Acta Technica *62* No. 2A/2017, 177–186

Network security audit system based on improved neural network

Ding Ding[1]

Abstract. With the rapid development of network technology, the network security has become the focus of the society. Therefore network security audit becomes an important way to protect the computer security. We present an network security audit model based on quantum genetic algorithm and BP neural network, which takes advantage of the global search property of the quantum genetic algorithm and the exact local search characteristics of the BP network. The weight and the thresholds of the BP neural network is optimized by the quantum genetic algorithm. As basic quantum genetic algorithm has week local search ability and is easy to premature, we also propose an improved quantum genetic algorithm. The experiments show that this method can be used to improve the efficiency and accuracy of network security audit system.

Key words. Network security audit, neural network, quantum genetic algorithm.

1. Introduction

With the rapid development of computer technology, microelectronics, communication technology and other kinds of sciences and technologies, especially the development of the Internet with its large amounts of information resources and rapid convenient efficient way to deliver information, the network has been an important tool in people's study and day-to-day life, but computer viruses, hackers, and any other uncertain dangerous problems have been threatening the security of the information on the network, testing people's wisdom to deal with the network danger and protecting the network security at the same time [1]. The network security audit plays an important role in the process of network security management, and it is also a function that the network environment security must support.

At present, the widely used characteristics detection method in security audit system is to define a series of characteristic patterns to identify intrusion by security experts in advance [2]. The problem of this approach is that if the model database is not timely updated, system cannot adaptively detect new attacks in the process of security audit, thus false alarm and alarm failure problem occur frequently. With the

[1]AnHui Audit College, Hefei, 230601, China

popularity of network applications, network data traffic has increased dramatically, some audit records itself contains a large number of irrelevant information. So, the problem of data overload and too low testing speed also appear.

In the process of the genetic algorithm applied to the security audit, it also has some drawbacks. The system can't detect multiple simultaneous attacks, and is unable to realize accurate positioning in the audit records, which makes the results of the detector do not include time information [3–5]. In network security audit based on agent technology, the monitor is the key component of the system. If a monitor stops working, all the repeater controlled by this monitor cannot submit results, and when more than one monitor reporting on the same issue, it may produce inconsistent and repetitive information. Network security audit based on the kernel technology collects data from the operating system kernel to be as basis to detect intrusion or abnormal behavior. This method is mainly used in open source Linux system, its advantage is that it has good detection efficiency and the reliability of data sources, but this method itself has a strong dependence on the safety of the operating system. Network security audit based on rule base is similar to some idea of firewall and anti-virus software, the testing accuracy of which is quite high, and can use the simplest matching method to filter out a lot of invalid audit data information, and is especially effective for to attack using a specific network tools [6]. But its shortcoming is that these rules only corresponds to known attack types or certain attack software. When there is a new attack software or software upgrade, omission of attack alarm is prone to occur, so safety audit method based on rule library has its own limitation. The largest problem based on the mathematical statistics method is how to set statistics threshold, and also is the cut-off point of normal and abnormal value, which often depends on the administrator's experience, and inevitably produce false alarm [7]. Neural network uses adaptive learning technology to extract the characteristics of the abnormal behavior, and obtain normal behavior pattern through training. The neural network dos not have stable network structure and its judgment of abnormal event will not provide any explanation or instruction information, this led to the users cannot confirm the invasion responsibility [8–10]. Introducing BP neural network into security audit system has certain practical significance, which open up new ways for the research of auditing system. Because of its many characteristics, such as adaptability, self-learning ability, in the security audit system based on neural network, we only need to provide the system audit data, then we can extract the characteristic pattern of system activity, without accessing to large amounts of data, thus it simplifies the design of the system. But BP algorithm has also obvious deficiencies. If the network structure and initial weights are not good, it not only makes its convergence speed slow, and may lead to network converge to local optimum. So the neural network is improved by quantum genetic algorithm [11, 12].

In the next section, a kind of network security audit system based on improved neural network is put forward. In section 3, in order to test the performance of network security audit system based on improved neural network, experiments are done. In the end, some conclusions are given.

2. Network security audit system based on improved neural network

Neural network has self-learning and adaptive ability. As long as the audit data or network packets of the system is provided, neural network can extract normal user or activity characteristics mode by self-learning, and detect the abnormal attack mode. These features make it get very good application in security audit detection. One of the most popular neural network learning algorithm is BP algorithm, but it has slow convergence speed and local optimal problem. The major task of the security audit based on neural network is efficiency and accuracy problem. Global search based on quantum genetic algorithm [13–14] and local accurate searching feature of BP thus can be an organically combined. We use quantum genetic algorithm optimization ability to optimize the BP network in audit research, and improve the effectiveness of the detection algorithm for unknown attack detection.

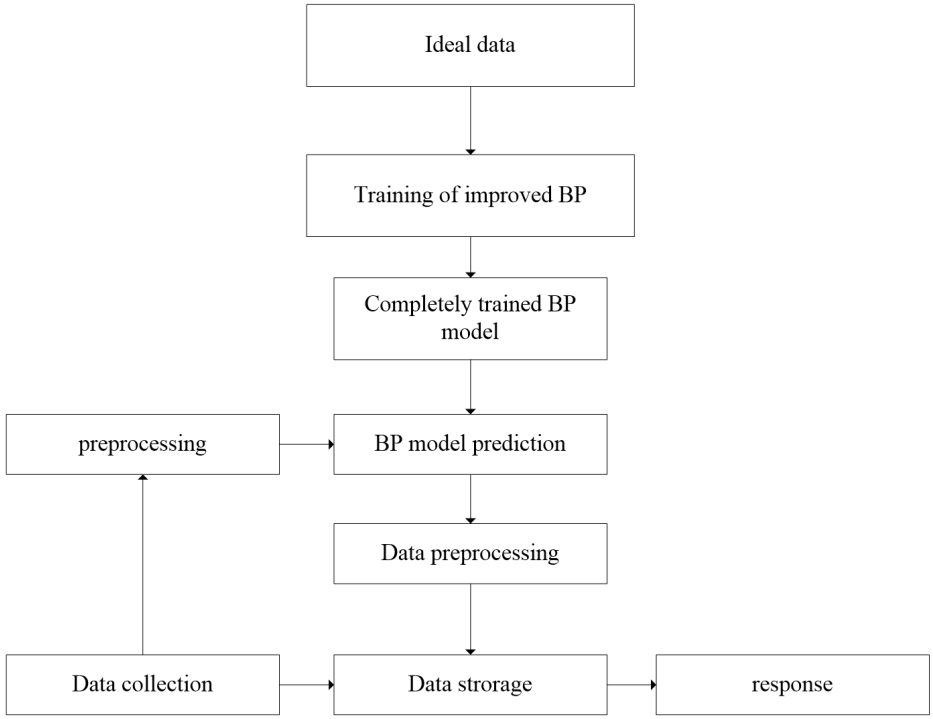

Fig. 1. Network security audit system based on quantum genetic BP

Quantum genetic algorithm simulates the natural evolution process, starting from the random generation of a group of individuals, the evolution strategy of survival of the fittest is adopted to converge to the optimal solution finally. For complex problems, the quantum genetic algorithm has strong search ability and optimization performance. The quantum genetic algorithm is used to optimize neural network weights and threshold value. At the same time, we improve the traditional quan-

tum genetic algorithm, and each link of quantum genetic algorithm is analyzed in detail, including quantum bit coding, fitness function design, quantum door update, mutation and so on. Coding uses quantum bit coding way, the parameters of neural network constitute a kind of chromosome after a certain combination and allocation, and it is converted into binary form further.

$$p_i^j =$$

$$= \left(\underbrace{\begin{array}{cccccccccccc} \alpha_{11}^{'} & \alpha_{12}^{'} & \dots & \alpha_{1l_1}^{'} & \alpha_{21}^{'} & \alpha_{22}^{'} & \dots & \alpha_{2l_2}^{'} & \dots & \alpha_{m1}^{'} & \alpha_{m2}^{'} & \dots & \alpha_{ml_m}^{'} \\ \beta_{11}^{'} & \beta_{12}^{'} & \dots & \beta_{1l_1}^{'} & \beta_{21}^{'} & \beta_{22}^{'} & \dots & \beta_{2l_2}^{'} & \dots & \beta_{m1}^{'} & \beta_{m2}^{'} & \dots & \beta_{ml_m}^{'} \end{array}}_{K_1K_2\dots K_{l_1}, K_1K_2\dots K_{l_2}, K_1K_2\dots K_{l_m}} \right).$$

Symbol m represents gene number of chromosome which corresponds to the number of neural network parameters, k represents the number of quantum bit of each gene. For one parameter, if the parameter is n, $k = \lfloor \log_2 n \rfloor$. Neural network parameters combination scheme is shown in the above equation. In designed code and its mapping sense, we choose a set of all possible neural network parameters. So a certain solution accurately represents a kind of neural network parameter combination scheme.

After selection, crossover and mutation operation, we can use parameter combination for neural network training, then the number of attacks detected correctly and the number of connections that are judged to be attacks mistakenly are worked out. According to the result of training and testing results, we evaluate parameter combination. The first value of chromosome in the first generation of quantum genetic algorithm is taken as parameters, which is assigned to BP neural network. Then BP neural network is used in audit system. Calculate error between experiment result and target result. If the error is greater than error range, quantum genetic algorithm is again used to assign value to the BP neural network parameters. Otherwise, the assignment process stops.

The rotation angle and direction of quantum gate are adjusted by means of evolution equation, and we no longer use look-up table. In this way there are two main advantages. One is to reduce the number of parameters, which simplifies the structure of the quantum genetic algorithm. Another is the evolution equation has characteristic memory, which not only can make use of the individual's own local optimal information, but also can use the optimal information of neighborhood population. It also uses the optimal state information of the whole population, thus it can adjust rotation angle theta more reasonably. It has better ability than traditional quantum genetic algorithm to jump out of local optimum. The evolution equation is

$$\theta = k_1(p_m - x_i) + k_2(p_i - x_i) + k_3(p_j - x_i) + k_4(p - x_i),$$

where k_1, k_2, k_3, k_4 are influence factors, p_i, p_j are population extreme value of the left and right neighborhood, p_m is the extreme value of individual population and p

represents global extreme value. We have designed a kind of quantum mutation in order to improve the performance of the traditional quantum genetic algorithm. In traditional genetic algorithm, the effect of mutation lies in providing algorithm local search ability and prevent premature convergence. Due to the quantum mutation needs to satisfy the mutation requirement of both genetic algorithm and quantum parallelism, we define a simple single quantum bit mutation operation, and the method can be further extended to the situation of more quantum bits. Network security audit system based on quantum genetic BP is shown in Fig. 1 and the specific methods are as follows.

The first step is to choose several individuals from the population randomly according to probability p_i. The second step is to determine one or more mutation bits for the selected individual according to fixed probability. The third step is to carry out exchange operation.The classifier analyzes characteristics of captured data, and then the unknown type is sent into the training sample, after neural network learning, the neural network classifier is used to classify again. According to the controllable network traffic data, we calculate each traffic characteristic statistics data during the period of every minute as the input of the neural network. Through the visual analysis of network traffic anomaly, the network traffic anomaly is divided into two categories. The advantages of quantum genetic algorithm is used to overcome the slow convergence and local convergence of BP algorithm, combined with the BP algorithm at the same time, it also solves the problem that quantum genetic algorithm cannot find the approximate optimal solution in a short period of time, and introducing gradient information of BP algorithm will avoid this kind of phenomenon. So the training of the BP neural network can be divided into two parts. Quantum genetic algorithm is used to optimize the initial weights of network, then BP algorithm is used to train the attack data to get the network model. Three layer of neural network is used. Symbol WI_{ij} represents connection weight value between the ith node of the input layer and the jth node of the hidden layer. Quantity WO_{ji} represents connection weight value between the jth node in the hidden layer and the ith node in the output layer. Symbol H_i represents output of the ith node of hidden layer, O_i represents output of the ith node of the output layer and I_i represents output of the ith node of the input layer. The optimization process is as follows.

Step 1. Initialize population p, including mutation probability and connection weight WI_{ij}, WO_{ji}.

Step 2. Calculate fitness value of each individual and sort it. Here

$$p_s = \frac{f_i}{\sum_{i=1}^{N} f_i,}$$

where f_i represents the fitness value of individual i, which can be measured by the sum of square errors.

Step 3. Use mutation probability p_m to generate the new individual $G_j^{'}$ of G_j.

Step 4. The new individual is inserted into population p and we should fitness of the new individual.

Step 5. Calculate square sum of error of BP neural network. If it achieves preset

value $\varepsilon_{\mathrm{GA}}$, the algorithm stops. Otherwise, it turns to step 3 to go on.

Step 6. The solution of quantum genetic algorithm is taken as initial weight value and BP algorithm is used to train the network until the accuracy meets $\varepsilon_{\mathrm{BP}} < \varepsilon_{\mathrm{GA}}$.

Repeat the above steps, quantum genetic algorithm stops until the network error satisfies the condition. We choose a group of weight value with the smallest network error as initial weights of BP network training. Then we use BP algorithm for training, until the final error requirement is met. The parameters of the neural network are coded into chromosomes directly involved in the genetic operation, which can make the quantum genetic algorithm combined with specific problem. All of the neural network weight value has no limit of the value space, belonging to the unconstrained problem, so that the quantum genetic operation can make global search in the space as possible.

3. Experiment and analysis

We use BP neural network based on genetic and BP neural network based on quantum genetic algorithms for security audit system, so as to verify the application effect of proposed scheme. Experiments data comes from KDD99 CUP data set. We use 10000 piece of data as the training data, and 3000, 5000, 8000, 12000 piece of data is taken as the testing data.

Training process based on quantum genetic BP is shown in Fig. 2, training process based on genetic BP is shown in Fig. 3 and training process based on BP is shown in Fig. 4. The training step of quantum genetic BP is 22, training time is 12.105000 seconds, and the mean square error is 1.2681e–003. The step of genetic BP training is 563, its time is 22.119000 seconds, and the mean square error is 1.2786e–003. The training step of BP is 1132, its time is 25.112000 seconds, and the mean square error is 1.213e–2. It can be seen that quantum genetic BP algorithm exhibits fast convergence speed and low error.

Security audit result based on BP neural network is shown in Table 1, security audit result based on genetic BP neural network is shown in Table 2 and security audit result based on quantum genetic BP neural network is shown in Table 3. It can be seen that network security audit system based on quantum genetic BP has higher detection rate than traditional schemes. Besides, the proposed scheme has lower false alarm rate and missing report rate.

Table 1. Security audit result based on BP neural network

sample number	3000	5000	8000	12000
correctly detected sample number	2709	4533	7284	10926
accuracy	90.3 %	90.66 %	91.05 %	91.05 %
false alarm number	203	362	497	737
false alarm rate	6.77 %	7.24 %	6.21 %	6.14 %
number of missing report	88	105	219	337
rate of missing report	2.93 %	2.10 %	2.74 %	2.81 %

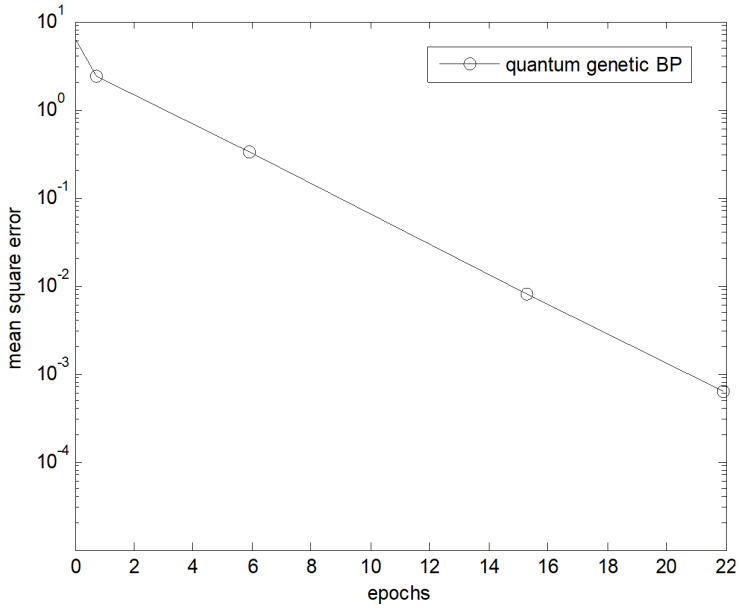

Fig. 2. Training process based on quantum genetic BP

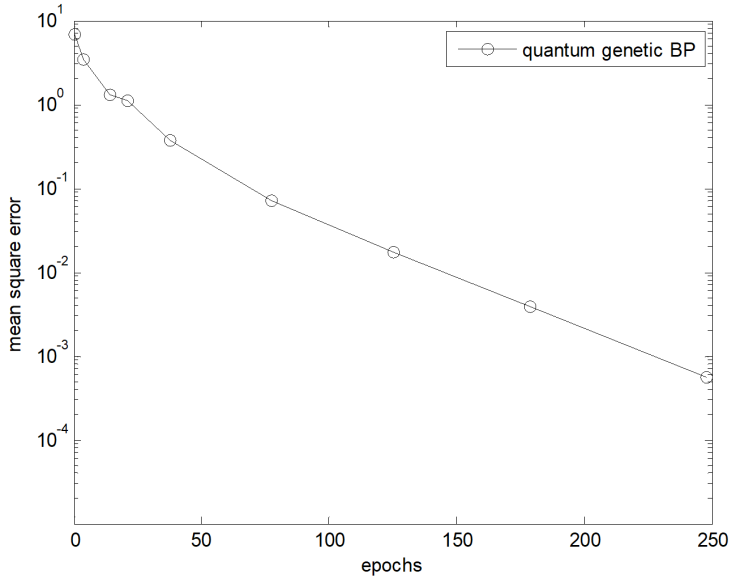

Fig. 3. Training process based on genetic BP

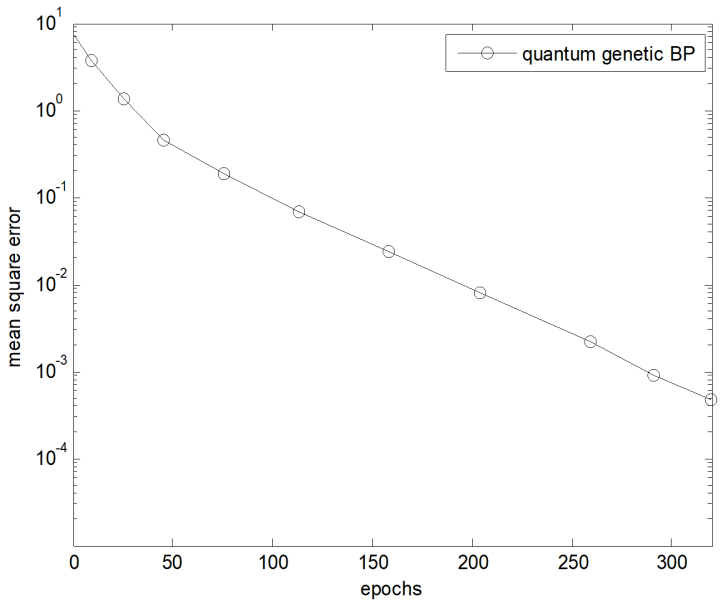

Fig. 4. Training process based on BP

4. Conclusion

BP neural network is applied to network security audit system. Because inherent defects of BP neural network, quantum genetic algorithm is given to optimize the initial weights of BP neural network, and it is applied in security audit system. The experiment results show the proposed scheme has good performance. Based on the practical point of view, the designed network security audit system is not perfect enough, especially the selection of training samples have certain effects on the accuracy of the network identification, which is one of the research direction in the future. With the continuous progress of science and development, interdisciplinary knowledge can be adopted to find out the better solution.

Table 2. Security audit result based on genetic BP neural network

sample number	3000	5000	8000	12000
correctly detected sample number	2827	4705	7518	11296
accuracy	94.23 %	94.10 %	93.98 %	94.13 %
false alarm number	112	221	356	577
false alarm rate	3.73 %	4.42 %	4.45 %	4.81 %
number of missing report	61	74	126	127
rate of missing report	2.03 %	1.48 %	1.58 %	1.06 %

Table 3. Security audit result based on quantum genetic BP neural network

sample number	3000	5000	8000	12000
correctly detected sample number	2871	4796	7618	11426
accuracy	95.70 %	95.92 %	95.23 %	95.22 %
false alarm number	98	156	303	407
false alarm rate	3.27 %	3.12 %	3.45 %	3.39 %
number of missing report	31	48	106	167
missing report rate	1.03 %	0.96 %	1.33 %	1.39 %

References

[1] X. W. Ning, P. Y. Liu: *Log system design in support of linkage analysis of security audit and computer forensics.* Computer Engineering and Design *30* (2009), No. 24, 5580–5583.

[2] M. Liu, Q. Zhang, H. Yhao, D. Yu: *Network security situation assessment based on data fusion.* Proc. International Workshop on Knowledge Discovery and Data Mining (WKDD), 23–24 Januar 2008, Adelaide, SA, Australia, IEEE Conference Publications (2008), 542–545.

[3] J. E. L. de Vergara, A. Guerrero, V. A. Villagrá, J. Berrocal: *Ontology-based network management: Study cases and lessons learned.* Journal of Network and Systems Management *17* (2009), No. 3, 234–254.

[4] J. Lai, H. Wang, X. Liu, Y. Liang: *A quantitative prediction method of network security situation based on wavelet neural network.* International Symposium on Data, Privacy, and E-Commerce (ISDPE), 1–3 November 2007, Chengdu, Sichuan, China, IEEE Conference Publications (2007), 197–202.

[5] Y. Liang, H. Q. Wang, J. B. Lai: *Quantification of network security situational awareness based on evolutionary neural network.* International Conference on Machine Learning and Cybernetics (ICMLC), 19–22 August 2007, Hong Kong, China, IEEE Conference Publications *6* (2007), 3267–3272.

[6] Y. Liang, H. Q. Wang, H. B. Cai, Y. J. He: *A novel stochastic modeling method for network security situational awareness.* International Conference on Industrial Electronics and Applications (ICIEA), 3–5 June 2008, Singapore, Singapore, IEEE Conference Publications (2008) 2422–2426.

[7] H. Wang, J. Lai, X. Liu: *A quantitative forecast method of network security situation basedon BP neural network with genetic algorithm.* International Multi-Symposiums on Computer and Computational Sciences (IMSCCS), 13–15 August 2007, Iowa City, IA, USA, IEEE Conference Publications (2007), 374–380.

[8] J. Li, H. Wang: *A quantification method for network security situational awareness based on conditional random fields.* Proc. International Conference on Computer Sciences and Convergence Information Technology (ICCIT), 24–26 November 2009, Seoul, South Korea, IEEE Conference Publications, (2009), 993–998.

[9] J. Gao, B. Zhang, X. Chen, Z. Luo: *Ontology-based model of network and computer attacks for security assessment.* Journal of Shanghai Jiaotong University (Science) *18* (2013), No. 5, 554–562.

[10] Yang J, Li B, Zhuang Z: *Research of quantum genetic algorith and its application in blind source separation.* Journal of Electronics (China) *20*, (2003), No. 1, 62–68.

[11] K. H. Han, J. H. Kim: *Quantum-inspired evolutionary algorithms with a new termination criterion gate, and two-phase scheme.* IEEE Transactions on Evolutionary Computation *8* (2004), No. 2, 156–169.

[12] X. R. Zhu, X. H. Zhang: *A quantum genetic algorithm with repair function and its application in knapsack question.* Journal of Computer Applications *27* (2007), No. 5, 1187–1190.

[13] P. C. Li, S. Y. Li: *Quantum genetic algorithm based on real-coded and objective function's gradient.* Journal of Harbin Institute of Technology *38* (2006), No. 8, 1216–1218,1223.

[14] S. H. Xu, C. Xu, X. Hao, Y. Wang, P. C. Li: *Improved quantum genetic algorithm with double chains and its application.* Application Research of Computers *21* (2010), No. 6, 2090–2092.

Received July 12, 2017