International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.193-202
http://dx.doi.org/10.14257/ijsia.2016.10.5.18

Intrusion Detection Method based on Improved BP Neural Network Research

Zhu YuanZhong

Electrical and Information Engineering Department of Beijing Polytechnic College Beijing China
Zyz107@163.com

Abstract

With the development of computer network technology, more closely the relationship between people and network.The current network security problem has also been gradually into the public's field of vision, actively carried out on the network intrusion detection becomes an important direction of the development of the network security technology.On the basis of the original BP neural network, this paper puts forward an improved algorithm, and applied to network intrusion detection. After the test, the method is better than traditional convergence, better performance.

Keyword*: Intrusion detection;The BP neural network;Network security*

1. Introduction

Development of and application of computer and network technology, for computer system security problem more and more attention, because the computer system once destroyed, will cause great economic losses to use unit, and seriously affect the normal work and smoothly.Therefore, to strengthen security and maintenance of the computer system, is one of the important tasks of information construction work.To some extent, the network management is a term can have a variety of interpretation.It can be a part-time administrators occasionally performed on a small network operation, or is a large communications providers, companies and organizations network operating staff all the time.

At present, China's Internet security actual situation still not optimistic.Various network security incidents have increased significantly compared with the same period last year.Number of security vulnerabilities and attacks have risen sharply, we faced by network security problem is more and more serious.Large number of various network security incidents, to break the range widely, explain the public Internet network in our country is faced with more serious security threats.And to benefit for the purpose of network attack will bring more direct economic losses for users.

Intrusion detection is an active and dynamic testing of computer network and system, in order to identify technology, in violation of security policy events can find security problems, identify intrusion, the intrusion alarm, and take the appropriate measures to prevent the intrusion events or make up for the damage caused by the computer and network.The research of intrusion detection technology is developed on the traditional auditing technique, has become an important part of network security technology.In recent years and the future hot topics in the study of network security over a period of time.To do a lot of research in this respect at home and abroad, also have related business products listed.It by collecting and analyzing network behavior, security logs, audit data and other information available on the network and a number of key information in a computer system, check the network or system whether there is a violation of security policy and the signs of being attacked.Intrusion detection as a proactive safety protection technology,

ISSN: 1738-9976 IJSIA

provides the internal attack, exterior attack and misoperation real-time protection, before network system compromised intercept and respond to invasion.Therefore is considered to be the second after the firewall security gate, in the case of does not affect the network performance to network monitoring.Intrusion detection by performing the following tasks: monitoring and analysis of user and system activities;System structure and the weakness of the audit;Recognizing patterns reflect the known attack activities and report to related people;Statistical analysis of abnormal behavior patterns;Evaluate the integrity of the important systems and data files;Operating system audit trail management, and to identify the user violation of security policy[1-4].

Intrusion detection is a rational supplement of the firewall, the help system against network attacks, expanded the system administrator safety management ability, improve the integrity of the information security infrastructure.For a successful intrusion detection system, it not only can make any changes to a system administrator time network information system, also to provide guidelines for network security strategy.More importantly, it should manage, simple configuration, so that the non-professional personnel is very easy to get the network security.In addition, the size of the intrusion detection should be according to the requirements of network security threats, system construction, and changed by.Intrusion detection system, after detection of the invasion will respond in time, including to cut off the network connection, record events and alarm, *etc*.

2. Related Works

2.1. The BP Neural Network

Neural network using the adaptive learning technology to describe abnormal behavior, neurons from a number of simple processing units, by using the weighted connection, interaction of instance can be used to the adaptive or form the weight function of neural network self-learning, so that the network correctly understand and solve specific problems and achieve the best performance.Neural networks can be classified according to different angles, such as according to the topology of the network points, a former type to the network and the feedback network;According to the study way, guiding learning network, without guide learning and reinforcement learning networks;According to the calculation model, mathematical model and cognitive model network;According to the network performance, there is continuous and discrete network, along with the models and determine the type of network.Common neural network model are perceptron network and linear neural network, BP network and radial basis function network, Hopfield network, self-organization network, *etc*.Among them, the BP network model is the most main multi-layer forward neural network learning algorithm, is mainly used in the function approximation, pattern recognition, classification, and data compression, *etc*.At present, in the practical application of artificial neural network, the vast majority of neural network model is based on BP algorithm or its change form.Before the people to master the design of the back propagation network, sensors and adaptive linear network are only suitable for single network model of training.

BP neural network is the forward neural network, in the process of calculating the output value, the input values from the input layer unit can spread step by step forward, through the hidden layer to output layer finally get the output.Prior to the first layer of the network unit and the second layer of all the cells are linked together, the second layer and a layer of cells on its linked, there is no connection between the units in same layer.Forward networks of neurons in the excitation function, can use linear hard threshold function or unit rise of nonlinear function, *etc*.In the process of training, they adjust the weights of the algorithm are adopted with mentor delta learning rule.

After determining the structure of BP network, through the input and output sample set

of network training, i.e. threshold and weight of the network learning and correction, so that the network to achieve the given input/output mapping relation.The learning process of BP network is divided into two phases:

1. Positive communication process: input the known learning samples, by setting the network structure and the last iteration of weights and thresholds, from the first layer of backward calculation of each neuron network output.
2. The back propagation process: the weights and thresholds, modified from the last layer of the forward calculation of weight and threshold effect on the total error, accordingly modify the weights and thresholds.

The above two processes, alternately repeatedly until reach the convergence.Due to error can post back step by step, to correct the weights and thresholds between layer and layer, so the algorithm of error back propagation algorithm.Standard of the algorithm is a kind of learning algorithm of gradient descent, as well as error correction learning rule, its weight correction is along the opposite direction of the gradient error performance[5-6].

2.2. The Improved BP Neural Network Algorithm

Since the BP algorithm is most affected, the most widely used a kind of neural network learning algorithm.Most of the neural network model is based on BP algorithm.BP network is global approximation network, that is, for each input/output data, the network of all parameters need to be adjusted.BP algorithm, in the fixed connection power of the negative gradient direction is in accordance with the current moment, without considering the moment before the gradient direction, which often cause a oscillation and divergence of the learning process, slow convergence speed, easily trapped in local optimal point, into the false saturation state.The improved algorithm is divided into two classes: first, there is improvement method based on gradient descent, we quoted the roll gradient back propagation algorithm to improve and implement;The second type of improved method based on standard numerical optimization, we quoted the LMBP algorithm to improve and implement.Using conjugate gradient algorithm and LMBP algorithm to optimize the BP network, there is a theoretical basis can be implemented to speed up the convergence speed of the network, to make learning time shorten, get rid of disadvantages of the training process in the local optimal point, get the training error smaller.

1. the conjugate gradient algorithm

BP algorithm is minimum mean square error of approximation of steepest descent algorithm, in theory when the step length at any hour, this method will reduce the error to local or global minimum, convergence speed is slow, but when the step length is too small makes the network learning.Ridge and total gradient method is able to overcome to a certain extent, the steepest decline in iteration path is the shortcoming of sawtooth phenomenon, need not calculate or store has two steps.the second derivative information, so it is quite useful in large scale problem.

Conjugate gradient method is used to train neural network called conjugate gradient back propagation algorithm.Among various kinds of optimization algorithm selected different search direction and step length is essential to the convergence of the algorithm, BP algorithm to select the search direction is along the negative direction of the gradient search, while CGBP algorithm using one dimensional search of tiny points obtained by the steepest descent direction to generate the conjugate direction as the search direction, than the steepest descent method has a great improvement on the speed and effect.

2. LMBP algorithm

LM algorithm using jacobian matrix calculation, while the standard BP algorithm using hazen matrix is calculated.Hazen matrix is formed by the second order partial derivative, correct calculation is difficult, difficult to achieve the most advantages when accuracy is not high, when a high dimension calculation hazen matrix inverse matrix of the need to consume more time, limit the practical application of this method.Jacobian matrix by the network error relative to the weights

and biases of a derivative, is hazen matrix approximation matrix, can be spread through the direction of the standard method to calculate.LMBP algorithm is used to minimize the nonlinear function of sum of squares, suitable for the performance index is the mean square error of the neural network training.Because the gradient descent method in the first few steps down quickly, but as close to the optimal value, gradient tends to zero, makes the objective function drops slowly.

2.3. Intrusion Detection Technology

Intrusion detection is refers to through to the behavior, security logs, or the audit data or other information available on the Internet, attempt to detect system into or enter.Intrusion detection is an active and dynamic testing of computer network technology and system to identify the violation of security policy events, can find security problems, identify intrusion, the intrusion alarm, and take the appropriate measures to prevent the intrusion events or make up for the damage caused by the computer and network.At present mainly adopts the international computer security association of the United States the definition of intrusion detection and intrusion detection is through the computer network or computer system in a number of key points to collect information and carries on the analysis, found in the network or system whether there is a violation of security policy and signs were attacked a security technology.Systems designed for this purpose is called an intrusion detection system is the combination of software and hardware of intrusion detection.

According to the data source of intrusion detection system, usually the intrusion detection system is divided into two categories: host-based intrusion detection systems and intrusion detection system based on network.Host-based intrusion detection systems from a single host to extract data analysis as a data source, and intrusion detection system based on network analysis to extract data from the Internet as a data source[7-8].

(1) the host-based intrusion detection system

Host-based intrusion detection system protected by extracting system audit trail run and system log data to analyze invasion and to realize the function of intrusion detection.Can be realized through various methods, such as detection system set up to detect improper system Settings and system Settings unfair changes;Regular checks on the system safety state to find abnormal security status: the host security audit log.The advantage of host-based intrusion detection system is: can accurate analysis of the invasion activity, which can accurate decision is a user and processes the attack on operating system, analysis the cost is small, fast analysis speed.Problems existing in the host-based intrusion detection system is: difficult to manage, for each monitored host configuration and management for all need one by one, requires the system itself should have basic security function and has a reasonable setting, and then you can extract intrusion information;Even if the correct Settings, familiar with the operating system of the attacker after completion of the intrusion behavior is still possible to erase system logs in a timely manner, which has not been found;Testing data sources generally the machine data, it can only detect the host of the invasion, especially powerless to from the underlying the network attack, so the host-based intrusion detection system in the network system has significant limitations.

(2) based on the network intrusion detection system

Intrusion detection system based on network monitoring through the network to realize the data extraction.The intrusion detection system based on network usually consists of multiple single function target monitor, they are placed in different locations in the network, to monitor and analyze network packets, and report to the central console.Due to monitor only run intrusion detection system, they are easy to ensure safety.And ears, the monitor is often designed to run in a secretive manner, so that the attacker is more difficult to find their existence and determine their position.

Based on the advantage of network intrusion detection system is: the system is

transparent for the invaders, can avoid itself by the invaders attack, at the same time, this way of intrusion detection of host less resource consumption.Test system can accomplish real-time traffic analysis and testing network IP packet, can finish the protocol analysis/find/rules matching content, can be used to detect a variety of attacks and sniffing.The problems existing in the intrusion detection system based on network is: high load for a large network produces the phenomenon of packet loss, and therefore may not be able to identify those attacks within the network transmission peak period;For switched networks can't listen to all network packets;Cannot analyze the encrypted network packets;Can only detect one's assault, not to judge whether the attack has been successful.

From the detection method and implementation technology, intrusion detection system can be divided into misuse detection and anomaly detection.

(1) the anomaly detection is through the normal history data of tianjin set or legal behavior model, and then compared it with the current activity behavior, if the deviation degree over a certain range of normal behavior model, think the intrusion behavior.The advantage of anomaly detection is to detect the unknown or new attacks, the dependence of the operating system is small, can detect the misuse of authority type of attack.Drawback is that this method is of high rate of false positives, because of limited training data expresses all behavior of the system.How to choose the right deviation in value, the anomaly detection technology is to improve the detection accuracy.Common anomaly detection methods such as statistical analysis and prediction model, feature selection.

(2) the misuse detection is based on the known intrusion method and system for all kinds of defects based on knowledge, first create a characteristic rule base, according to the rules in the library invasion characteristics of known attacks, matching with the collected data packets.When testing the user or the system behavior match the records in the library, the system will think that this kind of behavior is invasion.This kind of low detection rate of false positives, high non-response rates.Detection ability completely dependent on the characteristics of the rules in the rule base to develop and update, need a lot of time and a deeper knowledge of safe, powerless to new and unknown attack, and characteristics of the library must be constantly updated.Typical misuse detection method with expert system, based on the model and pattern matching and state transition analysis, *etc*.

3. The Intrusion Detection Model based on Improved BP Algorithm

With the development of computer network, solely rely on host audit information for intrusion detection system is difficult to meet the requirement of network security, intrusion detection system based on network are put forward, the detection system based on network traffic, network packets and protocol analysis technology to detect intrusion.System logs for host intrusion detection, the network packets used in the detection of attack in the network.Is the purpose of our design for large-scale distributed intrusion, the intrusion detection model based on network is established.Of the intrusion detection model based on BP neural network is mainly composed of event generator, detection analyzer, module, database and response are shown in figure 1 below[9-11].

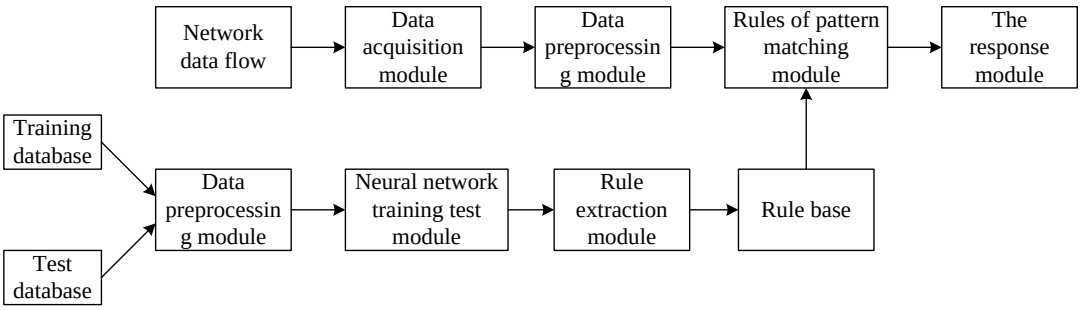

Figure 1. Intrusion Detection Module Architecture

3.1. Data Acquisition Module

As a result of the Ethernet data transmission by radio, usually within a Shared LAN all network interface has the ability to access to all the data on the physical media, but in the system to work normally, the application can only be received packets to the host for the destination address, other don't do processing packets will be discarded, the packet filtering mechanism into the link layer, network layer and transport layer three levels.

Link layer filter mainly refers to the purpose of judging nic driver receives packets MAC address, if not for your network card MAC address, and not for the broadcast address and multicast address, will be discarded directly, not submit to the upper.Network layer whether the destination IP address is bound by the machine's IP address, if it is not bound by the IP address, will not be submitted to the top.The transport layer is to determine whether a target port on the machine is open and if there is no open, will not be made, not submit to the upper.If you want to capture all the packets, you have to bypass the system to work normally, the processing mechanism of direct access to the network layer, the data capture module sets the network card to mixed mode, network card working in this kind of mode can receive all packets through it, regardless of whether the packet destination address for the unit.

3.2. Data Preprocessing Module

Data preprocessing module is responsible for the raw data from the data acquisition module further processing.Divided into protocol analysis, packet feature selection and data processing of three parts.

1. Protocol Analysis

The function of protocol analysis is to identify the packet's protocol type, in order to use the corresponding data analysis program to detect packets.Can put all of the agreements constitute a protocol tree.A particular protocol is a node of the tree structure, a network packet analysis is a path from the root to a leaf node.Maintenance and configuration of tree structure dynamically very flexible protocol analysis functions can be realized.At present, most of the network intrusion detection system for packet network layer, transport layer protocol decoding directly on the contents of the packet data in the area after the pattern matching to detect attacks.Adding rules the advantage of this implementation is simple, easy, high efficiency under the circumstances of less number of rules.But the scope of the data matching is very big, could not resist attacks, a variety of deformation. In the case of increase in the number of rules will be a sharp drop in efficiency.We use a high-level protocol analysis technology, to join the decoding and status of the application layer protocol analysis.

According to the protocol in packet information step by step analysis, parsing out each level agreement, until the application layer.Then according to the agreement's type, the detailed analysis of potential attacks.To do so, although increased the detection

complexity, reduced the matching range, can improve the accuracy of detection, and can detect some unknown attacks deal unusual, can reduce the rate of false positives.

2. Packages Feature Selection

IDS is characterized by identifying communication information in kinds of sample data, usually divided into a variety of, here are some typical case and identification method.

(1) connection attempt from the reserved IP address: through check the source of the IP header address recognition.
(2) with combination of packets: illegal TCP logo sign by contrast in the TCP header set with known marker combination difference to identify right and wrong.
(3) containing special virus E-mail: by comparing each information to identify the theme of the E-mail,. Or through the search area to identify specific names.
(4) the load of DNS query buffer overflow attempt: by parsing the DNS domain and check the length of each domain buffer overflow attempt to identify with the DNS domain.

Use based on the characteristics of the header data, also need to determine which packets to check.Determine the standard is according to actual needs.Because the ICMP and UDP packet are stateless, so in most cases, the need for every staff to inspect them.And TCP packet is connection state, so sometimes can only check the connection of the first packet.Other characteristics such as TCP marks will be different in the dialogue process is different in the packet, if you want to look for signs of special composite value, you need to inspection on each packet.

3. The Data Processing

Some attribute characteristics within the network packet is mainly used to be removed and the conversion of main attribute value characteristic vector neural network can handle, to study module designed neural network training and testing.The main process includes the following steps: (l) according to the attribute feature extraction and decompose the original data.(2) of the original data redundant and irrelevant attributes to remove.Delete unrelated to intrusion detection method based on the attributes, (3) to use neural network to handle symbol field into numeric fields.(4) the normalized processing.In order to reduce due to the large field numerical difference between records for the negative effects of the giant network training[12-13].

3.3. Rule Base Module

Rule base module by the main program calls, mainly the detection rules from the rules of the rule base file into the specified data structure, then to parsing rules and read into memory.Based on the rules of pattern matching in intrusion detection system, for each kind of invasion, need certain model to accurately describe it, in this way can test analysis module according to the rules to match it, if the match is successful, has said it is intrusion behavior.The use of the rules is very flexible, can at any time to add a new rule in the rule base, modify, or delete the original rules;The user can according to the environment of network, network services and the allowed and forbidden requirements of these services they want rules.At present, the description method of detection rules also did not form a unified standard.

Using a two-dimensional chain table stores detection rules, rules of one dimension for head, another dimension for rule option.Rules matching search using recursive method, when packets meet a rule, will trigger the corresponding operation.After the main program rules specified file, calls rules resolution interface functions.This function is only a transitional interface, its main function is to read the rules for each line in configuration file, and sent to the actual rules of the analytical module.Its function is to parse all system configuration rules, including the plug-in configuration, detection rule configuration,

variable definitions, type definitions, *etc*., and all kinds of rules in the rules list, call for testing.

3.4. Testing Analysis Module

In this model, detection analysis module is the rules of pattern matching module.In intrusion detection in the early period of the analysis, we use training data in the database has been established good BP neural network model, then use the test data in the database performance evaluation has already trained neural network model.To meet the performance requirements of neural network to the input data, according to the neural network input node of the input or output node of the output information, neural network can be extracted rules.After the rule extraction according to the format in the rule base.After creating the rule base, the intrusion detection analysis, directly from the rule base rules parsed and tested data from preprocessing module according to provisions of pattern matching[14-15].

4. The Experiment Results Analysis

Use Lincoln laboratory data as test data sets, intrusion detection model and BP neural network for training and testing.Designed an offline network IDS test environment, through the use of large amounts of network traffic samples with various attacks, as input of the IDS system, verify the detection ability of intrusion detection model, and calculates the detection rate and false alarm rate.

The establishment of the neural network model is divided into training and test in two stages.To record data in the training of the neural network experiments in four groups, each group of data including the normal data, Imapd and Teardrop abnormal data types.The first set of selection in the training set 36 records as the training sample data, each kind of data article 12;The second group in the training focus on selecting 60 record as the training sample data, each kind of article 20;The third group in the training set to select 120 records as the training sample data, in each kind of 40.Test, the test set selected 40 normal data, the article 40 Imapd abnormal data and 40 Teardrop abnormal data.In intrusion detection phase, the normal data and abnormal data Imapd, Teardrop detect abnormal data, were selected based on CGBPNN, BPNN model comparing the experimental data of detection, error detection results are shown in table 1.

Table 1. Result of Test

	Model of BPNN			Model of CGBPNN		
	Normal	Teardrop	Imapd	Normal	Teardrop	Imapd
1	1.384	0.981	0.294	0.481	0.006	0.014
2	0.944	0.017	0.421	0.256	0.002	0.026
3	0.913	0.642	0.023	0.205	0.0011	0.033

By the above results, it can be seen that the intrusion detection model based on CGBPNN detection accuracy is much better than that based on BPNN.CGBPNN minimal training sample can make detection model to get a good effect, thus can meet the needs of the training sample size is little, constantly updated, the situation of the real time processing.Especially for normal data detection error is small, intrusion detection of the low rate of false positives.Effectively lower the rate of false positives is intrusion detection based on BP neural network intrusion detection in a problem.CGBPNN model of training time is shorter than BPNN model to improve the detection efficiency.

Experimental data in the training process is divided into three groups: the first group in the training set to select 120 records as the training sample data, each kind of data 40;The

second group in the training set to select 270 records as the training sample data, each kind of article 90;The third group in the training set to select 600 records as the training sample data, in each kind of 200.Test, the test set the selected 40 normal data, the article 40 Imapd abnormal data and 40 Teardrop abnormal data.In test phase, intrusion detection model for normal data, Imapd abnormal data, Teardrop detect abnormal data, were selected based on LMBPNN, BPNN model comparing the experimental data of detection, error detection results are shown in Table 2.

Table 2. Result of Test

	Model of BPNN			Model of LMBPNN		
	Normal	Teardrop	Imapd	Normal	Teardrop	Imapd
1	0.719	0.122	0.112	0.572	0	0.528
2	0.422	0.051	0.188	0.572	0	0.088
3	0.648	0.0635	0.016	0.462	0	0.044

The table shows LMBPNN under the condition of the training samples were enough, intrusion detection system detection accuracy of the model is better than BPNN.LMBPNN shorter training time and enhance the intrusion detection efficiency of the model.In addition, the two models in the lower normal data test error at the same time can significantly increase Imapd abnormal data test error, while the Teardrop abnormal data test error does not change significantly affected.Test error for normal data is low, the intrusion detection of the low rate of false positives, testing for abnormal data error is low, the high rates of detection of intrusion detection, non-response rates low.

5. Conclusion

In this article, we tested the two kinds of network attack, denial of service attacks and buffer overflow attack.These are often seen on the network attack methods, for the attack detection becomes very meaningful.By completing the network attack detection model of the detection accuracy is verified by the experiments, in practice show that two kinds of improved BP algorithm can better application in the network intrusion detection system, can improve the intrusion detection system detection rates and reduce the rate of false positives.

References

[1] C Modi, D Patel, B Borisaniya, *et al*. A survey of intrusion detection techniques in Cloud[J]. Journal of Network & Computer Applications, vol. 36, no. 1, **(2013)**, pp. 42–57.
[2] H J Liao, C H R Lin, Y C Lin, *et al*. Intrusion detection system: A comprehensive review[J]. Journal of Network & Computer Applications, vol. 36, no. 1, **(2013)**, pp. 16–24.
[3] M Ajabi, I Boukhris, Z Elouedi. Big Data Classification Using Belief Decision Trees: Application to Intrusion Detection[J]. Revue Tiers Monde, vol. 33, no. 130, **(2016)**, pp. 429-453.
[4] H Altwaijry. Bayesian Based Intrusion Detection System[M]// IAENG Transactions on Engineering Technologies. Springer Netherlands, **(2013)**, pp. 29-44.
[5] H Altwaijry. Bayesian Based Intrusion Detection System[M]// IAENG Transactions on Engineering Technologies. Springer Netherlands, **(2013)**, pp. 29-44.
[6] Y Niu, Y Xie, X Cao, *et al*. The BP Neural Network Based on Matlab Application in Solar Flare[J]. Journal of Henan Normal University, **(2014)**.
[7] S Wang, L U Yonggang, X Chen. Application of the BP Neural Network Based on Conjugate Gradient Optimization Algorithm in the Identification of High Energy Particles and Other Fields[J]. Nuclear Physics Review, 2014.
[8] H Chang, B Zhang, Univercity J J. Structural Damage Identification Research Based on the BP Neural Network[J]. Journal of Jilin Institute of Architecture & Civil Engineering, **(2014)**.
[9] D Meng, C Fan, J Wang, *et al*. An Improvement to the BP Neural Network Algorithm Based on the Chaos Genetic Algorithm[J]. Mathematical Theory & Applications, **(2014)**.

[10] H Xiang. Research on the BP neural Network of Bus Unsafe Driving Behavior[J]. Telkomnika Indonesian Journal of Electrical Engineering, vol. 3, **(2014)**, pp. 2071-2078.
[11] J T Wang, X U Dan. The forecasting research for the electromechanical equipment spare parts demand based on the BP neural network model and markov chain[J]. Electronic Design Engineering, **(2014)**.
[12] X Ma, Y Qi, W Hu, *et al*. Heat Error Modeling Methods of NC Machine Tool Machining Holes or Slots of Wooden Door Based on the BP Neural Network Algorithms[J]. Scientia Silvae Sinicae, **(2013)**.
[13] Y X Fan, Y E Mao-Zhi, Computer D O, *et al*. Study on the BP neural network initialization[J]. Journal of Shaoguan University, **(2013)**.
[14] Wen S, Zhu L Y. The BP Neural Network PID Control for Application in Dual Temperature Zone of Automated Air Conditioner [J]. Instrumentation Technology, **(2013)**.
[15] Meng H, Ma J, Bao S F, *et al*. Based on the BP Neural Network VAc Synthesis Reactor in Temperature Control[J]. Applied Mechanics & Materials, no. 313, **(2013)**, pp. 1389-1392.

Authors

Zhu YuanZhong. Zhu YuanZhong received the B.Eng degree in Computer and Application from China University of Mining and Technology and the M.Eng degree in Computer application technology from Xiamen University,China in 1995 and 2005. He is an associate professor of Beijing Polytechnic College.His current research interests on Application of computer network and its teaching

