Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(6):1020-1026

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Study on prediction of network security situation based on fuzzy neutral network

[1]Wang Yong and [2]Hu Yitao

[1]Information Management Department, Xuzhou College of Industrial Technology, Xuzhou, China
[2]Nanjing Agricultural University Library, Nanjing, China

ABSTRACT

Network security problem has been concerned in recent years, the prediction of network security situation can ensure the safety of network, and therefore the application of fuzzy neutral network on it is studied in depth. First, the frame of predicting system of network security situation is designed; Second, the basic theory of fuzzy neutral network is analyzed; then prediction model of network security situation are established. Finally, the simulation is carried out, and results show that the fuzzy neutral can predict the network security situation correctly.

Key words: Prediction; network security situation; fuzzy neutral network

Openness, sharing and interconnection degree of network is widening, and all kinds of Network security events are piling up, and network security has become increasingly important, which focuses more and more attention. The traditional, single defense equipment or detection equipment has been not suitable for the demand of ensuring the safe operation of network system. It is necessary to evaluate and predict the network security situation accurately and objectively, the prediction of network security has become the research focus in network security field. The prediction of network security situation can make network security management transform from passivity into initiative. The network manager can judge the trend of state of network safety, then the state of network and attack for network can be understand. The network manager can take effective defensive measures to ensure the safety of network before the network is attacked and suffered to loss [1]. The safety situation of network is affected by several factors, such as attacks, viruses, vulnerabilities and trojan horse, the traditional predicting method only reflect partial information and can not obtain the correct predicting results, the changes of network security situation has time variation, probability and nonlinearity, therefore the effective predicting method should be put forward.

In recent years, the artificial intelligence has developed widely, and there are many ways for predicting the network safety situation such as support vector machine, Markov chain, and the good predicting effect is obtained. However, the current predicting methods have limits, for support vector machine, the parametric selection lacks appropriate theoretical guidance, the parameters obtained are so subjective and blind, when the sample is too much, the training speed will decrease. Markov chain has difficulty in constructing precise predicting model, which need to draw up the mathematical formulae largely, it is very complex. In order to overcome the disadvantages of the current predicting methods, the fuzzy neutral network is applied in the prediction of network security situation. The fuzzy neutral network has the advantage of quick tracking speed, which can obtain higher predicting precision, and it can be used to deal with the nonlinear problems. Then the prediction algorithm of network security situation based on fuzzy neutral network is established [2,3].

1 Frame of predicting system of network security situation

The prediction of network security situation is to use the relationship among time series to predict the value of network security situation. The calculation of value and the evaluation of network security situation makes up of the whole network security situation technique. The value of network security situation can produce the threat information for the network manager, and the manager can refer the evaluation results of network security situation, and confirm the possible threat, finally the manager can find a proper method to deal with the threat [4].

The evaluation of network security situation is the qualitative analysis based on evaluating the working state of network. The aim of the evaluation is to help the decider to percept the security situation quickly and correctly. The evaluation of security situation concludes three stages: situation perception, situation understanding and situation prediction. The frame of prediction of network security situation based on fuzzy neutral network is shown in figure 1.

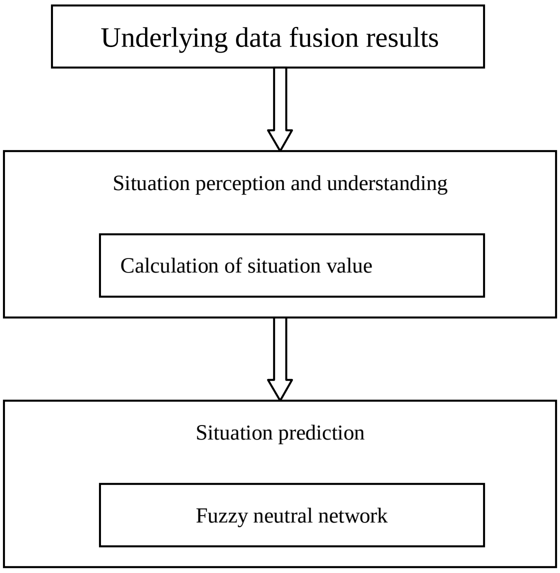
Underlying data fusion results
Situation perception and understanding
Calculation of situation value
Situation prediction
Fuzzy neutral network

Figure 1 prediction frame of network security situation based on fuzzy neutral network

The value of network security situation is a set of or several sets of values merged by huge network security information based on a series of mathematical methods [5,6]. The value can reflect the running character of network. The value can change with the changes of frequencies, number of network security events. The value of network security situation can be calculated based on figure 2.

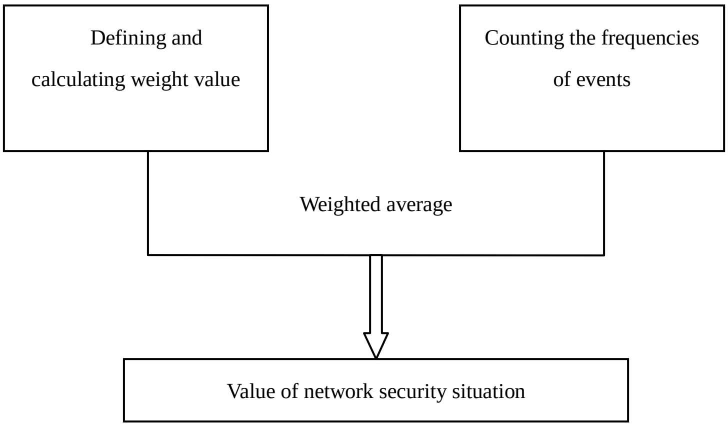
Defining and calculating weight value
Counting the frequencies of events
Weighted average
Value of network security situation

Figure 2 Calculation method of network security situation value

2 Basic theory of fuzzy neutral network

There are five layers for fuzzy neutral network, which are inputting layer, fuzzy layer, fuzzy association layer, association layer after fuzzy, and outputting layer, the corresponding diagram is shown in figure 3 [7].

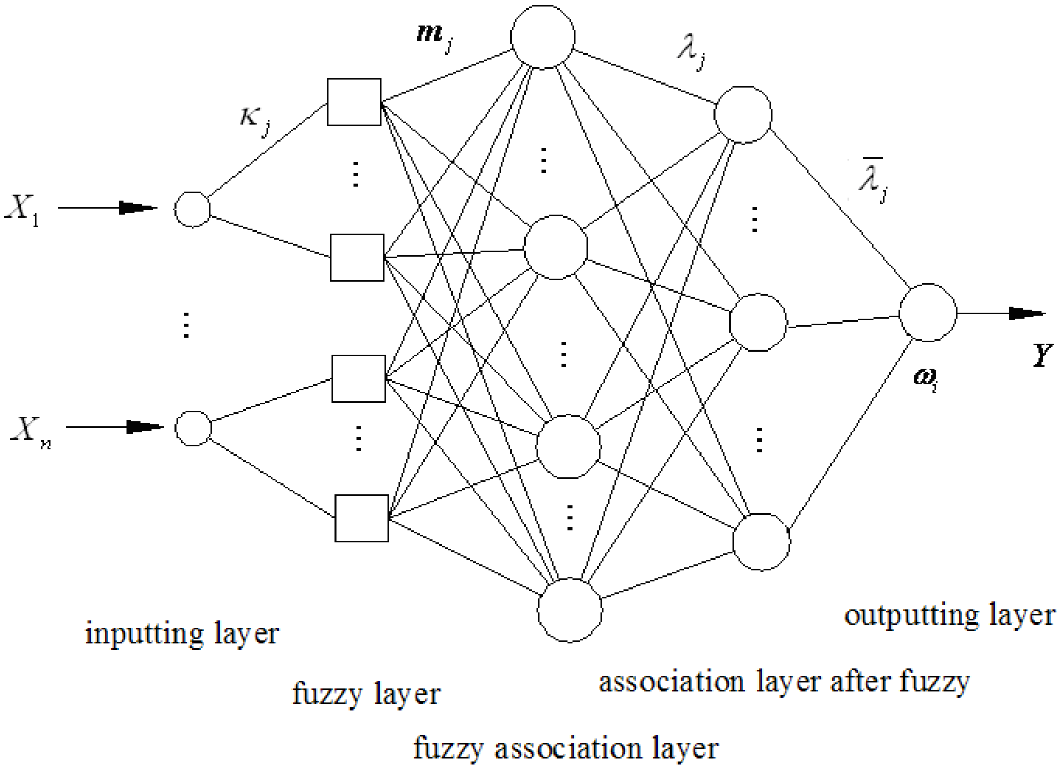

Figure 3 Diagram of fuzzy neutral network

Inputting layer: the function of inputting layer is to introduce the inputting variable into fuzzy layer, and the corresponding inputting variable vector is expressed as follows::

$$X = [x_1, x_2, \cdots, x_n]^T \tag{1}$$

The membership model of inputting vector can be expressed as follows [8]:

$$\kappa_j(x) = \phi_j\left(\frac{\|x - c_{ij}\|}{\sigma_{ij}}\right) = e^{-\frac{\|x-c_{ij}\|^2}{\sigma_{ij}^2}}, \quad j = 1,2,\cdots,\sum_{i=1}^{n} N_i \tag{2}$$

where, c_{ij} is the center of membership model, σ_{ij} is the width of membership, N_i is the dimension of i th inputting vector.

Fuzzy layer: different joint of fuzzy layer can be denoted by a language variable, which can calculate the membership degree of inputting vector, and the calculating formula of membership degree is expressed as follows:

$$m_j = e^{\frac{x-c_{ij}}{\sigma_{ij}^2}}, \quad j = 1,2,\cdots,\sum_{i=1}^{n} N_i \tag{3}$$

Fuzzy association layer: the fuzzy sum is carried out for the inputting variable in fuzzy layer, and the fuzzy association vector can be obtained, the corresponding mathematical model is expressed as follows:

$$\lambda_j = \min\{m_1, m_2, \cdots, m_k\}, \quad j = 1,2,\cdots,N_A, \quad k = 1,2,\cdots,N_n \tag{4}$$

where, $N_A = \prod_{i=1}^{n} N_i$.

Association layer after fuzzy：the association layer after fuzzy is to calculate the normalized results of association vector, and the calculating formula can be expressed as follows [9]:

$$\overline{\lambda_j} = \frac{\beta_j}{\sum_{i=1}^{N_A} \beta_i}, \quad j = 1,2,\cdots,N_A \tag{5}$$

$$\sum_{i=1}^{N_A} \overline{\lambda_j} = 1 \tag{6}$$

Outputting layer: the outputting layer is to carry out linear weighted sum of association strength normalized, and the corresponding mathematical model is listed as follows:

$$Y = \sum_{i=1}^{N_A} \omega_i \overline{\alpha}_i = \omega^T \Phi \tag{7}$$

where ω_i denotes the association weight between two elements, ω denotes association vector between two elements, $\omega = [\omega_1, \omega_2, \cdots, \omega_{N_A}]^T$, $\Phi = [\overline{\alpha_1}, \overline{\alpha_2}, \cdots, \overline{\alpha_{N_A}}]^T$.

3 Theory model of network security situation

Define the time series of network security situation as $X = \{x(t) \mid t = 1,2,\cdots,n\}$, and the sample space S can be expressed as follows:

$$\{X(t), Y(t)\} = \{[x(t-\tau), x(t-2\tau), \cdots x(t-d\tau)], [x(t)]\} \tag{8}$$

where $t = n, n-\tau, n-2\tau, \cdots, (d+1)\tau$, τ is time lag, d is embedding dimension, $X(t)$ is inputting sample of predicting model, $Y(t)$ is the object value of predicting model, and the number of sample in sample space is $n-(d-1)\tau$.

The prediction value is affected by the adjacent time series point during the procession of predicting the network security situation. Then the proper training samples that is close to predicting points chosen can improve the predicting precision. Assume that there are l samples in the space S, the length of sample window is defined by w, then when $Y(t)$ is predicted, the w samples before t are chosen to construct the predicting model $f: R^d \to R$, then the predicting model is used to predict $Y(t)$, the mapping relationship between the predicting value $\hat{Y}(t)$ and predicting model is expressed as follows:

$$\hat{Y}(t) = f(x(t-\tau), x(t-2\tau), \cdots x(t-d\tau)) \tag{9}$$

4 Prediction algorithm of network security situation

Predicting the network security situation based on fuzzy neutral network should solve the following problems: if the fuzzy segmentation of imputing vector is given in advance, the linking weight value ω_i between two elements, the membership degree model parameter c_{ij} and σ_{ij} should be trained. In order to reduce the training time of fuzzy neutral network, and improve the calculating efficiency, the intelligent algorithm is applied to training the parameters mentioned above, the genetic algorithm is used in this research, the main reason is that the genetic algorithm is an advanced optimum algorithm, which is put forward based on evolution rules of living things, it can reflect the optimum idea of “natural selection” and “survival of the fittest”, which can calculate the linking weight between two elements and relevant parameters of membership model, then the best prediction results of network security situation can be obtained, the analyzing procedure of prediction of network security situation based on fuzzy neutral network is listed as follows:

Step 1：construct the structure of fuzzy neutral network, and confirm the number of neutral elements for every layer according to the remand of prediction of network security situation.

Step 2：the value scope of parameter in fuzzy neutral network changes from 0 to 1, then the normalization calculation is carried out for the training data in fuzzy neutral network, and the corresponding normalization formula is expressed as follows:

$$f(x) = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \qquad (10)$$

where, x is the original data, $f(x)$ is the normalization function.

Step 3：the calculation procession can be simplified through direct real number encoding；When coding, the center and width of every membership model can be sorted by size. During the intersection, the probability that the center and width of membership for different individual change at the same time will improve, and the efficiency of genetic operation ban be improved.

Step 4: Calculate the fitness of individual, and the calculation formula of fitness d_{fit} is expressed as follows:

$$d_{fit} = \frac{n}{\sum_{i=1}^{n}(d_i - Y_i)^2} \qquad (11)$$

where, d_i is the rational output, and y_i is the output of fuzzy neutral network.

Step 5：the optimum individual obtained in this calculation before interacting operation can be transmitted into next generation, the algorithm can be avoid to Fall into the local optimal solution, the interacting operation and mutation operation can be carried out for other individuals according to the interacting probability and mutation probability, then the new individual can be formed.

Step 6：the fuzzy neutral network trained can be applied in the predicting the network security situation

5 Simulation on prediction of network security situation

In order to verify the effectiveness and rationality of fuzzy neutral network based on genetic algorithm, the simulation on the prediction of network security situation is carried out, the data comes from data set of hacker attack collected by Honeynet group. And the simulation program is compiled by MATLAB software.

The parameters of predicting model are listed as follows: the dimension of inputting vector is 4, the four days are used as a cycle; the dimension of output vector is 1, the situation value of one day can be predicted; the number of training samples are chosen as 84, which are data in fourteen weeks. In order to avoid the big error, the normalization processing is carried out for the situation value, the corresponding formula is expressed as follows:

$$\hat{x} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \qquad (12)$$

where $x_{\max}$ is the maximum value of situation value, $x_{\min}$ is the minimum value of situation value, $\hat{x}$ is the normalization value, x is the current situation value. The final results of situation value in the simulation are shown in figure 4.

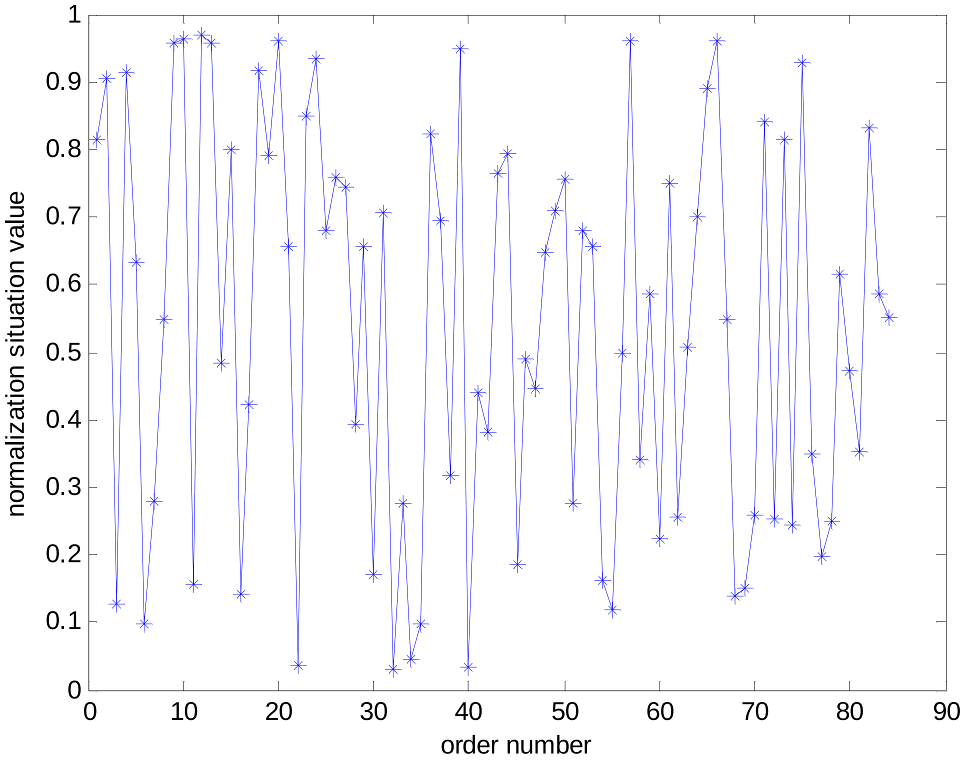

Figure 4 final results of situation value in the simulation

The maximum iteration times are taken as 250, the number of individuals in group is taken as 150, and the interacting probability is 0.75, and the mutation probability is 0.35. The trained fuzzy neutral is used to predict the situation value from Jan. 6 to Jan. 12, 2014, and the predicting results are shown in figure 5.

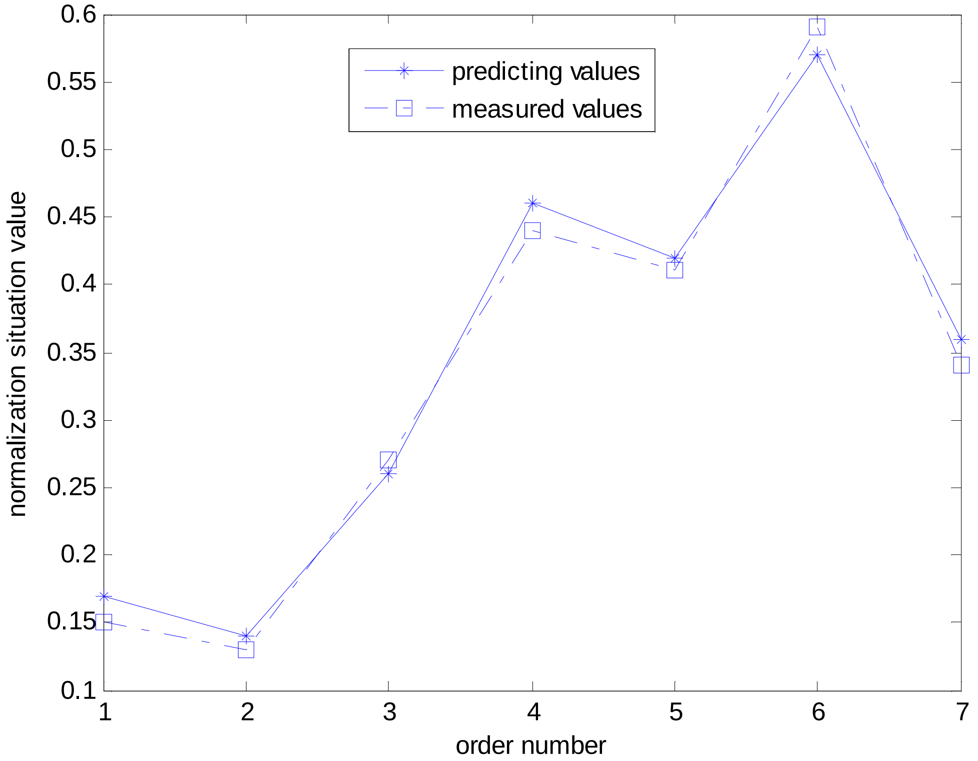

Figure 5 Predicting results of network security situation value based on fuzzy neutral network

As seen from figure 5, the fuzzy neutral network has better predicting precision in predicting the network security situation value, the changing rules of situation value are shown in figure 5, and the measured value is basically in agreement with prediction value.

According to the changing trends of situation value, the network manager can judge the probability of attack, then the manager can take measurement to avoid the attack and protect the network security.

CONCLUSION

According to the disadvantages of current predicting method of network security situation, the fuzzy neutral network with genetic algorithm is applied in the predicting the security situation of network. The fuzzy neutral network has ability in dealing with the nonlinear problems. Simulation is carried out, and results show that the fuzzy neutral network can obtain better reliable predicting results, which can reflect the security state of network.

REFERENCES

[1] Yaxing Zhang, Shuyuan Jin, Xiang Cui, et al. *Communications in Computer and Information Science* Volume 320, **2013**, pp 659-665.
[2] Boyun Zhang, Zhigang Chen, Xiai Yan, et al. *Lecture Notes in Computer Science*, Volume 6838, **2012**, pp 509-516
[3] Baoqin Cai. *Lecture Notes in Electrical Engineering,* Volume 273, **2014**, pp 619-626
[4] Jin Yang, Cilin Wang, Le Yu, et al. *Communications in Computer and Information Science,* Volume 308, **2012**, pp 488-495
[5] Zhang Ruirui, Li Tao, Xiao Xin, et al. *Communications in Computer and Information Science*, Volume 234, **2011**, pp 212-218
[6] Zeng Bin, Zhong Ping. *Computer Simulation*, **2012**, 29(5): 170-173 (In Chinese).
[7] Pei-Chann Chang, Chin-Yuan Fan, Jyun-Jie Lin. *International Journal of Electrical Power & Energy Systems*, Volume 33, Issue 1, **2011**, Pages 17–27
[8] Yüksel Özbay, Rahime Ceylan, Bekir Karlik. *Expert Systems with Applications,* Volume 38, Issue 1, **2011**, Pages 1004–1010.
[9] Long Xu, Junping Wang, Quanshi Chen. *Energy Conversion and Management,* Volume 53, Issue 1, **2012**, Pages 33–39