

Genetic Algorithm based Application Research in Computer Network Security Evaluation

Priya Rathi
Computer Science & Engineering
P.R.M.I.T.&R., Badnera

Prof. Falesh M. Shelke
Computer Science & Engineering
P.R.P.C.E., Amravati

Abstract—Network security is a complex systematic job. Current safety methods available are having some shortcomings like feasibility, man made interference, smaller application scope and so on. The imitation results shows that using the established evaluation model for network security assessment is simple, also eliminate the interference of human factors and can quickly find the correct results of the assessment. This article provides new ideas and methods to work for a wide-ranging evaluation of computer network security condition, specially with a certain reference value to predict and control of network security issues in the future.

Keywords- Genetic Algorithm, Computer Network, Security Evaluation.

I. INTRODUCTION

In 1980s countries around the world have developed a number of IT security evaluation criterion. From these standards, Trusted Computer System Evaluation Criteria (TCSEC) is known as Orange Book, introduced by the U.S. Department of Defense is the initial one. additional standards are basically the basis of it [1]. Initial TCSEC is for isolated computer systems specially for minicomputers and mainframe systems and this standard applies only to military & government not applicable for the enterprise. TCSEC and ITSEC are not involved in open systems and they are static model only reflecting the static security situation [2]. CTCPEC has a certain development based on them but failed to break above limitations. Then FC makes additions and modifications on the TCSEC which defined in protection profiles and security targets, cleared detailed outline of the system security requirements provided by the user, but it has not been formally put into use because of some defects. CC defines the basis guidelines as the assessment of IT products and systems security. compare with the early assessment criteria, its advantage is the openness of its construction, completeness of expression mode and usefulness [3].

II. SAFETY ANALYSIS OF COMPLEX NETWORK

A. Information security concept of space and time

Information system's component has three special characteristics.

Lateral distribution: Network makes the information system showing the geographical distribution characteristics. The LAN, MAN or even WAN across multiple provinces is characterized by a highly distributed.

Vertical levels: Any network device, that is, the nodes in the network topology, regardless of the lateral distribution structure and scale of the network has emerged as a top-down hierarchical characteristic.

Structural isomerization: Components parts of the network are ever-changing, and this poses a challenge for the information security system.

B. The safety of complex systems

Domain in complex systems. Security domain in complex system exists contain and cross relations, in fact, the definition of complex systems is only a relative relation, not strictly accurate. Although "cross" and "contain" in complex system domain can be simplistic in theory, it does not mean that the system is not complicated. Because of the size and number in complex system domain are much bigger than the simple systems, and the entire security policy in a complex system is also much more complex than the simple system. Complex system security. Inter-domain relations in complex system removed the 'cross' and 'contains', theoretically can be dealt with method as simple system security, provided that each domain's security policy after proper treatment can be reflected the security policy before processed accurately and completely. Maintaining the invariance of the entire system security policy is issue of security policy dealing with, and this can be accomplished through the management coordination in reality.

Security theorem of complex systems: In any composition of the complex system, set the domains in system are D_1, D_2, \dots, D_N . Inter-domain exists 'cross' and 'contains' relation, after removing 'cross' and 'contains', domains in systems is D_1, D_2, \dots, D_M . System is secure when:

- Simple system is consisted by domain

D_1', D_2', \dots, D_M' is secure;

•System policies before and after treatment are consistent,

that is,
$$\bigoplus_{i=1}^M P_i \oplus_{i=1}^N P_i$$

III. ESTABLISHMENT OF NETWORK SECURITY EVALUATION INDICATOR SYSTEM

In this paper, we use Delphi method to determine the comprehensive evaluation indicator system for network security. Through systematic analysis, initially study out the evaluation indicator and the classification. Prepare the evaluation inquiry form and seek expert advice to screen indicators. Importance degree of indicators is divided into five, and the smaller value means more important. Set a certain level in the proposed indicator system has two indicators, and request n experts' evaluation. Experts' concentration ratio is defined as:

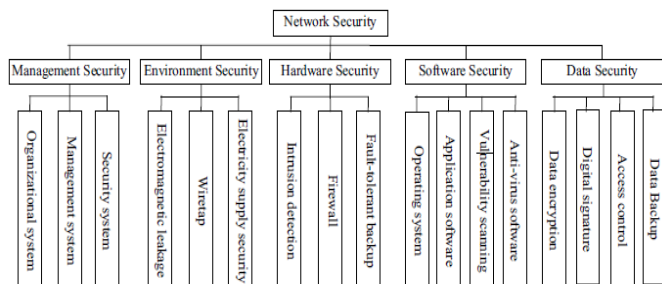


Figure1. Comprehensive evaluation indicator system of network security

IV. THE IMPLEMENTATION OF THE GA ALGORITHM

A. Coding

The real-coded is each connection weights represented by real number. Genetic manipulation is directly operated on the two sets of real numbers, which is very intuitive. Chromosome is expressed as:

$$(1, 2, \dots, 17) \phi \quad \phi = \text{the number of input unit,}$$

In this paper, it is the network security input indicator data. 10ϕ is threshold vector. The total length of the gene string is 96. In order to reduce the chromosome length, the network weights and threshold are independently coded and genetic manipulation.

B. Initialization and fitness function

The genetic operations are carried out among many individuals at the same time, and these individuals are formed a group. Population size must meet the diversity of the population, also taking into account the efficiency of the GA search. Consider the above factors, the popsize is 50 in

the system. Take a random value from each element range $[-1, 1]$ as the initial value and constitute the initial population.

$$E_i = \frac{1}{n} \sum_{j=1}^n a_j, (i=1, 2, \dots, m) \quad (1)$$

Experts' dispersed degree is defined as:

$$\sigma_i = \sqrt{\frac{1}{n-1} \sum_{j=1}^n (a_j - E_i)^2} \quad (2)$$

a_j is the j-th expert's rating.

According to the characteristics of network security, select the following indicators showed in figure1 in the condition $3, 0.62 \leq \sigma \leq 0.62$.

GA is used for searching for the optimal function

$$\theta_c = \{c_{ij}, b_{ij}\}, \text{ parameter in order to}$$

$$\min E = \frac{1}{2} \sum_{k=1}^r (y_{ak} - y_i)^2 \quad (3)$$

Y_{ak} and Y_i are represented the desired output and actual output. Then, calculate the fitness value of each chromosome

according to the following formula

$$f_t (t=1, 2, \dots, \text{popsize}),$$

$$f_t = \frac{1}{E} \quad (4)$$

C. Ratio Selection

Compute the fitness value of each chromosome

$$\theta_c = \{c_{ij}, b_{ij}\} (t=1, 2, \dots, \text{popsize})$$

Denoted by $eval(\theta_i)$

Compute the total fitness values:

$$f = \sum_{t=1}^{\text{popsize}} eval(\theta) \quad (5)$$

Compute selection probability P_t of each chromosome

$$\theta_c = \{c_{ij}, b_{ij}\} (t=1, 2, \dots, \text{popsize}),$$

$$p_t = \frac{eval(\theta_t)}{F} \quad (6)$$

Compute cumulative probability q_t each chromosome

$$\theta_c = \{c_{ij}, b_{ij}\} (t=1, 2, \dots, popsize),$$

$$q_t = \sum_{j=1}^t p_j \quad (7)$$

Produce a random float r in $[0,1]$.

If $r < q_t$, select the first one (q_t) chromosome, otherwise, select the t -th chromosomes $\theta_t (2 \leq t \leq popsize)$ that make $q_{t-1} \leq r \leq q_t$ established.

D. Crossover

Simple crossover: According to pattern of traditional Genetic Algorithm, similarly to the binary crossover, the crossover is divided between the floats. Arithmetical crossover: A linear combination of the two vectors. If they are described as S_1 and S_2 , the future generation is:

$$S_w^{t+1} = \alpha S_w^t + (1-\alpha) S_v^t \text{ and } S_v^{t+1} = \alpha S_v^t + (1-\alpha) S_w^t, \alpha \text{ is the probability of crossover. Produce a random float } r \text{ in } [0,1].$$

If $r < p_c$, select a given chromosome to crossover. Crossover operator use the arithmetical crossover and $\alpha = p_c$

E. Variation

In this paper, we use uniform variation. If $X_i^t = (v_1, \dots, v_n)$ is a chromosome, each element has the same variation opportunities. A single application of this life is the vector

$$(V_1, \dots, V_k, \dots, V_n), 1 \leq k \leq n. \text{ Produce a random float } r \text{ in } [0,1].$$

If $r < p_m$, make this element occur uniform variation.

An example

Assuming the agent detection unit reliability is R , the time of detection agents unit is T , and according to the model the time does not exceed S . The corresponding values are as follows:

$$R = \{r_t\} = \begin{bmatrix} 0.920 & 0.908 & 0.898 & 0.892 & 0.880 & 0.880 & 0.865 & 0.862 & 0.860 & 0.858 \\ 0.855 & 0.830 & 0.825 & 0.822 & 0.820 & 0.818 & 0.815 & 0.810 & 0.805 & 0.801 \\ 0.800 & 0.800 & 0.798 & 0.796 & 0.795 & 0.790 & 0.788 & 0.782 & 0.780 & 0.777 \\ 0.775 & 0.773 & 0.772 & 0.770 & 0.769 & 0.766 & 0.765 & 0.763 & 0.760 & 0.758 \\ 0.756 & 0.750 & 0.730 & 0.720 & 0.715 & 0.710 & 0.708 & 0.705 & 0.703 & 0.701 \end{bmatrix}$$

$$T = \{t_i\} = \begin{bmatrix} 0.80 & 0.82 & 0.85 & 0.80 & 0.82 & 0.80 & 0.86 & 0.80 & 0.85 & 0.85 \\ 0.80 & 0.85 & 0.80 & 0.88 & 0.80 & 0.82 & 0.82 & 0.80 & 0.80 & 0.82 \\ 0.80 & 0.88 & 0.75 & 0.72 & 0.75 & 0.78 & 0.70 & 0.72 & 0.70 & 0.80 \\ 0.75 & 0.60 & 0.60 & 0.60 & 0.70 & 0.60 & 0.75 & 0.60 & 0.65 & 0.70 \\ 0.70 & 0.75 & 0.75 & 0.70 & 0.70 & 0.60 & 0.74 & 0.64 & 0.72 & 0.71 \end{bmatrix}$$

About the above detection agents optimization problem, we use the modified genetic algorithm to optimize, taking the operating parameters of the genetic algorithm population size M , the maximum termination of the algebra T , the crossover probability P_c , and mutation probability P_m :

Table.1 Optimization results

S	Decision variables	Solution Results
8.5	0000000101010000000111000	9.804
	0101000011000010001000000	8.440
10	0000000100010000000111001	11.446
	0101000111001010001000000	9.960
13.1	0000000101010010000111001	15.047
	0101000111110011001000010	13.050
17.6	0100000101111011000110111	19.614
	0101000111011001011000001	17.530
23.4	0110000111111011000111111	25.798
	0101001111111011011001011	23.370

V. CONCLUSIONS

This paper firstly discussed the factors that affect network security and the most commonly used security measures, and used Delphi method to filter safety indicators and established a more comprehensive network security comprehensive evaluation indicator system. Then we established a network security comprehensive evaluation model by genetic algorithms to evaluate the results of further analysis. This paper provides a comprehensive evaluation of computer network security with new ideas and methods. Model established in this paper of the Network

Security Evaluation and Certification has a higher theoretical value and broad application prospects.

REFERENCES

- [1] M. R. Azimi-Sadjadi, R. J. Lion. Fast Learning Process of Multilayer Neural Networks Using Resursive Least Squares Method. IEEE Trans.On SP, Vol.40(2010), p.446~450.
- [2] Kennedy, J. and Eberhart. R. C. Particle swarm optimization. In Proc. IEEE International Conference on Neural Networks, IEEE Service Center, pisataway, NJ, 2010, p. 39~43.
- [3] Duta S, Shekhar S. Bond rating: a non-conservative application of neural networks. Proc IEEE Int Conf on Neural Networks[C].San Diego: IEEE, 2011, p. 443~450.
- [4] Sobajic DJ, Pao YH. Artificial neural net based dynamic security assessment for electric power systems.IEEE Trans.On Power Systems, Vol.4(2009), p.220~226.
- [5] Gordon R.T. Artificial neural network approach to assessment. Intelligent Engineering Systems Through Networks, Vol.4(2007), p.1175~1180.
- [6] Molina AM Chou K C. Application of Neural Networks for the Performance Evaluation of Bridges. Probabilistic Mechanics and Structural and Geotechnical Reliability, Proceedings of the Specialty Conference. Sponsored by ASCE,2008, p.298~301.