Application of Neural Network Model Combined with Fuzzy Theory in Computer Network Security

Xiaotian Liu

Yancheng Vocational Institute of Industry Technology, Yancheng Jiangsu, 224005,China

Key words: Fuzzy theory, Neural network model, Computer, Network security, Application.

Abstract. With continuous development of science and technology, actual data integration and operating path also change greatly. To better improve transmission accuracy of overall data information, and guarantee optimal establishment of computer network security system, accuracy of overall system can improve fundamentally and more efficient computer security treatment measures can be established only when efficient network model operates. This paper simply analyzes the connotation of computer network security risk assessment model, intensively interprets the principle of fuzzy theory and composition of neural network model and finally discusses neural network model of fuzzy theory and fusion system of computer network security. This paper aims to verify system security performance through effective data analysis.

Introduction

Fuzzy mathematic theory, rough set theory and grey system theory can be used to establish effective security risk assessment and calculation for computer system, and corresponding research results have been gained. The administrator should guarantee establishment of effective technical cognition for risk assessment model, fully mine adaptive ability and nonlinear mapping ability of system, actively operate intelligent control algorithm in risk quantification process and overall assess operation projects so as to effectively avoid influence of human factors, achieve objectivity of assessment results and establish more optimal project data.

Risk assessment model of computer network security

Security maintenance work of computer information system is a very complex project. It not just concerns corresponding management criteria, but also relates to corresponding risk analysis technology. If single management measure and control mechanism are applied, actual project cannot be effectively managed. Thus, the administrator should take risk orientation as assessment criteria, utilize computer network security risk assessment model to effectively cope with the possible threats, and carry out project analysis and assessment of uncertain factors when establishing management mechanism and management measures. Thus, computer network security risk assessment model has very important guiding significance in actual enterprise operation process. Effective measures can be used to establish ,research and develop security assurance system[1].

For computer network security risk assessments model, developed countries researched it early. System safety engineering capability maturity model (SSECMM) was applied early to establish computer network security risk assessments model. Physical security evaluation criterion, administrative security evaluation index, system security evaluation criterion, information security evaluation criterion and network security evaluation criterion serve as evaluation framework of five computer system security for network security assessment. During operating corresponding assessment mechanism and assessment strategy, engineering safety administrators should carry out

on-depth project analysis and mining and establish the optimal assessment model so as to effectively adjust safety prevention direction. The specific computer network security risk assessment model regards the system itself as radiation reference and draws forth subproject management system of physical criterion, environmental standard, network criterion, information standard, system standard and personnel standard. Then, safety assessment algorithm is applied to finally figure out security assessment result[2].

Neural network model of fuzzy theory

Fuzzy theory data integration

In the process of computer security risk assessment, the indexes have significant subjectivity and corresponding numerical values cannot e effectively confirmed. This generates influence on data processing. Thus, during establishing data set for computer network security risk assessment model, corresponding researchers should utilize fuzzy processing to carry out effective correlation analysis of computer system threats and vulnerability, intensively handle corresponding security risk factors and utilize fuzzy theory to construct computer risk factor set, such as $U = \{u_1, \ u_2, ... u_m\}$. Besides, researchers should intensively construct fuzzy assessment set. In practical construction process, corresponding administrators should intensively analyze integrity and use value of information in computer system, effectively analyze the severity of vulnerable points, effectively assess technical content of threats and ensure understanding of scores of each index, such as $V = \{v_1, \ v_2, ... v_m\}$. After exports give corresponding risk indexes, effective fuzzy mapping system should be established, $f : U = F(U)$; $u_1 = f(u_1) = (r_{i1}, r_{i2}, ... r_{im}) \in F(V)$. In the mapping system, $F(V)$ represents all fuzzy sets on V. In the process of establishing reference expert comment, the administrator should effectively judge each index and guarantee integrity of index empowerment. After all data go thought fuzzy processing, final computer security risk assessment utilizes neural network model algorithm for result output[3].

Neural network algorithm

In recent years, the application frequency of BP neural network algorithm is on the rise. Its overall structure is simple, and corresponding operation speed is also better than traditional algorithm. In overall neural network algorithm structure, three-layer feed-forward network is mainly established. The three-layer network is composed of hidden layer, input layer and output layer. The specific transfer process is as follows: the data enter algorithm system from the input layer; after forward transfer, the data directly enter hidden node in the system to ensure effective operation of data processing mechanism; then, the processed data are directly transmitted through the hidden node to the node at the output layer. In system operation process, interconnection operation mode can be used between neural network layer and node layer, and there should be no interconnected adhesion mode among nodes in the same layer. Besides, the administrator mainly utilizes S-type transformation function as transfer function in neural network algorithm to ensure effective exertion of overall generalization ability. After corresponding output and input mapping relationship is established, internal system and system data research will form benignant interaction mechanism[4].

Fusion of neural network model of fuzzy theory and computer risk assessment

Neural network security risk assessment of fuzzy theory

In the process of fusing fuzzy neural network and computer risk assessment project, corresponding administrator should carry out standard operation for actual assessment factors and assessment level, apply transformation principle of fuzzy set to handle corresponding projects intensively, effectively delimit fuzzy boundary of membership degree, enhance operation structure of thought assessment

matrix, effectively input the structure of neural network algorithm in the matrix and ensure effective level classification of neural network processing structure.

The detailed process of neural network security risk assessment of overall fuzzy theory is as follows: establish security risk factor set first, then establish assessment set and refer to the assessment set to effectively asses each factor as well as establish corresponding fuzzy mapping through applying expert comment. The administrator should utilize matrix structure to divide weight vector of each factor, and really achieve effective weight vector of resource, threat and vulnerability. Finally, the administrator should utilize three-element assessment set index in the system for number construction, intensively input it in the computer and then establish learning and training project. After computer security risk level is shown, the specific operation is completed. In other words, after the administrator gathers computer data, network data discretization is utilized to form RS simple mode with network attribute, and then neural network structure is confirmed to ensure optimal network. If the optimal neural network can effectively learn simplified data, network fault diagnosis directly operates. Finally, the output of neural network security risk assessment malformation diagnosis structure of fuzzy theory is utilized.

Risk assessment model of fusion of fuzzy theory and computer network security

In the process of establishing fuzzy theory, corresponding administrator should establish necessary project analysis mechanism according to specific conditions, connect fuzzy theory and BP neural network and establish corresponding computer system security risk assessment model. It is necessary to intensively corresponding processing model based on FNN information system. In actual model, the influence factors of computer system security risk serve as the source of radiation, and fuzzy assessment is used to judge subjection vector. Then, basic quantization processing is conducted to ensure initial establishment of factor risk quantification model. Then, BP neural network is inputted intensively to achieve effective generation of risk assessment results[5].

In practical modeling process, three aspects should be concerned. Effective risk assessment model can be really established only when standardization and normalization of specific operation are guaranteed. Firstly, effective sample set design should be trained intensively. In actual project operation process, experimenters should establish corresponding subjection measurement vector for risk factor i. Basic quantized value of risks can be expressed as . Besides, the result of multi-level fuzzy comprehensive evaluation of system is set to B in the experiment process. Then, corresponding expression can be used to effectively express comprehensive score of system security risk, i.e. $p = B \times \beta^T$. After corresponding data are measured, the first step of security assessment can be completed. Secondly, optimal design of BP network structure should be established. In practical risk assessment project, the administrator should utilize optimization of network structure. A key point is to input the number of nodes, i.e. actual number of risk factors. If the number of nodes at the input layer is 1, this indicates the hidden layer ha three-layer neural network. As long as the number of nodes at the hidden layer is more, the whole system can tend to a critical value with uniform precision value and present any continuous function. The administrator should establish simplified version of corresponding risk assessment model according to specific conditions, improve effective model training efficiency and utilize empirical formula and cut-and-trial to establish effective simulation experiment so as to guarantee integrity and balance of BP network structure design in overall risk assessment structure. Thirdly, practical optimization should be carried out for BP neural network training and testing items. In system operation process, corresponding administrator should test the rate of convergence for practical BP network learning algorithm and guarantee slowdown and effective settlement of local minimum of overall target function. Researchers can utilize Levenberg-Marquardt method for optimization and improvement of effective algorithm. This is mainly because in the operation process of Levenberg-Marquardt method, basic convergence rate and precision are high, and the number of iterations is small. These quite conform to corresponding project requirements. In addition, the administrator should utilize the measures which stop in the initial stage to improve generalization ability of overall system and BP network algorithm in actual

operation process of risk assessment mechanism. Besides, in actual project operation process, it is required to collect project data intensively and divide basic samples into two parts at random. Some data are combined to become training set, and the other data are aggregated to test set. In project system operation process, the administrator should intensively apply performance function and network weight in computer structure and make sure overall data gradient complies with practical project requirements. In practical training process, the administrator should supervise corresponding management behavior, guarantee low operation of training and testing projects and really make training error value and testing error value represent optimized values.

Simulation example

We suppose to design BP neural network, including three-layer structure. There are 25 nodes in the input layer. The input values are quantized values of 25 risk factors . 1 node is set at the output layer. The output value is comprehensive score of system security risk project. empirical formula is utilized to figure out the number of hidden nodes in the system, and establish corresponding Sigmoid function. Effective analysis and preprocess are conducted for input data. Meanwhile, effective training function trainlm is established, and Levenberg-Marquardt method is applied to intensively improve system algorithm to make sure error performance function complies with actual requirements. We suppose e=0.0001 in BP neural network. Basic network learning rate should be maintained at $\alpha = 0.05$. For the experiment, relevant administrator should utilize 30-40 samples to integrate training sample set, and utilize initial termination method to improve network generalization ability. In the sample set, 1/10 of sample sets is test set, and 9/10 of sample sets are training sets. After concentrated calculation, the contrast value of security assessment result and training result is used for effective analysis and processing, and establishment of relations among various elements in the system.

Conclusion

After the administrator effectively analyzes the system, risk assessment measures which combine multi-level fuzzy comprehensive judgment mechanism with BP neural network are established to deeply mine overall data items and establish optimized judgment criteria so as to achieve randomness and effectively reduce subjective uncertainties. In one word, when neural network model combined with fuzzy theory is applied in computer network security, relevant administrators should establish more scientific and rational project handling mechanism, operate targeted analysis strategy for different data, construct optimized risk assessment mode and offer more effective data and information for computer system security assessment,

Acknowledgement

References

[1] Qiu Xiaoqing, Study on adaptive median filtering algorithm based on fuzzy theory, Collected papers of the 23rd nationwide academic conference about coal mine automation and informatization – the 5th management forum for China coal mine automation and informatization. 2013:146-150.

[2] Pan Liangliang, Study on assessment of initial operation stage of 800kV SF6 breaker based on improved fuzzy theory, Collected papers of 2013 nationwide technical exchange seminar about equipment state maintenance of power grid enterprises. 2013:846-851.

[3] Mo Jiaqing, Hu Zhongwang, Ye Xuelin et al., Study on dependable computing trust assessment method based on fuzzy theory, *Journal of Computer Applications*, 2013,33(01):142-145.

[4] Chen Qin, Liu Qingqing, Study on construction of credit rating model of C2C e-commerce website based on fuzzy theory, Collected papers of 2013 annual meeting of Guizhou Computer Society. 2013:37-40.

[5] Wang Xinying, Chen Qin, Feasibility analysis on credit appraisal system of C2C e-commerce based on fuzzy theory, Collected papers of 2013 annual meeting of Guizhou Computer Society. 2013:32-36.