Fuzzy Systems and Data Mining VIII
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220405

Intrusion Detection System Using PSO and DE Algorithms with BP Neural Network

Ke WANG [a,b], Jingwei GUAN [c], Song LUO [d,1] and Zhi GUAN [e]
[a] *Key Laboratory of High Confidence Software Technologies (Peking University), MoE, Beijing, China*
[b] *Department of Computer Science and Technology, EECS, Peking University, Beijing, China*
[c] *Liangjiang International College, Chongqing University of Technology, Chongqing, China*
[d] *School of Computer Science and Engineering, Chongqing University of Technology, Chongqing, China*
[e] *National Engineering Research Center for Software Engineering, Peking University, Beijing, China*

Abstract. Intrusion detection system (IDS) combines software and hardware to detect network attacks. In this paper, we propose a new intrusion detection method based on an improved BP neural network algorithm. We improve the BP neural network algorithm by combining it with the particle swarm optimization (PSO) algorithm and the differential evolution (DE) algorithm. We also propose a new framework based on common intrusion detection framework to accommodate our improved BP neural network. The experiments based on the CICIDS2017 dataset show our approach achieves better detection efficiency.

Keywords. Intrusion detection system, BP neural network, particle swarm optimization, differential evolution

1. Introduction

With the development of network, network security is more and more important. Intrusion Detection System (IDS) [1] is a combination of software and hardware which detects network attacks. In an IDS, network traffic are collected and analyzed continuously. IDS will send alarm information and write log files once it detects an intrusion behavior. Classification and clustering are the main techniques used for detection. However, these techniques cannot predict future attacks. Therefore, previous IDS cannot deploy defense strategies in advance. Some IDS has a good detection effect on known attacks, but its efficiency will decline significantly when the network changes.

At present, artificial intelligence technologies such as machine learning algorithms are introduced to improve intrusion detection [2]. Back Propagation (BP) neural network

[1] Corresponding Author: ratio@cqut.edu.cn

is one of the most widely used neural networks proposed by Rumelhart et al. in 1986 [3]. It is a multi-layer neural network which has three types of layers: input layer, hidden layer and output layer. BP neural network has different thresholds and weights. These thresholds will be used in many various mapping functions to achieve different mapping effects. In this way, some relationships which cannot be expressed by mathematical formulas can be expressed. The neural network uses the loss function and the integral of the weight as the calculation method of the error data. By continuously adjusting the parameter value of each weight, we can reduce the error rate of each link gradually, and finally achieve an acceptable error rate. In recent years, BP neural network is a hot topic in IDS but its detection rate and speed are not very satisfactory [4].

Eberhart and Kennedy [5] proposed the Particle Swarm Optimization (PSO) algorithm in 1995. The algorithm is a random search algorithm based on group collaboration and was developed by simulating bird feeding. When the algorithm is executed, a set of random solutions will be initialized, and the current best particle will be drawn to find the best solution with the least error through continuous iteration, and then the particle will fly in the space of the entire solution set to find the best solution.

Differential evolution algorithm (DE) is a stochastic computing technology proposed by Storn and Price [6] for a long time and is now relatively mature compared to other algorithms. The algorithm filters and refreshes the data continuously which simulates evolution in the nature under the principle "survival of the fittest", so that the data adapting to the system environment will be reserved and become the optimal solution of the system.

Our Contribution. In this paper, we propose a new intrusion detection system based an improved BP neural network. To improve the detection rate and speed simultaneously, we combine the particle swarm optimization algorithm and the differential evolution algorithm with BP neural network. We propose a new framework based on common intrusion detection framework to accommodate our improved BP neural network. Experiments based on the CICIDS2017 dataset [7] show our approach achieves better detection efficiency, compared with the pure BP neural network algorithm and the PSO+BP neural network algorithm.

Related Works. Machine learning was introduced to intrusion detection by Lee et al. [2] for the first time and they got an anomaly detection model. In recent years, BP neural network was used to improve the detection efficiency of IDS. Wang et al. [4] utilized workflow to define the features of network attack which helpes BP neural network to recognize the possible attacks. Zhao and Li [8] used a real coding genetic algorithm to optimize the weights and threshold of BP neural network. Duan et al. [9] got an IDS in which BP neural network is combined with improved artificial bee colony algorithm with elite-guided search equations. Yang et al. [10] presented an LM-BP neural network model which optimizes the weight threshold of BP neural network. To improve the detection rate of IDS, Gong et al. [11] combined the multi-objective genetic algorithm with BP neural network and proposed a novel two-phase cycle training algorithm. Lu et al. [12] proposed an intrusion detection model named IPSO-BPNN which combines improved particle swarm optimisation algorithm and BP neural network. Chen et al. [13] carried out a subspace clustering algorithm on the network dataset and used BP neural network in different subspaces.

Organization. The rest of this paper is organized as follows. We show how to combine the PSO algorithm and the DE algorithm to get an improved PSO+DE+BP

neural network algorithm in Section 2. We describe the system architecture of our IDS in Section 3. In Section 4, we implement an experimental application based on our PSO+DE+BP neural network algorithm. Finally the paper is concluded with future work in Section 5.

2. Improved BP Neural Network

The BP neural network constructed in this paper is divided into 3 layers, the input layer is divided into 4 neurons, corresponding to the preprocessed 4-dimensional data, and the preprocessed 4-dimensional data is used as input; the number of hidden layer neurons is 6, the number of neurons in the output layer is 1. When obtaining the final result, we use the differential evolution algorithm to optimize the classification of the result. The workflow of the improved BP neural network is shown in Figure 1.

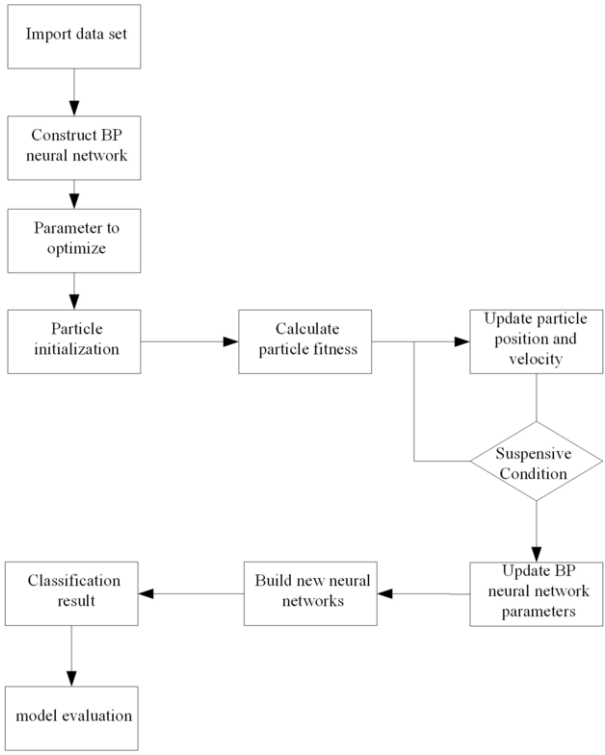

Figure 1. PSO+DE+BP Neural Network

The improved BP neural network can be summarized into the following four stages:

(i) The initial BP neural network is self-initialized, and a neural network is built on a training data set.
(ii) Extract the parameters that need to be optimized in the neural network, express them in the form of particles, and perform particle optimization.
(iii) Iterate the first and second steps until the fit is the smallest error value.

(iv) Use the differential evolution algorithm to optimize the output result of the neural network.

3. System Architecture

We realize our IDS system based on the Common Intrusion Detection Framework (CIDF) shown in Figure 2. According to the structure of CIDF, we develop and classify specific modules for the actual application of the entire system. Firstly, the main function of the event generator in the CIDF model is to collect and create specific event data, and collect data sets that may be identified as attacks in the event generator; secondly, the event analyzer receives the generated data from the event generator. After the data is collected, it is analyzed and passed to the next module; next, the response unit will return the analysis result. If the result is normal, the behavior is judged to be a normal system behavior and recorded in the whitelist of the event database. If the result is abnormal, the behavior is judged to be a malicious attack behavior and recorded in the blacklist of the event database and alarmed to the system administrator; finally, the event database is used to record the existing response events and the system will respond quickly if the same event occurs.

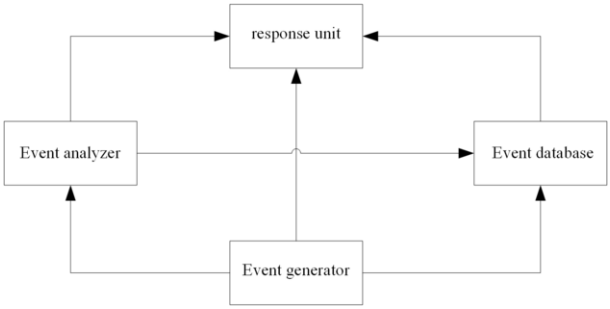

Figure 2. Common Intrusion Detection Framework

The data packets used in our IDS are based on the network data packets captured in the underlying transmission. By collecting these data packets, we can extract some network behavior characteristics and record them. We then put these characteristic values into the neural network for learning, and finally the computer can automatically recognize the attack behavior. Therefore, we design and divide the system into four major modules, called the network sniffer, the administrator audit terminal, the data detection platform and the database. The overall architecture of the system is shown in Figure 3.

(i) Sniffer module
The main function of this module is to monitor and capture a large number of data packets in the computer's network adapter or other equipment, analyze the information in the data packet, classify and filter the useful and useless information, such as intercepting the source IP address and the destination IP Address, including information such as the network communication protocol used, forward these intercepted data packets to the administrator data audit terminal for data splitting and audit classification.

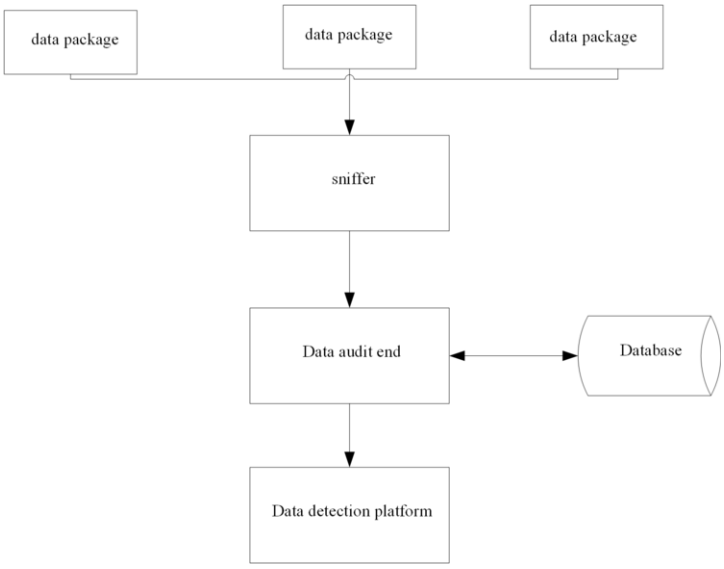

Figure 3. System Architecture

(ii) Data audit module
The module is mainly divided into two functions. First, the first function is to receive the data packet sent from the sniffer, split and classify the data in the data packet, and extract the feature value we need and the feature The value is packaged and sent to the data detection platform. The second function is to receive the results returned from the data test platform, and make the administrator make corresponding judgments based on the results returned to the audit end. This module is connected with the database module. Once abnormal behavior is found, the characteristic value of the behavior will be recorded in the blacklist of the database for future calls. If no normal behavior is found, the normal characteristic value will be recorded in the database. In the whitelist, it is convenient to check in the future.

(iii) Data detection module
This module is responsible for detecting the data sent by the auditing terminal and returning it to the auditing terminal. In this module, we use the CICIDS2017 dataset [7] for training. There are more than 80 features in CICIDS2017 which covers common updated attacks such as Brute Force, DoS/DDoS, Heartbleed, Web, Infiltration and Botnet attacks.

(iv) Database
We divide the database into two parts. The first part is a blacklist for abnormal behaviors. After extracting the characteristic values in the corresponding data packets, we record those characteristic values detected as abnormal behaviors into the blacklist. If the network is subjected to this same type of attack again, the corresponding characteristic value can be found in the database which improves the detection efficiency of the system. The second part is the whitelist for normal behaviors. We record those characteristic values detected as normal behaviors to the whitelist of the database to prevent normal behaviors from being mistakenly detected as abnormal behaviors, which can reduce the false alarm rate of the system.

4. Experiment

To evaluate our approach, we implement an application in Python. The results are computed on Windows 10 with AMD Ryzen 5 1600 Six-Core Processor and 8 GB RAM. We adopt Precision (Pr), Recall (Rc), Accuracy (Acc), False positive rate (FPR) as our performance metrics. These metrics are calculated from the following confusion matrix (Table 1) which compares the type of network flows and the result of classification:

Table 1. Confusion Matrix

Flow Type	Classification Result	
	Correct	Incorrect
Attack	TP	FN
Normal	TN	FP

Note: TP is number of attack flows classified correctly, FN is number of attack flows classified incorrectly, TN is number of normal flows classified correctly and FP is number of normal flows classified incorrectly.

The calculation of the four metrics are described as follows:

$$Pr = \frac{TP}{TP+FP} \tag{1}$$

$$Rc = \frac{TP}{TP+FN} \tag{2}$$

$$Acc = \frac{TP+TN}{TP+FN+TN+FP} \tag{3}$$

$$FPR = \frac{FP}{TN+FP} \tag{4}$$

We compare our PSO+DE+BP neural network algorithm with pure BP neural network algorithm and PSO+BP neural network algorithm. Table 2 shows the accuracy (Max, Min, Avg) and the average training time among these three algorithms. Experiments show that our PSO+DE+BP neural network algorithm achieves the highest detection accuracy of 84.39%. Furthermore, our PSO+DE+BP neural network algorithm requires the shortest execution time. Figure 4 shows the performance (Precision, Recall, Accuracy, False positive rate) of these three algorithms.

Table 2. Accuracy Comparison

Algorithm	Accuracy(%)			Average Time(sec)
	Min	Max	Average	
Pure BP	80.3	82.8	81.73	546
PSO+BP	80.9	84.3	83.25	481
PSO+DE+BP	81.2	85.2	84.39	397

Note: All the experiments were executed ten times on the same platform.

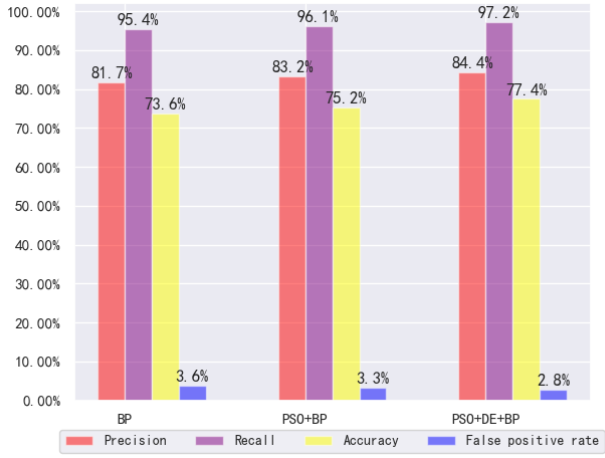

Figure 4. Performance Comparison

5. Conclusion

Intrusion detection system collects and analyzes network traffic continuously. The detection approach is the core of IDS which affects the efficiency of IDS heavily. BP neural network is a widely used algorithm in machine learning. We propose an improved BP neural network algorithm which combines the BP neural network algorithm with the PSO algorithm and the DE algorithm. Our approach achieves a better efficiency in detection than pure BP neural network algorithm or the PSO+BP neural network algorithm. It takes shorter time to training but gets the higher accuracy and precision rates. Future work may be combining other machine learning algorithms with BP neural network algorithm to shorten the training time and improve the detection efficiency simultaneously.

Acknowledgements

This work is supported by the National Key Research and Development Program of China No. 2020YFB1005404, Ministry of Education-China Mobile Scientific Research Fund MCM20200104, and National Natural Science Foundation of China (Grant No. 61872051).

References

[1] R Heady, G Luger, A Maccabe, and M Servilla. The architecture of a network level intrusion detection system. Technical report, Department of Computer Science, University of New Mexico, 1990.

[2] Wenke Lee, Salvatore J. Stolfo, and Kui W. Mok. A data mining framework for building intrusion detection models. In *1999 IEEE Symposium on Security and Privacy, Oakland, California, USA, May 9-12, 1999*, pages 120–132. IEEE Computer Society, 1999.

[3] David E. Rumelhart, Geoffrey E. Hinton, and Ronald J. Williams. Learning representations by back-propagating errors. *Nature*, 323:533–536, 1986.

[4] Yong Wang, Dawu Gu, Wei Li, Hongjiao Li, and Jing Li. Network intrusion detection with workflow feature definition using BP neural network. In Wen Yu, Haibo He, and Nian Zhang, editors, *Advances in Neural Networks - ISNN 2009, 6th International Symposium on Neural Networks, ISNN 2009, Wuhan, China, May 26-29, 2009, Proceedings, Part I*, volume 5551 of *Lecture Notes in Computer Science*, pages 60–67. Springer, 2009.

[5] J. Kennedy and R. Eberhart. Particle swarm optimization. In *Proceedings of ICNN'95 - International Conference on Neural Networks*, volume 4, pages 1942–1948 vol.4, 1995.

[6] Rainer Storn and Kenneth Price. Differential evolution - a simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization*, 11(4):341–359, 1997.

[7] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Paolo Mori, Steven Furnell, and Olivier Camp, editors, *Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Funchal, Madeira - Portugal, January 22-24, 2018*, pages 108–116. SciTePress, 2018.

[8] Jian-Hua Zhao and Wei-Hua Li. Intrusion detection based on BP neural network and genetic algorithm. In Chunfeng Liu, Leizhen Wang, and Aimin Yang, editors, *Information Computing and Applications - Third International Conference, ICICA 2012, Chengde, China, September 14-16, 2012. Proceedings, Part II*, volume 308 of *Communications in Computer and Information Science*, pages 438–444. Springer, 2012.

[9] Letian Duan, Dezhi Han, and Qiuting Tian. Design of intrusion detection system based on improved abc_elite and BP neural networks. *Comput. Sci. Inf. Syst.*, 16(3):773–795, 2019.

[10] Ai-Min Yang, Yunxi Zhuansun, Chenshuai Liu, Jie Li, and Chunying Zhang. Design of intrusion detection system for internet of things based on improved BP neural network. *IEEE Access*, 7:106043–106052, 2019.

[11] Yiguang Gong, Yunping Liu, Chuanyang Yin, and Zhiyong Fan. A two-phase cycle algorithm based on multi-objective genetic algorithm and modified BP neural network for effective cyber intrusion detection. In Xiaofeng Chen, Hongyang Yan, Qiben Yan, and Xiangliang Zhang, editors, *Machine Learning for Cyber Security - Third International Conference, ML4CS 2020, Guangzhou, China, October 8-10, 2020, Proceedings, Part I*, volume 12486 of *Lecture Notes in Computer Science*, pages 73–88. Springer, 2020.

[12] Xue Lu, Dezhi Han, Letian Duan, and Qiuting Tian. Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network. *Int. J. Comput. Sci. Eng.*, 22(2/3):221–232, 2020.

[13] Shuyu Chen, Wei Li, Jun Liu, Haoyu Jin, and Xuehui Yin. Network intrusion detection based on subspace clustering and BP neural network. In *8th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2021/7th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2021, Washington, DC, USA, June 26-28, 2021*, pages 65–70. IEEE, 2021.