Optimal Design of Computer Network Security Performance Based on Genetic Algorithm

Fengfeng Chen¹,*

¹Gongqing College of Nanchang University, GongQing City, China

*Corresponding author email: chenfengfeng@ncuphy.edu.cn

Abstract. With the current implementation of my country's reform and opening up, a large number of advanced concepts have been introduced for domestic science and technology, the purpose is to gradually optimize the security performance of domestic computer network (CN) systems. Network security cannot be guaranteed and the development process of CNs cannot be guaranteed. Therefore, people apply genetic algorithms to the innovation and development of CN security performance and obtain more optimization benefits. CN attack technology is diverse and concealed, which makes it difficult to be detected, seriously endangering CN security and accurately identifying network abnormalities. In order to overcome the shortcomings of traditional network security and the low detection accuracy of anomaly detection technology, a genetic algorithm-based support vector machine-based network security performance optimization method was developed. This article first reviews the research and development of CN security systems at home and abroad, summarizes the main problems currently facing the research field of CN security systems, and introduces the main performance optimization technologies, aiming at the current existing CNs, ubiquitous performance shortcomings and problems of security systems, based on the in-depth analysis of the characteristics of network attacks and intrusions, have carried out a more systematic study of the genetic algorithm theory. The experimental results show that the network anomaly detection accuracy of the least square support vector machine classifier based on genetic algorithm optimization is high and the effect is good, which provides a reliable guarantee for the optimization of network security performance.

Key words: Genetic Algorithm, Support Vector Machine, Network Security Performance, Intrusion Detection

1. Introduction

CN security mainly refers to the use of relatively effective network security management and control technology to protect the hardware and software resources in the network system to prevent accidental or malicious reasons from being destroyed, modified and leaked, so that the CN The system can operate normally, and the network service works normally and orderly. Computer security usually includes two major aspects. Information system security and control system security are mainly divided into the following aspects: on the one hand, it is the delivery of safe information to users, on
the other hand, the personal information privacy resources owned by users\textsuperscript{[2,3]}. The security of information systems pursues integrity, availability, confidentiality and truthfulness. The security of the control system requires identity authentication, authorization and access control. Compared with other systems, CNs have higher requirements for reliability, availability, confidentiality, integrity, authenticity, and controllability \textsuperscript{[4]}. However, with the development of computers and networks, the security threats they are subject to have become more and more serious. Due to the loopholes in network security, computers and networks are very vulnerable to various viruses and illegal intrusions from network hackers \textsuperscript{[5]}.

With the rapid development of the CN application field, the network environment has become increasingly complex, and the network security performance identification technology is designed to ensure the security of the network system, which can detect the types of network attacks in time \textsuperscript{[6]}. The diversity and concealment of CN attacks make it difficult to be discovered \textsuperscript{[7]}. In the description of the principle of the network anomaly detection method combining genetic algorithm and least square support vector machine, the classification theory of least square support vector machine is introduced first, and the combined classification method of genetic algorithm and support vector machine is proposed. On this basis, a network anomaly detection method combining genetic algorithm and least square support vector machine is proposed. Finally, the shortcomings of testing the model and analyzing over-fitting have led to a low detection rate of network attacks, which is far from being able to meet the needs of network intrusion detection \textsuperscript{[8]}. In this regard, according to the network intrusion detection method of support vector machines, the least squares support vector machine classifier (LSSVC) is an improved support vector machine classifier, which replaces the loss function in the support vector machine with a quadratic loss function \textsuperscript{[9]}. In the use environment of the CN system, due to the openness of the network, it will be interfered by many dangerous factors, such as virus intrusion, illegal access, malicious attacks, etc., if there is no good network security performance to optimize the maintenance of the system, it will cause the network system The damage seriously affects the normal work order. In the maintenance of the CN security system, in order to fully and effectively ensure the security of the network system and improve the performance and efficiency of the CN in intrusion detection, finally realized a CN intrusion detection system based on genetic algorithm research. Based on this, we first analyzed the basic model of CN security system intrusion detection, and then proposed an improved multi-mode genetic algorithm for CN intrusion detection system based on the obtained detection results, and put the updated genetic algorithm together CN. Then, by analyzing the multi-pattern matching algorithm of the security system of the CN during intrusion detection, a CN intrusion detection system based on the multi-pattern genetic algorithm is designed to improve the effectiveness of the algorithm \textsuperscript{[10]}.  

2. The establishment of genetic algorithm and its improvement analysis

2.1. The establishment of genetic algorithm

Suppose n samples are the input vector, and $x_{(i)}$ is the input vector. It replaces the insensitive function in the support vector machine with a quadratic function. The following functions are minimized as follows:

$$J(\omega + \delta) = \frac{1}{2} |\omega|^2 + \frac{1}{2} \sum_{i=1}^{n} y_i \delta_i^2$$

(1)

According to the above formula, where C is a parameter, it can be used to control $J(\omega+\delta)$.

Due to the above problems, Lagrange multipliers are introduced to solve the above optimization problems:

$$L(T_m(x_i) \neq y_i) = \sum_{i=1}^{N} w_{mi}exp\left(-a_{mi}y_i T_m(x_i)\right)$$

(2)
According to the above formula, the most classification function of least squares support vector machine is:

$$y(x) = \text{sign} \left[ \sum_{i=1}^{n} a_i y_i k(x, x_i) + b \right]$$

(3)

Among them, \(k(x, x_i)\) is the core function. This paper chooses the Gaussian radial basis kernel function to construct the least square support vector machine to classify it.

Genetic algorithm is an optimization algorithm that simulates biological evolution mechanism through natural selection and computer. In the rapid development of modernization, organisms adapt to the external environment through heredity and mutation, survive generation after generation of survival of the fittest, and develop and evolve. Genetic simulation of the above evolutionary phenomenon.

2.2. Analysis of network security performance based on data mining

2.2.1. Dynamic neighborhood radius

The reachable distance of dynamic neighborhood radius adaptive density is defined as:

$$R_A = R \frac{A_i}{A_{i+1}}$$

(4)

2.2.2. Data point density

The formula can be expressed as:

$$\text{density}(x_i) = \sum_{j=1}^{n} \ell \frac{d(x_i, x_j)^2}{2\sigma^2}$$

(5)

2.2.3. Density reachable distance

This is any specific data object \(x\) in the data cluster space, as well as the distance \(r\) between the data, a circular area centered on specific data, a circle whose radius is the data distance, corresponding to the accessible density distance field of the data object.

$$R = \text{coef} R_X \text{mean}(D)$$

(6)

3. Modeling method

3.1. BP neural network model establishment

As mentioned above, because of the limited number of samples in the training set, this article only fine-tunes on the basis of the training set, so the correction rate cannot be too large. In this article, the initial correction rate of the model is 30%, and the correction rate increases by 80% every 2 cycles of training.

$$l_r = l_{r0} \alpha^{t/2}$$

(7)

In the formula: \(l_{r0}=30\%\); \(\alpha=0.2\), \(t\) is the current number of training cycles; rounded down. The loss function is defined as cross entropy, and the formula is as follows:

$$L = \sum_{i=1}^{K} y_i \log y_i'$$

(8)

Where: \(y\) and \(y'\) are the true label and predicted input of the picture, respectively; \(K=6\) is the number of categories. This paper uses the stochastic gradient descent algorithm with momentum as the optimizer, and each parameter update is:

$$\omega_{t+1} = \omega_t - l_r \nabla L(\omega_t) + \gamma(\omega_t - \omega_{t-1})$$

(9)
In the formula: $\gamma=0.9$ is the momentum; $\nabla L(wl)$ is the loss function to derive the parameter $wl$. This is the result we finally got.

3.2. Automatic generation algorithm model of network security performance based on genetic algorithm

First, input individual code $w$, chromosome gene $1z$, population size $N$, evolution algebra $G$, fitness calculation function $f(* )$, sample crossover probability $\rho_c$, gene crossover probability $\rho_e$, gene mutation probability $\rho$.

Finally, output the optimal safety configuration $c$;
1. Randomly generate $N$ binary numeric strings of length $w$ as the initial population $P$, and the number of values 1 in each numeric string is $Z*W$.
2. Generation=0
3. While (generation<=$G$)
4. Begin
5. Calculate the fitness $f(i)$ of each individual in the population $p$, and its probability of being selected:
   $$\rho(i) = \frac{f(i)}{\sum f(i)}$$
6. Perform the selected operation: select the individuals $s$ and $t$ of the two parents according to the probability
7. According to the above formula, calculate the fitness $f(I)$ of each individual, and select the individual $I$ with the largest fitness to calculate its corresponding safety configuration

3.3. Network security performance control system

In order to ensure the linear performance of the network security performance control system, calculate the error of its control system, the specific process is as follows:

$$L = \frac{0.4-\pi N^2 S_{e}}{L_{g}^{+} L_{c}/\mu} \times 10^{-8}$$

Parameter design of network security performance system:

$$\begin{aligned}
\{ I_{0} & = P_{0}/U_{0} \\
\{ P_{0} & = P_{\text{max}} \eta = U_{\text{max}} I_{\text{max}} \eta \}
\end{aligned}$$

The results of simulation and comparison experiments show that compared with the anti-jamming circuit of the existing network security system, the designed network security performance anti-jamming circuit greatly improves the anti-jamming performance, fully indicating that the designed network security performance has better anti-jamming performance.

3.4. Network security performance analysis algorithm BP neural network number determination

The BP algorithm is an unsupervised learning algorithm, if the actual output does not match the expected output, the output error is transmitted layer by layer from the hidden layer to the input layer in some form or form. other, and the error is assigned to each cell in each layer to get the error signal.Number of units. The network weight coefficient is adjusted by Backpropagation of the error to complete the network formation. The principle of BP algorithm is simple and practical and can solve many problems. Therefore, the BP model has become one of the important models of neural networks.

4. Evaluation results and research

4.1. Network security performance optimization system based on genetic algorithm and its performance analysis
As shown in Figure 1, when other parameters remain unchanged, changing the network security performance allows the flatness of the data to be adjusted for different environments. On the long wavelength, the coefficient dispersion D is more sensitive to the variation of the optimization width W and can effectively adjust the slope of the zero dispersion point and the dispersion curve. In the meantime, the security performance of the IT network can be effectively managed by changing the operating width of the CN. In the process of optimizing the network security performance, the height change of the average gbb715 can adjust the fluctuation of the whole curve flexibly, especially when the shift loss is large, the higher order loss coefficient will be reflected, so that the influence of the higher order loss rate on the mixing effect at qu other waves are negligible in the distribution of the super-flatness coefficient; on the other hand, due to the ultra-low and flat dispersion, the harmonic cavity has an evenly distributed resonance peak and is also connected to the waterfall. The new frequency component of the four-wave mixing is superimposed to produce a frequency comb with almost the same interval, which improves the effect of four-wave mixing, therefore, it is necessary to design a low-anomaly flat array optimization system with high-quality bending output.

4.2. Analysis of relevant parameters of the CN security performance optimization system

In the process of CN security performance optimization system analysis, it is necessary to set relevant parameters reasonably. According to the performance parameters proposed in related documents, the transmission rate of different network environments is set as follows. The arrival rate and data packet length of M2M traffic running through the backhaul network and the arrival rate of Poisson flow are shown in Table 1. By default, the number of direct traffic and competing traffic are equal, and the values of a = 2, B = 5, and t = 7s recommended by 3GPP TR 37.68 are used to analyze the parameters of the beta distribution.

| Analysis parameters | Accurate value |
|---------------------|---------------|
| R_u                 | 2Gbps~5Gbps   |
| \( \lambda_r \)    | 0.0263pkt/s   |
| \( \lambda_a \)    | 16pkt/s       |
| \( \tau \)         | 220Bytes      |
| a,b,T              | a=2, b=5, T=7s|
| \( \lambda \)      | 3.2Mbps       |

4.3. Analysis of the risk rating of data processed by the performance optimization system
Figure 2. Post-processing state diagram A of network security performance optimization based on genetic algorithm

Figure 3. Post-processing state diagram B of subsequent network security performance optimization based on genetic algorithm

The data shown in Figure 2 and Figure 3 are processed intelligently after optimizing the network security performance based on genetic algorithm, and artificial intelligence processing on it will lead to the possibility of data interruption. The consequences of this situation are more serious. On the other hand, in a large number of normal operation and abnormal operation, the manager is mainly concerned about the abnormal operation, and the rest of the normal operation is actually out of everyone's consideration. In supervised learning, this type of unlabeled samples that are not part of the predictions play a very important role. They are usually included in the data set for risk assessment, analysis and processing; and in semi-supervised learning, this type of sample describes the data distribution. Building a learning model is very useful, therefore, using design experience, this article performed supervised learning and semi-supervised learning on the same dataset with the same tagged part, using consistent scoring indices to assess model performance, and ultimately choose the best network security model. Based on a genetic algorithm. The state of performance optimization is predicted and analyzed.

5. Conclusion
Based on the above analysis, the conclusion can be drawn as follows: The configuration of related network security performance testing equipment is an important task of network security management. In order to avoid potential network security risks, it is also inevitable. Due to the automatic generation of network security devices based on genetic algorithms, it is difficult to reasonably match multiple security device configurations when CN security performance testing is expanded. It also exposed its flaws that are prone to configuration errors and policy conflicts. The design of a genetic algorithm-based network security performance optimization algorithm. This algorithm can infer the actual use of computers under different security configurations on the basis of collecting the same semantics and managing network multi-domain information in multiple different regions of the network. Authority, and automatically generate network security device configuration through genetic algorithm. Experimental results show that the genetic algorithm and its improved genetic algorithm can be combined with other intelligent algorithms, and can automatically generate a reasonable network security early warning system equipment configuration based on the use of current network...
security optimization methods, and greatly reduce the computer potential security risks of the network.

Acknowledgments
This work is funded by Jiangxi Provincial Department of Education, by the Science and Technology Project. (Project number: GJJ181480).

References
[1] Gong D W, Sun J, Miao Z. A Set-Based Genetic Algorithm for Interval Many-Objective Optimization Problems[J]. IEEE Transactions on Evolutionary Computation, 2018, 22(99):47-60.
[2] Ivan S, Veselý Vojtech. Robust output feedback controller design: genetic algorithm approach[J]. IMA Journal of Mathematical Control and Information(3):257-265.
[3] Doerr B, Doerr C. Optimal Static and Self-Adjusting Parameter Choices for the ( 1 + ( λ, λ ) ) Genetic Algorithm[J]. Algorithmica, 2018, 80(5):1658-1709.
[4] Mustafa A, Heppenstall A, Omrani H, et al. Modelling built-up expansion and densification with multinomial logistic regression, cellular automata and genetic algorithm[J]. Computers, Environment and Urban Systems, 2018, 67(jan.):147-156.
[5] Guan J, Wei Z, You I. GRBC-based Network Security Functions placement scheme in SDS for 5G security[J]. Journal of Network and Computer Applications, 2018, 114(JUL.):48-56.
[6] Han W, Tian Z, Huang Z, et al. System Architecture and Key Technologies of Network Security Situation Awareness System YHSAS[J]. Computers, Materials and Continua, 2019, 59(1):167-180.
[7] Meng L, Yin S, Zhao C, et al. An Improved Image Encryption Algorithm Based on Chaotic Mapping and Discrete Wavelet Transform Domain[J]. International Journal of Network Security, 2020, 22(1):155-160.
[8] Zhang G, Gao Y, Luo H, et al. Security Performance Analysis for Best Relay Selection in Energy-Harvesting Cooperative Communication Networks[J]. IEEE Access, 2020, 8:26-36.
[9] Shone N, Ngoc T N, Phai V D, et al. A Deep Learning Approach to Network Intrusion Detection[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1):41-50.
[10] Weizhi M. Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling[J]. Computer, 2018, 51(7):36-43.