The Key Technology of Computer Network Vulnerability Assessment Based on Neural Network

Shaoqiang Wang (wangsq@ccu.edu.cn)

Research

Keywords: Neural Network, Network Vulnerability, Vulnerability Index, Vulnerability Database, Parallel Algorithm

Posted Date: September 11th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-37412/v2

Version of Record: A version of this preprint was published on October 31st, 2020. See the published version at https://doi.org/10.1186/s13638-020-01841-y.

The Key Technology of Computer Network Vulnerability Assessment Based on Neural Network

Shaoqiang Wang*

School of Computer Science and Technology, Changchun University, Changchun 130022, Jilin, China

wangsq@ccu.edu.cn

**Corresponding author*

Abstract: With the wide application of computer network, network security has attracted more and more attention. The main reason why all kinds of attacks on the network can pose a great threat to the network security is the vulnerability of the computer network system itself. Introducing neural network technology into computer network vulnerability assessment can give full play to the advantages of neural network in network vulnerability assessment. The purpose of this article is by organizing feature map neural network and the combination of multilayer feedforward neural network, the training samples using SOM neural network clustering, the result of clustering are added to the original training samples and set a certain weight, based on the weighted iterative update ceaselessly, in order to improve the convergence speed of BP neural network. On the BP neural network algorithm for LM algorithm was improved, the large matrix inversion in the LM algorithm using the parallel algorithm method is improved for solving system of linear equations, and use of computer network vulnerability assessment as the computer simulation and analysis on the actual example, design a set of computer network vulnerability assessment scheme, finally the vulnerability is lower than 0.75, which is beneficial to research on related theory and application to provide the reference and help.

Key words: Neural Network, Network Vulnerability, Vulnerability Index, Vulnerability Database, Parallel Algorithm

1. Introduction

According to the statistics reported by the Internet information center over the years, the number of hacker attacks on computer users worldwide increases by at least 10% on average every year. Network vulnerability analysis is a very complex work, and the correlation among vulnerabilities, the correlation between network hosts, the dynamic nature of network services and the complexity of network connections are worthy of attention. With the increasing attention paid to computer network security, computer network vulnerability assessment has important research and application value.

Due to its inherent super adaptability and learning ability, neural network has been widely studied and applied in many artificial intelligence fields, and has solved many information processing problems that are difficult to be solved by other traditional artificial intelligence methods and technologies. Because of the unique ability of nonlinear adaptive information processing, neural network overcomes the shortcomings of many traditional artificial intelligence information processing methods in pattern recognition, voice information recognition, unstructured information processing and other visual functions, so that it has been successfully applied in many fields of artificial intelligence. The close combination of neural network and other traditional information processing methods of artificial intelligence will greatly promote the continuous innovation and development of related technologies

such as traditional artificial intelligence and distributed information processing.

Several factors must be considered when designing large interconnections. Optimal design is important to achieve good performance and reduce construction and maintenance costs. Real communication networks are prone to network component failures. There are failures between nodes and connections, and network stability is desirable when a limited number of failures do not disrupt the entire system. The vulnerability of network topology is an important aspect of computer network design. Aysun Aytac proposed various methods to quantify network vulnerability and derived network reliability formulas using a large number of graph theory parameters. Based on the control concept in graph theory and the strong and weak control number of transformation graph Gxy+, this paper studies the vulnerability of the interconnection network to the failure of a single node and measures the vulnerability of the network [1]. Attack chart is an effective method to solve many problems in computer network security management. After a vulnerability scanner is used to identify a single vulnerability, the attack chart can relate a single vulnerability to the likelihood of an attack, and then analyze and predict which privileges an attacker can gain through a multi-step attack (in which multiple vulnerabilities are exploited in turn). Teodor Sommestad tested the practical application of this analytical method. The attack graph tool MulVAL obtained information from the vulnerability scanner Nexpose and network topology information from eight virtual organizations containing 199 machines. Two groups of attackers attempted to infiltrate these networks over a period of two days and reported which machines they had damaged and which attack paths they were trying to use [2]. Security metrics are powerful tools for organizations to understand the effectiveness of protecting computer networks. However, most of these measurement techniques are not sufficient to help companies make informed risk management decisions. Abraham proposes a stochastic security framework that allows for quantitative measures of security by considering vulnerability related dynamic attributes over time. Abraham's model is that existing research in attack graph analysis does not take into account the timing of vulnerabilities, vulnerabilities and patch availability, etc., which can be interlinked based on how the entire network is affected by vulnerabilities and leverage compromise systems. In order to more realistically describe the changes of the security state of the network over time, an inhomogeneous model is proposed, which contains a time-dependent covariable [3].

In this paper, based on neural network are studied under the study of computer network vulnerability analysis method and the model of network vulnerability index calculation, on the basis of clear vulnerability index and related concepts, emphatically discusses the vulnerability analysis method and based on the index system of vulnerability and vulnerability database index calculation model, aims to provide a kind of multidimensional network security status display, macro, so that the relevant enterprises and departments in a timely manner to master the Internet network security macro situation.

2.Proposed Method

2.1 Vulnerability of Computer Network

(1) Definition of vulnerability

Computer security vulnerability research is a new field of network security research. In the research process, researchers put forward different definitions according to different understanding and application requirements [4].

1) Software vulnerability

Software vulnerability is essentially a security vulnerability in software, which will endanger the security strategy of the system and eventually reduce the use value of the system [5].

2) Computer system vulnerability

A computer management system consists of a series of state descriptions that ultimately constitute the current initial state configuration of the entity of the computer management system. By using such a set of transitions to the initial states, all the initial states that can be reached from a given initial state are ultimately partitioned by the management system as two types of initial states defined in the security policy. Vulnerability is an authorized state that converts an authorized state to an unauthorized state. The damaged state refers to the state achieved by the above method. An attack is a sequence of authorization state transitions that ends with a corrupted state [6].

3) Network unit vulnerability

Vulnerability of a computer network refers to a set of characteristics of a computer network that can be used by malicious objects (attackers or attack programs) to gain unauthorized access to resources through authorized means and methods in the network, or cause damage to the network and the host network. Network vulnerability comes from the vulnerability of corresponding software providing services in the network and the vulnerability of hosts in the network [7-8].

4) Vulnerability of information systems

In the field of risk management technology system, there are system security process automation management system security automation and management automation, internal risk control, critical events, in the process of penetration can automatically prevent unauthorized access to information or damage the key steps of risk management, risk management weaknesses. Systematic risk management in the technical field. Weaknesses in risk management exist in the process of system physical layout. Organizations, processes, people, management, hardware or software can infiltrate the automatic collection and processing system or data. The existence of the vulnerability itself does not cause any damage to the system. In an automated data attack, the vulnerability of a system is only one or a set of conditions that cause damage or damage to two systems or behaviors. In the field of system risk management technology, any attack or vulnerability or attribute in the risk management system is defective. Any attack or harmful event or dangerous entity can provide a risk management opportunity to attack or implement automated data attacks. In the field of system information security, weaknesses that can be automatically evaluated are those that can be automatically infiltrated to overcome the risk attributes or security attributes of countermeasures [9-10].

(2) Vulnerability assessment

The evaluation of vulnerability is mainly to detect the vulnerability of the system by means of various management and scientific and technological means, to find out the potential security risks and the system vulnerability that may be damaged and utilized by illegal personnel in the process, and to analyze and evaluate the security and development status of the whole system according to the results of various tests. On this basis, according to the results of vulnerability assessment, appropriate security strategy is formulated, which provides reference and basis for the perfect design and implementation of security assessment system. One of the main objectives of vulnerability detection and assessment is to analyze and understand various security risks that may exist in the whole system development process, and to provide scientific basis and intention for how to protect the security and development of the whole system. The whole system vulnerability here can be just one device as a service, or just the device stored on the network as a computer, or the entire computer network [11-12].

(3) Vulnerability analysis method

As shown in Figure 1, from rule-based analysis to model-based analysis, from stand-alone analysis to distributed analysis. There are many methods of vulnerability assessment, which can be

summarized into three categories: quantitative assessment method, qualitative assessment method and comprehensive assessment method combining qualitative and quantitative methods.

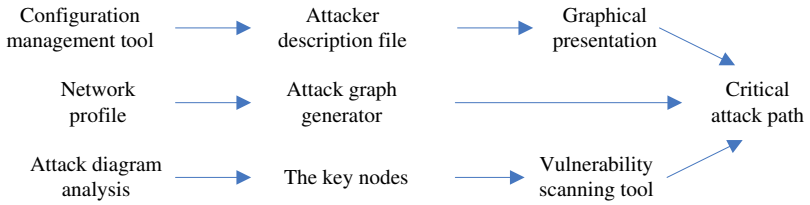

Figure 1. Attack diagram evaluation model

In the attack tree method, the tree structure in the form of and-or is used to model the network vulnerability. The nodes in the attack tree represent the attack, the root node represents the attacker's ultimate target, AND the children of a node represent the methods to achieve this target.

Figure 2 shows an example of an attack tree in which the attacker's goal is to get a free lunch. The AND node represents the conjunction, which means that all its child nodes must meet to achieve the current goal; the OR node represents the disjunction, which means that the current goal can be reached as long as any of its children are satisfied [13].

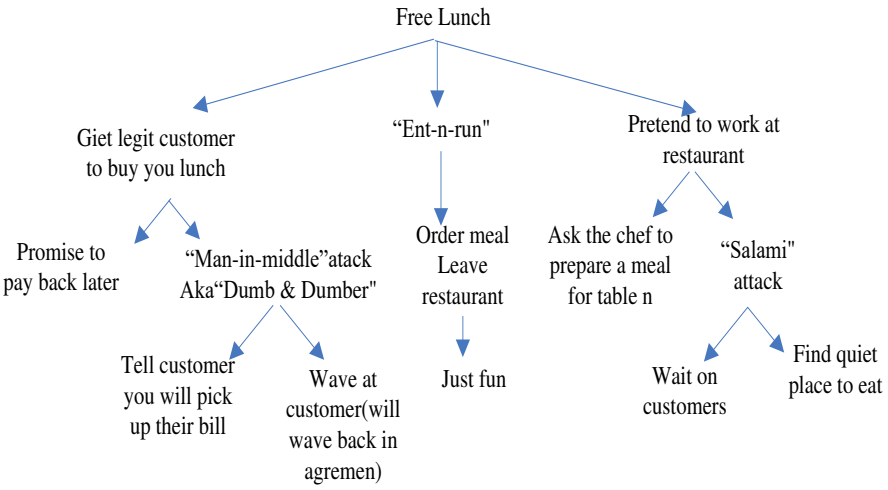

Figure 2. Attack tree method

(4)Model-based quantitative analysis

1) Network elements

Network element c_i is the set of network protocol entity e_i:

$$c_i = \{e_i | u(e_i) = i\}, i, j \in N \quad (1)$$

U is a mapping from the protocol entity to its network node number:

$$u : |e_i| \to N, C \equiv \bigcup_i \{c_i\} \quad (2)$$

2) Connection

There is l_k between c_i and c_j if and only if:

$$\exists e_m, e_n, u(e_m) = i \wedge u(e_n) = j \wedge u(e_m) = h(e_n) = k \wedge e_{ik} \leftrightarrow e_{jk} \quad (3)$$

h is a mapping from the protocol entity to its network level:

$$h:|e_i| \to N, L \equiv \bigcup_k \{l_k\} \quad (4)$$

3) Network

Net is a binary group, net=<C,L>. The vector e_i made up of the variables e_i made up of state $S_j \in S_{ej}$. Marked as safe if the expected value is met; If the expected value is not met but the security attribute of c_i is not destroyed, it is marked as an error state. Sets that do not meet expectations and break c_i's security properties are marked as failing [14-15].

4) Vulnerability point

Vulnerability point v_i is a vulnerability in net and satisfies:

$$\exists t \in T, t(v_i, S_{net}) = S'_{net}, S_{net} \neq S'_{net}, S'_{net} \in S_{net}^{fail} \quad (5)$$

5) Vulnerability

Vulnerability analysis measures the severity of vulnerability points in terms of availability and impact. Availability depends on the degree of vulnerability in W and is affected by the number of indirect precursors of vulnerability. The contribution of the precursor states to availability is inversely proportional to the distance between them and the vulnerability point [16]. Similarly, the influence of the vulnerability can be measured by the number of distances from the vulnerability to all its direct or indirect successor states. Its availability and impact are as follows:

$$a_{vk} = \sum_{i,j} \frac{1}{|U_{ijk}|} \quad (6)$$

$$b_{vk} = \sum_{i,j} \frac{1}{|E_{ijk}|} \quad (7)$$

The severity of a single vulnerability and network vulnerability are as follows:

$$\bar{vk} = a_{vk} + b_{vk} \quad (8)$$

$$\tilde{v} = \sum_k \bar{vk}, k \in N \quad (9)$$

The advantage of the model-based quantitative analysis method of network vulnerability is that it can analyze and calculate the vulnerability independently of network attacks, and can better reflect the degree of network vulnerability [17].

2.2 Neural Network

(1) Characteristics of neural network

1) The structure of neural network is different from that of current computers. It is composed of many small processing units connected with each other. The function of each processing unit is simple. This enables the neural network to be well applied to the parallel computer for calculation, which can greatly improve the speed of calculation [18].

2) Neural network has very strong fault tolerance. If one part of the neural network is destroyed, the overall performance of the network will decrease to some extent, but this does not prevent it from doing its job. The neural network still works. Even if the most important part of the network is damaged, it will not cause the complete loss of the whole network function [19-20].

3) Neural network memory information is stored on the connection weight between neurons, and the content of stored information cannot be seen from a single weight, so it is a distributed storage mode. Effective segmentation based on the training sample and training process, the whole sample set of learning are assigned to a distributed collaborative training neural network cluster environment, at the same time by competitive selection mechanism, makes the individual learning performance good training can effectively migration in the neural network group, in order to obtain more resources for learning.

4) Neural network has excellent imitation ability. Through its excellent imitation learning ability, it is expected that future neural network computers will provide economic prediction, market prediction and benefit prediction for mankind [21].

(2) Neural network model

The neuron model is often described by the first-order differential equation, which can simulate the change of synaptic potential in biological neural network over time:

$$\tau \frac{d\mu}{dt} = -\mu(t) + \sum w_{ij} x_j(t) - \theta_i \tag{10}$$

$$y_i(t) = f[\mu_i(t)] \tag{11}$$

In general, s-type function expressions are used to express the non-linear characteristics of the network:

$$f(\mu_i) = \frac{1}{1 + \exp(-\mu_i / c)^2} \tag{12}$$

As a technology that can carry out adaptive pattern recognition, neural network learning not only needs to provide the experience analysis knowledge of adaptive patterns and neural pattern discrimination function in advance, but automatically forms the learning and decision-making region required by the neural network through its own neural network learning and decision-making mechanism [22]. The structure and characteristics of neural network are determined by its topology structure, neuron characteristics, learning and decision-making training rules and other factors. By making full use of the neuron information of different states, it can learn and train the neuron information of different states in the network one by one to obtain certain state mapping and relationship. In addition, network mapping can be continuously learned, and if the environment in the network changes, the mapping can also adjust the environment accordingly [23].

For fault diagnosis based on neural network, the input node of the network corresponds to the fault symptom, and the output node corresponds to the fault cause. First, the network was trained with a set of fault samples, and its structure (transfer function of the middle layer and number of neurons) and parameters (connection weights and thresholds between neurons) were determined [24-25]. Fault mode classification is a process of realizing nonlinear mapping between symptom set and fault based on a group of signals after network training, as shown in Figure 3.

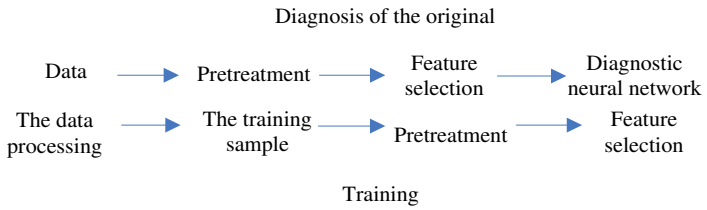

Figure 3. Design of network nonlinear mapping process

3.Experiments

3.1 Experimental Background

This system is mainly designed and developed on the platform of virtual resource environment provided by network shooting range. From the performance, platform compatibility considerations, in order to make the network range to provide users with the required test platform and realize the Metasploit adding auxiliary module Nmap and the function of the Nessus system mainly adopts the NS and Ruby script language, the NS script is established in order to realize the automation of network range experiment platform, the Ruby language is in order to achieve the load based on the framework of Metasploit existing auxiliary module Nmap and Nessus. In the structure of the whole software transaction management system, it adopts the browser/front-end server (B/S) structure. B/S structure of management system is characteristic of this structure is one of the more popular software architecture, in this architecture, the processing of the user interface is implemented directly by the user and the browser, few major transaction logic to handle the user and the front-end server implementation, the other major transaction logic processing in the user and the server side implementation, it has the advantage that can well realize different people and from different time and place of user access.

The system is based on a set of system platform of real equipment, accurately determine the weapons and equipment evaluation and training, completed the system platform, the file data layer and the combination of application service layer, the second is to build a high controllability, high availability, high reliability, system platform structure system, the system platform of network structure form domain includes the attack and defense domain and target domain. It includes six key function modules: hardware resource control, simulation and virtualization, operation control, detection and collection, evaluation and analysis, and network platform system display. The test process of network shooting range can be roughly divided into the following seven steps: determination of user needs, determination of experimental tasks, operational deployment, resource allocation, operational experiments, data collection and analysis and evaluation. All of the above are deeply explored by the system.

3.2 Experimental Design

(1) Determine the number of neurons in the input layer

The input layer parameters of specific problems are used to determine the number of neurons in the input layer, and the number of evaluation indicators is generally used. The number of neurons in input layer which is a three-level index number of network vulnerability evaluation indexes, the Table 1 shows that the degree of sensitivity involves 13 evaluation indexes, their coping capacity involves 15 evaluation index, so the sensitivity degree of BP neural network has 13 input neurons, their coping capacity BP neural network has 15 input neurons.

Table 1. Main parameters of BP neural network evaluation model

Input neuron	Implicit transfer function	Hidden layer neuron	Output layer transfer function	Output layer neuron	Algorithm	Learning rate	The performance function
13	logsig	7	logsig	1	traingdx	0.07	mse
15	logsig	8	logsig	1	traingdx	0.07	mse

(2) Determine the number of neurons in the output layer

The number of neurons in the output layer is the evaluation result of network vulnerability, namely 1. The evaluation of computer network vulnerability is a process from qualitative to quantitative to qualitative. The simulation results of sample setting are shown in Table 2, while the simulation results without weight setting are shown in Table 3.

Table 2. Sample simulation results

A1	A2	A3	A4	A5
0.2	0.597	0.191	0.697	0.232
0.3	0.218	0.650	0.479	0.238
0.3	0.174	0.710	0.954	0.196
0.7	0.498	0.301	0.973	0.131

Table 3. Sample simulation results without set weights

B1	B2	B3	B4
0.0080	0.4288	0.0014	0.9599
0.7484	0.0000	0.0000	0.0000
0.0000	0.8237	0.0006	0.0051
0.0008	0.0000	0.9254	0.0321

(3) Number of hidden layer neurons

In BP network, the selection of the number of hidden layer neurons is very important, which not only has a great impact on the performance of the established neural network model, but also is the direct cause of "overfitting" in training. However, there is no scientific and universal method to confirm it theoretically. At present, most formulas calculate the number of hidden layer neurons in the case of arbitrarily large number of training samples presented in most literature, and most of them are most unfavorable in the case that it is difficult to meet the general engineering practice and not suitable for use.

(4) The learning rate affects the stability of the system learning process

Large network learning rate may directly lead to the excessive weight correction of network weights, and may even directly lead to the incomplete convergence of network weights due to the irregular jump of the minimum value beyond a certain weight error in the process of each correction.

However, too small learning rate may lead to a relatively long learning time for weights, which can well ensure that weights converge to the minimum value of some error. If the learning rate is too small, it may lead to a slow rate of weight convergence, leading to a relatively long time for weight training. If the rate of weight learning is too high, it may directly lead to the instability of the system, and may also cause the system to iterate violently. At the same time, the initial training needs to be effective network learning operation speed, later training may not be appropriate. Therefore, the general training tends to select a smaller network learning rate to ensure the stability and convergence (that is, the stability of the system) of the network learning system, usually between 0.01 and 0.8.

4.Discussion

4.1 Network Vulnerability Assessment and Analysis Based on BP Neural Network Algorithm

Because BP neural network algorithm is very sensitive to network structure, different network structures have different solving abilities. The more complex the neural network, the better its ability to deal with complex nonlinear problems, but the longer the training time. If the neural network structure is too simple, the network training is difficult to convergence or convergence time is too long. The topology of neural network includes the number of layers, the number of neurons per layer and the connections between neurons. In the BP network structure, the number of input neurons and output neurons is determined by the problem itself. Therefore, the design of BP network structure focuses on determining the number of hidden layer and the number of hidden layer neurons. The choice of the number of hidden layers depends on the complexity of the problem, and the relationship is shown in Figure 4. The research shows that the increase of hidden layer can improve the ability of the network to solve complex nonlinear problems, but too much hidden layer can prolong the learning time of the network. For BP network, according to Kolmogrov theorem, three-layer BP network can complete arbitrary mapping from n dimension to m dimension, and implicit layer can meet the requirements. A hidden layer neural network, as long as the number of hidden layer neurons is reasonable, can meet the accuracy requirements. If the number of hidden layers changes from 1 to 2, it will not affect the accuracy much, but will make the network structure more complex and the training time will be greatly prolonged.

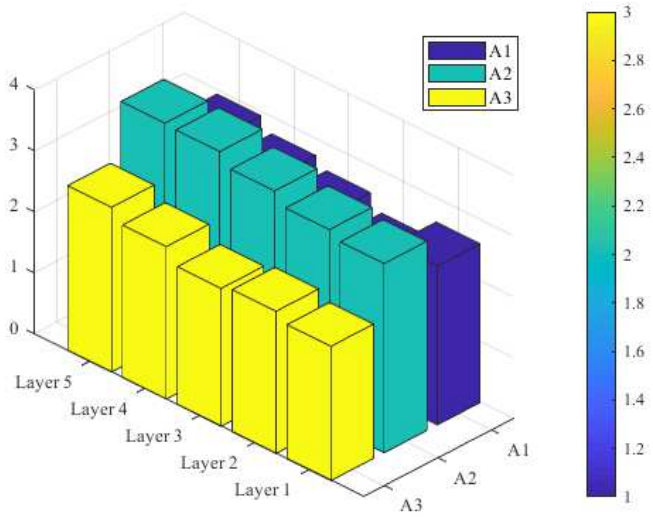

Figure 4. Changes of hidden layer neurons and layer number under BP neural network

The representation and number of the input hidden layer neurons and the output hidden layer neurons of the neural network are determined by the problem itself and the requirements and representation of the data. Number of hidden layer neurons representation selection and parsing is a very complex mathematical problems, it and the requirement to the problem, the representation of a neural input layer and output unit type and the number is a direct relationship, often need to be based on the experience of the system designer and neural unit to determine, with the results of the experiment many times and therefore not may be an ideal implicit layer analytical formula for said. Because the expression and number of hidden layer neurons are too many, the learning time is too long, the error is not necessarily the least, and the fault-tolerant and weak generalization ability may also be directly caused. Therefore, it is necessary to have an optimal number of hidden layer neurons.

According to the range of five grades of sensitivity index, 10 sets of data were randomly generated for each grade, and a total of 50 samples were formed. Choose one sample from each grade of sample (a total of five sample: sample 10, 20, 30, 40 samples, sample sample sample 50) as the test sample, the rest of the 45 samples as the training sample, make all kinds of samples were distributed evenly, solved the BP neural network evaluation model is set up without enough training samples and test samples. The sample processing of "self-coping ability" is similar, and the specific sample results are shown in Figure 5.

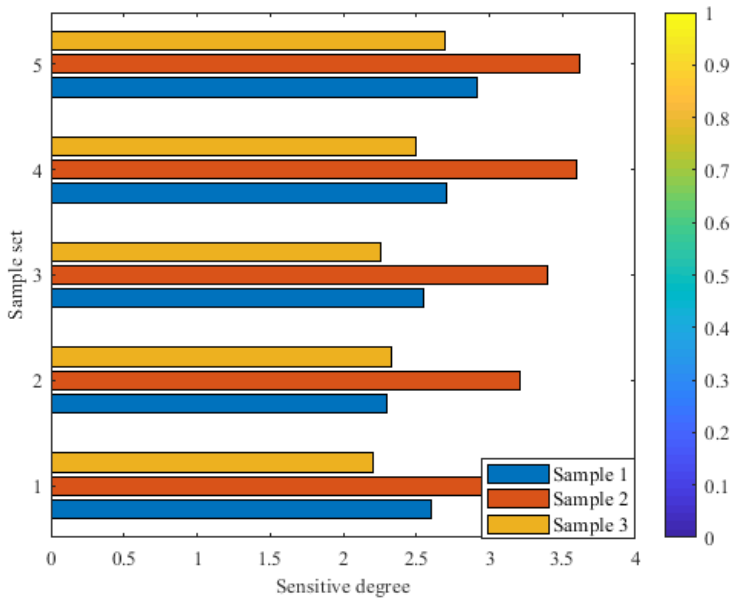

Figure 5. Sensitivity level sample training results

4.2 Network Vulnerability Assessment and Analysis Based on SOM Neural Network Algorithm

Analysis of computer network interface failure, interface generally four reasons of failure, B1 interface problem, B2 network fault, B3 equipment existing congestion and B4 communication protocols are not compatible to as SOM neural network output node, MIB - 2 of 2 interface state of five signs, A1 interface problem, characteristic values of A2 type A3 output characteristic values of A4 network utilization and A5 unknown agreement rate as input nodes of networks, the fault training result is shown in Figure 6.

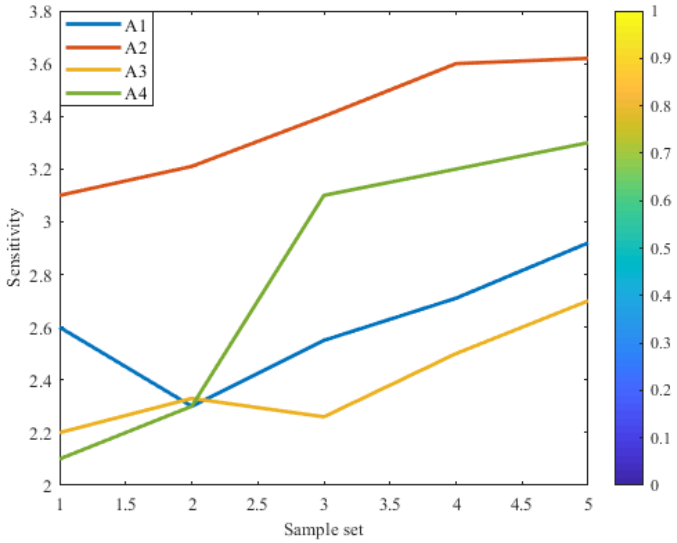

Figure 6. Training results of network fault samples

Since the SOM neural network is learning without teachers, the network will automatically cluster it. The number of network input vector elements is 5, ranging from [0,1]. In order to improve the network mapping and achieve the best clustering effect, the competition layer of the network is designed as a 4×3 structure after multiple neural network training. The number of training steps affects the clustering performance of the network. Here, the training times are set to 100, and the results are shown in Figure 7. The training function of neural network toolbox in MATLAB is used to train the SOM neural network. With the increase of training steps, the distribution of neurons is gradually reasonable. After the network training, the weights are fixed. After each input value, the network will automatically cluster it.

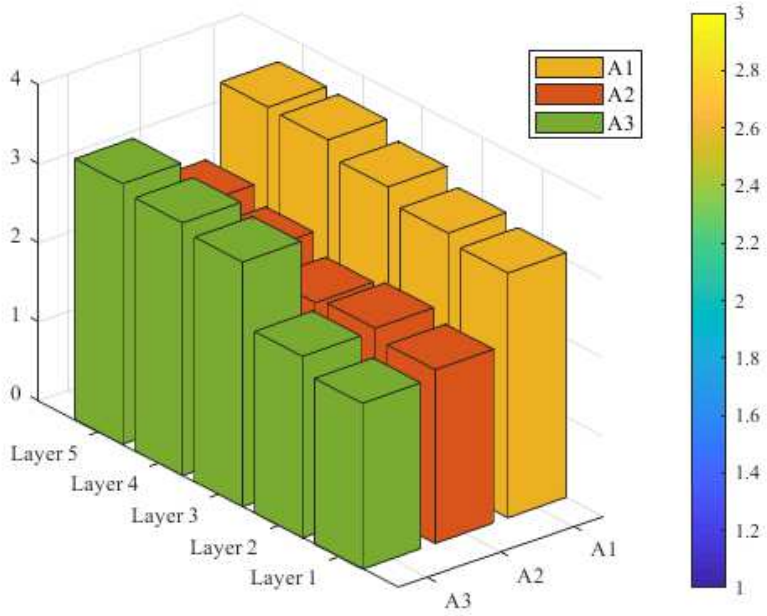

Figure 7. sample training results under SOM network

For the above after the weighting of training samples, the trained BP neural network is used in the simulation, for general need simulation data samples, the neural network training time for each training sample P two updates, the original R the elements of the columns Q transformation into the column vector R + 1, thus increasing the one-dimensional elements, make of the neural network input node number R + 1. In the simulation with the trained neural network, one dimension should be added to each sample to be simulated. Since the clustering of the samples to be simulated could not be known in advance, the added one-dimensional data should be set to the same value 1 to reflect the same clustering characteristics. When setting the weight of the sample, the pre-set weight in the training is also used to improve the sample data.

5.Conclusions

With the popularization of the Internet, the rapid dissemination and sharing of information has been realized, which makes people's work and life more convenient and promotes the progress of the society. With the development of 3G, 4G and fiber optic broadband, the network speed has been greatly improved, the construction of enterprise informatization has been promoted, and the competitiveness of enterprises has been improved. However, while the Internet brings us convenience, there are also many security risks, such as website information leakage, software vulnerabilities, hacker attacks and other network threats, which bring serious economic losses to people. Therefore, accurate network security assessment and effective security defense strategy become very urgent and necessary.

In order to predict the possible attack path and make quantitative evaluation, this paper establishes an attack graph model based on neural network. In the attribute attack graph, an algorithm to eliminate the attack cycle is proposed, and a method to transform the acyclic attribute attack graph into a bayesian network is proposed. This model takes network security state data as input, obtains all possible attack paths, and USES bayesian formula to calculate the probability of each attack path, so as to quantitatively evaluate the vulnerability of the network. Network administrator according to the forecast results, targeted to strengthen network security.

In this paper, the fault diagnosis of computer network is studied, and the computer network fault is simulated by using SOM method and BP neural network method. Based on the SOM neural network belongs to the self-organizing network of competitive learning, and it is not necessary to specify in advance the fault type of training samples for the fault diagnosis of computer network, so it has good clustering ability. SOM neural network and BP neural network are effectively combined by adding weights, and LM algorithm is improved by using parallel algorithm. It is significant to diagnose by example.

Declarations

Availability of supporting data: We can provide the data.

Competing interests

These no potential competing interests in our paper. And all authors have seen the manuscript and approved to submit to your journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Funding

This work was supported by Science and technology project of education department of Jilin province, Research on key technologies of network vulnerability assessment, JJKH20180950KJ.

Author's contributions

The author Shaoqiang Wang wrote the first version of the paper.

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Author details

Shaoqiang Wang, School of Computer Science and Technology, Changchun University, Changchun 130022, Jilin, China

References

[1] Aysun Aytaç, Tufan Turaci, Department of Mathematics, Ege University, 35100, Izmir, Turkey 2Department of Mathematics, Karabuk University, 78050, Karabuk, Turkey. Vulnerability Measures of Transformation Graph G xy +[J]. International Journal of Foundations of Computer Science, 2015, 26(06):1550037.

[2] Teodor Sommestad, Fredrik Sandström. An empirical test of the accuracy of an attack graph analysis tool[J]. Information & Computer Security, 2015, 23(5):516-531.

[3] Abraham, Subil, Nair, Suku. A Predictive Framework for Cyber Security Analytics using Attack Graphs[J]. International Journal of Computer Networks & Communications, 2015, 7(1):266.

[4] Pardeep Bhandari, Manpreet Singh. Formal Specification of the Framework for NSSA[J]. Procedia Computer Science, 2016, 92(2):23-29.

[5] Buthaina Mohammed. Penetration Testing of Vulnerability in Android Linux Kernel Layer via an Open Network (Wi-Fi)[J]. International Journal of Computer Applications, 2016, 134(6):40-43.

[6] Wei Gao, Juan L. G. Guirao, Yao Jun Chen. A Toughness Condition for Fractional (k, m)-deleted Graphs Revisited[J]. Acta Mathematica Sinica, 2019,25(2):323.

[7] Li, Q., Sun, B., Chen, M. et al. Detection malicious Android application based on simple-Dalvik intermediate language. Neural Comput & Applic 31, 185–194 (2019).

[8] Alan Kuhnle, Tianyi Pan, Victoria G. Crawford. Pseudo-Separation for Assessment of Structural Vulnerability of a Network[J]. Acm Sigmetrics Performance Evaluation Review, 2017, 44(1):13-14.

[9] Sanjib Sur, Vignesh Venkateswaran, Xinyu Zhang. 60 GHz Indoor Networking through Flexible Beams[J]. Acm Sigmetrics Performance Evaluation Review, 2015, 43(1):71-84.

[10] Soltan S, Yannakakis M, Zussman G. Joint Cyber and Physical Attacks on Power Grids:Graph Theoretical Approaches for Information Recovery[J].International Journal of Computer Applications, 2015, 43(1):361-374.

[11] Xiaowen Gong, Junshan Zhang, Douglas Cochran. Optimal Placement for Barrier Coverage in Bistatic Radar Sensor Networks[J]. IEEE/ACM Transactions on Networking, 2016, 24(1):259-271.

[12] Halappanavar, Mahantesh, Cotilla-Sanchez, Eduardo, Hogan, Emilie. A Network-of-Networks Model for Electrical Infrastructure Networks[J]. Computer Science, 2015,22(2):265.

[13] P. Sanò, G. Panegrossi, D. Casella. The Passive microwave Neural network Precipitation Retrieval (PNPR) algorithm for AMSU/MHS observations: description and application to European case studies[J]. Atmospheric Measurement Techniques, 2015,62(1):442-445.

[14] Yina Ma, Bingfeng Li, Chenbo Wang. Allelic varation in 5-HTTLPR and the effects of

citalopram on the emotional neural network[J]. British Journal of Psychiatry the Journal of Mental Science, 2015, 206(5):32.

[15] Xiaogang Yang, Francesco De Carlo, Charudatta Phatak. A convolutional neural network approach to calibrating the rotation axis for X-ray computed tomography[J]. Journal of Synchrotron Radiation, 2017, 24(2):422.

[16] S. Kahraman. Estimating the Penetration Rate in Diamond Drilling in Laboratory Works Using the Regression and Artificial Neural Network Analysis[J]. Neural Processing Letters, 2015, 43(2):211.

[17] N. Yuan, P. Yang, Z. Liu. Gait recognition by the mean impact value and probability neural network[J]. Harbin Gongcheng Daxue Xuebao/journal of Harbin Engineering University, 2015, 36(2):181-185.

[18] Jiang Qiangrong, Qiu Guang. Graph Kernels Combined with the Neural Network on Protein Classification[J]. Journal of Bioinformatics and Computational Biology, 2019,35(10):56-62.

[19] Zhao,Chang Long, Guan,Xue Song. The Prediction of Surface Roughness of Parallel Machine Tools Based on the Neural Network[J]. Applied Mechanics & Materials, 2015, 556-562:1328-1331.

[20] Leonardo Felizardo, Afonso Pinto. A Study on Neural Network Architecture Applied to the Prediction of Brazilian Stock Returns[J]. Papers, 2019,42(3):113.

[21] S Gavrylenko, O Babenko, E Ignatova. Development of the disable software reporting system on the basis of the neural network[J]. Journal of Physics Conference Series, 2018, 998(1):012009.

[22] Hayder M, Tony Han, Naz E. Hybrid Algorithm for the Optimization of Training Convolutional Neural Network[J]. International Journal of Cross Cultural Management, 2015, 6(10):343-359.

[23] Yajun Xu, Fengmei Liang, Gang Zhang. Image Intelligent Detection Based on the Gabor Wavelet and the Neural Network[J]. Journal of Computational & Theoretical Nanoscience, 2016, 8(11):130.

[24] LI Zhong, LIU Ming-de, JI Shou-xiang. The Identification of the Origin of Chinese Wolfberry Based on Infrared Spectral Technology and the Artificial Neural Network[J]. Spectroscopy & Spectral Analysis, 2016,26(3):423.

[25] H. Xing, S. Zou, W. Xu. The temperature compensation for humidity sensor based on the PSO-BP neural network[J]. Chinese Journal of Sensors & Actuators, 2015, 28(6):864-869.

Shaoqiang Wang was born in Changchun, Jilin, P.R. China, in 1976. He received the bachelor‘s degree from Changchun University of Technology, P.R. China. Now, He works in School of Computer

Science and Technology, Changchun University. His research interests include information security and big data analysis.
E-mail: wangsq@ccu.edu.cn
Figure

Abbreviations used in this paper
browser/front-end server (B/S)

Figures

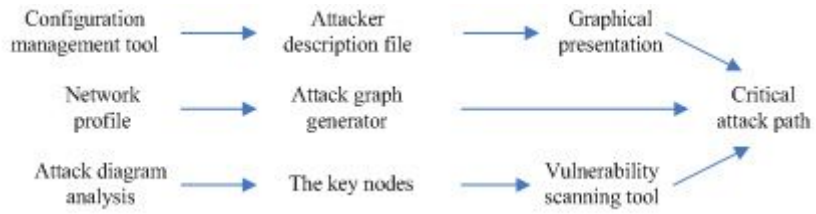

Figure 1

Attack diagram evaluation model

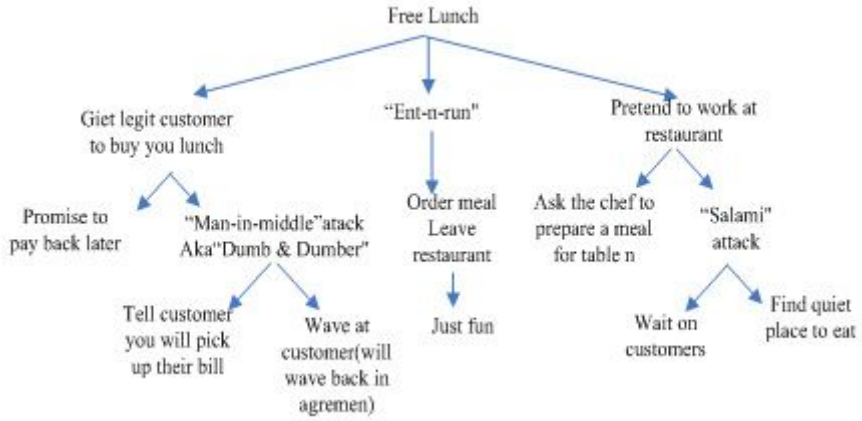

Figure 2

Attack tree method

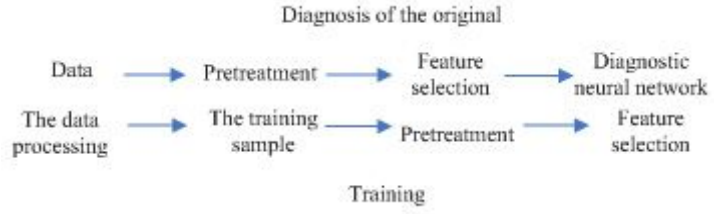

Figure 3

Design of network nonlinear mapping process

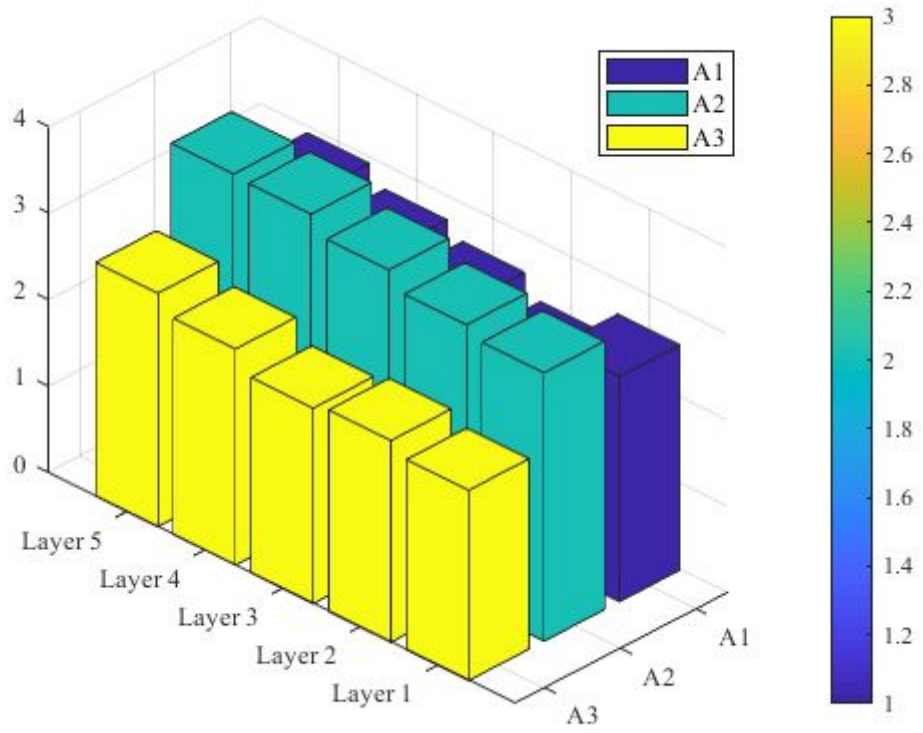

Figure 4

Changes of hidden layer neurons and layer number under BP neural network

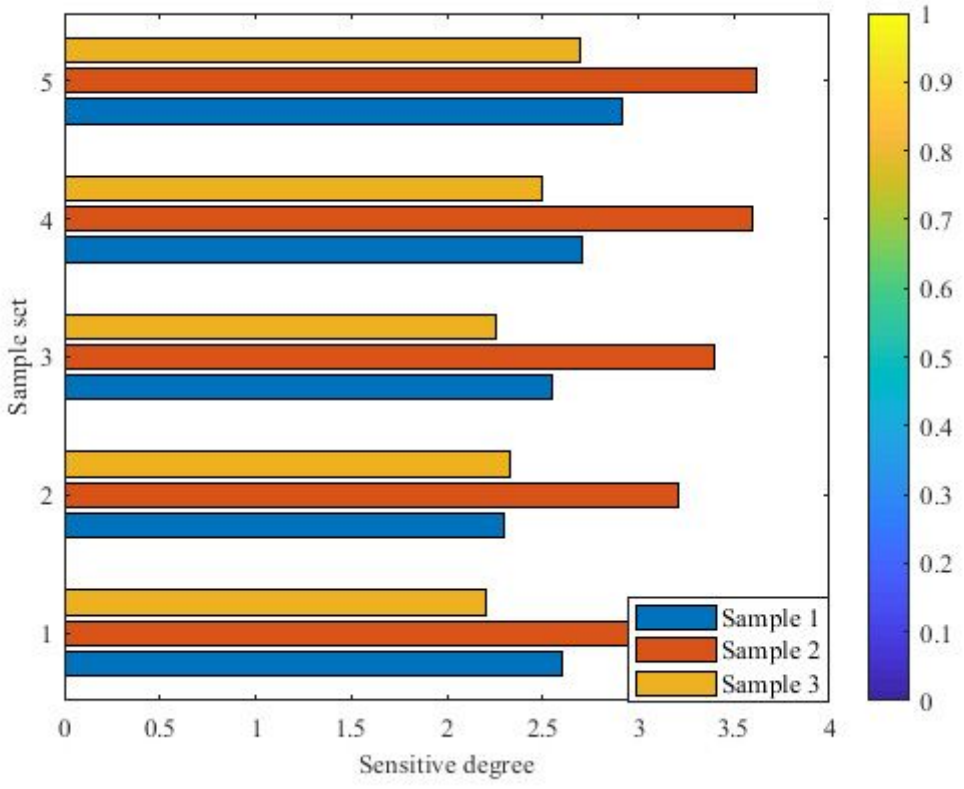

Figure 5

Sensitivity level sample training results

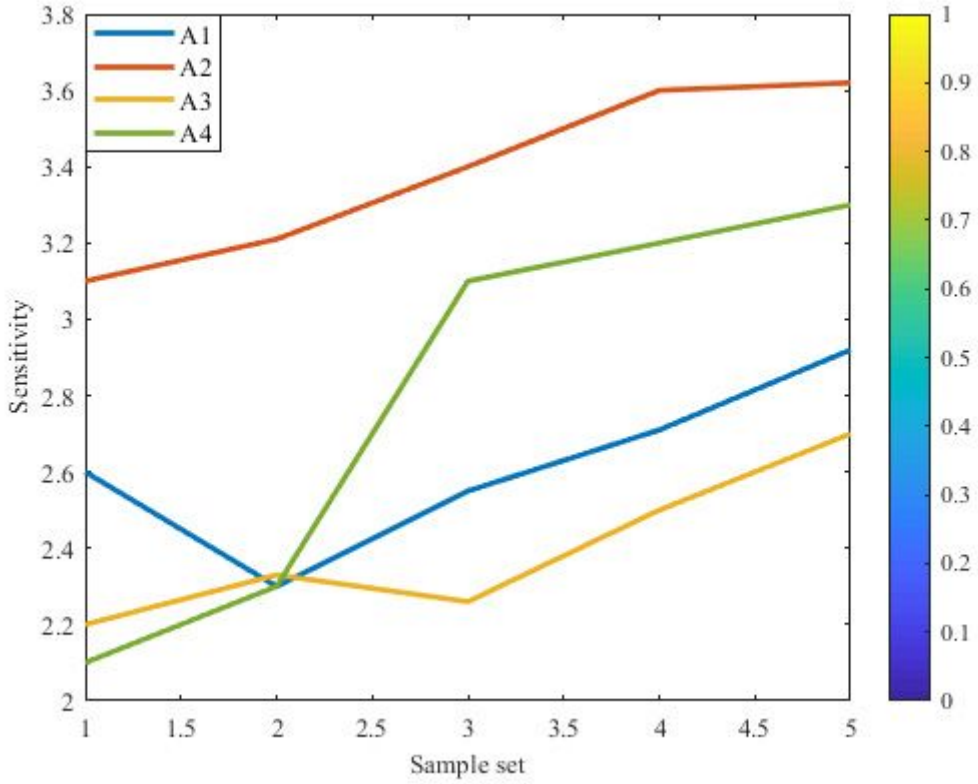

Figure 6

Training results of network fault samples

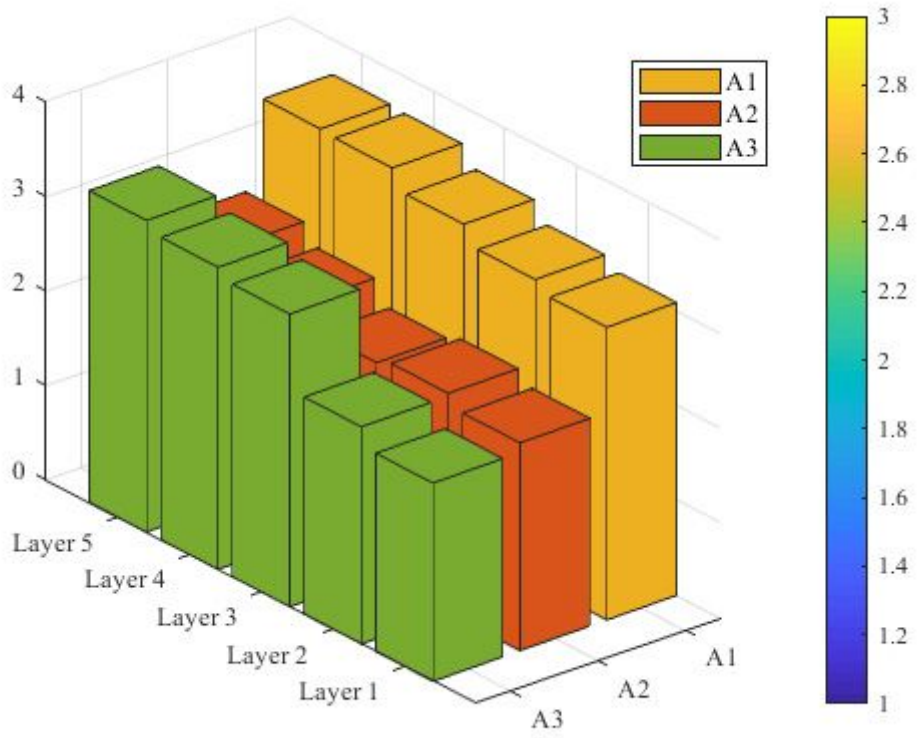

Figure 7

sample training results under SOM network