Evaluation of Network Connection Credibility based on Neural Network

Qingtao Wu
Electronic and Information Engineering College, Henan University of Science and Technology, Luoyang, China
wqt8921@126.com

Xintong Yang, Bin Hua and Ruijuan Zheng
Electronic and Information Engineering College, Henan University of Science and Technology, Luoyang, China
{yangxin409, huabin83, rjwo}@163.com

Abstract—This paper presents an innovative method to evaluate the credibility of network connections based on neural network with back propagation (BP) network model and Levenberg-Marquardt (LM) optimization algorithm. In it, the second-level index values are taken as input and expected evaluation values as output, based on which, L test samples are used to test the trained neural network. At last, a prediction is made to evaluate the current connection credibility according to the trained neural network and corresponding security strategies are adopted on the basis of the evaluation values. It is shown that the nonlinear relationship between the attributes and the credibility of network connections can be established by training neural-network using LM algorithm. Simulation results indicate this method could achieve high evaluation accuracy.

Index Terms—Trusted Computing, Credibility of Network Connection, Neural Network, KDDCup99 Data Set

I. INTRODUCTION

Increasing of network complexity, system size, and operation speed has resulted in ever-increasing risks and threats against the security of network systems. Traditional information security systems rely on whether or not user terminals have been certified and authorized to grant access to a protected network. However, due to the lack of reliable evidence for network systems to determine whether access to a network is credible, traditional methods cannot make accurate user credibility evaluation; hence fail to effectively protect network systems from security attacks. As a result, those traditional methods can only defend network passively and cannot meet the demand for security in the presence of complex attacks.

Trusted network connection (TNC) [1] introduced an innovative network access control mechanism, which utilizes trusted computing model in network access control system by combining traditional network security technology and “trusted computing” technology. A new trust model based on behavior and trusted computing to deal with the trusting relationship among the entities is proposed in[2], and by taking different methods to deal with to the trusting relationship between inner-domain and intra-domain based on the concept of Identity right, a method for measuring and evaluating the behavior trust are provided. In 2010, professor Zhang huanguo researched trusted network connection, In the paper, the development history, architecture, information flow and related specification of trusted network connection is introduced in detail; analysis is given on trusted network connection architecture; merits and the restriction are pointed out[3]. The Trusted Computing Group (TCG)[4] has prepared the specifications for credible network connection with the hope to establish trusted network to keep distrusted access under control at the source. The evaluation of the credibility of network connections is an important stage for building trusted network. Tian Li-qin et al. [5] have studied the behavior and credibility model of network users. They presented a prediction model for user credibility of multiple attributes using Bayesian network and determined the mixed Nash equilibrium strategies through risk analysis and game analysis. This model can be used to support decision-making for connection credibility evaluation. Currently, the study of TNC is still in the phase of engineering technology. Theoretical research still lags behind engineering practice. At the same time, study of remote automated anonymous attestation in trusted computing is carried out. The remote automated anonymous attestation hides the identity of platform by ring signature, replaces configuration by property-based certificate, which takes good reference for updates and patches of system [6]. While, how to describe the value of platform attributes and how to abstract the outer attributes certificate accurately are still the challenge that the researchers must face. Based on the model of trusted computing platform, a formal method of analyzing the trust chain transfer is proposed in [7]. It formalized specifies the security policy isolating the interference between components that can make the trust chain valid after integrity measurement. However, satisfying transfer the condition of intransitive noninterference will be strict, as a result, the more actual

Manuscript received July 1, 2010; revised September 14, 2010; accepted October 1, 2010.
and flexible trust transfer model needs to be researched in future.

In brief, integration of trusted computing and network security is just getting started, and there are still many problems, such as trusted network problem, content credibility, behavior credibility, transfer credibility, resource share credibility, etc.

Effective methods for making a quantitative evaluation of network credibility according to the attributes of network connections have not been found yet. The evaluation of network connection credibility can lay a solid foundation for implementing defense strategies for network security. By utilizing the learning and predicting ability and the nonlinear fitting abilities of neural network, this paper presents a neural network based model to evaluate network connection credibility.

This paper is organized as follows. Firstly, neural network method is introduced in order to establish an index system for connection credibility evaluation and as well as to determine expected evaluation values. The proposed method is presented in Section 3. A simulation study of the proposed method is given in Section 4, which is followed by the conclusion in Section 5.

II. NEURAL NETWORK METHOD

Artificial neural network studies human intelligent behavior from the perspective of physiological brain structure and stimulates the information processing function of the brain. It is characterized by parallelization of information storing and computing to achieve high adaptability, learning ability and fault-tolerance. Artificial neural network has been widely applied in pattern recognition, signal processing, modeling, prediction, system control and other fields. In modeling, the space between input data and output data is called the “black box.” Nonlinear mapping between input data and output data can be approximated by learning process. Such a characteristic could realize the mapping from the network connection attribute value to the credibility evaluation value. A quantitative evaluation and prediction of network connection credibility can be carried out accordingly.

A. Basic Theory of Neural Network

The neural network could be considered a high nonlinear mapping from input to output, i.e., \( f : \mathbb{R}^n \rightarrow \mathbb{R}^m \). For a sample input set and output set \( x_j (x_j \in \mathbb{R}^n) \text{ and } y_j (y_j \in \mathbb{R}^m) \), respectively, it is assumed that there is a mapping \( g \) that makes \( g(x_j) = y_j, (i = 1, 2, \ldots, n) \) true. Now, a mapping \( f \) shall be figured out. \( f \) is the best approximation to \( g \). BP neural network could make the simple nonlinear function approach any complex function through composition many times. Kolmogorov Theorem (i.e., mapping network existence theorem) ensures that any continuous function could be realized by a three-layer feed forward network.

Neural network training tasks can be considered as a set of network weights with the minimum deviation of expected output and actual output in all training modes.

If the number of modes if limited, the energy function can be written as:

\[
E(w) = \frac{1}{2} \sum_{q=1}^{Q} \left( d_q - x_{out, q}^{(3)} \right)^T \left( d_q - x_{out, q}^{(3)} \right) \\
= \frac{1}{2} \sum_{q=1}^{Q} \left( d_q - x_{out, q}^{(3)} \right)^2 
\]

(1)

Where \( Q \) is the total number of training patterns, \( w \) represents the vector which contains all of the weight in the network, \( d_q \) is the expected output vector of the network \( x_{out, q}^{(3)} \) expresses the actual output vector.

According to Newton’s method equation (1), the optimal energy function of the minimum weight set can be found by applying the following formula:

\[
w(k + 1) = w(k) - H_k^{-1} \nabla E(w)_{|w=w(k)}
\]

(2)

where

\[
H_k = \nabla^2 E(w)_{|w=w(k)}
\]

(3)

and

\[
\nabla E(w)_{|w=w(k)} = \frac{\partial E(w)}{\partial w(k)}
\]

(4)

Define \( P = n_3 Q \), equation (1) can be rewritten as:

\[
E(w) = \frac{1}{2} \sum_{p=1}^{P} \left( d_q - x_{out, q}^{(3)} \right)^2 = \frac{1}{2} \sum_{p=1}^{P} e_p^2
\]

(5)

where

\[
e_p = d_q - x_{out, q}^{(3)}
\]

(6)

In equation (4) the gradient of energy function can be calculated as:

\[
\frac{\partial E(w)}{\partial w(k)} = \frac{1}{2} \left[ \begin{array}{c}
\frac{\partial E}{\partial w_1} \\
\frac{\partial E}{\partial w_2} \\
\vdots \\
\frac{\partial E}{\partial w_N}
\end{array} \right] = \frac{1}{2} \left[ \begin{array}{c}
\sum_{p=1}^{P} \frac{\partial e_p}{\partial w_1} \\
\sum_{p=1}^{P} \frac{\partial e_p}{\partial w_2} \\
\vdots \\
\sum_{p=1}^{P} \frac{\partial e_p}{\partial w_N}
\end{array} \right] = J^T e
\]

(7)

Where \( J \) is the Jacobian matrix.

Next step is to find Hansen matrix expression. The \( k, j \) element of Hansen matrix can be expressed as:

\[
\left[ \nabla^2 E(w) \right]_{k,j} = \frac{\partial^2 E(w)}{\partial w_k \partial w_j}
\]

(8)

By using the expression of Jacobian matrix, Hansen matrix can be expressed as:

\[
\nabla^2 E(w) = J^T J + S
\]

(9)

where \( S \) is the second derivative matrix, and it can be expressed as:
\[ S = \sum_{p=1}^{P} e_p v_p^2 \]  

(10)

When close to the minimum energy function, the elements of \( J \) become very small, and Hansen Matrix can be approximately expressed as:

\[ H = J^T J \]  

(11)

The equation (7) and equation (11) into equation (2), we have neural network to iterate and adjust network weight in the step of \( k+1 \) as follows:

\[ w(k+1) = w(k) - [J_k^T J_k + \mu_k I]^{-1} J_k^T e_k \]  

(12)

Where subscript \( k \) indicates the corresponding matrix value in \( w = w(k) \).

B. LM Optimization Algorithm

Although BP neural network can ensure network training convergence, the speed of convergence is very slow and the algorithm may be stuck by local minimization. Hence, it is characterized by poor operability. Presently, many improvement algorithms have been put forward [8], such as momentum improvement algorithm, simulated annealing algorithm, adaptive variable step algorithm and LM algorithm, to enhance network training efficiency. LM algorithm is characterized by stable and quick convergence. However, due to the space cost, it may not be a good method for complicated problems. This paper proposes an improved LM algorithm for the training of BP neural network to evaluate connection credibility.

A problem of iterative updates in equation (12) is that \( H = J^T J \) may be sick or even singular matrix. The problem can easily be modified to solve by equation (11)

\[ H = J^T J + \mu I \]  

(13)

where \( \mu \) is a very small number, \( I \) is a unit matrix.

The equation (13) into equation (12), the iterative function, to be used by LMBP neural network to iterate and adjust network weight in the step of \( k+1 \), is given below:

\[ w(k+1) = w(k) - [J_k^T J_k + \mu_k I]^{-1} J_k^T e_k \]  

(14)

III. EVALUATION OF NETWORK CONNECTION CREDIBILITY

Many connection attributes may affect credibility evaluation. To quantitatively evaluate network connection credibility in a timely manner, so that security measures can be taken quickly, this paper makes a detailed analysis of the KDDCup99 data set [9] frequently adopted in network intrusion detection.

KDDCup99 data set refers to the nine-week network connection data acquired from a simulated US Air Force LAN, including labeled training data and non-labeled test data. Each connection record in the training data set is a 42-dimensional data, where the first 41 dimensions are the network connection attributes and the last dimension refers to the type of attack. In the following paragraphs, the author firstly examines the first 41 dimensions, i.e., the connection attributes, to determine an index system for credibility evaluation. Then the author analyzes the effect of the four types of attacks on system operation. A number between 0 and 1 will be used to evaluate the connection credibility when the network is under any of the four types of attacks.

A. Network Connection Attributes Index System

This paper establishes an index system for credibility evaluation using the attributes that could reveal the change of state best in the dataset. The index system includes 3 first-level indexes (basic feature of single TCP connection, content feature of one connection, traffic feature within two seconds) and 28 second-level indexes, as shown as Tables I, II, and III.

<table>
<thead>
<tr>
<th>Second-level indexes</th>
<th>Connotation of indexes</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Duration of connection</td>
<td>Continuous</td>
</tr>
<tr>
<td>Src bytes</td>
<td>Data traffic from source address to destination address</td>
<td>Continuous</td>
</tr>
<tr>
<td>Dst bytes</td>
<td>Data traffic from destination address to source address</td>
<td>Continuous</td>
</tr>
<tr>
<td>Land</td>
<td>0-other 1-the source address connected and the destination address connected are the same host</td>
<td>Discrete</td>
</tr>
<tr>
<td>Wrong fragment</td>
<td>Number of wrong fragments</td>
<td>Continuous</td>
</tr>
<tr>
<td>Urgent</td>
<td>Number of urgent data packages</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Second-level indexes</th>
<th>Connotation of indexes</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num_failed_logins</td>
<td>Number of failed login attempts</td>
<td>Continuous</td>
</tr>
<tr>
<td>Logged_in</td>
<td>1-successful login, 0-other</td>
<td>Discrete</td>
</tr>
<tr>
<td>Num_compromised</td>
<td>Times of receiving threats</td>
<td>Continuous</td>
</tr>
<tr>
<td>Root_shell</td>
<td>1-obtain super users shell; 0-other</td>
<td>Discrete</td>
</tr>
<tr>
<td>Su_attempted</td>
<td>1-su attempt to execute command; 0-other</td>
<td>Discrete</td>
</tr>
<tr>
<td>Num_root</td>
<td>Times of authorized access</td>
<td>Continuous</td>
</tr>
<tr>
<td>Num_file_creation</td>
<td>Times of file creation operation</td>
<td>Continuous</td>
</tr>
<tr>
<td>Num_shells</td>
<td>Number of complying presentation</td>
<td>Continuous</td>
</tr>
<tr>
<td>Num_access</td>
<td>Times of control files access</td>
<td>Continuous</td>
</tr>
<tr>
<td>Num_outbound_cmds</td>
<td>Times of command transmission in one ftp dialogue</td>
<td>Continuous</td>
</tr>
<tr>
<td>Is_hot_login</td>
<td>1-hot login; 0-other</td>
<td>Discrete</td>
</tr>
<tr>
<td>Is_guest_login</td>
<td>1-guest login; 0-other</td>
<td>Discrete</td>
</tr>
</tbody>
</table>

TABLE I.
BASIC FEATURE OF SINGLE TCP CONNECTION

<table>
<thead>
<tr>
<th>Second-level indexes</th>
<th>Connotation of indexes</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Duration of connection</td>
<td>Continuous</td>
</tr>
<tr>
<td>Src bytes</td>
<td>Data traffic from source address to destination address</td>
<td>Continuous</td>
</tr>
<tr>
<td>Dst bytes</td>
<td>Data traffic from destination address to source address</td>
<td>Continuous</td>
</tr>
<tr>
<td>Land</td>
<td>0-other 1-the source address connected and the destination address connected are the same host</td>
<td>Discrete</td>
</tr>
<tr>
<td>Wrong fragment</td>
<td>Number of wrong fragments</td>
<td>Continuous</td>
</tr>
<tr>
<td>Urgent</td>
<td>Number of urgent data packages</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

TABLE II.
CONTENT FEATURE OF ONE CONNECTION
of the connection types are listed as follows:

- Normal connection - the credibility of normal connection is defined as 0.95.
- Probing attack - this kind of attacks scan the target host and hence to operation of the host illegally. This type of attacks includes IP spoofing and Trojan horse. This paper defines the credibility of such network connections as 0.3.
- Remote to local attack (R2L) - an attacker that does not have any account in the target host tries to acquire root or administrator privilege to conduct an attack. Buffer overflow is a typical method used in this type of attacks. The major reason for buffer overflow is the system or application program does not detect the illegal parameters entered by users. This paper defines the credibility of such attacks as 0.2.
- U2R attack - this kind of attacks acquire access to the host and hence to operation of the system or application program. As there is no effective defending measure against it, it has become one of the most frequently used network attacks and imposed great threats on network systems. The credibility of such a connection is the lowest and is defined as 0.05.

To sum up, the credibility values of connections under different types of attacks are given in Table IV. These values will be taken as the expected output of neural network to train the neural network.

### Table III

<table>
<thead>
<tr>
<th>Second-level indexes</th>
<th>Connotation of indexes</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>Times of connection with the same destination address in the past 2s and currently</td>
<td>Continuous</td>
</tr>
<tr>
<td>Serror_rate</td>
<td>Times of connection where SYN error appears</td>
<td>Continuous</td>
</tr>
<tr>
<td>Rerror_rate</td>
<td>Times of connection where REJ error appears</td>
<td>Continuous</td>
</tr>
<tr>
<td>Same_srv_rate</td>
<td>Times of connection where the same service is created</td>
<td>Continuous</td>
</tr>
<tr>
<td>Diff_srv_rate</td>
<td>Times of connection where different services are created</td>
<td>Continuous</td>
</tr>
<tr>
<td>Srv_count</td>
<td>Times of connection where the same service appeared in the past 2s and also appears currently</td>
<td>Continuous</td>
</tr>
<tr>
<td>Srv_serror_rate</td>
<td>Times of connection where SYN error appears</td>
<td>Continuous</td>
</tr>
<tr>
<td>Srv_rerror_rate</td>
<td>Times of connection where REJ error appears</td>
<td>Continuous</td>
</tr>
<tr>
<td>Srv_diff_host_rate</td>
<td>Times of connection to different hosts</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

### Table IV

<table>
<thead>
<tr>
<th>Type</th>
<th>Detailed description</th>
<th>Evaluation value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Normal</td>
<td>0.95</td>
</tr>
<tr>
<td>Probing</td>
<td>Ipsweep, nmap, portsweep, satan</td>
<td>0.3</td>
</tr>
<tr>
<td>R2L</td>
<td>rp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster</td>
<td>0.2</td>
</tr>
<tr>
<td>U2R</td>
<td>buffer_overflow, loadmodule, perl, rootkit</td>
<td>0.2</td>
</tr>
<tr>
<td>DOS</td>
<td>back, land, neptune, pod, snarf, teardrop</td>
<td>0.05</td>
</tr>
</tbody>
</table>

### C. Structure of BP Neural Network

BP neural network is composed of three layers: input layer, hidden layer, and output layer. The structure of the neural network is given as Fig. 1.

![Figure 1. Structure of BP Neural Network for Evaluation of Network Connection credibility](image-url)

There are 28 neurons in the input layer, representing the second-level indexes of the evaluation index system of connection credibility. There are 10 neurons on the hidden layer and 1 neuron on the output layer, representing the evaluation index of connection credibility. The index range is (0, 1). As the activation function used to calculate neuron values, the hidden layer adopts the hyperbolic tangent function and the output layer adopts the S-type logarithmic function. The output range is (0, 1). For a given input vector (second-level index), the network generates an output vector (evaluation index) to approximate the nonlinear mapping function.
D. Preprocessing of Input Data

BP network restricts the range of input data, so input samples can be normalized. In this paper, it is assumed that the original sample is \( x_i = (x_{i1}, x_{i2}, \ldots, x_{i28}) \) (i=1, 2…n, where n represents the number of samples). The original samples are then normalized,

\[
x'_{ij} = \frac{x_{ij} - \min(x_{ij})}{\max(x_{ij}) - \min(x_{ij})}
\]

where \( \max(x_{ij}) \) and \( \min(x_{ij}) \) represent the maximum and minimum values of Index \( j \) of all samples, respectively. The normalized, sample is \( x''_i = (x'_{i1}, x'_{i2}, \ldots, x'_{i28}) \). In this way, the original samples could be converted to the range of (0, 1) and be accepted by the BP network.

E. Proposed Method for Connection Credibility Evaluation

The proposed method for the evaluation of network connection credibility is given as follows:

1. Select data records from the KDDCup99 data set and make them cover as many types of attacks as possible. Then group the data records into M training samples and L test samples.
2. Select the attribute of data set on the basis of the evaluation index system and process the data.
3. Take the second-level index values as input and expected evaluation values as output. Use M training samples to train the BP neural network.
4. Use L test samples to test the trained neural network. If the accuracy rate reaches 90%, then the neural network training is a success; otherwise, the network should be retrained.
5. Capture network packet and generate connection records according to the index system.
6. Make a prediction and evaluate the current connection credibility according to the trained neural network and adopt corresponding security strategies on the basis of the evaluation values.

Evaluation flowchart is given as Fig. 2.

IV. SIMULATION RESULTS

The simulation experiment is carried out in MATLAB 7.0 using a Pentium 4 Processor with 2.66 GHz and 512M memory running Windows XP. 1000 records are selected from the KDDCup99 data set for BP Neural Network training, among which 800 records are attack records covering the four types of attacks. The distribution of probing attacks in training set is given as Fig. 3. Probing attack is an attempt to gather information about a network of computers for the apparent purpose of circumventing its security controls. The distribution of R2L attacks in training set is given as Fig. 4. Remote to local attack occurs when an attacker who has the ability to send packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine. The distribution of U2R attacks in training set is given as Fig. 5. User to Root Attack is a class of exploit in user account on the system and is able to exploit some vulnerability to gain root access to the system.
Then select 1700 records as test samples. The training error curve is shown in Fig. 7. Simulation results of the training set are presented in Fig. 8 and simulation results of the test set in Fig. 9. Training and test are carried out many times each and the best results are given in Table V, where \(P = \frac{1}{N} \sum_{i=1}^{N} I(t_i - y_i) \leq \epsilon \) represents the evaluation accuracy and \(\text{MSE} = \frac{1}{N} \sum_{i=1}^{N} (t_i - y_i)^2 \) represents the mean-square error. In the experiment, \(\epsilon = 0.05 \).

![Figure 6. Distribution of DOS Attacks in Training Set](image)

![Figure 7. Training Error Curve.](image)

![Figure 8. Training Results of Network Connection Credibility.](image)

![Figure 9. Evaluation and Test Results of Network Connection Credibility.](image)

As is shown in Fig. 3-6, the training set covers as many types of attacks as possible when training the neural network. In this manner, the neural network can learn various abnormal network models and make an effective evaluation of connection credibility. After training many times, good simulation results are achieved (Fig. 8). The evaluation accuracy is 93.50% while the mean-square error is 0.0310, indicating a small difference between the actual output and the expected output. According to the evaluation flow of network connection credibility, the neural network training achieves success. Fig. 9 shows the simulation results achieved by a successfully trained neural network. The evaluation accuracy is 91.94% and the mean-square error is 0.0702, indicating that the successfully trained neural network could achieve high accuracy in connection credibility evaluation and prediction.

### V. CONCLUSIONS

Different from the traditional research on network security, this paper studies the quantitative evaluation of connection credibility and corresponding security strategies. Based on the analysis of the KDDCup99 data set, this paper proposes an index system for the evaluation of connection credibility and an innovative method for credibility evaluation, using the learning and generalization ability of BP Neural Network. The simulation results indicate the method achieves high evaluation accuracy and can be applied to various network security systems effectively. Of course, applying trusted computing to the research on evaluation of network connection credibility is a novel research domain, and during the research process, various difficulties will turn up. As a result, some assumption and restriction can help the promotion of relative research. At
the same time, attack assorting, connection differentiation initiative set, and the dynamic evaluation of connection state are not accurate now. In future research, we’ll focus on breaking the theory and technology difficulties in principle integration of network credibility evaluation and dynamic tuning of actual evaluation process. Ultimately, the perfect match between the whole model and all of the technology will be reached, implementing the dynamics, automaticity, accuracy; and efficiency.

ACKNOWLEDGMENT

The authors want to thank anonymous reviewers for their valuable comments and suggestions. The work was supported by National Natural Science Foundation of China Grant No. 61003035, Foundation of He’nan Educational Committee No. 2009A520012, Foundation for University Young Key Teacher by He’nan Educational Committee No.[2009]844.

REFERENCES


Qingtao Wu was born in Jiangxi Province, China on 03/13/1975. He received M.S. degree in computer science from Henan University of Science and Technology, Luoyang, China in 2003, the D.E. degree in computer applications from East China University of Science and Technology, Shanghai, China in 2006. Currently He is working as an Associate Professor and Vice-Director in Electronic and Information Engineering College, Henan University of Science and Technology. His interest includes information security and software formal methods.

Xintong Yang was born in Henan Province, China in 1985. She received her bachelor of engineering degree in computer science and technology in Henan Agricultural University in China in 2008. Since September 2008, she has been working for her master of engineering degree in Henan University of Science and Technology. Her research interests are in the area of information security.

Bin Hua was born in Henan Province, China in 1983. He received his B.S degree in mathematics in Henan University of Science and Technology in China in 2007. Since September 2008, he has been working for his master of engineering degree in Henan University of Science and Technology. His research interests are in the area of intrusion tolerance technology.

Ruijuan Zheng was born in Henan Province, China in 1980. She received her bachelor of engineering degree and PhD degree all from the computer application, at Harbin Engineering University. Currently She is working as an Associate Professor and Vice-Head in Dept. of computer Science, Electronic and Information Engineering College, Henan University of Science and Technology in China. Her main interests are in the area of network security theory and technology and autonomic computing.