International Journal of Autonomous and Adaptive Communications Systems

ISSN online: 1754-8640 - ISSN print: 1754-8632
https://www.inderscience.com/ijaacs

Vulnerability detection of the authentication protocol in the IOT based on improved wavelet packet

Shihong Chen

DOI: 10.1504/IJAACS.2023.10034567

Article History:

Received:	12 March 2020
Accepted:	30 June 2020
Published online:	17 March 2023

Vulnerability detection of the authentication protocol in the IOT based on improved wavelet packet

Shihong Chen

Department of Information Engineering,
Guangdong Eco-Engineering Polytechnic,
Guangzhou 510520, China
Email: shihong@mls.sinanet.com

Abstract: To overcome the problems of long detection time and large detection error in traditional vulnerability detection methods for the authentication protocol in the internet of technology (IOT), this paper proposes a new method based on improved wavelet packet for vulnerability detection of the authentication protocol in the IOT. This method uses the improved wavelet packet to preprocess the data packet and form a small amount of original data. Combined with the method of protocol state diagram, it improves the coverage of traversal path and the effectiveness of trial cases. At the same time, it uses the method of sending TCP detection packets to detect whether there is vulnerability in the IOT authentication protocol. The experimental results show that the proposed method can effectively reduce the detection time and improve the detection accuracy, with the highest detection accuracy of 98.2%.

Keywords: improved wavelet packet; IOT; internet of technology; authentication protocol; vulnerability detection; traversal path; protocol state diagram; simulation.

Reference to this paper should be made as follows: Chen, S. (2023) ‘Vulnerability detection of the authentication protocol in the IOT based on improved wavelet packet’, *Int. J. Autonomous and Adaptive Communications Systems*, Vol. 16, No. 1, pp.1–16.

Biographical notes: Shihong Chen received his Master’s degree in Computer Technology from Guangdong University of Technology in 2008. He is currently an Associate Professor in the Department of Information Engineering, Guangdong Eco-Engineering Polytechnic. His research interests include IOT technology, data mining, and image processing.

1 Introduction

The existence of the internet of things effectively promotes the global human communication without borders and obstacles, and effectively promotes the development of society. The development of all walks of life is inseparable from the internet of things. All kinds of data and information are transmitted through the Internet of things. Therefore, in order to ensure the security of information exchange of the internet of things, the internet of things authentication protocol can be applied. Through the internet of things authentication protocol, the port of information transmission in the internet of things can be detected to improve the security of the internet of things communication.

However, the internet of things authentication protocol can not fully guarantee the communication security of the internet of things, and the internet of things authentication protocol also has vulnerabilities that can be attacked. Therefore, effective detection of the security authentication protocol vulnerabilities of the internet of things can greatly improve the communication security of the internet of things. However, there are still some problems to be overcome in the detection of security authentication protocol vulnerabilities in the internet of things at this stage, such as large bandwidth loss and imperfect programming technology. Due to the long-term operation of the internet of things, there are a lot of loopholes in the whole system at this stage. In order to improve the security of internet of things communication, it is necessary to study a vulnerability detection method of internet of things authentication protocol (Chang et al., 2016; Qiang et al., 2016; Wang and Zhou, 2018).

At present, relevant scholars have made some very significant research results. Ling and Sun (2019) proposes a vulnerability detection method for the authentication protocol in the internet of technology (IOT) based on improved ant colony algorithm. This method uses pseudo-random proportional rule to optimise the state transition function in the IOT, and triggers ant colony to search path through neighbour information of nodes and arc information which are not covered on monitoring boundary. The identification node of the concentration of pheromone can get the corresponding vulnerability boundary information and complete the vulnerability detection of the authentication protocol in the IOT. However, the detection accuracy of this method is low and it is difficult to ensure the security in the IOT. In Zhao and Chen (2019), a vulnerability detection method for the security authentication protocol in the IOT based on hidden Markov model is proposed. This method uses the hidden Markov model to build the word set model, and uses the word set model to observe and train the training sample sequence in the IOT, and generates the HMM detector to complete the vulnerability detection of the security authentication protocol in the IOT. However, the detection efficiency of this method is low, which is difficult to meet the detection demand. In He and Ye (2019), a vulnerability detection method for the security authentication protocol in the IOT based on AOP and dynamic stain analysis is proposed. In this method, firstly, the pole coordinates of sensors are constructed by covering the vulnerability discovery algorithm, and the dynamic stains between the closest nodes are obtained. At the same time, the edge's arc information sequence corresponding to any node is calculated, and the number of new sensors that need to be added between each node is obtained. However, the detection accuracy of this method needs to be further improved.

To solve the problems of low detection accuracy and low detection efficiency in the above methods, an improved wavelet packet based vulnerability detection method for internet of things authentication protocol is proposed. The overall scheme of this method is as follows:

1 To improve the effect of wavelet packet processing, the threshold value of wavelet packet is improved. The improved wavelet packet is used to preprocess the measured data to improve the detection accuracy.

2 According to the pre-processing results, combined with the protocol state diagram method, increase the coverage of detection traversal path, and use the method of sending TCP detection packets to complete the detection of security authentication vulnerabilities in the internet of things.

3 Experimental verification. Taking the detection accuracy, detection efficiency and missed detection rate as experimental indexes, the proposed method is compared with Ling and Sun (2019), Zhao and Chen (2019), He and Ye (2019), and the experimental results are analysed to prove the effectiveness of the proposed method.

Through the above scheme, the accurate and fast detection of internet of things security authentication protocol is realised to ensure the operation security of internet of things.

2 Vulnerability detection of the authentication protocol in the IOT

To accurately detect the vulnerability of internet of things authentication protocol, based on the above overall research scheme, the vulnerability of internet of things authentication protocol is detected.

2.1 Packet preprocessing

The tested data are set as:

$$f_i(t) = y_i(t) + n_i(t), \quad i = 1, 2, \ldots, n \tag{1}$$

In the above formula, $y_i(t)$ represents the original data; $n_i(t)$ represents the noise, and the signal can obtain the corresponding wavelet packet sequence after the wavelet packet decomposition. Then there are,

$$w = \theta + \gamma \tag{2}$$

In the above formula, θ represents signal coefficient and γ represents noise coefficient.

If W and W^{-1} respectively represent wavelet packet transform and inverse operation (Wang and Zhou, 2018), the wavelet packet threshold preprocessing method of data is as follows:

$$w = W(f) \tag{3}$$

$$w_\lambda = \eta(w, \lambda) \tag{4}$$

$$\tilde{y} = W^{-1}(w_\lambda) \tag{5}$$

In the above formula, η represents the threshold de-noising operator, that is, the threshold function; λ represents the threshold. The core step of wavelet packet preprocessing is the threshold de-noising operator and threshold calculation. In the improvement of wavelet packet, it mainly aims at the following aspects, specifically as follows:

(1) Selection of threshold function:

Threshold function is the most critical part of the whole de-noising process. Different values of threshold function make different de-noising curves and different rules of threshold processing for different sizes. Combined with the above analysis, it is necessary to determine an adaptive threshold adjustment which can be made by signal type and noise situation.

(2) Determination of threshold value:

In the process of wavelet packet threshold de-noising, the selection of threshold value has a great influence on the de-noising effect. Firstly, the threshold value needs to divide the signal and the wavelet packet coefficient of noise. If the threshold value is too small, it means that the wavelet packet coefficient of noise has some residual; otherwise, if the threshold value is too large, it will kill the signal.

(3) Determination of decomposition layers:

In the process of de-noising the original data with wavelet packet threshold, the first step is to decompose the signal with wavelet, and at the same time, the number of decomposition layers that meet the conditions should be selected. If the number of decomposition layers is too low, the amplitude of the signal and noise coefficients will be small, and it is difficult to distinguish the signal and noise coefficients, and affect the final de-noising effect. On the contrary, if the number of decomposition layers is too high, it means that the wavelet threshold amplitude of the signal will be seriously compressed, and the de-noising effect of the signal will also be affected.

In the process of wavelet packet de-noising, when the threshold value is determined, different threshold rules are selected for wavelet packet coefficients with different threshold values to obtain brand-new wavelet packet coefficients (Tao and Sun, 2016; Zhao et al., 2016), which are reconstructed to obtain the de-noising signal. The above processing rule is the determination of wavelet packet threshold function.

The hard threshold function can be expressed in the following forms:

$$\eta(w,\lambda)=\begin{cases} w, |w| \geq \lambda \\ 0, |w| < \lambda \end{cases} \tag{5}$$

The soft threshold function can be expressed in the following forms:

$$\eta(w,\lambda)=\begin{cases} w-\lambda, & |w| \geq \lambda \\ 0, & |w| < \lambda \\ w+\lambda, & w \leq -\lambda \end{cases} \tag{6}$$

In the above formula, η represents threshold de-noising operator; λ represents threshold; w represents wavelet packet coefficient.

Compared with the hard threshold, the soft threshold has certain continuity at the threshold point, and all wavelet packet coefficients higher than the threshold are shrunk. This shows that the soft threshold can effectively remove more noise than the hard threshold, and the signal has higher continuity (Liu et al., 2016; Zhu, 2018), but this will cause the original components of the signal to be killed, and the important information in the signal will be lost.

On the basis of the above analysis, a semi soft threshold function is proposed by combining the soft and hard threshold methods, and the expression of the semi soft threshold function is as follows:

$$\eta(w, \lambda_1, \lambda_2) = \begin{cases} 0, & |w| \le \lambda \\ \operatorname{sgn}(w) \dfrac{\lambda_2(|w| - \lambda_1)}{\lambda_2 - \lambda_1}, & \lambda_1 < |w| \le \lambda_2 \\ w, & |w| > \lambda \end{cases} \tag{7}$$

In the above formula, λ_1 represents the lower threshold value; λ_2 represents the upper threshold value, where:

$$\lambda_2 = \sigma\sqrt{2InN} \tag{8}$$

On the basis of the above, the threshold function is improved as follows (Li and Li, 2019; Yao et al., 2016):

$$\eta(w, \lambda) = \begin{cases} \operatorname{sgn}(w)\left(|w| \dfrac{(-2\lambda)}{1 + e^{|w| - \lambda_1}}\right) \\ 0, |w| < \lambda \end{cases} \tag{9}$$

According to formula (9), it is necessary to add exponential function to the above threshold function to process the wavelet coefficients.

Based on the above analysis, combined with the sample entropy algorithm, the threshold function is adjusted as follows:

$$\eta(w, \lambda, s) = \begin{cases} \operatorname{sgn}(w)\left(|w| - \dfrac{\lambda}{\exp(|w| - \lambda)\dfrac{1-s}{s}}\right), & |w| > \lambda \\ 0, & |w| < \lambda \end{cases} \tag{10}$$

To adjust the threshold function adaptively, first of all, it is necessary to analyse the noise in the wavelet packet coefficients of noisy signals. Because in the process of wavelet de-noising of signals, it is necessary to compare each wavelet coefficient and the size of the threshold one by one, so in the subsequent research process, it is hoped that each parameter corresponds to an adjustment parameter value. Combined with the above analysis, the threshold value can be obtained. The calculation method of function adjustment parameters is as follows (Wu et al., 2016):

1 The wavelet packet coefficients of the data are divided into several subsequences of the same length in order, and then k_{i+1} can be obtained by moving k_i backward one digit.

2 The sample entropy (Guo et al., 2019; Peng et al., 2019) of the above subsequence is calculated, and the obtained value is set as the sample entropy of the intermediate data points of the subsequence, to obtain the corresponding sample's entropy sequence, then:

$$\tilde{s} = \{\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_n\} \tag{11}$$

3 By normalising the extremum of the sequence, the sequence of adjusting parameters of threshold function can be obtained

$$s_k = \frac{\tilde{s}_k - \tilde{s}_{\min}}{\tilde{s}_{\max} - \tilde{s}_{\min}} \tag{12}$$

Let $s = (s_1, s_2, \ldots, s_k)$ be the adjustment parameter, and it is brought into the improved threshold function, so that it can have the self adaptability of the noise distribution of wavelet packet coefficient.

The calculation formula of threshold estimation is:

$$\lambda = \sigma_n \sqrt{2 \log N} \tag{13}$$

In the above formula, σ_n represents the standard deviation of noise; N represents the length of signal. Among them, when the variance of noise is larger, the wavelet threshold is also large, and noise interference can be reduced as much as possible (Tang et al., 2016). When the noise variance is reduced, the threshold value is smaller, and the wavelet packet coefficients of the effective data can be better preserved.

2.2 Improved wavelet packet

After completing the above packet processing, it is found that the threshold can affect the noise removal effect, and reducing the threshold can improve the effectiveness of wavelet packet coefficients, so the wavelet packet algorithm is improved. Wavelet packet analysis is a method to analyse the signal change while keeping the window area unchanged. Wavelet packet can optimise the time and frequency window locally by changing the window shape. Wavelet packet decomposition can adaptively select the corresponding frequency band according to the characteristics of the signal, so as to improve the accuracy of the detection results. Through the above analysis of data preprocessing threshold, it can be seen that the noise variance will affect the adjustment parameters, resulting in detection errors. Therefore, the wavelet packet threshold is improved to ensure the accuracy of the final detection results. Using the logarithmic function of decomposition layers to improve the above threshold, the improved threshold is estimated as follows:

$$\lambda = \frac{\sigma_n \sqrt{2 \log N}}{In(j+1)} \tag{14}$$

In the process of wavelet packet threshold de-noising, the threshold divides the original data and the existing data, and the coefficients processed by the threshold are processed by wavelet packet inverse operation to obtain the pre processed data packets (Jiang et al., 2016; Shi et al., 2018). The noise in the original data packets can be estimated as:

$$\tilde{n}(t) = f(t) - \tilde{y}(t) \tag{15}$$

It can be seen from formula (15) that the more noise is removed, the greater the sample entropy of $\tilde{n}(t)$ is. When the signal is killed, there are some regular signals in $\tilde{n}(t)$. If the complexity of $\tilde{n}(t)$ decreases, the sample entropy will also decrease. The sample entropy is set as the basis for determination, and the maximum value of estimated sample entropy of noise signal is selected as the basis for determination, where the estimation formula of threshold is:

$$\lambda = \lambda_{\max(Samp[En])} \tag{16}$$

The operation steps for determining the number of layers of wavelet packet decomposition are as follows:

1 The initial number of wavelet decomposition layers is set as $j = 1$, and the maximum number of decomposition layers is set as $j_{\max} = 6$.

2 According to the above operations, the sample entropy corresponding to the wavelet packet coefficients of different layers is calculated and the average value is obtained.

3 Assuming that the set constraint conditions are met, the number of decomposition layers selected is $j - 1$, otherwise, it is judged that $j > j_{\max}$, if it is true, the number of decomposition layers *J* can be determined; otherwise, repeat the operation steps 2 and 3.

On the basis of the above analysis, the specific operation process of the threshold de-noising method based on improved wavelet packet is given as follows (Chen et al., 2016; Zhou and Yue, 2017):

1 The appropriate mother wavelet is selected, and the above operations are combined to determine the number of decomposition layers to decompose the noisy signal with wavelet packet, to obtain the different wavelet packet nodes and the corresponding coefficient sequence of wavelet packet on the maximum decomposition scale.

2 The sample's entropy sequence corresponding to the wavelet coefficient sequence is calculated and standardised to obtain the improved adaptive threshold function and the adjusted parameter sequence.

3 The initial threshold value is set, and the corresponding threshold increment is selected, that is, the threshold size is:

$$\lambda_{i+1} = \lambda_i + a \tag{17}$$

4 After getting the denoised wavelet packet coefficients and performing the wavelet packet inverse operation, the preprocessed data packets can be obtained and part of the original data can be obtained at the same time.

2.3 Vulnerability detection of the authentication protocol in the IOT based on improved wavelet packet

On the basis of the original data obtained above, in order to ensure the accuracy of the detection results, it is necessary to carry out fuzzy test on different data packets. Because the basic block contains a lot of repeated parts, the statistical results of test cases are not accurate. In order to effectively solve this problem, it is necessary to reduce the formation efficiency of test cases. At the same time, it is necessary to traverse all test samples to obtain the largest basic block, and divide the samples into:

- maximum basic block
- remained basic blocks.

The protocol state diagram is a kind of relation diagram which is constrained by the relevant rules of the authentication protocol in the IOT. Through the state diagram of the authentication protocol in the IOT, different values in the whole protocol can be randomly mutated, and the corresponding test stress can be formed at the same time.

If there are multiple undetected packets in the whole authentication protocol of the IOT for repeated verification, each file may contain an overlapping number of basic blocks. In order to improve the efficiency of the whole algorithm, it can be removed optimally. At the same time, it can effectively test the repeated execution path in the formation process, improve the algorithm's traversal speed to the basic block (Zhou and Zhu, 2019), and reduce the execution time.

The finite state machine is mainly composed of the following five parts, and the specific calculation formula is as follows:

$$P_{FSM} = s_0, S, M, F, L \tag{18}$$

In the above formula, s_0 represents the initial state of the authentication protocol in the IOT, and it is also the beginning of the whole state space. Combined with the above analysis, it can achieve any other state after a series of transformations; M represents the test case set; S represents the state set of P_{FSM} .

Analysis of the above conclusions shows that FSM can better reflect the message driven protocol, the protocol state can be transferred from some state to the corresponding state, and it can also reflect the context sensitive authentication protocol in the IOT, and it is related to the historical trajectory of the packets.

After analysing the basic block after de duplication, we need to associate the constraints between different basic blocks, and set up the state diagram in the authentication protocol of the IOT. The maximum traversal depth needs to be set to ensure the reduction of traversal efficiency. This paper mainly uses the state graph as the input to traverse the system. After completing a state traversal, it needs to carry out the transition between each state to ensure the effectiveness of the whole algorithm.

The following uses the corresponding packet capturing tool to obtain the packets of the authentication protocol in the IOT, completes the packet preprocessing through Section 2.1, filters and de duplicates the name and port number of the authentication protocol in the IOT (Chen et al., 2016; Lu and Feng, 2016). Then the contents contained in the packets are divided. Through the association function, multiple fields are managed, the authentication protocol chart in the IOT is established, the fuzzy test is carried out in combination with the execution path, and the whole test is monitored and analysed. The specific operation process is as follows:

(1) Start;

(2) Obtain the data package of the target object;

(3) Preprocess the data package;

(4) Process the packets of the authentication protocol in the IOT in blocks;

(5) Setup the status chart of the authentication protocol in the IOT;

(6) The whole graph is traversed according to first traversal mode with different depth, and test cases are formed at the same time, which are sent to the system server;

(7) Send the detection packet, and determine whether the detection target is alive or not;

(8) End of ergodic graph;

(9) End.

The performance of fuzzy testing mainly depends on the proportion of effective test cases and the path coverage of the authentication protocol in the IOT. The traditional test method can not meet the development needs at this stage. At this stage, the method mainly makes random byte variation for different fields of the authentication protocol in the IOT. The number of test cases formed by the above methods shows a violent growth trend (Li and Luo, 2018). Although the coverage of the whole algorithm is high, in the actual application process, the running time is long, so the method is not available.

To further improve the comprehensive performance of the whole detection method, we need to focus on the following aspects, as follows:

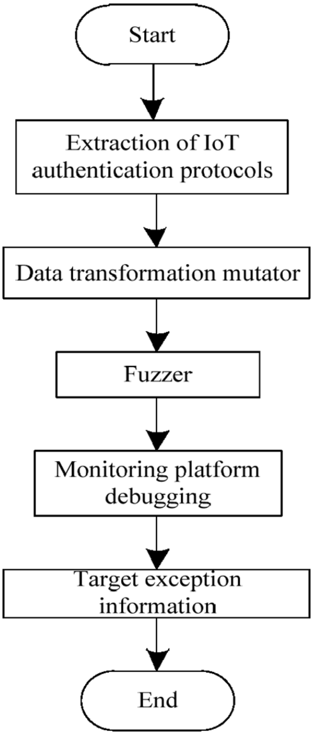
- to improve the operation efficiency, it is necessary to improve the automation of the whole workflow, simplify the implementation of fuzzy test, and form the input file required by the corresponding framework through the identification algorithm of the authentication protocol field in the IOT
- adding the de duplication algorithm to the detection algorithm, the duplicate fields in the authentication protocol in the IOT can be deleted, to reduce the formation of redundant test cases, and increase the sample set
- the mutation device of user-defined test data is implemented, and the negative characters in the process of test are expanded
- the relationship between various authentication protocols in the IOT is analysed (Hao et al., 2016), to set up the status chart of authentication protocol in the IOT, and effectively improve the coverage of the implementation path of the authentication protocol in the IOT (Hao et al., 2016).

Figure 1 is used to show the specific flow chart of the whole framework work.

On the basis of the above analysis, combined with the automatic analysis and the manual analysis, the function association of the basic blocks of the data package is carried out, and the value constraints and length constraints among the basic blocks are obtained. According to the preparation of the definition script for automatically forming the original data, at the same time, the original data will be saved to the system server, and the corresponding fields need to be set. According to the preparation of automation script, the device IP, port and other types that are not monitored are bind, and the communication with each target monitoring device is established. This paper uses the method of sending TCP detection packet to detect whether there is a vulnerability in the authentication protocol in the IOT.

According to the above process, the wavelet packet threshold is improved to obtain accurate original data. According to the results of the original data, the TCP detection packet method is used to analyse the relationship between various authentication protocols in the IOT, and establish the state chart of authentication protocols in the IOT, so as to effectively improve the coverage of the implementation path of authentication protocol in the IOT, and realise the vulnerabilities detection of authentication protocol in the IOT. The above process only realises theoretical research and needs further experimental verification.

Figure 1 Specific flow chart of framework work


Start
Extraction of IoT authentication protocols
Data transformation mutator
Fuzzer
Monitoring platform debugging
Target exception information
End

3 Experimental verification

In order to verify the comprehensive effectiveness of the proposed vulnerability detection method for authentication protocol in the IOT based on improved wavelet packet, simulation experiments need to be carried out. The simulation experiment in this paper is implemented in the network connected by switch, i.e., switched Ethernet, as shown in Figure 2.

Figure 3 shows the structure of the experimental environment, in which the IP of the attack host is 192.168.0.98, the IP of the attacked host is 192.168.0.93, and the IP of the address of the gateway is 192.168.0.3.

3.1 Experimental scheme

According to the above experimental environment, the overall experimental scheme is: select 10 GB of data from MySQL database, take the detection accuracy, detection efficiency and missed detection rate as the experimental comparison index, and compare the proposed method with Ling and Sun (2019), Zhao and Chen (2019), and He and Ye (2019) for verification.

- *Detection accuracy*: it refers to whether the method can completely identify the vulnerabilities in the authentication protocol in the IOT. The higher the detection accuracy is, the more complete the vulnerabilities can be detected by the method, and the more secure the operation in the IOT can be guaranteed.
- *Detection efficiency*: in the case of the same number of vulnerabilities, the shorter the detection time is, the higher the detection efficiency of the method is.
- *Missed detection rate*: the missed detection rate refers to the probability that the method fails to detect the vulnerability, which is an important index to evaluate the detection performance of the authentication's vulnerability detection method for IOT. The higher the missed detection rate is, the worse the detection performance of the method is.

Figure 2 Topology of local area network (see online version for colours)

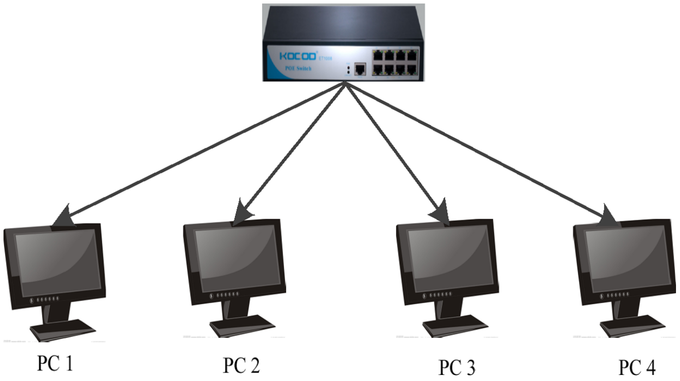
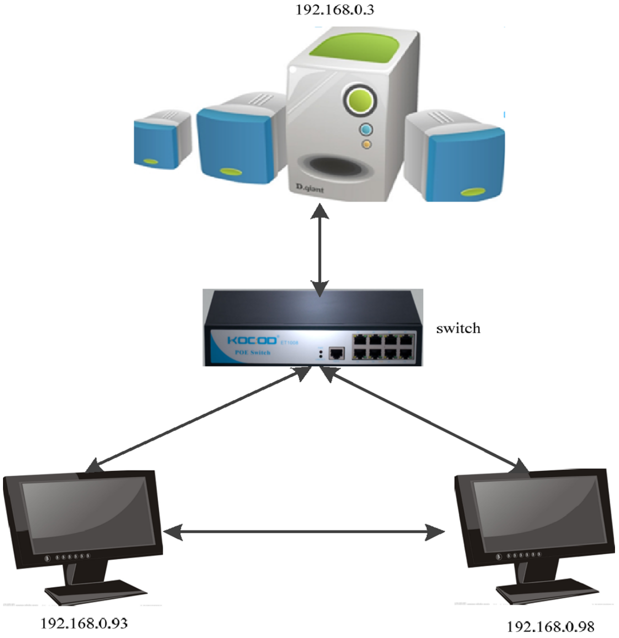


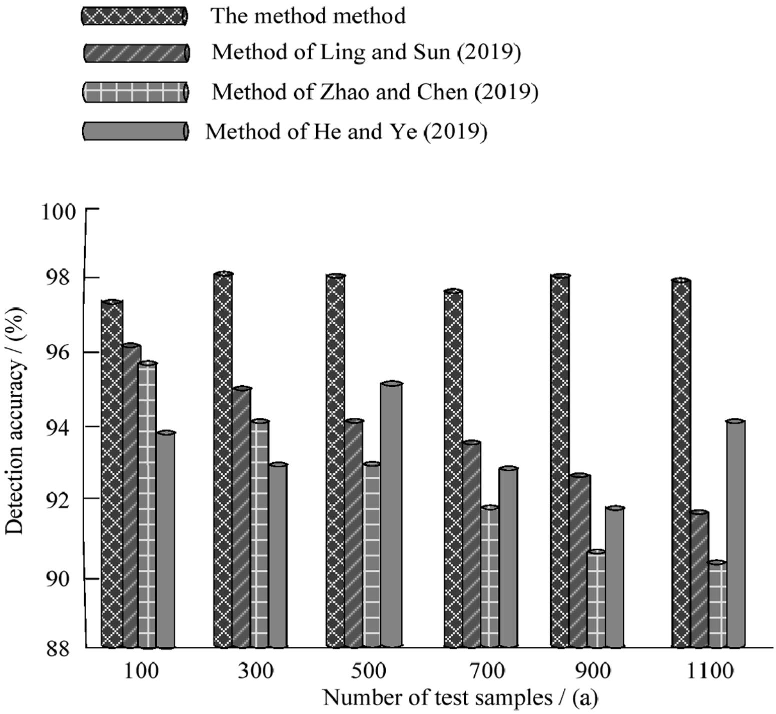
Figure 3 Topology of experimental environment (see online version for colours)



3.2 Comparison results of test accuracy

The comparison results of the four detection methods are shown in Figure 4.

Figure 4 Comparison results of detection accuracy of different detection methods



According to Figure 4, with the increasing number of samples, the detection accuracy of the four detection methods is also changing. Compared with the traditional three detection methods, the detection accuracy of the proposed method is significantly higher, with the highest detection accuracy of 98.2%. Because this method improves the threshold value of traditional wavelet packet algorithm, obtains the improved wavelet packet algorithm, uses the improved wavelet packet algorithm to preprocess the internet of things data packets, extracts the effective internet data, thus greatly improves the detection accuracy of authentication protocol vulnerabilities.

3.3 Comparison results of test efficiency

In order to further verify the effectiveness of the proposed method, the following needs to compare the detection efficiency of four vulnerability detection methods for authentication protocol of IOT. The specific comparison results are shown in Table 1.

According to the above experimental data, with the continuous increase of the number of decomposition layers, the execution efficiency of various detection methods does not change constantly. The execution efficiency of the traditional three IOT authentication protocol vulnerability detection methods has been in a linear downward trend, but the execution efficiency of the proposed detection methods has been in a very stable state. The proposed method uses the protocol state graph method to improve the coverage efficiency of traversal path in the detection process, so it greatly shortens the detection time of authentication protocol vulnerabilities.

Table 1 Change of detection efficiency of four methods

Number of decomposition layers	*Detection efficiency* (%)			
	Proposed method	*Method in Ling and Sun* (*2019*)	*Method in Zhao and Chen* (*2019*)	*Method in He and Ye* (*2019*)
j = 1	98.51	98.74	98.58	94.21
j = 2	97.84	97.85	98.14	93.14
j = 3	98.54	96.96	97.85	92.20
j = 4	99.69	95.85	97.21	91.15
j = 5	99.47	94.25	96.32	90.18
j = 6	98.89	93.41	96.27	89.23
j = 7	97.66	92.36	95.61	88.26
j = 8	98.85	91.12	95.62	87.34
j = 9	97.69	90.45	94.64	86.37
j = 10	96.47	89.78	94.81	85.78
j = 11	98.58	88.25	93.71	84.75
j = 12	99.69	87.63	93.66	83.95
j = 13	99.74	86.27	92.51	82.54
j = 14	99.50	85.54	92.74	81.48
j = 15	99.20	84.60	91.30	80.25
Average	98.69	91.54	95.26	87.39

3.4 Comparison results of missed inspection rate

The comparison results of the four detection methods are shown in Table 2.

Table 2 Change of missed detection rate of four methods

Number of experiments (*times*)	*Missed detection rate/*(%)			
	Proposed method	*Method in Ling and Sun* (*2019*)	*Method in Zhao and Chen* (*2019*)	*Method in He and Ye (2019)*
1	0.15	0.15	0.12	0.18
3	0.12	0.18	0.19	0.23
5	0.11	0.22	0.18	0.27
7	0.08	0.26	0.16	0.31
9	0.07	0.30	0.17	0.35
11	0.09	0.35	0.20	0.42
13	0.06	0.38	0.15	0.48
15	0.03	0.42	0.13	0.56
17	0.00	0.47	0.18	0.62

Table 2 Change of missed detection rate of four methods (continued)

Number of experiments (times)	*Missed detection rate/*(%)			
	Proposed method	*Method in Ling and Sun (2019)*	*Method in Zhao and Chen (2019)*	*Method in He and Ye (2019)*
19	0.02	0.48	0.22	0.68
21	0.01	0.52	0.17	0.75
23	0.04	0.55	0.15	0.81
25	0.01	0.57	0.12	0.82
27	0.02	0.60	0.16	0.76
Average	0.06	0.39	0.166	0.52

Analysing the data in Table 2, we can see that the missing detection rate of the proposed method is significantly lower than the other three detection methods, which shows that the proposed method can accurately detect the loopholes in the internet of things authentication protocol. The proposed method improves the coverage of traversal path, effectively improves the detection range of authentication protocol vulnerabilities, and completes the detection of authentication protocol vulnerabilities by using TCP packet detection method, so the recall rate of the proposed method is significantly improved.

4 Conclusions

In view of the problems of low detection efficiency and accuracy in the traditional vulnerability detection method for authentication protocol in the IOT, this paper proposes a vulnerability detection method for authentication protocol in the IOT based on improved wavelet packet. The following conclusions are proved in theory and experiment. When detecting the vulnerability of the security authentication protocol in the IOT, this method has high detection accuracy and efficiency. Specifically, compared with the detection method based on the improved ant colony algorithm, the detection accuracy is greatly improved, with the highest detection accuracy of 98.2%; compared with the method based on the hidden Markov model, the detection efficiency is significantly improved, with the average detection efficiency of 98.68%. Therefore, it fully shows that the proposed detection method based on improved wavelet packet can better meet the requirements of security authentication protocol detection in the IOT. In the follow-up, we will focus on the study of some serious security problems, and provide solutions to meet the needs to ensure the normal operation of the whole network.

References

Chang, Q., Liu, Z.J., Wang, M.T., Chen, Y., Shi, Z.Q. and Sun, L.M. (2016) 'Vdns: a cross-platform firmware vulnerability correlation algorithm', *Computer Research and Development*, Vol. 53, No. 10, pp.2288–2298.

Chen, X.L., Li, Y.Z. and Yu, H.L. (2016) 'Research on intrusion detection algorithm based on ipmeans-kelm', *Computer Engineering and Applications*, Vol. 52, No. 22, pp.118–122.

Chen, Y., Wei, Z., Yu, Z.T. and Huang, S.W. (2016) 'Preliminary study on information network anomaly detection based on the correlation of coupling dynamic discrete event chains', *Automation of Electric Power Systems*, Vol. 40, No. 17, pp.38–43.

Guo, X.D., Li, X.M., Jing, R.X. and Gao, Y.Z. (2019) 'Intrusion detection based on improved sparse de-noising autoencoder', *Computer Applications*, Vol. 39, No. 3, pp.769–773.

Hao, Y.Z., Zheng, Q.H., Chen, Y.P. and Yan, C.X. (2016) 'Abnormal behavior recognition for Internet public opinion data', *Computer Research and Development*, Vol. 53, No. 3, pp.611–620.

He, C.W. and Ye, Z.P. (2019) 'SQL injection behavior detection method based on AOP and dynamic taint analysis', *Acta Electronica Sinica*, Vol. 47, No. 11, pp.2413–2419.

Jiang, F., Zhang, Y.Q., Du, J.W., Liu, G.Z. and Wu, Y.F. (2016) 'Ensemble learning algorithm based on approximate reduction and its application in intrusion detection', *Journal of Beijing University of Technology*, Vol. 42, No. 6, pp.877–885.

Li, Y. and Li, Y.Z. (2019) 'Intrusion detection algorithm for industrial control network based on autoencoder and extreme learning machine', *Journal of Nanjing University of Science and Technology (Natural Science)*, Vol. 43, No. 4, pp.408–413.

Li, Y.J. and Luo, X. (2018) 'Identification of key section sets in urban road networks under sudden environments', *Transportation System Engineering and Information*, Vol. 18, No. 2, pp.128–135.

Ling, C. and Sun, W.S. (2019) 'Wireless sensor network routing based on improved ant colony algorithm', *Computer Engineering and Design*, Vol. 40, No. 3, pp.34–38+44.

Liu, Y., Fang, Y., Sun, H. and Liu, S. (2016) 'Smart grid attack detection method based on physics-information fuzzy reasoning', *China Science and Technology Paper*, Vol. 11, No. 14, pp.1619–1625.

Lu, G.H. and Feng, D. (2016) 'Implementation of security situation awareness algorithm for industrial control network', *Control Theory and Applications*, Vol. 33, No. 8, pp.1054–1060.

Peng, H.K., Peng, C., Sun, H.T. and Yang, M.J. (2019) 'Microgrid's incremental detection mechanism under false data injection attacks', *Information and Control*, Vol. 48, No. 5, pp.522–527.

Qiang, X.H., Chen, B. and Chen, G.K. (2016) 'Openssl heartbleed vulnerability analysis and detection technology research', *Computer Engineering and Applications*, Vol. 52, No. 9, pp.88–95.

Shi, X., Xie, S.P. and Li, H.B. (2018) 'Detection of pulmonary nodules based on convolutional neural network', *China Medical Imaging Technology*, Vol. 34, No. 6, pp.934–939.

Tang, Y., Wang, Q., Ni, M. and Liang, Y. (2016) 'Analysis of network attacks in power information physical fusion system', *Automation of Electric Power Systems*, Vol. 40, No. 6, pp.148–151.

Tao, L. and Sun, Z.W. (2016) 'Kipso spoofing attack detection model for wireless sensor networks', *Journal of Transduction Technology*, Vol. 29, No. 7, pp.1049–1055.

Wang, G.C. and Zhou, Y.P. (2018) 'Simulation of vulnerability in active network virus intrusion', *Computer Simulation*, Vol. 35, No. 7, pp.245–248.

Wu, X.G., Huang, Y.H., Liu, H.T., Zhang, L.M. and Wu, K.B. (2016) 'Vulnerability analysis of metro line network based on complex network theory', *Journal of Chongqing Jiaotong University (Natural Science Edition)*, Vol. 35, No. 4, pp.93–99.

Yao, Y.Z., Yang, A., Shi, Z.Q. and Sun, L.M. (2016) 'Application of bp neural network model in industrial equipment state detection', *Journal of Beijing University of Posts and Telecommunications*, Vol. 39, No. 6, pp.14–18.

Zhao, C. and Chen, J.X. (2019) 'Reflected XSS detection technology based on HMM', *Journal of Zhejiang University of Technology*, Vol. 47, No. 4, pp.442–447.

Zhao, X.J., Liu, Y. and Sun, J. (2016) 'Network anomaly detection based on transfer learning and d-s theory', *Application Research of Computers*, Vol. 33, No. 4, pp.1137–1140.

Zhou, A.P. and Zhu, C.G. (2019) 'A continuous network detection method based on summary data structure', *Computer Applications*, Vol. 39, No. 8, pp.2354–2358.

Zhou, M. and Yue, L.N. (2017) 'Design of bridge structure safety information platform based on IOT and cloud technology', *Journal of Wuhan University of Technology (Information and Management Engineering Edition)*, Vol. 39, No. 6, pp.765–768.

Zhu, Y.D. (2018) 'Network intrusion detection scheme based on rough set and spso', *Control Engineering*, Vol. 25, No. 11, pp.2097–2101.