Using improved neural network for the risk assessment of information security

Zne Jung Lee[1], Zhao Yun Yang[2], Chou Yuan Lee[1], Zhi Hao Chen[1] and Wen Bing Wu[1]

[1]School of Technology, Fuzhou University of International Studies and Trade, China
[2]School of Economics and Management, Fuzhou University of International Studies and Trade, China

Email: lrz@fzfu.edu.cn

Abstract. Because of the information age, protecting information is very important to satisfy the three main aspects of information security, namely confidentiality, integrity and availability. In this case, information security has become one of the most important problems in information technology. Information security is a very important activity and risk assessment is the kernel of information security. However, most of the current risk assessment activities are comparatively subjective and the performances are not good enough. To understand this problem, we propose the improved neural network for the risk assessment of information security. Basically, it is processed under back-propagation neural network (BPN). Moreover, particle swarm optimization (PSO) is used for fine parameter optimization of BPN. The experimental results show that the proposed algorithm has the best performance among these compared approaches.

1. Introduction

The progress and rapid development of information technology have changed the way of life of human beings. With the wide application of information technology in daily life, information security has become an important issue under the conditions of information service. Information security is a very critical activity, and the kernel core of information security is risk assessment. However, most of the current risk assessment activities are conducted manually. The evaluation process might be subjective, such as participant analysis, retrospective analysis, historical comparison method, Delphi method and analytic hierarchy process (AHP), because they depend on judgment and experience [1]. A number of researchers used fuzzy methods, data mining and regression models to analyze the risk assessment of information security [2-3]. These above methods have ameliorated the subjective nature of risk assessment, but these results are not good enough. Recently, neural networks have successful applied to solve problems in many fields. In this paper, a new type of neural network is used to evaluate the risk assessment of information security. In the proposed improved neural network, these parameters are optimized to improve performance by PSO.

This paper is summarized as follows. Section 2 introduces the concept of neural network. The third section introduces the proposed algorithm. In section 4, the simulation results of the proposed algorithm are introduced. From the simulation results, it is found that the proposed algorithm is superior to other approaches. The concluding remarks are presented in section 5.

2. The concept of neural networks

This paper focuses on the use of improved neural network for the risk assessment of information security. The objective of neural network is to simulate human brain. It lets the computer through the learning process find the features, not from the human brain to determine the characteristics. For neural network, it mostly uses multilevel structures and widely used in many fields such as function approximation, classification, and data processing. At the same time, the rapid progress of the hardware can shorten the execution time required by the computer learning algorithm and become an important reason for the attention of neural network in recent years [4-5]. The neural network can be divided into different models according to variant characteristics such as convolution neural network (CNN) and BPN. The applications of these kind of neural networks are very extensive, among which supervise learning network is the most widely used [6]. BPN is the most widely used neural network model, whose network behavior is based on input-output learning pairs (x_j, d_j) where $j = 1, \cdots, m$. BPN trains the neural network by identifying a set of weights to minimize errors [7]. There are two main stages in BPN, forward propagation and backward propagation. A three-layer of BPN is shown in Figure 1. The function of forward propagation is to transmit the input samples to produce the current output. For a neuron q in the hidden layer, the input sample of net is shown as Eq. (1),

$$net_q = \sum_{j=1}^{m} v_{qj} x_j \tag{1}$$

and its output is shown as Eq. (2):

$$z_q = a(\sum_{j=1}^{m} v_{qj} x_j) \tag{2}$$

where $a(\sum_{j=1}^{m} v_{qj} x_j)$ in Eq. (2) is called the activation function, and v_{qj} is the weight between input x_j and neuron q. For the output neuron i, it is shown as Eq. (3),

$$net_i = \sum_{q=1}^{l} w_{qj} z_q = \sum_{q=1}^{l} w_{iq} a(\sum_{j=1}^{m} v_{qj} x_j), \tag{3}$$

and its output is shown as Eq. (4):

$$y_i = a(net_i) = a(\sum_{q=1}^{l} w_{iq} a(\sum_{j=1}^{m} v_{qj} x_j)) \tag{4}$$

The function of backward propagation is to backward propagate the error to update the weights by gradient descent method. The weights between the hidden layer and output are updated as shown in Eq. (5).

$$\Delta w_{iq} = \eta (d_i - y_i) a'(net_i) z_q \tag{5}$$

where η is learning constant. The weight between the input layer and the hidden layer will be updated as Eq. (6):

$$\Delta v_{qj} = \eta \sum_{i=1}^{n} ((d_i - y_i) a'(net_i) w_{iq}) a'(net_q) x_j \tag{6}$$

3. The proposed algorithm

The standard of ISO/IEC 27005 is mainly to explore the steps and methods for the risk management of information security. It proposes to use information assets, threats, and vulnerability for risk assessment. In this paper, we also use these 3 aspects to evaluate risk for information security. The use

of Internet services, information systems, and data transmission can generally be regarded as valuable that is called information assets. For these information assets, like other important valuable assets, should be properly protected. The most important aspects of information assets are confidentiality, integrity, and availability. In addition, there could also involve some qualities such as authentication, accounting, non-repudiation, and reliability [1]. The assessment of confidentiality is shown in Table 1. The assessment of integrity is shown in Table 2. The assessment of availability is shown in Table 3. After the completion of above 3 assessments, the maximum value of these assessments shall be taken as the value of the information asset.

In this paper, we propose the improved neural network for the risk assessment of information security. The flowchart of the proposed algorithm is shown in Figure 2. In the flowchart, we use BPN with one hidden layer as the main architecture for the risk assessment of information security. For BPN, there are many parameters that need to be well adjusted to achieve good risk assessment performance, such as the number of neurons of hidden layer, the weights between input and the hidden layer, and the weights between hidden layer and output neuron. Particle swarm optimization (PSO) is easy to implement with few parameters, and it has been successfully applied in many fields. In the proposed algorithm, we use PSO to adjust these parameters. For PSO, each particle has a position and velocity vector. In n-dimension, the position P_i^n and velocity V_i^n of the i^{th} particle can be explicitly described as $\overrightarrow{P_i} = (P_i^1, P_i^2, \cdots, P_i^n)$ and $\overrightarrow{V_i} = (V_i^1, V_i^2, \cdots, V_i^n)$ respectively. The PSO algorithm is represented as follows [8].

$$V_i^n = \Omega * V_i^n + \theta_1 * \pi * (pbest_i^n - X_i^n) + \theta_2 * \pi * (gbest^n - X_i^n) \tag{7}$$

$$P_i^n = P_i^n + V_i^n \tag{8}$$

where Ω is called inertia weight, θ_1 and θ_2 are real numbers, π is a random number in [0,1], $pbest_i = (pbest_i^1, pbest_i^2 \cdots, pbest_i^n)$ is the best position for the i^{th} particle, and $gbest = (gbest^1, gbest^2 \cdots, gbest^n)$ is the global best position.

4. Simulation results

For the risk assessment of information security, it is related to the value of information asset, threat, and vulnerability. Threat refers to the damage caused by the information security of the harmful event. It is shown in Table 4. Vulnerability is the weakness of using information assets. It is shown in Table 5. To calculate the final risk value, it is done by the product of the value of information asset, likelihood of occurrence, and level of impact [1].

This paper uses the proposed algorithm to calculate the accuracy for the risk assessment of information security. There are 22 attributes and 84 records for the risk assessment of information security. We use 54 records for train data and 30 records for test data. Three learning algorithms of decision tree (DT), support vector machine (SVM), and BPN are implemented for comparing results in this paper. The decision tree, known as the classification tree, is an inductive learning method that can analyse and classify data from entropy. It takes the concept of a tree into account and produces interpretable rules [9]. Based on the principle of structural risk minimization, SVM is mainly for classification issues. It finds a hyperplane in high dimensional states to divide data into different classification to get the best accuracy [10-11]. The result of classification accuracy is shown in Table 6. In Table 6, it finds that the improved neural network has the best classification accuracy.

5. Conclusions

This paper proposed the improved neural network for the risk assessment of information security. In the proposed method, we use BPN as the main architecture to classify data and use PSO to adjust the

best values of parameters of BPN. A comparison of classification accuracy with DT, SVM, and BPN. It demonstrates that the proposed algorithm can conduct risk assessment and effectively control the information security risk.

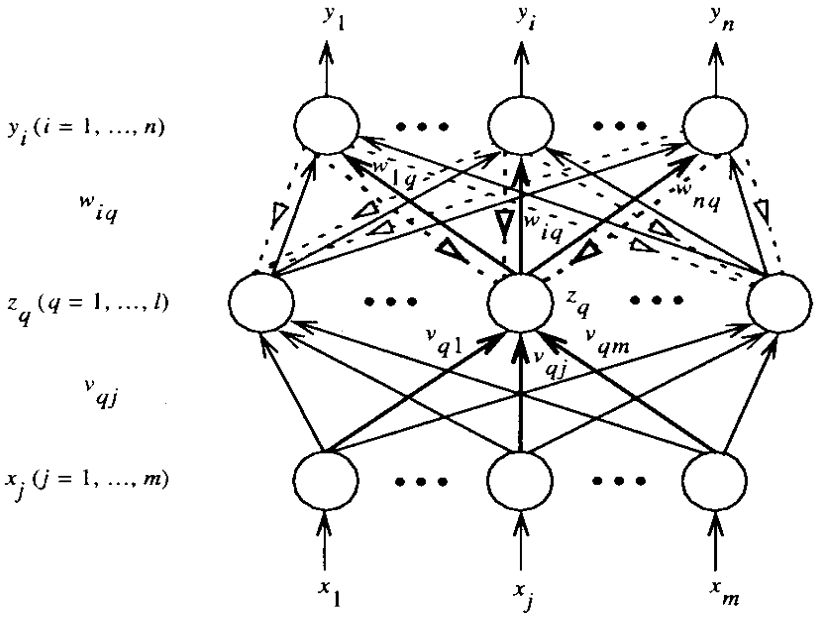

Figure 1. A three-layer BPN neural network

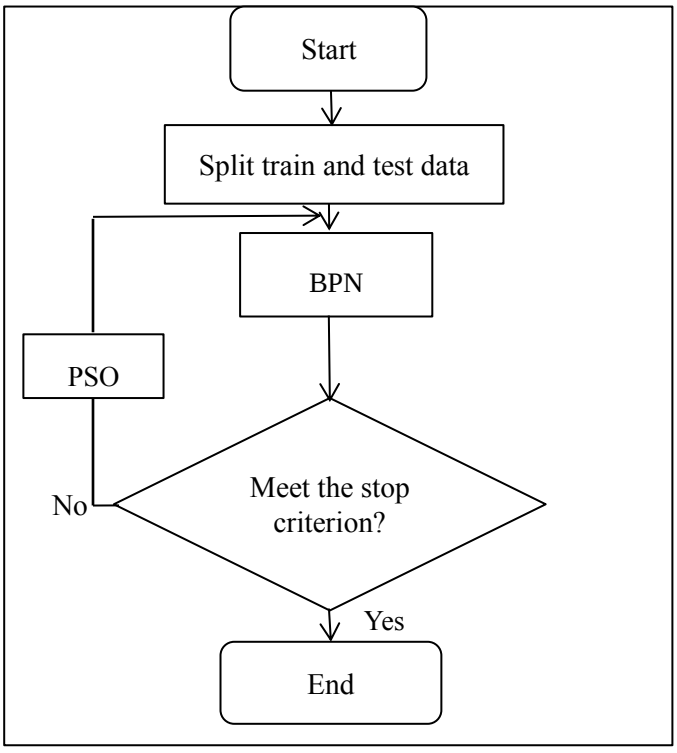

Figure 2. The proposed algorithm

Table 1. The assessment of confidentiality

Number	Item	Value
1	Confidential information assets are not required.	1
2	Information assets containing sensitive information, but no confidentiality	2

	requirements, limited use of internal staff.	
3	Limited use of information assets within relevant department staff.	3
4	Information assets in information, including confidential information regulated by relevant laws or regulations.	4

Table 2. The assessment of integrity

Number	Item	Value
1	The integrity requirements of information assets are very low.	1
2	Information assets have integrity requirements, but will not be damaged by integrity.	2
3	Information assets have integrity requirements that can cause harm if integrity is compromised.	3
4	Information assets have integrity requirements that can disrupt business due to a breach of integrity.	4

Table 3. The assessment of availability

Number	Item	Value
1	Information assets allow for failures of more than 3 working days and do not need to be repaired or alternatives are needed in real time.	1
2	Information assets allow for failures of more than 8 working hours and 3 working days or less, without real-time repair or search for alternatives.	2
3	Information assets allow for failures of more than 4 working hours and less than 8 working hours, without real-time repair or search for alternatives.	3
4	Information assets allow for failures of more than 4 working hours, without immediately repair or to find alternatives.	4

Table 4. The assessment of threats

Number	Item	Value
1	Possibility of it happening once a season.	1
2	Possibility of it happening once a month.	2
3	Possibility of it happening once a weak.	3

Table 5. The assessment of vulnerability

Number	Item	Value
1	This weakness is not easily exploited by threats.	1
2	This weakness is vulnerable to threats.	2
3	This weakness is very vulnerable to threats.	3

Table 6. The classification accuracy of test data

Number	Method	Classification accuracy
#1	DT	83.3%
#2	SVM	89.1%
#3	BPN	90.%
#4	The proposed algorithm	93.33%

Acknowledgment
This research was supported by Fuzhou City research Grant No. 2019-SG-6. It was partially supported by 2020 and 2019 Fujian Province research Grant No. FBJG20200371 and FBJG20190284. It was also supported by Fuzhou University of International Studies and Trade research Grant No. 2018KYTD-02 and FWB19003.

References
[1] Chang L Y and Lee Z J 2013 Applying fuzzy expert system to information security risk

Assessment-A case study on an attendance system *2013 IEEE International Conference on Fuzzy Theory and Its Applications* p 346
[2] Bojanc R and Jerman-Blažič B 2013 A quantitative model for information-security risk management *Engineering Management Journal* **25** 25
[3] Lee Z J and Chang L Y 2014 Apply fuzzy decision tree to information security risk assessment *International Journal of Fuzzy Systems* **16** 265
[4] El-Khatib M J *et al* 2019 Glass Classification Using Artificial Neural Network
[5] Roblek D *et al* 2019 *U.S. Patent No. 10,467,493*. Washington, DC: U.S. Patent and Trademark Office
[6] Asuntha A *et al* 2019 A hybrid feature extraction approach for the detection of melanoma using neural network *International Journal of Research in Pharmaceutical Sciences* **10** 1836
[7] Maru A *et al* 2020 Effective Software Fault Localization Using a Back Propagation Neural Network *Computational Intelligence in Data Mining* p 513
[8] Dabhi D and Pandya K 2020 Enhanced velocity differential evolutionary particle swarm optimization for optimal scheduling of a distributed energy resources with uncertain scenarios *IEEE Access* **8** 27001
[9] Lee Z J and Lee C Y 2020 A parallel intelligent algorithm applied to predict students dropping out of university *The Journal of Supercomputing* **76** 1049
[10] Huang Y C and Zheng J H 2018 Ball Nut Preload Diagnosis of the Hollow Ball Screw through Support Vector Machine *Adv. technol. innov.* **3** 94
[11] Lee Z J *et al* 2020 A hybrid system for imbalanced data mining *Microsystem Technologies* **26** 3043