

Prediction Algorithm of Network Security Level with Time Parameters

Banggui Liu^a and Qingsheng Zeng^{b,*}

^a*School of Artificial Intelligence, Open University of Guangdong, Zhongshan, 528400, China*

^b*Canada Federal Communications Research Center Senior Research Engineer, Montreal (QC), H5A 1K6, Canada*

Abstract

In order to improve the prediction ability of network security level, a design method of network security level prediction system based on time window parameter identification and spatial interval sampling is proposed. According to the prediction feature of network security level, the browsing information and intrusion information feature of network users are detected, the distribution set of network intrusion and attack behavior characteristics reflecting network security level is constructed, the statistical feature quantity of network security level prediction is extracted, and the distributed feature extraction and adaptive detection of network intrusion are carried out according to the combined feature distribution of the network security level prediction network behavior feature set. The feature set and similarity attribute of network spatial distribution information of the load network security level are mined and combined with the estimation results of time parameters, the security level evaluation and optimization prediction are carried out, and the network intrusion optimization detection and security early warning are realized. The simulation results show that the method has strong response ability to predict the network security level, and the accurate detection performance of the network intrusion is better, which improves the prediction ability of the network security level and ensures the network security.

Keywords: time parameter; network security; grade prediction; intrusion detection

(Submitted on October 28, 2019; Revised on November 30, 2019; Accepted on December 16, 2019)

© 2019 Totem Publisher, Inc. All rights reserved.

1. Introduction

Computer networks have become an important tool of data transmission. The security of networks is based on big data information transmission and communication in computer network systems. In order to avoid information leakage and network paralysis, it is necessary to optimize the design of network security level prediction systems, construct a distributed feature extraction and adaptive detection model of network intrusion, and design a network security level prediction system according to the user behavior characteristics of the network. This will realize the optimal mining and monitoring of user behavior characteristics in the network environment and improve the security early warning and emergency response ability of the network [1]. It is of great significance to study the optimal design method of network security level prediction systems in network security design and information encryption transmission control. Research on the design methods of network security level prediction systems has attracted great attention [2].

The design of a network security level prediction system is based on the hardware security detection and software security design of the network system. The information feature quantity of network security level prediction is extracted, the security monitoring and intrusion interception are carried out according to the distributed feature extraction and adaptive detection results of network intrusion, and the prediction ability of network security level is improved. The main prediction methods of network security level are the principal component detection method, autocorrelation information fusion, fuzzy detection method, and time-frequency analysis method [3]. The statistical features of network security level prediction are extracted, the distributed feature extraction and adaptive detection of network intrusion are performed according to the computer network security transmission information model, and the network security level prediction and response analysis are conducted according to the intrusion detection results. A good prediction ability of network security level has been obtained [4]. However, the computational complexity of the above methods for network security level prediction is high,

* Corresponding author.

E-mail address: dfsdfshb6945@163.com

and the performance of intrusion detection for plaintext attacks and strong attacks is not good.

In order to solve the above problems, a design method of network security level prediction system based on time window parameter identification and spatial interval sampling is proposed in this paper. Firstly, the browsing information and intrusion information feature detection of network users is carried out according to the prediction feature of the network security level, the distribution set of network intrusion and attack behavior characteristics reflecting the network security level is constructed, the statistical feature quantity of network security level prediction is extracted, and the distributed feature extraction and adaptive detection of network intrusion are carried out according to the combined feature distribution of the network security level prediction network behavior feature set. Then, the feature set and similarity attribute of network spatial distribution information of the load network security level are excavated, and the security level evaluation and optimization prediction are carried out and combined with the estimation results of time parameters. The network intrusion optimization detection and security early warning are realized. Finally, the simulation results demonstrate the superior performance of this method in improving the prediction ability of the network security level.

2. Detection of User Behavior Characteristics in Network Security Early Warning Response

2.1. Network Intrusion and Aggressive Behavior Feature Sampling

In order to realize the design of a network security level prediction system based on time window parameter identification and spatial interval sampling, the network intrusion and attack behavior feature sampling model of network security is constructed, the statistical feature quantity of network security level prediction is extracted, and the user behavior feature collection model of network security is constructed by using the dynamic migration algorithm [5]. The discrete sequence feature sampling method is used to collect discrete sequence information of the network security level. In the cloud computing mode, the network intrusion information acquisition model is shown in Figure 1.

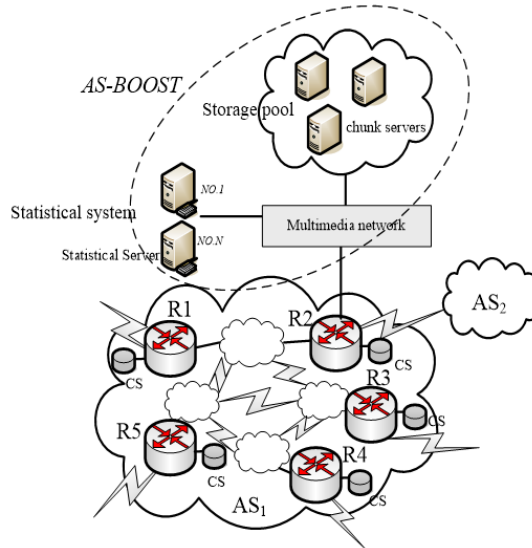


Figure 1. Network intrusion information collection model

The network security early warning is carried out according to the characteristic distribution of the association information of the user, and a distributed feature extraction and an adaptive detection model of the network intrusion are constructed. According to the association information distribution of the user, the user behavior association distribution set of the network security is obtained as follows:

$$C_1(m, n) = \sum_{i=1}^L c_{4s_i} e^{j2\phi_i(m-n)} \quad (1)$$

Where $c_{4s_i} = \text{cum}\{|s_i(t)|^4\}$ represents the energy spectrum feature distribution set of the user requesting access to the network data transmission node s_i , C_{4S} represents a node energy spectrum density with a large difference in load, and the distribution intensity of the network intrusion state information is

$$C_{4s} = \text{diag}[c_{4s_1}, c_{4s_2}, \dots, c_{4s_L}] \quad (2)$$

It is known that $a(t) \geq |s(t)|$ represents the load amplitude of network intrusion under maximum likelihood estimation. The maximum envelope amplitude is $a(t)$, and it is combined with the nonlinear statistical sequence analysis method to detect the network behavior characteristics of network security level prediction [6]. The distribution matrix of network security level prediction network behavior is an $|s(t)|$ matrix.

$$C = \begin{bmatrix} C_1 & C_2 & C_5 & C_4 \\ C_2^H & C_1 & C_6 & C_7 \\ C_5^H & C_6^H & C_1 & C_3^H \\ C_4^H & C_7^H & C_3 & C_1 \end{bmatrix} = \bar{A} C_{4s} \bar{A}^H \quad (3)$$

Where $\bar{A} = [A^H, (A\Lambda)^H, (A\Omega)^H, (A\Phi)^H]^H$ represents the residual statistics of the network behavior feature set of the network security early warning network, thereby obtaining a set of all the edges of the network under the continuous invasion. A behavior characteristic decomposition model of the network security early warning is obtained as follows:

$$C = E \sum E^H \quad (4)$$

In this paper, $E = [e_1, e_2, \dots, e_{4p}]$ is used to predict the unitary matrix of network behavior characteristic distribution symbol on transmission link (a, b_m) for the network security level, and $\sum = \text{diag}[\sigma_1, \sigma_2, \dots, \sigma_{4p}]$ is the spatial distribution density predicted by the network security level. The least mean square error estimation method is used to obtain the network intrusion and attack behavior characteristics of network security as follows:

$$\sigma_1 > \dots > \sigma_L > \sigma_{L+1} = \dots = \sigma_{4p} = 0 \quad (5)$$

A network security level prediction network behavior characteristic large data distribution model can be obtained as follows:

$$f_{s,\tau}(t) = [U(1/s, \tau)f(t)] = \sqrt{|s|}f(s(t-\tau)) \quad (6)$$

The feature mapping of network intrusion and attack behavior is carried out in the whole time-frequency plane. $a = 1/s$ and $b = \tau$ detect the browsing information and intrusion information of network users according to the prediction characteristics of the network security level. A distribution set of network intrusion and attack behavior characteristics reflecting the network security level is constructed, and the network security early warning and response analysis is conducted according to the sampling results of network security network intrusion and attack behavior characteristics [7].

2.2. Network Behavior Feature Detection

Based on the above network intrusion and attack behavior feature sampling, the regression analysis of network security level prediction network behavior feature set is carried out by quantitative regression analysis and statistical sequence analysis. A binary directed graph $G = (V, E)$ is used to represent the graph model structure of the network security level prediction network behavior feature set, where V is the vertex set deployed in the network security early warning monitoring and E is the network security level prediction network behavior feature set distributed in a limited domain. The vector quantization feature decomposition method is used to predict the network security level and the fusion feature decomposition, which makes the network security level predict the network early warning response weight value $\hat{\mathbf{w}}(0) = \mathbf{0}$. The iterative formula for the network security level prediction response analysis is as follows:

$$\theta_i(k+1) = \theta_i(k) - \mu \text{Re}[y(k)\phi^*(k)] \quad (7)$$

Where μ is the iterative step size of the network security early warning, $\varphi(k)$ is the intrusion response intensity, and the network security level is extracted to predict the network behavior feature set under persistent attack [8]. The dynamic response feature quantity $u(k)$ of the network security early warning is linear transformation according to the square fitting method, which is expressed as follows:

$$H_B(z) = \frac{(1 + \sin \theta_2)}{\cos \theta_2} \frac{\cos \theta_1(k) \cos \theta_2 z^{-1}}{1 + \sin \theta_1(k)(1 + \sin \theta_2) z^{-1} + \sin \theta_2 z^{-2}} G(z) \quad (8)$$

Wherein

$$G(z) = \frac{1 - \sin \theta_2}{2} \frac{1 - z^{-2}}{1 + \sin \theta_1(k)(1 + \sin \theta_2) z^{-1} + \sin \theta_2 z^{-2}} \quad (9)$$

According to the attribute mining results of the network security level prediction network behavior feature set, the error between the network security early warning response and expectation is minimized [9-11]. $d(k)$ represents the network behavior feature component of network security early warning, and the error component of network security early warning is obtained.

$$\varepsilon(k) = d(k) - y(k) = d(k) - \sum_{i=1}^M W_i x(k-i) \quad (10)$$

The mathematical expectation is taken from both sides of the above formula, and the network security early warning and response are carried out with the minimum error. The distributed feature extraction and adaptive detection model of network intrusion is constructed, and the network behavior feature detection is carried out according to the network security early warning results, so as to improve the dynamic detection and real-time early warning ability of network intrusion [12].

3. Network Security Level Evaluation and Optimization Prediction and Optimization

3.1. Distributed Feature Extraction and Adaptive Detection of Network Intrusion

On the basis of constructing a network intrusion and attack behavior feature distribution set that reflects the network security level and extracting the statistical feature quantity of network security level prediction, the distributed feature extraction and adaptive detection of network intrusion are carried out [13]. According to the combined feature distribution of network security level prediction network behavior feature collection, the distributed feature extraction and adaptive detection of network intrusion are carried out, and the network intrusion symbol form is obtained as follows:

$$s(t) = \underbrace{\sum_{k=1}^N p_k \sin(\omega_k n + \Phi_k)}_{u(n)} + \zeta(n) \quad (11)$$

Where Φ_k is the statistical average value of the network security early warning, $\zeta(n)$ is the intrusion symbol pulse, and p_k is the scale parameter. The association rule set of network security level prediction network behavior feature set is constructed, and the network behavior feature set is obtained as follows:

$$\frac{1}{2\pi m} \sum_{k=-q/2}^{q/2} b_k \phi(n + c_k m) = \hat{f}_{i_q}(n) \quad (12)$$

Where b_k is the main component feature of network intrusion, ϕ is the phase angle, m is the desired response, and c_k is the dynamic response characteristic of the network security early warning. If $x_1(t)$ and $x_2(t)$ represent the detection statistic of network security intrusion, then

$$x_1(t) = -\sum_{k=1}^{p_1} a_{1k} x_1(t-k) + \varepsilon_1(t) \quad (13)$$

$$x_2(t) = -\sum_{k=1}^{p_2} a_{2k} x_2(t-k) + \varepsilon_2(t) \quad (14)$$

Where $\varepsilon_1(t)$ is a Gaussian white noise with variance σ_{12} , and the distribution set of network security level prediction network behavior is obtained.

$$u(t) = \frac{1}{\sqrt{T}} \text{rect}\left(\frac{t}{T}\right) \exp\left\{-j[2\pi K \ln(1 - \frac{t}{t_0})]\right\} \quad (15)$$

Where $\text{rect}(t) = 1, |t| \leq 1/2$. The envelope feature detection of network behavior characteristics predicted by the network security level is carried out. Combined with the fuzzy correlation detection method [14], the dynamic feature distribution set of network intrusion is obtained as follows:

$$\begin{cases} y(t) = x(t-t_0) \Rightarrow W_y(t, v) = W_x(t-t_0, v) \\ y(t) = x(t)e^{j2\pi v_0 t} \Rightarrow W_y(t, v) = W_x(t, v-v_0) \end{cases} \quad (16)$$

The network security intrusion detection is carried out by adopting an adaptive association rule scheduling method, and the description is expressed as follows:

$$\begin{aligned} W_a u(a, b) = e^{j2\pi K \ln a} \times \frac{K}{\sqrt{a}} \left\{ \left[\frac{ae^{\frac{j2\pi f_{\min}(b-b_a)}{a}}}{f_{\min}} - \frac{e^{j2\pi f_{\max}(b-b_a)}}{f_{\max}} \right] \right. \\ \left. + j2\pi(b-b_a) \left[Ei(j2\pi f_{\max}(b-b_a)) - Ei\left(\frac{j2\pi f_{\min}(b-b_a)}{a}\right) \right] \right\} \end{aligned} \quad (17)$$

Where $b_a = (1-a)(\frac{1}{af_{\max}} - \frac{T}{2})$, and $Ei(\cdot)$ represents the symbol distribution of distributed feature extraction and adaptive detection of network intrusion. According to the results of intrusion detection, the network security early warning and response control are carried out [15].

3.2. Network Security Early Warning Network Behavior Mining and Response Output

The feature set and similarity attribute of network spatial distribution information of the load network security level are mined, and the security level is evaluated, optimized, and combined with the estimation results of time parameters [16]. The detection statistics of network security level prediction network behavior early warning using big data information fusion and association rule mining method are as follows:

$$\begin{cases} H_0 : \tilde{x}(t) = \tilde{w}(t) \\ H_1 : \tilde{x}(t) = \sqrt{E_t} \tilde{f}(t-\lambda) \tilde{b}_D(t-\frac{\lambda}{2}) + \tilde{w}(t), \quad 0 \leq t \leq T \end{cases} \quad (18)$$

Where $\tilde{w}(t)$ is the source distribution set of network intrusion, the test set $V = [V_1, V_2, \dots, V_m] \in R^{m \times m}$ of the network security level prediction network behavior feature set is orthogonal, and the network behavior characteristic distribution directivity domain can be expressed as follows:

$$\min_w w^H \tilde{R}_y w \quad (19)$$

$$\text{subject } a_t(\theta_0)w = 1 \text{ to } C^H w = g$$

Under the known intrusion intensity and combined with the average mutual information distribution of the estimated results of time parameters, the weight in the process of intrusion detection is adjusted, and the output w_{BLCMV} is as follows:

$$w_{BLCMV} = \tilde{R}_y^{-1}[a_t(\theta_0), C][[a_t(\theta_0), C]^H \tilde{R}_y^{-1}[a_t(\theta_0), C]]^{-1} \begin{bmatrix} 1 \\ g \end{bmatrix} \quad (20)$$

Where $C = [c_1, c_2, \dots, c_g]$, C is the fusion correlation feature distribution set of the network security early warning, g is the G intrusion symbol detection sequence, and the detection coefficient of network intrusion is w_{BLCMV} . According to the above analysis, the network security early warning is carried out by using the network behavior detection method, and the iterative process is obtained as follows:

$$a(\theta_0 + \Delta\theta) = [1, \exp(-j\phi_1), \dots, \exp(-j(M-1)\phi_1)]^T \quad (21)$$

Wherein

$$\phi_1 = 2\pi d \sin(\theta_0 + \Delta\theta) / \lambda, \quad \phi_2 = 2\pi d \sin(\theta_0 - \Delta\theta) \quad (22)$$

Based on the analysis, the confidence level of the network security early warning in the mode of user behavior feature detection is obtained as follows:

$$MSD_{a \rightarrow b} = 1 - \frac{\sum_{i=1}^{|I_{a,b}|} \sqrt{(d_{a,i} - \bar{d}_a)^2 + (d_{b,i} - \bar{d}_b)^2}}{|I_{a,b}| \times \sum_{i=1}^{|I_{a,b}|} \left[\sqrt{(d_{a,i} - \bar{d}_a)^2} + \sqrt{(d_{b,i} - \bar{d}_b)^2} \right]} \quad (23)$$

According to the description of the above algorithm, the optimal network intrusion detection and security early warning response are realized [17]. The fuzzy association rule scheduling method is used to predict the reliability of the network security level, and the prediction function is obtained as follows:

$$f(x) = \text{sgn} \left\{ \sum_{j=1}^l \alpha_j^* y_j K(x, x_j) + b^* \right\}, \quad x \in R^n \quad (24)$$

Where $b^* = y_i - \sum_{j=1}^l y_j \alpha_j K(x_j, x_i)$ and $i \in \{i | 0 < \alpha_i^* < u(x_i)C\}$. According to the above prediction function, the optimization control of network information popularity prediction is carried out by using the multiple iterative method, the fuzzy correlation set of network security level is analyzed by the principal component analysis method [18], and the network security level prediction is realized based on time window parameter identification and the spatial interval sampling method. The optimized prediction model is as follows:

$$\begin{cases} G_1 = b_{11}a_1 + b_{12}a_2 + \dots + b_{1n}a_n \\ G_2 = b_{21}a_1 + b_{22}a_2 + \dots + b_{2n}a_n \\ \vdots \\ G_n = b_{n1}a_1 + b_{n2}a_2 + \dots + b_{nn}a_n \end{cases} \quad (25)$$

Where G_j and G_k have strong correlation, which indicates that the convergence and accuracy of prediction are good [19]. Based on this analysis, the realization flow of network security level prediction is shown in Figure 2.

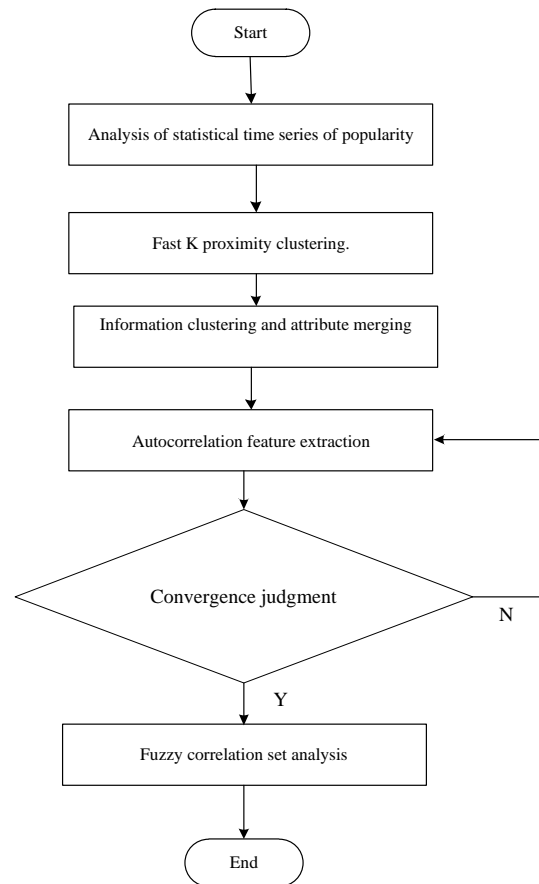


Figure 2. Implementation flow of prediction

4. Simulation Experiment and Result Analysis

The experiment is based on a Matlab 7 simulation environment. The types of network intrusion are DoS, Probe, and collision database attack. The sample size of each type of network intrusion is 2,000 groups, the size of the test sample set is 1,200, the data length of browsing information and intrusion information feature detection of network users is 1,024, the network attack data is simulated in the KDD Cup2018 database, and the initial frequency $f_1 = 1.5$ Hz. According to the above simulation environment and parameter settings, the statistical feature quantity of network security level prediction is extracted, and the distributed feature extraction and adaptive detection of network intrusion are carried out according to the combined feature distribution of the network behavior feature set predicted by the network security level prediction network behavior feature set. The signal-to-noise ratio (SNR) of $n(k) = n_r(k) + jn_i(k)$ network intrusion is -20dB. The distributed feature distribution of the network behavior feature set is predicted according to the network security level. The response time series of network security early warning is shown in Figure 3.

Taking the above sampling samples as the test object set, the distributed feature extraction and adaptive detection of network intrusion are carried out, and the security level evaluation and optimization prediction are conducted with the time parameter estimation results. The intrusion behavior feature detection output is shown in Figure 4.

The analysis of Figure 4 shows that the convergence degree and beam directivity of the behavior feature detection of network security early warning are high, which improves the ability of network security level evaluation and optimization prediction. The detection performance is compared with the traditional method, and the accurate probability of network security early warning is taken as the test index. The comparison results are shown in Figure 5. The analysis of Figure 5 shows that the distributed feature extraction, adaptive detection, and early warning of network intrusion using this method have higher accuracy and better anti-interference performance. The network intrusion optimization detection and security early warning response are realized.

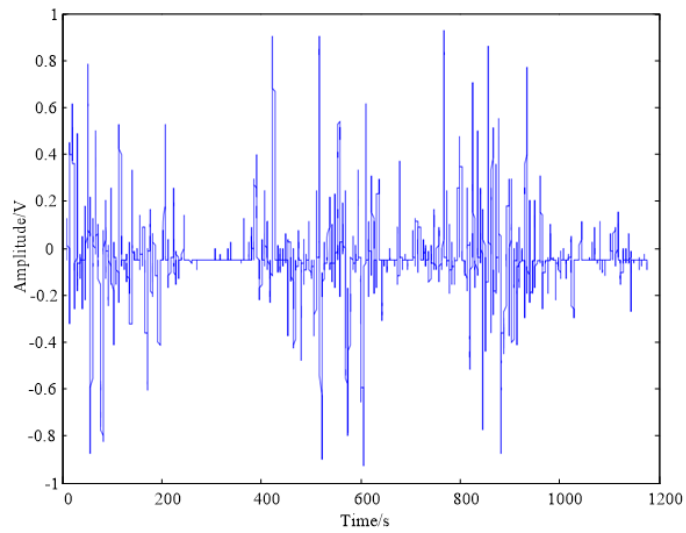


Figure 3. Network security early warning response time series

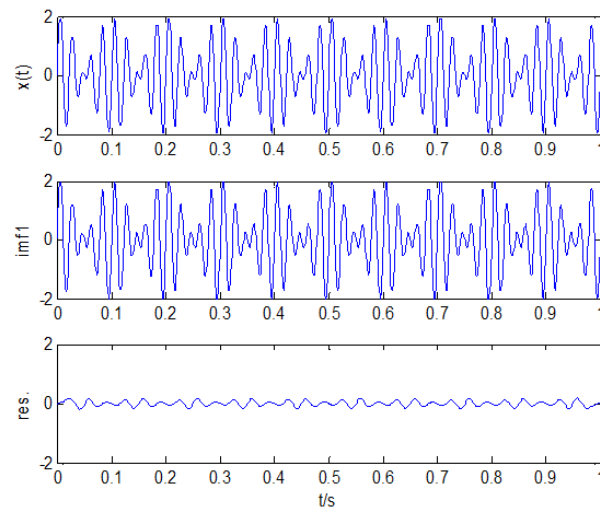


Figure 4. Intrusion behavior feature detection output

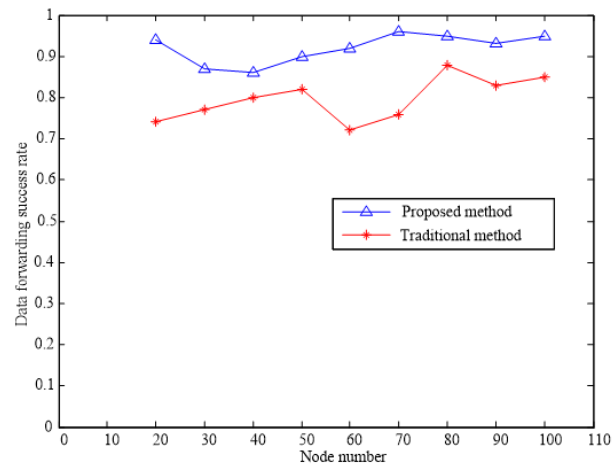


Figure 5. Comparison of network security early warning performance

5. Conclusions

In this paper, a design method of network security level prediction system based on time window parameter identification

and spatial interval sampling is proposed. According to the prediction feature of the network security level, the browsing information and intrusion information feature of network users are detected, the distribution set of network intrusion and attack behavior characteristics reflecting network security level is constructed, the statistical feature quantity of network security level prediction is extracted, and the distributed feature extraction and adaptive detection of network intrusion are carried out according to the combined feature distribution of the network security level prediction network behavior feature set. The security level evaluation and optimization prediction are carried out, and the network intrusion optimization detection and security early warning are realized. The simulation results show that the method has strong response ability to predict the network security level, and the accurate detection performance of the network intrusion is better, which improves the prediction ability of the network security level and ensures the network security. This method has good application value in the prediction of network security levels.

References

1. X. S. Wei, J. H. Luo, and J. Wu, "Selective Convolutional Descriptor Aggregation for Fine-Grained Image Retrieval," *IEEE Transactions on Image Processing*, Vol. 26, No. 6, pp. 2868-2881, 2017
2. A. S. Razavian, J. Sullivan, and S. Carlsson, "Visual Instance Retrieval with Deep Convolutional Networks," *ITE Transactions on Media Technology and Applications*, Vol. 4, No. 3, pp. 251-258, 2016
3. N. Saxena, S. Grijalva, V. Chukwuka, and A. Vasilakos, "Network Security and Privacy Challenges in Smart Vehicle-to-Grid," *IEEE Wireless Communications*, Vol. 12, No. 99, pp. 2-12, 2017
4. H. Guo, H. Liu, C. Wu, et al., "Logistic Discrimination based on G-Mean and F-Measure for Imbalanced Problem," *Journal of Intelligent and Fuzzy Systems*, Vol. 31, No. 3, pp. 1155-1166, 2016
5. S. Ijaz, F. A. Hashmi, S. Asghar, and M. Alam, "Vector based Genetic Algorithm to Optimize Predictive Analysis in Network Security," *Applied Intelligence*, Vol. 48, No. 2, pp. 1-11, 2017
6. Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. L. Zhu, "The Individual Identification Method of Wireless Device based on Dimensionality Reduction and Machine Learning," *Journal of Supercomputing*, Vol. 75, No. 6, pp. 3010-3027, 2019
7. Y. Lin, C. Wang, J. X. Wang, and Z. Dou, "A Novel Dynamic Spectrum Access Framework based on Reinforcement Learning for Cognitive Radio Sensor Networks," *Sensors*, Vol. 16, No. 10, pp. 1675, 2016
8. S. Liu, "Introduction of Key Problems in Long-Distance Learning and Training," *Mobile Networks and Applications*, Vol. 24, No. 1, pp. 1-4, 2019
9. C. L. Ma, H. Shan, and T. Ma, "Improved Density Peaks based Clustering Algorithm with Strategy Choosing Cluster Center Automatically," *Computer Science*, Vol. 43, No. 7, pp. 255-258, 2016
10. S. B. Zhou and W. X. Xu, "A Novel Clustering Algorithm based on Relative Density and Decision Graph," *Control and Decision*, Vol. 33, No. 11, pp. 1921-1930, 2018
11. H. He and Y. Tan, "Automatic Pattern Recognition of ECG Signals using Entropy-based Adaptive Dimensionality Reduction and Clustering," *Applied Soft Computing*, Vol. 55, No. 12, pp. 238-252, 2017
12. J. H. Park, Y. Sung, P. K. Sharma, et al., "Novel Assessment Method for Accessing Private Data in Social Network Security Services," *Journal of Supercomputing*, Vol. 73, No. 3, pp. 1-19, 2017
13. H. S. Gill, S. S. Gill, and K. S. Bhatia, "A Novel Approach for Physical Layer Security in Future-Generation Passive Optical Networks," *Photonic Network Communications*, Vol. 35, No. 11, pp. 1-10, 2017
14. D. He, S. Chan, and M. Guizani, "Win-Win Security Approaches for Smart Grid Communications Networks," *IEEE Network*, Vol. 31, No. 6, pp. 12-18, 2017
15. S. Gao, Z. C. Li, B. Xiao, and G. Y. Wei, "Security Threats in the Data Plane of Software-Defined Networks," *IEEE Network*, Vol. 32, No. 4, pp. 108-113, 2018
16. Y. L. Li, N. Hua, Y. F. Yu, Q. S. Luo, and X. P. Zheng, "Light Source and Trail Recognition via Optical Spectrum Feature Analysis for Optical Network Security," *IEEE Communications Letters*, Vol. 5, No. 99, pp. 1, 2018
17. D. J. He, X. R. Li, S. Chan, J. H. Gao, and M. Guizani, "Security Analysis of a Space-based Wireless Network," *IEEE Network*, Vol. 33, No. 1, pp. 36-43, 2018
18. Q. Wang, X. F. Gong, and R. S. Luo, "Coherent Sources Number Estimation based on Circular Array Virtual Array Translation," *Computer Engineering*, Vol. 44, No. 9, pp. 78-82, 2018
19. S. Liu, Z. J. Li, and X. C. Cheng, "Introduction of Recent Advanced Hybrid Information Processing," *Mobile Networks and Applications*, Vol. 23, No. 4, pp. 673-676, 2018