International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.317-324
http://dx.doi.org/10.14257/ijsia.2016.10.11.26

Research on Optimal Attack and Defense Decision of Network Security Based on Fuzzy Neural Network

Ye Ru-jun

Zhejiang Business College
yerujun1972@163.com

Abstract

In order to improve the safe level of network security, the fuzzy neutral network is applied in optimal attack and defense decision. Firstly, the theory model of attack and defense decision system for network security based on game theory is constructed, the game model of attack and defense model and the dynamical game model of incomplete information are deduced respectively. Secondly, the basic theory of fuzzy neutral network is analyzed, the framework of diagram of fuzzy neutral network is confirmed, and the model of fuzzy membership function is constructed.. Thirdly, the training algorithm of fuzzy neutral network based on improved genetic algorithm is designed, and computing method in every step is given in detail. And the Evaluation of suspicious person and system is carried out. Finally, simulation experiments are carried out, and results show that system profit and response efficiency is improved, then fuzzy neutral network can obtain higher system profit and response efficiency.

Keywords*: fuzzy neutral network; network security; attack and defense decision*

1. Introduction

Currently the network attack technology has developed in the direction of diversified, collaborative and intelligent, and combined penetration attack with multi-step has threatened the safety of network. In order to ensure the safety and robustness, the attack and defense of network has become the research hotspots, the conventional attack and defense of network does not consider the cost of attack and defense, and cannot find out a balance between investment and profit, therefore the final decision is not optimal. In recent years, the attack events happen frequently, and the attack aim has changed from showing off technology to economic interest driving, and has formed a underground economy industrial chain with organization, scale and openness. Specifically, the network attack concludes Trojan horse manufacturing, Trojan communication, theft of account information, money laundering. With technology development of network attack technology, the cost is decreasing, while the network defense is increasing. The attack on network information safety not only affects the network itself, but also brings out the serious consequence, then the Economic security, military security, cultural security, political security of country will be endangered.

In recent years, all kinds of counter defense technologies in the light of all kinds of network attack has been put forward, such as firewall, intrusion detection, anti-virus software, and intrusion forensics. However, the traditional defense technology is static and one-sided passive technology and the defense lags behind the attack, and it is in the passive situation. This delayed reaction will cause the serious losses. Therefore, it is necessary to design a new technology, which can analyze and predict the strength, objective, damage and attack type and aim before the network is attacked, then the passive defense can be changed to active defense. The active defense system aims to judge the security situation of network through situation awareness, risk evaluation and safe inspection and other means, and then the active defense system of network safety can

ISSN: 1738-9976 IJSIA

be constructed according to the judging results. Currently the stochastic game was used to describe and deduce for attack and defense system, and the aim and strategy of attacker can be described based on attack Figure, the income, preference and strategy of attacker and system can be processed effectively, however the uncertainty is not considered, in order to improve the performance of defense system for network security, the fuzzy neutral network is applied in optimal attack and defense decision of network security.

2. Theory Model of Attack and Defense Decision System for Network Security

(1) Game activity of attack and defense decision system

The counter game refers to the decision activity of decision maker, which is the non-cooperative game, and the basic principle of counter decision is lest loss and biggest profit, and the activity plans can be made based on this principle, generally the one side can not grasp the activity and intension of other side in the counter system, the counter strategy generally is chosen based on game theory, the counter game more emphasizes the importance of time and information, time and information are considered as the main factors of affecting game results. In game process, the information awareness and evaluation of two sides in game can decide the activity space. At same time, the activity sequence can affect the game results directly during the procession of game, the optimal strategy should be found out in real time, the whole game is the process of choosing the strategy by different interest subjects based on information symmetry [1].

(2) The game model of attack and defense model of network security

The game model is expressed as follows [2]:

$$(T, W^1, W^2, U, P^1, P^2, \lambda) \tag{1}$$

where T is the status collection, $T = \{t_1, t_2, \cdots, t_N\}$; $W^k = \{w_1^k, L, w_{M^k}^k\}$, $k = 1,2$, M^k is the strategy collection for person k in the system, $M^k = \{W^k\}$; the strategy collection of person k is the sub collection W^k, that is $W_s^k \subseteq W^k$, $\bigcup_{i=1}^{N} W_{s_i}^k \subseteq W^k$.

U is the status transformation function: $T \times W^1 \times W^2 \times T \to [0,1]$;

P^k is the profit function of person k in the system: $T \times W^1 \times W^2 \times T \to \hbar$, $k = 1,2$;

λ is the discount rate, $0 < \lambda \le 1$, the income value of next status is λ times than that of current status. If the value of λ is big, the person in the system more concerns the further, if the value of λ is small, the person in the system more pays attention to the current status.

There are two game sides in the system, the suspicious person can be considered as person1, and the system can be considered as person2. At moment, this model is in the status $t_t \in T$, the suspicious person chooses $w_t^1 \in A^1$ from its strategy collection, and the system chooses $w_t^2 \in A^2$, and then the suspicious person can get a profit $p_t^1 = P^1(t_t, p_t^1, p_t^2)$, and the system can get a profit $p_t^2 = P^2(t_t, p_t^1, p_t^2)$. In this model, the two sides also play an important role.

The type of suspicious person is defined by $\sigma^1 \in \Omega^1$, and the type of system is defined by $\sigma^2 \in \Omega^2$, where Ω^1 and Ω^2 are type spaces of suspicious person and system. In this status, the profit of suspicious person can be expressed as follows [3]:

$$p_t^1 = P^1(t_t, w_t^1, w_t^2, \sigma^1) \tag{2}$$

The profit of system is expressed as follows:

$$p_t^2 = P^2(t_t, w_t^1, w_t^2, \sigma^2) \tag{3}$$

The type of system can not be grasped completely, therefore the original belief $b_2(\sigma^1)$ is given, the suspicious person can also not grasp the type of system completely, then another belief is defined as $b_1(\sigma^2)$, the types of system conclude "can attack" and "can not attack", and the types of suspicious person conclude "Hackers" and "ordinary users", and the dynamical game of incomplete information is corresponding to perfect Bayesian Nash equilibrium, then following expressions can be obtained [4]:

$$w^2 * (w^1, \sigma^2) \in \arg\max_{w^2} \sum_{\sigma^1} p_2^{'}(\sigma^1 \mid w^1) P^2(T_2, w^1, w^2, \sigma_2) \tag{4}$$

$$w^1 * (w^2, \sigma^1) \in \arg\max_{w^1} \sum_{\sigma^{21}} p_2^{'}(\sigma^2) P^1(T_2, w^1, w^2, \sigma_1) \tag{5}$$

where the posterior probability $p_2^{'}(\sigma^1 \mid w^1)$ is obtained based on Bayesian rules through $p_2(\sigma^2)$, which shows that the system can confirm the type of customer based on activity of suspicious element. The type belief of system $p_1(\sigma^2)$ can be confirmed based on the information collected by suspicious element. The type can be evaluated based on fuzzy neutral network.

3. Basic Theory of Fuzzy Neutral Network

The fuzzy neutral network has many advantages, such as good knowledge expression level and fault tolerance ability, it also has good knowledge storing ability. The fuzzy neutral network can be used to evaluate the type of suspicious person and system, different fuzzy membership function can be used to describe the different status of suspicious person and system, the neuron can and the connection weight can distribution the status distribution of suspicious person and system, and the effective training algorithm can be used to train the fuzzy neutral network, and the relating knowledge can be obtained finally, and the numerical simulation method can be applied in reasoning of type, then the correct knowledge can be obtained, which is benefit for knowledge storage, then the evaluation correct of type for person and system, and the optimal attack and defense decision of network security can be obtained finally [5].

The basic framework of fuzzy neutral network is shown in figure 1. The inputting layer can input language, which is the first layer. The membership degree function is in the second layer, which can obtain the fuzzy sub set membership degree of different inputting variables, it can express importance of attack and defense decision of network security, then the optimal decision can be obtained, therefore a class of conventional fuzzy membership degree function can applied in confirming the optimal attack and defense decision of network security, then the too small, the best, too large attack and defense decision parameters can be obtained, which are input into the fuzzy neutral network in the form of inputting parameters.

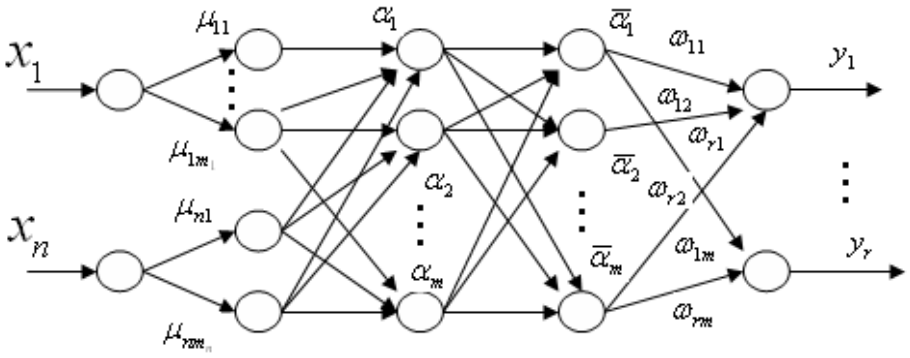

Figure 1. Framework Diagram of Fuzzy Neutral Network

The mathematical model of fuzzy membership degree function is expressed as follows [6]:

(1) If the sign parameters are relative small, the mathematical model of membership degree is expressed as follows:

$$\mu_L = \begin{cases} 1 & \Delta x < \Delta x_{\min} \\ \dfrac{\Delta x_0 - \Delta x}{\Delta x_0 - \Delta x_{\min}} & \Delta x_{\min} < \Delta x < \Delta x_0 \end{cases} \tag{6}$$

(2) If the sign parameters are good, the mathematical model of membership function is expressed as follows:

$$\mu_L = \begin{cases} \dfrac{\Delta x - \Delta x_{\min}}{\Delta x_0 - \Delta x_{\min}} & \Delta x_{\min} < \Delta x < \Delta x_0 \\ \dfrac{\Delta x - \Delta x_{\max}}{\Delta x_0 - \Delta x_{\max}} & \Delta x_0 < \Delta x < \Delta x_{\max} \\ 0 & \text{其他} \end{cases} \tag{7}$$

（3）If the sign parameters are relative high, the mathematical model of membership degree is expressed as follows:

$$\mu_L = \begin{cases} \dfrac{\Delta x - \Delta x_0}{\Delta x_{\max} - \Delta x_0} & \Delta x_0 < \Delta x < \Delta x_{\max} \\ 1 & \Delta x > \Delta x_{\max} \\ 0 & \text{其他} \end{cases} \tag{8}$$

where $\Delta x_{\max}$ is the maximum value of positive offset of attack and defense decision parameters, $\Delta x_{\min}$ is the minimum value of negative offset of attack and defense decision parameters, Δx_0 is the optimal offset of attack and defense decision parameters. Generally, $\Delta x_0 = 0$.

The third layer of fuzzy neutral network is deducing layer, which mainly is corresponding to fuzzy rules, and then the fitness of different fuzzy rules can be obtained.

The fourth layer has same number of nodes with the third layer, which is benefit for normalization. The output layer of fuzzy neutral network is fifth layer; the computing precision of outputting layer is very high. The arrow between two neutrons can be used to denote the transmitting direction of signal of fuzzy neutral network, the relationship between the inputting and outputting can be expressed as follows:

$$y = \frac{\sum_{i=1}^{m}\left(\prod_{i=1}^{m}\mu_j^i(x_j)\right)y^i}{\sum_{i=1}^{m}\left(\prod_{i=1}^{m}\mu_j^i(x_j)\right)} \tag{9}$$

4. Training Algorithm of Fuzzy Neutral Network Based On Improved Genetic Algorithm

According to real situation of attack and defense decision of network security, the improved genetic algorithm is applied in optimization of parameters of fuzzy neutral network, the chaos optimization is introduced into the genetic algorithm, and the original population can be expressed by chaos sequence, the searching precision can be regulated in real time according to genetic procedure of population in optimization of parameters, then searching precision can be improved effectively [7].

The training procedure of fuzzy neutral network is listed as follows [8]:

Step 1: the scale of population is defined by N, and the maximum iteration number is defined by $I_{\max}$, and the controlling parameters of chaos optimization are defined by β and ψ respectively.

Step 2: the initialization operation is carried out for evolution iteration, let $I = 0$, and the initialization operation is carried out for chaos population, which is defined by H_g, according to Logistic mapping principle, the corresponding optimal model is expressed as follows:

$$\phi_{i,j} = \lambda\phi_{i,j}^0(1-\phi_{i,j}^0) \tag{10}$$

where $\phi_{i,j}$ is the chaos vector, $\phi_{i,j}^0$ is the original value, $i = 1,2,\cdots N-1$, $j = 1,2,\cdots,m$, m is the number of decision vector. The chaos variable is transferred to decision variable, and the corresponding interval is defined as $(x_{j\min}, x_{j\max})$, and the model is expressed as follows:

$$x_{i,j} = x_{j\min} + (x_{j\max} - x_{j\min})\phi_{i,j} \tag{11}$$

Step 3: the non-dominated sorting method is used to process the population H_g, and the non-dominated level can express the fitness corresponding to different solution, and then the choose, interaction, and mutation operation can be used to obtain the next generation population S_g.

Step 4: the intersection of last and next population is taken, and the expression is defined as $C_g = H_g \bigcup S_g$. The front surface of the synthetic population C_g can be

obtained through non dominated sorting method, and the expression is defined by $U=(U_1,U_2,\cdots)$.

Step 5: the crowding distance of non-dominated front surface is calculated, and the interaction is taken, and the expression is defined as $H_{g+1}=H_{g+1}\bigcup U_i$, $i=i+1$, and the end iteration condition is $|H_{i+1}|+|U_i|\leq N$. The $(N-|H_{g+1}|)$ optimal solutions can be obtained.

Step 6: judge the evolution population whether is in the best status, if the individual number that the non inferiority is equal to 1 in population is agree with scale of population, top 15% of next generation population is searched based on chaos thinning method, and the search space is $(x'_{j\min},x'_{j\max})$, which is solve by the following expression:

$$\begin{cases} x'_{j\min}=x^*_{i,j}-\eta(x_{j\max}-x_{j\min}) \\ x'_{j\max}=x^*_{i,j}+\eta(x_{j\max}-x_{j\min}) \end{cases} \quad (12)$$

where η is searching factor.

If $x'_{j\min}<x_{j\min}$, then $x'_{j\min}=x_{j\min}$; if $x'_{j\max}>x_{j\max}$, then $x'_{j\max}=x_{j\max}$.

The new chaos variable $x'_{i,j}$ can be calculated based on the following expression:

$$x''_{i,j}=(1-\gamma)x'_{i,j}+\gamma x_{i,j} \quad (13)$$

where γ is the self suitable factor.

Repeat step 3-step 5, if the maximum interaction times are satisfied, goes into next step.

Step 7: if the maximum evolution times $I_{\max}$ is obtained, the optimal solution is output, and the calculation is over.

5. Evaluation of Suspicious Person and System

The game type can be evaluated by fuzzy neutral network, the suspicious person can consider the following aspects: system vulnerability severity, risk of open ports, security of architecture, rigor of personnel and system management, simple degree of password and system investment level. And the four activities of suspicious person should be mainly observed, which conclude entering the wrong password, threat of user access, a large number of abnormal data packets and scan port, and the activity analysis table of suspicious person is listed in Table 1.

Table 1. Activity Analysis Table of Suspicious Person

Serial number	entering the wrong password	threat of user access	a large number of abnormal data packets	scan port frequently	Probability of Hacker
1	0.92	0.81	0.86	0.86	0.91
2	0.82	0.71	0.79	0.81	0.82
3	0.74	0.68	0.77	0.82	0.78
4	0.76	0.68	0.72	0.75	0.76

5	0.65	0.53	0.64	0.72	0.65
6	0.42	0.45	0.66	0.61	0.54
7	0.39	0.34	0.46	0.33	0.36
8	0.23	0.21	0.45	0.27	0.26

The bigger the value of the four activities of suspicious person is, the higher the probability that the network is attacked by Hacker.

6. Simulation Analysis of Optimal Attack and Defense Decision of Network Security

The response efficiency is used in the simulation, which is calculated by the following expression:

$$E_L = 1 - \frac{L_r}{L_m} \tag{14}$$

where L_r is the residual losses brought by intrusion, L_m is the total loss by attack.

Three simulation experiments are carried out, and the three attack strategies are used, in order to verify the effectiveness of this new method, the traditional game model is also used, and the responses results are obtained which are listed in Table 2.

Table 2. Response Results for Three Attack Strategies

Attack strategy		Strategy 1	Strategy 2	Strategy 3
System profit	Traditional game model	421	275	318
	New game model	621	564	573
Response efficiency	Traditional game model	42.3	45.7	42.5
	New game model	55.2	76.9	69.2
Response time	Traditional game model	556	1368	896
	New game model	227	379	371

As seen from Table 2, the new game model based on fuzzy neutral network is better than the traditional game model, and the system profit and response efficiency are higher from the new game model is higher than traditional game model, and the response of new game model is also small, the response speed is higher. Results showed that the response speed and processing ability of optimal attack and defense decision are improved.

7. Conclusions

With the popularization and simplicity of intrusion technique, the disadvantage of static passive defense has become obvious, and the positive defense strategy has been concerned, in order to consider the uncertainty in attack and defense decision, the fuzzy neutral network is introduced in optimal decision for network security, and the algorithm procedure is designed, Three simulation experiments are carried out, and the three attack strategies are used, Comparison of response results between the new game model and traditional game model is carried out, simulation results show that the fuzzy neutral network has higher system profit and response, which can be applied in actual engineering, and the network security can be ensured.

References

[1] Liu Gang, Zhang Hong, Li Qianmu, Network security optimal attack and defense decision-making method based on game model, Journal of Nanjing University of Science and Technology, 38, 1**(2014)**
[2] Ma C.Y.T., Yau D.K.Y., Xin Lou, Rao N.S.V., Markov game analysis for attack-defense of power networks under possible misinformation, IEEE Transactions on Power Systems, 28, 2**(2013)**
[3] Garnaev A., Baykal-Gursoy M., Poor H.V.,Incorporating Attack-Type Uncertainty into Network Protection, IEEE Transactions on Information Forensics and Security, 9, 8**(2014)**
[4] Ma Chris Y. T., Yau David K. Y., Lou Xin, Rao Nageswara S. V., Markov game analysis for attack-defense of power networks under possible misinformation, IEEE Transactions on Power Systems, 28, 2**(2013)**
[5] Jagadeesh Kadali, Prasad Dasari, Ramesh P., 3-phase 4-wire UPQC topology with reduced DC-link voltage rating for power quality improvement using fuzzy controller, International Journal of Signal Processing, Image Processing and Pattern Recognition, 9, 1**(2015)**
[6] Gaikar Dipak Damodar, Marakarkandy Bijith, Dasgupta Chandan, Using twitter data to predict the performance of bollywood movies, Industrial Management and Data Systems, 115, 9**(2015)**
[7] Bhoskar T., Kulkarni O.K., Kulkarni N.K., Patekar S.L., Kakandikar G.M., Nandedkar V.M., Genetic algorithm and its applications to mechanical engineering: a review, Materials Today: Proceedings, 2, 4**(2015)**
[8] Nizam A., Ravi J., Subburaya K., Cyclic genetic algorithm for multiple sequence alignment, International Journal of Research and Reviews in Electrical and Computer Engineering, 1, 2**(2011)**

