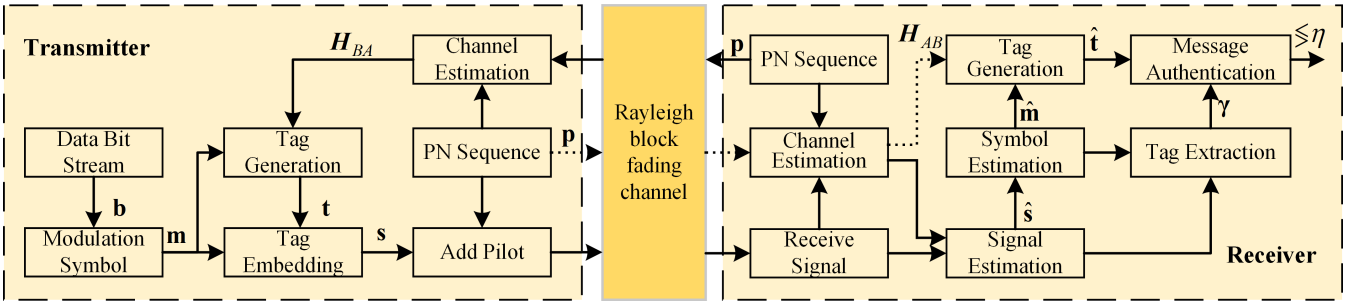


FIGURE 2. Authentication framework.

sequence, tag generation and embedding of transmitter, tag generation and extraction of receiver, and hypothesis test authentication. As illustrated in Fig. 2, firstly, Alice and Bob send the probing sequence $\mathbf{p}$ to each other for channel estimation, and use the channel measurements as a shared random source to generate secret sequences; then Alice utilizes the secret sequence $\boldsymbol{H}_{BA}$ and modulation symbols $\mathbf{m}$ to generate an authentication tag $\mathbf{t}$ and embeds the tag into the modulation symbol to send to the receiver; Bob performs signal estimation and demodulation, then utilizes the estimated signal $\hat{\mathbf{s}}$, modulation symbols estimated value $\hat{\mathbf{m}}$, and secret sequence $\boldsymbol{H}_{AB}$ for tag extraction and generation; finally, Bob extracts the residuals for hypothesis testing authentication.

A. CHANNEL ESTIMATION

Based on the short-term reciprocity of wireless channels, Alice and Bob transmit $\mathbf{p}$ to each other for channel probing, they can obtain consistent or highly similar CSI. Assuming that the signals received by both parties after $\mathbf{p}$ passing through the channel is $\mathbf{y}_p$. The linear minimum mean square error algorithm is used for channel estimation to obtain CSI measurements. Thus, we have

$$\hat{\mathbf{h}} = R_{hh}(R_{hh} + \beta\sigma_n^2 I)^{-1}\mathbf{h}_{ls} \tag{1}$$

$$\mathbf{h}_{ls} = \mathbf{y}_p \frac{1}{|\mathbf{p}|^2}\mathbf{p}^H \tag{2}$$

where R_{hh} is the channel autocorrelation matrix. β is related to the signal modulation mode, e.g., when the QPSK modulation is adopted, $\beta = 1$; when the 16QAM modulation is adopted, $\beta = 9/16$. $\mathbf{h}_{ls}$ is the channel estimation value obtained by the least squares algorithm.

Due to the influence of noise, the probing signals received by Alice and Bob are slightly different. Therefore, the CSI measurements of Alice and Bob are also different, denoted by $\hat{\mathbf{h}}_{BA}$ and $\hat{\mathbf{h}}_{AB}$, respectively. After down-sampling the CSI measurements, Alice and Bob perform four-level uniform quantization on the CSI modulus value; then conduct Gray coding on the quantized value, and map the coding sequence

to zero-mean and variance of one private sequences $\boldsymbol{H}_{BA}$ and $\boldsymbol{H}_{AB}$ which consists of N symbols.

B. TAG GENERATION AND EMBEDDING OF TRANSMITTER

In order to protect the security of the secret sequence and prevent the signal from being tampered, Alice utilizes a one-way hash function $hash(\cdot)$ to couple the secret sequence and the modulation symbol to generate a tag sequence, which can be written as

$$\mathbf{t} = hash\left(\boldsymbol{H}_{BA}, \mathbf{m}\right) \tag{3}$$

Specific algorithm as follows:

a) The initial authentication sequence of length $N + L$ is composed of sequences $\boldsymbol{H}_{BA}$ and $\mathbf{m}$

$$\mathbf{AUC} = [\boldsymbol{H}_{BA}, \mathbf{m}] \tag{4}$$

b) Use a hash function to map the initial authentication sequence to a tag sequence with length L, the ith tag can be written as

$$t_i = a_i \cdot \left(\begin{array}{l} \sum_{k=1}^{N+L} AUC_k \cdot \cos \dfrac{2\pi i(k-1)}{N+L} \\ -AUC_{N+i} \cdot \cos \dfrac{2\pi i(N+i-1)}{N+L} \end{array} \right) \tag{5}$$

Because both $\boldsymbol{H}_{BA}$ and $\mathbf{m}$ are random sequences with zero-mean and variance of one, and they are independent of each other, we can get the t_i with zero-mean and variance of $a_i^2 b_i$, where b_i is

$$\begin{aligned} b_i &= \sum_{k=1}^{N+L} \left(\cos \frac{2\pi i(k-1)}{N+L} \right)^2 - \left(\cos \frac{2\pi i(N+i-1)}{N+L} \right)^2 \\ &= \frac{N+L}{2} - \cos^2 \left(\frac{2\pi i(N+i-1)}{N+L} \right) \end{aligned} \tag{6}$$

If $a_i = 1/\sqrt{b_i}$, there will have $\mathrm{E}\{t_i\} = 0$, $\mathrm{E}\,|t_i|^2 = 1$, and $\mathrm{E}\{\mathbf{m}\mathbf{t}^H\} = 0$, which means that the signal is statistically uncorrelated of the tag. Alice embeds the generated tag into the modulation symbol to get the tagged signal, so we have

$$\begin{aligned} s_i &= \rho_s m_i + \rho_t t_i \\ s.t.\ \rho_s^2 + \rho_t^2 &= 1, \quad 0 < \rho_s^2, \rho_t^2 < 1 \end{aligned} \tag{7}$$

where ρ_s^2 and ρ_t^2 determine the power allocation between the message signal and the tag signal.

C. TAG GENERATION AND EXTRACTION OF RECEIVER

The ith received signal obtained by the receiver can be written as

$$y_i = h_{AB,i} \cdot s_i + n_{AB,i} \tag{8}$$

The LS algorithm was employed to get the tagged signal estimated value, so we have

$$\hat{s}_i = (\hat{h}_{AB,i}^* \cdot \hat{h}_{AB,i})^{-1} \hat{h}_{AB,i}^* \cdot y_i \tag{9}$$

Bob demodulates the estimated value of the tagged signal to obtain $\hat{b}_i = f_d(\hat{s}_i)$, then modulates the demodulated bit $\hat{b}_i$ to obtain a symbol estimate $\hat{\boldsymbol{m}}_i = f_e(\hat{b}_i)$; finally uses the symbol modulation estimated value $\hat{m}$ and the channel secret sequence $\boldsymbol{H}_{AB}$ to generate tag $\hat{\mathbf{t}} = hash(\boldsymbol{H}_{AB}, \hat{\mathbf{m}})$. Afterwards, the tagged signal estimated value $\hat{s}_i$ and $\hat{b}_i$ are exploited to the tag extraction, so we have

$$\gamma_i = \hat{s}_i - \rho_s f_e(\hat{b}_i) \tag{10}$$

D. AUTHENTICATION

Bob extracts the residuals between the estimated value of the tag $\hat{\mathbf{t}}$ and the observed value of the tag γ, then carry out authentication with the test function $\boldsymbol{\ell}(\mathbf{z})$

$$\boldsymbol{\ell}(\mathbf{z}) \triangleq \mathbf{z}\mathbf{z}^H \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \eta \tag{11}$$

$$\mathbf{z} = \gamma - \rho_t \cdot \hat{\mathbf{t}} \tag{12}$$

$$\begin{cases} \mathcal{H}_0 : \boldsymbol{\ell}(\mathbf{z}) < \eta & Authentic \\ \mathcal{H}_1 : \boldsymbol{\ell}(\mathbf{z}) > \eta & Unauthentic \end{cases} \tag{13}$$

where $\boldsymbol{\ell}(\mathbf{z})$ is sufficient statistic, $\mathbf{z}$ is residuals, and η is the judgment threshold. The residuals $\mathbf{z}$ contains not only channel noise, but also the tag difference between Alice and Bob. Assuming that the tag difference between Alice and Bob is $\Delta\mathbf{t}$, the shared secret sequence difference is $\Delta\boldsymbol{H}$, the symbol error is $\Delta\mathbf{m}$, and the initial authentication sequence error is $\Delta\mathbf{AUC} = \Delta\boldsymbol{H} + \Delta\mathbf{m}$, then there is

$$\Delta t_i = a_i \rho_t \cdot \left(\begin{array}{l} \sum_{k=1}^{N+L} \cos \dfrac{2\pi i(k-1)}{N+L} \cdot \Delta AUC_k \\ -\Delta AUC_{N+i} \cdot \cos \dfrac{2\pi i(N+i-1)}{N+L} \end{array} \right) \tag{14}$$

When $\mathbf{t} = \hat{\mathbf{t}}$, i.e., $\Delta\mathbf{t} = \mathbf{O}$, because $z_i = \gamma_i - \rho_t \cdot \hat{t}_i$, we can get $z_i \sim CN\left(0, \frac{\sigma_n^2}{\sigma_h^2}\right)$, if $\alpha = \frac{\sigma_n^2}{2\sigma_h^2}$, we will have $\frac{\boldsymbol{\ell}(\mathbf{z})}{\alpha} \sim \chi^2(2L)$. When $\mathbf{t} \neq \hat{\mathbf{t}}$, the errors caused by the tag difference is $\Delta\mathbf{t}\Delta\mathbf{t}^H$, Assuming that the tag is not correlated with channel noise, so the test function satisfies $\frac{\boldsymbol{\ell}(\mathbf{z}) - \Delta\mathbf{t}\Delta\mathbf{t}^H}{\alpha} \sim \chi^2(2L)$.

In (13), hypothesis testing is used for authentication, which will also bring two types of unavoidable errors [27]. One is false alarm rate (the probability of Bob rejecting a normal signal), denoted by $\mathrm{P_f}$; the other is missed detection rate, denoted by $\mathrm{P_m}$ (the probability of Bob accepting a forged signal). $\mathrm{P_f}$ and $\mathrm{P_m}$ can be given by

$$\mathrm{P_f} = \mathrm{p}\{\boldsymbol{\ell}(\mathbf{z}) > \eta | \mathcal{H}_0\} = 1 - \mathrm{F}_{\chi_{2L}^2}\left(\frac{\eta}{\alpha}\right) \tag{15}$$

$$\mathrm{P_m} = \mathrm{p}\{\boldsymbol{\ell}(\mathbf{z}) < \eta | \mathcal{H}_1\} = \mathrm{F}_{\chi_{2L}^2}\left(\frac{\eta - \Delta\mathbf{t}\Delta\mathbf{t}^H}{\alpha}\right) \tag{16}$$

where $\mathrm{F}_{\chi_{2L}^2}(\cdot)$ is a right-tail probability function for a χ_{2L}^2 random variable with $2L$ degrees of freedom.

In this paper, we utilize $\mathrm{P_f}$ to measure the authentication performance of our scheme, and $\mathrm{P_m}$ is employed to analyze the security performance under impersonation attacks.

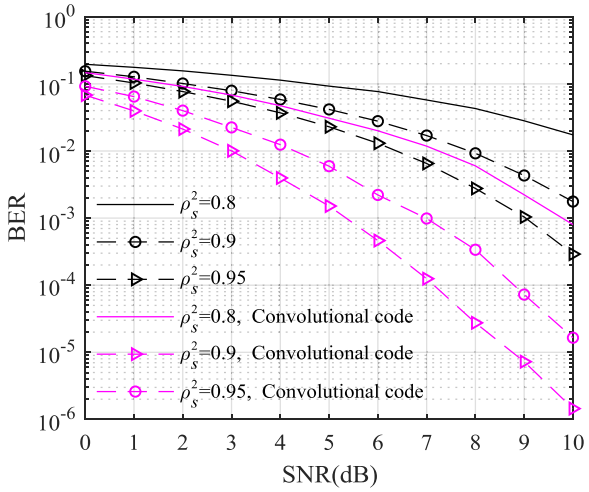


FIGURE 3. BER for signal in rayleigh fading channel with different ρ_s^2.

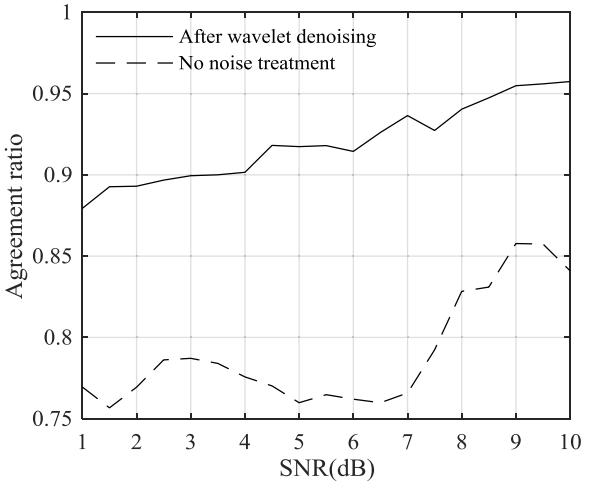


FIGURE 4. Agreement ratio of shared sequence between wavelet denoising and no noise processing.

V. PERFORMANCE ANALYSIS

A. ROBUSTNESS

A strong authentication scheme should be able to withstand the influence of channel noise and could continue the identity verification process under interference. Because Bob exploited the CSI measurements $\hat{\mathbf{h}}_{AB}$ and symbol estimated value $\hat{\mathbf{m}}$ when generating tags, the accuracy of estimated parameters and the fault tolerance of the hash function become very important.

In general, increasing the average power of the transmitted signal (i.e., increasing the SNR) can improve the robustness of the system. In Fig. 3, when using the QPSK modulation, the bit error rate (BER) decreases with the increase of the SNR and the message signal allocation power ρ_s^2. After we utilize convolutional codes for channel coding, the BER is reduced a lot. When channel coding is adopted, ρ_s^2 reaches 0.95 and the SNR reaches 10dB, the BER is close to 10^{-6} which means a good performance.

The agreement ratio of the shared secret sequence generated by the channel estimation is mainly affected by noise. In recent years, wavelet threshold denoising is often used in signal processing fields such as image denoising, and it has good results in various fields [31], [32]. In this paper, wavelet threshold denoising is used for channel estimation, which can reduce the interference of noise to the system and improve the performance of the system.

Fig. 4 shows that the agreement ratio of the shared secret sequences generated by Alice and Bob rises with the increase of SNR. If the legitimate nodes perform wavelet denoising preprocessing on the received probing sequence, the agreement ratio will be as high as 96%, with SNR = 10dB, which is better than no noise treatment.

Although high parameter accuracy can be achieved under high SNR, errors are inevitable. In security authentication, hash functions [33], [34] are often utilized to generate digital signatures and identity authentication codes. The hash algorithm in the existing cryptography will get completely different results even if the input information has one bit error, which does not conform to the noisy characteristics of wireless communication. Therefore, this paper adopts a fault-tolerant hash algorithm, i.e., the input values are similar, and the same or similar results can be obtained. Through (14), we can deduce $\Delta t_i \Delta t_i^H < a_i^2 \rho_t^2 \sum_{k=1}^{N+L} |\Delta AUC_k|^2$, as long as $\Delta\mathbf{AUC}$ is small enough, the estimation error does not significantly affect the performance of safety authentication. This shows that the hash algorithm we used has high robustness and is more suitable for noisy wireless channels.

B. AUTHENTICATION PERFORMANCE

From (12) and (15), we can see that the main factors affecting the false alarm rate are the setting of judgment threshold, the length of authentication tags and the accuracy of the tag generated by Bob. As mentioned in the previous section, parameter estimation errors are inevitable, however, in practice, channel coding and check codes [23] can be used to reduce channel interference to ensure the accuracy of data transmission. Through consensus negotiation, we can ensure the consistency of the secret sequence generated by Alice and Bob. Therefore, for the convenience of analysis, we can assume that Alice and Bob can get a consistent tag, i.e. $\hat{\mathbf{t}} = \mathbf{t}$.

Fig. 5 compares the changes of P_f under different tag lengths L and thresholds η. It can be seen that P_f decreases as the SNR increases. When L is fixed, P_f decreases monotonically with the increment of η; when η is fixed, the shorter L case the lower P_f. The P_f can be close to 10^{-15} with SNR = 10dB and $L = 30$, $\eta = 30$. Although under certain conditions, P_f can reach a very low value, we still need to consider other factors, because the decrease of P_f comes at the cost of an increase of P_m. e.g., if η is set too high, it will increase the attack success rate of the attacker and reduce the security of the authentication scheme. Therefore, η must be set based on various factors, such as tag length and security of the authentication scheme.

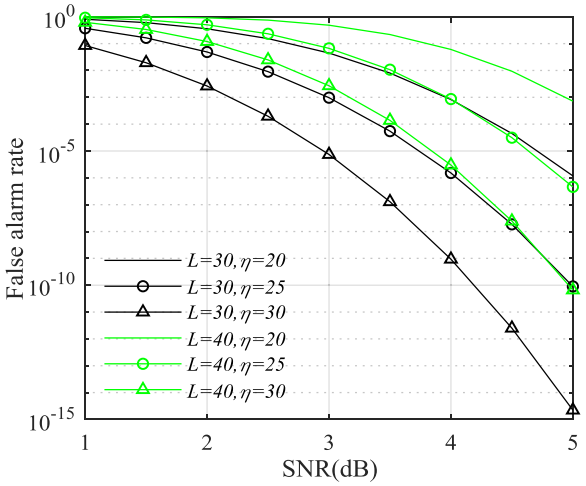


FIGURE 5. Probability of false alarm for various η with different L and η.

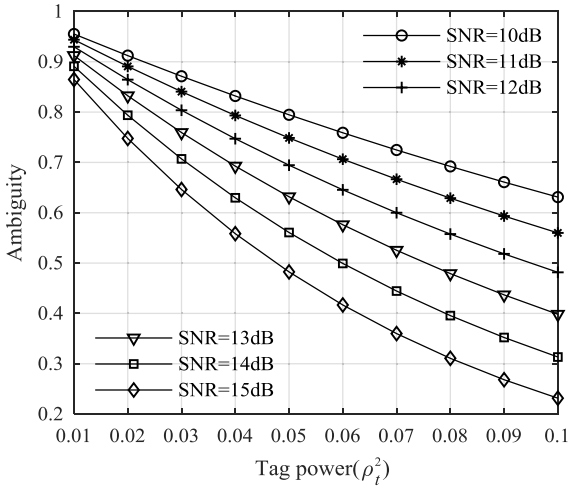


FIGURE 6. Ambiguity under different ρ_t^2 with various SNR.

C. SECURITY PERFORMANCE

In this part, the security performance of our scheme under different attack methods are analyzed.

1) REPLAY ATTACKS

In a replay attack, Adv tries to record the transmission signals form Alice at a certain moment, then replay the recording signals, in hopes of passing authentication. Replay attack will cause Bob to fail to authenticate normally and disrupt normal communications. In our scheme, the tags used for authentication have time-varying characteristics. Bob will reject outdated tags.

2) JAMMING ATTACKS

Adv attempts to delete or destroy the tag so that Bob cannot accurately authenticate the message. Due to the ''open air'' nature of wireless networks, Adv can receive legitimate transmitted signal. Assuming that Adv utilizes the same method as Bob to extract tags from the tagged signal to obtain γ_i, the tag-to-noise ratio (TNR) in γ_i is $\rho_t^2\delta_h^2/\delta_n^2$. So, the error probability p_e [9] of original tag t_i inferred from the observation value γ_i can be written as

$$p_e = \Phi(-\rho_t\delta_h/\delta_n) \tag{17}$$

We utilize the ambiguity to describe the security performance of the tag, and the total average value of the conditional information is used for calculating the ambiguity. Thus, we have

$$H(t_i|\gamma_i) = p_e \log_2 \frac{1}{p_e} + (1-p_e)\log_2 \frac{1}{1-p_e} \tag{18}$$

As shown in Fig. 6, when $\rho_t^2 = 0.1$, and SNR = 10dB, the ambiguity is higher than 0.6, and the ambiguity is lower than 0.3 with SNR = 15dB; when SNR = 10dB, and $\rho_t^2 = 0.01$, the ambiguity is exceed 0.9. This illustrates that the ambiguity rises as the SNR and ρ_t^2 decrease. The higher the ambiguity, the more difficult it is for Adv to infer the authentication tag.

3) TAMPERING ATTACKS

Suppose that Adv can extracts the authentication tag form the intercepted signal. Adv tampers with the intercepted message signal or creates a novel message, and embeds the extracted tag into the message signal, hoping to pass authentication of Bob. Fig. 6 shows that with the increase of ρ_t^2 and the SNR, the accuracy of tag extracted by Adv rises. Since we use a hash algorithm (5) to generate authentication tags, even if Adv can obtain accurate authentication tags and message signals, it still cannot generate a valid tag, unless knowing the shared secret sequence between Alice and Bob. Due to (3), Adv tampers with the message signal will cause errors in the authentication tag $\hat{\mathbf{t}}$ generated by Bob, that will reduce the probability of successful authentication. Equation (4), (14), and (16) reveals that the longer the signal length of Adv tampering, the lower the probability of passing authentication.

4) IMPERSONATION ATTACKS

In this attack method, Adv attempts to create his own message signal and tags to try to pass authentication. Although Adv can forge message signal and tags, it cannot obtain the shared secret sequence between Alice and Bob. We assume that the generated sequence after Adv channel estimation is $\boldsymbol{H}_{EB}$, and the sequence difference between Adv and Bob is $\Delta\boldsymbol{H}$, the kth $\Delta\boldsymbol{H}$ can be written as

$$\Delta H_k = H_{AB,k} - H_{EB,k} \tag{19}$$

Since $\boldsymbol{H}_{AB}$ and $\boldsymbol{H}_{EB}$ are random sequences with zero-mean and variance of one, we can get a random sequence $\Delta\boldsymbol{H}$ with zero-mean and variance of two. Taking $N = L$, $\Delta\mathbf{m} = \mathbf{O}$, using (14), we can get

$$\begin{aligned}\Delta t_i \Delta t_i^H &= a_i^2\rho_t^2 \cdot \sum_{k=1}^{N}\left(\cos\frac{2\pi i(k-1)}{N+L}\right)^2 \cdot \Delta H_k \Delta H_k^H \\ &= a_i^2\rho_t^2 L \end{aligned} \tag{20}$$

$$\Delta\mathbf{t}\Delta\mathbf{t}^H = \sum_{i=1}^{L}\Delta t_i \Delta t_i^H = \sum_{i=1}^{L} a_i^2\rho_t^2 L \tag{21}$$

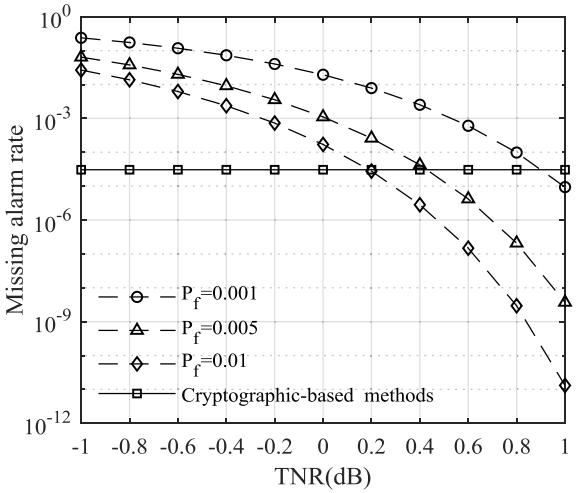


FIGURE 7. Miss detection rate for $P_f = \{0.001, 0.005, 0.01\}$ and traditional cryptographic algorithm over different TNR.

Assuming that $\varepsilon = \sum_{i=1}^{L} a_i^2 \rho_i^2 L$, so we have $\frac{\ell(\mathbf{z})-\varepsilon}{\alpha} \sim \chi^2(2L)$, then P_m can be written as

$$P_m = p\{\ell(\mathbf{z}) < \eta | \mathcal{H}_1\} = F_{\chi^2_{2L}}\left(\frac{\eta - \varepsilon}{\alpha}\right) \tag{22}$$

As shown in Fig. 7, in the case of a specific P_f, P_m decreases monotonically as the TNR increases; when the SNR is fixed, P_m decreases with the increment of P_f. Traditional cryptographic-based authentication methods rely on computational complexity and the privacy of keys to achieve secure authentication. In 1985, Simmons [35] used the methods of information theory to analyze the success rate of attacks based on cryptography, and obtained the lower bound of attack success rate as $1/\sqrt{|K|}$, where $|K|$ is the key size of space. In Fig. 7, with $K = L = 30$, TNR = 1dB, and $P_f = 0.01$, P_m is lower than 10^{-10}, which is far less than the lower bound of the attack success rate of traditional cryptographic-based authentication methods.

VI. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

In this section, we analyze some challenges which are yet to be solved, and some of the future research directions are discussed.

In our scheme, a higher bit agreement ratio is obtained through wavelet denoising. Nevertheless, in large scale IoT scenarios, the computational power of terminals is limited. How to use the limited computational power terminal to get a higher bit agreement ratio is the focus of our future research. The bit generation rate is also an important factor affecting security authentication. In future research work, increasing the bit generation rate is also a research focus. In the performance analysis of this paper, the impact of the judgment threshold on the authentication performance is discussed, and the trade-offs among them are analyzed. However, the fixed threshold may not adapt to dynamically changing wireless channels. Therefore, the adaptive threshold will also be applied to our next work.

Recently, deep learning has been introduced to perform feature mining and regular analysis on a large amount of CSI data, so as to realize the secure access of users. Combining artificial intelligence with authentication will also be a hot research topic.

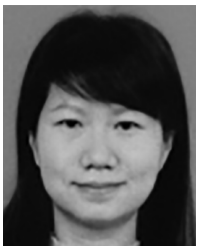
VII. CONCLUSION

Based on the watermarking authentication mechanism, we have proposed a PLSA scheme, which utilizes channel characteristics to generate authentication tags. The scheme does not require to distribute keys, but generates the shared secret sequence based on the uniqueness, location difference, time-varying and difficulty to imitate of the channel between legitimate nodes. And a fault-tolerant hash function is employed for tag generation, the hash algorithm does not depend on the computational complexity and only needs simple multiplication, so it has high practical value. We have analyzed the robustness, authentication performance and security of the scheme. Simulation results show that it has high bit consistency rate and robustness at high SNR, and can resist against multiple attacks such as replay, jamming, tampering and impersonation attack. In the case of high SNR, it is much better than the traditional cryptographic algorithms, which means that our scheme has a very great application prospect.

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[2] L. Zhu, M. Li, Z. Zhang, C. Xu, R. Zhang, X. Du, and N. Guizani, "Privacy-preserving authentication and data aggregation for fog-based smart grid," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 80–85, Jun. 2019.
[3] H. Wen, G. Gong, and P.-H. Ho, "MIMO cross-layer secure communication architecture based on STBC," in *Proc. IEEE GLOBECOM*, Miami, FL, USA, Dec. 2010, pp. 1–5.
[4] 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.
[5] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Trans. Depend. Sec. Comput.*, vol. 17, no. 5, pp. 1079–1093, Sep. 2020.
[6] 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.
[7] X. Ji, J. Yang, K. Huang, and M. Yi, "Physical layer authentication scheme based on hash method," *J. Electr. Inf. Technol.*, vol. 38, no. 11, pp. 11–19, Nov. 2016.
[8] 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.
[9] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.
[10] R. Jin, X. Du, K. Zeng, L. Huang, L. Xiao, and J. Xu, "Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2526–2535, Mar. 2017.
[11] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, no. 5, p. 497, May 2019.
[12] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[13] A. Soni, R. Upadhyay, and A. Kumar, "Wireless physical layer key generation with improved bit disagreement for the Internet of Things using moving window averaging," *Phys. Commun.*, vol. 33, pp. 249–258, Apr. 2019.
[14] Z. Jiang, J. Zhao, X.-Y. Li, J. Han, and W. Xi, "Rejecting the attack: Source authentication for Wi-Fi management frames using CSI information," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 2544–2552.
[15] S. Jiang, "On the optimality of keyless authentication in a noisy model," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1250–1261, Jun. 2015.
[16] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.
[17] J. W. Wal and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.
[18] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
[19] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.
[20] L. Jiao, J. Tang, and K. Zeng, "Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel," in *Proc. CNS*, Beijing, China, May 2018, pp. 1–9.
[21] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information (CSI)," in *Proc. ASIACCS*, Kyoto, Japan, Jun. 2014, pp. 389–400.
[22] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE ICC*, Budapest, Hungary, Jun. 2013, pp. 4724–4728.
[23] D. Chen, N. Zhang, R. Lu, X. Fang, K. Zhang, Z. Qin, and X. Shen, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.
[24] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, Jun. 2019.
[25] S. Sezer, "T1C: IoT security: Threats, security challenges and IoT security research and technology trends," in *Proc. SOCC*, Arlington, VA, USA, Sep. 2018, pp. 1–2.
[26] Y. Zheng, S. S. Dhabu, and C.-H. Chang, "Securing IoT monitoring device using PUF and physical layer authentication," in *Proc. ISCAS*, Florence, Italy, May 2018, pp. 1–5.
[27] 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.
[28] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar, and H. Zhang, "Physical-layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, Sep. 2020.
[29] J. B. Perazzone, "Key-based authentication at the physical layer," Ph.D. dissertation, Dept. Electr. Eng., Lehigh Univ, Bethlehem, PA, USA, 2020.
[30] W. C. Jakes, *Microwave Mobile Communications*. Hoboken, NJ, USA: Wiley, 1974, pp. 13–39.
[31] C. Li, D. Cao, and Y. Yuan, "Research on improved wavelet denoising method for sEMG signal," in *Proc. CAC*, Hangzhou, China, Nov. 2019, pp. 5221–5225.
[32] Y. Qian, "Image denoising algorithm based on improved wavelet threshold function and median filter," in *Proc. IEEE ICCT*, Chongqing, China, Oct. 2018, pp. 1197–1202.
[33] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Comput. Commun.*, vol. 34, no. 3, pp. 391–397, Mar. 2011.
[34] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, and N. Bagheri, "Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol," *J. Comput. Appl. Math.*, vol. 259, no. 1, pp. 571–577, Mar. 2014.
[35] G. J. Simmons, "Authentication theory/coding theory," in *Proc. CRYPTO*, New York, NY, USA, 1985, pp. 411–431.



YONGLI AN received the Ph.D. degree in information science from Beijing Jiao tong University, Beijing, China, in 2015. She is currently a Professor with the North China University of Science and Technology, China. Her current research interests include wireless network security, interference cancellation technology, and large-scale MIMO technology.

SHIKANG ZHANG is currently pursuing the master's degree with the College of Information Engineering, North China University of Science and Technology, Tangshan, China. His current research interests include wireless network security and physical layer security authentication.

ZHANLIN JI received the M.Eng. degree from Dublin City University, in 2006, and the Ph.D. degree from the University of Limerick, in 2010. He is currently a Professor with the North China University of Science and Technology, China, and a Researcher with the Telecommunications Research Centre (TRC), University of Limerick, Ireland. He has authored/coauthored 70 research articles in refereed journals and conference papers. His research interests include UCWW, the Internet of Things (IoT), cloud computing, big data management, and data mining.