Application of Genetic Algorithm-Grey Wolf Optimization-Support Vector Machine Algorithm in Network Security Services Assessment and Prediction

Guoying Han, Bin Zhou* and Yazi Zhang

College of Network and Communication, Hebei University of Engineering Science, Shijiazhuang, 050091, China
E-mail: 15630175085@163.com
**Corresponding Author*

Received 21 February 2024; Accepted 11 May 2024

Abstract

The continuous development of information technology has also promoted the progress of the Internet. More people are joining the Internet. The amount of data stored in the network is also increasing, including some important information, which leads to criminals launching attacks on network security. In order to solve the large error in network security situation assessment and poor progress in network security prediction, the study uses spectrum clustering analysis to evaluate the network security situation. Then genetic algorithm, grey wolf optimization algorithm and support vector machine fusion algorithm are used to predict the Network Security Service (NSS). The genetic algorithm is used to optimize the global search ability of the gray wolf optimization algorithm and the parameters of the support vector machine are optimized to evaluate and predict the NSS. The results showed that the maximum error of the proposed model was 0.4112, and the maximum error was 0.5896. The absolute percentage error of this algorithm was 0.0270, while the

Journal of Cyber Security and Mobility, Vol. 13_5, 941–962.
doi: 10.13052/jcsm2245-1439.1356

other algorithms were 0.0745 and 0.0952, respectively. The proposed model has lower errors and time consumption in training and simulation testing compared with other current methods. The network situation assessment and prediction method proposed in the study can effectively improve network security services, ensure the personal information security, and enhance the security of the Internet.

Keywords: Spectral cluster analysis, cyber security posture, GA, GWO, SVM.

1 Introduction

In today's digital age, cyber security has become a global focus. As the dependence of businesses and individuals on cyber technology continues to rise, the frequency and complexity of network attacks are also increasing, posing unprecedented challenges to cyber security protection [1]. Efficient cyber security assessment and prediction can not only strengthen cyber defense, but also prevent potential security threats, which is a key measure to maintain cyber security [2]. Cyber security assessment involves real-time monitoring, analysis, and evaluation of security events in the network environment to provide decision support for future cyber defense and policy adjustment [3]. The existing security situation assessment methods often rely on expert knowledge or traditional rule-based systems, such as Support Vector Machine (SVM) improved by Particle Swarm Optimization (PSO) Algorithm and SVM optimized by Artificial Bee Colony Algorithm. Both algorithms improve the accuracy of network security situation assessment and prediction, but each has some unresolved problems and significant limitations [4]. To improve the evaluation accuracy and prediction ability of Network Security Services (NSS), a combination of Genetic algorithm (GA), Grey Wolf Optimization (GWO), and SVM is proposed. Firstly, GA is used to optimize the global search ability of GWO. Secondly, the optimized GWO is applied to optimize the kernel function parameters of the SVM. Finally, the SVM model is used to predict NSS. In addition, this paper also proposes an NSS assessment method using spectral cluster analysis.

The research innovatively combines multiple swarm intelligence optimization algorithms, and draws on the advantages of various optimization algorithms to complement each other. The core contribution of this research is to develop a more robust network security posture assessment tool, which can effectively adapt to the dynamic network environment and provide real-time

and accurate security assessment information for network security managers. The performance of the GA-GWO-SVM algorithm on different types of network security datasets is demonstrated by applying the proposed algorithm. The superiority of this method has been verified through comparative analysis with current popular security situation assessment methods. In practical applications, parameter setting, model training, and algorithm adaptability are also discussed in depth.

The first part is a review of the NSS and swarm intelligence optimization algorithms. The second part designs the NSS assessment and prediction method. The third part verifies the method proposed in the study. The fourth part is a summary of the research content.

2 Related Works

Accurately evaluating and predicting NSS can effectively improve security. The existing NSS assessment methods cannot accurately reflect large-scale cyber-attacks. Therefore, Kou G et al. [5] proposed an assessment method using attack intent identification. This method conducted situational assessment by carrying out causal analysis on attack events. Experiments showed that this method more accurately reflected the real situation of attacks without the need to train historical sequences. To improve NSS awareness data fusion, Zhang et al. [6] proposed a cloud computing method. This method used cloud computing technology to collect and process data in parallel. Results showed a high fusion accuracy and short fusion time, which had advantages over existing methods. To improve computer NSS assessment, Ariann B et al. [7] proposed a simulation model. Back Propagation neural network was used to construct a computer NSS assessment model. The network detection algorithm was combined for evaluation and prediction. The test simulation showed that the algorithm has good application effects, which was worth further promotion. To improve the accuracy and adaptability of computer network security assessment, Elhoseny M et al. [8] proposed a simulation model using neural networks. This study presented a system security detection algorithm incorporating a refined calculation scale selection strategy and an enhanced prefix span algorithm. Results demonstrated high accuracy and adaptability. Ye et al. [9] utilized the dynamic dimensional method with gray correlation analysis to enhance the gray correlation model and developed the NSS prediction model. Findings indicated that the improved model yielded prediction results that closely approximated the actual values, with smaller errors and lower time complexity.

To improve the safety of road transportation, Mokhtarimousavi S et al. [10] used PSO, harmony search algorithm, and whale optimization algorithm to improve the SVM. The influencing factors of collision severity in the work area were explored. Results showed that the proposed algorithm had the best improvement effect on SVM. To predict soil moisture content under different substrate potentials in agricultural soils, Navidi et al. [11] proposed an intelligent model to optimize SVM using firefly and particle swarm element heuristic algorithms. Results showed that the hybrid prediction accuracy of the two improved SVMs was high. They could be used to predict soil moisture content with different soil textures. The health status of lithium-ion batteries is difficult to measure directly. Therefore, Wu et al. [12] proposed a joint Bat algorithm and regression SVM to predict the health status of lithium-ion batteries. The results indicated that the prediction accuracy was high, which effectively determined the optimal SVM hyper-parameters and verified their high correlation with battery health. To solve the linear and nonlinear models in time series forecasting, Nawi W et al. [13] combined SVM and Autoregressive Integrated Moving Average Model (ARIMA) to test the effectiveness of the hybrid model with sea surface temperature data. The results showed that it was more accurate than a single ARIMA or SVM model, which produced predictions that were closer to the actual values. To improve the execution time and accuracy of SVM, Vrigazova et al. [14] proposed a feature selection method using ANOVA to optimize the performance of the support vector classifier. Then a cross-validation alternative for model selection was established. Compared with the existing methods, the method significantly improved its accuracy and calculation time.

In summary, the NSS assessment and prediction is a hot research topic in network security. Current methods have low efficiency and poor accuracy. Therefore, the swarm intelligence optimization algorithm is used to improve the SVM and then applied to the evaluation and prediction of the NSS, to improve the accuracy of the NSS assessment and prediction.

3 NSS Assessment and Prediction Using Spectral Clustering and GA-GWO-SVM Algorithm

Cyber security situation assessment and prediction is an important operation in network security. Therefore, a new NSS assessment and prediction method is proposed in Section 3. The research content is divided into two parts. The first part is the research on NSS assessment with spectral clustering, and the second part is the research on NSS prediction with GA-GWO-SVM.

3.1 NSS Assessment and Prediction Index System Construction

NSS assessment is a key step in NSS awareness. Therefore, a reasonable evaluation index needs to be established when evaluating the NSS. The NSS assessment indicators should comply with three principles. Firstly, the evaluation indicators must not affect each other. Meanwhile, the selected indicators can fully cover all aspects of the NSS as much as possible. Secondly, the selected evaluation indicators should be determined according to their importance, and the factors that have little impact on the changes in NSS should be excluded. Thirdly, the evaluation indicators must contain both static indicators and dynamic indicators. Based on the above principles, when constructing the NSS assessment index system, the three directions of network asset operation, system vulnerability, and security risk are taken as the selection direction of the evaluation indicators. The specific index system is shown in Figure 1.

There are 14 specific indicators in the evaluation system. These network indicators need to be quantified in the evaluation process. Total network traffic reflects the amount of data flowing through the network over a period,

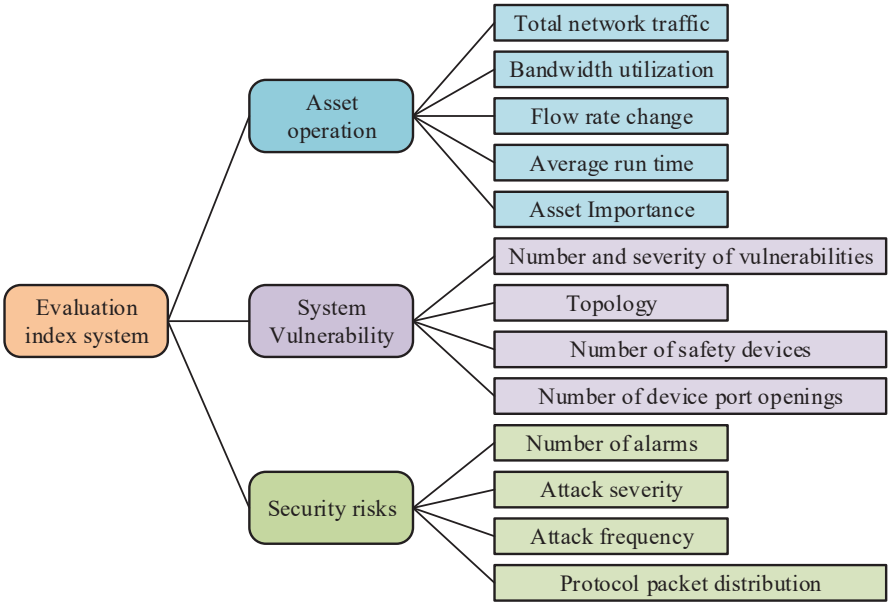

Figure 1 NSS evaluation index system.

quantified by Equation (1) [15].

$$Q_{total} = \sum_{t=1}^{\tau} \sum_{i=1}^{n} q_t^i,\ t \in \{1, 2, \ldots, \tau\} \tag{1}$$

In Equation (1), Q_{total} represents the total network traffic, t represents a certain moment in the τ time, and q_t^i represents the amount of data transmitted by the i data stream at time t. n represents the total number of data flows in a single moment t. Bandwidth utilization is the ratio between the traffic passing through the network and the limited traffic of the system in a certain period. The change rate in traffic represents the increase or decrease in traffic in a network system over a period, as quantified by Equation (2) [16].

$$Q_c = \frac{Q_{\tau-1}}{Q\tau} \times 100\% \tag{2}$$

In Equation (2), the network traffic change rate is described as Q_c. The amount of data transferred in the current τ time period is represented by Q_τ. The amount of data transferred in the previous $\tau - 1$ time period is described as $Q_{\tau-1}$. The importance of assets is an important indicator for assessing the risk, which is usually measured by the information importance score of the system host and the system security score. It is quantified by Equation (3).

$$V_{asset} = \frac{1}{2} \sum_{k=1}^{N} (I_k + S_k) \tag{3}$$

In Equation (3), the importance of the asset is described as V_{asset}, the number of devices in the system is described as N, the importance score of host information is described as I_k, and the OS kernel score of the device is described as S_k. The number and severity of system vulnerabilities can reflect the risk importance of the network security situation, which is usually quantified by Equation (4).

$$Severity_{bug} = \sum_{i=1}^{N} \sum_{j=1}^{M_b} W_{ij}^b H_i A_{ij}^b \Big/ Num_{bug} \tag{4}$$

In Equation (4), $Severity_{bug}$ represents the severity of the vulnerability, Num_{bug} represents the number of vulnerabilities, M_b represents the number of types of vulnerabilities, A_{ij}^b represents the number of class j vulnerabilities in the device i, and W_{ij}^b represents the severity of the vulnerability. Network

topology is a classic static metric in network security situation assessment, which is quantified by the number of nodes in the topology, as shown in Equation (5) [17].

$$\begin{cases} Score_i = \begin{cases} 1. & nodes \in [0,3) \\ 0.7 & nodes \in [3,6) \\ 0.4 & nodes \in [6,8) \\ 0.1 & nodes \in [8,+\infty) \end{cases} \\ Score_{topology} = \sum_{i=1}^{n} Score_i \end{cases} \tag{5}$$

In Equation (5), $Score$ is the score of the network topology with different numbers of nodes, $Score_{topology}$ represents the score of the entire network topology, n denotes the number of subnets, and $nodes$ is the number of subnet nodes. The frequency of security incidents can reflect the security of network systems, which is usually quantified by Equation (6).

$$freq_t = Num_t/t \tag{6}$$

In Equation (6), $freq_t$ represents the frequency of network security incidents, and Num_t denotes the number of attacks and threats to the network system during the time period t. The severity of a cyber-attack, which reflects the impact of an attack or threat on a network system, is quantified by Equation (7).

$$Severity_{attack} = \sum_{i=1}^{N} \sum_{j=1}^{M_b} W_{ij}^a H_i A_{ij}^a \Big/ Num_{attack} \tag{7}$$

In Equation (7), $Severity_{attack}$ is the attack severity, H_i represents the information importance of the i device, Num_{attack} denotes the number of detected attacks in time period, M_b is the number of attack categories, A_{ij}^a represents the number of attack at which device i is subjected to class j attacks, and W_{ij}^a represents the level of attack at which device i is subjected to class j attacks. The assessment level of cyber security situation is generally divided into four levels in Table 1.

Spectral clustering analysis is a clustering method based on graph partitioning, which can effectively mark the abnormal data hidden in the network system when evaluating the NSS. The process of the NSS assessment algorithm based on spectral clustering is shown in Figure 2.

Table 1 NSS level and index range

Security Level	Numerical Labeling	Situational Value Range	Description of Network Status
Secure	1	0.00∼0.20	Normal
Mild danger	2	0.20∼0.40	Mild threat
Moderate risk	3	0.40∼0.75	Moderate threat
High risk	4	0.70∼0.90	Heavy threat

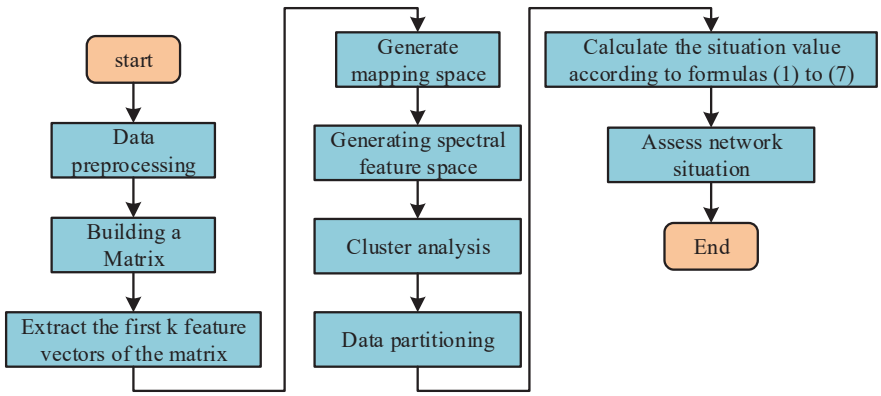

Figure 2 Situation assessment process based on spectral clustering.

3.2 NSS Prediction Using GA-GWO-SVM

SVM is a common classification model for predicting NSS, but the prediction accuracy of conventional SVM is poor. Therefore, it is necessary to improve and optimize its kernel function. SVM realizes the classification prediction of samples by finding the optimal partition hyperplane in the classification space. The distance from a certain point to the hyperplane in the n-dimensional sample space can be represented by Equation (8) [18].

$$r = \frac{|w^{\mathrm{T}}x + b|}{\|w\|}. \tag{8}$$

In Equation (8), r represents the distance from a point in the sample space to the hyperplane, w represents the normal vector, and $|w^{\mathrm{T}}x + b|$ represents the hyperplane expressed by the vector method. If the SVM is correctly divided, then the data on the same side of the hyperplane have the same properties. At any point (x_i, y_i) in the sample space, y_i is consistent with the positive or negative of the hyperplane, the data point is a support vector, and

the distance between the support vector and the hyperplane can be expressed as Equation (9) [19].

$$d = \frac{|w^{\mathrm{T}} x_i + b|}{\|w\|} \tag{9}$$

The SVM's actual purpose is to find the support vector with the largest data interval. To find the maximum interval, it is necessary to make $\|w\|$ smallest, so the solution problem of SVM can be expressed as Equation (10) [20].

$$\begin{aligned} &\min_{w,b} \frac{1}{2}\|w\|^2 \\ &s.t.\ y_i(w^{\mathrm{T}} x_i + b) \geq 1,\ i = 1, 2, \ldots, n \end{aligned} \tag{10}$$

SVM is usually used to improve the classification and prediction of linear classifiable data, but the data in NSS awareness are linear and inseparable. Therefore, when using SVM to process the data in NSS awareness, it is necessary to conduct high-dimensional mapping processing on the data, so that SVM can classify and predict this problem. If $\phi(x)$ represents the x's eigenvector in the high-dimensional space, the partitioned hyperplane of the nano-high-dimensional space is calculated in Equation (11).

$$f(x) = w^{\mathrm{T}} \phi(x_i) + b \tag{11}$$

Correspondingly, the solution problem for SVM should be rewritten as Equation (12).

$$\begin{cases} \min\limits_{w,b} \dfrac{1}{2}\|w\|^2 \\ s.t.\ y_i(w^{\mathrm{T}} \phi(x_i) + b) \geq 1,\ i = 1, 2, \ldots, n \end{cases} \tag{12}$$

When using SVM to solve nonlinear separable data, it is allowed to have points in the training set that do not satisfy Equation (12). This class of SVMs, also known as soft-spaced SVMs, introduces an alternative function that converts Equation (12) into Equation (13).

$$\begin{cases} \min\limits_{w,b} \dfrac{1}{2}\|w\|^2 + C\sum\limits_{i=1}^{n} \xi_i \\ s.t.\ y_i(w^{\mathrm{T}} \phi(x_i) + b) \geq 1 - \xi_i,\ \xi \geq 0, i = 1, 2, \ldots, n \end{cases} \tag{13}$$

In Equation (13), the relaxation factor is denoted as ξ_i, and the penalty factor is described as C. After introducing the Lagrange multiplier, the duality problem of soft-spaced SVMs can be expressed by Equation (14).

$$\begin{cases} \max\limits_{\alpha} \sum\limits_{i=1}^{n} \alpha_i - \dfrac{1}{2} \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} \alpha_i \alpha_j y_i y_j \phi(x_i)^{\mathrm{T}} \phi(x_j) \\ s.t. \sum\limits_{i=1}^{n} \alpha_i y_i = 0, 0 \le \alpha_i \le C, i = 1, 2, \ldots, n \end{cases} \tag{14}$$

In Equation (14), the Lagrangian multiplier is described as α, and the inner product of the sample points x_i and x_j in the high-dimensional space are described as $\phi(x_i)^{\mathrm{T}} \phi(x_j)$. The kernel function is used to replace the inner product to effectively reduce the computational cost of SVM. The kernel function used in the study is a mixture of Gaussian kernel function and polynomial kernel function, as shown in Equation (15).

$$k(x_i, x_j) = \mu (x_i^{\mathrm{T}}, x_j)^{\theta} + (1 - \mu) \exp\left(- \frac{\|x_i - x_j\|^2}{2\sigma^2} \right) \tag{15}$$

In Equation (15), σ is the radial basis radius of the Gaussian kernel function, θ represents the polynomial kernel function order, and μ denotes the linear combination coefficient. GA is an intelligent optimization algorithm based on the basic laws of biological development. In algorithm implementation, it is necessary to first determine the encoding rules, initialize the population, and then calculate the individual fitness. All individuals' fitness in the population is obtained. Individual genetic operations are performed to generate the next generation population until the algorithm completes the maximum number of iterations, as shown in Figure 3.

In the iterative optimization, the GA has good global search ability and individual retention ability, with strong adaptability, but it also has problems such as the slow iterative calculation speed. The GWO algorithm is an intelligent algorithm simulating the hunting style of wolves, a highly hierarchical animal population. Usually, the wolf pack includes four classes, namely α, β, δ, and ω. α is the leader, responsible for the overall decision-making of the wolf pack. β is the successor of the leader in the wolf pack, which can assist the leader's work. δ and ω are ordinary members of the wolf pack, of which ω has the lowest status. In the GWO algorithm, the highest fitness in the pack is the leader of the pack. At the beginning of the GWO algorithm, it is necessary to complete the α, β, δ, and ω classification of the wolf pack, followed by the

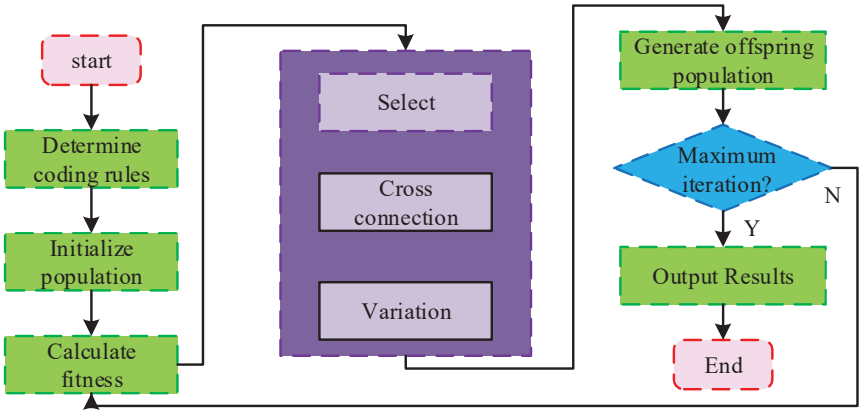

Figure 3 GA flow.

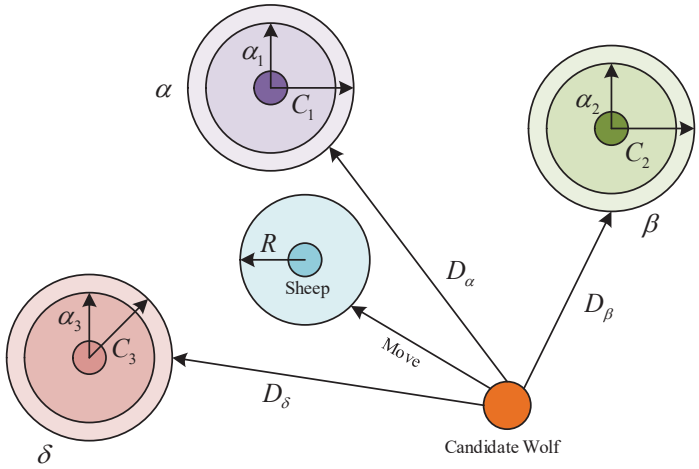

Figure 4 Schematic diagram of Wolf pack hunting behavior.

hunting of the wolf pack. After selecting the prey, the individual position and parameters of the wolf pack are updated. Finally, after the algorithm reaches maximum iteration, the output result is sufficient. The GWO's hunting part is the core part. The hunting behavior of wolves is shown in Figure 4.

The GWO algorithm is a simple and flexible swarm intelligence optimization algorithm, which has weak global search ability and relatively single population. Circular chaotic map is a nonlinear dynamical system that is usually used to describe chaotic phenomena in the complex plane. One

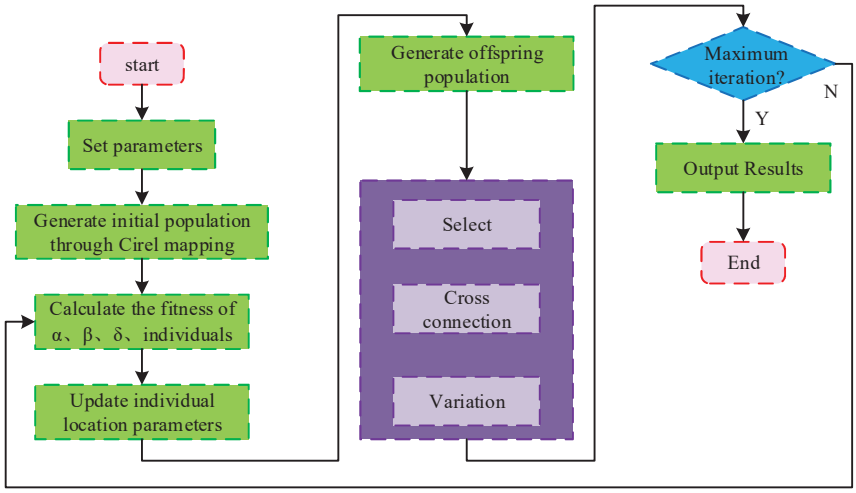

Figure 5 GA-GWO algorithm flow.

of the characteristics of circular chaotic mapping is that it has parameter sensitivity. Small parameter changes may lead to drastic change in system behavior, which is one of the common characteristics in the chaotic system. This parameter sensitivity makes cyclic chaotic mapping possible in cryptography, random number generation, and signal processing. Therefore, the Circle chaotic mapping method is used in the initialization of wolf packs. The GA is added to improve the GWO algorithm. The improved GA-GWO algorithm is as follows. Firstly, the initial parameters are set. Secondly, the initial population is generated by using the Circle chaos map. Thirdly, the individual fitness is calculated. The fourth is to update the position parameters of the wolf pack and generate offspring wolf packs. The fifth is the genetic operation of the offspring wolf pack when the termination condition is met, as shown in Figure 5.

Therefore, the GA-GWO algorithm constructed above is designed to optimize the parameters of the hybrid kernel function. The optimization steps are as follows. Firstly, the mapping relationship is established between the feasible solution and the solution space. Secondly, the wolf pack size is set to 30, and the number of algorithm iterations is set to 500. The crossover operator is set to 0.7 and mutation operator is set to 0.02. Thirdly, the fitness function is constructed. Fourthly, the fitness function of the population individuals is calculated, and the top three individuals with fitness are marked as the leader. Then the location information of the rest of the population is

updated according to the leader wolf information. Fifthly, according to the elite retention strategy of the GA, the individuals demonstrating the highest fitness are retained for the subsequent generation. Sixthly, the population individuals are selected until the population size of the offspring is consistent with the size of the primary population. Seventh, the cross-mutation operation is carried out according to the crossover operator and the mutation operator's coefficient is adjusted iteratively until the maximum number of iterations is reached. Finally, the optimized parameters of the SVM kernel function are obtained using GA-GWO. The SVM model can be trained.

4 Experimental Verification Analysis of GA-GWO-SVM Algorithm

A NSS prediction method based on spectral clustering analysis and GA-GWO-SVM is proposed in Section 2. Therefore, the feasibility of the proposed method is experimentally verified in Section 3, which is divided into three parts. The first part analyzes the experimental parameters and environment. The second part verifies the effect of NSS assessment. The third part analyzes of the effect of NSS prediction.

4.1 Experimental Parameters and Environmental Settings

The dataset used in the study is CIC-IDS2017, which is created by the Cybersecurity laboratory at Concordia University in Canada. This dataset is dedicated to evaluate network intrusion detection system performance. It collects a large amount of network traffic data, including normal traffic and various types of network intrusion behaviors, such as Denial-of-service attack (DoS), Distributed Denial-of-service attack (DDoS), malware, etc. This data can help researchers and developers train and evaluate network security solutions, thereby improving network security. The experimental operating system is Windows 10, the CPU is Intel(R) Core (TM) i5-1035G1, the system memory is 16GB, and the experimental development software is PyCharm 2019.1.3. The environment details are shown in Table 2.

4.2 Effect Analysis of NSS Assessment

K-means clustering analysis is a common clustering method to verify the evaluation effect of the proposed spectral clustering analysis method on NSS awareness. The evaluation effects are fitted and analyzed in Figure 6.

Table 2 Experimental environment information

Category	Device	System	IP
Safety equipment	Firewall	Fortinet	172.16.0.1
Attack network	PC	Ubuntu14.4-32 / 64	192.168.10.19
		Windows 8	205.174.165.72
		Windows 8-64	192.168.10.5
		Kali-Linux	205.174.165.73
		Ubuntu16.4-32/64	192.168.10.16
		Windows 7-pro-64	192.168.10.9
		Windows Vista	192.168.10.8
Attacked network	PC	Windows 10-pro-64	192.168.10.15
		Mac	192.168.10.25
	North	Ubuntu16	192.168.10.50
		Ubuntu12	205.174.165.66
		Web Server 16	192.168.10.3

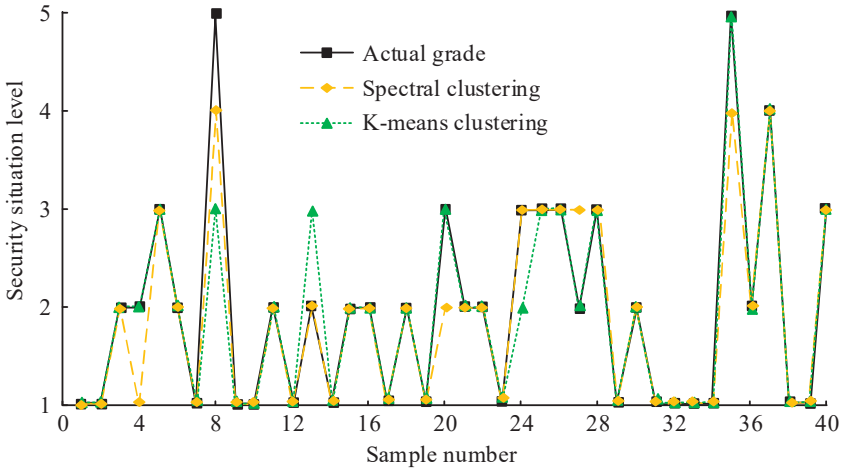

Figure 6 Fitting effect of NSS awareness assessment.

From Figure 6, in samples 8, 13, and 24, the NSS assessment algorithm based on spectral clustering analysis had poor fitting effect on the evaluation of the samples, and the fitting effect of the other samples was better. The actual network security situation level of sample 8 was 5, and the spectral clustering evaluation level was 3. Sample 13 had an actual network security posture level of 2 and a 3 for spectral clustering. Sample 24 had an actual cyber security posture level of 3 and a 2 for spectral clustering. In samples

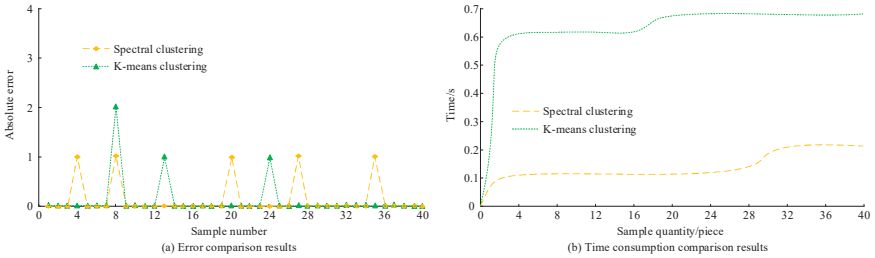

Figure 7 Error-wise and time-consuming comparison.

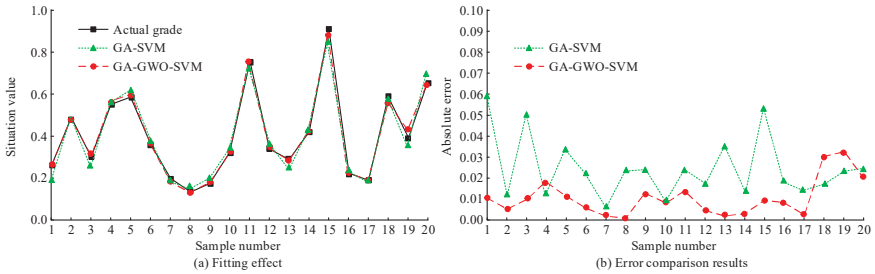

Figure 8 Comparison results of fitting effect and error.

4, 8, 20, 27, and 35, the network situation assessment algorithm based on K-means cluster analysis had a poor fitting effect on the samples, while the fitting effect in the other samples was more in line with the actual situation. The error and time taken in the NSS assessment are compared in Figure 7.

Figure 7(a) shows a comparison of the errors of the two analysis methods. In samples 13 and 24, the error of the spectral clustering method was higher than the K-means clustering method. In the rest of the samples, the spectral clustering method's error was always lower than the K-means clustering. Figure 7(b) presents the time comparison taken by the two methods to complete the NSS assessment. The assessment time of the spectral cluster analysis method was maintained below 0.3s, while the network situation assessment based on the K-means cluster analysis method was maintained at about 0.6s. The evaluation method of NSS uses K-means clustering analysis for both accuracy and efficiency.

4.3 Analysis of the Prediction Effect of NSS

To verify the feasibility of the improved GA-SVM, the fitting effect and absolute error of GA-GWO-SVM and the GA-SVM are compared in Figure 8.

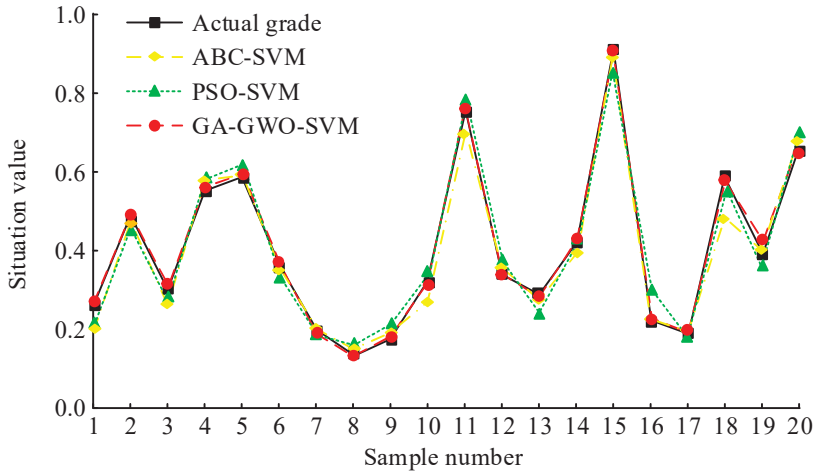

Figure 9 Prediction effects comparison for different algorithms.

Figure 8(a) presents the comparison of the fitting effect of the two algorithms. The overall fitting effect of the GA-GWO-SVM algorithm was better than that of the GA-SVM algorithm. The GA-SVM algorithm had obvious errors in samples 1, 3, 8, 9, 11, 13, 15, 19 and 20. However, the error of the GA-GWO-SVM algorithm was only obvious in samples 15 and 19. The error of the GA-GWO-SVM algorithm on these two samples was also smaller than that of the GA-SVM. In Figure 8(b), the GA-GWO-SVM algorithm had a maximum error of 0.4112 in sample 19 and a minimum error of 0.0023 in sample 8. The GA-SVM obtained the maximum error value of 0.5896 in sample 1 and 0.0051 error value in sample 7. After optimizing the GWO algorithm, the error of the GA-SVM algorithm was significantly reduced. It is feasible to study the improvement of the GA-SVM algorithm. After determining the feasibility of the improved algorithm, the GA-GWO-SVM is compared with PSO-SVM and ABC-SVM. The results are shown in Figure 9.

In Figure 9, among the three NSS prediction methods, the ABC-SVM algorithm had the worst fitting effect. There were serious errors in sample 11 and sample 18. In sample 11, the error of the ABC-SVM algorithm was about 0.04. In sample 18, the error of the ABC-SVM algorithm was about 0.18. The GA-GWO-SVM algorithm had the best fitting effect. The error in each sample is at a low level. The Mean Absolute Percentage Error (MAPE) and Root Mean Square Error (RMSE) of the three algorithms are also compared in Figure 10.

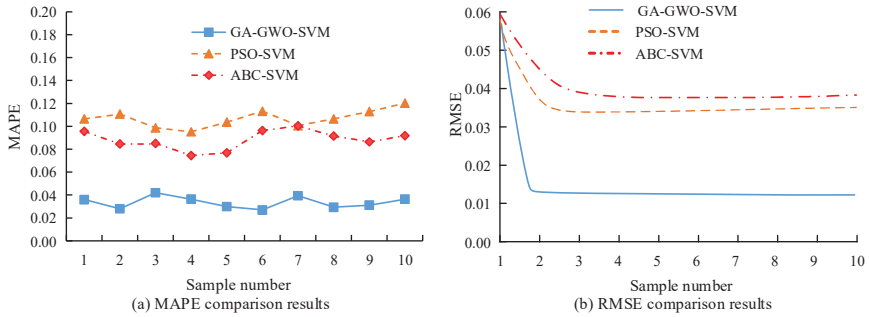

Figure 10 Comparison results of MAPE and RMSE.

Figure 10(a) shows the comparison of the MAPE values of the three algorithms. The MAPE value of GA-GWO-SVM was 0.0270 in sample 6, 0.0745 in sample 4, and 0.0952 in sample 4. Figure 10(b) presents the comparison of the RMSE values of the three algorithms. The RMSE value of the GA-GWO-SVM was the lowest 0.0130, the RMSE of the ABC-SVM algorithm was 0.0362, and the RMSE value of the PSO-SVM algorithm was 0.0349.

5 Conclusion

To realize the NSS assessment and prediction, an NSS assessment method using spectral cluster analysis and based on GA-GWO-SVM was proposed. Spectral cluster analysis is a cluster analysis, which has good application effects in system evaluation. The GA-GWO-SVM algorithm used the GA to optimize the GWO algorithm to improve global search ability and elite retention ability of the GWO. Finally, the improved GWO was used to optimize SVM parameters to improve its prediction ability. The results proved that the GA-GWO-SVM had significant advantages in NSS assessment and prediction. The proposed solution showed better fitting effects than other algorithms in error analysis. When comparing the GA-SVM algorithm, the GA-GWO-SVM had a significant error improvement in 11 samples, especially in samples 15 and 19. The GA-SVM exhibited errors of 0.5896 and 0.0051, while the maximum error of the GA-GWO-SVM was 0.4112, and the minimum error was 0.0023. In addition, compared with PSO-SVM and ABC-SVM algorithms, the GA-GWO-SVM algorithm also showed the best fitting performance. Especially, the error of ABC-SVM on samples 11 and 18 was about 0.04, which was particularly significant compared with the

GA-GWO-SVM algorithm. This study effectively improves the accuracy of NSS assessment and prediction, but GA-GWO-SVM is slightly insufficient in terms of computing speed. The algorithm efficiency in NSS prediction will be further improved in the future.

References

[1] Salman, F. M., Lehmoud, A. A. M., and Joda, F. A. (2023). Adaptation of the Ant Colony Algorithm to Avoid Congestion in Wireless Mesh Networks. Journal of Cyber Security and Mobility, 12(05), 785–812. https://doi.org/10.13052/jcsm2245-1439.1258.

[2] Shen M, Tang X, Zhu L, Du X, Guizani M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal, 2019, 6(5): 7702–7712.

[3] Patil N. An enhanced segmentation technique and improved support vector machine classifier for facial image recognition. International Journal of Intelligent Computing and Cybernetics, 2021, 15(2): 302–317.

[4] Tan L, Yu K, Ming F, Cheng X, Srivastava G. Secure and resilient artificial intelligence of things: a HoneyNet approach for threat detection and situational awareness. IEEE Consumer Electronics Magazine, 2021, 11(3): 69–78.

[5] Kou G, Wang S, Tang G. Research on key technologies of NSS awareness for attack tracking prediction. Chinese Journal of Electronics, 2019, 28(1): 162–171.

[6] Zhang H, Kang K, Bai W. Hierarchical NSS awareness data fusion method in cloud computing environment. Journal of Computational Methods in Sciences and Engineering, 2023, 23(1): 237–251.

[7] Hussain, S. S., Razak, M. F. A., and Firdaus, A. (2023). Deep Learning Based Hybrid Analysis of Malware Detection and Classification: A Recent Review. Journal of Cyber Security and Mobility, 13(01), 91–134. https://doi.org/10.13052/jcsm2245-1439.1314.

[8] Tang Y, Elhoseny M. Computer network security evaluation simulation model based on neural network. Journal of Intelligent & Fuzzy Systems, 2019, 37(3): 3197–3204.

[9] Ye C, Shi W, Zhang R. Research on gray correlation analysis and situation prediction of network information security. EURASIP Journal on Information Security, 2021, 2021(1): 1–6.

[10] Mokhtarimousavi S, Anderson J C, Azizinamini A, Hadi, M. Improved support vector machine models for work zone crash injury severity

prediction and analysis. Transportation research record, 2019, 2673(11): 680–692.

[11] Navidi M N, Seyedmohammadi J, Seyed Jalali S A. Predicting soil water content using support vector machines improved by meta-heuristic algorithms and remotely sensed data. Geomechanics and Geoengineering, 2022, 17(3): 712–726.

[12] Wu T, Huang Y, Xu Y, ian, J, Liu S, Li Z. SOH prediction for lithium-ion battery based on improved support vector regression. International Journal of Green Energy, 2023, 20(3): 227–236.

[13] Nawi W, Lola M S, Zakariya R, Zainuddin N H, Abd Hamid A A K, Aruchunan E, Nazzrol N S A. Improved of forecasting sea surface temperature based on hybrid ARIMA and support vector machines models. Malaysian Journal of Fundamental and Applied Sciences, 2021, 17(5): 609–620.

[14] Vrigazova B, Ivanov I. Optimization of the ANOVA procedure for support vector machines. International Journal of Recent Technology and Engineering, 2019, 8(4): 5160–5165.

[15] Chen Z. Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm. Journal of Computational and Cognitive Engineering, 2022, 1(3): 103–108.

[16] Raj D J S, Ananthi J V. Recurrent neural networks and nonlinear prediction in support vector machines. Journal of Soft Computing Paradigm, 2019, 1(1): 33–40.

[17] Purohit J, Dave R. Leveraging Deep Learning Techniques to Obtain Efficacious Segmentation Results. Archives of Advanced Engineering Science, 2023, 1(1): 11–26.

[18] Zhang H, Li Y, Lv Z, Sangaiah A K, Huang T. A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA Journal of Automatica Sinica, 2020, 7(3): 790–799.

[19] Salman, F. M., Lehmoud, A. A. M., and Joda, F. A. (2023). Adaptation of the Ant Colony Algorithm to Avoid Congestion in Wireless Mesh Networks. Journal of Cyber Security and Mobility, 12(05), 785–812. https://doi.org/10.13052/jcsm2245-1439.1258.

[20] Wang J, Wu L, Wang H, Choo K K R, He D. An efficient and privacy-preserving outsourced support vector machine training for internet of medical things. IEEE Internet of Things Journal, 2020, 8(1): 458–473.

Biographies

Guoying Han graduated from Shijiazhuang Tiedao University in 2015 with a Master's degree in Computer Technology Engineering. He is currently a full-time teacher in the Department of Network Engineering at Hebei University of Engineering and Technology. Hosted one provincial-level project and published 17 papers in well-known domestic peer journals. His research areas include computer technology, Internet of Things technology, and artificial intelligence.

Bin Zhou obtained a Master's degree in Engineering Management from Hebei University of Economics and Trade in Shijiazhuang in 2024. At present, he serves as a full-time teacher and department head in the Department of Electronic Information Engineering at Hebei University of Engineering and Technology. He is the head of the provincial-level first-class professional electronic information engineering and the course leader of the provincial-level first-class course computer network. Main courses include computer networks, fiber optic communication, artificial intelligence, and network optimization. He is also a national undergraduate thesis sampling expert of the Ministry of Education. Published articles in 8 well-known domestic peer-reviewed journals and conference proceedings. Interest areas

include machine learning, image processing, pattern recognition, and network security.

Yazi Zhang graduated from Qingdao University of Technology in 2011 with a Bachelor's degree in Measurement and control technology and instruments. She has published 3 papers. Current full-time teacher at Hebei University of Engineering and Technology. Her research interests include Internet of things control system and Artificial Intelligence.