sensors

MDPI

Article

Channel Prediction-Based Security Authentication for Artificial Intelligence of Things

Xiaoying Qiu [1,*], Jinwei Yu [2], Wenying Zhuang [1], Guangda Li [1] and Xuan Sun [1]

[1] School of Information and Management, Beijing Information Science & Technology University, Beijing 100192, China; 20182165@bistu.edu.cn (W.Z.); 20172037@bistu.edu.cn (G.L.); sunxuan@bistu.edu.cn (X.S.)
[2] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; hahayuswag@bupt.cn
* Correspondence: 20192329@bistu.edu.cn

Abstract: The emerging physical-layer unclonable attribute-aided authentication (PLUA) schemes are capable of outperforming traditional isolated approaches, with the advantage of having reliable fingerprints. However, conventional PLUA methods face new challenges in artificial intelligence of things (AIoT) applications owing to their limited flexibility. These challenges arise from the distributed nature of AIoT devices and the involved information, as well as the requirement for short end-to-end latency. To address these challenges, we propose a security authentication scheme that utilizes intelligent prediction mechanisms to detect spoofing attack. Our approach is based on a dynamic authentication method using long short term memory (LSTM), where the edge computing node observes and predicts the time-varying channel information of access devices to detect clone nodes. Additionally, we introduce a Savitzky–Golay filter-assisted high order cumulant feature extraction model (SGF-HOCM) for preprocessing channel information. By utilizing future channel attributes instead of relying solely on previous channel information, our proposed approach enables authentication decisions. We have conducted extensive experiments in actual industrial environments to validate our prediction-based security strategy, which has achieved an accuracy of 97%.

Keywords: artificial intelligence of things; edge computing; security authentication; intrusion detection

Citation: Qiu, X.; Yu, J.; Zhuang, W.; Li, G.; Sun, X. Channel Prediction-Based Security Authentication for Artificial Intelligence of Things. *Sensors* **2023**, *23*, 6711. http://doi.org/10.3390/s23156711

Academic Editors: Dapeng Wu, Zhidu Li and Boran Yang

Received: 29 June 2023
Revised: 15 July 2023
Accepted: 24 July 2023
Published: 27 July 2023

1. Introduction

The combination of core technologies such as 5G, artificial intelligence (AI), and the internet of things (IoT) has opened the door to innovation [1,2]. A new type of IoT structure known as artificial intelligence of things (AIoT) is coming into play. AIoT has become a hot area for realizing real-time information acquisition through IoT sensors and performing intelligent data analysis tasks anywhere along the terminal—edge—cloud continuum. This forms a smart and enabling ecosystem that brings extensive economic benefits [3–5]. Benefiting from these advantages, AIoT solutions have expanded into many emerging areas, including commercial surveillance, autonomous driving, smart retail, and drone-based traffic monitoring [6].

AIoT has the potential to offer various new application services [7,8]. AI-based systems have been developed to provide real-time monitoring, analysis, and protection [9,10]. However, to effectively utilize AIoT, networks capable of processing large amounts of information quickly are necessary [11]. Furthermore, the complexity of devices and environments exposes IoT networks to malicious attacks that exploit security vulnerabilities [12]. Due to the large number of IoT sensor nodes and the openness of wireless networks, attackers can eavesdrop on communications, modify transmitted messages, and even send false data [13–15]. For instance, in unsupervised industrial IoT networks [16–18], clone node attacks can occur, where adversaries hijack control devices and deploy cloned nodes, leading to significant security risks by collecting sensitive information. Industrial control centers may struggle to differentiate these fraudulent nodes, potentially causing serious

safety accidents within the AIoT network. In the aforementioned case, the authentication of devices utilizing AIoT applications can be severely compromised, highlighting the increasing concern over the security of AIoT in wireless systems [19].

1.1. Existing Methods and Their Challenges

The AIoT network needs to verify the legitimacy of wireless sensors during the initial joining process of communication nodes. The increasing complexity of standard encryption methods has motivated the study of physical layer authentication techniques.Several security technologies have been proposed for IoT networks [13]. For instance, physical unclonable functions (PUF) and wireless fingerprinting (WF) have shown promise in improving authentication in challenging scenarios. Li et al. [20] developed a security framework based on channel virtual representation in millimeter wave (mmWave) massive multiple-input and multiple-output (MIMO) 5G networks, aiming to address a one-class classification problem. Qiu et al. [21] proposed a physical layer authentication framework in IoT networks that utilized a 2D feature measure space for data enhancement. The model's performance was evaluated using a Gaussian mixture model and tested on the USRP dataset. However, these conventional physical layer approaches are not suitable for future AIoT networks and can be easily compromised by fraudsters, especially in the era of quantum computing.

To enhance authentication in next-generation wireless networks, such as a decentralized, dynamic, and heterogeneous AIoT network, researchers have explored the concept of lightweight flexible group authentication mechanisms for fingerprint identification [22–25]. A group authentication scheme was proposed in [23,24] to detect devices' identities based on generated tokens for decentralized edge collaboration. Additionally, a game theory framework was proposed to extract random characteristics of IoT devices, enabling the cloud to effectively verify signal reliability [26]. A hybrid privacy-preserving mechanism for the IoT is introduced in [27], employing the federated learning (FL) method to identify malicious participants. Gao et al. [28,29] conducted research on the impact of PUF-based deep learning in wireless sensor networks, specifically focusing intelligent spoofing. They compared the results of several adversarial attacks with deep Q networks. Wang et al. [30,31] developed a novel CSCB fingerprinting framework to detect spoofing attacks. Their proposed scheme utilizes sector-level sweep (SLS) trace-based fingerprinting to enhance effectiveness in mmWave 60-GHz IEEE 802.11 ad networks. Furthermore, the authors in [32] developed a graph neural network (GNN) to effectively detect message injection in control area networks. Other deep learning (DNN)-based security authentication methods are also mentioned in the literature [33,34]. However, the authentication approaches of [25,32] remain inflexible and risk-agnostic in future AIoT network deployments and have low authentication reliability. These solutions also exhibit low authentication reliability and fail to address robustness improvements in dynamic environments. Additionally, the PUF algorithms introduced in [13], do not fully account for changes in the surrounding environment or the time-varying properties of the channel. In a nutshell, a new learning-based dynamic authentication solution is highly beneficial for the next generation of IoT networks. Such a technique should encompass a comprehensive physical layer security scheme that allows IoT devices to authenticate without sharing keys.

1.2. Contributions

This paper proposes a novel dynamic authentication scheme that leverages an intelligent learning model capable of predicting future channel features. In future AIoT networks, the cloud may be unable to identify all transmission signals from access sensor nodes due to limited computing resources and network heterogeneity. Therefore, in a real wireless communication system, the control center must perform dynamic intelligent authentication for a large number of IoT devices. The main objective of this research is to present an intelligent framework that integrates new ideas from dynamic feature extraction and prediction to achieve computationally-efficient authentication of smart nodes.

The key contributions of this paper can be summarized as follows:

- A Savitzky–Golay filter (SGF) is utilized to preprocess wireless channel estimation, aiming to improve spectrum smoothness and reduce interference. Then, the relationship between time series and dynamic characteristics of wireless channels is exploited to extract fingerprints of IoT devices using the high order cumulant model (HOCM). This SGF-HOCM feature extraction enables the edge computing node to effectively track the channel model during two adjacent communications;
- An intelligent framework is proposed to enable the receiver to verify the reliability of received signals and detect the presence of network fraudsters attempting to compromise security performance. The proposed deep learning scheme employs long short-term memory (LSTM) blocks to predict dynamic fluctuations in channel information elements. This allows the security framework to effectively utilize predicted channel information for authentication instead of relying solely on previously estimated data;
- Simulations are conducted using open datasets from the National Institute of Standards and Technology (NIST). The results demonstrate that the proposed learning algorithms enhance the authentication performance of the system. This improvement makes the method highly valuable for time-varying channel prediction, dynamic feature extraction, and security authentication.

The remainder of this article is organized as follows: the system model and analysis are introduced in Section 2. The proposed authentication scheme is described in detail in Section 3, followed by simulation and experimental verification for our dynamic authentication strategy in Section 4. Finally, the paper concludes in Section 5.

2. System Model

We introduce a clone attack scenario, as shown in Figure 1. The legitimate receiver is the edge computing node, which intends to communicate with other IoT devices, including N1, N2, . . ., and N5. An attacker imitates the identity of legitimate transmitter N5 and creates a clone node that injects illegal messages to the edge computing node. The clone node participates in data communication with industrial edge computing. The edge computing node needs to authenticate messages to detect whether they are from legitimate wireless devices.

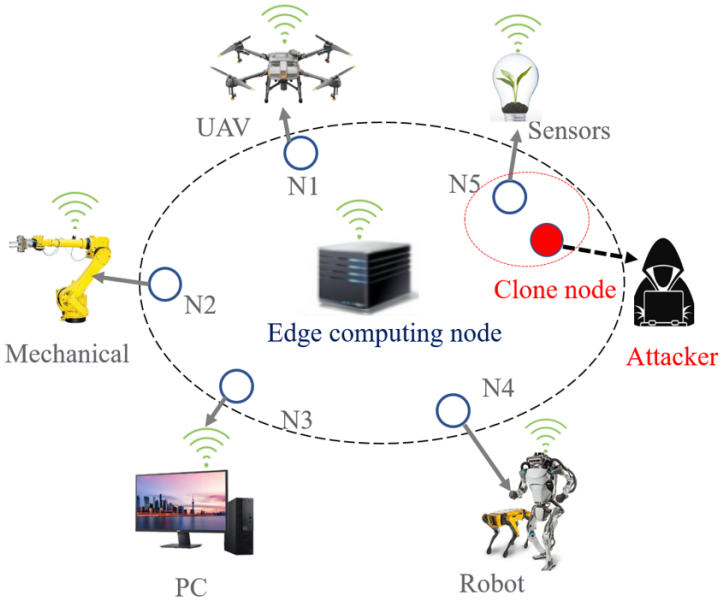

Figure 1. High-level architecture and system model. N1, N2, . . ., and N5 are all legitimate IoT devices. The attacker replicated the clone node based on a legitimate node, such as N5.

The extraction of the physical layer channel response is performed by the legitimate receiver. According to the wireless channel model [35,36], the expression of the received signal can be written as

$$y(t) = h(t) * x(t) + n(t) \tag{1}$$

where t is the time slot, h denotes the channel impulse response, x is a pilot signal known to the transmitter and receiver for estimating channel information, and $n(t)$ is the additive white Gaussian noise with variance σ^2. The corresponding frequency-domain representation obtained through Fourier transform is

$$Y(f_k, t) = H(f_k, t)X(f_k) + N(f_k, t) \tag{2}$$

where Y, H, X, and N represents y, h, x and n, respectively, in frequency domain. f_k is the frequency of the kth subcarrier. Then, the wireless channel estimation can be given by

$$\hat{H}(f_k, t) = \frac{Y(f_k, t)}{X(f_k)} = H(f_k, t) + \hat{N}(f_k, t) \tag{3}$$

where

$$\hat{N}(f_k, t) = \frac{N(f_k, t)}{X(f_k)}. \tag{4}$$

From the wireless channel model in (3), we have the channel estimations of different receivers as

$$\hat{H}_a(f_k, t) = H_a(f_k, t) + \hat{N}_a(f_k, t) \tag{5}$$

$$\hat{H}_c(f_k, t) = H_c(f_k, t) + \hat{N}_c(f_k, t). \tag{6}$$

where $\hat{N}_a(f_k, t)$ and $\hat{N}_c(f_k, t)$ in (5) and (6) are the channel estimation errors, and a and c, respectively, denote legitimate node A and clone node C. Different positions of the wireless device indicate different channel characteristics. Therefore, the channel estimations of the legitimate node are supposed to be different from that of the cloned node, that is

$$\hat{H}_a(f_k, t) \neq \hat{H}_c(f_k, t). \tag{7}$$

We first analyze the traditional problem of binary hypothesis testing. The authentication can be formulated as

$$\begin{cases} \mathcal{H}_0 : \hat{H}_i(t+1) \to \hat{H}_a(t), \\ \mathcal{H}_1 : \hat{H}_i(t+1) \to \hat{H}_c(t), \end{cases} \tag{8}$$

where $\mathcal{H}_0$ indicates that the future estimation $\hat{H}_i(t+1)$ is an authentic packet from legitimate device A, and $\mathcal{H}_1$ means that $\hat{H}_i(t+1)$ comes from different wireless transmission terminals, such as a cloned node.

Existing methods compare the channel measurements received at adjacent times within the channel coherence time, and then determine whether the variables are from a legitimate sender or a malicious attacker, just like the authentication problem in (8). We have adopted an authentication classification function based on machine learning, without using the attacker's channel information, which can be described as

$$\begin{cases} \mathcal{H}_0 : f(\hat{H}_a(t), \hat{H}_i(t+1)) < \eta, \\ \mathcal{H}_1 : f(\hat{H}_a(t), \hat{H}_i(t+1)) \geq \eta, \end{cases} \tag{9}$$

where $f(\cdot)$ is a function that quantifies the difference between the previous value $\hat{H}_a(t)$ and future estimation $\hat{H}_i(t+1)$, η denotes an attack threshold. In this paper, we directly use the estimated channel matrices $\hat{H}$, and then consider a physical layer authentication strategy to detect malicious attacks. There are several algorithms to obtain wireless channel estimations [37–41].

3. Intelligent Prediction-Based Authentication Strategy

The proposed authentication strategy based on intelligent prediction consists of four components, as shown in Figure 2. The security model uses physical layer attributes to prevent cloning attacks. The wireless characteristics are learned using the SGF-HOCM method. This derives time-varying features from preprocessed data using Savitzky–Golay filtering and HOCM feature extraction. Using the extracted features as input, two-layer LSTM network is trained to predict time-varying channel parameters. Finally, the predicted values are compared with the actual values to identify different IoT nodes.

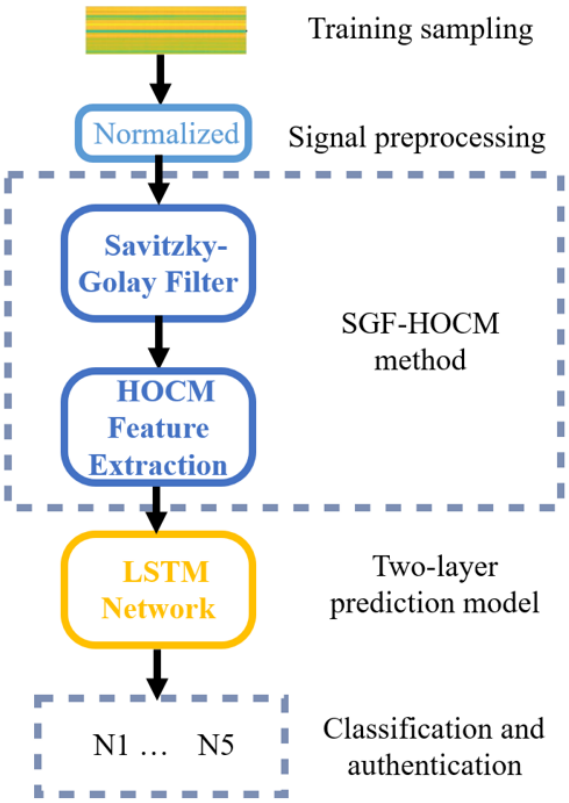

Figure 2. The proposed model of security authentication.

3.1. Channel Information Processing Based on SGF-HOCM

The channel measurement value is vulnerable to the interference of channel estimation error and environmental noise. In view of this analysis, it can be concluded that Gaussian noise and estimation error in (1) and (3) are the main factors to impair the authentication model. These urge us to explore an effective authentication scheme based on time-varying channel prediction to improve the robustness and reliability of the authenticator.

SGF is widely used in data stream smoothing and denoising, and is a filtering method based on local polynomial least square fitting in the time domain. The biggest advantage of SGF is that it can ensure that the shape and width of the signal remain unchanged while filtering out noise. The filtering effect of SGF varies with the selected window width, which can meet the needs of various occasions. The mathematical expression of SGF is formulated as follows:

$$h_{k,smooth} = \frac{1}{2w+1} \sum_{i=-w}^{+w} h_{k+i} \tag{10}$$

where w is the length of the window and k denotes the order of the polynominal. The smaller the value of w, the closer the curve is to the actual curve. The k value is also important for smoothing curves. The larger the k value, the closer the curve is to the real curve, whereas the smaller the k value, the smoother the curve is. In addition, when

the value of k is large, due to the limitation of the window length, fitting may encounter problems, such as high-frequency curves becoming straight lines.

Due to the time-varying nature of wireless links and the difficulty of tracking changes, the existing methods have limited authentication capabilities for intelligent access terminals. One of the main advantages of HOCM is that it contains both amplitude and phase information [42]. Therefore, HOCM is very likely to be a matrix in the authentication scheme, providing a robust feature extraction method. As previously mentioned, a key technology for enabling intelligent prediction models for clone node detection in wireless networks is to extract key features. Assuming that $\{x'_1, x'_2, \cdots, x'_d\}$ is the channel estimations after SGF, their corresponding dth-order cumulant can be defined as the coefficient of $\{v_1, v_2, \cdots, v_d\}$ in the Taylor series expansion of the cumulant-generating function

$$\psi(v) = InE\{exp(jvx')\} \tag{11}$$

where $E[\cdot]$ is a mathematical expectation operator, representing the statistics average. The dth-order cumulant of x' is defined as

$$cum(x'_1, x'_2, \cdots, x'_d) = (-j)^d [\partial/\partial v_1 \partial v_2 \cdots \partial v_d] \psi(v)|_{v=0}. \tag{12}$$

Because the mathematical expressions of the third order and above are very complicated, zero-average processing is used for the channel estimates in the practical application of the security authentication, to simplify the high-order cumulant. When the random variable $\{x'(t)\}$ is a zero mean, the dth-order cumulant is defined as

$$\begin{aligned} C_{kk} &= (\Delta_1, \Delta_2, \cdots, \Delta_{d-1}) \\ &= cum(x'(t), x'(t+\Delta_1), \cdots, x'(t+\Delta_{d-1})) \end{aligned} \tag{13}$$

where $\Delta_1, \Delta_2, \cdots, \Delta_{d-1}$ are the time delays.

According to (12) and (13), the mathematical expressions of the corresponding second moment, third moment and fourth moment of $x'(t)$ are then formulated as follows [42]:

$$C_{2x'}(\Delta) = E\{x'(t)x'(t+\Delta)\} \tag{14}$$

$$C_{3x'}(\Delta_1, \Delta_2) = E\{x'(t)x'(t+\Delta_1)x'(t+\Delta_2)\} \tag{15}$$

$$\begin{aligned} C_{4x'}(\Delta_1, \Delta_2, \Delta_3) =& E\{x'(t)x'(t+\Delta_1)x'(t+\Delta_2)x'(t+\Delta_3)\} \\ &- C_{2x'}(\Delta_1)C_{2x'}(\Delta_2 - \Delta_3) - C_{2x'}(\Delta_2)C_{2x'}(\Delta_3 - \Delta_1) \\ &- C_{2x'}(\Delta_3)C_{2x'}(\Delta_1 - \Delta_2) \end{aligned} \tag{16}$$

In this paper, the SGF-HOCM analysis method is introduced for signal processing of wireless channel information.

3.2. Channel Prediction Based on Two-Layer LSTM

The channel estimations processed by SGF-HOCM method form a sequence, which serves as the input of the two-layer LSTM network. Let the previously SGF-HOCM preprocessed finite segment be the training dataset of two-layer LSTM model, shown as $H_{train} = [h''_p, h''_{p-1}, h''_{p-1}, \cdots, h''_1]$, where p is the size of LSTM training data. The original data of the testing sample is shown as $H_{test} = [h''_{p+1}, h''_{p+2}, h''_{p+3}, \cdots, h''_{p+q}]$, where q denotes

the size of LSTM testing data. Specifically, we consider a model with ten inputs to predict channel vector in the future, as $\tilde{h}_{p+1}$. The prediction procedure can be expressed as

$$\begin{aligned}
\tilde{h}_{p+1} &= \mathcal{L}(h''_p, h''_{p-1}, h''_{p-2}, \cdots, h''_{p-9}),\\
\tilde{h}_{p+2} &= \mathcal{L}(h''_{p+1}, h''_p, h''_{p-1}, \cdots, h''_{p-8}),\\
\tilde{h}_{p+3} &= \mathcal{L}(h''_{p+2}, h''_{p+1}, h''_p, \cdots, h''_{p-7}),\\
&\vdots\\
\tilde{h}_{p+q} &= \mathcal{L}(h''_{p+q-1}, h''_{p+q-2}, h''_{p+q-3}, \cdots, h''_{p+q-10})
\end{aligned} \tag{17}$$

where $\mathcal{L}(\cdot)$ is the prediction function of LSTM model. In our two-layer LSTM network, the predictor always uses the original data in the training step. For instance, we predict $\tilde{h}_{p+q+1}$ based on the same function, whereas the inputs are updated to $h''_{p+q}, h''_{p+q-1}, h''_{p+q-2}, \cdots, h''_{p+q-9}$. The timing schedule for training and prediction is shown in Figure 3.

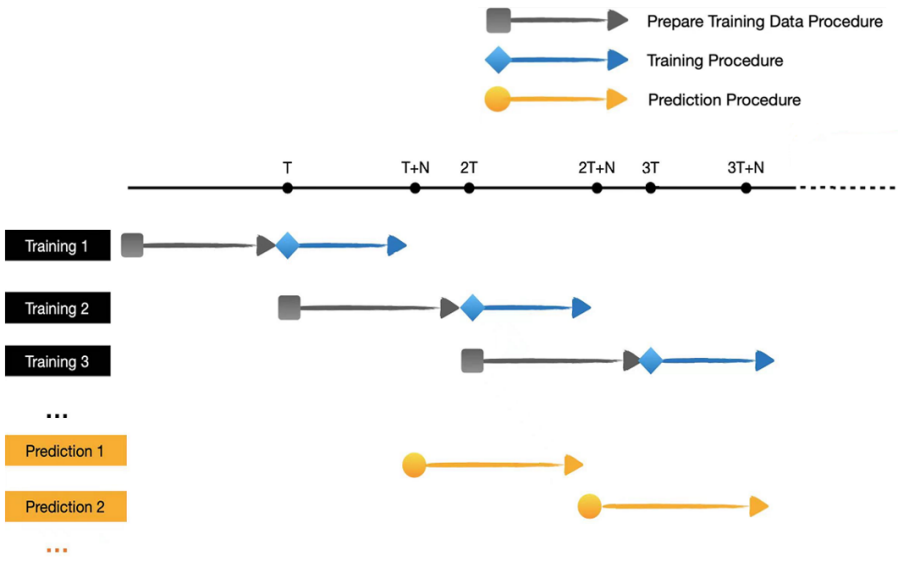

Figure 3. The timing schedule for training and prediction.

One of the attractions of a predictor is that it can use previous channel information to predict future channel attributes (i.e., $\tilde{H}_a(t+1) = [\tilde{h}_1, \tilde{h}_2, \cdots, \tilde{h}_L]$) of legitimate node. Mathematically, the parameters of two-layer LSTM can be formulated as [43,44]

$$f^t = \sigma(W^f \cdot [h^{t-1}, x^t] + b^f) \tag{18}$$

$$f_t = \sigma(W_f x_f + R_f h_{t-1} + b_f) \tag{19}$$

$$i_t = \sigma(W_i x_t + R_i h_{t-1} + b_i) \tag{20}$$

$$o_t = \sigma(W_o x_t + R_o h_{t-1} + b_o) \tag{21}$$

$$\tilde{c}_t = \tanh(W_c x_t + R_c h_{t-1} + b_c) \tag{22}$$

$$c_t = f_t * c_{t-1} + i_t * \tilde{c}_t \tag{23}$$

$$h_t = o_t * \tanh c_t \tag{24}$$

where $f^t = 0$ represents complete blocking of information, $f^t = 1$ denotes passing information, and the notations are defined in Table 1.

Table 1. Parameters of two-layer LSTM predictor.

Parameters	Representations
σ	Sigmoid function
tanh	Hyperbolic tangent function
i_t	Input gate
f_t	Forgot gate
o_t	Output gate
c_t	State of current memory cell at time t
$\tilde{c}_t$	Candidate value for state at time t
h_t	Output value
x_t	Input value
W_i, w_f, w_o, w_c	Weights
R_i, R_f, R_o, R_c	Weights
b_i, b_f, b_o, b_c	Bias vectors of three gates
$*$	Element-wise multiplication

In this paper, the mean squared error (MSE) is the loss function in the predictor network. MSE is popular as a measure because it is sensitive to outliers and provides greater penalties [43]. MSE can be formulated as

$$MSE = \frac{1}{L}\sum_{i=1}^{L} e_i \tag{25}$$

$$e_i = \frac{1}{Q_1 Q_2}\sum_{Q_1,Q_2}\left(H''_{Q_1,Q_2} - \tilde{H}_{Q_1,Q_2}\right)^2 \tag{26}$$

where L represents the number of channel samples, e_i is the $Q_1 \times Q_2$ element-wise mean squared error, and H'' and $\tilde{H}$ denote the real measurement after SGF-HOCM processing and the predicted value of LSTM network, respectively. Wireless channel prediction is achieved by first SGF-HOCM processing an estimation sequence $\hat{H}_a$, and then forecasting the future channel value $\tilde{H}_a(t+1)$.

Through the above two-layer LSTM predictor, we aim to track time-variant channel values. The parameters of the prediction network model are summarized in Table 2. In other words, we can directly use the observed channel estimation and the prediction values to perform the authentication in Section 3.3.

Table 2. Model parameters.

Parameters	Value
LSTM	2
Epoch	25
Batch size	32
Time step	10
Unit	50
Activation function	Relu
Optimizer	adam
Loss function	mean_squared_error

3.3. Prediction-Based Authentication Model

Once we obtain the predicted value $\tilde{H}_a(t+1)$ at time $t+1$, we will perform physical layer authentication. The proposed scheme constructs the authentication process based on the predicted channel information of legitimate nodes. The authentication problem in (9) is reconstructed as

$$\begin{cases} H_0 : MSE(\tilde{H}_a(t+1), H_i''(t+1)) < \eta, \\ H_1 : MSE(\tilde{H}_a(t+1), H_i''(t+1)) \geq \eta, \end{cases} \tag{27}$$

where $\tilde{H}_a(t+1)$ represents the predicted future characteristics of legitimate node A, and $H_i''(t+1)$ is the real observation. Since the wireless channel attributes are dynamic, we compare the predicted channel features with the real observations of time $t+1$, instead of comparing the values (i.e., $H_a''(t)$ and $H_i''(t+1)$) of two adjacent times to make authentication decisions. The MSE between the predicted value and the actual value is used as a metric. According to the information in (27), we obtain the acceptance region of legitimate node A. If the MSE between the predicted channel characteristics and the observed samples is greater than the threshold η, the transmission should be denied.

To evaluate the prediction and authentication results, two performance metrics (i.e., R^2 and Loss value) are used to measure the accuracy of the dynamic authentication model. For a prediction-based authenticator, higher R^2 means better authentication capability. For instance, $R^2 = 1$ indicates that the predicted data exactly matches the actual data. The predictor we trained perfectly predicts all the real time-varying information. If $R^2 = 0$, that is, each predicted value of the sample is equal to the mean value, then the trained authentication model has poor accuracy. The formula of R^2 can be expressed as

$$R^2 = 1 - \frac{MSE}{Var} \tag{28}$$

where Var is the variance and MSE is the mean squared error in (25). To sum up, we introduce the SGF-HOCM processing method and the authenticator based on LSTM prediction. In the dynamic learning model, we test a variety of combinations of processing steps to find the best-performing authenticator with LSTM prediction method. The results of dynamic authentication scheme are reported in the next section.

4. Results and Discussions

4.1. Measurement Setup

In this section, we use the channel information dataset provided by NIST in the automotive factory to simulate malicious attack scenarios. As shown in Figure 4, a typical multi-acre transmission assembly factory of the automotive industry is selected for radio frequency propagation measurement [45]. The floor size of the automotive factory is more than 400 m $\times$ 400 m. The ceiling is about 12 m high. In this scenario, a channel sounder system is used to take the measurements at a continuum of points throughout the facility by fixing the transmitter and moving the receiver at a constant rate. The analysis is based on channel impulse response data collected using equipment developed by NIST. The NIST channel sounder measurement system is a positive-negative sequence correlation system, which consists of a single sender with a power amplifier and a receiver [45]. The transmitter continuously transmits a sequence of positive–negative digital symbols modulated by a binary phased-shift keying signal, and is up-converted to a radio frequency carrier frequency. After passing through the power amplifier, the signal traverses the automotive factory and is detected by the channel sounder receiver. The statistics of channel estimates include frequency, expected value of the path loss exponent, delay, delay spread, and K-factor. The frequency is 5.4 GHz, the expected path loss exponent is 3.6, the delay is 644.4 ns, the delay spread is 177.4 ns, and the K-factor is 4.7 dB. The dataset splits into two sets: training (60,000 packets) and testing (2000 packets). From the training set, 10% of randomly selected samples are put aside and used for validation.

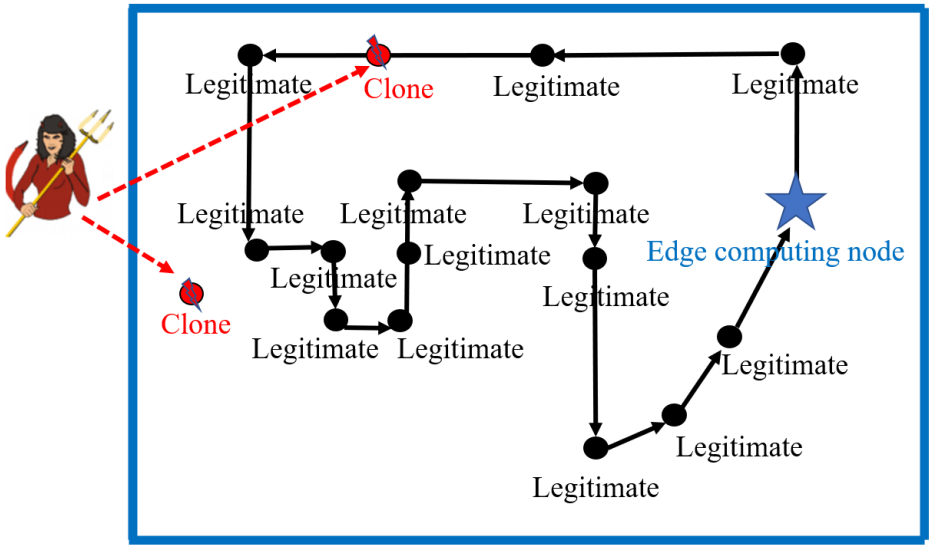

Figure 4. Simulation experiment under automotive assembly using NIST datasets. Fix the transmitter while moving the receiver at a constant rate to measure at continuous points throughout the entire facility.

4.2. Performance of Feature Extraction

In order to achieve denoising and feature extraction, we propose the SGF-HOCM method to process the channel estimates. This section first determines the optimal order cumulant to obtain the SGF-HOCM processing process. In the following section, we evaluate the effectiveness of using the proposed HOC3-based approach. The previously estimated channel data is divided into training and testing, in which 58,000 training samples are used for training the predictor, while 2000 testing samples are used for verification. The features extracted from different order domains are demonstrated in Figures 5–7. The simulation results certify the effectiveness of our HOC3 strategy. Because the third-order cumulant of channel estimation is superior to the second-order and fourth-order cumulants, the third-order cumulant is selected. The HOC3 preprocessing signal matches the measurement very well. The advantage of the HOC3 method in denoising is that it shows more promising performance, while the improvement in HOC2 and HOC4 methods is limited. We can observe that the SGF-HOCM step can extract useful features and minimize the impact of noise. According to the above description, we can reasonably select an optimal order cumulant for subsequent prediction during feature extraction process of time-varying channels. We utilize SGF-HOCM to preprocess the estimated values and provide training sample for the prediction model.

4.3. Comparison of Prediction Performance

As shown in Figures 8 and 9, to achieve accurate prediction of wireless channel information, two different preprocessing methods are compared. From Figures 8 and 9, we can see that, the predicted future values based on our proposed SGF-HOCM-assisted LSTM scheme match the real channel estimates very well. As described above, the denoising and dynamic feature extraction of channel sequences are important factors affecting the accuracy of the predictor. The performance of the prediction-based authenticator depends on the features of channel estimation, and the LSTM learning model could perform better with high complexity and strong time-varying series. Therefore, we introduced the SGF-HOCM processing method in dynamic authentication strategies to ensure the superiority of denoising.

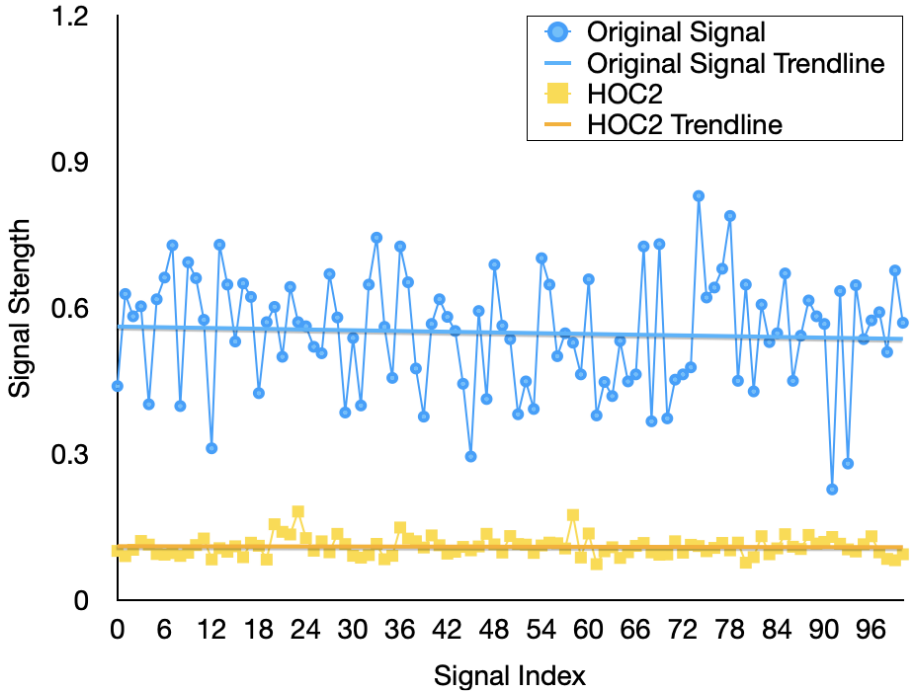

Figure 5. Extracted channel features using the different HOC2 methods.

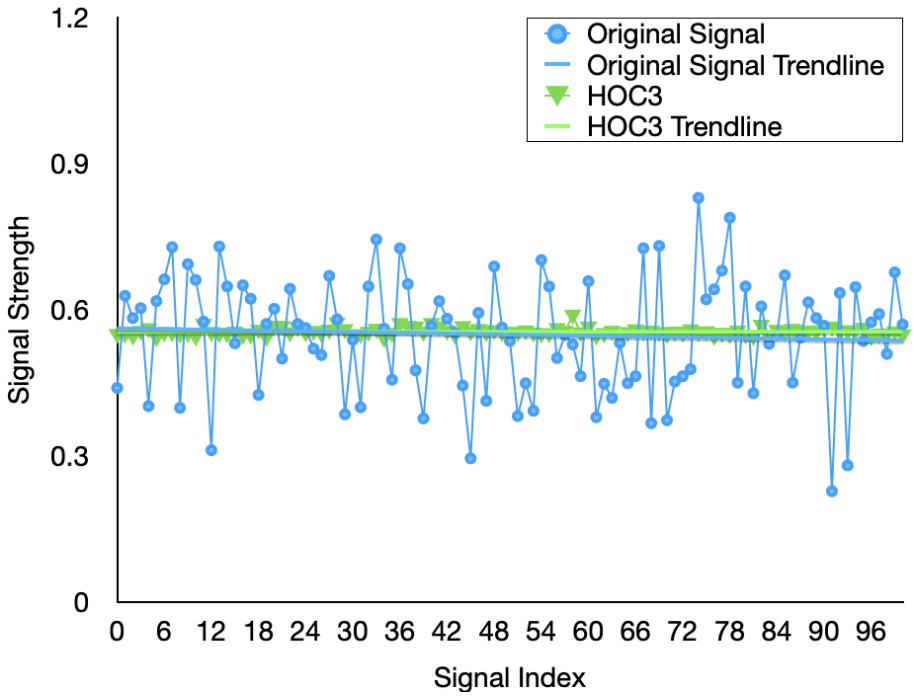

Figure 6. Extracted channel features using the different HOC3 methods.

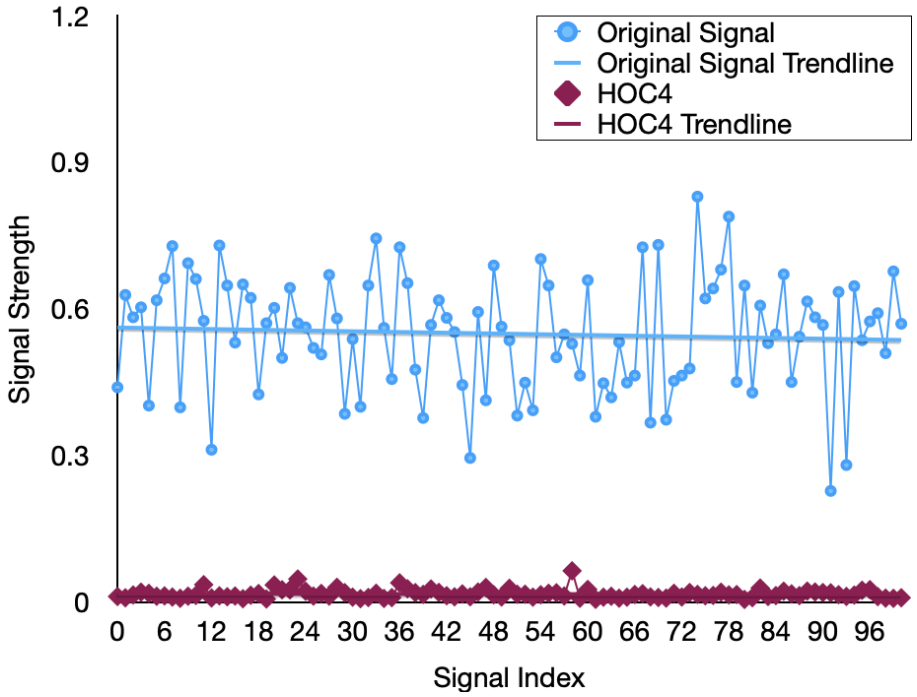

Figure 7. Extracted channel features using the different HOC4 methods.

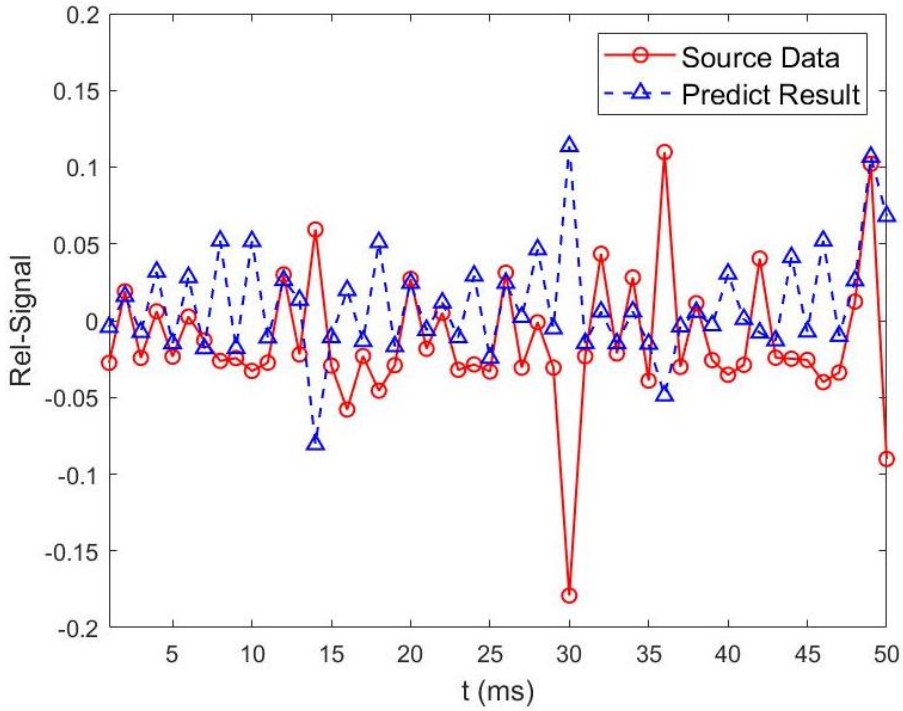

Figure 8. No preprocessing method is used for channel information prediction based on two-layer LSTM scheme.

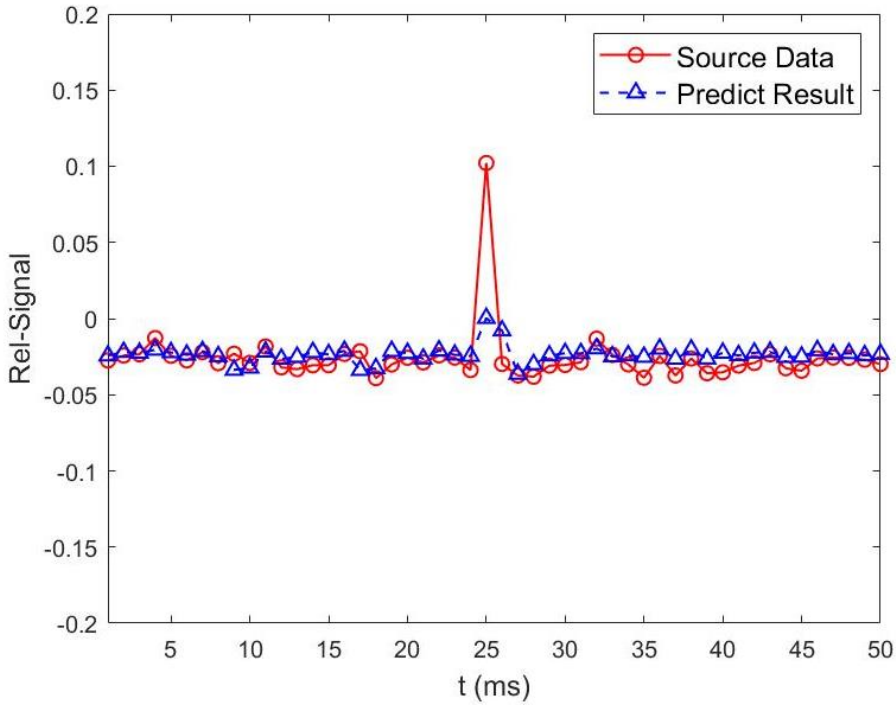

Figure 9. SGF-HOCM method is used for channel information prediction based on two-layer LSTM scheme.

4.4. Comparison of R^2 Performance

We compared the security performance of the predictor where R^2 has been applied for the authentication function. Figure 10 shows the R^2 curve of dynamic forecasting model. $R^2 > 0.8$ shows the forecasting performance, which is desirable for malicious node identification in wireless networks. We further discussed the potential reasons for using forth order polynominal in SGF-HOCM-assisted LSTM scheme.

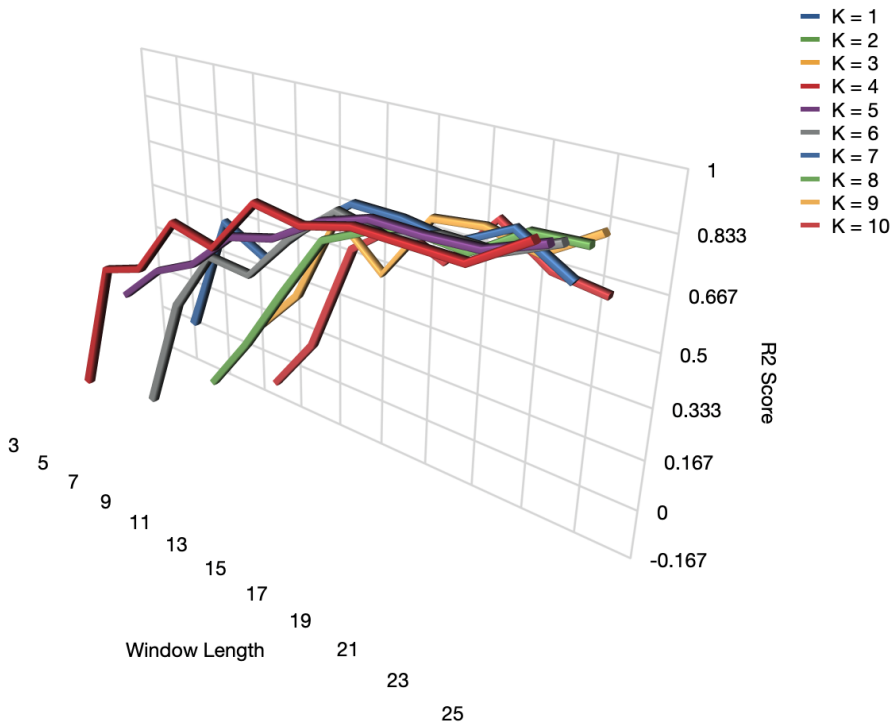

Figure 10. Performance of R^2 under different SGF parameters.

4.5. Training Performance

To capture the training performance of our proposed SGF-HOCM combined with LSTM approach, we provide the loss value of the network, as shown in Figure 11. We considered a two-layer LSTM network on the cloud, which is very useful in channel information prediction. From Figure 10, we know that $k = 4$ results in higher authentication performance. We can see from Figure 11 that the loss values of LSTM is approximately zero after the number of iterations is greater than 15. Note that when the proposed scheme can accurately predict future channel information, the verifier can compare the predicted values with the next actual observation results to achieve malicious attacker detection.

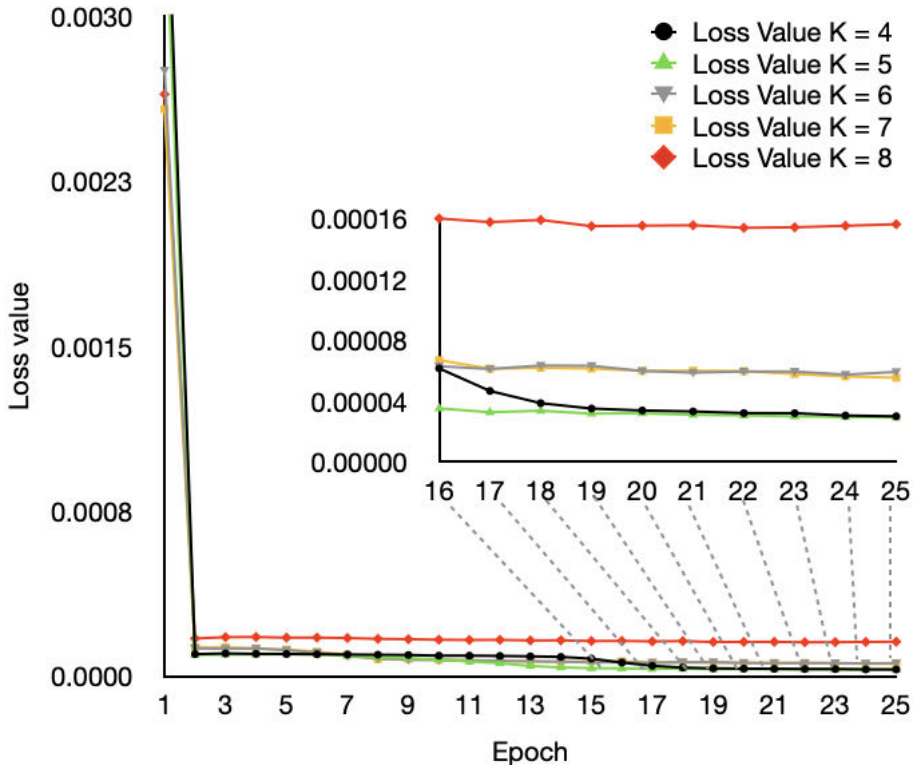

Figure 11. Training performance of the proposed SGF-HOCM-assisted LSTM scheme.

4.6. Authentication Performance

In addition, Figure 12 shows the impact of two important parameters in SGF on R^2, namely, the length of the window w and a kth order polynominal. From the table, we observe that when $k = 4$, R^2 achieves the best performance, which is $R^2 = 0.97$. The results represented by the green line have achieved high predictive performance. The SGF-HOCM-assisted LSTM scheme does not require key transmission, which avoids problems with possible key leakage. In addition, we note that increasing the number of layer and window length increases both accuracy and computational time overhead. Therefore, as shown in Figure 12, the proposed method uses a two-layer LSTM network with a window length of 25 to balance computation time and authentication performance. More importantly, physical layer security authentication does not depend on computational complexity and can accurately quantify security. By contrast, the key-based cryptography approach requires more time and complexity, which is problematic for sensor devices. Thus, given the potential of LSTM for PLUA in AIoT, dynamic authentication mechanisms have considerable interest in future IoT systems.

Window length\K	K = 1	K = 2	K = 3	K = 4	K = 5	K = 6	K = 7	K = 8	K = 9	K = 10
3	0.64	0.01								
5	0.75	0.48	0.35	0.01						
7	0.76	0.7	0.6	0.47	0.36	-0.06				
9	0.8	0.74	0.7	0.52	0.49	0.35	0.26	0.01		
11	0.69	0.8	0.71	0.71	0.56	0.56	0.65	0.21	0.25	0.01
13	0.79	0.85	0.81	0.68	0.69	0.55	0.58	0.44	0.41	0.21
15	0.77	0.78	0.83	0.85	0.73	0.71	0.72	0.66	0.71	0.59
17	0.74	0.73	0.85	0.83	0.82	0.83	0.83	0.73	0.58	0.7
19	0.82	0.86	0.87	0.87	0.87	0.8	0.83	0.77	0.79	0.64
21	0.63	0.89	0.85	0.87	0.87	0.85	0.81	0.76	0.81	0.81
23	0.6	0.87	0.88	0.87	0.88	0.85	0.89	0.86	0.78	0.71
25	0.72	0.85	0.91	0.97	0.94	0.92	0.8	0.87	0.88	0.69

Figure 12. R^2 authentication performance of the proposed scheme.

We demonstrate the superiority of our proposed SFG-HOCM-assisted LSTM scheme by comparing with the traditional RNN scheme, which only exploited HOC to model the time-varying channel. Figure 13 shows a clear comparison of accuracy between LSTM method and RNN approach under different signal-to-noise ratios. Our SGF-HOCM-assisted LSTM scheme shows a more promising performance due to the superiority of LSTM in predicting future channel characteristics, and it has a significant improvement when exploiting SGF-HOCM preprocessing, while the traditional method only shows limited promotion.

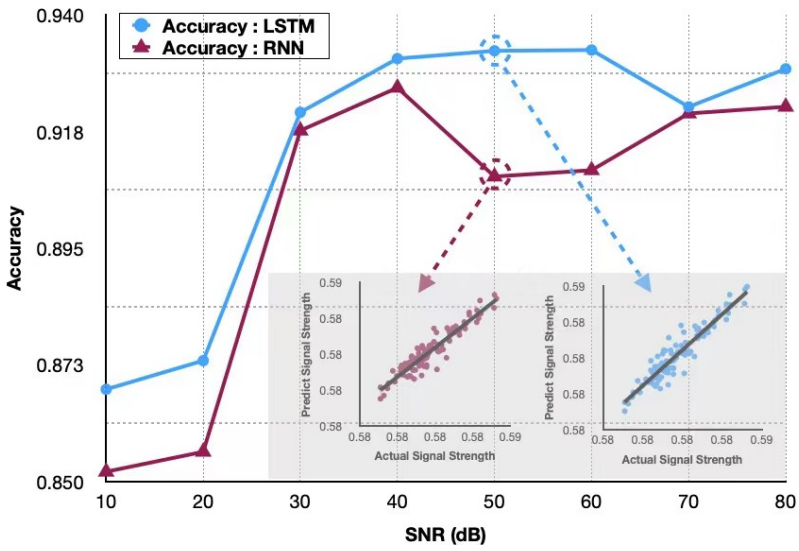

Figure 13. Authentication accuracy comparison between proposed LSTM scheme and the traditional RNN scheme.

5. Conclusions

In this work, we have developed a dynamic authentication mechanism to address the security challenges in next-generation AIoT networks. We adopted SGF-HOCM processing method to extract time-varying characteristics based on physical layer attributes. We used a two-layer LSTM algorithm to predict future channel vectors based on existing channel information, and compared them with observed channel variations extracted from the transmitter to perform security detection. We proposed an intelligent authentication scheme, which only needs the channel information of legitimate nodes, and avoids using the channel model of spoofing devices. Finally, we conducted a simulation using the dataset from the National Institute of Standards and Technology, demonstrating the advantages of the proposed dynamic authentication scheme.

This channel prediction-based security authentication scheme was shown to achieve a very high accuracy compared to other methods. Although the maximum accuracy is high, $R^2 = 0.97$, there is room for future work. One is in the area of preprocessing engineering and feature selection with the goal of creating better prediction-based models. Although the SGF-HOCM feature vector that is based on Savitzky–Golay filter and HOCM method have been used successfully, other attribute characteristics are possible, and the use of more than two filters could be considered. The training efficiency of LSTM is much lower than that of traditional RNN under the same computational power. LSTM alleviates the long-term dependency problem of RNN, but for longer sequence data, it requires higher computational complexity and longer training time. Another important study would be to implement this security algorithm in a real AIoT system in order to evaluate its performance under real conditions and in different scenarios.

Author Contributions: Conceptualization, X.Q.; methodology, X.Q.; software, J.Y.; validation, J.Y. and X.Q.; formal analysis, X.Q.; investigation, X.Q. and J.Y.; resources, X.Q.; data curation, J.Y. and X.Q.; writing—original draft preparation, X.Q.; writing—review and editing, X.Q., W.Z., G.L. and X.S.; visualization, J.Y. and X.Q.; supervision, X.Q.; project administration, X.Q.; funding acquisition, X.Q., W.Z. and G.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by R&D Program of Beijing Municipal Education Commission under grant no. KM202211232012.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: NIST datasets are available at http://doi.org/10.18434/T44S3N, accessed on 1 January 2023.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhong, A.; Li, Z.; Wu, D.; Tang, T.; Wang, R. Stochastic Peak Age of Information Guarantee for Cooperative Sensing in Internet of Everything. *IEEE Internet Things J.* **2023**. [CrossRef]
2. Tang, T.; Li, L.; Wu, X.; Chen, R.; Li, H.; Lu, G.; Cheng, L. TSA-SCC: Text Semantic-Aware Screen Content Coding with Ultra Low Bitrate. *IEEE Trans. Image Process.* **2022**, *31*, 2463–2477. [CrossRef]
3. Li, Z.; Zhu, N.; Wu, D.; Wang, H.; Wang, R. Energy-Efficient Mobile Edge Computing under Delay Constraints. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 776–786. [CrossRef]
4. Li, Z.; Zhou, Y.; Wu, D.; Tang, T.; Wang, R. Fairness-Aware Federated Learning with Unreliable Links in Resource-Constrained Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 17359–17371. [CrossRef]
5. Wasilewska, M.; Bogucka, H.; Poor, H.V. Secure Federated Learning for Cognitive Radio Sensing. *IEEE Commun. Mag.* **2023**, *61*, 68–73. [CrossRef]
6. Wang, C.X.; You, X.; Gao, X.; Zhu, X.; Li, Z.; Zhang, C.; Wang, H.; Huang, Y.; Chen, Y.; Haas, H.; et al. On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 905–974. [CrossRef]
7. Li, Z.; Li, F.; Tang, T.; Zhang, H.; Yang, J. Video caching and scheduling with edge cooperation. *Digit. Commun. Netw.* 2022, *in press*. [CrossRef]
8. Zhang, Z.; Liu, Y.; Huang, J.; Zhang, J.; Li, J.; He, R. Channel Characterization and Modeling for 6G UAV-Assisted Emergency Communications in Complicated Mountainous Scenarios. *Sensors* **2023**, *23*, 4998. [CrossRef]
9. Zhang, X.; Hu, M.; Xia, J.; Wei, T.; Chen, M.; Hu, S. Efficient Federated Learning for Cloud-Based AIoT Applications. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2021**, *40*, 2211–2223. [CrossRef]
10. Rathee, G.; Garg, S.; Kaddoum, G.; Choi, B.J.; Hassan, M.M.; AlQahtani, S.A. TrustSys: Trusted Decision Making Scheme for Collaborative Artificial Intelligence of Things. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1059–1068. [CrossRef]
11. Cheng, S.-M.; Hong, B.-K.; Hung, C.-F. Attack Detection and Mitigation in MEC-Enabled 5G Networks for AIoT. *IEEE Internet Things Mag.* **2022**, *5*, 76–81. [CrossRef]
12. Zhang, C.; Yuan, X.; Zhang, Q.; Zhu, G.; Cheng, L.; Zhang, N. Toward Tailored Models on Private AIoT Devices: Federated Direct Neural Architecture Search. *IEEE Internet Things J.* **2022**, *9*, 17309–17322. [CrossRef]
13. Mitev, M.; Chorti, A.; Poor, H.V.; Fettweis, G.P. What Physical Layer Security Can Do for 6G Security. *IEEE Open J. Veh. Technol.* **2023**, *4*, 375–388. [CrossRef]
14. Lu, X.; Xiao, L.; Li, P.; Ji, X.; Xu, C.; Yu, S.; Zhuang, W. Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 425–466. [CrossRef]

15. Guo, H.; Li, J.; Liu, J.; Tian, N.; Kato, N. A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 53–87. [CrossRef]
16. Rahman, M.A.; Hossain, M.S. A Deep Learning Assisted Software Defined Security Architecture for 6G Wireless Networks: IIoT Perspective. *IEEE Wirel. Commun.* **2022**, *29*, 52–59. [CrossRef]
17. Mahmood, N.H.; Berardinelli, G.; Khatib, E.J.; Hashemi, R.; Lima, C.D.; Latva-aho, M. A Functional Architecture for 6G Special-Purpose Industrial IoT Networks. *IEEE Trans. Ind. Inform.* **2023**, *19*, 2530–2540. [CrossRef]
18. Nguyen, V.-L.; Lin, P.-C.; Cheng, B.-C.; Hwang, R.-H.; Lin, Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428.
19. Xiong, Z.; Cai, Z.; Takabi, D.; Li, W. Privacy Threat and Defense for Federated Learning with Non-i.i.d. Data in AIoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1310–1321. [CrossRef]
20. Li, W.; Wang, N.; Jiao, L.; Zeng, K. Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks. *IEEE Access* **2021**, *9*, 60419–60432. [CrossRef]
21. Qiu, X.; Jiang, T.; Wu, S.; Hayes, M. Physical Layer Authentication Enhancement Using a Gaussian Mixture Model. *IEEE Access* **2018**, *6*, 53583–53592. [CrossRef]
22. Wang, X.; Jia, P.; Shen, X.S.; Poor, H.V. Intelligent and Low Overhead Network Synchronization for Large-Scale Industrial IoT Systems in the 6G Era. *IEEE Netw.* 2022, *early access*. [CrossRef]
23. Fang, H.; Wang, X.; Tomasin, S.; Al-Dhahir, N. Lightweight Group Authentication for Decentralized Edge Collaboration. *IEEE Commun. Mag.* **2022**, *60*, 124–129. [CrossRef]
24. Fang, H.; Xiao, Z.; Wang, X.; Al-Dhahir, N. Lightweight Flexible Group Authentication Utilizing Historical Collaboration Process Information. *IEEE Trans. Commun.* **2023**, *71*, 2260–2273. . [CrossRef]
25. Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Khyam, M.O.; He, J.; Pesch, D.; Moessner, K.; Saad, W.; Poor, H.V. 6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities. *Proc. IEEE* **2022**, *110*, 712–734. [CrossRef]
26. Ferdowsi, A.; Saad, W. Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems. *IEEE Trans. Commun.* **2019**, *67*, 1371–1387. [CrossRef]
27. Liu, W.; Xu, X.; Li, D.; Qi, L.; Dai, F.; Dou, W.; Ni, Q. Privacy Preservation for Federated Learning with Robust Aggregation in Edge Computing. *IEEE Internet Things J.* **2022**, *10*, 7343–7355. [CrossRef]
28. Gao, N.; Qin, Z.; Jing, X.; Ni, Q.; Jin, S. Anti-Intelligent UAV Jamming Strategy via Deep Q Networks. *IEEE Trans. Commun.* **2020**, *68*, 569–581. [CrossRef]
29. Gao, N.; Ni, Q.; Feng, D.; Jing, X.; Cao, Y. Physical Layer Authentication under Intelligent Spoofing in Wireless Sensor Networks. *Signal Process.* **2020**, *166*, 107272. [CrossRef]
30. Wang, N.; Li, W.; Jiao, L.; Alipour-Fanid, A.; Xiang, T.; Zeng, K. Orientation and Channel-Independent RF Fingerprinting for 5G IEEE 802.11ad Devices. *IEEE Internet Things J.* **2022**, *9*, 9036–9048. [CrossRef]
31. Wang, N.; Jiao, L.; Wang, P.; Li, W.; Zeng, K. Exploiting Beam Features for Spoofing Attack Detection in mmWave 60-GHz IEEE 802.11ad Networks. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 3321–3335. [CrossRef]
32. Zhang, H.; Zeng, K.; Lin, S. Federated Graph Neural Network for Fast Anomaly Detection in Controller Area Networks. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 1566–1579. [CrossRef]
33. Xing, Y.; Hu, A.; Zhang, J.; Peng, L.; Wang, X. Design of A Channel Robust Radio Frequency Fingerprint Identification Scheme. *IEEE Internet Things J.* **2022**, *10*, 6946–6959. [CrossRef]
34. Benaddi, H.; Jouhari, M.; Ibrahimi, K.; Benslimane, A.; Amhoud, E.M. Adversarial Attacks Against IoT Networks using Conditional GAN based Learning. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 2788–2793.
35. Guo, D.; Cao, K.; Xiong, J.; Ma, D.; Zhao, H. A Lightweight Key Generation Scheme for the Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 12137–12149. [CrossRef]
36. Junejo, A.K.; Benkhelifa, F.; Wong, B.; Mccann, J.A. LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks. *IEEE Internet Things J.* **2022**, *9*, 4110–4124. [CrossRef]
37. Senigagliesi, L.; Baldi, M.; Gambi, E. Comparison of Statistical and Machine Learning Techniques for Physical Layer Authentication. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1506–1521. [CrossRef]
38. Ghaddar, N.; Kim, Y.-H.; Milstein, L.B.; Ma, L.; Yi, B.K. Joint Channel Estimation and Coding over Channels with Memory Using Polar Codes. *IEEE Trans. Commun.* **2021**, *69*, 6575–6589. [CrossRef]
39. Zhang, Y.; Venkatesan, R.; Dobre, O.A.; Li, C. Efficient Estimation and Prediction for Sparse Time-Varying Underwater Acoustic Channels. *IEEE J. Ocean. Eng.* **2020**, *45*, 1112–1125. [CrossRef]
40. Vinogradova, J.; Fodor, G.; Hammarberg, P. On Estimating the Autoregressive Coefficients of Time-Varying Fading Channels. In Proceedings of the 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 19–22 June 2022; pp. 1–5. [CrossRef]
41. Mattu, S.R.; Theagarajan, L.N.; Chockalingam, A. Deep Channel Prediction: A DNN Framework for Receiver Design in Time-Varying Fading Channels. *IEEE Trans. Veh. Technol.* **2022**, *71*, 6439–6453. [CrossRef]
42. Zhong, Y.; Yang, Y.; Zhu, X.; Dutkiewicz, E.; Zhou, Z.; Jiang, T. Device-Free Sensing for Personnel Detection in a Foliage Environment. *IEEE Geosci. Remote Sens. Lett.* **2017**, *14*, 921–925. [CrossRef]

43. Gwon, H.; Lee, C.; Keum, R.; Choi, H. Network Intrusion Detection based on LSTM and Feature Embedding. *arXiv* **2019**, arXiv:1911.11552.
44. Kumar, S.; Kumar, D.; Donta, P.K.; Amgoth, T. Land Subsidence Prediction using Recurrent Neural Networks. *Stoch. Environ. Res. Risk Assess.* **2021**, *36*, 373–388. [CrossRef]
45. Candell, R.; Remley, K.A.; Moaveri, N. Radio frequency measurements for selected manufacturing and industrial environments. *NIST Tech. Rep.* **2016**. [CrossRef]