

Research on Weak Fault Detection Algorithm Chaotic Neural Network

Zhu YuanZhong

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

Abstract

Because the network consisting of computers worldwide has its individual network nodes are also unusually large, traditional manual testing methods can not be applied to computer network monitoring, and fault may cause slight paralysis of large-scale networks, for this problem, in this paper, chaotic neural network artificial intelligence monitoring methods for large-scale networks can cause paralysis of the failure to monitor the accuracy of the algorithm is significantly improved compared with other algorithms, and the algorithm converges faster, less calculation, suitable for online testing.

Keywords: *Chaos Theory; weak fault; neural network; accuracy; computation*

1. Introduction

Computer network refers to the number of units distributed independently of each other in different areas of the computer, via a communication link, interactive equipment and related network protocols, the Internet to be able to perform specific functions of complex network systems. The so-called independent, which means that any computer can not completely control the network of other computers, and each computer can freely access the computer network of information resources. Computer network by its very nature, is to communicate with each other to provide a path between a computer, computer network terminal in order to be able to exchange information. Computer network resources by users and communication subnets subnet, the user is responsible for providing the resources and subnet information processing resources, responsible for computer network communication subnet information is transmitted to the computer network. Computer networks inherent structure and specific functions can be completed, the computer determines the distribution network has the following characteristics in a computer network computers in geographical span is usually larger than the computer network computers are functionally independent computer to achieve network interconnection to communicate, communications facilities via the communication network of facilities in general by the communication link and associated transmission switching equipment the exchange of information through computer networks to perform communication infrastructure consisting of, resource sharing interoperability and collaborate. Achieve a variety of user requirements and interoperability thousand or coprocessor is a computer network applications that require a higher level of properties, it needs to have a mechanism to support the process of communication between dissimilar computer systems interconnected network environment interoperability to achieve work and application integration. It requires a computer network topology. Computer network topology computer network is essentially the "skeleton" that is, the computer network hardware facilities of various interconnected physical configuration^[1-4]. The topology of the computer network reliability concepts of computer networks as a systems engineering science, after half a century of development, has formed a relatively complete, robust

system. Scholars at home and abroad to measure the reliability of computer network connectivity grouped into four broad categories of computer networks, survivability of computer networks, computer networks against damaging the effectiveness of computer network components in a multi-mode operation. If the normal operation of computer networks, network infrastructure components must point and provide a reliable link for each user terminal. Thus, the connectivity of computer networks in the field of research related to the reliability of the most widely used. Connectivity computer network is generally used to measure the reliability of a computer network. Computer Network reliability definitions. Within a computer network under the conditions laid down operation mode, maintenance mode, load conditions, temperature, humidity, radiation, etc^[5-7]. specified time hours and a quarter, and so, network connectivity and the ability to maintain communications to meet the requirements, called the computer network reliability . It reflects the ability of computer network topology to support the normal operation of the computer network, it is one of the important parameters of the computer network planning, design and operation. Computer network reliability is defined. Within a computer network under the conditions laid down operation mode, maintenance mode, load conditions, temperature, humidity, radiation, *etc.*, specified time hours and a quarter, where Internet probability of specified functions, called computer network reliability, remember to which the computer network reliability with three types of a terminal reliability, that the probability of the drawing, there is a probability of at least the normal operation of the link between the specified source and sink, terminal reliability, the probability that the figure , set between any two pair of nodes designated brother nodes constituted, have the normal operation of the probability of the link. All - terminal reliability, that the probability of drawing, specify any two nodes households, between the probability of the link are normal operation. Under normal circumstances, the three used to indicate the reliability of the computer network in general.

Chaos is inherent pseudo randomness uncertainty generated by the system, with initial sensitivity, parameter sensitivity, ergodicity. Chaotic systems for these features characterize the main index, entropy topological entropy, entropy measure fractal dimension capacity dimension, information dimension, correlation dimension and other indicators. Analyzing a system is not chaotic system, in addition to the above-mentioned judgment index, the commonly used criterion perturbation method or vaccine methods, see whether the power system horseshoe transform, or whether there is cross with the sink, there is a show that is chaotic. Chaos can be divided into the overall chaotic time, space chaos, chaos, chaos function. Time chaotic motion reflects the complexity of the state space of chaotic reflect the spatial complexity, temporal complexity reflects spatiotemporal chaos, chaos function reflects the complexity of the system output functions.

Impact on the reliability of computer network equipment user. The key to the user terminal is directly facing the user's device, its reliability is critical, but also a reliable computer network or not. In the process of running the computer network maintenance, mainly to ensure reliable user terminal. Ability to interact with the user terminal is higher, the higher the reliability of its network. Such as installing two network cards connected to a different LAN segment than the reliability of a piece of card to be high a lot. Server is the information center and the entire computer network service provider, which typically include database servers, file servers, print servers, email servers, the event server, intestinal servers. These sub-server reliability directly affects the reliability and efficiency of computer networks. In general, the error recovery server, the response time is proportional to its reliability. Improve the reliability of each sub-server at the same time, the server should be dual-switching system that is running in a computer network system, using two servers, one as the master and the other as a backup machine. Although doing so will cause a computer network cost increases, but the reliability of the corresponding

computer network increases.

Reliability of transmission switching equipment for computer networks. In computer networking, operating practice, researchers often find "computer network problems caused by cabling systems are generally the most difficult to find, the price paid for this is often also the largest." Therefore, the standard of communication should be used wiring and cabling systems. In order to improve the reliability of computer networks and meet the needs of future development of the computer network, it is necessary to consider a certain degree of redundancy and fault tolerance. For very important and do not worry about the cost of construction of computer networks, in the wiring is preferably arranged in a two-lane, so the computer network line fails to timely switch. Computer network hub terminal together several users connected to the network through which the computer network errors and other parts of the connected device can be separated to form a computer network to ensure the reliability of the first line of defense. A hub is a single point of failure device itself if it fails, users connected to it will not work, we can see a computer network hub plays an important role in improving the reliability of the computer network. For this reason, in the design of computer networks, they often have to consider the use of effective measures to ensure its reliability. LAN switch for connecting several independent, and in between a packet filtering network interconnection devices can be used to solve insufficient bandwidth and network exchange bottleneck problems and meet the needs of the interaction between the user terminal and the server, improving overall network performance. Router is one of the connected devices at the network layer, using it only to achieve the same type of local area network, but also to achieve the interconnection between local area and wide area networks and wide area networks and WANs. In the analysis of the reliability of the router, the first problem is to select a protocol, the protocol as resilient. Improve the reliability of the router most insurance is redundant routing design techniques, so that when the primary router fails, the router can automatically sub in place of its work, in order to ensure the normal operation of computer networks^[8-10].

Usually a large computer network is a different network products and equipment from different manufacturers posed by the large-scale, complex structure. To ensure the integrity of information transmission, reducing the failure rate, reduce the rate of loss of information, reduce errors and errors, improve the reliability of the computer network, it should be the use of advanced network management technology, real-time statistics collection network operating parameters and network information, monitoring network operation status, time to find and troubleshoot. In the actual planning of computer networks, design, construction, operation, we should pay attention to the following aspects of the first two areas, scientific and rational choice of computer network management software, pay attention to its functionality meets the requirements to be able to meet configuration, security, At the same time demand management and billing, network management software requires a computer should be able to provide a unified network management interface, follow standard network management protocol. This will not only manage its own network equipment, but also can manage the exchange of information with other computer network management software. Use of computer network management software can monitor and manage the network, detect network problems and failures occur, and provide a strong basis for the network management and maintenance strategies to improve the reliability and efficiency of the whole computer network. Second, in order to ensure the normal operation of computer networks, in the development of the necessary network management system and regulations on the basis of, but also to strengthen the computer network of personnel training and education, develop good habits and applied ethics. In order to prevent human operational errors and vandalism, the use of administrative and legal measures to ensure the normal operation of the order of computer networks.

Computer network topology computer network belonging planning issue, but also congenital factors affect the reliability of the computer network. Practice shows that the different application areas, different levels of scale computer network must have different network topologies, otherwise improve the reliability of the computer network is just empty talk. Analysis of computer network topology computer networks affect the reliability of this chapter to be studied core content. Interconnection network topology is the main connection between the computer network components, which can be used diagram, graph theory is the study and therefore the most powerful mathematical tool interconnection network performance. At first people through the diameter and to measure the effectiveness of communication with fault-tolerant computer network, computer network topology with in-depth research and analysis.

2. Related Works

2.1. Chaos Theory

Chaos research can be divided into two categories, one is known system characteristics, can create deterministic system of equations, and dynamical characteristics of the system and the other is the system itself does not know, only that time the system output signal sequence and therefore need to rebuild the system, and then analyze characteristics of the system, in practice, the signal sequence is time noise pollution, the need for the implementation of separation of signal and noise, thereby producing a number of specific practical problems. Chaos pioneering stage of research work has focused on the former, theoretical research center is now focused on the latter, more focused application of chaos. Chaos in engineering technology, information detection is one of the main content. Due to the sensitivity of chaotic systems with weak signal and noise immunity, the initial value of the sensitivity and other characteristics, such chaos in information detection and measurement technology has great potential. Chaos in engineering applications are generally divided into the following three aspects of the phenomenon of chaos engineering system generated and controlled. Many previously considered noise signal has been shown to be deterministic chaos. Therefore, as long as the adjustment parameters can effectively control the chaos, so as to achieve similar results filtering. Chaos here is still considered useless noise, the only progress is recognition of the difference between chaos and noise, and thus be controlled more effectively. Classical control problem is different, there is no chaos control unified theoretical framework, but its physical state characterized by the presence of a common denominator, that is, change the original field that is positive index is negative, in order to achieve the transition from stable to unstable^[10-12].

In the case of the model can not know the system, you can use some common nonlinear techniques, starting directly from the experimental data, obtaining certain information Poincare section, enabling the characterization of attractors. Which are typical of phase space reconstruction method, and the like. All of these methods, research tools are relatively fixed. Are generally based on basic physics chaos in engineering applications are generally divided into the following three aspects of the phenomenon of chaos engineering system generated and controlled. Many previously considered noise signal has been shown to be deterministic chaos. Therefore, as long as the adjustment parameters can effectively control the chaos, so as to achieve similar results filtering. Chaos here is still considered useless noise, the only progress is recognition of the difference between chaos and noise, and thus be controlled more effectively. Classical control problem is different, there is no chaos control unified theoretical framework, but its physical state characterized by the presence of a common denominator, that is, change the original field that is positive index is negative, in order to achieve the transition from stable to unstable.

In the case of the model can not know the system, you can use some common nonlinear techniques, starting directly from the experimental data, obtaining certain information Poincare section, enabling the characterization of attractors. Which are typical of phase space reconstruction method. All of these methods, research tools are relatively fixed. It is generally based on basic physics equation, mathematical model of the system. Then analyze chaotic phenomena that may arise, and validated experimentally. Researchers just need some math skills. Chaotic and utilized. Here, the chaos is considered to have certain characteristics, can I use things. These methods require researchers chaotic nature and its philosophical significance have a full understanding, require more imagination. Compared with the pure theory of chaos theory, and can be workable in practice, which further deepened the difficulty of the problem. Attractor is the system state vector in time after evolution will eventually fall into a particular trajectory. For chaotic signals, the trajectory is confined within a limited area or space of the phase plane, and never cross, can be seen as the rail lines are repeated folding and stretching results. Among the many attractors, some of present's attractor fractal dimension structure, which we call strange attractor. Strange attractor is determined whether a signal Chaos important basis.

And just generally not quantitatively represent the system evolution phenomena in a certain period of time, it is necessary to seek some features to characterize the amount or characterization system consists of a time series, and these amounts should be able to reveal some of the features associated with most systems characteristics of nature. We know that a fundamental purpose of the study is to understand the chaotic dynamics asymptotic final state of the system or the law of development. For discrete systems, it is to understand the whole process of the system evolution trick, that attractor. Therefore, it can be described by a chaotic system and chaotic signals generated by quantitative analysis of certain characteristics of attractor.

2.2. Neural Networks

Artificial neural network is a large number of neurons as the processing unit from the interconnected network by abstracting the behavior of the human brain reflects the way it works, its features include: (1) self-learning through the training process from the external environment; (2) projecting touch weights used to store information. It can be seen as parallel distributed processor by a large number of simple processing units composed, and includes related natural characteristics of the human brain neurons, such as the ability to store knowledge and application experience. Its development consists of three stages.

The first stage in 1943, Mc Culloch in the "Bulletin of Mathematical Biophysics" proposed based on neuronal bioelectrical operation mechanism of biological and biochemical model and prove the MP: If the number of neurons enough, have the appropriate connection and run the synchronization, then the neural network of any computable function can be calculated. Subsequently, neuropsychologist D.O.Hebb proposed Hebb rule proposed learning and synaptic contacts had set nerves, synapse connection strength with activities before and after the neurons change dynamically. This time with the rapid development of digital computers, artificial neural network into the depression stage.

The second stage in 1972 James Anderson developed a new type of neural network memory. Amari proposed neuron model is applied to a random connection, John Hopfield statistical mechanism explains the cycle network running, David Rumelhart and James Mc Celland, *etc.* to achieve the back-propagation algorithm for training multilayer perceptron, neural network again a rise.

The third stage, from 1986 to date, in 1986, Rumelhart Hinton Williams developed the back-propagation algorithm BP, on the back-propagation algorithm is applied to produce a significant impact on the algorithm to solve the multi-NN learning problems. BP neural

network at the desired point error output and actual output gradually adjust the connection weights, in order to reduce the error, in the process, it is a positive signal propagation, and error is the back-propagation weights in the forward signal transfer process is fixed, while the back propagation process, the connection weights feedback regulation by the error; the type of learning is supervised learning; learning is constantly thinking back propagation to the output of each unit, and Fixed connection weights. BP neural network, hidden layer determines the number of layers is important, experiments show that: the deviation threshold, and more than one hidden layer Sigmoid type and comprises a linear output layer network can approximate any rational function, increase the number of hidden layers help to improve accuracy and reduce network error, so many hidden layer network access to any desired decision boundaries in order to achieve classification, but the more the number of hidden layer BP neural network training time is longer. For a single hidden layer neural network, hidden layer neuron number, the more enhanced the learning ability and can achieve the desired accuracy, but the relative weakening of the generalization, easily reached fitting state; the fewer the number of hidden layer neurons but also easily lead to learning ability is not enough. Akaike criteria put forward: there is an optimal number of neurons in the hidden layer, so that the accuracy and generalization ability of neural network reaches a predetermined requirements.

3. The Proposed Scheme

Chaotic system and its sensitivity to perturbation parameters, so that periodic changes in the nature of the characteristics of solutions occurrence detecting weak periodic signal is to be tested as a small signal period chaotic system disturbances, noise, although strong, but change the system state has no effect, and once there is a specific small-signal perturbation due to the sensitivity of chaotic systems small periodic signal, even if the amplitude is small, the system will change the nature of the phase, the computer identification system by the state, It may determine whether there is a signal, so that the weak periodic signal strong background noise detected. An error occurred while using the system as a test signal based on the state transition is detected, whether artificial or computer systems are based on the change of pattern recognition, so the system in the two states greater the difference between the phase diagram, then the pattern recognition the probability is smaller. Through experiments and theoretical analysis, we found chaos chaotic system in the state and large-scale periodic state of the phase diagram of the system very different, so the system phase diagram of transition from chaos to a state as large-scale cycle state signal detection basis.

That test whether a particular form of attack data input, the output results are divided into three types: (1) normal data flow; (2) is shown as a certain kind of attack, for both cases, the neural network will indicate whether the attack or normal data stream, the system administrator to record the input and output vectors at this time, that adding these do not exist in the input and output data samples for training, and then the neural network training; (3) is not defined at the time of neural network training this encoding, for this case can not be determined whether the attack. In the abnormality detection mode, the response can be divided into three kinds: For TCP connections types of attacks, mainly by way of withdrawal connection, but for purposes of the UDP protocol, when an attacker manufacturing backdoor in the system, this time by the revocation connection approach can not solve the problem, then use evasive way, do not accept or send any packets to the attacker, while normal user record information, so as not to affect the normal network traffic; the last way is to isolate, if detected within a period of time to a variety of attacks to take this approach, mainly used in DOS attack scenario.

Variables are defined as follows:

Input vector:

$$X = (x_1, x_2, \dots, x_n) \quad (1)$$

Hidden layer input vectors:

$$hi = (hi_1, hi_2, \dots, hi_p) \quad (2)$$

Hidden layer output vectors:

$$ho = (ho_1, ho_2, \dots, ho_p) \quad (3)$$

Output layer input vectors:

$$yi = (yi_1, yi_2, \dots, yi_p) \quad (4)$$

Output layer output vectors:

$$yo = (yo_1, yo_2, \dots, yo_p) \quad (5)$$

Desired output vector:

$$d_0 = (d_1, d_2, \dots, d_q) \quad (6)$$

Connection weights input layer and the intermediate layer: w_{ih}

Connection weights hidden layer and output layer: w_{ho}

Hidden layer neuron threshold: b_h

Each neuron output layer threshold: b_0

The number of sample data: $k = 1, 2, \dots, m$

Solving chaos gradient, to give the formula (6)

$$\frac{\partial yi_0(k)}{\partial w_{ho}} = \frac{\partial \left(\sum_h^p w_{ho} ho_h - b_0 \right)}{\partial w_{ho}} = ho_h(k) \quad (7)$$

Global convergence of computing, according to the global error can be calculated as

$$E = \frac{1}{2m} \sum_{k=1}^m \sum_{o=1}^q (d_o(k) - y_o(k))^2 \quad (8)$$

According to the global error, it can blur correction can be

$$w_{ho}^{N+1} = w_{ho}^N + \eta \delta_0(k) h_{o_h}(k) \quad (9)$$

Finally we got the system for processing

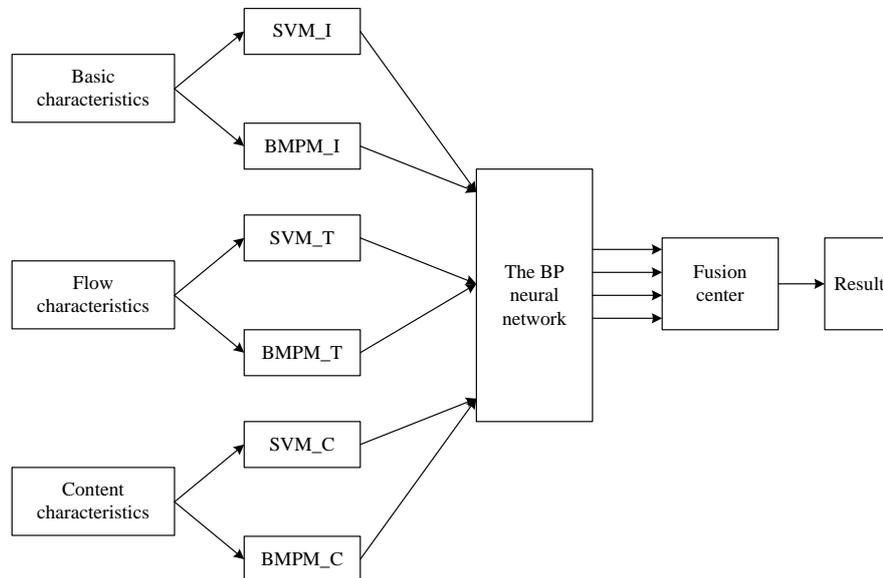


Figure 1. The Fusion of SVM and BMPM Network Anomaly Detection Model

4. The Experiment Results Analysis

Experiments using 10% of KDD Cup1999 training data set, the data set includes a total of 23 different types of attacks, 326421 link records, 92373 normal connection records, each connection record is composed of 31 different attributes, 34 of them for numeric, 7 for character attributes. Test data set contains 241225 link records, 37 kinds of different types of attacks, including 14 types of attack did not appear in the training sample. At the same time, all of these attack types can be divided into the following four categories:

Dos: namely the denial of service attacks, such as the smurf, teardrop, syn flood, *etc.*;

Probe: namely to detect attacks, such as port scanning and vulnerability scanning;

U2R: elevated privileges, such as buffer overflow attacks, *etc.*;

R2L: namely remote access permissions, such as guess password attacks.

Experiment of using 10% Normal KDD Cup1999 data set, DOS, the Probe and R2L type of connecting the 4125 attack, U2R type attack connection 236. Selection of these data are for the selected data set of a variety of services, including all the network services. Experiments, such as the selection of data is divided into two, and a as the training data set, another one as a test data set, to train the fusion anomaly detection model, and to test the test data set. In order to reflect the effectiveness of the detection model in the fusion, here will use the same set of training data to train the SVM, BMPM and use the same test data set to test the SVM, BMPM and BP, and finally with the comparative analysis of monitoring results of fusion of anomaly detection model^[12-15].

Table 1. The Detection Result of all the Attacking Types with SVM

Attack types	The total number of attacks	Detect attack number	Detection rate
Dos	1800	1765	0.980
Probe	1700	1692	0.995
U2R	153	142	0.928
R2L	1800	1750	0.972
Total	5453	5349	0.980

Table 2. The Detection Result of all the Attacking Types with BMPM

Attack types	The total number of attacks	Detect attack number	Detection rate
Dos	1800	1736	0.964
Probe	1700	1682	0.989
U2R	153	146	0.954
R2L	1800	1759	0.977
Total	5453	5343	0.979

Table 3. Detection Rate for all Types of Attacks with Fusion of SVM and BMPM

Attack types	The total number of attacks	Detect attack number	Detection rate
Dos	1800	1756	0.975
Probe	1700	1692	0.995
U2R	153	150	0.980
R2L	1800	1787	0.992
Total	5453	5425	0.994

Can be seen in the chart, and the SVM, BMPM compared single anomaly detection methods, such as the integration of the SVM and BMPM detection methods in keeping the detection rate of reduce the false alarm rate (SVM false-alarm rate = 1.83%, BMPM false-alarm rate = 1.26%, the integration of the SVM and BMPM false-alarm rate = 0.48%). At the same time, specific to a variety of different types of attacks on the detection, fusion method on the DOS attack types of testing, slightly lower than the SVM detection rate and high detection rate than BMPM, namely in made a balance between two kinds of detection methods, on the three other types of attacks also played a balance SVM and BMPM high detection rate on a single attack type, low detection rate on other types of defects, this fusion model is used to detect multiple attack types with higher stability.

5. Conclusion

Characteristics of fault data presented herein based on the network, be modeled, according to the characteristics of chaos theory, neural network combined with the depth of its network failure is detected, the convergence speed test results are given in the data, you can see from the data out, this method is suitable for online network status detection of weak fault detection correct rate.

Acknowledgement

This work was all supported by the Key research project of Beijing Polytechnic College under grant NO. bgzykyz201405.

References

- [1] Cao S., Cao G. and Chen K., "The Ground Objects Identification for Digital Remote Sensing Image Based on the BP Neural Network[M]",// Computer Engineering and Networking. Springer International Publishing, (2014), pp. 671-677.
- [2] Peng H. Y., "The BP neural network's GA optimization and its realization on MATLAB[C]",// Control and Decision Conference (CCDC), 2013 25th Chinese. IEEE, (2013), pp. 536-539.
- [3] Zhang K., Zhang B. and Qu R., "Analysis of eight volume pulse elements based on the BP neural network[C]",// Advanced Computational Intelligence (ICACI), 2015 Seventh International Conference on. IEEE, (2015).
- [4] Shi T., Yuan T. and Shi B., "Bus turnaround time prediction research based on the BP neural network[J]", Journal of Shandong Jianzhu University, (2015).
- [5] Li Q. H. and Liu D., "Aluminum Plate Surface Defects Classification Based on the BP Neural Network[J]", Applied Mechanics & Materials, vol. 734, (2015), pp. 543-547.
- [6] Benmoussat M. S., Guillaume M. and Caulier Y., "Automatic metal parts inspection: Use of thermographic images and anomaly detection algorithms[J]", Infrared Physics & Technology, vol. 61, no. 11, (2013), pp. 68-80.
- [7] Bhuyan M. H., Bhattacharyya D. K. and Kalita J. K., "Network Anomaly Detection: Methods, Systems and Tools[J]", Communications Surveys & Tutorials IEEE, vol. 16, no. 1, (2014), pp. 303-336.
- [8] Lee Y. J., Yeh Y. R. and Wang Y. C. F., "Anomaly Detection via Online Over-Sampling Principal Component Analysis[M]",// Anomaly Detection via Online Over. IEEE, (2013), pp. 1-1.
- [9] Li W., Mahadevan V. and Vasconcelos N., "Anomaly Detection and Localization in Crowded Scenes.[J]", IEEE Transactions on Pattern Analysis & Machine Intelligence, vol. 36, no. 1, (2013), p. 1.
- [10] R. Vrabič, G. Škulj and P. Butala, "Anomaly detection in shop floor material flow: A network theory approach[J]", CIRP Annals - Manufacturing Technology, vol. 62, no. 1, (2013), pp. 487-490.
- [11] Bhattacharyya D. K. and Kalita J. K., "Network Anomaly Detection: A Machine Learning Perspective[J]", Crc Press, (2013).
- [12] Poletto M. A., Ratin A. and Gorelik A., "Aggregator for connection based anomaly detection: US", US8479057 B2[P]. (2013).

Author



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