Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5380481, 11 pages
https://doi.org/10.1155/2018/5380481

Research Article

A Security Situation Prediction Algorithm Based on HMM in Mobile Network

Wei Liang[1], **Jing Long**[2], **Zuo Chen**[2], **Xiaolong Yan**[2], **Yanbiao Li**[3], **Qingyong Zhang**[4] and **Kuan-Ching Li**[5]

[1]*School of Opto-Electronic and Communication Engineering, Xiamen University of Technology, Xiamen 361024, China*
[2]*College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*
[3]*Computer Science Department, University of California at Los Angeles, USA*
[4]*Fujian Key Laboratory of Automotive Electronics and Electric Drive (Fujian University of Technology), Fuzhou 350118, China*
[5]*Department of Computer Science and Information Engineering, Providence University, Taichung 43301, Taiwan*

Correspondence should be addressed to Kuan-Ching Li; kuancli@gm.pu.edu.tw

Received 18 April 2018; Accepted 1 August 2018; Published 14 August 2018

Academic Editor: Ao Zhou

The increasingly severe network security situation brings unanticipated challenges to mobile networking. Traditional HMM (Hidden Markov Model) based algorithms for predicting the network security are not accurate, and to address this issue, a weighted HMM based algorithm is proposed to predict the security situation of the mobile network. The multiscale entropy is used to address the low speed of data training in mobile network, whereas the parameters of HMM situation transition matrix are also optimized. Moreover, the autocorrelation coefficient can reasonably use the association between the characteristics of the historical data to predict future security situation. Experimental analysis on DARPA2000 shows that the proposed algorithm is highly competitive, with good performance in prediction speed and accuracy when compared to existing design.

1. Introduction

With the rapid development and popularization of Internet technology, mobile network becomes an indispensable communication mean [1]. Nevertheless, one of largest issues is security threat in mobile network [2–4]. People has developed many protection techniques to cope with these threats, such as mobile firewall, intrusion detection, and virus killer. Though these techniques are active and useful for already occurred threats but cannot monitor the complete situation of the mobile network. In this case, prediction technique of mobile network security situation has emerged as a trend of network security monitoring, which can rapidly acquire, understand, and display the security elements and use them to predict the future situation [5]. By analyzing the changes of mobile network security situation, network manager can predict the security situation and protect the network from illegal attacks.

In existing security situation prediction techniques, the warning is classified on the basis of the damage degree caused by network attacks and the risk level of the security vulnerability [6–8]. In such a case, the threats in mobile network can only be evaluated by the feature of attacks. Other factors such as environment are not investigated. Snort [9] classified the priority of warning into three levels. The warning of priority 1 illustrates a threat with the highest level, usually including security vulnerability with high risk, such as buffer overflow. The risk level of security vulnerability is analyzed by professional institutes, such as CVE (Common Vulnerability Exposure) [10] and Bugtraq [11], and classified into high, medium, and low. The classification result can also be obtained from a more complete quantified evaluation mechanism of vulnerability risk, namely, CVSS (Common Vulnerability Scoring System) [12].

The threat level of mobile network attack is closely related to the running condition and the vulnerability of target computer system. A typical example is worm virus Code Red II targeting at Linux computer systems. It has extremely low threat level since it is designed on the basis of Windows IIS

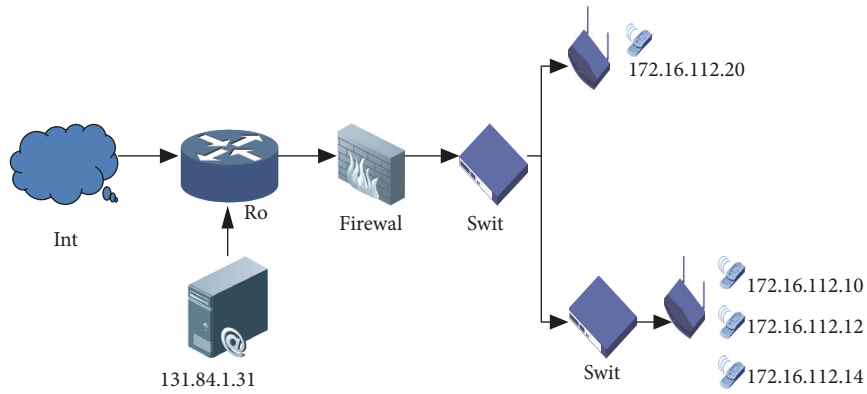

Figure 1: Topology structure of mobile network.

vulnerability, since there is no similar vulnerability in Linux systems, and therefore, it is not a threat. Many researchers proposed to evaluate the threat level by cross correlation of the mobile network warning and vulnerability scanning tool. Kruegel et al. [13] realized correlation analysis of Snort warning and Nessus [14] (a vulnerability scanning tool) and used it to confirm the warning. The target vulnerability of the attack is compared to the scanned vulnerability result of the target computer in terms of the port, service, vulnerability ID, etc. The matching result is used to confirm or filter the warning. If the target vulnerability of the attack exists in the target computer, the probability of a successful attack is larger, as well higher the threat level. Otherwise, the threat level is low, and the warning may be a false alarm. The proposed method has fully considered the network running state for the attack, by better recognizing false alarm and real threats. Nevertheless, the drawback is that it cannot evaluate the threats not targeting at vulnerability, since the information of the target vulnerability should be stored. Besides, the instantaneity of the vulnerability scanning report should be also considered.

The topology of a mobile network is depicted in Figure 1. "Mission" is the target service, port of the attack, which is determined by the manager. For example, HTTP service of 80 port on a Web server is a key Mission. The attack targeting at the Mission has the highest threat level. Porras et al. [15] calculated the probability of a successful attack using Bayesian network. Most of the SIM (Security Information Management) software provides a method to determine the warning level by making a security strategy. It is convenient for the manager to recognize the interesting attacks by custom rules and reducing the threat level of some of attacks.

2. Related Work

With the rapid development of mobile network, security situation prediction becomes an important network security technique, which plays a significant role in defending 802.11 wireless network threats. Due to its intrinsic features, the risk detection system can operate normally in wireless mobile network. There are increasing security threats of communication devices in mobile network, and therefore, it is urgent to evaluate and predict the security situation of mobile network. The network security report published by Chinese government in 2017 shows several security issues in mobile network. The Shadow Brokers leaked many 0-day vulnerabilities. There are serious security vulnerabilities in Bluetooth protocol, and a security research company in Internet-of-Thing (IoT) Armis has identified eight 0-day vulnerabilities in Bluetooth protocol. The company creates a group of network attack vectors for demonstration, where attackers can completely host the Bluetooth-supported network devices. Malicious attack software is propagated through these devices. A man-in-the-middle (MITM) connection is created, which makes lots of home cameras be intruded by Trojan, due to the fact that many intelligent cameras have weak password or vulnerabilities, which turns the main reason of camera intrusion. Security issues have arisen the concerns of government security departments in various countries, and a new generation of network security assessment prediction model emerges under this situation. The situation assessment of network communication security turned to be a hotspot in researches of network security.

In recent years, network intrusion detection systems have been replaced by security situation prediction techniques. Markov model has the nonaftereffect property and only related to the probability of its previous state. It is suitable to predict the random process which largely varies, as the future state is predicted by using the transfer probability matrix between states. The calculation of the transfer probability matrix uses statistical method and the prediction is to use the frequency to approximate the probability function. Therefore, the Markov model is suitable for security prediction of large data sample in mobile network communication. A typical Markov process includes Bernoulli process, Wiener process, and Poisson process. Based on continuous or discrete state and time parameter, Markov process can be classified into three categories: (1) discrete time discrete state Markov process, called Markov chain, (2) continuous time discrete state Markov process, called continuous time Markov chain, and (3) continuous time continuous state Markov process.

In the security prediction techniques for mobile network, Shake et al. proposed a network vulnerability evaluation method based on the electric current theory [16]. Bass

created a network situation framework using data fusion of multiple sensors. The network security situation is evaluated by deriving the identity of intruder, speed, threat level, and intrusion object [17]. There are various network attacks, which pretend to be normal data packet and perform attacks on the target computer, despite more difficult to detect the attacks. So, most of network attacks cannot be detected only be matching the features of data packet format. Meanwhile, the current detection techniques should unpack the packet, causing detection delay.

The intrusion techniques have been rapidly developed to cope with the increasing attacks in mobile network. To improve the detection accuracy, the commercial network intrusion detection system [18, 19] abstracted the characteristics of network attack using multiple algorithm and created a misuse detection model of network attacks. The network intrusion detection system based on misuse detection has high detection efficiency and low probability of false alarm. Since the detection system requires a real-time updated attack characteristic library, the characteristics of most network attacks are stored. If a new attack emerges, the detection system cannot detect it successfully since there is no information about the attack in the library. Therefore, the misuse-based detection model has higher false negative rate.

There are many situation awareness models for mobile network. Endsley [20] is the most concerned model that defines situation awareness as perception, by including the current state and future trend of the element in a space during a time period. Endsley model divides situation awareness into three parts: (1) Perception: it acquires and collects important information in network, which is the fundamental step of situation awareness model, (2) Comprehension: the collected data is integrated and analyzed and then used to evaluate the current situation, and (3) Prediction: the future trend is predicted on the basis of the results in (1) and (2). The data is collected from the management device, monitoring device and security device in the network. The collected original data is further integrated and processed to evaluate the current network security situation. On this basis, the future situation can be also predicted.

Due to its good performance in statistics, HMM (Hidden Markov Model) [21–25] technique is rapidly developed and applied in fields as voice recognition, classification, security situation prediction, intrusion detection, etc. In the field of security situation prediction, Hisham [26] proposed the first HMM model with finite state to predict the multistep attack in cloud computing system. The probability of potential attack can be calculated through an adaptive risk model, whereas such potential attack can be found through the autonomous cloud intrusion detection systems. In this case, the countermeasure can be adopted in advance. This method successfully predicts the alarm on the dataset DARPA2000 LLDDOS1.0. Luktarhan [27] proposed a HMM-based false alarm filtering algorithm that can detect the multistep attack and achieve higher detection accuracy rate. Experiments of this algorithm on DARPA2000 show good performance. As mentioned, the HMM technique usually uses Viterbi algorithm although it is applied to predict the hidden state on the basis of the observed state. Additionally, the precondition of multistep attack prediction should know all steps of multistep attack. The prediction is the upcoming step, yet not the future network security situation.

Multiscale entropy is a nonlinear characteristic analysis method. In 2002, Costa et al. [28, 29] proposed the theory of multiscale entropy on the basis of sample entropy and applied it in HRV research. Results show that the multiscale entropy can give a more reasonable explanation on the differences of CHF and AF between disease and health than the sample entropy. MSE (Mean Square Error) and RMSE (Root Mean Square Error) are metrics to evaluate the complexity and irregularity of time series with different scale factors. It is used in classification of physiological time series [30], eccentricity fault detection of motor spindle [31], dynamical change of crude oil price [32], and network traffic analysis and anomaly detection [33]. In this work, the multiscale entropy with different scale factors is used to select the scale information to process the alarm time series. HMM is used to train the security state parameters, whereas the prediction is realized by weighting the value of autocorrelation coefficient between security situations.

The remaining of this paper is organized as follows. Section 2 introduces the multiscale entropy based Markov model; the details of the prediction algorithm are illustrated in Section 3. The experimental results and analysis are presented in Section 4, and finally, summary and future work are depicted in Section 5.

3. Multiscale Entropy Based Weighted HMM

3.1. Multiscale Entropy Analysis. In mobile network, the complexity of time sequence with limit length is usually measured by nonlinear characteristic analysis. The entropy values for different scale factors are used to select suitable scale and process next the time sequence, and the sequence is further trained by the HMM. The acquired data is one-dimensional alarm time sequence. The multiscale entropy not only can be used to characterize the complexity of the one-dimensional sequence, but also can display the detailed characteristics of one-dimensional alarm sequence from different scales. Therefore, it can be used to analyze the complexity of one-dimensional alarm sequence. For the alarm time sequence, N is the length of the sequence, and the calculation process of the multiscale entropy is described in this section.

Firstly, the coarse-grained sequence is generated. The original sequence is divided into nonoverlapping window with length s. The sequence values in the window are averaged to obtain the coarse grain sequence $\{y^s\}$ on the s scale. Each element of sequence y_j^s can be obtained via the following formula:

$$y_j^s = \frac{1}{s} \sum_{i=(j-1)s+1}^{js} x_i, \quad 1 \le j \le \frac{N}{S} \tag{1}$$

The length of each coarse-grained sequence is the value divided by the original length s. Here, the time sequence of s = 1 is the original sequence.

Secondly, the sample entropy is calculated. For coarse-grained sequence $\{y(1), y(2), \ldots, y(M)\}$, M is the length of the

sequence. Detailed steps to calculate the sample entropy is described next.

Step 1. The given model dimension is m, and the m dimensional vector is composed by the original sequence.

$$Y(i) = [y(i), y(i+1), \ldots, y(i+m-1)] \tag{2}$$

where $i = 1, 2, \ldots, M + m - 1$.

Step 2. The distance between $Y(i)$ and $Y(j)$ is defined as

$$d(i, j) = \max |y(i+k) - y(j+k)| \tag{3}$$

where $k = 0, 1, \ldots, m - 1$.

Step 3. Given a threshold value r, for each i statistic value, we have the ratio of the number $d(i, j) < r$ and the number of the total number $N - m + 1$ is denoted as $B_i^m(r)$.

$$B_i^m(r) = \frac{[d(i,j) < r]}{N - m + 1} \tag{4}$$

where $1 \le j \le N - m$, $j \ne i$, seeking its average value for all i.

$$B^m(r) = \frac{1}{N - m + 1} \sum_{i=1}^{N-m+1} B_i^m(r) \tag{5}$$

Step 4. Repeat the three steps above for $m+1$, get the $B^{m+1}(r)$.

Step 5. In theory, the sequence sample entropy is as

$$\text{SampEn}(m, r) = \lim_{N \to \infty} \left[-\ln \frac{B^{m+1}(r)}{B^m(r)} \right] \tag{6}$$

As N takes a finite value, sample entropy for sequence of length n can be estimated by

$$\text{SampEn}(m, r, N) = -\ln \frac{B^{m+1}(r)}{B^m(r)} \tag{7}$$

Step 6. With the sample entropy formula, each scale factor sequence can be calculated. A function with scale factor s as argument and with sample entropy as dependent variable can be created. Thus, it can be used to analyze the complex nature of the alarm time sequence.

$$MSE(s) = SampEn(y^s, m, r) \tag{8}$$

It is obvious that the multiscale entropy is related to the scale factor s, the embedding dimension m, and the similarity coefficient r. In this paper, parameters $m = 2$ and $r = 0.2$ are set.

With the above method, multiscale entropy of one-dimensional alarm time sequence can be calculated. This result is used in next-step data processing and brought in HMM for training. Finally, the corresponding scale state transition probability matrix can be obtained.

3.2. HMM Definition. HMM is a statistical learning model in mobile network, which can describe the process of generating observed sequence. Developed on the basis of Markov chain, HMM is a double random process, including the transfer from state to state and the transfer from state to output. In this work, the transfer probability matrix between states is calculated by HMM. There is a Markov assumption of state transfer, of which the probability of state at time t shifting to state at time t + 1 is only related to the state at time t and not related to any other states. Nevertheless, the assumption is not reasonable in practice since this probability depends on the current state and the historical states. To address this issue, this work has improved the Markov assumption of the state transfer probability in traditional HMM model. A new model is realized by weighting and used to predict the future security situation of the network.

The HMM includes two random processes, transition between states and transition between state to output. Markov chain prediction for state transition at hidden layer utilizes the idea of weighted Markov chain prediction in [34]. Namely, the weight probability distribution by using multistep situation transition probability is used to predict the system's next status. The correlation coefficient in each order reflects the strength of relationship between time sequences with different step. Analysis between transition probability and time sequence makes full use of known conditions for prediction. On this basis, the proposed prediction model is described as follows.

Step 1. Calculate correlation coefficients in various steps:

$$r_k = \frac{\sum_{t=1}^{n-k} (x_t - \overline{x})(x_{t+k} - \overline{x})}{\sum_{t=1}^{n} (x_t - \overline{x})^2} \tag{9}$$

where k represents k-order (with step length of k) correlation coefficient, x_t represents the security situation at time t, $\overline{x}$ is the mean value of the security situation, and n is sequence length of security situation value.

Step 2. Normalize the self-correlation coefficient of each order:

$$\omega_k = \frac{|r_k|}{\sum_{k=1}^{m} |r_k|} \tag{10}$$

ω_k is regarded as the normalized weight of the Markov chain with various steps (M is the largest order in prediction).

Step 3. Establish security situation grading standards (to determine hidden state space). The security situation is divided into four states [35]:

(i) *Good (G)* indicates the system is in good condition with no attack.

(ii) *Probed (P)* is in the state of being attacked. Under this state, the availability of a host is slightly decreased, and the probability of being attacked increases.

(iii) *Attacked (A)* indicates that the host has been attacked and the probability of being invaded increases.

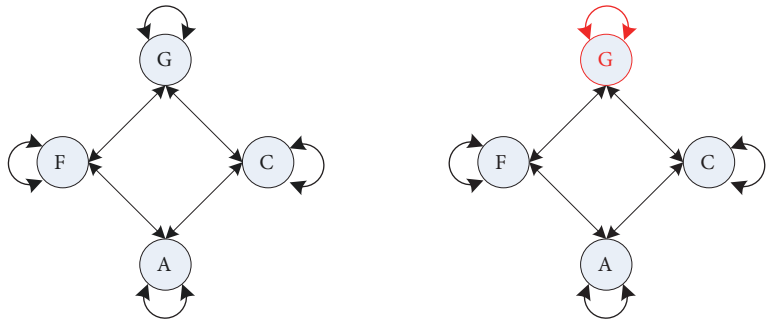

Figure 2: The state transition graph of Markov model.

(iv) *Compromised (C)* shows that the host has been invaded and is in a dangerous state. The confidentiality, integrity and availability of the host are destroyed.

The four states are, respectively, denoted by G, P, A, and C, so S = {G, P, A, C}. The transition between the host states constitutes a complete Markov chains, as shown in Figure 2.

Step 4. According to the security situation grade and alarm information, we sample security situation with different step lengths via HMM. Samples are trained to generate the transition probability matrix of different steps, determining as well the probability laws of security situation transition.

Step 5. On the basis of current state of the security situation, we can predict the probability of security status in the next time by using the security state transition matrix.

Step 6. Use the weight of prediction probability with different steps for a state as probability of secure state appeared in the next moment.

$$P_i = \sum_{k=1}^{m} \omega_k p_i^k \tag{11}$$

Step 7. With the obtained value of security state, the network situation can be analyzed.

Step 8. Repeat above Steps 4 to 7 to calculate the situation result under the scale factor and perform comparison to verify the proposed algorithm.

4. Algorithm Implementation

4.1. Algorithm Description. This work proposes a weighted hidden Markov prediction model on the basis of multiscale entropy in mobile network. The suitable scale factor is selected by using multiscale entropy, whilst the HMM is used to train the state transition probability matrix in mobile network. Changes of future security situation in mobile network are calculated by the weighting algorithm, of which entropy values of different scale data are obtained using the multiscale entropy. Two sets of data, respectively, with the maximum and the minimum entropy value which are processed to generate the multiorder state sequence matrixes are trained using HMM. The multiorder state transition probability matrix is used to calculate the security states with different scale at next time. The next security state is iteratively predicted using the obtained result, and differences between prediction value and the actual value are evaluated by MSE and RMSE. Besides, the prediction results for difference scale factors are also compared. Comparison shows the effect of multiscale entropy on weighted HMM prediction, and steps are detailed next.

Step 1. DARPA2000 dataset is processed by Snort, yielding original alarm time sequence.

Step 2. Time sequence is processed by multiscale entropy method. It generates the entropy value of different scale data. Two data sets with the maximum and the minimum entropy values are selected as the input of the next step.

Step 3. Selected data sets are used to generate the multiorder state sequence matrix, which are regarded as the parameter to train the original data.

Step 4. Multiorder alarm time sequence matrix is trained using HMM, yielding the multiorder state transition probability matrix.

Step 5. The weighting algorithm is used to calculate the autocorrelation coefficient of each order of the time sequence.

Step 6. The weighted prediction algorithm is used to calculate the network security state at next time for each scale factor.

Step 7. The prediction result is used as the input the prediction iteration to predict the next security state.

Step 8. The difference between the prediction result and the actual value is evaluated by the MSE. Besides, the prediction results for different scale factors are also compared.

4.2. Data Preprocessing. In the mobile network, the DARPA2000 dataset is collected using Snort. The alarm type is selected as the original time sequence. Based on the calculation results of multiscale entropy, nine data sets with the scale factors from 2 to 10 are used in the experiments. For each scale factor, we divide the original data on the basis of scale, yielding the multiorder data matrixes. These matrixes

```
Input: alarm data, α, β
Output: triple <signature, srcIP, dstIP>
{
    (1) Record the number N of all alarms
    (2) Foreach signature in Snort
    (3)  alarms generated by signature are written in set A;
    (4)  record the number n of alarms in set A;
    (5)   If (n/N > α)
    (6)   all the srcIPs and dstIPs in A respectively construct set S and set D;
    (7)     Foreach srcIP in S
    (8)       If (the ratio of srcIP > β)
    (9)       Return <signature, srcIP, any>
    (10)        Endfor
    (11)     Foreach dstIP in D
    (12)       If (the ratio of dstIP > β)
    (13)       Return <signature,any, srcIP>
    (14)       Endfor
    (15)    endif
    (16)    Endfor
}
```

Algorithm 1: The extraction of alarm stream.

will be further trained by HMM, and the corresponding state transition probability matrixes are generated next.

The different order of matrix that corresponds to the different scale factor is used as HMM training data. Next, the corresponding state transition probability matrix is obtained, following formula (12), where s is scale factor and k (k=1,2,3,4) is multiorder transition probability.

$$P_s^k = \begin{bmatrix} p_{11}^{(k)}(t') & p_{12}^{(k)}(t') & p_{13}^{(k)}(t') & p_{14}^{(k)}(t') \\ p_{21}^{(k)}(t') & p_{22}^{(k)}(t') & p_{23}^{(k)}(t') & p_{24}^{(k)}(t') \\ p_{31}^{(k)}(t') & p_{32}^{(k)}(t') & p_{33}^{(k)}(t') & p_{34}^{(k)}(t') \\ p_{41}^{(k)}(t') & p_{42}^{(k)}(t') & p_{43}^{(k)}(t') & p_{44}^{(k)}(t') \end{bmatrix} \quad (12)$$

4.3. Implementation of Prediction Algorithm. The distribution of various attributes of alarm in mobile network is not uniform. By analysis, there are lots of alarm streams generated by a few attributes.

The alarm stream is represented by triple <Signature, src IP, dst IP>, where "Signature" is the rule to generate the alarm and "src IP" and "dst IP" are, respectively, original IP address and the destination IP address. First, the one-day alarms of intrusion detection system in mobile network are collected, as the ratio threshold α of "Signature" to generate the alarm and the ratio threshold β of IP to generate alarm are determined. If the ratio threshold of "Signature" exceeds the value of α, the corresponding src IP and dst IP should be recorded. Moreover, if the ratio threshold of IP to generate alarm exceeds the value of β, the triple will be further analyzed as shown in Algorithm 1.

The returned triple in algorithm will be recorded each hour. The alarm sequence of a certain triple can be denoted by a random process $\{x(t) : t \in N\}$, where x(t) is the number of alarms generated by the triple within t hours. The period of the sequence will be further analyzed with Algorithm 2.

5. Results and Discussion

5.1. Dataset. DARPA2000 is an offline intrusion detection dataset, available and maintained by MIT's Lincoln Laboratory [36]. It has become a standard dataset to verify effectiveness of intrusion alert correlation algorithm, scene construction algorithm, and trend prediction algorithm.

DARPA2000 dataset includes all monitored data package in demilitarized zone (DMZ) and the internal (INSIDE) by using TCPDUMP. The dataset contains instances in attack scenarios of LLDOS 1.0 and LLDOS2.0.2. In LLDOS1.0 scenario, the attacker captures and controls 3 hosts in Eyrie airbase via vulnerability of Solaris Sadmind, uploads Mstream tool, and performs DDOS attack on a government website. Different with LLDOS 1.0, LLDOS2.0.2 utilizes a more concealed method to seek host with vulnerability and setup Mstream.

In this research, we make use of DARPA2000 dataset to verify the effectiveness of the proposed algorithm. It contains two multistep DDOS attack scenarios. There are lots of data, redundancies, and false alarms in both scenarios. To verify the effectiveness of the method, we just take attack alarm data in five steps to complete the experiments: the attack scene time is about three hours to LLDDOS1.0 and about 1.5 hours for LLDDOS2.0.

5.2. Calculation of Multiscale Entropy. With corresponding formula, the original alarm time sequence can be calculated, and the scale factor is selected from 2 to 20. The histogram of entropy values is depicted in Figure 3.

In this figure, samples of entropy values change with the scale factor, where the minimum and the maximum values

Input: the alarm sequence $\{x(t) : t \in N\}$ generated by triple <*Signature, srcIP, dstIP*>
Output: alarm removal rule <*Signature,srcIP,dstIP*>
{
(1) select an alarm sequence $\{x(t) : 1 \le t \le N,\ N > 5p\}$ generated by a triple;
(2) determine the autocorrelation sequence $\{R(m) : 1 \le m \le N\}$;
(3) while $(1 \le f \le N)$
(4) calculate the energy value of frequency f;
(5) endwhile
(6) calculate the frequency f_{max} with the maximum energy;
(7) calculate the cycle of alarm sequence;
(8) calculate the value of F;
(9) if $F \ge F_\alpha (b - 1, nb - b)$
(10) generate the alarm removal rule <*Signature,srcIP,dstIP*>;
(11) Endif
}

Algorithm 2: Period analysis algorithm.

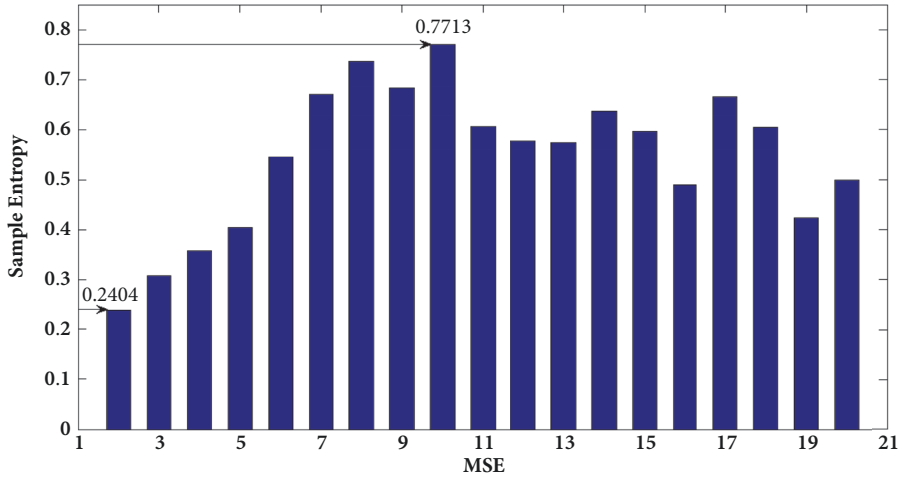

Figure 3: Multiscale entropy histogram sequence of the original data of the alarm time.

are obtained when the scale factors are 2 and 10, respectively. The value of entropy reflects complexity of time sequence and frequent changes of alarm data. Thus, the security situation can be easily reflected by entropy value. We assume that the entropy value has effect on prediction results, whose assumption will be further proven in experiments that follow next.

5.3. Weighted Prediction Performance. After calculating the formulas (5) and (6), the autocorrelation coefficients of the training data are obtained and normalized, as shown in Table 1.

The normalized autocorrelation coefficients are calculated as the weighted values, and the results are compared with the calculated results. The maximum probability of state is used as the prediction result at the next time.

We added the multiscale entropy method on the basis of method introduced in [35]. The overall changes of network security situation cannot be clearly observed due to dramatic changes, and therefore, we introduce Bezier curve to describe the overall trend of network security situation. Advantages using Bessel curve include smoothing the change curve of network security situation. The actual security situation prediction graph for LLDDOS2.0 is shown in Figure 4.

As depicted in this figure, the network security situation value is not high at the beginning. During this period, the network is attacked by Ipsweep scanning and the host is probed by Sadmind Ping. After 3:00 hours, the trend of value decreases during a period, which shows that the attacker has completely controlled the host. The rising trend reflects the attackers' launch DDOS attacks; the decline shown next reflects that the attack is gradually weakened. As a result, the trend curve is more vivid to describe the trend of the network security situation. It is helpful for administrators to manage the network security situation. After the preprocessing of the data, the multiorder state transition probability matrix is obtained. As listed in Tables 2 and 3 the state transition probability matrix when the scale factors are 2 and 10.

As the original data is preprocessed to generate the matrix of multiorder state transition probability with different scales,

Table 1: The autocorrelation coefficients training data and the normalized results.

Evaluation	Order 1	Order 2	Order 3	Order 4
r_k	0.5628	0.4658	0.4507	0.2757
w_k	0.3207	0.2654	0.2568	0.1571

Table 2: The state transition probability matrix when scale factor =2.

Prediction step	State	G	P	A	C
P=1	G	0.9168	0.0012	0.0385	0.0435
	P	0.0615	0.9259	0.0126	0.0000
	A	0.0000	0.0000	1.0000	0.0000
	C	0.0000	0.0000	0.0015	0.9985
P=2	G	0.8156	0.0000	0.1755	0.0086
	P	0.0042	0.9956	0.0000	0.0000
	A	0.0000	0.0000	0.9861	0.0138
	C	0.0021	0.0000	0.0018	0.9961
P=3	G	0.7271	0.0032	0.2697	0.0000
	P	0.1689	0.8311	0.0000	0.0000
	A	0.0000	0.0866	0.8864	0.0269
	C	0.0000	0.0000	0.0000	1.0000

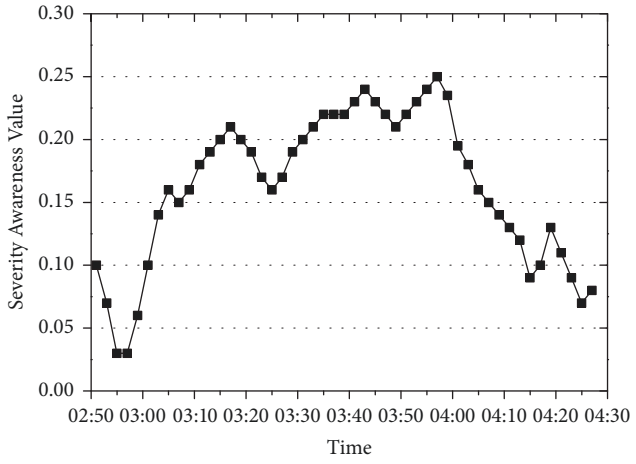

Figure 4: The actual value of network security situation.

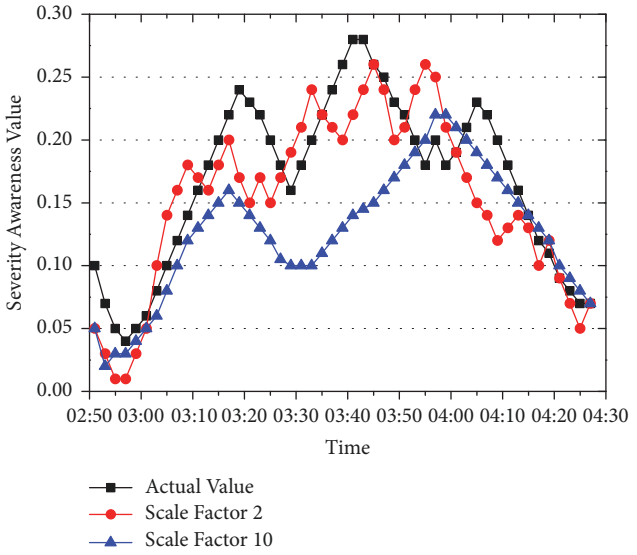

Figure 5: The one-step prediction result.

the scale factor as 10 and the order as 4 are chosen for evaluation. The prediction results are listed in Table 4.

In Table 4, C is shown to be the secure state at the next time with the largest probability, representing that the host is intruded under a dangerous state. The confidentiality, integrity, and availability are damaged. In this case, corresponding measures should be adopted and result in the fact that Table 4 can be used as the input of the next iteration for future prediction.

The probability of each state at the next moment of time sequence is obtained through this proposed method. The value of the probability is used to determine the status of the security situation. Figure 5 shows the actual value and the predictive value of the different scale factors in the time period from 2:51 to 4:25 hours. The horizontal axis represents time and the vertical axis represents the security situation. It shows the actual value of security situation; curves with other color represent the prediction results of different scales. The overall trend predictions and actual values are almost the same. It demonstrates the effectiveness of the weighted prediction method proposed in this paper.

The MSE is introduced to illustrate the different scaling factors of prediction and the difference between actual and predictive value. The multiscale entropy and the MSE values in one-step prediction are listed in Table 5.

The different scale factor corresponding to RMSE and MSE in one-step prediction is shown in Table 5. As the scale factor is 2, it gets smaller entropy and larger RMSE, and with the scale factor 10, the results are opposite ones. Therefore,

Table 3: The state transition probability matrix when scale factor =10.

Prediction step	State	G	P	A	C
P=1	G	0.8357	0.0657	0.0801	0.0185
	P	0.0487	0.8778	0.0736	0.0000
	A	0.0015	0.0187	0.9763	0.0035
	C	0.0139	0.0108	0.0000	0.9753
P=2	G	0.7155	0.0311	0.2238	0.0295
	P	0.1148	0.8192	0.0660	0.0000
	A	0.0076	0.0271	0.9578	0.0075
	C	0.0257	0.0214	0.0000	0.9529
P=3	G	0.5375	0.0698	0.3236	0.0691
	P	0.1557	0.7434	0.1009	0.0000
	A	0.0015	0.0802	0.8802	0.0381
	C	0.0396	0.0000	0.0101	0.9503

Table 4: Results of security situation prediction at next time.

Initial state	delay		G	P	A	C
P	1	0.321	0.0487	0.8778	0.0736	0.0000
C	2	0.265	0.0257	0.0214	0.0000	0.9529
C	3	0.257	0.0396	0.0000	0.0101	0.9503
A	4	0.157	0.0000	0.0000	0.9888	0.0112
	Weighting sum P_i		0.03262	0.2874	0.1815	0.4985

Table 5: The multiscale factor and the MSE /RMSE values in one-step prediction.

Scale factors	2	3	4	5	6	7	8	9	10
MSE	0.2404	0.3082	0.3586	0.4051	0.5456	0.6720	0.7372	0.6839	0.7713
RMSE	0.1849	0.1885	0.1887	0.1877	0.1865	0.1857	0.1771	0.1849	0.1849

Table 6: The multiscale factor and the MSE /RMSE values in two-step prediction.

Scale factors	2	3	4	5	6	7	8	9	10
MSE	0.2404	0.3082	0.3586	0.4051	0.5456	0.6720	0.7372	0.6839	0.7713
RMSE	0.1989	0.1978	0.1975	0.1971	0.1981	0.1976	0.1891	0.1968	0.1968

Table 7: The multiscale factor and the MSE /RMSE values in three-step prediction.

Scale factors	2	3	4	5	6	7	8	9	10
MSE	0.2404	0.3082	0.3586	0.4051	0.5456	0.6720	0.7372	0.6839	0.7713
RMSE	0.1919	0.1986	0.1982	1980	1973	1946	0.1829	0.1919	0.1919

scale factor with larger entropy entails prediction with higher accuracy, what verifies the assumption presented in previous section. In addition, RMSE and MSE are verified between predicted value and real value under scale factor from 2 to 10 with the step length of 2 and 3. Weighted prediction method can be used to predict security state at the next moment. It can also predict the results of iterations to obtain the future network security conditions within period. The prediction results and root mean square error values with different scale factors and different steps are given in Tables 6 and 7 and Figures 6 and 7.

The prediction curves show the predictive values are close to actual values, what demonstrates the effectiveness of the proposed weighted HMM algorithm. At the same time, it is possible to note that the change on prediction steps will not affect the effectiveness of multiscale factor predicted results.

6. Conclusions

Current HMM-based prediction algorithms predict the unknown state via a known state. It has limitations and the prediction accuracy is not high enough. To address this issue,

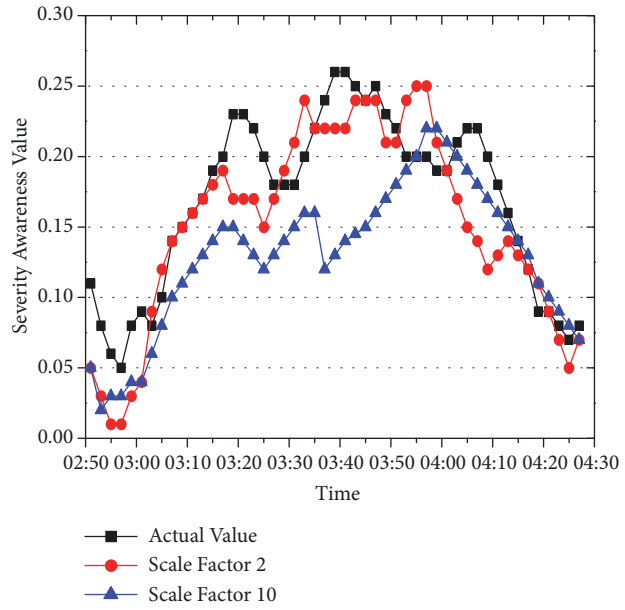

Figure 6: The two-step prediction result.

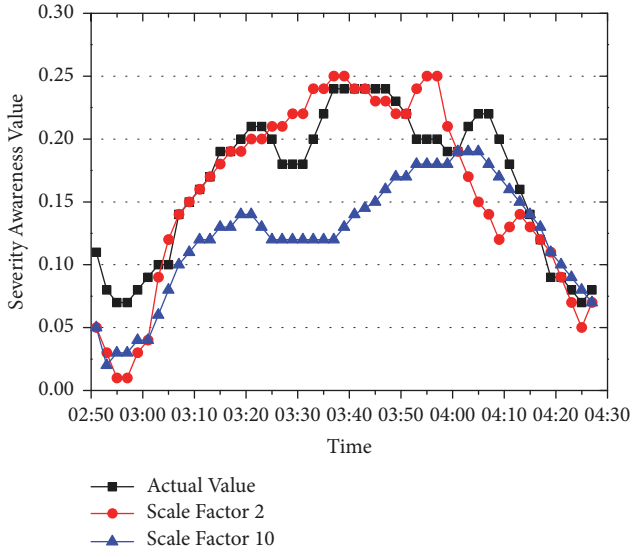

Figure 7: The three-step prediction result.

this work presents the application of the weighted HMM model to predict the security situation of mobile networks, where the multiscale entropy method is used to select the appropriate scale factor of the data. It will be regarded as training data for HMM model to obtain the state transfer probability matrix, whilst the correlation coefficients are considered as weights to predict changes of network security situation. In the proposed model, we use the alarm time sequence as original data, and with the multiscale entropy method, an appropriate scale factor is selected as training data to train the parameters in HMM model. Finally, the predictive results are evaluated and compared to real security situation. Experimental results have shown that the proposed method is accurate and effective. Weighted method can not only use current network state, but also consider the historical security situation. The dependent relationship between the security situations is fully used. It could predict network security at the next state. The network security administrator could take measures to maintain network security and avoid more attacks in advance.

Based on the prediction issues in mobile network, several security situation prediction algorithms are analyzed as follows: (1) there is causal relationship between attack behaviors, (2) the probability to occur different attacks is different, (3) the evidence of future attacks includes the attack itself, (4) the purpose of attack can be inferred, and (5) the evidence of future attacks has relationship with the change of network security situation. These features provide a thought to predict the security situation by extracting evidence. Besides, other aspects can be also researched, such as real-time data extraction and data fusion of multisource heterogeneous sensors.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Science Foundation of China (Grant 61572188), Xiamen Science and Technology Foundation (Grant 3502Z20173035), Scientific Research Program of New Century Excellent Talents in Fujian Province University, Fujian Provincial Natural Science Foundation of China (Grant 2018J01570), the CERNET Innovation Project (Grant NGII20170411), the National Nature Science Foundation of Fujian Province (Grant 2018J01544), the Scientific Research Program of Outstanding Young Talents in Universities of Fujian Province, the Key Project of Natural Foundation for Young in Colleges of Fujian Province (Grant JZ160466), and Hunan Provincial Natural Science Foundation of China (Grant 2016jj2058).

References

[1] S. Touboul, "System and method for providing network security to mobile devices," *Yoggie Security Systems*, 2017.

[2] W. Liang, Y. Xie, and X. Chen, "A two-step MF signal acquisition method for wireless underground sensor networks," *Computer Science & Information Systems*, vol. 13, no. 2, pp. 623–638, 2016.

[3] W. Liang, Y. Huang, J. Xu, and S. Xie, "A distributed data secure transmission scheme in wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 13, no. 4, pp. 1–11, 2017.

[4] W. Liang, Z. Ruan, Y. Wang, and X. Chen, "RESH: a secure authentication algorithm based on regeneration encoding self-healing technology in WSN," *Journal of Sensors*, vol. 2016, 11 pages, 2016.

[5] R.-F. Wu and G.-L. Chen, "Research of network security situation prediction based on multidimensional cloud model," in *Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS '12)*, pp. 409–414, July 2012.

[6] J. Wang, M. Ouyang, W. Liang, and J. Hou, "Device-to-device relay cooperative transmission based on network coding," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 7, 2017.

[7] J. Wang, W. Luo, W. Liang, X. Liu, and X. Dong, "Locally minimum storage regenerating codes in distributed cloud storage systems," *China Communications*, vol. 14, no. 11, pp. 82–91, 2017.

[8] C. Jiang, T. Li, J. Liang, and H. Wu, "Low-latency and energy-efficient data preservation mechanism in low-duty-cycle sensor networks," *Sensors*, vol. 17, no. 5, p. 1051, 2017.

[9] Snot, https://www.snort.org/, 2017-12-21.

[10] CVE, http://cve.mitre.org/, 2017-12-23.

[11] Bugtraq, http://www.bugtraq-team.com/, 2017-12-23.

[12] CVSS, http://resources.infosecinstitute.com/common-vulnerability-scoring-system/, 2017-12-23.

[13] C. Kruegel and W. Robertson, "Alert Verification - Determining the Success of Intrusion Attempts," pp. 1-14, 2004.

[14] Nessus, https://www.tenable.com/products/nessus/nessus-professional, 2017-12-23.

[15] P. A. Porras, M. W. Fong, and A. Valdes, "Mission-impact-based approach to INFOSEC alarm correlation," in *Proceedings of the International Conference on Recent Advances in Intrusion Detection*, pp. 95–114, Springer-Verlag, 2002.

[16] H. Shake, B. Hazzard, and D. Marquis, "Assessing network infrastructure vulnerabilities to physical layer attacks," in *Proceedings of the 22nd National Information Systems Security Conference*, 1999.

[17] T. Bass, "Intrusion detection systems and multisensor data fusion," *Communications of the ACM*, vol. 43, no. 4, pp. 99–105, 2000.

[18] F. Hock and P. Kortiš, "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks," in *Proceedings of the 13th IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA '15)*, pp. 1–4, November 2015.

[19] D. A. Bhosale and V. M. Mane, "Comparative study and analysis of network intrusion detection tools," in *Proceedings of the 1st International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT '15)*, pp. 312–315, October 2015.

[20] W. Hu, J. Li, X. Chen, X. Jiang, and M. Zuo, "Scalable model for network situational awareness based on Endsley's situation model," *High Technology Letters*, vol. 13, no. 4, pp. 395–401, 2007.

[21] A. Årnes, F. Valeur, G. Vigna, and R. A. Kemmerer, "Using hidden Markov models to evaluate the risks of intrusions system architecture and model validation," *Lecture Notes in Computer Science*, vol. 4219, pp. 145–164, 2006.

[22] W. Liang, Z. Chen, X. Yan, X. Zheng, and P. Zhuo, "Multi-scale entropy-based weighted hidden markov network security situation prediction model," in *Proceedings of the 2nd IEEE International Congress on Internet of Things (ICIOT '17)*, pp. 97–104, June 2017.

[23] K.-L. Yap and Y.-W. Chong, "Optimized access point selection with mobility prediction using hidden Markov model for wireless network," in *Proceedings of the 9th International Conference on Ubiquitous and Future Networks (ICUFN '17)*, pp. 38–42, July 2017.

[24] X. Tan, W. Wang, and X. Hong, "A hidden markov model used in intrusion detection," *Journal of Computer Research & Development*, 2003.

[25] G. Zhu, K. Song, P. Zhang, and L. Wang, "A traffic flow state transition model for urban road network based on Hidden Markov Model," *Neurocomputing*, vol. 214, pp. 567–574, 2016.

[26] H. A. Kholidy, A. Erradi, S. Abdelwahed, and A. Azab, "A finite state hidden markov model for predicting multistage attacks in cloud systems," in *Proceedings of the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC '14)*, pp. 14–19, August 2014.

[27] N. Luktarhan, X. Jia, L. Hu, and N. Xie, "Multi-stage attack detection algorithm based on hidden markov model," in *Web Information Systems and Mining*, vol. 7529 of *Lecture Notes in Computer Science*, pp. 275–282, Springer Berlin Heidelberg, 2012.

[28] M. Costa, A. L. Goldberger, and C.-K. Peng, "Costa, goldberger, and peng reply," *Physical Review Letters*, vol. 92, no. 8, 2004.

[29] M. Costa, A. L. Goldberger, and C. Peng, "Multiscale entropy analysis of biological signals," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 71, no. 2, 2005.

[30] R. Istenič, P. A. Kaplanis, C. S. Pattichis, and D. Zazula, "Multiscale entropy-based approach to automated surface EMG classification of neuromuscular disorders," *Medical & Biological Engineering & Computing*, vol. 48, no. 8, pp. 773–781, 2010.

[31] P. Xie, G.-Q. Jiang, X. Wu, and X.-L. Li, "Rolling bearing fault diagnosis based on multiscale entropy and distance evaluation," *Acta Metrologica Sinica*, vol. 34, no. 6, pp. 548–553, 2013.

[32] E. Martina, E. Rodriguez, R. Escarela-Perez, and J. Alvarez-Ramirez, "Multiscale entropy analysis of crude oil price dynamics," *Energy Economics*, vol. 33, no. 5, pp. 936–947, 2011.

[33] Y. Ruo-Yu and Z. Qing-Hua, "Multi-scale entropy based traffic analysis and anomaly detection," in *Proceedings of the 8th International Conference on Intelligent Systems Design and Applications (ISDA '08)*, pp. 151–157, Kaohsuing, Taiwan, November 2008.

[34] Y. Feng and W. Han, "The application of weighted Markov-chain to the prediction of river runoff state," *Systems Engineering—Theory & Practice*, vol. 19, no. 10, pp. 89–94, 1999.

[35] J. Lei, *Research on Network Security Threats and Situation Assessment*, Huazhong University of Science and Technology, 2008.

[36] MIT Lincoln Laboratory, https://www.ll.mit.edu/r-d/datasets.