Alarm Elements Based Adaptive Network Security Situation Prediction Model

Hongyu Yang[1(✉)], Le Zhang[1], Xugao Zhang[1], Guangquan Xu[2], and Jiyong Zhang[3]

[1] School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China
yhyxlx@hotmail.com
[2] College of Intelligence and Computing, Tianjin University, Tianjin 300350, China
[3] Swiss Federal Institute of Technology in Lausanne, 1015 Lausanne, Switzerland

Abstract. To improve network security situation prediction accuracy, an adaptive network security situation prediction model based on alarm elements was proposed. Firstly, we used the entropy correlation method to generate the network security situation time series according to Alarm Frequency (AF), Alarm Criticality (AC) and Alarm Severity (AS). Then, the initial situation predicted value is calculated through sliding adaptive cubic exponential smoothing. Finally, based on the error state, we built the time-varying weighted Markov chain to predict the error value and modify the initial predicted value. The experimental results show that the network security situation prediction results of this model have a better fit with the real results than other models.

Keywords: Network situation · Alarm element · Entropy correlation · Cubic exponential smoothing · Time-varying weighted Markov · Predicated value

1 Introduction

With the rapid development of computer network technology, great changes have taken place in the network structure and interaction scenarios, making network security a key issue in the field of work and life. In order to avoid losses in all aspects, the evaluation of network security is particularly important. According to the historical information in the network structure, it is the hotspot of network security research to complete the prediction of network security situation and the evaluation of security status. The network security situation prediction forms a nonlinear time series through the factors affecting network security. Based on the historical data and the current network state, the network security status is predicted in a future period through a specific mathematical model, which facilitates network management personnel to detect threats in time and take corresponding protective measures. Currently used network security situation prediction methods include gray prediction method, time series based prediction and neural network based prediction [1].

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 41–53, 2021.
https://doi.org/10.1007/978-3-030-66922-5_3

Zhang et al. [2] proposed a network security situation prediction model based on grey neural network with multi-group chaotic particle optimization. The model improves the prediction of network conditions by establishing a nonlinear mapping relationship between the influence factors of the security situation and the situation and using the multi-group chaotic particles to optimize the key parameters of the gray neural network. Xiao et al. [3] proposed a network security situation prediction method based on MEA-BP. The method uses the Mind Evolution Algorithm (MEA) to optimize the weight and threshold of the BP neural network to improve the prediction accuracy and efficiency of the security situation, but the standardization of historical data is not perfect. Sun et al. [4] proposed a Markov prediction model based on complex networks. The model constructs the transformation relationship of network security status into a complex network, and uses the weighted Markov chain to predict the security situation, which can reflect the security status of the network to a certain extent, but the state transition probability matrix constructed by the multi-state network is too large. Zhou et al. [5] proposed a network multi-node security situation prediction model based on improved G-K algorithm. The model extracts the main factors affecting network security by grey entropy correlation method. Based on this, the Kalman filter equation is established to improve the accuracy of security situation prediction. Zhang et al. [6] reduced the training complexity of neural network situation prediction model by improving convolutional neural network, and improved the efficiency of network security situation prediction, but the quality of extracted features needs to be improved.

In view of the uneven quality of historical data in the above network security situation prediction methods and the lack of accuracy of the above methods for multi-peak changes in network security situation prediction, in order to improve the accuracy of network security situation prediction, this paper proposes an adaptive network security situation prediction model based on alarm elements.

2 Network Security Situation Prediction Model

The network security situation prediction model proposed in this paper is shown in Fig. 1.

The network security situation prediction process is designed as follows:

Step 1: Generating a non-linear time series of safety situation values by using an entropy correlation method based on the network alarm information;
Step 2: Using a sliding window to divide the network security situation value sequence segment, and each time a security situation value is updated, the sliding window slides backward by one unit;
Step 3: Establish a three-dimensional exponential smoothing prediction model based on the safety situation sequence in the sliding window, and adaptively adjust the static smoothing coefficient α □ to improve the prediction accuracy of the module;
Step 4: Calculate the error between the predicted and actual value of the safety situation in the sliding window, and divide the error into n error intervals, which are recorded as n error states. Using a time-varying weighted Markov chain to predict the error value and correct the situation predictor;

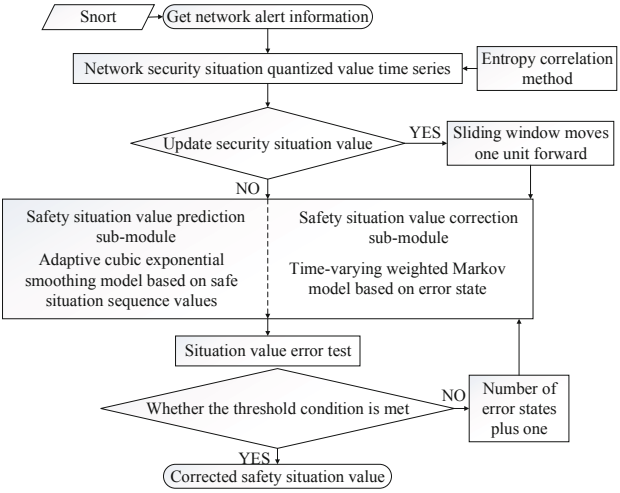

Fig. 1. Network security situation prediction model diagram

Step 5: Check the error. If the threshold condition is not met, return to step 4 and divide the error state into $n + 1$; if the threshold condition is met, obtain the next cycle safety situation value according to steps 1–4.

3 Quantification of Network Security Situation Assessment

First, the alarm information is acquired based on the Snort intrusion detection system. Then, the entropy correlation method is used to calculate the network security situation value in each quantization period. The specific method is designed as follows:

The network security situation quantified value is determined by Alarm Frequency (AF), Alarm Criticality (AC), and Alarm Severity (AS). Referring to the alarm quality quantification method [7], the observation vector obtained by this method based on the alarm quality can effectively improve the data source and the evaluation accuracy. Therefore, the alarm with the highest quality quantization value is selected as the basis for quantifying the network security situation in each cycle.

Let a total of T quantization periods, the network security situation quantization value of the i-th cycle is V_i ($i = 1, 2, \cdots, T$), and the alarm with the highest quality quantization value of the i-th cycle is H_i, then define $V_i = V_i\ (AF_{Hi}, AC_{Hi}, AS_{Hi})$ ($i = 1, 2, \cdots, T$), where

$$\mathrm{AF}_{Hi} = \frac{H_i \ number\ of\ \ alarms\ in\ T_i}{Number\ of\ \ all\ alarms\ in\ T_i} \tag{1}$$

AC_{Hi} is the critical degree of the alarm H_i, indicating the possibility that the occurrence of the alarm H_i causes a change in the network security state. When AC_{Hi} is higher, it means that the network security state is more likely to change. If the alarm AC_{Hi} is an alarm that has occurred in the period i, its priority is set to 1; If the alarm is generated in the period $i - N$ to the period $i - 1$, the priority is 2; If there is no alarm in the

AC_{Hi} from period i-N to period $i-1$, the priority is set to 3. According to the intrusion detection alarm aggregation association algorithm [8], the algorithm aims at acquiring intrusion-detection alerts and relating them together to expose a more condensed view of the security issues raised by intrusion-detection systems, this paper takes $N = 2$.

AC_{Hi} is the severity of the alarm and indicates the negative impact of the alarm on the network. The greater the severity, the greater the impact of H_i on the network security status. In this paper, the severity of the alarm is divided into low, general, and high, and the corresponding priority values are 1, 2, and 3.

In order to quantify the network security situation of the period i, the comment support matrix P is set as shown in Table 1. Let $X_1 = AF_{Hi}$, $X_2 = AC_{Hi}$, $X_3 = AS_{Hi}$, then X_1, X_2, X_3 correspond to the three quantitative indicators of the alarm H_i with the highest alarm quality in period i, namely alarm frequency, alarm criticality and alarm severity; p_{ij} indicates The degree to which the i-th indicator supports the j-th comment $(i, j \in 1, 2, 3)$.

Table 1. Comment support matrix diagram

Index	Low	General	High
X_1	P_{11}	P_{12}	P_{13}
X_2	P_{21}	P_{22}	P_{23}
X_3	P_{31}	P_{32}	P_{33}

Among them, X_1's support for each comment is determined according to Table 2.

Table 2. X_1 comment interval table

Comment	Low	General	High
Frequency interval C_j	[0, 0.3)	[0.3, 0.7)	[0.7, 1]

Let $X_1 = x$, then calculate the support of the index for each comment by formula (2):

$$P_{ij} = \frac{1 - \left|x - \left((a_j + b_j)/2\right)\right| + \left(b_j - a_j\right)/2}{\sum_{j=1}^{3}\left[1 - \left|x - \left((a_j + b_j)/2\right)\right| + \left(b_j - a_j\right)/2\right]} \tag{2}$$

Where a_j and b_j respectively correspond to the lower end point and the upper end point of the interval $c_j, j = 1, 2, 3$.

The support for X_2 and X_3 for each comment is shown in Table 3.

Table 3. X_2, X_3 Comment support scale table

Priority	Low	General	High
1	0.5	0.333	0.167
2	0.25	0.5	0.25
3	0.167	0.333	0.5

Use Eq. (3) to calculate the absolute entropy of each indicator of the alarm:

$$H_i = -\sum_{j=1}^{n} P_{ij} \ln P_{ij} \tag{3}$$

When $P_{i1} = P_{i2} = \ldots = P_{in}$, $H_{max} = \ln n$, the relative entropy values of the alarm indicators are:

$$\mu_i = -\frac{1}{\ln n} \sum_{j=1}^{n} P_{ij} \ln P_{ij} \tag{4}$$

The larger the relative entropy value of an indicator is, the smaller the influence of the indicator on the quantized value of the alarm is, the weight of the corresponding indicator is represented by $(1 - \mu_i)$, namely:

$$\tau_i = \frac{1}{n - \sum_{i=1}^{n} \mu_i} (1 - \mu_i) \tag{5}$$

Where $\tau_i \in [0, 1]$ and $\tau_1 + \ldots + \tau_n = 1$. τ_i is the entropy weight coefficient of the index X_i. The vector of the comment weight is $W = (w_{low}, w_{normal}, w_{high}) = (1/5, 1/3, 7/15)$ [9]. Then the network security situation value operator [10] of period i is:

$$V_i = \mu \cdot \tau \cdot P \cdot W^T \tag{6}$$

Among them, μ is the correction factor, this paper takes $\mu = 10000$. The higher the security situation value, the greater the threat to the network and the less optimistic the network security situation.

4 Network Security Situation Prediction Sub-module

4.1 Sliding Window Mechanism

In view of the failure problem of the exponential smoothing prediction method under long time series, this paper defines the length of the historical data sequence based on the three-index exponential prediction by the sliding window mechanism.

Let the sliding window width be L (L is a positive integer), and the current network security posture values are arranged in chronological order as V_1, V_2, …, V_m (m is a positive integer), then the sliding window mechanism is designed as follows:

(1) If the number of safety situation values in the sliding window is k ($1 \le k \le m$), the sequence of safety situation values in the width of the sliding window is $V_1^{'}$, $V_2^{'}$, …, $V_k^{'}$. If $k + 1 \le L$, the window does not move, predicting the $m + 1$th safety situation value and waiting for a new safety situation value to enter the window.
(2) If $k + 1 > L$, the sliding window moves forward by one unit when a new safety situation value is added to the sequence, and the safety situation value of the $m + 1$th period is predicted based on the sequence value in the new window.

4.2 Adaptive Cubic Exponential Smoothing Model

Let the network security situation value of m period currently have V_1, V_2, …, V_m, and there are k security situation values in the sliding window width. If $m \le L$, then $V_1^{'} = V_1$ and $V_k^{'} = V_m$; if $t > L$, then $V_1^{'} = V_{m-L+1}$, and $V_k^{'} = V_m$. This paper proposes a network security situation prediction model based on the cubic exponential smoothing method:

$$V_{t+T}^{1} = a_t + b_t T + c_t T^2 \tag{7}$$

$$a_t = 3s_t^{(1)} - 3s_t^{(2)} + s_t^{(3)} \tag{8}$$

$$b_t = \frac{\alpha}{2(1-\alpha)^2}\left[(6-5\alpha)s_t^{(1)} - 2(5-4\alpha)s_t^{(2)} + (4-3\alpha)s_t^{(3)}\right] \tag{9}$$

$$c_t = \frac{\alpha^2}{2(1-\alpha)^2}\left(s_t^{(1)} - 2s_t^{(2)} + s_t^{(3)}\right) \tag{10}$$

$$s_t^{(1)} = \alpha X_t + (1-\alpha)s_{t-1}^{(1)} \tag{11}$$

$$s_t^{(2)} = \alpha s_t^{(1)} + (1-\alpha)s_{t-1}^{(2)} \tag{12}$$

$$s_t^{(3)} = \alpha s_t^{(2)} + (1-\alpha)s_{t-1}^{(3)} \tag{13}$$

In Eqs. (7)–(13), $V_{t+T}^{'}$ is the predicted value of the $t + T$ safety situation, T is the predicted lead period, and X_t is the actual value of the safety situation in the tth period. $S_t^{(1)}$, $S_t^{(2)}$, and $S_t^{(3)}$ are the first, second, and third smoothing indices of the t-th period; a_t, b_t, c_t are the prediction coefficients of the t-th period; $s_{t-1}^{(1)}$, $s_{t-1}^{(2)}$, and $s_{t-1}^{(3)}$ are the initial values of the first, second and third exponential smoothing of the tth period. In this paper, the initial value of the smoothing index is $s_0^{(1)} = s_0^{(2)} = s_0^{(3)} = (V_1^{'} + V_2^{'} + V_3^{'})/3$; α is the static smoothing coefficient, and $\alpha \in [0, 1]$, its value indirectly affects the final prediction accuracy. Generally, when the actual value sequence shows a horizontal trend, $\alpha \in [0.05, 0.2]$; when the actual value sequence fluctuates, but the long-term fluctuation is small, $\alpha \in [0.3, 0.5]$; when the actual value sequence fluctuates greatly, it is obvious When rising or falling, $\alpha \in [0.6, 0.8]$. The larger the value of x, the greater the impact of the forward data on the predicted value. In order to adapt to the sliding window mechanism caused by the change of the actual value sequence, in this paper, we propose to minimize the sum of the absolute errors of predicted and actual values, and aim at this to obtain the optimal dynamic solution of α. The optimal dynamic solution process for α is designed as follows:

Step 1. It is assumed that the k network security situation actual values in the current sliding window constitute a vector $V' = (V_1^{'}, V_2^{'}, \cdots, V_k^{'})$, and the static smoothing coefficient α initial value is 0.
Step 2. It is known that $s_0^{(1)} = s_0^{(2)} = s_0^{(3)} = (V_1^{'} + V_2^{'} + V_3^{'})/3$, and $X_1 = V_1^{'}$. From Eqs. (11)–(13), $s_t^{(1)}, s_t^{(2)}, s_t^{(3)}$ $(t = 0, 1, \cdots, k)$ are obtained, and from the Eqs. (8)–(10), a_t, b_t, c_t are obtained $(t = 0, 1, \cdots, k)$.
Step 3. Let $t = 0, 1, \cdots, k-1$, let the lead prediction period $T = 1$, and obtain the predicted value sequence $V_1 = (V_1^1, V_2^1, \cdots, V_k^1)$ based on the current static smoothing coefficient from Eq. (7).
Step 4. The sum of the absolute values of the errors of the predicted value sequence and the actual value sequence is $E = \sum_{i=1}^{k} \left| V_i^1 - V_i^{'} \right|$, $\alpha = \alpha + 0.001$;
Step 5. Repeat steps 1–4 to $\alpha = 1$, and record the absolute error generated by each cycle as E_j $(j = 0, 1, \cdots, 1000)$, and obtain min $\{E_j\}$ (j = 0, 1, $\cdots$, 1000). The corresponding α value is taken as the optimal dynamic solution of the static smoothing coefficient under the current sliding window, and is denoted as α_{best}.
Step 6. Let $t = k$=m, $\alpha = \alpha_{best}$, $T = 1$, and obtain the safety situation value of the $m+1$th cycle from Eqs. (7)–(13).

5 Predictive Value Correction Sub-module

According to the theoretical analysis, it can be known that the initial predicted value of the network security situation in each period is in error with the actual value of the known security situation in the same window, and the error is related to the fluctuation of the security situation in the sliding window. In order to reduce the difference between the predicted value and the actual safety situation quantization value, this paper proposes a time-varying weighted Markov correction model based on error state.

5.1 Error State Division

As the new security situation is added, the sliding window moves, and the volatility of the network security situation sequence contained in the sliding window changes, and the distance between the upper and lower limits of the error also changes. Suppose there are k known safe situation values in the current sliding window, taking $V = \{V_i^{'} \mid i = 1, 2, 3, \cdots, k\}$, and the corresponding safety situation prediction value is $V^1 = \{V_i^1 \mid i = 1, 2, 3, \cdots, k\}$, the lower limit of the error is $F^L = \min\{V_i^1 - V_i^{'} \mid i = 1, 2, 3, \cdots, k\}$, and the upper limit of the error is $F^U = \max\{V_i^1 - V_i^{'} \mid i = 1, 2, 3, \cdots, k\}$, the distance between the upper and lower limits of the error is denoted as $FL = F^U - F^L$. The process of dividing the error state is designed as follows:

Step 1. The upper and lower limits of the error are divided into n intervals, and the interval length is FL/n, and the interval range is $[F^L, F^L + FL/n)$, $[F^L + FL/n, F^L + 2FL/n)$, $\cdots$, $[F^L + (\mathrm{n} - 1) \bullet FL/n, F^U]$.

Step 2. The sequence of error values in the current sliding window is $F = \{F_i = V_i^1 - V_i^{'} \mid i = 2, 3, \cdots, k\}$. If $F_i \in [F^L + (j-1) \bullet FL/n, F^L + j \bullet FL/n)$, then the error F_i is in the error state j, where $j \in \{1, 2, \cdots, n\}$. In particular, when $F_i = F^U$, F_i is considered to be in state n.
Step 3. If the predicted value does not satisfy the threshold test requirement after the error correction, the number of error states needs to be increased, that is, $n = n + 1$ to refine the error correction result.

5.2 Time-Varying Weighted Markov Chain Based on Error State

Based on the sequence of error states in the current sliding window, this paper uses the time-varying weighted Markov chain to predict the error value. The error prediction process is designed as follows:

Step 1. Determine an error state transition probability matrix. There are currently n error states, the current period is t, the error state at the adjacent time is $f_{t-1}f_t$, and the error state after q cycles is recorded as f_{t+q}, then

$$p_{ijr} = p\{f_{t+q} = r \mid f_{t-1} = i, f_t = j\}, i, j, r \in 1, 2, \cdots, n$$

Wherein, p_{ijr} represents the probability that the error state of the period $t-1$ is i, and the error state of the period t is j, and the error state is r after q cycles, and the probability is obtained by a statistical method. When the initial value of the error state number n is 3, the q-order error state transition probability matrix is

$$P^q_{(n\times n)\times n} = \begin{pmatrix} p_{111} & p_{112} & \cdots & p_{11n} \\ p_{121} & p_{122} & \cdots & p_{12n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{nn1} & p_{nn2} & \cdots & p_{nnn} \end{pmatrix} \tag{14}$$

$q = 1, 2, \cdots, \beta$. In this paper, $\beta_0 = [L/3]$, L is the sliding window width, and the X value adjustment is determined by step 3.
Step 2: Calculate the weight of each order error state transition probability matrix. First calculate the correlation coefficient η_q between $f_{t-1}f_t$ and f_{t+q}

$$\eta_q = \frac{\sum_{t=1}^{n-q}(y_{t-1} + y_t - 2\overline{y})(y_{t+q} - \overline{y})}{\sqrt{\sum_{t=1}^{n-q}(y_{t-1} + y_t - 2\overline{y})^2 \sum_{t=1}^{n-q}(y_{t+q} - \overline{y})^2}} \tag{15}$$

Where $q = 1, 2, \cdots, \beta$; y_{t-1}, y_t, y_{t+q} respectively represent the error value of period $t-1$, period t and period $t+q$ in the original error sequence in the current window. $\bar{y}$ represents the average of the original error sequence in the current window. Then the q-order error state transition probability matrix weight q is

$$\omega_q = \frac{|\eta_q|}{\sum_{q=1}^{\beta}|\eta_q|}, \ q = 1, 2, \ldots, \beta \tag{16}$$

Step 3. Adjust the value of β. Check the value of ω_β, and set the weight threshold of the error state transition probability matrix to 0.05 [11]. If $\omega_\beta < 0.05$, it indicates that the β-order error state transition probability matrix can ignore the error, and discard the matrix, $\beta = \beta - 1$, recalculate the value of ω_β until $\omega_\beta \geq 0.05$, at this time $q_{max} = \beta$.
Step 4. The error of the predicted value of the security situation in the current window is predicted. The probability that the error value of the period t + 1 is in the error state r ($r = 1, 2, \ldots, n$) is $P_{r(t+1)}$

$$p_{r(t+1)} = \sum_{q=1}^{\beta} p_{ijr}^{(q)} \cdot w_q \tag{17}$$

Where $q = 1, 2, \ldots, \beta$; $i, j \in 1, 2, \ldots, n$, $p_{ijr}^{(q)}$ is taken from the q-order error state transition probability matrix P^q, which represents probability of the adjacent error state $f_{t-q} = i, f_{t-q+1} = j$ steering error state $f_{t+1} = r$. q is the q-order error state transition probability matrix weight, then the error state probability distribution vector of period $t + 1$ is $P_{r(t+1)} = \{p_{1(t+1)}, p_{2(t+1)}, \ldots, p_{n(t+1)}\}$.

Let the error median vector composed of the median values of each error interval be

$$F_{mid} = \{[F^L + (F^L + FL/n)]/2, [F^L + FL/n + (F^L + 2FL/n)]/2, \ldots, [F^L + (n-1) \cdot FL/n + F^U]/2\},$$

Then the error prediction value operator at time $t + 1$ is

$$F_{t+1}^{'} = P_{r(t+1)} \cdot F_{mid} \tag{18}$$

The $t + 1$ time prediction value correction result is

$$V_{c(t+1)} = V_{(t+1)}^{1} - F_{(t+1)}^{'} \tag{19}$$

Among them, V_{t+1}^{1} is the uncorrected security situation prediction value based on the network security situation prediction sub-module.

5.3 Threshold Test

The proximity of the corrected safety situation predictor value to the actual value is analyzed to determine whether the error state division number n is sufficient. It is known that the sequence of corrected safety situation predictors and the actual value sequence in a window are as shown in Table 4.

Table 4. Sequence table of predicted and actual values

Correction value	$V_{c(2)}$	$V_{c(3)}$	$\cdots$	$V_{c(k)}$
Actual value	V_2	V_3	$\cdots$	V_k

The method for judging the accuracy of prediction in this paper is:

(1) Post-test difference test: the difference between the actual value and the predicted correction value is the residual, which is denoted as $R_i = V_i - V_{c(i)}$, $i = 2, 3, \ldots, k$. The safety situation value variance S_1^2 in the current safety situation sequence segment is

$$S_1^2 = \frac{1}{k} \sum_{i=2}^{n} (V_i - \frac{1}{k} \sum_{i=2}^{k} V_i)^2 \tag{20}$$

The residual sequence variance S_2^2 is calculated by Eq. (21):

$$S_2^2 = \frac{1}{k} \sum_{i=2}^{k} (R_i - \frac{1}{k} \sum_{i=2}^{k} R_i)^2 \tag{21}$$

Then, the posterior difference ratio $c = S_2/S_1$, the smaller the value, the better the prediction accuracy.

(2) Small probability test:

$$P = P(|R_i - \frac{1}{k} \sum_{i=2}^{k} R_i| < 0.6745 S_1) \tag{22}$$

A small probability test result P is obtained from Eq. (22), and the larger the value, the better the prediction accuracy.

According to the c value and the P value, according to the prediction accuracy level table (as shown in Table 5), it is judged whether it is necessary to increase the number of error state divisions. If the model prediction result is the first-level prediction accuracy or the second-level prediction accuracy, it is not necessary to increase the number of error state divisions, otherwise the number of error state divisions is $n + 1$.

Table 5. Rank table of prediction accuracy

Prediction accuracy level	c	P
First level	<0.35	>0.95
Second level	<0.50	>0.80
Third level	<0.65	>0.70
Fourth level	≥0.70	≥0.65

6 Experimental Results and Analysis

The predictive validity of the model is verified using Lincoln Laboratory's standard dataset LL_DOS_1.0.

6.1 Experimental Data Processing

Under the Ubuntu 16.04 operating system, the LL_DOS_1.0 packet is replayed using the Tcpreplay technology, and the Snort intrusion detection system is used to generate an alarm log for the replay traffic under the Windows 10 operating system.

Based on the entropy correlation method described in Sect. 2, the network security situation is quantified, and the quantization period $T = 4$ min is set, and 90 security situation values in the interval [2800, 4000] are generated in 1–360 min. In this paper, 10 safe situation values within 1–40 min are taken as the actual safety situation sequence. Compare the actual values of 80 network security situations and the corresponding network security situation predictions within 41–360 min to test the prediction effect of the model.

6.2 Experimental Comparison and Analysis

The experimental data set is the LL_DOS_1.0 data set, which uses the model of this paper, the traditional Markov prediction model, and the improved Convolutional Neural Network (ICNN) prediction model [6] to obtain the network security situation prediction value and compare the predictions effect. Through experiments, the network security situation prediction value sequence of three methods (as shown in Fig. 2) and the security situation prediction value absolute error sequence (shown in Fig. 3) are obtained.

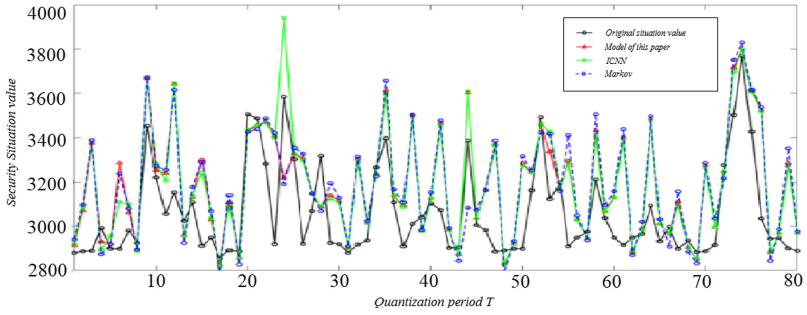

Fig. 2. Network security situation prediction value sequence diagram

It can be seen from Fig. 2 and Fig. 3 that the network security situation prediction result obtained by the model is better than the original state potential value. ICNN model fits better than Markov model. The reasons are as follows:

(1) The prediction of the traditional Markov model depends on the state transition probability matrix, and the state transition probability matrix lacks dynamic adjustment.
(2) The hyper-parameters in the neural network model training are set to be affected by prior experience, which causes the prediction results to deviate from the actual values;

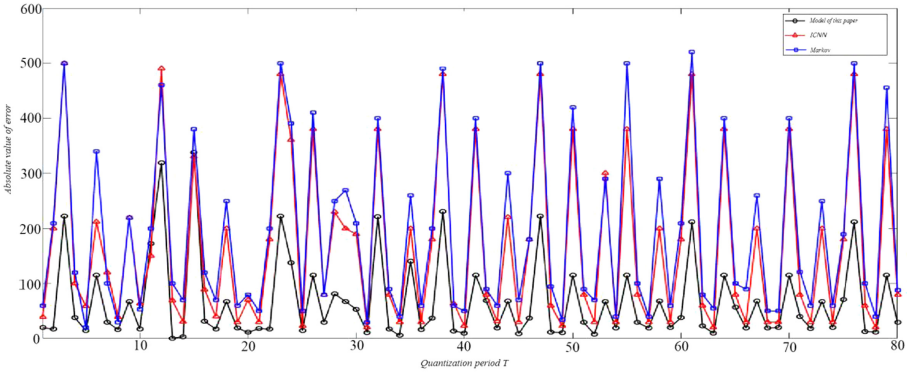

Fig. 3. Predictive value absolute error sequence diagram

(3) The model uses a sliding window mechanism to fragment a long nonlinear time series. The security posture value in the window is continuously updated, so that correlation coefficient can be adaptively and dynamically adjusted, and the network security situation prediction value with higher precision is corrected, and the accuracy of the network security situation prediction is improved.

7 Conclusion

This paper proposes an adaptive network security situation prediction model based on alarm elements. The model quantifies the network security situation values of several cycles by entropy correlation method, and segments the security situation values arranged in time series based on the sliding window mechanism. The adaptive three-dimensional exponential smoothing method is used to generate the initial safety situation prediction results, and the time-varying weighted Markov chain is used to predict the error and correct the safety situation prediction value.

Acknowledgements. This work was supported by the Civil Aviation Joint Research Fund Project of the National Natural Science Foundation of China under granted number U1833107.

References

1. Leau, Y.B.: Network security situation prediction: a review and discussion. Commun. Comput. Inf. Sci. **516**, 424–435 (2015)
2. Zhang, S.B.: Network security situation prediction model based on multi-swarm chaotic particle optimization and optimized grey neural network. In: IEEE International Conference on Software Engineering and Service Science, Piscataway. IEEE Press, Nanjing (2018)
3. Xiao, P.: Network security situation prediction method based on MEA-BP. In: IEEE International Conference on Computational Intelligence & Communication Technology. IEEE Press, Nanjing (2017)

4. Sun, S.X.: The research of the network security situation prediction mechanism based on the complex network. In: IEEE International Conference on Computational Intelligence and Communication Networks. IEEE Press, Nanjing (2015)
5. Zhou, X.W.: Multi node network security situation prediction model based on improved G-K algorithm. Sci. Technol. Eng. **18**(25), 72–77 (2018)
6. Zhang, R.C.: Network security situation prediction method using improved convolution neural network. Comput. Eng. Appl. **55**(6), 86–93 (2019)
7. Xi, R.R.: An improved quantitative evaluation method for network security. Chin. J. Comput. **38**(4), 749–758 (2015)
8. Debar, H., Wespi, A.: Aggregation and correlation of intrusion-detection alerts. In: Lee, W., Mé, L., Wespi, A. (eds.) RAID 2001. LNCS, vol. 2212, pp. 85–103. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45474-8_6
9. Zhao, D.M.: Fuzzy risk assessment of entropy-weight coefficient method applied in network security. Comput. Eng. **30**(18), 21–23 (2004)
10. Fu, Y.: An approach for information systems security risk assessment on fuzzy set and entropy-weight. Chin. J. Electron. **38**(7), 1489–1494 (2010)
11. Wang, X.: Network anomaly detection model based on time-varying weighted Markov Chain. Comput. Sci. **44**(9), 136–141+161 (2017)