Network Security Evaluation Based on Improved Genetic Algorithm and Weighted Error Backpropagation Algorithm

Jinlong Pang, Chongwei Liu*
School of Information Engineering, Heilongjiang Polytechnic, Heilongjiang, China

***Abstract*—As the speed advancement of network technology and the popularization of applications, network security problems are becoming more and more prominent, all kinds of network attacks and security threats are increasing, and the demand for network security evaluation is becoming more and more urgent. To address the issues of long time-consuming and low accuracy in the traditional network security evaluation model, the study proposes a network security evaluation model based on improved genetic algorithm and weighted error BP algorithm. The study first combines the weighted error BP algorithm with the improved genetic algorithm for data analysis and research, and then integrates the two to construct a network security evaluation model. The results show that in the detection of network security vulnerabilities, the evaluation model of the data processing vulnerability detection accuracy, risk detection rate of 93.28%, 91.88%, respectively. The function training error of the model is 8.93% respectively, while the decoding accuracy and stability are 90.43% and 92.07% respectively, which are better than the comparison method. This indicates that the method has high accuracy and robustness in network security evaluation, and can provide network administrators and users with a more scientific and reliable basis for decision-making.**

Keywords*—Genetic algorithm; return propagation algorithm; cybersecurity evaluation; weighting; network vulnerability

I. INTRODUCTION

Network security evaluation (NSE) is a critical means to guarantee network security, and its purpose is to do a comprehensive and objective evaluation of the security of the network system to provide network administrators and users with a scientific basis for decision-making. Traditional NSE methods are mainly based on expert experience, vulnerability scanning and other technologies, but these methods often have problems such as low evaluation accuracy and poor adaptability [1-2]. Therefore, NSE methods based on data and algorithms have attracted much attention from researchers. Genetic Algorithm (GA) is a kind of search and optimization algorithm with evolutionary ideas, which has global search capability and self-adaptability. The traditional GA has some problems in NSE. To improve the effectiveness of GA in NSE, it is necessary to improve the performance and convergence speed of the algorithm by introducing new optimization strategies and operators [3-4]. Weighted Error Back Propagation (BP) algorithm is a commonly used neural network training algorithm, which is able to adjust the weights and thresholds of the network by back-propagating the errors between the inputs and outputs of the network, so as to raise the performance of the network. In NSE, the weighted error BP algorithm can be applied to the training and optimization process of the evaluation model to raise the accuracy and reliability of NSE [5-6]. The study firstly combines the BP algorithm with the improved GA for the analysis and research of data, and then constructs an NSE model with GA_BP. The study expects that the NSE model constructed using the GA_BP algorithm can overcome the limitations of traditional methods and raise the accuracy and reliability of evaluation.

Section I is the introduction. Section II introduces the current status of research related work to NSE and deep learning in NSE; Section III uses the weighted BP algorithm and the improved GA to process the data and constructs an NSE model; Section IV uses simulation experiments to verify the effectiveness of the NSE model constructed by the study; discussion and conclusion is given in Section V and Section VI respectively..

The main contributions of the research can be divided into two points. First, the method constructed in the experiment improves the genetic algorithm and enhances its global search capability and local search accuracy to adapt to the complexity of weight allocation in network security evaluation. Second, the weighted error back propagation algorithm is improved to adapt to the characteristics of the network security evaluation model and improve training efficiency and accuracy. At the same time, a weighting mechanism is introduced to enable the model to pay more attention to important evaluation indicators during the training process, thereby improving the model's predictive ability.

II. RELATED WORK

With the quick advancement of Internet technology, network security problems are becoming more and more prominent, and the demand for NSE is becoming more and more urgent. Traditional NSE methods often have problems such as low evaluation accuracy and poor adaptability, which are hard to satisfy the demands of practical applications. Therefore, the study of new NSE methods has become one of the current hot issues in the field of network security, and many experts and scholars have conducted in-depth research. Chen J and Miao have proposed an NES system with rough sets to solve the problems of poor system stability and long response time in the traditional network information system. The study first extracted the relevant evaluation indexes using network topology, then processed the indexes using gray comprehensive evaluation, and

finally simplified the evaluation model by applying rough set. The findings denoted that the model is able to improve the system stability to more than 80% and the response time is less than 1.32ms [7]. Salitin et al. To provide a reliable solution for analyzing the customer's behavior, they proposed an evaluation criterion based on a quantitative method. The study obtained relevant data from cybersecurity practitioners and then used validation factors to analyze the results and construct a reliable measurement model. The outcomes indicated that the standard can not only improve the reliability of the assessment, but also provide corresponding solution strategies [8]. Zhang et al. proposed an information security assessment method based on fuzzy neural network to improve the security capability of network information platform. The study utilizes the weight calculation method and the minimal neural network pruning algorithm to process the data on the basis of the comprehensive analysis of security events, and then utilizes the fuzzy neural network to control the information so as to complete the adaptive training. The results show that the evaluation method can significantly improve the ability of information encryption and transmission [9]. Zhao and Rao raised a network security situational awareness model based on the D-S theory to promote the ability of network security situational awareness. The study first preprocesses the warning information using clustering methods, and then establishes data fusion rules using D-S evidence theory to provide detection accuracy. The outcomes indicated that the model is able to accurately assess the provided cybersecurity situation [10].

Zhao, to enhance the role of BP neural network in campus network information security, a complete analysis model of BPNN network based on weight improvement is proposed. The study first uses particle swarm algorithm to process the information, then uses BPNN to analyze the data, and finally combines the two for constructing the analysis model. The outcomes denoted that the accuracy of the improved BPNN analysis model for data analysis can reach 92.57%, which can significantly improve the campus network security [11]. He and Yang proposed a concern dual feedback model to effectively predict the level of network security posture. The study first established a security posture indicator system, then processed the information using the reverse feedback model, and finally constructed a model for the prediction of posture. The findings denoted that the prediction accuracy of the model is increased to 96.97%, which verifies that the model has high prediction reliability [12]. Xing et al. proposed a vector machine model based on simulated annealing algorithm to raise the prediction ability of network security posture development trend. The study first reconstructed the sample data of cyber security state, then processed it using simulated annealing algorithm, and finally optimized the relevant vectors using vector machine. The outcomes indicated that the model can significantly raise the accuracy of prediction [13].

In summary, it can be seen that currently, network security evaluation is a key link in ensuring network security, and its research importance is increasingly prominent. In recent years, various network security evaluation methods based on machine learning, especially genetic algorithms and error back propagation algorithms, have been widely used in network security evaluation. Although various theoretical research contents are very rich, network security involves many aspects such as computers, physics, and communications. The existing security evaluation methods still have problems such as poor operability, small scope of application, and interference from human factors. To this end, by analyzing the ideas of GA algorithm and BP algorithm, the research conducted a deeper design and analysis of the coding method and fitness function in the BP network architecture, and obtained an improved genetic algorithm and weighted error back propagation algorithm. The network security evaluation model is expected to eliminate the interference caused by human factors and quickly obtain correct network security evaluation results.

III. Construction of Network Security Evaluation Model Fusing GA and BP Algorithm

NSE is a key link in ensuring network security, and its core objective is to provide a comprehensive and objective assessment of the security of the network system. Such evaluation not only helps to identify potential security risks, but also provides network administrators and users with a scientific and reliable basis for decision-making. To accomplish this task more accurately, the study is based on improving and combining the GA with the BP algorithm. And the combination of these two algorithms will provide strong support for constructing an efficient and accurate NSE model.

A. Research on Network Security Evaluation Data Analysis by BP Algorithm Combined with Improved GA

The BP algorithm is capable of problem learning and systematic problem solving through the implicit units in the multilayer network results. In NSE, the BP algorithm will first take the relevant data involving network security as input through forward propagation, and effectively analyze and calculate the actual value output value. Then in the use of the reverse process for the case of not getting the expected value, if not getting the expected value, the BP algorithm will carry out layer by layer recursion, so as to calculate the error between the output value and the actual value. Finally, the weighting weights are adjusted according to this error value to ensure that the desired output value is obtained, and the network security is effectively evaluated according to the output value [14-15]. Fig. 1 is the schematic diagram of the neural network model of the BP algorithm.

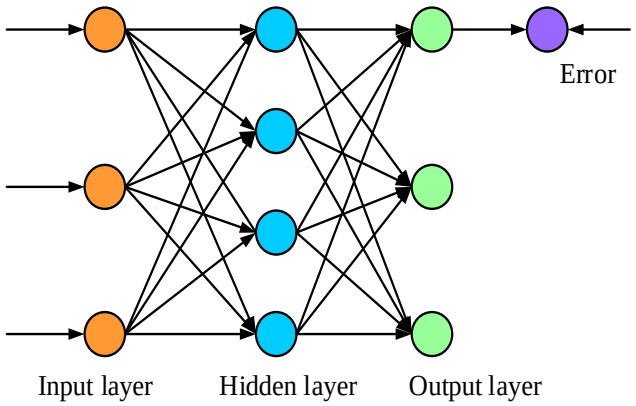


Fig. 1. Schematic diagram of neural network model for BP algorithm.

Combined with Fig. 1, we can find that the BP algorithm contains implicit layers, which can back-propagate the input network information, by activating the activation function on different levels to enhance the ability of information transmission. The BP of the BP algorithm can reduce the loss of the signal in the process of transmission through the modification of neuron weights in each layer, so as to enhance the success rate of signal transmission. The study in order to simplify the whole process of weighting processing, assuming that there are a total of n nodes and L layers of the network in the neural network of the BP algorithm, at this time, the Eq. (1) can be applied to calculate the value of the node input of a unit in a certain layer.

$$net_{ij}^{l} = \sum_{j} w_{ij}^{l} f(o_{jk}^{l-1}) \tag{1}$$

In Eq. (1), w_{ij}^{l} denotes the weights from the i neuron to the j neuron in the l layer of the network; k denotes the input corresponding sample; and o_{jk}^{l-1} denotes the node output value of the j neuron corresponding to the $l-1$ layer of the network. The error function at this point can be expressed by Eq. (2).

$$E_k = \frac{1}{2}\sum_{l}(y_{lk} - \bar{y}_{lk})^2 \tag{2}$$

In Eq. (2), y_{lk} denotes the predicted output of neuron j; $\bar{y}_{lk}$ denotes the actual output of neuron j. After obtaining the error function, the total error in the process of NSE can be calculated, as shown in Eq. (3).

$$E = \frac{1}{2N}\sum_{k=1}^{N} E_k \tag{3}$$

In Eq. (3), N denotes the given sample. The weighting operation can realize the combination of the existing weights with the BP algorithm. When the error reaches the range set by the control coefficient, according to the specific value of the error, the corresponding set the weight value between the hidden layer and the output layer, so that the output value can meet the requirements. In this process, if the corresponding node is the output unit, the neuron node output is equal to the actual output value. If the corresponding node is not the output unit, the output of the corresponding node corresponds to the actual output value of the next neuron. This indicates that for weighted BP in BP networks, the weight coefficients need to be determined first, and then the error values are evaluated, and if the error values do not meet the accuracy demands, the coefficients need to be adjusted to meet the accuracy demands. The requirement of accuracy can be expressed by Eq. (4).

$$E = \frac{1}{2N}\sum_{k=1}^{N} E_k < \varepsilon \tag{4}$$

In Eq. (4), ε denotes the accuracy value. At this point the weight correction for BP can be expressed in Eq. (5).

$$w_{ij} = \mu \frac{\partial E}{\partial w_{ij}} \tag{5}$$

In Eq. (5), μ denotes the correction coefficient; ∂E denotes the total error value after updating; ∂w_{ij} denotes the weight value after updating. The inverse operation of the weights can improve the accuracy of the output value of the BP algorithm network and make it meet the set requirements. However, through a large number of studies, it is found that the BP algorithm converges according to the direction of the error gradient decline, and there are certain global and local minima in its error decline gradient. This leads to the situation of local optimization when performing network security assessment, and at the same time, the BP algorithm also has the situation of slower convergence speed, which also leads to excessive time consumption when performing network security assessment. Therefore, the study to address these issues, the improved GA is used for the improvement of the BP algorithm. The improved GA is obtained by improving the network degree correlation in the GA. The algorithm is able to manipulate data based on probabilistic optimization of cybersecurity assessment objects without the need to derive the function [16-17]. This makes it possible to search for cybersecurity assessment without the need to determine the optimization rules, but to automatically adjust the search direction to find its required object data. The flowchart of the improved GA for optimization is denoted in Fig. 2.

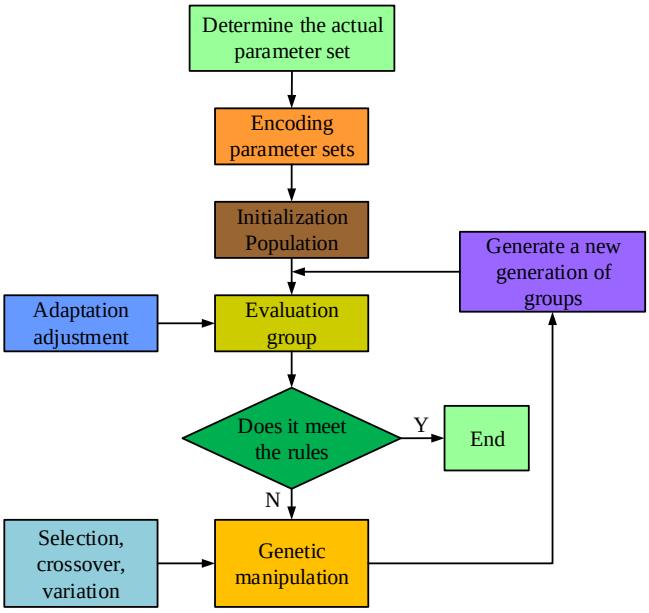


Fig. 2. Optimization flowchart for improving GA.

The study, in improving the GA, found that the gradient correlation coefficients of the neural network are also required to be calculated if reliable combinations are to be obtained. The correlation coefficient at this point can be calculated using Eq. (6).

$$r=\frac{M^{-1}\sum_i G_i H_i-\left[M^{-1}\sum_i \frac{1}{2}(G_i+H_i)\right]^2}{M^{-1}\sum_i \frac{1}{2}(G_i^2+H_i^2)-\left[M^{-1}\sum_i \frac{1}{2}(G_i+H_i)\right]^2} \quad (6)$$

In Eq. (6), M denotes the total amount of edges in the network; G_i and H_i denote the vertex degree value on the i edge in the connected network. If the value range of the calculation result r is [-1,], the positive correlation is when r is greater than 0, and the negative correlation is when it is smaller than 0. Comprehensive analysis of the above research, the combination of the improved GA and the weighted BP algorithm for the processing of network security data can avoid the emergence of local optimum in the process of data optimization, and significantly raise the convergence speed of the algorithm. Thus, the accuracy of data processing can be improved, and the optimal solution required by the load can be found. As shown in Fig. 3, the flow chart of network security data processing after the combination of the improved GA and the weighted BP algorithm is shown.

B. *Network Security Evaluation Model Construction Based on GA_BP*

Through the processing of network security data by the improved GA combined with the weighted BP algorithm, it is found that the NSE is the assessment of network risk. This requires analyzing the vulnerabilities and risks in the network system, evaluating and predicting them, and formulating corresponding security measures and strategies based on the results of the evaluation [18]. Based on this, the study constructs an NSE model using the combined algorithm based on the improved GA combined with the weighted BP algorithm for network security data processing. After obtaining the output data of NSE, the GA_BP algorithm is utilized to construct the evaluation model. In the process of constructing the model, the GA will correspond to the connection weights and the network structure in the neural network, so that it can overcome the problems in the BP algorithm and significantly improve the data generalization ability [19-20]. The study takes the data vulnerabilities and risks in network security as inputs to the model, and utilizes the global search capability of the GA to search for the data vulnerabilities that exist. After completing the search, the data nodes in the implicit layer are optimized so that they can match the nodes in the input and output layers. Thus, the accuracy and reliability of the NSE model are improved. Through the above processing, the model obtained at this time can deal with the nonlinear problems in NSE, and this process can be expressed as Eq. (7) with mathematical thinking.

$$\min E(w,v,\theta,r)=\frac{1}{2}\sum_{k=1}^{N_1}\sum_{t=1}^{n}\left[y_k(t)-\hat{y}_k(t)\right]^2$$

In Eq. (7), $y_k(t)$ means the network output value at the time of k; $\hat{y}_k(t)$ means the real network output value corresponding to the time of k. Through the model's treatment of nonlinear problems in NSE, the error in the evaluation process can be determined more accurately. Through the accurate calculation of the error, the application of the model to the actual evaluation can be improved. After completing the processing of the nonlinear problem, to promote the effectiveness of network security vulnerability detection, the improved GA will take the maximum value of the objective function as its corresponding fitness function, which can be expressed by Eq. (8).

Network security vulnerability detection, the improved GA will take the maximum value of the objective function as its corresponding fitness function, which can be expressed by Eq. (8).

$$F(w,v,\theta,r)=\sqrt{\sum_{k=1}^{N_1}\sum_{t=1}^{n}\left[y_k(t)-\hat{y}_k(t)\right]^2}$$

After solving the fitness function, it is necessary to spatially decode the cybersecurity vulnerabilities. Decoding spatial coding consists of two parts: the control code and the weight coefficient code. The control code indicates the connectivity between nodes and consists of a string of 0 and 1, where 0 means no connection and 1 means connected. The length of the control code is determined according to the number of input nodes. The weight coefficient code is used to control the weight of the connection. The codes are connected sequentially to form long strings, and each string corresponds to a set of connection weights and structures. Taking three input nodes as an example, there are up to six hidden layer nodes. In Fig. 4, the fitness function decodes the linear difference special case analysis graph.

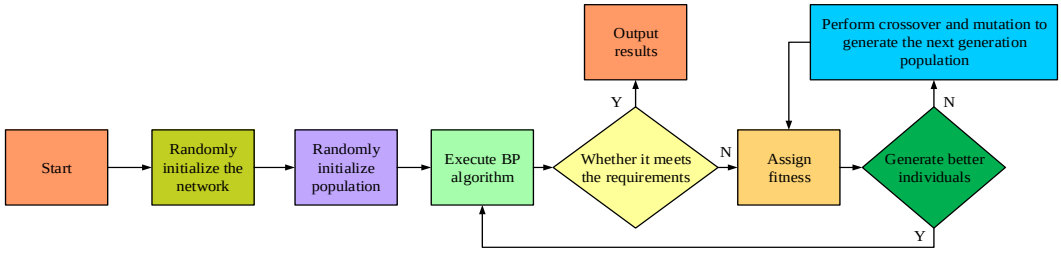


Fig. 3. Network security data processing flowchart after combining improved GA and weighted BP algorithm.

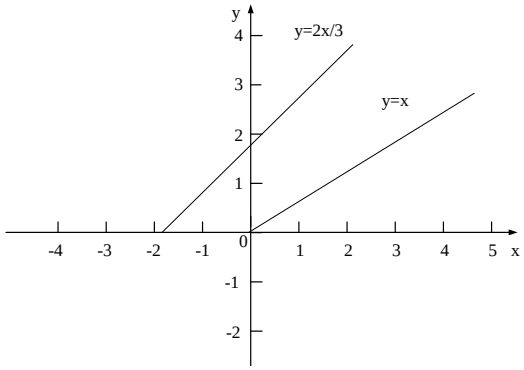


Fig. 4. Special case analysis of decoding linear differences using fitness function.

The decoding of network security vulnerabilities reveals that the number of nodes also needs to be effectively encoded in the decoding process using arithmetic crossover. The study assumes that two vulnerability individuals are encoded and the new individual after processing using arithmetic crossover can be represented by Eq. (9).

$$\begin{cases} X_1' = aX_2 + (1-a)X_1 \\ X_2' = aX_1 + (1-a)X_2 \end{cases} \tag{9}$$

In Eq. (9), a denotes the constant coefficients; X_1, X_2 denote the old individuals before decoding the crossover. After completing the decoding of the crossover, the study utilizes Gaussian approximate mutation to enhance the local search capability in the network security region. Gaussian approximate variation is the use of variation operation to find the abnormal data in the vulnerability, and then more data distribution to find the normal distribution of its variance, so as to complete the vulnerability search, and the relevant data for the evaluation process of network security. At this time the variation can be expressed by Eq. (10).

$$y = \lambda x + (1-\lambda)\beta \tag{10}$$

In Eq. (10), x denotes the characteristics of vulnerability individuals before mutation; λ and β denote the constant coefficients. Combining the above process of model construction, the flow of the study of NSE model using improved GA combined with weighted BP is shown in Fig. 5.

As can be seen in Fig. 5, the method constructed in the experiment first uses a neural network to estimate the preliminary solution space, then determines the encoding and decoding methods of the solution space individuals, and randomly generates a new generation of initial population. Then 5 to 8 repeated crossovers and mutations begin. Every time an individual in the group mutates, the group will evolve in this generation and continue to evolve until the Kth generation. The individual with the highest fitness in the Kth generation is decoded to obtain the connection weight and number of hidden nodes of the corresponding network. Here, the sample is input to test the generalization ability of the model. Here we cannot simply think that the individual with the highest fitness in the kth generation is the global optimal solution of the network. If the obtained k-th generation is smaller than the group value that continues to K generations, then the algorithm will decode all individuals in the last generation group; then substitute it into training sample 2, solve for the satisfied network weight coefficient and network structure, and Output the network weight coefficients and networks that meet the conditions, and finally output detection samples to test the generalization ability of the network. If the obtained k-th generation is greater than or equal to the population value that continues to the K generation, selection, crossover, and mutation will be continued to generate a new generation of population, and this operation will be repeated until the optimal solution is obtained.

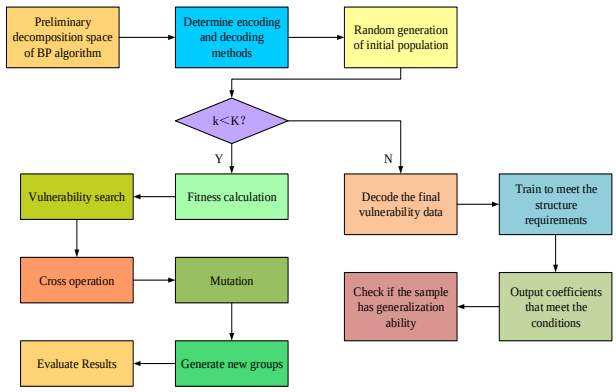


Fig. 5. The flowchart of improving the network security evaluation model based on GA combined with weighted BP.

IV. Performance Analysis of Network Security Evaluation Model Based on GA_BP Algorithm

To validate the performance of the NSE model based on GA_BP algorithm in the study. The study uses Linear Discriminant Analysis (LDA) and Logistic Regression Model (LRM) as a comparison method with the evaluation model constructed by GA_BP algorithm.

A. Comparison of Detection Results of Network Training Errors with Different Numbers of Nodes

To effectively analyze the evaluation model, the study selects accuracy, risk detection, training error, network stability, evaluation fitness and time-consuming as performance evaluation indicators; and continuously solves the performance of the algorithm through repeated experiments. Compare the model constructed in the experiment with the LDA and LRM methods, and comprehensively consider multiple indicators to comprehensively evaluate the model performance. Research and conduct experiments in Matlab language. Set the number of network nodes to 8 nodes, the weight value to 0.2, the learning accuracy to 0.001, and the number of training times to 1000. The parameters of the experimental simulation environment are as follows: the processor is Intel Core i7-9700K; the memory is 32GB RAM; the storage hard disk is a high-speed solid state drive (SSD) 512GB; the operating system is Windows 10; the programming language is Python 3.8; the database is MySQL; simulation software for MATLAB R2020a; Fast Ethernet or Wi-Fi 6, ensuring stability and speed of data transmission. The public KDD99 intrusion detection data set was selected as the

task data set. This data set is nine weeks of network connection data collected from a simulated US Air Force LAN, and is divided into labeled training data and unlabeled test data. The training data set contains 1 normal identification type normal and 22 training attack types. In addition, 14 types of attacks only appear in the test data set. Use research methods to examine and detect the network adapted to this data set. The training error of the network with different number of nodes in GA_BP algorithm is denoted in Fig. 6.

As analyzed in Fig. 6, the error rate of network training decreases with the increase in the amount of nodes. The training error when the amount of nodes is 2, 4, 6, 8 and 10 is 53.18%, 42.02%, 22.38%, 18.21%, 10.27% and 7.93%, respectively. In which the training error of the whole network is significantly reduced when the amount of nodes is 6. This denoted that the learning ability of the prediction model is increasing with the increase of the number of nodes, and the understanding ability is also improved. When the amount of nodes is between 6-10, the training error of the network does not change significantly. This indicates that in the GA_BP algorithm, it is not that the more nodes the better the training effect of the network is, and even the situation of over-matching of the network occurs, which leads to a decrease in the accuracy of the training efficiency of the network.

B. Comparative Results of Network Security Vulnerability and Risk Detection using Three Methods

To verify the detection ability of GA_BP prediction model in network security vulnerabilities, the study uses LDA and LRM as comparison methods with GA_BP. The outcomes of the comparison of the three methods for network security vulnerability and risk detection are shown in Fig. 7.

From Fig. 7(a), GA_BP has the highest accuracy rate of 93.28% in the detection of network security vulnerabilities. And the accuracy rate of LRM and LDA is obviously lower, in which the accuracy rate of LRM and LDA in detecting cybersecurity vulnerabilities is 89.01% and 86.58%, respectively. From Fig. 7(b), in the detection of cybersecurity risk, the accuracy rate of GA_BP is also the highest, followed by LRM and LDA. The risk detection accuracy rates of the three methods are 91.88%, 88.63% and 85.06%, respectively. This indicates that the GA_BP algorithm used by the study to construct the NSE model has good robustness and adaptability.

C. Comparison of Function Training Errors and Decoding Results of the Three Methods

To verify the training error of the function in the GA_BP algorithm, the study compares the three methods using the labeled objective function as a standard. The results of the comparison of the function training error of the three methods are shown in Fig. 8.

In Fig. 8, the training error of the standard objective function is only 2.08%, while the training errors of the functions of GA_BP, LRM and LDA are 8.93%, 18.66% and 21.75%, respectively. Among the three methods, the smallest difference in training error from the standard objective function is the GA_BP algorithm, with a difference of 6.85% between the two. While the training error difference between LRM and LDA and the standard objective function is 16.58% and 19.67% respectively. The comparison illustrates that the GA_BP algorithm, which is used to construct the evaluation model for the study, is also highly reliable in function training. In order to further verify the performance of the GA_BP algorithm in the evaluation model, the study takes the accuracy and reliability of the decoding of the NSE data as an indicator for performance verification. The comparison outcomes of the accuracy and stability of the three methods in the decoding process are shown in Fig. 9.

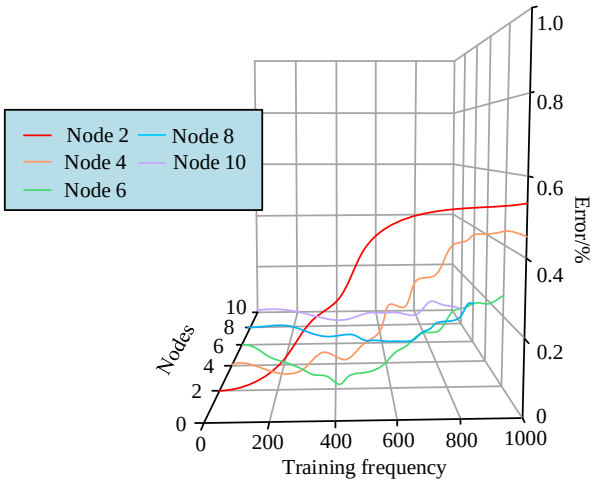
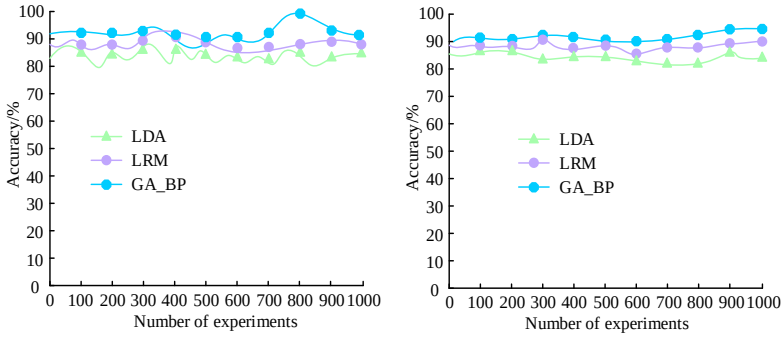


Fig. 6. The network training error of different node numbers in GA_BP algorithm.



(a) Three methods for detecting vulnerabilities in network security

(b) Three Methods for Risk Detection Results in Network Security

Fig. 7. Comparison results of three methods for detecting network security vulnerabilities and risks.

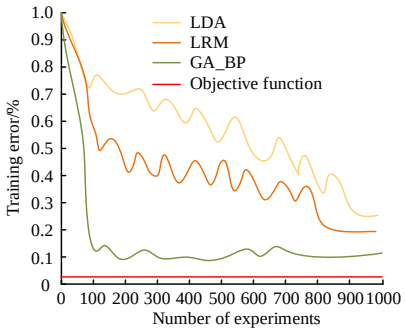
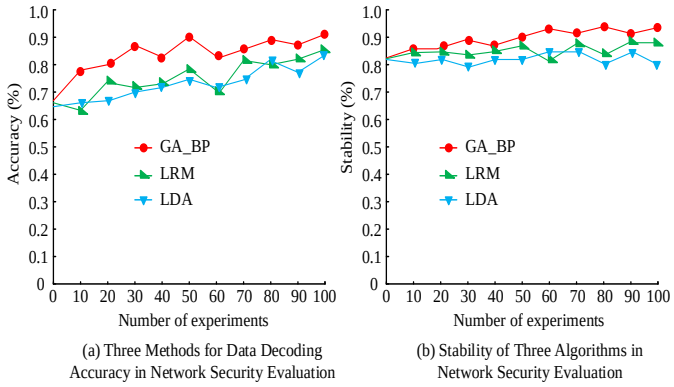


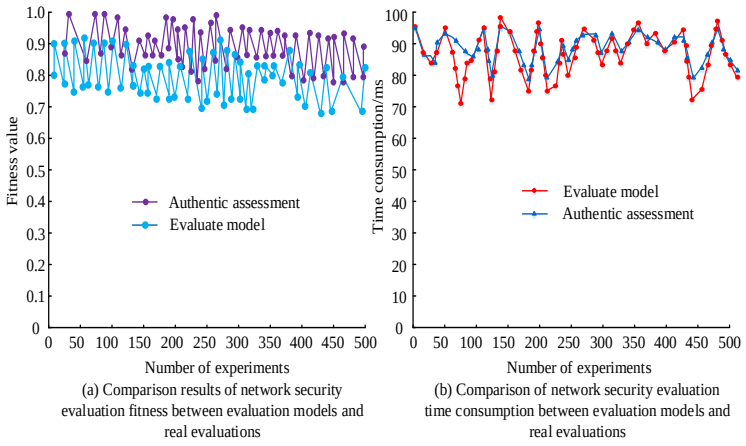
Fig. 8. Comparison of function training errors among three methods.



(a) Three Methods for Data Decoding Accuracy in Network Security Evaluation

(b) Stability of Three Algorithms in Network Security Evaluation

Fig. 9. Comparison of accuracy and stability of three methods in the decoding process.



(a) Comparison results of network security evaluation fitness between evaluation models and real evaluations

(b) Comparison of network security evaluation time consumption between evaluation models and real evaluations

Fig. 10. Comparison of fitness and time consumption between network security evaluation models and real evaluations.

As can be seen in Fig. 9(a), the decoding ability of all three methods for network security data also shows an increasing trend as the amount of experiments increases. The highest decoding accuracy is achieved by GA_BP algorithm, followed by LRM and LDA with 90.43%, 86.25% and 82.31% respectively. From Fig. 9(b), in the stability comparison of cybersecurity evaluation, the stability of GA_BP is 92.07%, and the stability of LRM and LDA is 85.03% and 83.99%, respectively. This denotes that both the reliability and accuracy of the NSE, the evaluation model constructed by the study is better than the more commonly used assessment methods, reflecting the good performance of the evaluation model.

D. Comparison Results of Network Security Evaluation Fitness and Time Consumption

To verify the specific application performance of the NSE model, the study utilizes simulation experiments for corresponding performance testing and analysis. To verify its performance in the process of NSE, the study uses the evaluation adaptability and time-consuming as indicators for the performance test of the NSE model. As shown in Fig. 10, the results of the comparison of the evaluation model and the real evaluation of the NSE adaptability and time-consuming are shown.

In Fig. 10(a), in the comparison of the adaptability of NSE, the average value of the adaptability of the evaluation model is 0.86, and the average value of the adaptability of the real

evaluation is 0.91, with a difference of 0.05. In Fig. 10(b), in the comparison of the time-consumption of the NSE, the difference in the time-consumption of the two evaluations is not large. The average time consumed in the real evaluation is 85.3 ms, and the average time consumed in the evaluation model is 92.5 ms, with a difference of 7.2 ms. It can be found that the gap between the NSE model constructed by the study and the real evaluation is not large, which can also reflect that the NSE model constructed by the study has a strong adaptability.

E. Comparison of Evaluation of Network Security Confidentiality Situation and Comprehensive Situation

To verify the effect of the NSE model, the research evaluates the confidentiality posture and comprehensive posture in network security, and takes them as evaluation indexes for the analysis of the performance of the evaluation model. In Fig. 11, the evaluation comparison results of confidentiality posture and integrated posture in network security are shown.

From Fig. 11(a), in the comparison of network security confidentiality posture, the real posture value of network security confidentiality is 15.6, the posture value of evaluation model is 14.8, and the posture value of traditional evaluation method is 12.3. From Fig. 11(b), in the comparison of comprehensive posture value of network security, the real value of comprehensive posture is 19.1, the comprehensive posture value of evaluation model is 18.6, and the comprehensive posture value of traditional The comparison of posture values reveals that evaluating the network security confidentiality posture and comprehensive posture is crucial for organizations to safeguard network and information security, which can help organizations identify threats and vulnerabilities, conduct risk assessment and decision support, improve security protection capabilities, and also monitor and warn to respond to cybersecurity events in a timely manner. To further prove the effect of the NSE model, the study chooses the number of nodes as 8 and evaluates the detection samples. The detection outcomes are denoted in Table I.

As can be seen from Table I, in the six experiments on the nodes, the relative error is the maximum of 2.57 and the minimum of 1.33. The evaluation value is the maximum of 9.01 and the minimum of 8.69. This indicates that the NSE model constructed by the study meets the desired output results and can be used for the comprehensive evaluation of the network security with a high accuracy.

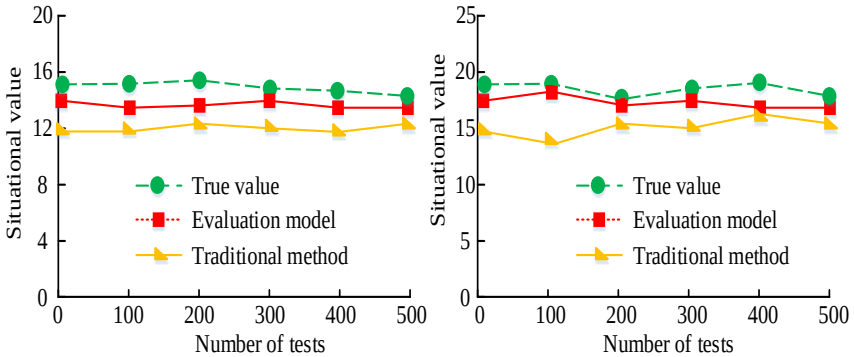


Fig. 11. Comparison of evaluation results between network security confidentiality situation and comprehensive situation.

TABLE I. NETWORK SECURITY EVALUATION SAMPLE DETECTION RESULTS

Node number	Evaluate expected output	Evaluate actual output	Relative error	Corresponding evaluation value	Output level
1	0.896	0.901	2.13	9.01	A
2	0.834	0.859	2.57	8.72	B
3	0.883	0.896	1.96	8.69	B
4	0.879	0.897	1.87	8.77	B
5	0.892	0.902	1.33	8.82	B
6	0.871	0.891	2.56	8.76	B

V. DISCUSSION

The improved GA and BP have significant application potential in the field of network security evaluation. By optimizing the selection, crossover and mutation operations of GA, the solution space can be explored more effectively and a better network security evaluation model can be found. At the same time, the introduction of BP enables the model to more accurately assess network security risks, especially when dealing with imbalanced data sets. I believe that these improvements not only improve the performance of the model, but also provide new perspectives and solutions in the field of network security. Although the constructed method was successful in specific cybersecurity evaluation tasks, I also realize that the current model may require further adjustments and optimizations when facing more complex cybersecurity environments. For example, when processing large-scale data sets, the algorithm's computational efficiency and convergence

speed may be affected. In addition, dynamic changes in the network security environment require models to quickly adapt to new threats and attack patterns. In order to generalize to more complex situations, the algorithm can be optimized and improved from several aspects. For example, further improve GA and BP to improve their efficiency and accuracy on large-scale data sets; consider combining the current model with other machine learning or deep learning models to improve adaptability to complex cybersecurity scenarios. In addition, the online learning and real-time update modes of the model can also be explored to cope with the rapid changes in the network security environment.

VI. Conclusion

Aiming at the problems of high error rate and time-consuming of the traditional NSE model, the study is based on the improvement of GA method and BP algorithm, and the GA_BP algorithm is used to construct the NSE model. The findings denote that the average value of the adaptability of the evaluation model in the process of NSE is 0.86, while the average value of the adaptability of the real evaluation is 0.91, with a difference of 0.05. Meanwhile, the average value of the time-consuming of the evaluation model is 92.5ms, with a difference of 7.2ms compared with the real value, and in the process of the NSE, the posture value and the integrated posture value of the evaluation model are 14.8 and 18.6, respectively. In summary, the study of NSE method based on improved genetic algorithm with weighted error BP algorithm has significant effect in improving network security. The research can provide a new idea and method for NSE, which has important theoretical and practical value for improving network security. Although the research has achieved good results, there are still some shortcomings. As the network environment becomes increasingly complex, it is difficult for a single data source or algorithm to fully capture the diversity of network security threats. Therefore, it is particularly important to develop assessment models that can integrate multiple data sources and threat types. In addition, since artificial neural networks require a large number of learning samples to train the network, calculating the network security performance-price ratio also requires evaluation data of typical networks. However, the current comprehensive evaluation work has just begun. There is still a lack of data in this area. Therefore, in future work, attention should be paid to collecting security evaluation data of various networks to improve the evaluation models and methods.

References

[1] Z. Bo, and W. Tao, "Cyberspace Security Evaluation Technology on the Condition of Attack and Defense Confrontation," Communications, Signal Processing, and Systems: Proceedings of the 2018 CSPS Volume III: Systems 7th. Springer Singapore, vol. 17, no. 6, pp. 983-989, 2020.

[2] M. Gheisari, H. Hamidpour, Y. Liu, P. Saedi, A. Raza, A. Jalili, H. Rokhsati, and R. Amin, "Data Mining Techniques for Web Mining: A Survey," Artif. Intell. Appl, vol. 1, no. 1, pp. 3-10, 2023.

[3] G. Zhao, P. Zou, and W. Han, "Network Security Incidents Frequency Prediction Based on Improved Genetic Algorithm and LSSVM," China Commun, 2010, vol. 7, no. 4, pp. 126-131, 2010.

[4] S. S. Alshamrani, and A. F. Basha, "IoT data security with DNA-genetic algorithm using blockchain technology," Int. J. Comput. Appl. T， vol. 65, no. 2, pp. 150-159, 2021.

[5] B. Chen, H. Chen, and M. Li, "Feature selection based on BP neural network and adaptive particle swarm algorithm," Mob. Inf. Syst, vol. 21, no. 3, pp. 1-11, 2021.

[6] N. Leema, K. H. Nehemiah, E. C. VR, and A. Kannan, "Evaluation of parameter settings for training neural networks using backpropagation algorithms: a study with clinical datasets," Int. J. Oper. Res. Inf. Syst, vol. 11, no. 4, pp. 62-85, 2020.

[7] J. Chen, and Y. Miao, "Research on security evaluation system of network information system based on rough set theory," Int. J. Internet Proto, vol. 14, no. 3, pp. 155-161, 2021.

[8] M. A. Salitin, and A. H. Zolait, "Evaluation criterion for network security solutions based on behaviour analytics," Int. J. Syst. Control Commun, vol. 14, no. 2, pp. 132-147, 2023.

[9] Y. Zhang, and Z. Rao, "Research on Information Security Evaluation Based on Artificial Neural Network," 2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). IEEE, vol. 10, no. 5, pp. 424-428, 2020.

[10] Z. Zhao, Y. Peng, J. Huang, T. Zhou, and H. Wang, "An evaluation method of network security situation using data fusion theory," Int. J. Performability Eng, vol. 16, no. 7, pp. 1046-1057, 2020.

[11] X. Zhao, "Security analysis of information in campus network based on improved back-propagation neural network," Telecommun. Radio Eng, vol. 80, no. 2, pp. 35-46, 2021.

[12] J. He, and J. Yang, "Network security situational level prediction based on a double-feedback Elman model," Informatica, vol. 46, no. 1, pp. 87-93, 2022.

[13] J. Xing, and Z. Zhang, "Prediction model of network security situation based on genetic algorithm and support vector machine," J. Inte. Fuzzy Syst, no. 3, pp. 1-9, 2021.

[14] H. Wang, D. Zhao, and X. Li, "Research on network security situation assessment and forecasting technology," J. Web Eng, vol. 19, no. 7–8, pp. 1239-1266, 2020.

[15] R. X. Liu, "A computer network intrusion detection technology based on improved neural network algorithm," Telecommun. Radio Eng, vol. 79, no. 7, pp.593-601, 2020.

[16] D. W. Kim, M. S. Kim, J. Lee, and P. G. Park, "Adaptive learning-rate backpropagation neural network algorithm based on the minimization of mean-square deviation for impulsive noises," IEEE Access, vol. 8, no. 6, pp. 98018-98026, 2020.

[17] B. Raharjo, N. Farida, P. Subekti, R. H. S. Siburian, and R. Rahim, "Optimization forecasting using back-propagation algorithm," J. Appl. Eng. Sci, vol. 19, no. 4, pp. 1083-1089, 2021.

[18] T. Yerriswamy, and G. Murtugudde, "An efficient algorithm for anomaly intrusion detection in a network," Glob. Trans. Proceedings, vol. 2, no. 2, pp. 255-260, 2021.

[19] A. Biradar, "A secure GA approach in mesh based multicast network," Glob. Trans. Proceedings, vol. 2, no. 1, pp. 117-122, 2021.

[20] H. Suhaimi, S. I. Suliman, I. Musirin, A. Harun, and S. Shahbudin, "Network intrusion detection system using immune-genetic algorithm (IGA)," Indonesian J. Electr. Eng. Comput. Sci, vol. 17, no. 2, pp. 1060-1065, 2019.