Design of Network Attack Intrusion Detection System Based on Improved FWA Algorithm

Qingsong Chang[1]*, Weiyan Feng[2], Xingguo Wang[3]
Party Committee Propaganda Department Network Information Center, Weifang Engineering Vocational College, Weifang, 262500, China[1]
Department of Information Engineering, Weifang Engineering Vocational College, Weifang, 262500, China[2, 3]

***Abstract*—The increasing diversity of network attack behaviors has led to increasingly serious network security issues. Based on this, this study proposes an optimized fireworks algorithm to build an intrusion detection model. Firstly, the traditional algorithm is optimized by improving the uniformity of initial individual distribution and designing a fitness value update strategy, which greatly reduces the computational burden of the model and improves recognition accuracy. Then, the feature analysis detection strategy is selected and the model is fused to ensure system stability. Finally, to validate the effectiveness of the model, a comparative experimental analysis is conducted. The results validated that the average accuracy of the research model was 99.06%, with an average detection rate of 96.98%, which is relatively higher than the other models by 2.57%. The error warning rate was only 0.13%, lower than the other models of 1.60%. In summary, the proposed intrusion detection model based on the fireworks algorithm and feature analysis can effectively identify attack behaviors and classify them correctly.**

Keywords*—Fireworks algorithm; fitness; initial cluster; characteristics; intrusion detection; network

I. Introduction

At present, the popularity of the network is constantly improving. The internet has become an indispensable part of people's daily life, providing great convenience for users. However, corresponding cybersecurity issues have emerged one after another, gradually evolving from personal privacy breaches, online fraud, etc. to major issues that disrupt social order and public security, and even national defense security. At the same time, the types of network intrusion are diverse and constantly evolving, seriously threatening the privacy of individuals and businesses. In response to the increasingly severe network security issues, Network Intrusion Detection (NID) technology has emerged. This technology aims to identify abnormal behavior or unreasonable data flow in network systems by monitoring and analyzing network traffic. After timely detection of attack behavior, preventing it from continuing to invade further maintains the integrity, confidentiality, and availability of the network system [1-2]. As an important carrier of information transmission, the security of image is directly related to the protection of personal privacy and business secrets. In recent years, the problems of image tampering, forgery and unauthorized access are frequent, which puts forward higher requirements for image security.

In recent years, NID technology has received widespread attention from the academic community. Common strategies can be divided into attack behavior recognition through feature analysis and comparison, as well as recognition strategies based on behavior detection. In addition, cutting-edge technologies such as artificial intelligence and machine learning have been integrated, further improving the model's detection accuracy. Some scholars have also proposed image authentication technology based on digital watermarking to ensure the integrity and authenticity of images to a certain extent. In addition, encryption technology is also widely used in the protection of images to prevent unauthorized access and protect the privacy of image content.

However, NID technology still faces various challenges. Firstly, with the continuous advancement of network attack methods, Intrusion Detection Systems (IDSs) are facing increasingly diverse types and methods of attacks. This requires IDS to quickly adapt to new security threats. With the development of image processing technology, attackers can use more advanced technology to tamper with and forge images. Secondly, how to maintain the availability and access efficiency of images while ensuring the security of images is also an urgent problem to be solved [3-4].

Therefore, this study proposes an intrusion detection model based on the Fireworks Algorithm (FWA) optimization, which solves the problem of local optima by optimizing the initial cluster distribution. The contributions of this research are as follows: (1) A deep learning based image tamper detection algorithm is proposed, which can effectively identify abnormal regions in images. (2) The fitness value update strategy optimization reduces the time complexity of the model, which greatly reduces the operating burden of the model while ensuring accuracy. The research content consists of six sections. Section II introduces the current research status of NID. Section III designs intrusion detection methods based on FWA. Section IV conducts experimental analysis on the model. Section V summarizes the experimental results. Finally, Section VI concludes the paper.

II. Related Works

Many scholars have conducted research on NID technology to address the issue of network security maintenance. Ahmed et al. proposed an IDS based on load balancing algorithm, which optimizes task allocation between sensor data and individuals to be identified, greatly reducing latency. Subsequently, a dynamic convergence strategy was introduced to integrate entropy-based active learning and attention modules to improve the efficiency of intrusion recognition. Their model could significantly improve the efficiency of intrusion detection [5].

Liu et al. abandoned conventional deep learning models and proposed a widely learned intrusion detection system based on LU decomposition. It excavated deep information from data by constructing graph Laplacian operators and embedded them into manifold regularization frameworks to enhance the accuracy of the model in detecting attack behavior. Finally, LU decomposition was used to improve the training speed of the model, and their model outperformed traditional machine learning algorithms in intrusion detection performance across multiple datasets [6]. Subramani et al. designed an intelligent IDS built on feature analysis to address security threats in wireless sensor networks in the Internet of Things. Their model combined rules and multi-objective particle swarm optimization algorithm, aiming to build a feature selection model. In addition, an enhanced multi class support vector machine classification algorithm has been introduced to further improve the recognition accuracy of intrusion detection behavior. Finally, they tested the model on the KDD'99 Cup and CIDD, and found that the model significantly improved the recognition accuracy of intrusion detection behavior and reduced the False Alarm Rate (FAR) [7]. Ma et al. constructed a programmable IDS for the security maintenance of micro-grid networks. Firstly, programmable signals were injected into the system and their response results were analyzed. Micro-grids had low inertia characteristics, indicating that the system was highly sensitive to attacks and was highly susceptible to intrusion behavior, even spreading to adjacent systems. The model they designed significantly reduced the probability of this situation occurring [8].

Vitorino et al. proposed an adaptive intrusion detection system for adversarial attack behavior in network intrusion. Firstly, the basic constraints in the model were designed, and then an adaptive perturbation mode was introduced to strengthen the constraints in the gray box setting. This indicated that their methods heavily relied on the adaptability of various features. Finally, the experimental analysis showed that the model significantly improved the recognition accuracy of the system against adversarial attacks [9]. Pande et al. realized the limitations of traditional intrusion detection techniques and therefore improved common deep learning models. They compared and analyzed deep learning frameworks with traditional machine learning. Their proposed learning framework has significantly improved the average detection accuracy index, reaching over 99% [10]. Thakkar et al. optimized the detection of transformation attack behavior. They also used deep learning as the basic design model and introduced Dropout and regularization techniques to optimize the model in response to the over-fitting defects of traditional models. The focus was on integrating regularization techniques. To verify the model performance, they compared it on multiple datasets, and the model was able to effectively monitor network intrusion attacks [11]. Through the analysis of recent studies, the limitations of similar research fields are obtained, and the corresponding treatment methods are proposed, as shown in Table I.

TABLE I. EXISTING RESEARCH ANALYSIS AND RESEARCH TREATMENT METHODS

Research	Major technology	Limitation	Optimization of research methods
Ahmed et al. [5]	IDS based on load balancing algorithm	It is easy to fall into local optimality when dealing with large-scale data	Optimize initial individual distribution and fitness update strategies
Liu et al. [6]	Extensive learning IDS based on LU decomposition	The detection accuracy is unstable	The manifold regularization frame is used to improve the detection accuracy
Subramani et al. [7]	Intelligent IDS based on feature analysis	Lack of generalization ability	The generalization ability of the model is improved by feature analysis
Ma et al. [8]	Programmable IDS	Lack of sensitivity to attack	A programmable signal is injected and the response is analyzed
Vitorino et al. [9]	Adaptive IDS for adversarial attack behavior	Depends on the adaptability of various characteristics	An adaptive perturbation model is introduced to strengthen the constraint
Pande et al. [10]	IDS based on deep learning	The detection accuracy is not stable	Compare deep learning frameworks
Thakkar et al. [11]	Detection and optimization of deformation attack behavior	Insufficient accuracy in detecting unknown attack behavior	Introduce Dropout and regularization techniques

Numerous studies have optimized the recognition accuracy of intrusion detection models, but this can also lead to an increase in model time complexity. Therefore, this study proposes strategies such as updating fitness values and optimizing initial positions to greatly reduce the computational burden, while also ensuring the recognition accuracy of the algorithm.

III. AN INTRUSION DETECTION MODEL THAT INTEGRATES OPTIMIZED FWA AND FEATURE ANALYSIS STRATEGIES

In response to the security issues arising from network attacks, this study proposes using FWA to establish an intrusion detection model. Firstly, the uniformity of the initial individual distribution is optimized, and improvements are made to address convergence performance issues. Then, it is applied to NID, and a feature analysis based detection strategy is selected to fuse the model.

A. Improvement Design of FWA Based on Initial Cluster Optimization Strategy

With the growing popularity of the Internet and frequent network attacks, network security maintenance has become a research hotspot. Therefore, this study proposes to use FWA to build an intrusion detection model. FWA aims to simulate the phenomenon of fireworks explosions and treat each explosion point as an effective solution, searching for the global optimum

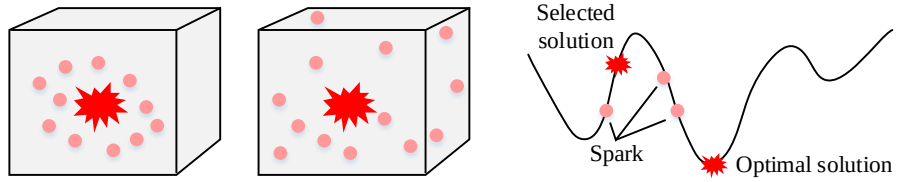
in the entire explosion space. This requires calculating the fitness value of each solution and combining it with the explosion operator to generate feasible solutions. If there are a large number of sparks around the fireworks, the corresponding fitness value is higher, and vice versa, the fitness value is lower, as shown in Eq. (1) [12-13].

$$S_i = S\frac{f_{\max} - f(x_i) + \delta}{\sum_{i=1}^{N}\left(f_{\max} - f(x_i)\right) + \delta} \quad (1)$$

In Eq. (1), S_i represents the explosion intensity of fireworks x_i. S is the explosion intensity control parameter. $f(x_i)$ represents the fitness value of cover x_i. $f_{\max}$ represents the maximum fitness value among all fireworks. δ is a constant that takes an infinitesimal value to avoid division by zero. In addition, to ensure population diversity and better search for global optimal solutions, the algorithm introduces Gaussian mutation, as shown in Eq. (2).

$${}_g X_i^k = X_i^k \cdot Gaussian(1,1) \quad (2)$$

In Eq. (2), ${}_g X_i^k$ is the position vector of Gaussian variation sparks in the k dimension. X_i^k represents the position vector value of fireworks x_i in the k dimension. $Gaussian(1,1)$ is a Gaussian distribution with both mean and variance of 1. The fitness value judgment and Gaussian variation process of fireworks are shown in Fig. 1.



(a) Excellent spark (b) Bad firework (c) Gaussian variation

Fig. 1. Visualization of FWA operation.

The population of individuals after Gaussian mutation includes initial fireworks, as well as mutation sparks and explosion sparks. Finally, it is necessary to determine whether the algorithm has completed the iteration based on the convergence requirements. If the requirements are not met, the initial fireworks cluster will be regenerated and the search for the global optimal solution will continue. However, the initial fireworks distribution of classical FWA is uneven, and the iterative strategy is complex, resulting in poor efficiency and accuracy of the algorithm. Therefore, this study addresses the above issues by improving the initial algorithm by introducing an initial individual discretization strategy aimed at avoiding local optimization problems caused by the initial fireworks position. Before this, it is needed to design the coverage length of the solution space, as shown in Eq. (3).

$$l_i = (x_i)_{\max} - (x_i)_{\min}, i \in [1,k] \quad (3)$$

In Eq. (3), l_i is the coverage length of the i-dimensional search space. $(x_i)_{\max}$ / $(x_i)_{\min}$ represents the min and max values of the corresponding coordinates in the search space. Additionally, the update position of classical FWA is related to the previous iteration data, so the global optimization effect is greatly affected by whether the initial position is uniform. The pseudo-random nature of its random function determines that the initial cluster distribution is relatively concentrated. In response to this issue, this study introduces an initial fireworks dispersion strategy aimed at screening through fireworks distance, as shown in Eq. (4) [14-15].

$$d = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \ldots + (x_k - y_k)^2} \quad (4)$$

If the distance between different fireworks is less than the threshold R of the movement range, fireworks individuals with larger abscissa are excluded. The calculation of threshold R is Eq. (5).

$$R = MIN\left\{\left((x_1)_{\max} - (x_1)_{\min}\right), \left((x_2)_{\max} - (x_2)_{\min}\right), \ldots, \left((x_k)_{\max} - (x_k)_{\min}\right)\right\} / N \quad (5)$$

Eq. (5) represents the minimum horizontal coordinate distance $\frac{1}{N}$ in dimension k. When all fireworks individuals are evenly distributed in the solution space, it indicates the minimum value of their force position to ensure uniform distribution. When the distance between individuals is less than the threshold, it indicates that the distribution between individuals is too close. When the number of individuals that meet the requirements is less than N, continuous screening is required until the number reaches the standard, as shown in Fig. 2.

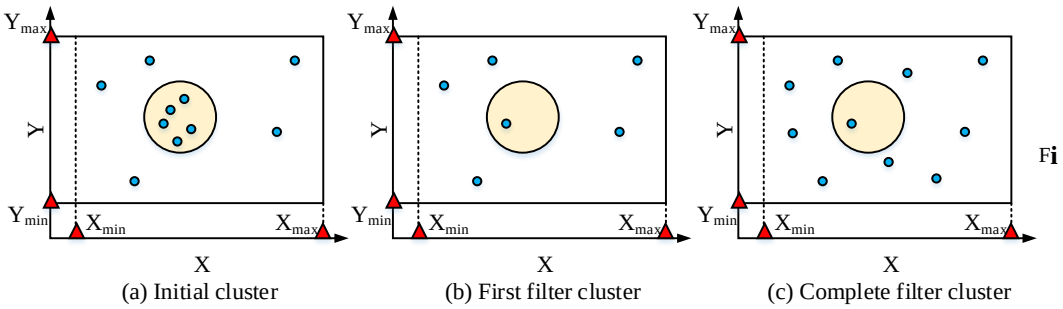


Fig. 2. Initial cluster dispersion strategy.

Fig. 2 shows the dispersion process of the initial cluster in two-dimensional space. Among them, the dashed box represents the searchable space. The fireworks individuals in the yellow circle indicate those who are too concentrated and excluded. In Fig. 2 (a), there are five individuals in the initial cluster that do not meet the dispersion requirements, and this initial cluster is prone to falling into local optima. After excluding overly concentrated individuals and achieving a more uniform distribution of the cluster, continuing to select and screen the remaining fireworks individuals, meeting the requirements for the initial number and uniformity of clusters. The traditional algorithm chooses the classic roulette wheel strategy and uses Euclidean distance to achieve individual screening, as expressed as Eq. (6).

$$P_i = \frac{\sum_{j \in K} D_{ij}}{\sum_{i \in K} \sum_{j \in K} D_{ij}} \tag{6}$$

In Eq. (6), P_i is the probability that individual i is selected. D_{ij} represents the Euclidean distance between individuals i / j. Although the above strategies can maintain cluster diversity, the high computational complexity can affect the final convergence performance of the algorithm. Therefore, this study directly screened individuals by comparing fitness values, as shown in Eq. (7) [16].

$$\Delta f(x) = \alpha\left(f(x_i) - f(x_j)\right) \tag{7}$$

In Eq. (7), $\Delta f(x)$ represents the difference in fitness between two individuals. $f(x_i) / f(x_j)$ is the fitness evaluation function for different individuals. $\Delta f(x)$ needs to be less than the β constant, and α is the screening parameter that caters to β. The overall optimized FWA process is Fig. 3.

In Fig. 3, the treatment of inferior fireworks is to ensure population diversity. Therefore, by increasing the amplitude of its fireworks explosion, it can be added to the population, as shown in Eq. (8).

$$R_i = R\frac{f(x_i) - f_{\min} + \delta}{\sum_{i=1}^{N}\left(f(x_i) - f_{\min}\right) + \delta} \tag{8}$$

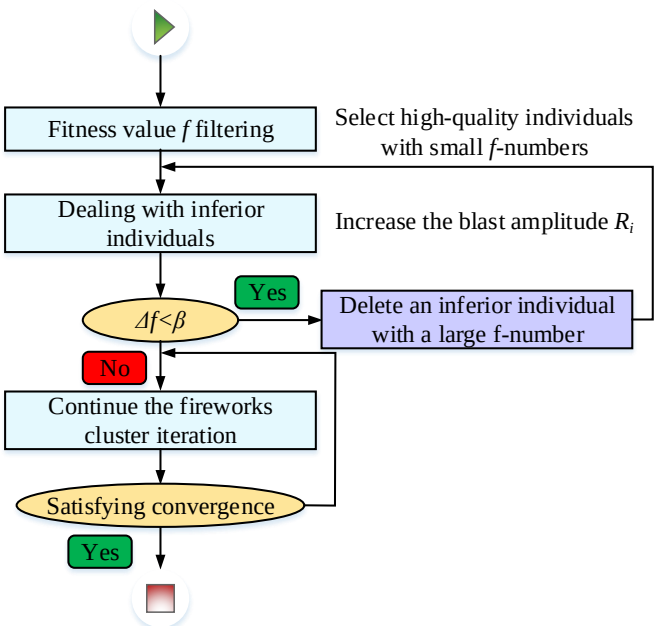


Fig. 3. Operation of optimized FWA.

In Eq. (8), R_i represents the explosion amplitude of individual x_i. After optimizing the low-quality algorithm, the fitness difference is judged and whether it will enter the next generation of individual updates is determined.

B. Design of FWA Intrusion Detection Model Based on Feature Analysis

After optimizing the performance of FWA, it is necessary to update and map the solution space. This is because the feasible domain of the traditional solution space is continuous, while intrusion detection requires discrete feature selection. Therefore, this study maps the feature extraction solution to the corresponding fireworks cluster and re encodes its position vector. In the model, individual fireworks and their sparks are possible features of themselves, and their position vector X_i is Eq. (9).

$$X_i = \left\{ x_{i1}, x_{i2}, ..., x_{ij}, ..., x_{in} \right\} \tag{9}$$

In Eq. (9), x_{i1} represents whether the first feature is selected in the subset. n is the total quantity of features. The features processed by binary discretization are shown in Eq. (10) [17-18].

$$x_{ij} = \begin{cases} 0 & rand < 0.5 \\ 1 & others \end{cases} \tag{10}$$

In Eq. (10), $0/1$ represents the corresponding features unselected and selected, respectively, which are uniformly distributed random values in the [0, 1] interval. When there are multiple features in the feature subset, the final encoding form is Fig. 4.

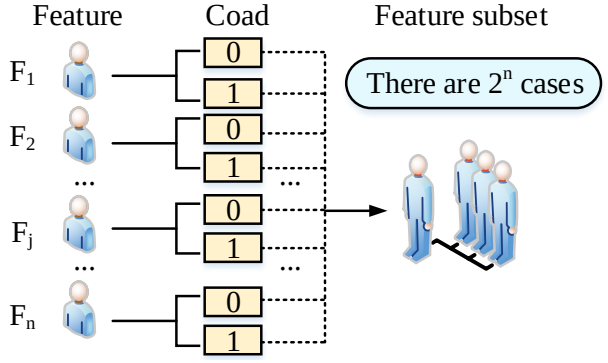


Fig. 4. Binary discrete coding.

Next, the decoding step should be performed to collect the features encoded as "1", obtain the optimal feature subset, and input it into the model for testing and training. To match the search for the optimal feature subset, this study will initialize the fireworks and feature subset one-to-one mapping. The initial position vector length of its individual is the same as the number of elements n in the original feature subset. Next, to define the fitness function as expressed in Eq. (11).

$$f\left(X_i\right) = \begin{cases} -acc & sum\left(x_i\right) \neq 0 \\ 0 & sum\left(x_i\right) = 0 \end{cases} \tag{11}$$

Eq. (11) reflects the accuracy of classification. When the fitness value is higher, the classification accuracy is poor, and the corresponding individual quality is poor. Conversely, the quality of fireworks individuals is better. Among them, acc represents the classification accuracy, as shown in Eq. (12).

$$acc = \frac{Num\_correct\_pre}{Total\_num\_pre} \tag{12}$$

In Eq. (12), $Num\_correct\_pre / Total\_num\_pre$ represents the correct number of predicted samples and the total number of predicted samples. Next, this study introduces the K-nearest neighbor algorithm for data classification. The K value is related to classification accuracy. If it is too small, noise interference may occur, and vice versa, it will increase its computational pressure. If it is an even value, it is easy to encounter problems with the same quantity. In addition, this study introduces K-fold cross validation, which divides the dataset into K subsets for accuracy ten fold cross validation, as shown in Fig. 5.

In Fig. 5, the dataset needs to be evenly divided into ten parts, and one subset should be continuously selected as the test set and the remaining as the training set in order. Finally, 10 test results can be obtained and calculated for arithmetic mean. This result serves as an evaluation indicator for the accuracy of the algorithm. Generally speaking, N repeated trials are required, and the mean of N trials is taken as the final accuracy measurement result. Subsequently, the FWA optimization model based on feature analysis is applied to intrusion detection. Unlike intrusion detection models based on anomaly analysis, research models directly compare input values with illegal operations to determine whether they belong to intrusion behavior. Therefore, the model needs to analyze all attack behaviors first. Compared with the analysis model for legitimate behavior, this greatly reduces computational complexity, but at the same time, it also lacks the timeliness of monitoring new intrusion behaviors. Common attack behavior detection algorithms include conditional probability, state transition analysis, and rule feature analysis. The conditional probability strategy is efficient, but computationally complex. The state transition analysis strategy is more suitable for long-term attack behavior, but its accuracy needs to be improved. The rule feature analysis detection strategy has high accuracy and strong timeliness, but can only achieve static recognition. Due to the fact that intrusion detection models do not require dynamic recognition, a rule feature analysis detection strategy was chosen in this study. The overall optimized FWA model is Fig. 6.

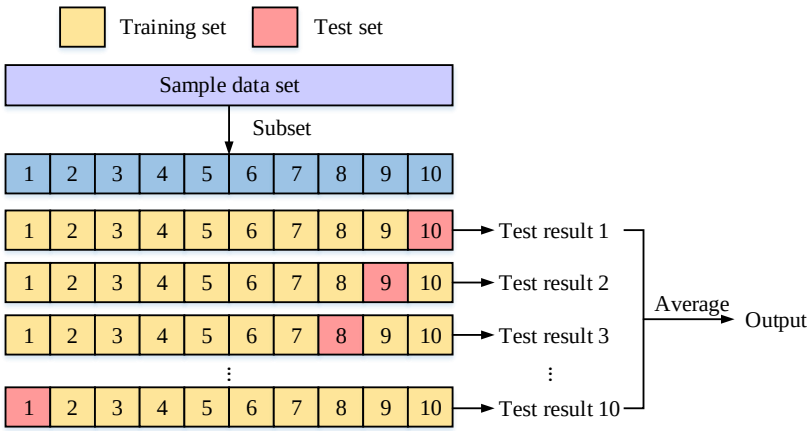


Fig. 5. K-fold cross-validation process.

In Fig. 6, the main modules of the model are the preprocessing module and the learner module. Firstly, it is necessary to preprocess the data and perform numerical normalization and dimensionality reduction operations. Data dimensionality reduction refers to parameter initialization, cross validation of fitness values, and continuous iteration until the requirements are met. Next, the obtained optimal feature subset is input into the learner module, and after spark generation and iteration, it is determined whether it meets the convergence condition. Finally, returning to the best self and obtaining the intrusion detection model. Afterwards, the test dataset can be input into the model, and after feature filtering and detector structure, the final detection result can be obtained.

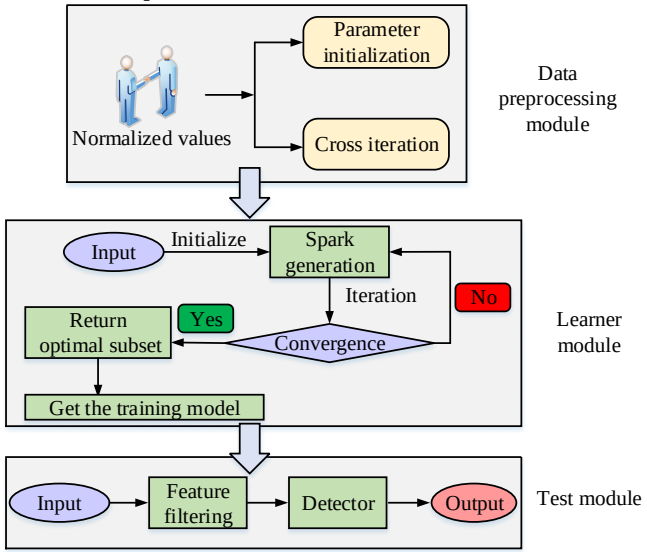


Fig. 6. Optimized FWA model.

IV. Analysis of NID Recognition Performance of FWA Optimization Algorithm

To verify the effectiveness of the research method in NID, this study first validates the overall attack behavior recognition performance of the model, including computation time and accuracy. Subsequently, specific attack behaviors are classified and detected, and compared with other algorithms in multiple datasets.

A. Performance Analysis of Training and Detection Accuracy for Optimizing FWA Models

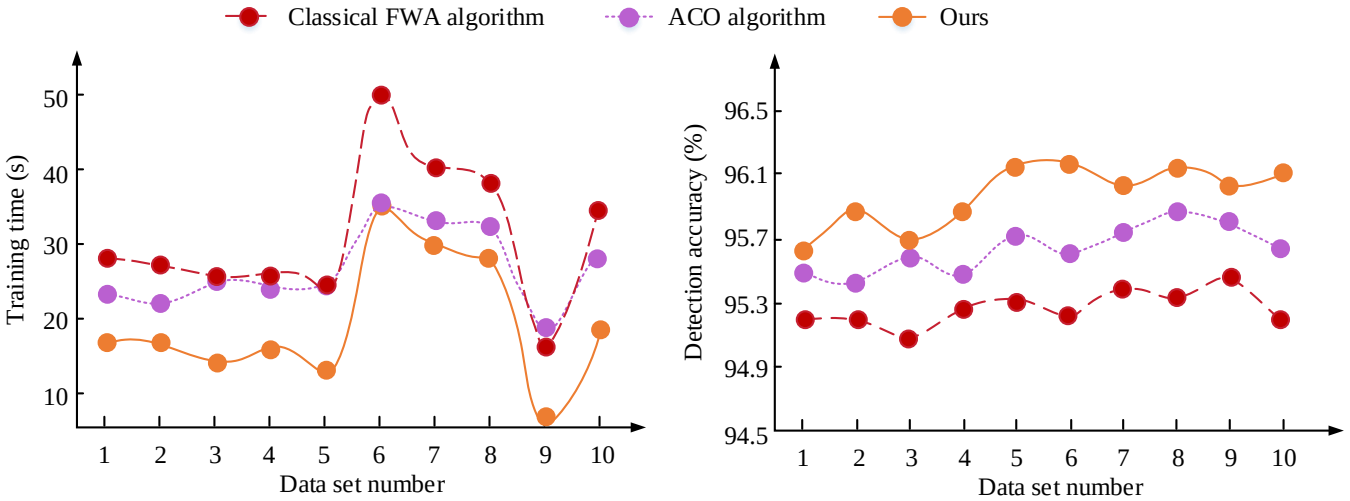
This study first analyzes the training and testing performance of the model. Table II shows the related parameters and environment.

TABLE II. Experimental Environment and Parameter Selection Settings

Name	Settings
Operating system	Win10
Processor	Inter (R) Core (TM) i5-4590CPU@3.30GHz 3.30GHz
Simulation platform	MATLAB R2019a
Number of initial fireworks clusters N	5
Spark-limiting parameter	50
Constant α	0.04
Constant β	0.8
Maximum iterations	200
Data sets	KDD CUP99
	NSL-KDD
Training: Verification	7:3

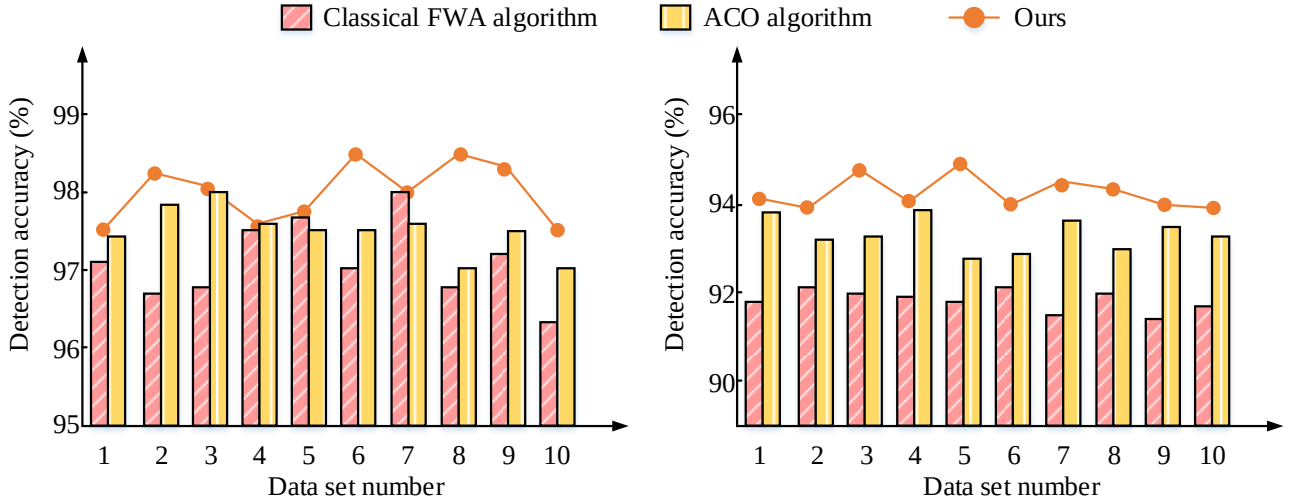
In Table II, the NSL-KDD is a derivative dataset of KDD CUP99, which incorporates some novel intrusion data. This study first used 10% randomly selected from KDD CUP99 as the test dataset. According to the above extraction method, a total of 10 subsets of test data are formed. This study designs a model for comparison with traditional FWA and similar swarm intelligence-based Ant Colony Optimization (ACO). The results are displayed in Fig. 7.

Fig. 7 (a) compares the training time, which trends of the three models are the same. The training time of the first five sub datasets fluctuates relatively smoothly, with a significant increase in training time in the 6-8 sub datasets, followed by a significant decrease. This may be related to information such as feature quantities of different data in the sub dataset. Among them, the training time of the research model is greatly lower than that of the other models, with an average training time of 22.46 seconds. The average training time for traditional FWA and ACO is 38.81 seconds and 29.57 seconds, respectively. Therefore, the training time of the research model decreased by 36.2% compared to other models. This is because strategies such as studying the fitness screening mechanism of the model have reduced the computational burden of the model, while other models have not made improvements in computational complexity. Fig. 7 (b) shows the accuracy comparison of various models in different sub datasets. Compared to the training duration, its accuracy fluctuates less. The average detection accuracy of the research model is 96.02%, which is a relative improvement of 0.76% in recognition accuracy compared to the 95.01% and 95.52% accuracy of traditional FWA and ACO algorithms. This is because classical FWA is prone to falling into local optima, while ACO also experiences a stagnation phenomenon where all solutions are the same due to the increase in iteration times and limited search space. This study conducts a comparative analysis to further validate the recognition accuracy of various models on large-scale datasets and under the introduction of unknown attacks. The results are shown in Fig. 8.



(a) Algorithm time comparison (b) Algorithm precision comparison

Fig. 7. Training and test performance of each model.



(a) Large data sets (b) Unknown attacks

Fig. 8. Comparison of model performance under different data scenarios.

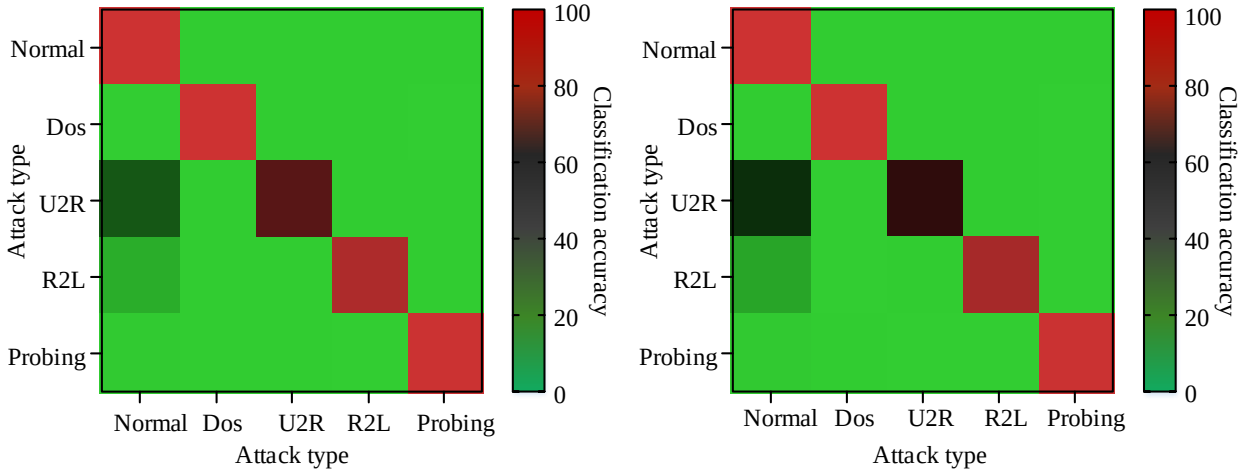
The dataset used in Fig. 8 (a) is twice as large as the dataset in Fig. 7, and for more data information, the recognition accuracy of each model has significantly improved, with mean values above 96%. However, the recognition accuracy of the research model in large volume datasets has shown a more significant improvement compared to in small volume datasets. For example, in sub dataset 8, there are many features in the data, making it difficult for classical FWA to handle such high-dimensional data, with a recognition accuracy of 96.72%. In sub-dataset 10, the data features are relatively fuzzy, so the recognition accuracy of each model has decreased. Overall, the average detection accuracy of the research model in big datasets is 98.21%, which is an increase of 3.53% compared to the other two models. In Fig. 8 (b), each model faces unknown attack data and the recognition accuracy decreases. The average detection accuracy of the research model is 94.16%, which is an increase of 2.47% compared to the other two models. In summary, the research model has stronger adaptability and stability in detecting larger amounts of data. It is also more oriented towards detecting unknown attacks.

B. The Recognition and Classification Performance of Models on Attack Behavior Under Different Datasets

The above experiment verifies the overall intrusion detection performance, and in practical applications, it is necessary to classify different types of attacks for targeted repair in the future. The common types of attacks include Denial of Service (DoS), Root (U2R), Remote to Local (R2L), and Probing. The classification performance of the optimized FWA model designed in this study for different data types is Fig. 9.

Fig. 9 (a) shows the classification performance in the KDD CUP99. The classification accuracy of the model for normal behavior, DoS, and Probing attack behavior is over 99%, with an average of 99.73%. However, the classification accuracy for U2R and R2L attack behaviors is poor, at 75.43% and 95.36%, respectively. This is because these two types of attacks have higher discreteness and similarity to normal behavior. In the NSL-KDD, the classification accuracy of the research model for normal behavior, DoS, and Probing remains above 99%. The confusion rate between normal behavior and U2R reaches 38.56%, and the confusion rate with R2L is 9.59%. In summary, the research model can effectively achieve intrusion type classification. This study further conducts experiments on the DARPA1988 and ISCX2012 datasets. Among them, the distribution of DARPA1988 is seven weeks of training traffic and two weeks of testing traffic, and the attack type is the same as described above. The distribution of ISCX2012 is one week of traffic data, and the attack types are divided into four types: Brute Force SSH (BFSSH), DDoS, Infiltrating, and HttpDoS. Fig. 10 shows the comparison.

Fig. 10 (a) analyzes the accuracy and detection rate (DR) of the model in ISCX2012. The recognition accuracy for different types of attacks is above 99%, with an average of 99.69%. The DR value has a recognition rate of 93.12% for DDoS attack types, and a detection rate of over 95% for other attack types. This is because DDoS is easily confused with Infiltrating attack behavior. Fig. 10 (b) shows the performance of the model in DARPA1988, which also lacks detection of U2R and R2L attack behaviors. Although the recognition accuracy is above 99%, the detection rates are 83.35% and 74.19% respectively, and the overall recognition rate is 97.78%. Fig. 10 (c) shows the FAR of the model. In the ISCX2012 model, the total FAR value is 0.07%, while in DARPA1988, the total FAR value is 0.22%. Next, this study introduces the Dynamic Convergence Method (DCM) model proposed by Ahmed et al. and the Broad Learning System (BLS) model proposed by Liu et al. for further comparative analysis. Table III shows the specific results.



(a) KDD CUP99 (b) NSL-KDD

Fig. 9. Classification accuracy under different data sets.

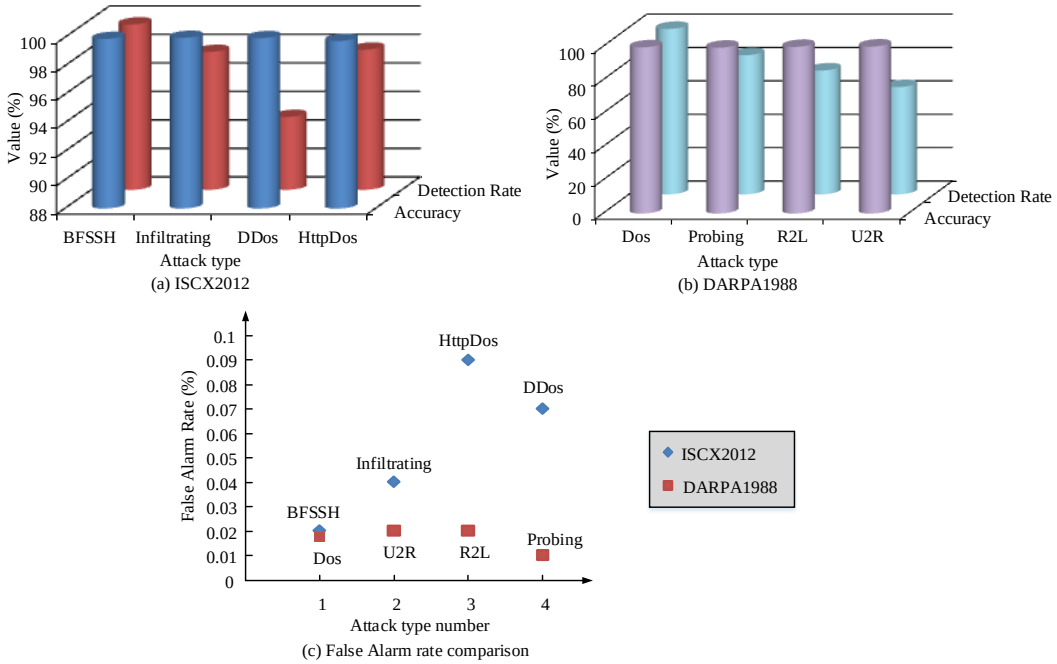


Fig. 10. Model performance analysis under different data sets.

TABLE III. COMPARISON OF MODEL PERFORMANCE UNDER DIFFERENT DATA SETS

Data set	Index	DCM	BLS	Ours
DARPA1988	DR (%)	96.63	95.42	97.78
	FAR (%)	0.07	0.05	0.07
	ACC (%)	99.24	99.98	99.68
ISCX2012	DR (%)	92.81	95.75	96.91
	FAR (%)	0.31	0.29	0.22
	ACC (%)	97.56	97.24	99.69
KDD CUP99	DR (%)	98.65	98.97	98.52
	FAR (%)	0.26	0.20	0.15
	ACC (%)	98.54	98.99	99.04
NSL-KDD	DR (%)	95.31	95.87	97.52
	FAR (%)	0.40	0.31	0.26
	ACC (%)	96.48	97.22	98.04

In Table III, the comprehensive performance of the research model is the best in different datasets. In DARPA1988, the DR index of the designed model is relatively 1.54% higher, but slightly lower than the BLS model by 0.02% in FAR index and slightly lower than the BLS model by 0.3% in ACC index. In the remaining datasets, the performance of various indicators of the research model has always been superior to the other models. Its average accuracy is 99.06%, which is relatively higher than the other models by 1.78%. The average detection rate is 96.98%, which is relatively higher than the other models by 2.57%. The mean FAR is 0.13%, which is lower than the other models by 1.60%. Therefore, studying models can better achieve network intrusion behavior detection and maintain network security.

V. RESULTS AND DISCUSSION

The proposed network intrusion detection model was tested on several standard datasets, including KDD CUP99, NSL-KDD, DARPA1988, and ISCX2012. On the KDD CUP99 dataset, the model's classification accuracy for normal behavior, DoS and Probing attack types exceeded 99%, with an average of 99.73%. However, the classification accuracy for U2R and R2L attack types is relatively low, at 75.43% and 95.36%, respectively. This may be due to the high similarity between these attack types and normal behavior, causing the model to have difficulty distinguishing between them. On the NSL-KDD dataset, the accuracy of the model classification of normal behavior, DoS and Probing remained above 99%. The experimental results show that the proposed method has high accuracy and stability in network intrusion detection. In particular, when dealing with large data sets and unknown attacks, the model can quickly adapt to new security threats, reducing the need for computing resources. In addition, the model has a slightly lower false positive rate on the DARPA1988 dataset than the BLS model, but a slightly lower accuracy rate. This suggests that there is room for improvement in the generalization ability of the model and the ability to identify unknown attacks. Future work could consider introducing more machine learning techniques, such as ensemble learning or deep learning, to improve the overall performance of the model.

VI. Conclusion

This study designed an optimized intrusion detection model on the basis of FWA to address the frequent occurrence of network security issues. By optimizing the initial individual distribution and updating fitness values, the recognition performance of the model was enhanced. Finally, it was combined with intrusion detection to achieve the recognition and classification of attack behavior. This study first conducted experimental analysis on the training and testing performance. Compared to traditional FWA models, the training time of the research model has decreased by 36.2%, and the recognition accuracy has relatively improved by 0.76%. In large-scale datasets, the detection accuracy of the research model was 98.21%, which was 3.53% higher than other models. Under the influence of unknown attacks, the detection accuracy of the research model was 94.16%, an increase of 2.47%. In specific attack behavior classification, the model had a classification accuracy of over 99% for DoS and Probing, with an average of 99.73%. But the classification accuracy for U2R and R2L was poor, at 75.43% and 95.36%, respectively. The research model was only available in the DARPA1988 dataset, with FAR slightly lower than the BLS model by 0.02% and ACC slightly lower than the BLS model by 0.3%. But in the remaining datasets, the research models performed the best. The average accuracy was 99.06%, and the average detection rate was 96.98%, which was relatively higher than the other models by 1.78% and 2.57%, respectively. The mean FAR was 0.13%, which was lower than the other models by 1.60%. In summary, the research model can better achieve network intrusion behavior detection and maintain network security. With the increasing complexity of network environment, the integration of multiple data sources for intrusion detection will become an important research direction. In the future, we can explore how to effectively integrate network traffic, system logs, user behavior and other data to improve the accuracy and robustness of detection, and at the same time, we can also work on developing intelligent detection systems that can self-evolve and update.

References

[1] Jiang W, Yang Z, Zhou Z, J Chen. Lightweight data security protection method for ami in power internet of things. *Mathematical Problems in Engineering*, 2020, 1(5):8896783-8896792.

[2] Vanitha V, Vallimurugan E. A hybrid approach for optimal energy management system of internet of things enabled residential buildings in smart grid. *International journal of energy research*, 2022, 46(9): 12530-12548.

[3] Zhou Z, Xiang Y, Xu H, Y Wang , D Shi. Unsupervised Learning for Non-intrusive Load Monitoring in Smart Grid Based on Spiking Deep Neural Network. *Journal of Modern Power Systems and Clean Energy*, 2022, 10(003): 606-616.

[4] Gothawal DB, Nagaraj SV. An intelligent and lightweight intrusion detection mechanism for RPL routing attacks by applying automata model. *Information Security Journal: A Global Perspective*, 2023, 32(1): 1971803-1971823.

[5] U Ahmed, CW Lin, G Srivastava, U Yun, AK Singh. Deep active learning intrusion detection and load balancing in software-defined vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 24(1): 953-961.

[6] Yaodi Liu, Kun Zhang, Zhendong Wang. Intrusion detection of manifold regularized broad learning system based on LU decomposition. *Journal of supercomputing*, 2023, 79(18): 20600-20648.

[7] S Subramani, M Selvi. Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks. *Optik*, 2023, 273(1):170419-170424.

[8] S Ma, Y Li, L Du, J Wu, Y Zhou, Y Zhang, et al. Programmable intrusion detection for distributed energy resources in cyber–physical networked microgrids. *Applied Energy*, 2022, 306(1):118056-118056.

[9] Vitorino J, Oliveira N, Praça I. Adaptative perturbation patterns: realistic adversarial learning for robust intrusion detection. *Future Internet*, 2022, 14(4): 108-108.

[10] Pande S, Khamparia A, Gupta D. An intrusion detection system for health-care system using machine and deep learning. *World Journal of Engineering*, 2021, 19(2): 166-174.

[11] Thakkar A, Lohiya R. Analyzing fusion of regularization techniques in the deep learning-based intrusion detection system. *International Journal of Intelligent Systems*, 2021, 36(12): 7340-7388.

[12] Alshammri GH, Samha AK, Hemdan EED, M Amoon, W El-Shafai. An efficient intrusion detection framework in software-defined networking for cybersecurity applications. CMC-Comput. *Mater. Contin*, 2022, 8(72): 3529-3548.

[13] Makani R, Reddy BVR. Trust-based-tuning of Bayesian-watchdog intrusion detection for fast and improved detection of black hole attacks in mobile ad hoc networks. *International journal of advanced intelligence paradigms*, 2022, 21(1): 53-71.

[14] Liu H, Han H, Sun Y, G Shi , M Su , Z Liu , H Wang , X Deng. Short-term wind power interval prediction method using VMD-RFG and Att-GRU. *Energy*, 2022, 251(3): 123807-123807.

[15] Pradhan A, Senapati MR, Sahu PK. A multichannel embedding and arithmetic optimized stacked Bi-GRU model with semantic attention to detect emotion over text data. *Applied Intelligence: The International Journal of Artificial Intelligence, Neural Networks, and Complex Problem-Solving Technologies*, 2023, 53(7): 7647-7644

[16] Shreenidhi HS, Ramaiah NS. A two-stage deep convolutional model for demand response energy management system in IoT-enabled smart grid. *Sustainable Energy, Grids and Networks*, 2022, 1(30): 100630-100630.

[17] Nedeljkovic D, Jakovljevic Z. CNN based method for the development of cyber-attacks detection algorithms in industrial control systems. *Computers & Security*, 2022, 144(1): 102585-102602.

[18] Choudhuri S, Adeniye S, Sen A. Distribution Alignment Using Complement Entropy Objective and Adaptive Consensus-Based Label Refinement for Partial Domain Adaptation. *Artificial Intelligence and Applications*. 2023, 1(1): 43-51.