Improved BP Neural Network for Intrusion Detection Based on AFSA

Tian Wang[1, a], Lihao Wei[1, b], Jieqing Ai[1, c]
[1] *Guangdong Power Grid Software Testing Lab, Guangdong, Guangzhou, 510000, China*
[a]*email: wangtian@gdxx.csg.cn* [b]*email: weilihao@gdxx.csg.cn* [c]*email: aijieqing@gdxx.csg.cn*

Abstract

Establishing a complete information security policy is the most important step to solve the problem of information security and the basis for the entire information security system. Using intrusion detection technology to identify the source of threats and adjusting security policy is an effective operation of network protection. Trained BP neural network model is usually adopted as detector, but because of defects of weights training algorithm of BPNN, the weights always fall into local minima area. In order to address this problem, we propose a detection model based on BP neural network training by AFSA (Artificial Fish Swarming Algorithm). The algorithm optimizes the weights of BP neural network by AFSA. It shortens the sample training time and improves BP neural network classification accuracy. Experimental results demonstrated that it has a shorter training time and can achieve a superior detection rate than BPNN.

Keywords: Security Policy; Intrusion Detection; BP Neural Network; AFSA

1 Introduction

The concept of intrusion detection was proposed in 1987 as an abstract model called intrusion detection systems [1]. Intrusion detection technology can help quickly identify network intrusions, and respond [2]. It expanded the system administrator's security management capabilities and has been rapidly developed and widely applied in recent years [3][4].

Intrusion detection refers to analyze the information collected from a number

of key points of the computer network or computer system, and then found the activation that violating the security policy behavior or attacking the network system and feedback the responding. Intrusion detection is a proactive security protection technology, can well make up for the lack of a firewall [5].

Following methods are commonly used in intrusion detection: pattern matching [6], protocol analysis [7], expert systems [8], statistical analysis [9], data mining [10], neural networks [11], genetic algorithms [12]. In the practical application and researching, usually do not use a single detection method. Instead of using a variety of detection methods combine to detect attacks.

Since all intrusions have certain characteristics, and all the characters are performed by their data. So, how to accurately analyze the relationship between their data and behaviors is the most hotspot of the study. Earlier network intrusion detection models were based on pattern matching algorithm, which has been considerable development in network intrusion detection system, but the efficiency of this algorithm to match the packet is quite low.

In recent years, the neural network model has been widespread concern, and it shows a very high recognition rate. Based on the previous studies, this paper proposed a novel intrusion detection model based on AFSA-BPNN.

2 Back Propagation Neural Network

BPNN has self-adaptive, self-organizing and self-learning ability [13]. First, the information from the audit log or normal network access behavior is processed to generate the input vector, and then input to the neural network. The output vector can be utilized to determine whether the intrusion. The structure of BPNN using for intrusion detection is showed in Fig.1.

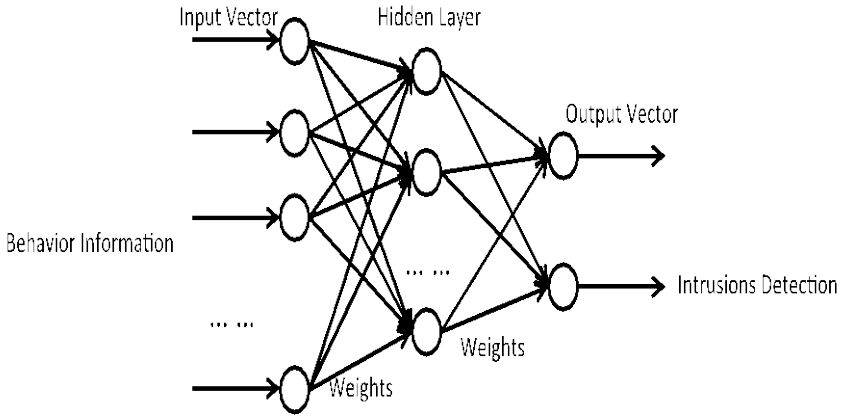


Fig.1. The structure of BPNN

BPNN not needs to know the exact relationship between the input and output data. It can be trained to use the network to simulate the mapping between them. Therefore, BP neural network has excellent non-linear fitting and pattern recognition capabilities for intrusion test problem is very reasonable and effective.

3 Artificial Fish Swarming Algorithm

AFSA is a swarm intelligence optimization algorithm based on animal behavior [14], has a highly parallel, self-organizing, adaptive and collaborative and other features. It can effectively overcome the local optimum value problem and achieve the global optimum. AFSA algorithm has the following three kinds of intelligence operations.

Operation1 (Foraging): By detecting the concentration of food to determine the direction of movement, and move towards the best direction.

Operation2 (Swarming): Fish gather in groups, together with the collection of food and avoid predators.

Operation3 (Following): When a fish finds food, the other will swim to it quickly.

With the above operations, AFSA can fast solve the complexity nonlinear problem and it has a fast convergence speed. In order to better exhibit the

proposed model, we have produced a flow chart of the algorithm as showed in Fig.2.

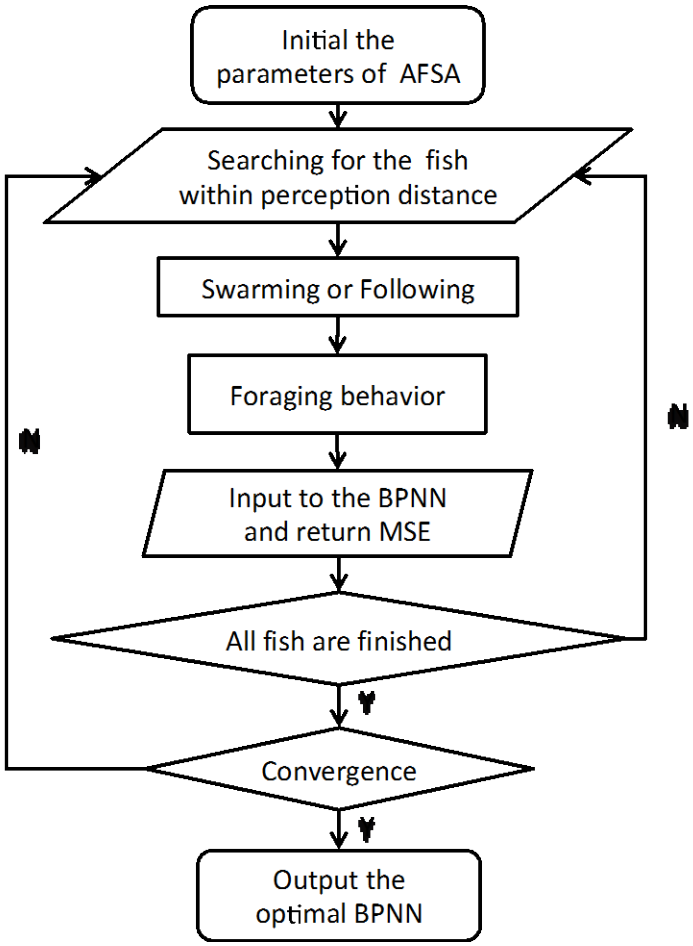
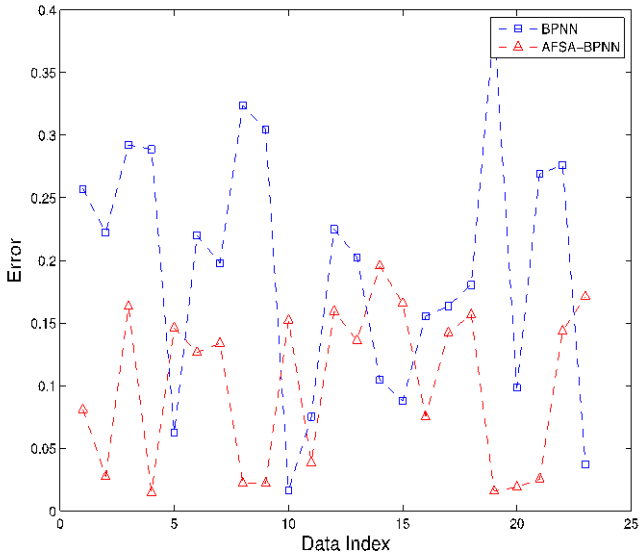


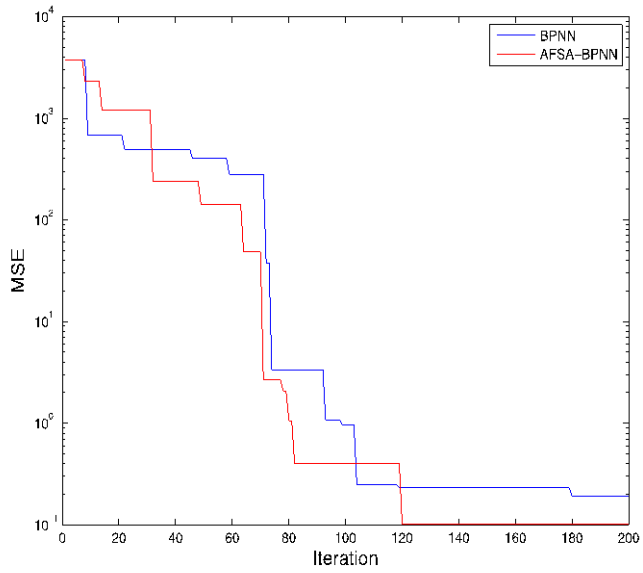
Fig.2. The flowchart of AFSA-BPNN

4 Experimental Results

In order to better demonstrate the advantages proposed model, we first compare the algorithm with BPNN. The detection results and the iteration curves are shown in Fig.3.



(a) detection results



(b) iteration curves

Fig.3. Detection error and the iteration curves

From the above experimental results, we can observe that AFSA significantly

improved the convergence speed and detection performance of BPNN. Further, two other algorithms (GA-PBNN [15], PSO-BPNN [16]) are provided for comparison. The results are detailed in Tab.1.

Detection Algorithm	**MSE**
BPNN	0.1934
GA-BPNN	0.1759
PSO-BPNN	0.1410
AFSA-BPNN	0.1014

Tab.1. The detection results of different algorithms

As can be seen from Tab.1. Although the other algorithm enhanced the performance of BPNN, but AFSA-BPNN achieved the most accurately results. In summary, the novel proposed algorithm has good performance and more stable on intrusion detection.

5 Conclusion

In this paper, a novel intrusion detection model was established which is based on AFAS and BPNN. By embedding AFSA into BPNN, significantly improves the accuracy and convergence speed of the intrusion detection model. Further work will focus on: i) embed the algorithm into software, and apply it to real-time monitoring applications; ii) establish more training data, so that the trained BPNN can detect more abnormal kinds of behavior.

References

[1] Lunt T F. Automated audit trail analysis and intrusion detection: A survey[C]. In Proceedings of the 11th National Computer Security Conference. 1988.

[2] Denning D E. An intrusion-detection model[J]. Software Engineering, IEEE Transactions on, 1987 (2): 222-232.

[3] Wang Y, Fu W, Agrawal D P. Gaussian versus uniform distribution for intrusion detection in wireless sensor networks[J]. Parallel and Distributed Systems, IEEE Transactions on, 2013, 24(2): 342-355.

[4] Vieira K, Schulter A, Westphall C, et al. Intrusion detection for grid and

cloud computing[J]. It Professional, 2010, 12(4): 38-43.
[5] Zhou C V, Leckie C, Karunasekera S. A survey of coordinated attacks and collaborative intrusion detection[J]. Computers & Security, 2010, 29(1): 124-140.
[6] Kumar S, Spafford E H. A pattern matching model for misuse intrusion detection[J]. 1994.
[7] Dreger H, Feldmann A, Mai M, et al. Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection[C]. USENIX Security. 2006.
[8] Anderson D, Frivold T, Valdes A. Next-generation intrusion detection expert system (NIDES): A summary[M]. SRI International, Computer Science Laboratory, 1995.
[9] Ye N, Emran S M, Chen Q, et al. Multivariate statistical analysis of audit trails for host-based intrusion detection[J]. Computers, IEEE Transactions on, 2002, 51(7): 810-820.
[10] Phua C, Lee V, Smith K, et al. A comprehensive survey of data mining-based fraud detection research[J]. arXiv preprint arXiv:1009.6119, 2010.
[11] Prasad M V S, Babu A V, Rao M K B. An Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms[J]. International Journal of Computer Science and Management Research, 2013, 2.
[12] Li W. Using genetic algorithm for network intrusion detection[J]. Proceedings of the United States Department of Energy Cyber Security Group, 2004: 1-8.
[13] Jayalakshmi T, Santhakumaran A. Statistical normalization and back propagation for classification[J]. International Journal of Computer Theory and Engineering, 2011, 3(1): 1793-8201.
[14] Wang C R, Zhou C L, Ma J W. An improved artificial fish-swarm algorithm and its application in feed-forward neural networks[C]. Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on. IEEE, 2005, 5: 2890-2894.
[15] Fu Z, Mo J. Springback prediction of high-strength sheet metal under air bending forming and tool design based on GA–BPNN[J]. The International

Journal of Advanced Manufacturing Technology, 2011, 53(5-8): 473-483.
[16] Guo W, Xiong N, Vasilakos A V, et al. Multi-source temporal data aggregation in wireless sensor networks[J]. Wireless personal communications, 2011, 56(3): 359-370.