Method of Risk Assessment Based on Classified Security Protection and Fuzzy Neural Network

Chaoju Hu
Department of Computer Science
North China Electric Power University, NCEPU
Baoding Hebei, China
chunmeilv2004 @126.com

Chunmei Lv
Department of Computer Science
North China Electric Power University, NCEPU
Baoding Hebei, China
51250035@163.com

***Abstract*—Risk assessment of information security is an important assessment method in the process of detecting potential threats and vulnerabilities. Select methods of risk assessment based on the requirements and the security level of organizational or enterprise information system. The general assessment methods simply calculate the risk value, In this paper, we propose a risk assessment model based on classified security protection. We also build a modle combined fuzzy theory and BP neural network, so that the learn capability and the expression capability can be improved. Firstly, we form a risk elements set according to the classified criteria for security protection. Secondly, we quantitate the risk factors with fuzzy theory. Thirdly, we take the results the output of multi-level fuzzy system as the input of BP neural network. According to experiment testing, the risk evaluation model can estimate risk level of the information security accurately and real-timely.**

Keywords- classified security protection, risk assessment, fuzzy neural, BP neural network

I. INTRODUCTION

Classified security protection of information means classifying the information system and executing security protection, responding and coping with security issue of the information system systematically, and administering equipments, operating environment, system software, as well as the network system systematically. The basic method to classify the security of the information system is by classifying these three aspects of the system, as are secrecy, integrality and usability, to make certain the security classification.

Nationally, more and more importance has been attached to the integrative method for risk assessment of information system security, considering both the classified security strategy and method of the risk assessment. In1996, Information Technology Security Criteria Standard is put forward and evolve as International standard ISO. Internally, In November 2007, Risk Assessment Specification For Information Security was issued and come into practice. On June 22 2007, Information Security Grading Protection Policy (No. 43 document) is put out, standardizing the management of the classified security protection of information [1].

Current frame of law of the classified security protection of information systerm, does not assimilate the concept of the risk management, the behavior of the risk assessment just stay at the policy implementation stage. This thesis is going to bring forward the risk assessment method basing on the classified security protection [2]. After classifying the information system, information system security should be built and modified, in order to fulfill the proper degree of the security protection capability.

II. METHODS AND PRINCIPLES

A. Classify the Security Protection

Understand of the security level protection requirements completely and accurately, can we make full use of the level protection in the information security. The general principles of China's National Computer Protection is <<Classified criteria for security protection of Computer information system>> (GB17859) [3]classify our country's information system security into five levels. The protection ability grows stronger and the scope of protection expands larger progressively.

First-Level: Self-protection level, information systems based on this level can isolate users and data, control the users access, protect user group information from reading and writing illegally, this level is the foundation level.

Second-Level: System audit protection level, addition to include the first-class protection, it use the protective mechanism to identify users, to prevent unauthorized user using identification data.

Third-Level: Security mark protection level, which provide a model of information security policy, mark the output data tags, and control the mandatory access object by the subject.

Fourth-Level: Structure protection level, extend the control of mandatory access to all subjects and objects, Strengthen identification mechanisms, support system management and operator, make the system have ability of resist penetration [4].

Fifth-Level: Authentication access protection level. To protect the security mechanisms not to be attacked and modified, the system have an extremely ability of resist penetration.

B. BP Neural Network

BP (Back Propagation) network is a kind of error back-propagation algorithm based on the training of multilayer feed forward networks, and it is one of the most widely used neural network model [5]. BP network have the ability of self-learning and carry out complex non-linear relationships between the input and output without having

978-0-7695-4003-0/10 $26.00 © 2010 IEEE
DOI 10.1109/APWCS.2010.103

to describe the mapping of mathematical equations firstly. Use the back-propagation to constantly to adjust the network weights and thresholds, so that the network error function can reach to minimum. BP neural network model include input layer, hidden layer and output layer (Figure 1).

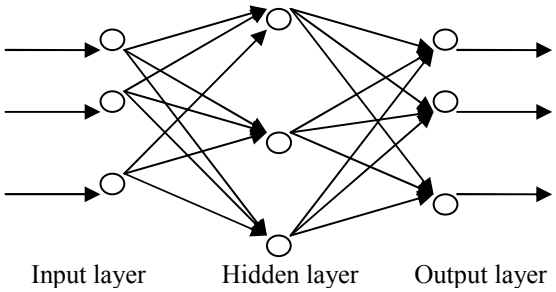

Figure 1. Structure of BP neural network

We take $x_1, x_2, \cdots, x_n$ as the input of each neuron, $w_{i1}, w_{i2}, \cdots, w_{i3}$ as the strength of the connections of different neurons. BP neural network's demands the transfer function $f(\ )$ differentiable.

The values of the neuron's net S_i :

$$S_i = \sum_{j=1}^{n} w_{ij} \cdot x_j + b_i \qquad (1)$$

1) Forward propagation: Suppose the number of the node in the input layer is n, that of output is l, m in the middle layer, u_{ij} is the connection weight between input layer and output layer and w_{ik} is the connection weight between hidden layer and output layer. $f_h(\ )$ is the transfer function of hidden layer. $f_o(\ )$ is the transfer function of output layer.

The output of the hidden layer is

$$h_i = f_h\left(\sum_{j=0}^{n} u_{ij} x_j\right) \quad i = 1,2,\cdots,m \qquad (2)$$

The output of the output layer is

$$y_k = f_o\left(\sum_{i=1}^{m} w_{ik} h_i\right) \qquad k = 1,2,\cdots,l \qquad (3)$$

2) Back propagation: Establish P groups sample as the input and output of BPNN, as follows:

$$x_p = \left[x_{p1}, x_{p2}, \cdots, x_{pn}\right]^T \ (p = 1,2,\cdots,m) \qquad (4)$$

$$d_p = \left[d_{p1}, d_{p2}, \cdots, d_{pm}\right]^T \ (p = 1,2,\cdots,m) \qquad (5)$$

The output of BPNN is y_{pi}, Error E_p and the general error E as follows:

$$E_p = \frac{1}{2}\sum_{i=1}^{m}\left(d_{pi} - y_{pi}\right)^2 \qquad (6)$$

$$E = \sum_{p=1}^{P} E_p = \frac{1}{2}\sum_{p=i}^{P}\sum_{i=1}^{m}\left(d_{pi} - y_{pi}\right)^2 \qquad (7)$$

3) The changes of the output layer weights: BP algorithm uses accumulated error to adjust w_{ik}, So that the general error can get smaller, μ is the learning rate, the formula as fllows:

$$\Delta w_{ik} = -\mu\frac{\partial E}{\partial w_{ik}} = -\mu\frac{\partial E}{\partial S_i}\frac{\partial S_i}{\partial w_{ik}} = \sum_{p=1}^{P}\sum_{i=1}^{m}\mu\left(d_{pi} - y_{pi}\right)f_o'(S_i)h_k \qquad (8)$$

Type in: μ -learning rate, δ_{yi} -error signal as follows:

$$\delta_{yi} = -\frac{\partial E_p}{\partial S_i} = \sum_{i=1}^{m}\left(d_{pi} - y_{pi}\right)f_o'(S_i) \qquad (9)$$

The changes of the hidden layer weights

$$\Delta h_{ij} = -\mu\frac{\partial E}{\partial u_{ij}} = \sum_{p=1}^{P}\sum_{i=1}^{m}\mu\left(d_{pi} - y_{pi}\right)f_o'(S_i)w_{ik}f_h'(S_k)x_j \qquad (10)$$

4) Adjust algorithm: If there is a error of between the output results with the expected results of the calculation training, and the *error* exceeded the error range, then the network begin back propagation to adjust the weights and thresholds; Calculate the output of each layer with the under the new the weights and thresholds until the training set up to meet the stop condition.

The wavelet BP neural network has some obvious advantages, such as oscillations and slow convergence. We can use the Momentum method to adjust the present values according to the last calculated results.

$$\Delta W(n) = -\eta\Delta E(n) + \alpha\Delta W(n-1) \qquad (11)$$

III. APPLICATION OF FUZZY-NEURAL NETWORK IN CLASSIFIED SECURITY PROTECTION

A. The Model of Risk Assessment

A computer information system consists the physical and operating environment layer, system layer, network layer, application layer and management layer, We must classify protection level based on the five dimensions in order to achieve the whole system security level. After ensuring the safety of all levels to meet a certain level of

protection, We should consider the relevance and complementarity among the security features of each layer as a whole.

Then, we analyze the asset, threaten and vulnerabilities of the five layer according to the risk level. The methods of information security risk evaluation can be mainly divided into the three types, i.e. qualitative, quantitative assessment method and qualitative combined with quantitative assessment method, we take the method of fuzzy neural network which belong to the third one.

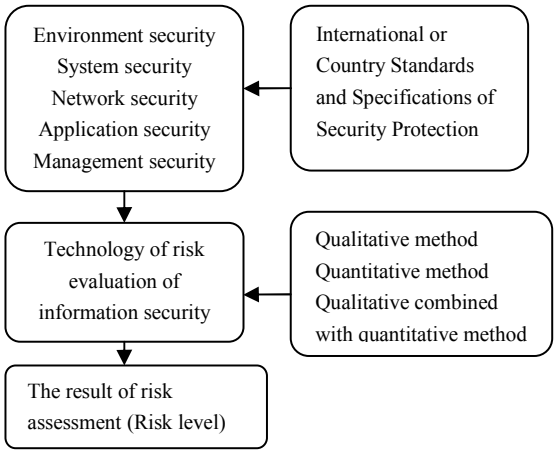

Figure 2. The model of risk calculation

We use fuzzy theory to quantify the risk factors, then calculate the risk value through back propagation neural network, at last rectificate information systems targeted.

The risk calculation can be described as follows:

Risk=R (A, T, V)

Where: R is the function of risk of security evaluation, A is asset, T is threat, V is vulnerability.

B. Fuzzy pre-dispose of inputs

1) Extract and quantitate basic elements

Extraction and quantitative of risk assessment elements must reflect the requirements of Classified criteria for security protection of Computer information system.

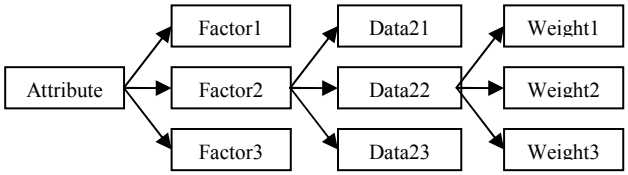

Figure 3. Hierarchy of information system security elements

First, determine which level the system security attribute belong to, then, extract primary elements according to CB17895. Hierarchize primary elements for further refinement in the third level, the fourth layer is the weight of each elements.

2) Establish a multi-level fuzzy comprehensive evaluation

Fuzzy theory based on fuzzy mathematics abstract relationship between different elements, build a model of mathematical abstraction [6]. We take the fuzzy evaluation method to quantitative the index of information security risk factors, i.e. The details realized steps is as follows.

a) Forming the elements set: Based on the analysis in section Forming the risk factors set $A=\{a_1,a_2,\cdots,a_n\}$, $a_i(i=1,2,\cdots,n)$ stand for different risk factors.

b) Forming the weight set: Based on the experts estimate, suppose the weight of right distribution, we set $B=\{b_1,b_2,\cdots,b_n\}$.

$$b_i=\frac{1}{k}\sum_{j=1}^{k}b_{ij} \tag{12}$$

Practical application requires b_{ij} meet the non-negative and normalized.

c) Forming the judgment set: The risk factors are evaluated from following the classified criteria for security protection i.e. the value of confidentiality, integrity, and availability etc. Experts give the comment of each risk factors, and divides the comment of each index into m grades, the set of judgement is $V=\{v_1,v_2,\cdots,v_m\}$.

d) Single-factor fuzzy evaluation: Based on single-factor, we evaluate the risk factors to determine the subordination of indicators, and form the fuzzy mapping $f:A\to F(V)$, *the mapping* f the supporting degree of the risk factors a_i. Suppose the membership vector of risk factors a_i to the set of judgment $R_i=\{r_{i1},r_{i2},\cdots,r_{im}\}$, $i=1,2,\cdots,n$ .We can get the membership degree matrix R is:

$$R=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & & \vdots \\ r_{ni} & r_{n2} & \cdots & r_{nm} \end{bmatrix} \tag{13}$$

e) The fist level of fuzzy evaluation evaluation: According to the basic factors,we evaluate the levels and set the results as $D_i: D_i=B_i*R_i=[d_{i1},d_{i2},\cdots,d_{in}]$, use average weight.

$$d_{ij}=\sum(b_i\times r_{ij}) \tag{14}$$

f) Multi-level fuzzy comprehensive evaluation: Based on the fist level of fuzzy evaluation evaluation D_i, we use the fuzzy mapping f to determine the next level on the weight of a layer of evaluation factors B .Then we use the formula $D=B*R$ and get the final vector D ,and its value is between 0 and 1, can be taken as the nput of BPNN. In this paper, we take the two layers fuzzy evaluation.

IV. APPLICATION EXAMPLES

In this paper, we use three-layer fuzzy neural network. The number of hidden layer neurons is in the range of 3-13.We take eleven as the number of hidden layer neurons through experiments and one as the number of output layer neurons. The Sigmoid transfer function is taken as function in hidden layer and the type of purelin transfer function is taken as function in output layer.

According to Protection standards, we analysis the information system security from five aspects, such as environmental, network, application, system and management safety, each of which can be divided into various aspects, for example, environmental safety can be divided into physical access control, anti-sabotage , location selection and power supply. From the analysis we make 25 input Volumes. We use 25 group of input and output characteristic quantities as the sample of fuzzy neural network learning which are taken from a small company information systems evaluation results. 15 groups are used as a training sample of training, and 10 groups are used to test the network generalization ability. This experiment is under MATLAB environment and used neural network toolbox.

TABLE I. EVALUATING RESULT AND TRAINING RESULTS

Evaluating result by experts			**Training results by FNN**		
1	2	3	1	2	3
0. 8788	0. 7569	0. 6954	0. 8988	0. 7206	0. 6803
4	5	6	4	5	6
0. 6541	0. 6048	0. 5736	0. 6659	0. 6207	0. 5698
7	8	9	7	8	9
0. 4821	0. 3795	0. 3491	0. 4796	0. 3718	0. 3691
10	11	12	10	11	12
0. 3018	0. 2973	0. 2854	0. 3301	0. 2934	0. 2902
13	14	15	13	14	15
0. 2247	0. 1084	0. 0983	0. 2247	0. 2289	0. 0956

TABLE II. EVALUATING RESULT AND SIMULATION RESULTS

Evaluating result by experts			**Simulation results by FNN**		
1	2	3	1	2	3
0. 7534	0. 6899	0. 5931	0. 7610	0. 6813	0. 5816
4	5	6	4	5	6
0. 4259	0. 3918	0. 3677	0. 4210	0. 3977	0. 3602
7	8	9	7	8	9
0. 2986	0. 2418	0. 1977	0. 2948	0. 2440	0. 1993
10			10		
0. 1066			0. 1003		

The network error precision function we setup is 10^{-4}. We can know the error precision is less than the set up value after the network right has been iterated for 306 times. The contrast between the evaluating results by experts and the simulation results are shown in Figure.4, from which we can conclude that fitting results are satisfactory, and the network has a strong self-adaptive ability.

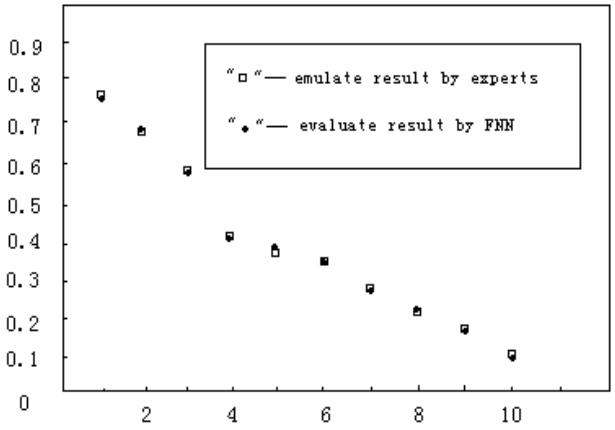

Figure 4. Contrast between the evaluating results and simulation results

V. CONCLUSION

In this paper, we propose a risk assessment model based on classified security protection, which is combined fuzzy theory and BP neural network, so that the impact of uncertain elements and man-made factors can be reduced, and the learn capability and the expression capability can be improved. Further more, the division of risk factors based on level protection standard makes the level protection and risk evaluation combined closely. We use the output of multi-level fuzzy system as the input of BP neural network, and the simulation results show that the risk evaluation method based on the fuzzy BP neural net work can provide a credible algorithm for the risk assessment of information security. This risk evaluation model can analyze the information security independently and estimate risk level real-timely.

REFERENCES

[1] Zhang Jun. Build Backup and Recovery System Based on National_level Protection Standards [J]. Southern China Financial Computer 1-3,2009,1 (1) :1-3.

[2] Xu Chaohan. Computer Information Security Management [M]. Electronics Industry Press,2006,04, first edition.

[3] GB17859. Classification Criteria of Computer Information Systems security [S] .1999.

[4] GB/T 20984-2007.(2007). "Information security technology: risk assessment norm of information system", National Criteria of CHINA.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] Zheng Chengxing.Theory and Practice of Network intrusion Prevention [M]. Mechanical Engineering Press, 2006,09.

[6] Dong-Mei Zhao, Jin-Xing Liu, Ze-Hong Zhang.Method of Risk Evaluation of Information Security .