Computer Network Information Security Analysis and Management Based on Improved Wavelet Neural Network

Ruiqi Peng[1,*], Sirui Liu[2], Tianling Li[3]

1. Jishou University, Jishou, Xiangxi Autonomous Prefecture, Hunan, 416000, China

2. Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 210000, China

3. Xiangtan Institute of Technology, Xiangtan, Hunan, 411100, China

*Corresponding Author

Keywords: Wavelet neural network, Computers, Information security

Abstract: In view of the uncertainty and complexity of information security risk assessment and the limitation of traditional mathematical methods in assessing information security risk grade, an information security risk assessment model based on fuzzy wavelet neural network is established by organically combining artificial neural network theory, wavelet analysis and fuzzy evaluation method. The fuzzy evaluation method is used to quantify the index of risk factors, and the output of fuzzy system is taken as the input of neural network, and the fuzzy wavelet neural network is constructed and trained [1]. The simulation results show that the fuzzy wavelet neural network model can quantitatively evaluate the risk factor level of information system, and solve the defects of subjective arbitrariness and fuzzy conclusion existing in the existing evaluation methods. Compared with BP neural network, the fuzzy wavelet neural network model has higher fitting accuracy and faster convergence speed.

1. Introduction

Due to the complexity, nonlinearity, uncertainty and real-time characteristics of information security risk assessment, the traditional mathematical model for information security risk assessment has certain limitations, and the assessment method is subjective and arbitrary, ambiguous, complex in operation and lacking in self-learning ability. However, the artificial neural network has the intelligence characteristics that the conventional methods do not have, can deal with uncertain problems, has the functions of self-learning and acquiring knowledge, and is suitable for dealing with nonlinear problems. Gradient descent method is widely used in the training of wavelet neural networks, which depends on the selection of initial weights, and its convergence speed is slow and it is easy to fall into local optimum. Particle Swarm Optimization (PSO) adopts the global search strategy based on population, and coordinates the global search and local search through inertia weight, which can guarantee the optimal solution with high probability and overcome the defect of local optimization of gradient descent method. An improved wavelet neural network is constructed by combining wavelet neural network with particle swarm optimization algorithm, and a wavelet neural network model (PWNN) based on particle swarm optimization algorithm is proposed, which is used for information security risk assessment, so as to effectively assess the risk level of information security risk influencing factors.

2. Improvement of Weight and Parameter Correction Method

WNN must have a training process before running, which requires n input samples and m output samples. During training, each predicted value should be compared with the output samples (i.e., the expected value), and the error e between the predicted value and the expected value should be calculated. Then, according to the error, the parameters such as the connection weight ω of the network, the expansion coefficient A and the translation coefficient B of the wavelet basis function should be corrected [2]. This process is iterative, so that the predicted value keeps approaching the

DOI: 10.25236/iccem.2021.049

expected value. The parameter correction process mainly includes two steps.

Step 1: Calculate the prediction error.

$$\mathrm{e} = \sum_{K=1}^{M} \left| Y_K - \overline{Y_K} \right| \tag{1}$$

In which Y_K represents the predicted value and $\overline{Y_K}$ represents the expected value.

Step 2: Modify the network parameters.

WNN uses gradient descent method to modify the connection weights of the network and the parameters of wavelet basis functions, which may be called gradient WNN(Gradient_WNN, GWNN).

The calculation formula is:

$$\omega^{(new)} = \omega^{(old)} + \Delta\omega^{(new)} \tag{2}$$

$$\alpha_j^{(\mathrm{new})} = \alpha_j^{(old)} + \Delta\alpha_j^{(\mathrm{new})} \tag{3}$$

The formulas for $\Delta\omega^{(\mathrm{new})}$ and $\Delta\alpha_{\mathrm{j}}^{(\mathrm{new})}$ are as follows:

$$\Delta\omega^{(\mathrm{new})} = -\eta_1 \frac{\partial \mathrm{e}}{\partial \omega^{(old)}} \tag{4}$$

$$\Delta\alpha^{(\mathrm{new})} = -\eta_2 \frac{\partial \mathrm{e}}{\partial \alpha_{\mathrm{j}}^{(old)}} \tag{5}$$

In formulas (4) and (5), η represents the learning rate. The selection of η is more critical: the greater the value of η, the greater the change rate of weights, and the faster the convergence speed of training, but the greater the value of η, the more unstable the network is. On the contrary, the smaller the η value, the smaller the change rate of weights. Naturally, the convergence speed of training is slower, but the network is more stable.

3. Information Security Risk Assessment

3.1 Information Security Risk Assessment Hierarchy Construction

Information security risk assessment is to systematically analyze the threats faced by the network and information systems and their existing vulnerabilities from the perspective of risk management by using scientific methods and means, to assess the degree of harm that may be caused by security incidents, and to put forward targeted protection measures and rectification measures against threats, so as to prevent and resolve information security risks, or to control the risks at an acceptable level, so as to maximize the protection of network and information security. Information security risk assessment should first establish a set of evaluation index system, and scientifically and reasonably solve the problem of weight distribution of each evaluation index through analytic hierarchy process [4]. According to the hierarchical requirements of analytic hierarchy process, the information security evaluation system can be divided into target layer, criterion layer and indicator layer. The specific hierarchical structure is shown in Figure 1.

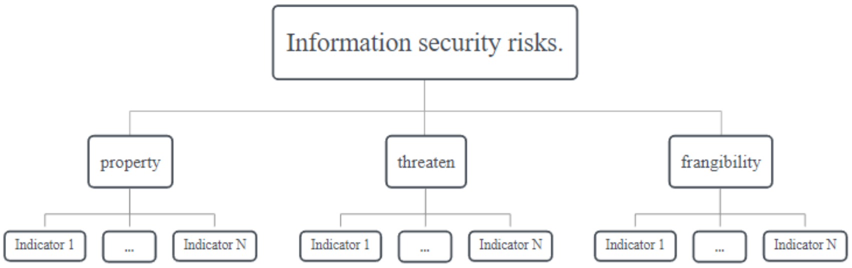

Fig.1 Hierarchical Structure of Information Security Risk Assessment

On the basis of constructing the hierarchical structure of information security risk assessment of a certain system, this paper intends to use the nine-point scale method to make pairwise comparison, so as to obtain the judgment matrix of each layer element:

$$A = \begin{pmatrix} a_{11} & . & . & a_{1m} \\ . & & & . \\ . & & & . \\ a_{n1} & . & . & a_{nm} \end{pmatrix} \qquad (6)$$

Among them, $a_{ij} = 1 / a_{ij} = a_i / a_j$, a_i and a_j represent the size of expert language evaluation of the I and J elements, respectively.

When experts judge the elements of each layer in pairs, they often need to check the consistency to prevent large errors. The consistency test index of matrix A is $CI = \frac{\lambda_{\max} - n}{n - 1}$, where $\lambda_{\max}$ is the maximum eigenvalue of judgment matrix. Theoretically, when C<0.1, the consistency of judgment matrix is better, otherwise, it needs to be re-evaluated. The feature vector corresponding to the maximum eigenvalue is calculated, and the normalized feature vector $\omega = (\omega_1, \omega_2,...\omega_n)$ is the relative weight value of each layer element [5].

3.2 Determine the Calculation Formula of Risk Assessment

The Code for Information Security Risk Assessment, jointly drafted by the National Information Security Research and Service Center and the State Key Laboratory of Information Security, Chinese Academy of Sciences, gives the workflow of risk assessment shown in Figure 2 on the basis of in-depth study of the factors and measurement standards of information security risk assessment.

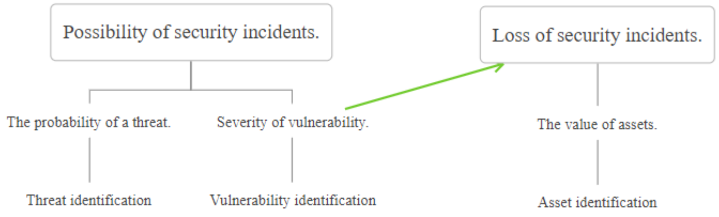
Possibility of security incidents.
Loss of security incidents.
The probability of a threat.
Severity of vulnerability.
The value of assets.
Threat identification
Vulnerability identification
Asset identification

Fig.2 Information Security Risk Assessment Process

According to the workflow in Figure 2, the following information security risk assessment calculation formula can be obtained:

$$Rt = V \times Pt \times Pv \qquad (7)$$

In which: Rt stands for risk; V stands for assets; Pt stands for threat; Pv stands for vulnerability. If an information system adopts security measure M, new threat factors may be introduced, and the calculation formula of risk assessment should be modified as follows:

$$Rt = V \times Pt \times Pv \times Sm + R_j \qquad (8)$$

In which: Sm is the effective degree of safety measures m; Rj is the risk value introduced by safety measure m.

Information security risks are generally caused by different subjects who are independent of each other. Considering that the risk occurrence times can be regarded as random events in probability statistics, each threat is independent of each other and has only two results: occurrence or non-occurrence, this paper intends to use poisson distribution to simulate the probability of threat occurrence. Considering that poisson distribution has the following characteristics: when the number of threats is less than λ, the probability of threats increases with the increase of its number; However, when the number of threats is greater than λ, its probability decreases with the increase of the number of threats. Therefore, the quantitative model of security risk assessment based on information system can be defined as follows:

$$Rt=\sum_{k=1}^{n}(v\times\frac{\mathrm{e}^{-\lambda}\lambda^{k}}{k!}\times Pv\text{）} \tag{9}$$

$$Rt=\sum_{k=1}^{n}(v\times\frac{1}{\sqrt{2\pi\lambda}}e^{\frac{(k-\lambda)^{2}}{2\lambda}}\times Pv\text{）}\text{ ，}\ \mathrm{n}\geq 10 \tag{10}$$

In the information security risk assessment, the risk factors are mainly evaluated from the threat, vulnerability and their mutual relations. Firstly, the assets, existing threats and vulnerabilities of the system are analyzed. Then, it evaluates the level of risk factors from various evaluation indexes, such as the frequency of threats, the severity of vulnerabilities, and the value of assets. These evaluation indexes are very vague and uncertain, which is difficult to be measured by conventional methods. Moreover, there is a nonlinear relationship and dynamic change rule between these quantities and the risk level of risk factors, which is difficult to be handled by conventional methods. In order to solve this problem, this paper makes use of the characteristics that fuzzy system has easy-to-understand expression ability and neural network has strong self-adaptive ability, and combines them organically to realize the evaluation of the risk level of uncertain and fuzzy risk factors [6]. In the training of wavelet neural network, particle swarm optimization algorithm is used to solve the defects of slow convergence and local optimum.

3.3 Intrusion Detection System Based on Wavelet Neural Network

Because of the diversity of intrusion patterns, intrusion detection strategies and models also have many different types. At present, applying artificial intelligence technology to intrusion detection technology has become a research hotspot. The introduction of this paper also points out that intrusion detection is ultimately a problem of pattern recognition, and one of the powerful applications of neural network is pattern recognition, so neural network method is an effective intrusion detection method. Wavelet network is an important branch of neural network, which combines the advantages of both wavelet analysis and neural network. Intrusion detection based on wavelet neural network can improve the performance of intrusion detection based on traditional BP network. Wavelet analysis and neural network have been widely studied, which is based on BP neural network, considering and analyzing the characteristics of the excitation function of BP neural network and the structure of BP neural network, and combining the knowledge of wavelet analysis. Wavelet neural network has the characteristics of blocking: firstly, the determination of wavelet primitives and the whole network structure has reliable theoretical basis, which can avoid the omnipotence of structure design such as BP neural network; Secondly, the linear distribution of network weight coefficient and the convexity of learning objective function make the network training process fundamentally avoid nonlinear optimization problems such as local optimization. Third, they have strong ability to learn and popularize functions. All these characteristics make wavelet neural network a promising research direction in the field of artificial neural networks [7].

The intrusion detection model of wavelet network algorithm based on BP has been established, and the next step is the learning and training process of wavelet network. This learning algorithm belongs to the 6-learning rule, which is a learning algorithm with tutors, so it is necessary to have rich and representative training data. At present, in the field of intrusion detection at home and abroad, researchers generally adopt the world-recognized data sources based on KDDCUP'99 standard. Since 1998, the Intrusion Detection Evaluation Project Team of DARPA of the U.S. Department of Defense has collected a large amount of network connection data on the simulated LAN as an intrusion detection evaluation database. The database contains 5 million TCP/IP connection records for training and 2 million records for testing. Training data is marked (normal or some kind of attack 1), and the data set contains 38 kinds of attacks, which are divided into four categories: DOS, Probing, R2L and U2R. Because the data set contains a large amount of redundant security information, Wenke Lee abstracted the feature set which is beneficial to judgment and comparison from the data set, and established KDDCUP'99 project. Lee extracted 41-dimensional features from DARPAl998 data and divided them into four categories: basic TCP features (features 1 ~ 9), payload-related features (features 10 ~ 22), time-based traffic features (features 23 ~ 31) and host-based traffic features (features 32 ~ 41).

3.4 Wavelet Transform Analysis

Wavelet transform is based on the idea of polynomial interpolation. The most remarkable feature is that Fourier analysis is not introduced, and all operations are carried out in the spatial domain, thus getting rid of the dependence on the frequency domain. With wavelet transform, all traditional CDF (CoherDaubechies-Feauveau) biorthogonal wavelets can be generated, and a fast algorithm (the speed is about twice that of traditional wavelet transform) can be easily found. Inverse transformation is also easy to realize, and has the same complexity as the forward transformation. The signal can be of any length (not necessarily 2n), allowing in-situ calculation and saving computer memory. It can be easily extended to integer transformation [8].

The input signal 2^k with S_j discrete values is decomposed into low-frequency signal S_{j-1} and high-frequency detail signal d_{j-1} by wavelet. The wavelet transformation process composed of lifting method can be divided into splitting, as shown in Figure 3.

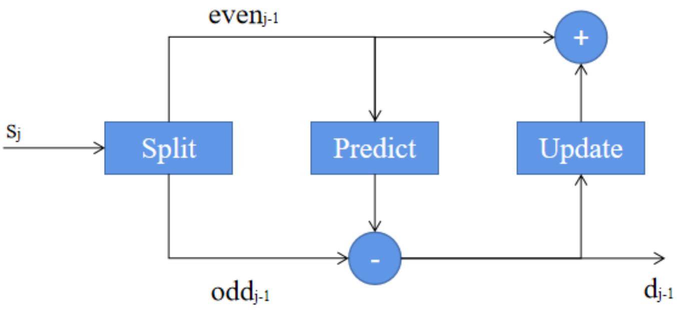

Fig.3 Block Diagram of Wavelet Transform.

To make the mean value of the coefficient subset S_{j-1} generated through the above steps equal to the mean value of the original signal S_j, d_{j-1} can be used to update, that is,

$$S_{j-1} = even_{j-1} + U(d_{j-1}) \qquad (11)$$

In this way, after a certain number of iterations, a multi-level decomposition of the original signal set can be obtained, and the same result as the traditional wavelet transform can be obtained, that is, the signals are separated in different frequency bands, and the decomposed vibration signals have components in each frequency band, but these frequency bands are not all useful for fault identification, so it is necessary to screen characteristic frequency bands. Usually, 0.5 times of power frequency, power frequency and its components are closely related to faults, so the frequency bands where these characteristic frequencies are located are selected as characteristic frequency bands. The energy values in each frequency band form a vector, which corresponds to different values for different faults, so that relevant fault information can be extracted, which provides an effective way for fault diagnosis.

4. Conclusion

Wavelet network combines the advantages of both wavelet analysis theory and neural network theory. Its research and development has opened up a new expanding space for neural network, which makes neural network widely and deeply applied in more fields. At present, a large number of research results also prove this point. In this paper, the good characteristics of wavelet network are used in intrusion detection technology, and a new network structure of intrusion detection model is established. At the same time, the intrusion detection model based on wavelet network with different algorithms is deeply studied. Finally, according to the results and data of simulation experiment, the five algorithms are compared and analyzed from four aspects: error training curve, training result, test result and selection of activation function and cost function, and the conclusion is drawn: Firstly, it is feasible to apply wavelet network to intrusion detection technology; Secondly, based on the Morlet wavelet function as the activation function of the hidden layer and the mean square error function as the training objective function, the intrusion detection model of wavelet network is established, and its convergence speed, test results and other comprehensive performance are better than those of neural networks of other algorithms. The test results fully prove this point. Compared with the intrusion detection model based on the traditional BP algorithm, the detection rate is increased by 4.96%, and the false alarm rate and the false alarm rate are reduced by 3.84% and 1.29%, respectively. Applying it to intrusion detection technology can improve the security performance of the network, and has certain reference significance in the future research of intelligent intrusion detection model.

From the simulation experiment, it is known that the selection of feature vectors will also affect the effect of network training and test results. Secondly, the threshold value, weight value, translation factor and expansion factor of wavelet network are initialized, and there is no other theory for reference at present. There is also the problem of determining the number of nodes in the hidden layer. It can be seen that there is no mature theory to guide, and researchers always determine the range according to the empirical formula, and then debug in the experiment to select the optimal parameters. Finally, the selection of learning rate and momentum coefficient of wavelet network is also a subject worth studying. In a word, the application of wavelet neural network in intrusion detection technology needs continuous in-depth research and experiments to further improve the performance of wavelet network. The intrusion detection model established in this paper is simple in algorithm, easy to program and consume less resources, so the research and design of the detection engine at the back end of the network intrusion detection system in high-speed environment has certain practical value.

References

[1] Su Yangang. Application of integrated immune wavelet neural network model in computer virus detection [J]. Information security and technology, Vol. 7, No. 003, pp. 76-782016

[2] Wang Chao, Ma Chi, Chang Junjie. Evaluation of cooperative combat capability based on improved wavelet neural network [J]. Command information system and technology, Vol.011, No.001, pp.41-452020

[3] Chen Yiping, Yu Long, Chen Chao. Traffic anomaly detection based on wavelet neural network and ARMA model in big data environment [J]. Journal of Chongqing University of Technology (NATURAL SCIENCE), 2019, V.33; No.414(10):155-160,2019,.

[4] Yan Guirong. Research on the implementation of computer network information security analysis and security management [J]. Scientist, Vol. 4, No. 012, pp. 25-27, 2016

[5] Liang Bo. Computer network information security analysis and management [J]. Electronic technology and software engineering, vol.000, no.009, pp.196-196.2017

[6] Tang Zhengjun, song Jianshe. Research on radar target recognition method based on wavelet analysis and neural network [J]. Computer and digital engineering, Vol. 027, No. 004, pp. 22-2622019

[7] Liu Bin, Wang Jie, he Guangjun, et al. UAV inversion control based on recursive wavelet neural network [J]. Computer simulation, vol.33no.02, pp.116-1212016

[8] Zhu Jie. Evaluation of information security encryption management based on artificial neural network [J]. Computer technology and development, Vol. 29, No. 269 (09, pp. 103-1072019