Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 11, November 2019, pp. 2908-2915
DOI: 10.23940/ijpe.19.11.p9.29082915

Information Security Evaluation based on Artificial Neural Network

Rong Li*, Bing Tian, Yan Li, and Yansheng Qu

State Grid Shandong Electric Power Company, Jinan, 250021, China

Abstract

In order to improve the information security ability of the network information platform, an information security evaluation method is proposed based on artificial neural networks. Based on the comprehensive analysis of the security events in the construction of the network information platform, the risk assessment model of the network information platform is constructed based on the artificial neural network theory. The weight calculation algorithm of artificial neural networks and the minimum artificial neural network pruning algorithm are also given, which can realize the quantitative evaluation of network information security. The fuzzy neural network weighted control method is used to control the information security, and the non-recursive traversal method is adopted to realize the adaptive training of the information security assessment process. The adaptive learning of the artificial neural network is carried out according, and the ability of information encryption and transmission is improved. The information security assessment is realized. The simulation results show that the method is accurate, and the information security is ensured.

Keywords: artificial neural network; information security; evaluation; information encryption

(Submitted on August 7, 2019; Revised on October 11, 2019; Accepted on November 10, 2019)

1. Introduction

The 21st century is the information age, and information systems play an increasingly important role in contemporary society. Information systems consist of computer hardware, network systems, computer software, communication equipment, user groups, network protocols, network rules and regulations, information flow, and so on [1]. The appearance of information systems greatly facilitates information sharing and information transmission. With the rapid development of social economy, both the speed and capacity of information transmission are constantly creating new heights. Information transmission is closely related to people's daily lives. The rapid development of the Internet has greatly improved people's lives, work, and learning efficiency; however, at the same time, security risks have emerged. People can obtain information effectively through the Internet, but information can be intercepted by a third party in the process of information transmission. Information confidentiality, integrity, and reliability are all affected. From the point of view of information security, risk assessment seeks to analyze the weaknesses of the information system and identify possible threats. It is an important way to study information security and belongs to the planning process of organizational information security management systems. The main content of risk assessment includes identifying the risk that the information system may face, the probability of the occurrence of the risk, the possible consequences of the risk, the risk elimination strategy, and the risk control strategy. The composition of information systems is extremely complex, so information system security risk assessment is a comprehensive work. Its organizational structure is more complicated and mainly includes a technical system, organizational structure, legal system, standard system, business system, and so on. In order to avoid risks, network security managers must formulate appropriate security policies, and the purpose of risk assessment is to provide the basis for the formulation of security policies [2-3].

The special contributions of this paper include the following:

* Corresponding author.
E-mail address: wangchong-2009@hotmail.com

(1) The algorithm flow and application range of the artificial neural network model are introduced.

(2) The evaluation of network information security is analyzed theoretically.

(3) The artificial neural network model is applied to network information security.

The rest of this paper is organized as follows. Section 2 discusses related work. Section 3 introduces the encryption design of network information. Section 4 introduces the evaluation of information security optimization and the realization of process optimization. Section 5 carries out experimental simulation. Finally, Section 6 summarizes the full text.

2. Related Works

The task of network security is to ensure the basic functions of the network and realize various security requirements. Network security requirements are mainly reflected in protocol security requirements, and protocol security services put forward the protocol security requirements. In order to meet the requirement of protocol security [4], it is necessary to take effective preventive measures against the attack of the protocol. Protocol vulnerability exposes the risk of protocol, and the existence of protocol risk leads to the security requirements of protocols. Attacks on network protocols lead to protocol threats and increase protocol risks, resulting in new security requirements. Taking effective preventive measures against protocol attacks can reduce the protocol risk, meet the protocol security requirements, and realize protocol security services. Preventive measures are aimed at certain risks, cannot be omnidirectional, and can lead to new safety risks while achieving the purpose of prevention.

In order to improve the information security ability of the network information platform, this paper puts forward an information security evaluation method based on artificial neural networks. It constructs the risk assessment model of the network information platform based on the artificial neural network theory. The weight calculation algorithm of artificial neural networks and the minimum artificial neural network pruning algorithm are also given, which can realize the quantitative evaluation of network information security. The fuzzy neural network weighted control method is used to control the information security. When the risk calculation method is selected, the strategy of weighted synthesis of various risk calculation methods is adopted. It is a combination of multiple risk analysis methods to improve the ability of information security prevention and evaluation. Finally, the performance test is carried out through the simulation experiment, which shows the superiority of this method in improving the ability of information security evaluation.

Information security assessment is divided into two categories: quantitative assessment methods and qualitative evaluation methods [5].

Qualitative assessment is the most frequently used method for information security risk assessment. This method is taken based on the comprehensive evaluation of system risks by specific assessment methods, summing up experience, history, and other factors [6]. The method pays more attention to the possible consequences of security risks and neglects the probability of safety time. There are many factors in qualitative evaluation that cannot be quantified, so there is uncertainty in the evaluation result itself, and this evaluation method is suitable for all kinds of insufficient data collection [7].

Quantitative assessment and qualitative evaluation are opposites of each other, and this method needs to be standardized on the basis of all factors. Quantitative evaluation needs to collect relevant data and ensure the accuracy of the data. Then, a mathematical method is used to establish a model to verify the various processes and draw a conclusion. Quantitative assessment requires sufficient data and is a method of extrapolating results using formulas. In essence, quantitative evaluation of customer service qualitative evaluation of shortcomings is more objective [8]. Quantitative evaluation can quantify complex evaluation processes, but this method must be based on accurate data. The quantitative evaluation method is not subjective enough, and its conclusion is not profound or concrete enough. The representative method of quantitative evaluation is fault tree evaluation. The fault tree method adopts logical thinking for risk assessment, and its characteristics are intuitionistic and clear. It is a method of deductive logic reasoning, in which the reasoning process is from result to reason, which is mainly used in the stage of risk prediction. The concrete probability of risk occurrence is obtained, and the risk control method is obtained as well.

3. Design of Information Encryption and Coding for Network Information Platform

3.1. Data Encryption Algorithm for Information Security

The binary pseudorandom sequence is constructed to express the Turbo code of the network information platform, and the

key scheme is designed. The risk assessment model of the network information platform is constructed. The probability that the information in the *i* storage node can be accurately transmitted to the Sink node is λ_i, and the encryption key randomly selects a vector $\boldsymbol{u}$ to obtain the matching degree of data encryption.

$$\lambda_{SRm} = \sum_{i=1}^{M} \lambda_i p_{im} \tag{1}$$

The model of queuing theory is used to evaluate the information security, and the accurate transfer probability distribution of ontology resource m is given as follows:

$$\rho_{SRm} = \frac{\lambda_{SRm}}{\mu_{SRm}} = \sum_{i=1}^{M} \frac{\lambda_i p_{im}}{\mu_{im}} \tag{2}$$

Under the condition of steady state convergence, the stochastic queuing mechanism is introduced to calculate the average time $T_{service}$ of data coding in the clear text block. The information security is monitored, and the waiting time T_{wait} is obtained.

$$T_{service} = \frac{1}{\mu_{SRm}} = \frac{\rho_{SRm}}{\lambda_{SRm}} = \frac{1}{\sum_{i=1}^{M} \lambda_i p_{im}} \cdot \sum_{i=1}^{M} \frac{\lambda_i p_{im}}{\mu_{im}} \tag{3}$$

The response characteristic of information security assessment is obtained as follows:

$$\sigma_{service} = \sqrt{\frac{1}{M} \sum_{i=1}^{M} (\frac{1}{\mu_{im}} - T_{service})^2} \tag{4}$$

Under the suffrage scheduling policy [9], the autocorrelation statistical characteristic of replica *m* performing information security evaluation is

$$T_{wait} = \frac{\rho_{SRm} T_{service} [1 + (\frac{\sigma_{service}}{T_{service}})^2]}{2(1 - \rho_{SRm})} = \frac{\sum_{i=1}^{M} (\frac{\lambda_i p_{im}}{\mu_{im}}) T_{service} [1 + (\frac{\sigma_{service}}{T_{service}})^2]}{2(1 - \sum_{i=1}^{M} \frac{\lambda_i p_{im}}{\mu_{im}})} \tag{5}$$

The significant level of the frequency test is defined as $x_0 = q_0 \cdot \pi$, in which q_0 satisfies $q_0 \leftarrow \mathbb{Z} \cap \left[0, 2^{\gamma} / \pi\right)$, the frequency of information security evaluation is less than 2^{λ^2}, the error correction is carried out by 0 and 1 distribution, and the data encryption is realized by the orthogonal vector quantization analysis method. The definition of quantization encoding $\boldsymbol{v}_1^*, \boldsymbol{v}_2^*, \cdots, \boldsymbol{v}_m^*$ of the encrypted output is obtained.

$$\begin{aligned} \boldsymbol{v}_i^* &= \boldsymbol{v}_i - \sum_{j=1}^{i-1} \mu_{i,j} \boldsymbol{v}_j^* \\ \boldsymbol{v}_1^* &= \boldsymbol{v}_1 \end{aligned} \tag{6}$$

Where $i = 1, \cdots, m$ and $\mu_{i,j} = \frac{\langle \boldsymbol{v}_i, \boldsymbol{v}_j^* \rangle}{\langle \boldsymbol{v}_j^*, \boldsymbol{v}_j^* \rangle}$.

According to the above definition, information security evaluation and key construction are realized. The encryption keys for the information security evaluation are

$$dsk_{ID_i} = (sk_{i1}, sk_{i2}) = (g_2{}^{a}(g_1{}^{t_i}h)^{u_i}, g^{u_i}) \tag{7}$$

$$rsk_{ID_i} = (sr_i = g_1^{u_i}) \tag{8}$$

The link layer protocol is updated adaptively, and the risk assessment model of the network information platform is constructed based on the artificial neural network theory to improve the information evaluation ability [10-12].

3.2. Artificial Neural Network Algorithm

In order to improve the ability of information security evaluation, the artificial neural network algorithm is used to code the information by vector quantization [13]. The three-layer artificial neural network model is shown in Figure 1.

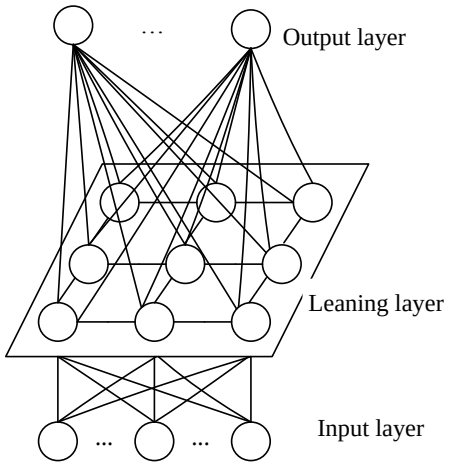


Figure 1. Algorithm flow of three-layer artificial neural network model

Based on the theory of artificial neural network, the risk assessment model of network information platform is constructed. The steps are expressed as follows [14]:

Step 1 Set $x(t)$, where $t = 0,1,\cdots,n-1$, as the training time for the network information platform, and set the time as $t = 0$.

Step 2 Input a new training vector mode to the network information platform $x(t) = (x_0(t), x_1(t), \cdots, x_{k-1}(t))^{\mathrm{T}}$.

Step 3 Calculate the distance between input vector $x(t)$ and weight vector $x(t)$ of all output nodes in the artificial neural network.

$$d_j = \sum_{i=0}^{k-1}(x_i(t) - \omega_{ij}(t))^2, \ j = 0,1,\cdots,N-1 \tag{9}$$

Step 4 Find the minimum distance nodes in the hidden layer of the artificial neural network transmission N_{j^*}, $d_{j^*} = \min\limits_{0 \le j \le N-1}\{d_j\}$.

Step 5 By adjusting the weights connected to output node N_{j^*} and the weights connected to the nodes in N_{j^*} geometry neighborhood $NE_{j^*}(t)$, the self-organizing feature mapping of the Kohonen network is realized. The weighted update iterative formula of information security evaluation is obtained as follows:

$$\omega_{ij}(t+1) = \omega_{ij}(t) + \alpha(t)(x_i(t) - \omega_{ij}(t)) \tag{10}$$

Where $N_j \in E_{j^*}(t)$ and $0 \le i \le k-1$, $0 \le \alpha(t) \le 1$. It is the speed of learning and training, which decreases with time just like $NE_{j^*}(t)$.

Step 6 According to the adaptive learning and weighted control method, the information security evaluation is carried out and the sample data is input, and $t = t+1$. It is applied to information fusion by using the minimum artificial neural network pruning algorithm, so that the fuzzy judgment capability is improved.

4. Optimization of Information Security Evaluation and Realization of Flow Optimization

Based on the artificial neural network theory, the risk assessment model of the network information platform is constructed [15], and the information classification is carried out by using the C-means clustering method. The objective function of the information security assessment is obtained as follows:

$$L_{SRm} = \lambda_{SRm} T_{SRm} = \sum_{i=1}^{M} \lambda_i p_{im} (T_{wait} + T_{service}) \tag{11}$$

According to the pruning of the kernel minimum artificial neural network, the information vector quantization of the unit m resource fusion center is obtained, and the output is the following [16]:

$$I_{SRm} = \frac{L_{SRm}}{\rho_{SRm}} = \frac{\sum_{i=1}^{M} \lambda_i p_{im} (T_{wait} + T_{service})}{\rho_{SRm}} \tag{12}$$

The strategy of weighted synthesis of various risk calculation methods is used to evaluate information, and the relevance integration of information security assessment is carried out. The optimized objective function can be described as

$$I_{total} = \frac{L_{total}}{\rho_{SRm} \mid S_{SR} \mid} = \frac{\sum_{i=1}^{M} \sum_{m=1}^{|S_{SR}|} \frac{\lambda_i p_{im} T_{SRm}}{\rho_{SRm}}}{\mid S_{SR} \mid} \tag{13}$$

The risk assessment to the network protocol is taken, and the security information monitoring is realized. The implementation flow of the improved algorithm is shown in Figure 2 [17].

5. Simulation Experiment and Result Analysis

In order to test the performance of this method in realizing information security evaluation, the simulation experiment is carried out. The hardware environment of the experiment is Windows 7 system, the computer of processor 3.6GHz, and the simulation tool is Matlab 2010b [18]. In the experiment, the information security assessment and testing of the large data in the information platform of different block length are tested, and the data sampling is divided. The length of the block is 500, the length of each block of each group is 10,000, the number of iterations is set to 100, the public key size is 72MB, and the security parameter is 2.5. The encrypted bit sequence of quantized encoding is the following [19]:

1101001010010010101001010010101001001010010101001010010100010100101001010010010010101111010010100100100101001001010010100100101001010101010010100101001010010101000010100100101001010010111

According to the simulation environment and parameter setting, the information security evaluation is carried out to obtain the test interface as shown in Figure 3 [20].

In the interface shown in Figure 3, the information security evaluation test is carried out, and the time domain waveform of the information output is obtained as shown in Figure 4.

Taking the data of Figure 3 as the research object, the data is encrypted to realize the digital protection of social network, and the output of data encryption is shown in Figure 5.

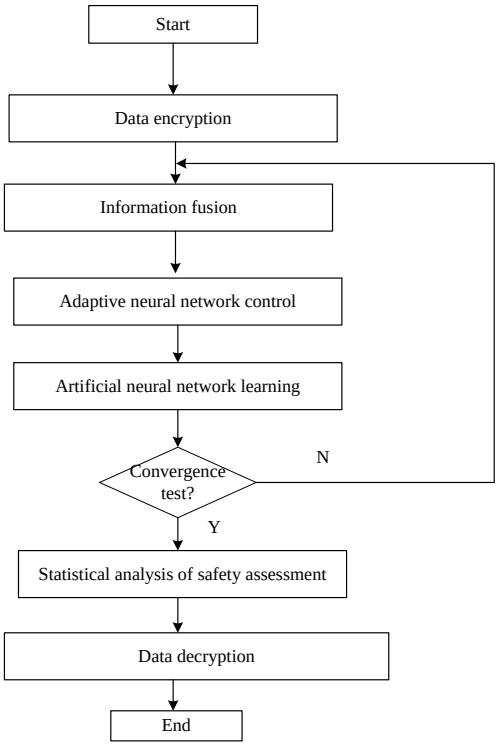
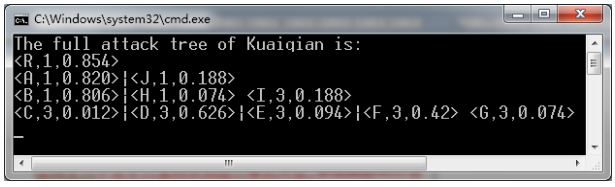
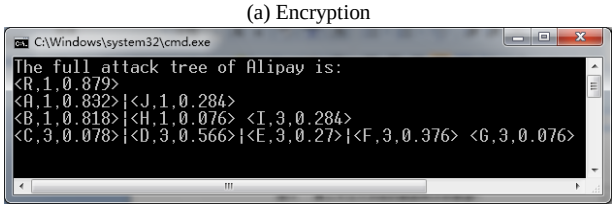


Figure 2. Implementation flow of the improved algorithm



(a) Encryption



(b) Deciphering

Figure 3. Test interface for information security assessment

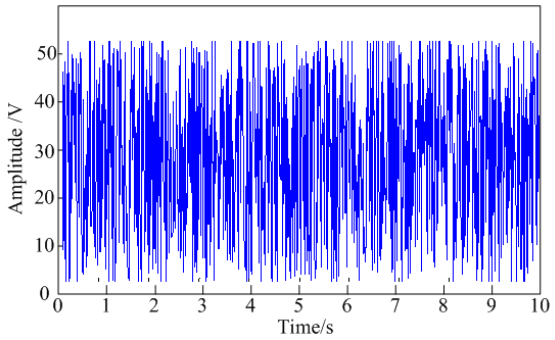


Figure 4. Information transmission time domain waveform

On this basis, the information security evaluation is carried out, and the comparison of the number of ciphertext digits in the information security assessment is shown in Figure 5. The larger the change in ciphertext, the worse the information

security, and the test result in Figure 6 is analyzed. The method of this paper is used to evaluate the information security, and the number of plaintext bits is 63 ± 7 . It can be seen that when this algorithm is used to encrypt the data, the number of ciphertext changing bits is higher, and the ability of resisting plaintext attacks is better. It improves the performance of data steganography and has better information security control and transmission ability.

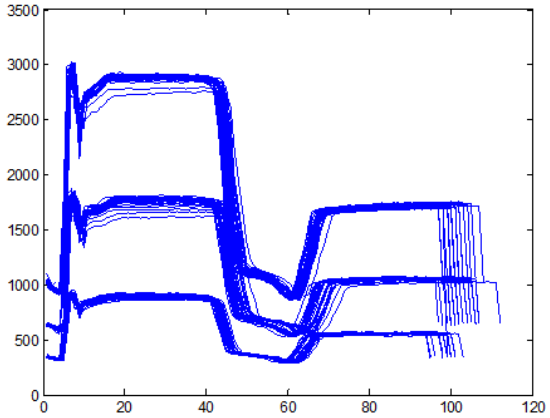


Figure 5. Data encrypted output

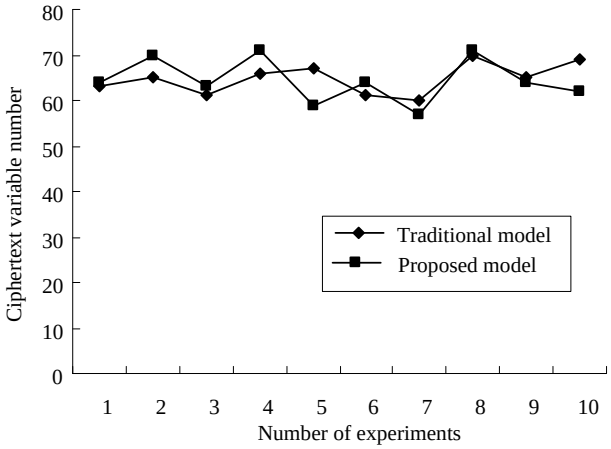


Figure 6. Information security evaluation performance test

6. Conclusions

In this paper, an information security evaluation method is proposed based on artificial neural networks. Based on the comprehensive analysis of the security events in the construction of the network information platform, the risk assessment model of the network information platform is constructed based on the artificial neural network theory. The weight calculation algorithm of artificial neural networks and the minimum artificial neural network pruning algorithm are also given, which can realize the quantitative evaluation of network information security. The fuzzy neural network weighted control method is used to control the information security, and the non-recursive traversal method is adopted to realize the adaptive training of information security assessment processes. The adaptive learning of the artificial neural network is carried out according to the conditions, and the ability of information encryption and transmission is improved. The information security assessment is also realized. The simulation results show that the method is accurate, and the information security is ensured. It has good application value in information security construction.

References

1. P. A. Fouque, B. Hadjibeyli, and P. Kirchner, “Homomorphic Evaluation of Lattice-based Symmetric Encryption Schemes,” in *Proceedings of the 22nd International Conference on Computing and Combinatorics*, pp. 269-280, Springer, Berlin, January 2016
2. F. Z. Feng, C. S. Zhang, Q. X. Min, and P. F. Wang, “Heating Characteristics of Metal Plate Crack in Sonic IR Imaging,” *Infrared and Laser Engineering*, Vol. 44, No. 5, pp. 1456-1461, July 2015
3. H. Y. Zhang, Y. L. Kuang, G. H. Wang, and L. Ji, “Soft Sensor Model for Coal Slurry Ash Content based on Image Gray

Characteristics," *International Journal of Coal Preparation and Utilization*, Vol. 34, No. 1, pp. 24-37, September 2015
4. F. Y. Xu, G. H. Gu, X. F. Kong, P. C. Wang, and K. Ren, "Object Tracking based on Two-Dimensional PCA," *Optical Review*, Vol. 23, No. 2, pp. 231-243, February 2016
5. R. Kumar, B. K. Verma, and S. S. Rastogi, "Social Popularity based SVD++ Recommender System," *International Journal of Computer Applications*, Vol. 87, No. 14, pp. 33-37, October 2014
6. M. Ovesny, P. Krízek, J. Borkovec, Z. Svindrych, and G. M. Hagen, "ThunderSTORM: A Comprehensive ImageJ Plug-in for PALM and STORM Data Analysis and Super-Resolution Imaging," *Bioinformatics*, Vol. 30, No. 16, pp. 2389-2390, February 2014
7. Z. H. Wu and P. Hu, "Analysis on VANET Routing Protocols," *Journal on Communications*, Vol. 36, No. 5, pp. 75-84, October 2015
8. L. S. Li and Q. Q. Weng, "Self-Adaptive Differential Evolution Algorithm based on Opposition-based Learning," *Journal of Computer Applications*, Vol. 38, No. 2, pp. 399-404, July 2018
9. S. L. Xiao, X. Chen, and Z. Li, "Distributed Neural Network for Classification of Attack Behavior to Social Security Events," *Journal of Computer Applications*, Vol. 37, No. 10, pp. 2794-2798, January 2017
10. Y. L. Li and J. Dong, "Study and Improvement of MapReduce based on Hadoop," *Computer Engineering and Design*, Vol. 33, No. 8, pp. 3110-3116, September 2012
11. Z. Moghaddam and M. Piccardi, "Training Initialization of Hidden Markov Models in Human Action Recognition," *IEEE Transactions on Automation Science and Engineering*, Vol. 11, No. 2, pp. 394-408, October 2014
12. B. B. Amor, J. Su, and A. Srivastava, "Action Recognition using Rate-Invariant Analysis, of Skeletal Shape Trajectories," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 38, No. 1, pp. 1-13, July 2016
13. X. Luo ,"Fuzzy Wavelet Neural Network Control based on Ant Colony Learning Algorithms," *Fujian Computer*, Vol. 11, No. 6, pp. 178-180, January 2008
14. D. M. Zhao, J. X. Liu, and J. F. Ma, "Information Security Risk Assessment based on Improved Wavelet Neural Network," *Computer Science*, Vol. 2, No. 5, pp. 125-129, September 2010
15. J. Wan, D. M. Xu, and Y. Q. He, "Research on a Wavelet Neural Network Structure and Its Learning Algorithms," *System Engineering and Electronic Technology*, Vol. 3, No. 5, pp. 69-74, February 2002
16. C. X. Yang, K. C. Liu, and X. Y. Che, "Application of Improved Wavelet Neural Network in Teaching Quality Evaluation," *Journal of Nanyang Institute of Technology*, Vol. 10, No. 6, pp. 201-206, October 2011
17. D. M. Zhao, J. X. Liu, and J. F. Ma, "Information Security Risk Assessment based on Fuzzy Wavelet Neural Network," *Journal of Huazhong University of Science and Technology* (*Natural Science Edition*), Vol. 11, No. 5, pp. 189-200, February 2009
18. H. R. Wang and B. Y. Yan, "Information Security Risk Assessment Method based on Wavelet Neural Network Algorithm," *Information Technology*, Vol. 12, No. 15, pp. 169-172, February 2018
19. W. Wang, "Power System Load Forecasting based on Wavelet Neural Network," *Monthly Journal of Science and Technology Entrepreneurship*, Vol. 12, No. 5, pp. 189-201, January 2017
20. H. Q. Wang and B. Wang, "Research and Application of Internal Model Control based on Self-Constructed Wavelet Neural Network," *Computer Measurement and Control*, Vol. 8, No. 9, pp. 265-269, September 2014