Analysis of Network Security Situation within a National Perspective using the Analytic Hierarchy Process

Rui WU¹, Jun ZHU², xiaolong ZHAO¹

¹Department of Computer Science and Technology, Anhui Technical College of Industry and Economy, Hefei Anhui, 230051, China
²Department of Computer Science and Technology, Anhui University of Science and Technology, Huainan 232001, China

Abstract — In order to promote the accurate evaluation of network security situation, a model integrating grey correlation analysis and support vector machine is proposed. An evaluation index system is selected first, and index weight is determined according to grey correlation analysis, then a training sample is input into support vector machine. Improved particle swarm optimization is used to optimize the support vector machine parameters and establish network security situation evaluation model. Finally a data set DARPA99 is adopted to conduct simulation test for model performance. Stimulation results show that the model can evaluate network security situation accurately and objectively and evaluation results can provide certain advisory opinion for network administrators.

Keywords- network security; network attack; situation evaluation; grey correlation analysis; support vector machine

I. INTRODUCTION

Traditional detection system is a passive network security defense method and it can not describe current network system security status and future status accurately and comprehensively. However, network security situation (NSS) is a positive defense method which can monitor network security situation in real time and can predict future security status accurately. It overcomes shortcomings of traditional detection system effectively and becomes hot issues in current network security study [1,2]. Grey correlation analysis method is a multi-factor statistical analysis method, which can determine index weight objectively. Particle swarm optimization has advantages such as few parameters and global searching ability and it is an intelligent optimization algorithm. It is widely used in multi-objective optimization. Therefore, they can be introduced into network security situation evaluation to promote accuracy of situation evaluation results and enhance reliability of evaluation results [10]. For this reason, a network security situation evaluation model integrating grey correlation analysis and support vector machine is proposed. Grey correlation analysis is used to determine weight of evaluation index first of all and then particle swarm optimization is adopted to optimize support vector machine parameters and establish network security situation evaluation model. At last, specific simulation tests are conducted to test effectiveness and superiority of the model.

II. NETWORK SECURITY SITUATION INDEX CONSTRUCTION AND QUANTIFICATION

The word “situation” comes from military domain and it describes status of the study object with huge scope, complicated structure and multiple factor influence. “Situation” is introduced into network security to establish a set of feasible network security situation system so as to understand comprehensive security status of network quickly and comprehensively. Network security system is influenced by many factors and is the result under their comprehensive effects and it has uncertainty and randomness. Network security is influenced by attack frequency and number of attack source and occupancy rate of bandwidth. Influence of factors on network security varies along time change and there is a non-linear relationship between network security and influence factor. Therefore, in order to evaluate network security accurately, the most suitable network security evaluation index shall be selected first of all to establish corresponding evaluation system.

A. Establish Network Security Situation Evaluation Index System

According to network security situation evaluation principle and based on uncertainty and dynamic nature of network complexity, 6 evaluation indexes closely related to network system security situation are selected in the research to establish network security evaluation index system. They are: attack type priority, number of attack source, attack frequency, time importance degree, bandwidth occupancy rate and importance of host. Namely: \( U = \{ \text{attack type priority, number of attack source, attack frequency, time importance degree, bandwidth occupancy rate, importance of host}\}. \)

B. Network Security Situation Evaluation Index Quantification

(1) More frequency network attack in certain period shows more serious threat confronted by network. In order to reduce influence of attack frequency on threat degree into \([0,0,1,0]\) scope, specific quantification is as follows:
\[ y(f) = f / (1 + f), f \in [0, \infty), y \in [0, 1) \] (1)

Where, \( f \) is number of times for the same type of attack event which occurs in unit time.

(2) Generally, for coordinated attack, the more attack source, the huger threat network may face. In order to reduce influence of number of attack source on threat degree into \([0.0, 1.0)\) value domain scope, specific quantification is as follows:

\[ y(u) = u / (1 + u), u \in [0, \infty), y \in [0, 1) \] (2)

(3) For risk level features evaluation of network security, evaluation set \( V \) of the model is divided into 5 grades: Very Low, Low, Moderate, High and Very High, namely

\[ V = \{ VL, L, M, H, VH \} \] (3)

Network security evaluation standard is shown in Table 1.

<table>
<thead>
<tr>
<th>Evaluation index</th>
<th>VL</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>VH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack threat grade</td>
<td>3.0</td>
<td>2.5</td>
<td>2.0</td>
<td>1.5</td>
<td>1.0</td>
</tr>
<tr>
<td>Number of attack source</td>
<td>0.0</td>
<td>1.0</td>
<td>2.0</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Attack frequency</td>
<td>1.0</td>
<td>5.0</td>
<td>10.0</td>
<td>15.0</td>
<td>20.0</td>
</tr>
<tr>
<td>Time importance degree</td>
<td>1.0</td>
<td>2.0</td>
<td>3.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Bandwidth occupancy rate</td>
<td>0.0</td>
<td>1.0</td>
<td>2.0</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Importance of host</td>
<td>0.0</td>
<td>2.0</td>
<td>4.0</td>
<td>6.0</td>
<td>8.0</td>
</tr>
</tbody>
</table>

C. Establish Network Security Situation Evaluation Matrix

First of all, each index \( u_i \) shall be graded according to \( v_j \) in evaluation set \( V \); then the following formula shall be used to calculate value rij of each index \( u_i \) in relation to the jth element \( v_j \) in the evaluation set \( V \), namely

\[ r_{ij} = n_{ij} / n_{\text{\#}} \] (4)

Where, \( n_{ij} \) is the number of expert making the jth evaluation for the ith index \( u_i \) in the index set; \( n_{\text{\#}} \) is total number of expert.

Evaluation vector of index \( u_i \) can be gained

\[ r_i = (r_{i1}, r_{i2}, \cdots, r_{ik}) \] (5)

Above method shows that there are \( n \) evaluation vectors \( r_1, r_2, \cdots, r_n \) for \( n \) indexes. A mapping relation can be determined in this way.

\[ R = (r_1, r_2, \cdots, r_n) \] (6)

Network security situation evaluation matrix is

\[ R = \begin{pmatrix} r_1^1 & \cdots & r_1^n \\ \vdots & \ddots & \vdots \\ r_n^1 & \cdots & r_n^n \end{pmatrix} \] (7)

III. GREY CORRELATION ANALYSIS DETERMINES WEIGHT OF INDEX SET

Assume \( X_i \) is system evaluation index and its observation data is \( x_{ik}(k), k = 1, 2, \cdots, n \). \( X_i = (x_i(1), x_i(2), \cdots, x_i(n)) \) is called behavioral sequence of evaluation index \( X_i \). Grey correlation analysis method can be divided into the following steps:

(1) Assume m data sequences form the following matrix:

\[ \begin{pmatrix} \hat{x}_1 \cdots \hat{x}_n \\ \vdots \ddots \vdots \\ \hat{x}_1 \cdots \hat{x}_n \end{pmatrix} \] (8)

Where, \( n \) is the number of indexes, 

\[ X_i = (x_i(1), x_i(2), \cdots, x_i(n)) \] (9)

(2) Reference data is listed as

\[ X_0 = (x_0(1), x_0(2), \cdots, x_0(n)) \] (10)

(3) Index data shall be non-dimensional. Specific process is as follows

\[ x_i(k) = \frac{x_i(k)}{\sum_{k=1}^{m} x_i(k)} \] (11)

\[ x_i(k) = \frac{x_i(k)}{x_i(1)} \] (12)

(4) Compare absolute difference between sequence and corresponding element of reference sequence, namely

\[ \left| x_i(k) - x_i(k) \right| \] (13)
(5) Determine \( \min_{i=1}^{n} \min_{k=1}^{m} |x_{0}(k) - x_{i}(k)| \) and \( \max_{i=1}^{n} \max_{k=1}^{m} |x_{0}(k) - x_{i}(k)| \).

(6) Calculate correlation coefficient between each comparative sequence and corresponding element of reference sequence respectively, namely

\[
\xi(k) = \frac{\min_{i=1}^{n} \min_{k=1}^{m} |x_{0}(k) - x_{i}(k)| + \rho \max_{i=1}^{n} \max_{k=1}^{m} |x_{0}(k) - x_{i}(k)|}{|x_{0}(k) - x_{i}(k)| + \rho \max_{i=1}^{n} \max_{k=1}^{m} |x_{0}(k) - x_{i}(k)|}
\]

Where, \( k = 1, 2, \ldots, m \) . \( \rho \) is resolution ratio and its value is in \((0,1)\). Less \( \rho \) shows stronger distinguishing capability of correlation coefficient.

(7) Calculate average correlation coefficient. For comparative sequence, mean value of its \( n \) indexes and correlation coefficient of corresponding element of reference sequence shall be calculated to reflect correlation relationship between reference sequence and comparative sequence, which is called average correlation coefficient, namely \( r_{0i} \). There is

\[
r_{0i} = \frac{1}{m} \sum_{k=1}^{m} \xi_{i}(k) \quad i = 1, \ldots, n
\]

(8) Get evaluation results according to average correlation coefficient.

(9) \( r_{0i} \) shall form vector \( r = (r_{01}, r_{02}, \ldots, r_{0n}) \) according to the results of grey correlation analysis. After normalization processing, weight vector of each index is

\[
W = (w_{1}, w_{2}, \ldots, w_{n})
\]

IV. ESTABLISH NETWORK SECURITY SITUATION EVALUATION MODEL

A. Principle of Support Vector Machine

For the given data set: \((x_{i}, y_{i})\), according to risk minimization principle, optimal hyperplane expression of SVM is:

\[
y = w^{T} \varphi (x) + b
\]

Where, \( w \) is normal vector of hyperplane and \( b \) is offset vector of hyperplane.

If it is a nonlinear classification problem, the nonlinear classification problem will turn into quadratic optimization problem, namely:

\[
\min_{w, \xi} J(w, \xi) = \frac{1}{2} ||w||^{2} + c \sum_{i=1}^{n} \xi_{i}
\]

Corresponding constraint condition is:

\[
y_{i}(w^{T} \Phi(x_{i}) + b) \geq 1 - \xi_{i}
\]

\[
\xi_{i} \geq 0, i = 1, 2, \ldots, n
\]

Where, \( \xi = (\xi_{1}, \ldots, \xi_{n})^{T} \), \( c \) is penalty parameter.

For classification problem of large sample, learning rate of SVM is slow. Lagrange multiplier may be introduced to turn SVM classification problem into its dual problem, which can be used to solve this hyperplane optimization problem and accelerate classification speed and gain SVM decision-making function:

\[
f(x) = \text{sign} \left( \sum_{i=1}^{n} \alpha_{i} y_{i} (\varphi(x) \cdot \varphi(x_{i})) + b \right)
\]

Where, \( \text{sign} \) is sign function and \( \alpha_{i} \) is Lagrange multiplier.

Different kernel functions shall be used to generate different support vector classifiers. Commonly-used kernel functions are radial base function (RBF), polynomial kernel function and Sigmoid function. As RBF only needs to determine one parameter (namely width parameter \( \sigma \) of kernel function), it is good for parameter optimization. Therefore, RBF kernel function is selected in the research to construct support vector machine. Definition of RBF kernel function is as follows:

\[
k(x_{i}, x_{j}) = \exp \left( - \frac{||x_{i} - x_{j}||^{2}}{2\sigma^{2}} \right)
\]

B. Principle of Particle Swarm Optimization Algorithm

Enlightened by flying behavior of bird flock, Eberhart and some people proposed particle swarm optimization (PSO) algorithm in 1999, which takes particle as a feasible solution in problem space and lead particle to fly in the multi-dimensional space of solution through information of itself and its companions so as to find optimal position of the particle [11]; Position and speed of particle \( i \) are represented as \( Xi(t) \) and \( Vi(t) \) respectively. Individual optimal solution (Pbest) and population optimal solution (gbest) of the particle will update their speed and position in iteration process. Specific content is:
\[ V_a(t+1) = w(t) + c_1(P_{best}(t) - \mathbf{x}_a(t)) + c_2(P(t) - \mathbf{x}_a(t)) \]  
\[ X_a(t+1) = X_a(t) + V_a(t+1) \]  

(22)  

(23)  

Where, \( w \) is inertia weight; \( c_1, c_2 \) is acceleration constant. Generally \( c_1 = c_2 = 2; r_1 \text{ and } r_2 \) are random between 0 and 1.

Many research show that, in basic particle swarm optimization algorithm, when certain particle finds a local optimal solution, it will attract other particles and other particle will fly to the particle quickly and flaws such as precocity of particle swarm and local optimization may occur. In order to overcome shortcomings of basic particle swarm optimization algorithm, based on uncertainty and randomness of chaos theory, chaotic mutation operator can be used to improve basic particle swarm optimization algorithm. Specific improvement thought is: chaotic mutation operation shall be conducted for \( \mathbf{g}_{best} \) particles corresponding to particle swarm when particle flies so as to prevent position convergence of particles and make other particles jump out of the local optimal solution as soon as possible.

Logistic mapping formula is

\[ Z_{n+1} = 4Z_n(1 - Z_n) \]  

(24)  

Where, \( Z_n \) is chaos variable.

Chaotic disturbance shall be added to (25) according to chaos principle, namely:

\[ Z'_k = (1 - \alpha)Z^* + \alpha Z_k \]  

(25)  

Where, \( \alpha \in [0,1] \) showing strength of disturbance. \( Z_k \) and \( Z'_k \) represent chaos vector after \( k \) times of and iteration and addition of disturbance.

Disturbance strength \( \alpha \) is adopted for self-adaptive value-taking. In the initial period of searching, its value is huge, which will strengthen disturbance to solution vector and then its value will decrease gradually. Specific process is:

\[ \alpha(k) = 1 - \left( \frac{k - 1}{k} \right)^a \]  

(26)  

Where, \( n \) is integer.

C. Steps for support Vector Machine Parameter of Particle Swarm Optimization

1. Determine particle swarm scale \( m \) according to problem scale; conduct initialization treatment on particles; two-dimensional vectors of particle represent parameter \( C \) and \( \sigma \); determine maximum iteration times and other parameters.

2. Use support vector machine to conduct training modeling for training sample; calculate fitness value of particles.

3. Compare and update particle and its individual history optimum value and population history optimum value.

4. Use Equation (22) and (23) to update particles.

5. Conduct chaotic disturbance for partial optimal particles; keep individual diversity of particle swarm.

6. Judge end condition; if it meets end condition, transfers to step (6); otherwise, iteration time shall be added and it will return to step (2) for continuous optimization.

7. Conduct anti-coding for position of optimal particle and gain optimal value of support vector machine parameter \( C \) and \( \sigma \).

8. Use support vector machine of optimal parameter \( C \) and \( \sigma \) to train network security situation training sample and establish corresponding network security situation evaluation model.

9. Use specific network security situation data to inspect model performance.

To sum up, work flow of network security situation evaluation model integrating grey correlation analysis and support vector machine is shown in Fig.1.
V. SIMULATION EXPERIMENT

A. Simulation Environment

In order to test performance of network security situation evaluation model in the research, hardware environment of simulation is: CPU P4 3.0G, 1G memory, free space of hard disk is 20G, 2M special network card; software environment: Windows XP operating system, Matlab 2007 kit. Simulation experiment data comes from network intrusion detection data set KDD CUP99 of American MIT Lincoln Laboratory [12]. Data is divided into two parts. One part is training sample, which is used for support vector machine training and used to establish network security situation evaluation model; the other parts are testing sample, which are used to inspect consistency between network security situation evaluation results of model and truth results.

B. Model Performance Evaluation Index

Model performance evaluation index uses attack energy. According to network threat situation evaluation principle, calculation function of network attack energy is:

\[ E = \sum F(H + 1)T / A \]  

(27)

Where, \( F \) is attack frequency; \( T \) is time importance degree; \( H \) is importance of host; \( A \) is threat grade of attack.

C. Results and Analysis

Grey correlation analysis is adopted to determine weight of evaluation index and then particle swarm optimization support vector machine is adopted to evaluate network security situation. Network security situation evaluation results are shown in Fig.2. Network attack energy change

![Diagram of network security evaluation procedure]
Figure 2. Network security situation figure

Figure 3. Network attack energy change curve

Comparison of results of Fig.2 and Fig.3 shows that, network security threat situation value curve of the model coincides with network attack energy curve basically. It shows that, result of network security threat situation evaluation conducted with evaluation algorithm proposed in the research is reasonable and effective and it is a network security situation evaluation algorithm with high evaluation accuracy.

VI. CONCLUSIONS

Network security situation evaluation can monitor network security change tendency and find out potential and possible network attack behaviors. Therefore, effective protection measures can be taken to promote network security. In terms of current problems in network security situation evaluation, based on advantages of gray correlation analysis theory and support vector machine algorithm, a network security evaluation model integrating grey correlation analysis and support vector machine is proposed. Simulation results show that, the model can capture comprehensive change tendency of network security and make accurate and objective evaluation on network security situation. Evaluation results help to guide network administrator to take corresponding countermeasures for possible network security events in the future.

ACKNOWLEDGMENTS

The Anhui province quality engineering teaching research project Foundation of China under Grant No. 2015CKJH135; the Key project of quality engineering teaching research in Anhui Province Foundation of China under Grant No. 2014jyxm588.

REFERENCES


