ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

Wireless Sensor Network Physical Layer Authentication Technology Based on Dynamic Prediction of Electromagnetic Fingerprints

Dai Hang[1,a], Jin Jing[2,3,b,*]

[1]*Wuhan University of Technology, Wuhan, China*
[2]*Chn Energy Zhishen Control Technology Co. Ltd.*
[3]*Beijing Engineering Research Center of Power Station Automation, Beijing, China*
[a]*1021323918@qq.com,* [b]*12111534@chnenergy.com.cn*
**Corresponding author*

Abstract: *The physical layer characteristics of the signal, such as electromagnetic fingerprints, will change with the time-varying channel's variation under the influence of various factors, so that the reliability of traditional electromagnetic fingerprint authentication systems that don't consider the dynamic changes of electromagnetic fingerprints would be reduced. In this paper, we explore and design a wireless sensor network physical layer authentication mechanism based on electromagnetic fingerprint dynamic prediction to improve the reliability of the authentication system. This system uses the LSTM network to learn and predict the dynamic of electromagnetic fingerprints affected by wireless channels and combines the unique electromagnetic fingerprint differences of legal transmitters with the channel corresponding changes to transceivers to improve the difference between the electromagnetic fingerprints from legitimate communication and the attack link, further improving the accuracy of electromagnetic fingerprint authentication. In addition, the LSTM network can also find the abnormal data and learn through continuous adaptive training to improve the detection probability.*

Keywords: *Time-varying channel, physical layer authentication, electromagnetic fingerprint, LSTM network*

1. Introduction

Identity authentication is the basis for preventing spoofing attacks and ensuring communication security in wireless sensor networks while the traditional authentication mechanisms based on upper-layer encryption has some problems when used in wireless sensor networks[1].First of all, wireless sensors are easily broken by attackers with strong computing power due to its low computing power which couldn't carry high-complexity encryption algorithms[2].Secondly, it is easy for attackers to obtain from the air interface and carry out spoofing arracks when the wireless sensor network performs the first authentication and the device identity ID will be sent in cleartext on the channel[3].In summary, we can see that the identity authentication mechanism based on upper-layer encryption is difficult to apply to wireless sensor networks with limited energy consumption and computer power. In order to solve the above problems, physical layer security technology has been proposed in recent years[4].

At present, physical layer security technology are mainly divided into the following three categories: physical layer security(PLS)[5],physical layer key generation(PLKG)[6]and physical layer authentication(PLA)[7].Among them PLS which performs encrypted transmission by using the transmission characteristics of the physical layer instead of key setting makes the authentication process simpler. Hence the encrypted information can only be transmitted to the recipient and the attacker cannot decode the sent encrypted information[8].The current feasible schemes of PLS include: injecting noise into the channel to deteriorate the communication quality of the spoofing channel[9]and plasticizing the wave speed of the transmitted signal to make it unacceptable to the attacker[10]. PLKG provides a key agreement channel between legitimate senders and receivers through a random broadcast channel which can be accessed by both receivers and attackers, but the results they observed are different. Because the key extracted in the channel between the sender and the receiver is random, the attacker cannot extract the same key as the receiver and the protecting legitimate information transmission is achieved.[11].Compared with the previous two schemes, the PLA which based on electromagnetic fingerprint of the communication signal or the channel information shared by the sender and receiver for

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

authentication is more secure and efficient, additionally it occupies less resources[12].First, the physical layer features provided by PLA will be affected by noise during transmission, which makes it difficult for attackers to extract the information and deduce the key. Although the legitimate receiver will also receive physical layer feature information affected by noise, it is easier to process this information than for attackers. This advantage that can be explained based on Shannon's analysis of information-theoretic secrecy; Second, PLA allows legitimate receivers to quickly distinguish legitimate senders from rogue senders without upper-layer processing, which obviously saves computational complexity and processing delays; Third, PLA provides high compatibility because incompatible devices may not be able to decode each other's upper layer signalling but should be able to successfully decode physical layer bit-streams in heterogeneous coexistence systems; At last, The PLA scheme aims to compensate the upper-layer authentication scheme and provide a higher level of security. Specifically, the upper-layer authentication mechanism is used to authenticate the identity of the legitimate user while the PLA mechanism is used to authenticate the device used by the legitimate user[13].Hence, this paper will pay more attention to physical layer authentication(PLA).

The electromagnetic fingerprint contained in the RF signal is one of the main features used in PLA certification, which is derived from the unique intrinsic errors in the production process of the equipment's RF devices. There are two types of electromagnetic fingerprints named steady and transient fingerprints. The transient fingerprint is mainly extracted from the electromagnetic emission signal generated when the radio frequency device is turned on or off. The envelope and phase contain the unique intrinsic process error of the radio frequency device, they are not affected by the modulation information[14].However its application range is limited for the influence of SNR and the difficult capture. Steady fingerprints are mainly illustrated by the unique frequency offset, I/Q offset, amplitude phase error and other radio frequency characteristics of the communication signal[15]. The steady fingerprint is so much more stable than the transient one that the fingerprint extraction based on the steady response was more widely used. The transmitted signal is affected by the channel and changes and the electromagnetic fingerprint will also be affected, resulting in the damage and dynamic change at the receiving end affecting the identity authentication. At present, a method based on machine learning is created to solve this problem. This method establishes an integrated learning model for the changes and uses random forest and Adaboost solutions to identify and predict electromagnetic fingerprints respectively[16]. But the prediction effect of the random forest scheme is poor in the case of large noise, and the training of the Adaboost scheme and requires a long time and a large storage space.

In order to solve the above problems, this paper proposes a wireless sensor network physical layer authentication mechanism based on electromagnetic fingerprint dynamic prediction. This mechanism can continuously predict the dynamic changes of the channel and electromagnetic fingerprints at the authentication end then match them with the received electromagnetic fingerprints. Since the channel change is coherent in a certain time, the channel has a strong correlation with the change of the electromagnetic fingerprint in the coherent time. Based on this characteristic, this mechanism uses the LSTM network model to solve the problem of wrong judgment and omission of authentication caused by the damaged and dynamic change of the electromagnetic fingerprint received by the receiving end. The adaptive learning of LSTM network can also solve the problem of excessive storage resource consumption of the current parameter modeling method and improve the accuracy of prediction. The electromagnetic fingerprint authentication algorithm based on LSTM network makes full use of the electromagnetic fingerprint of radio frequency equipment and the information of the channel space fading fingerprint to turns the influence of the channel on the electromagnetic fingerprint into a benefit. This paper constructs a 3-layer LSTM network to learn the Rice channel, predict the change of the electromagnetic fingerprint and evaluate the fingerprint quantitatively by Euclidean distance. In addition, we use MATLAB and Pycharm to simulate and verify the proposed algorithm, then comparing with the traditional algorithm shows that the physical layer authentication mechanism of wires sensor network based on electromagnetic fingerprint dynamic prediction can be achieved under certain conditions with accuracy of 97%.

The contributions of this paper are summarized as follows:

1) Constructing a LSTM network model for the problem that the electromagnetic fingerprint is affected by the channel, proposing an electromagnetic fingerprint channel simulation algorithm based on LSTM, realizing the dynamic prediction of electromagnetic fingerprint based on the slow time-varying Rice channel.

2) Constructing an identity authentication mechanism based on dynamic electromagnetic fingerprint prediction which can combine the newly arrived fingerprint information with the device fingerprint information and learn the dynamic changes of the channel adaptively, then analyse the received

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

fingerprint information and the prediction to detect abnormal fingerprints.

The rest of this paper is organized as follows: In Section 2, the authentication model is presented; In Section 3, the proposed algorithm is introduced; In Section 4, the simulation analysis of the algorithm is carried out; In Chapter 5, the final conclusions are given.

2. System model

As shown in Figure 1, considering an authentication scenario under the time-varying situation consisted of Alice, Bob and Eve.Alice is the sender of the signal, Bob receive the signal and Eve is the attacker. Alice and Bob know the channel information between them each other and they could use the pilot to measure the channel information in advance. During the first communication Alice and Bob use the upper-layer encryption protocol to establish preliminary authentication, at that time, Bob can extract Alice's relevant identity information such as the electromagnetic fingerprint through the received signals. After that, when Bob receives the signal whose identity information is Alice, he will put it through the LSTM network to generate the predicted the next moment value and store it. Bob will compare the identity information received at next time with the predicted value of the signal generated by the stored value LSTM network. If the authentication passes, the reception would be successful; If the authentication fails, the signal is considered to be from another illegal person. The attacker Eve couldn't know the channel information between Alice and Bob, His goal is to attack the communication link by extracting Alice's identity information and listening to the signal to extract Alice's identity information. It is difficult for Eve to observe the channel information between Alice and Bob, but he can obtain the identity information and communication protocol information contained in the signal sent by Alice.

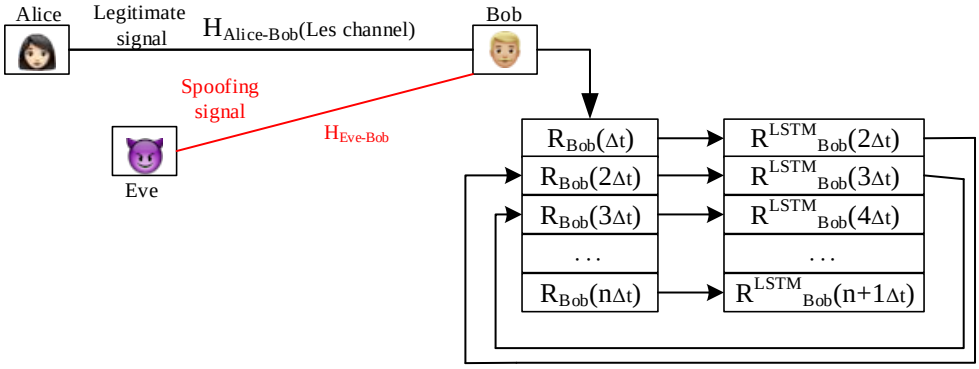

Figure 1: The communication between Alice and Bob was attacked by Eve and made a judgment

Bob's main purpose is to identify the sender through physical layer authentication, assuming that the electromagnetic fingerprint of the signal sent by Alice can be expressed as $R_{Alice} = [R_1, R_2, ..., R_N]$, Each R_x represents the N electromagnetic fingerprint related features sent by Alice, such as frequency offset, constellation offset, etc. The communication channel between Alice and Bob is assumed to be a Rice channel dominated by a direct path, expressed as $h_{Alice-Bob} = \frac{z}{\sigma_n^2}\exp\left[-\frac{1}{2\sigma_n^2}\left(z^2+A^2\right)\right]I_0\left(\frac{A_Z}{\sigma_n^2}\right), z \geq 0$. n means that the signal transmission process is affected by noise and other factors, then the fingerprint information contained in the signal received by Bob is:

$$R_{Bob} = R_{Alice} * h_{Alice-Bob} + n \tag{1}$$

In order to simulate the process of the electromagnetic fingerprint affected by the channel, we need to compare the electromagnetic fingerprint $R_{Bob}\left[(n+1)\Delta t\right]$ received by Bob with the electromagnetic fingerprint $R_{\text{Bob}}^{LSTM}\left[(n+1)\Delta t\right]$ predicted by the received signal at the previous moment, Δt represents the pilot interval. Assume that the first authentication between Alice and Bob is based on the upper layer encryption mechanism, after the authentication is successful, Bob extracted and store the

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

electromagnetic fingerprint then compared it with the authentication at the next moment.

When Alice and Bob communicate legally, the change of the electromagnetic fingerprint received by Bob from time $n\Delta t$ to time $(n+1)\Delta t$ can be expressed as:

$$Y[n] = R_{Bob}[(n+1)\Delta t] - R_{Bob}^{LSTM}[(n+1)\Delta t] \tag{2}$$

$$R_{Bob}^{LSTM}[(n+1)\Delta t] = f_{LSTM}[R_{Bob}(n\Delta t)]$$

f_{LSTM} is the electromagnetic fingerprint prediction network based on LSTM.

Since the channel changes very slowly within the coherence time, if Δt is in the coherence time the electromagnetic fingerprints received by Bob at time $n\Delta t$ and time $(n+1)\Delta t$ have greater coherence, we can make a prediction on the changing process of electromagnetic fingerprint based on this characteristic. The judgement process can be expressed as follows:

$$\begin{Bmatrix} \Psi_0 : 0 < Y[n] < u \\ \Psi_1 : u \le Y[n] \le 1 \end{Bmatrix} \tag{3}$$

u is the authentication threshold, Ψ_0 indicates that the information received by the receiver at this moment can be considered to be from Alice, and Ψ_1 indicates that the information received at this moment is from other attackers. In the case that the sender is known to be Alice, Ψ_0 indicates that the authentication is correct, and Ψ_1 indicates that there is a missed judgment.

If Eve steals and disguises the identity information sent by Alice and sends information to Bob, the electromagnetic fingerprint of the signal sent by Eve can be represented as $R_{Eve} = [R_1, R_2, ..., R_N]$, and the communication channel between Eve and Bob is represented as $H_{Eve-Bob}$, then Bob receives The fingerprint information contained in the signal is:

$$R_{Bob}' = R_{Eve} * H_{Eve-Bob} + n \tag{4}$$

At that time, the change of electromagnetic fingerprint is expressed as:

$$Y'[n] = R_{Bob}'[(n+1)\Delta t] - R_{Bob}^{LSTM}[(n+1)\Delta t] \tag{5}$$

Based on (3), the judgement of $Y'[n]$ can be expressed as:

$$\begin{Bmatrix} \Psi_0' : 0 < Y'[n] < u \\ \Psi_1' : u \le Y'[n] \le 1 \end{Bmatrix} \tag{6}$$

Ψ_0' indicates that the information received by the receiver at this moment can be considered to be from Alice, but in fact the information comes from the attacker Eve, and there is a misjudgement. Ψ_1' indicates that the received information is not from Alice, and the attacker's masquerading attack is successfully identified and rejected.

3. The communication system based on LSTM

During the transmission process, the signal will change according to the channel change. We established an electromagnetic fingerprint authentication mechanism based on LSTM network to predict the change of electromagnetic fingerprint in the channel to counteract the change of the channel, so that the receiving end can more accurately judge the signal acceptance. Then this section will give an introduction about each component of the LSTM network and describe the mechanism of the LSTM

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

network to predict the electromagnetic fingerprint.

The overall structure of the system is shown in Figure 2:

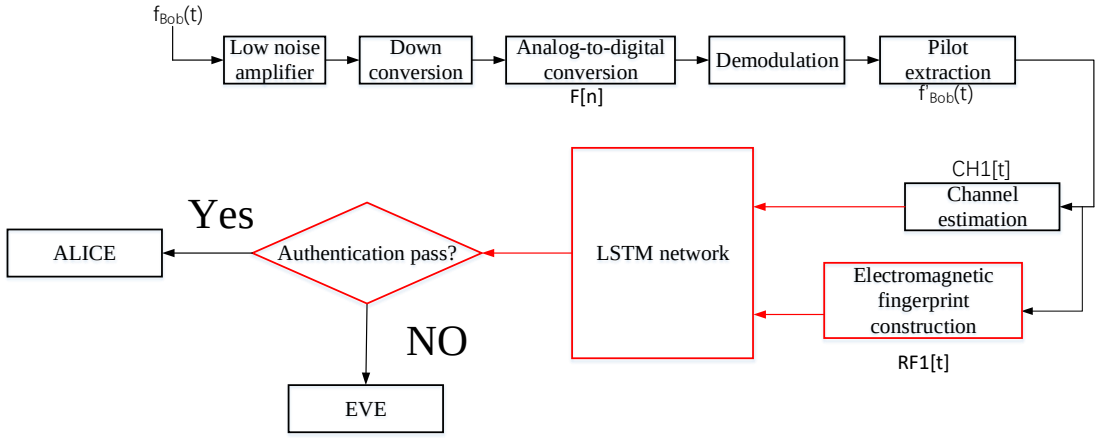

Figure 2: Overall structure of electromagnetic fingerprint authentication system based on LSTM

After Bob receiving the signal, receiver firstly processes the baseband analog signal through a low-noise amplifier and down-conversion, next performs analog-to-digital conversion and demodulation on the baseband analog signal, then extracts the pilot of the demodulated signal, estimates steady electromagnetic fingerprint information and channel information, finally inputs the estimated channel information and electromagnetic fingerprint information into the LSTM network for judgement. If the judgement is passed, it is considered that the received signal is from the legitimate communicator Alice; If the judgement is not passed, it is considered that the received signal is from the attacker Eve.

The LSTM network which based on the traditional neural network structure connects several repetitive neural network modules into a chain, and introduces a gate mechanism into the network to build a unique memory unit as shown in Figure 3:

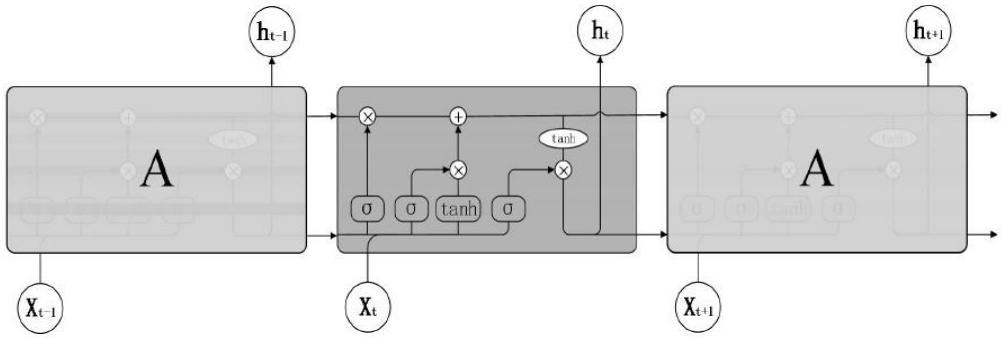

Figure 3: The construction of memory unit

The core of the memory cell's ability to transmit information is the two lines that traverse the entire connected structure. The upper line is used to update the state of the memory unit, while the lower line is used to decide which information needs to be forgotten and which information needs to be left. The control of forgetting and memory mainly depends on three gates namely forgetting gate, input gate and output gate. According to the special structure of the memory unit, the LSTM model constructed in this paper can be divided into three layers, namely the input layer, the hidden layer and the output layer. The electromagnetic fingerprint information at the next moment is predicted by inputting the electromagnetic fingerprint information and the channel information at this moment, the channel information at the next moment is predicted by inputting the channel information at this moment. The number of neurons in the input layer and output layer should be 2, the hidden layer should be 3 layers.

MSE is a convenient method for evaluating the average error. According to the value of the MSE loss function, the error between the predicted value and the actual value can be inferred. The smaller the MSE, the better the prediction effect of the model. We adopt the MSE arithmetic function as the error size between the predicted value and the actual value of electromagnetic fingerprint prediction. y_i represents the received electromagnetic fingerprint value, y_i' represents the electromagnetic fingerprint

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

predicted value, and n represents the number of predicted values. The MSE loss function can be expressed as:

$$MSE = \frac{\sum_{i=1}^{n} (y_i - y_i')^2}{n} \tag{7}$$

How to use the optimization algorithm to solve the minimum loss under the premise that the loss function has been defined is the core task of machine learning. Adam algorithm can use gradient first-order moment estimation and second-order moment estimation to automatically and dynamically adjust the learning rate in the training phase, it can also fix the learning rate to a certain range through bias correction to make the changes of each parameter tend to be stable; Meanwhile, it can adjust the dimension learning rate to avoid model oscillation, and there will be no deviation in the update speed of each dimension in the face of high-dimensional data; In addition, Adam can use the historical accumulated momentum to make the saddle point converge to a more reasonable position. Therefore, this paper chooses the Adam algorithm to optimize the prediction model. The steps are as follows:

$$m_t = \beta_1 m_{t-1} + (1-\beta_1) g_t \tag{8}$$

$$v_t = \beta_2 v_{t-1} + (1-\beta_2) g_t^2 \tag{9}$$

$$m_t' = \frac{m_t}{1-\beta_1^t} \tag{10}$$

$$v_t = \frac{v_t}{1-\beta_2^t} \tag{11}$$

$$\theta_t = \theta_{t-1} - \alpha \frac{m_t'}{\sqrt{v_t' + \varepsilon}} \tag{12}$$

t represents the current moment, g_t represents the current gradient, β_1 represents the mean of the derivative, β_2 represents the squared exponentially weighted average, m_t represents the exponential moving average, v_t represents the moving squared gradient, α represents the learning rate, and ε is a constant value of 10^{-8}.

With the LSTM prediction algorithm, this paper establishes a dynamic prediction and judgment mechanism for electromagnetic fingerprints, as shown in Figure 4 below.

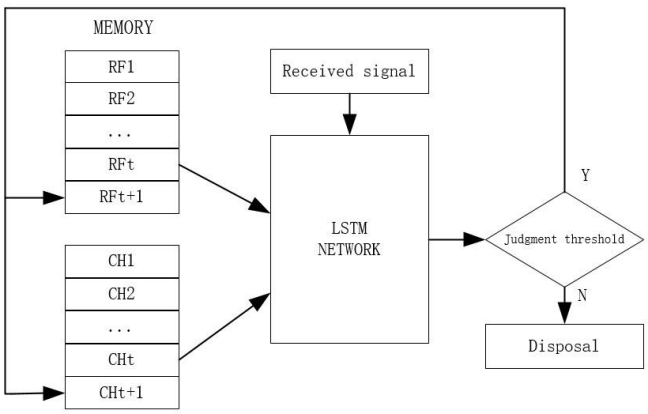

Figure 4: Schematic diagram of LSTM workflow

The algorithmic program in which LSTM works can be represented by Algorithm1

Algorithm 1: The theory of How LSTM works

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

Assuming that the initial authentication has been successful, the channel information and fingerprint information received at this time t and the previous time t-1 are all authenticated correctly and stored successfully

1) Receive channel information CH_t and fingerprint information RF_t at this moment.

2) Extract the stored channel information CH_{t-1} and fingerprint information RF_{t-1} at the last moment.

3) Using the LSTM network, calculate the channel information CH_t^{LSTM} at this moment according to the channel information CH_{t-1} at the previous moment.

4) According to the channel information RF_{t-1} at this moment calculated in the previous step and the fingerprint information RF_{t-1} received at the previous moment, Predict the fingerprint information RF_t^{LSTM} at this moment

5) Based on formula (3), compare RF_t and RF_t^{LSTM}, if it passes, it is considered that the received information is from Alice and then storing the received value; if it does not pass, it is considered that the received information is from Eve, and then discarding the received value.

4. Simulations and analysis

In this chapter, the performance of the authentication mechanism proposed in this paper and the prediction characteristics of the LSTM network are simulated and tested. We use MATLAB software to simulate the system by Monte Carlo method, the simulation generation of the channel uses the randn function in MATLAB to generate a Gaussian random variable with a specific mean variance. A Gaussian random variable with mean mu and variance sigma is generated to characterize the obedience to the channel parameters with mean μ and variance σ as: H=sqrt(sigma)*randn(1)+mu. It is also necessary to use a first-order autoregressive model to model the correlation of channel parameters at different times, where α is the correlation coefficient, and $u[t+1]$ represents a Gaussian distribution with a mean of 0 and a variance of 1 as follows:

$$H[t+1]=\alpha H[t]+\sqrt{(1-\alpha^2)\sigma}u[t+1] \tag{13}$$

The electromagnetic fingerprint feature is characterized by the offset of the constellation point, which is estimated based on the offset of the constellation point of the pilot. In this paper, the code written by pycharm software is used to predict electromagnetic fingerprints. The LSTM network needs to be trained according to the data in the training set to predict and compare the data changes in the test set. This simulation test collects the values predicted by the LSTM network under various conditions and uses MSE to quantify the prediction effect. We conducted 100 independent simulations for each situation, and set the MSE threshold to 0.2. The prediction result is less than this threshold indicating that the prediction is acceptable. The detection probability is the percentage of predicted acceptable results in 100 independent simulations, and the false alarm probability is the percentage of unacceptable results. In the simulation test, some other indicators such as noise intensity are set to 0dBm, transmit power varies from -10dBm to 10dBm, path attenuation factor varies from 2 to 2.5, and coherence time is set to 0.1ms.

The comparison algorithms used in this paper are selected as the following two categories:

comparison algorithm1: The received fingerprint information is directly matched with the stored fingerprint information without considering the influence of the channel. The algorithm needs to store the sender's electromagnetic fingerprint information such as constellation information and then quantify and compare the received fingerprint information constellation point offset with the stored fingerprint information constellation.

comparison algorithm2: Considering the influence of the channel, the fingerprints received before and after the time are directly used for matching. The algorithm makes predictions based on the electromagnetic fingerprint characteristics of the signals received before and after, such as changes in

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

constellation offsets, and then uses MSE for quantitative comparison.

This paper explores the influence of four different factors, signal correlation, signal-to-noise ratio of input signal, pilot density and input information amount on the prediction probability of the system, and compares and analyses with the above two comparison algorithms.

Set the signal-to-noise ratio of the signal to -3dB, the pilot interval to 1/2 of the coherence time, input the fingerprint information of the previous moment to the LSTM network for prediction, and change the correlation coefficient α in the channel model to represent the signal correlation, the resulting graph is shown in Figure 5. The stronger the signal correlation, the more accurate the predicted electromagnetic fingerprint. Algorithm 1 ignores the influence of channel dynamic changes on the signal, but the electromagnetic fingerprint information measured by the receiving end will change unpredictably compared to the stored electromagnetic fingerprint information, so the overall performance of algorithm 1 is the worst. Algorithm 2 takes into account the influence of channel changes, but only considers channel changes at adjacent moments. The insufficient number of samples leads to poor prediction performance, it is better than Algorithm 1 overall. The authentication system in this paper uses the LSTM network after data training to make predictions, so the overall prediction performance is better than Algorithm 1 and Algorithm 2, and it is significantly better than other algorithms under the condition of strong correlation, the detection probability can reach more than 97%.

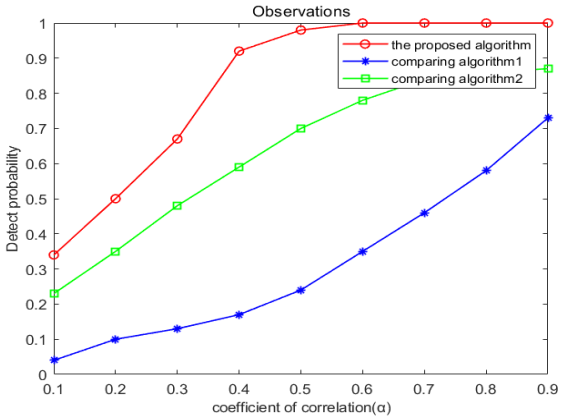

Figure 5: The effect of correlation on system detection probability

Set the correlation coefficient to 0.5, the pilot interval to 1/2 of the coherence time, input the fingerprint information of the previous moment to the LSTM network for prediction, and change the signal-to-noise ratio of the input signal. The result is shown in Figure 6. The greater the signal-to-noise ratio of the signal, the greater the proportion of effective information in the input system, and the better the prediction effect of the system. When the signal-to-noise ratio reaches -3dB, the system detection probability can reach more than 97%, which is obviously better than the other two types of algorithms.

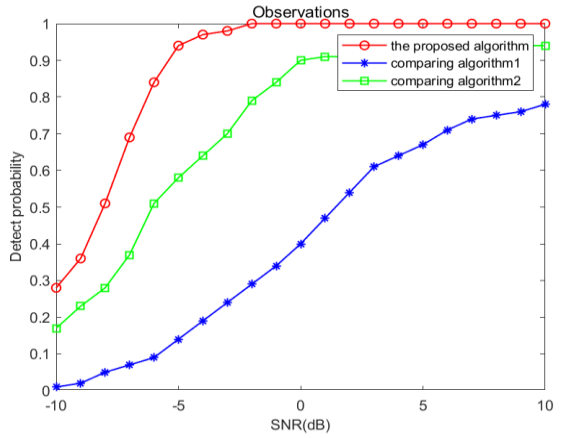

Figure 6: The effect of signal-to-noise ratio on detection probability

Set the correlation coefficient to 0.5 and the signal-to-noise ratio to -3dB, and input the fingerprint information of the previous moment to the LSTM network for prediction. A value δ is established to

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

represent the ratio of the pilot interval to the coherence time. The smaller the δ, the denser the pilots are, and the larger the δ, the longer the pilot interval. The result is shown in Figure 7. When the channel coherence time is greater than the pilot interval, the detection performance of the system is slightly better than that of the second algorithm, but when the channel coherence time is less than the pilot interval the performance of the second algorithm deteriorates sharply. The system can predict the change of the channel to evaluate the change range of the electromagnetic fingerprint beyond the coherence time and provide the authentication accuracy.

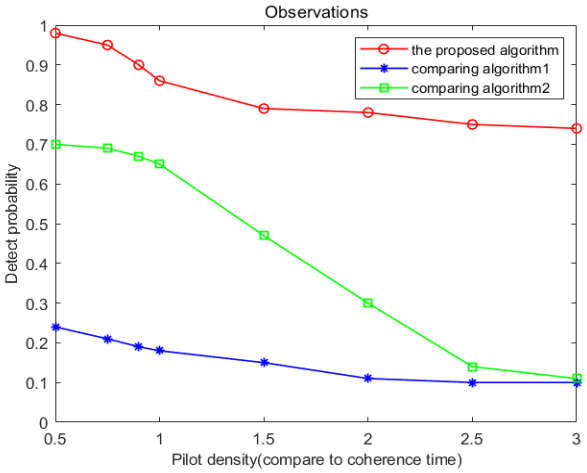

Figure 7: The effect of pilot density on detection probability

Finally, set the correlation coefficient to 0.4 and the signal-to-noise ratio to -3dB, input the fingerprint information of the n times to the LSTM network for prediction when the pilot interval is 1/2 and 2 times of the coherence time respectively, the result as shown in Figure 8. When the pilot frequency interval is smaller than the coherence time, the system can more accurately predict the change of channel information according to the results of data training. The more fingerprint information is input, the more accurate the prediction can be within a certain range. When the pilot interval is smaller than the coherence time, the system needs to predict and evaluate the channel variation beyond the variation range of the fingerprint information after the coherence time. The more fingerprint information is input, the more accurate the system will predict the change of fingerprint information beyond the coherence time. According to the results in the figure, after inputting the fingerprint information of the first three moments the detection probability of the two cases is not much different, so it is recommended to input the fingerprint information of the first three moments optimally.

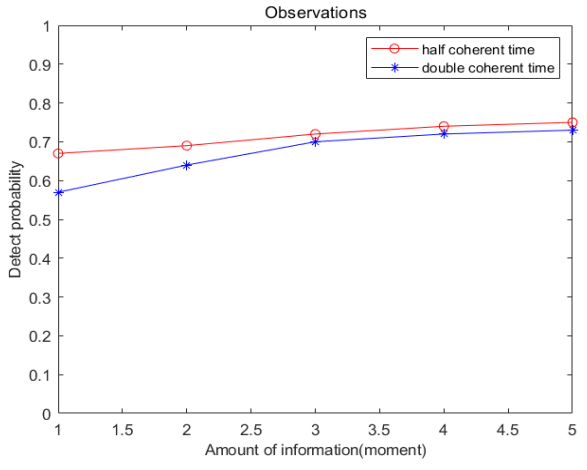

Figure 8: The effect of the amount of input information on detection probability

5. Conclusion

This paper explores and designs a wireless sensor network physical layer authentication mechanism based on electromagnetic fingerprint dynamic prediction. By using the LSTM network to dynamically

ISSN 2616-5775 Vol. 5, Issue 11: 18-27, DOI: 10.25236/AJCIS.2022.051103

predict the changes of the signal in the channel to improve the success rate of the electromagnetic fingerprint authentication mechanism to better protect the communication. In the simulation test, the influence of different factors on the prediction reliability of the system is tested and the detection probability is compared with the traditional authentication method, which proves that the proposed scheme has better authentication performance than the traditional scheme.

References

[1] Yuwen Chen et al. A Bilinear Map Pairing Based Authentication Scheme for Smart Grid Communications: PAuth [J]. IEEE Access, 2019, 7: 22633-22643.
[2] Q. Y e, J. Li, K. Qu, W. Zhuang, X. S. Shen, and X. Li, "End-to-endquality of service in 5G networks: Examining the effectiveness of anetwork slicing framework," IEEE Veh. Technol. Mag., vol. 13, no. 2,pp. 65–74, Jun. 2018.
[3] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligentauthentication in 5G and beyond wireless networks," IEEE Wireless Commun., vol. 26, no. 5, pp. 55–61, Oct. 2019.
[4] Amal Hyadi and Zouheir Rezki and Mohamed-Slim Alouini. An Overview of Physical Layer Security in Wireless Communication Systems with CSIT Uncertainty [J]. IEEE Access, 2016, 4 : 6121-6132.
[5] Irram Fauzia et al. Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions [J]. Journal of Network and Computer Applications, 2022, 206.
[6] Long Jiao et al. Physical Layer Key Generation in 5G Wireless Networks [J]. IEEE Wireless Commun., 2019, 26(5) : 48-54.
[7] Wang Ning et al. Physical Layer Authentication for 5G Communications: Opportunities and Road Ahead [J]. IEEE NETWORK, 2020, 34(6) : 198-204.
[8] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, andM. Ylianttila, "Security for 5G and beyond," IEEE Commun. SurveysTuts., vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.
[9] J. Hamamreh, H. Furqan, and H. Arslan, "Classifications and appli-cations of physical layer security techniques for confidentiality: Acomprehensive survey," IEEE Commun. Surveys Tuts., vol. 21, no. 2,pp. 1772–1828, 2nd Quart., 2019.
[10] M. A. Arfaoui et al., "Physical layer security for visible light com-munication systems: A survey," IEEE Commun. Surveys Tuts., vol. 22,no. 3, pp. 1887–1908, 3rd Quart., 2020.
[11] Guyue Li et al. Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities [J]. Entropy, 2019, 21(5): 497-497.
[12] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authen-tication in wireless communication networks: A survey," J. Commun. Netw., vol. 5, no. 3, pp. 237–264, Sep. 2020.
[13] N. Xie, Z. Li and H. Tan, "A Survey of Physical-Layer Authentication in Wireless Communications," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 282-310, Firstquarter 2021, doi: 10.1109/COMST. 2020.3042188.
[14] Zhou Xinyu et al. A Robust Radio-Frequency Fingerprint Extraction Scheme for Practical Device Recognition [J]. Ieee Internet of Things Journal, 2021, 8(14) : 11276-11289.
[15] Jianyin Lu. A New Indoor Location Algorithm Based on Radio Frequency Fingerprint Matching [J]. IEEE Access, 2020, 8: 83290-83297.
[16] Arun Kumar K A. RF Fingerprinting of Software Defined Radios Using Ensemble Learning Models [J]. Journal of Communications, 2022, 17(4).