ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20240524001658
Original scientific paper

Anomalous Network Traffic Detection: An Application of Deep Learning Algorithms

Liming LIN*, Ang XIA, Fangfang DANG, Qin YIN, Xirong LV

Abstract: With the development of the electric power system, the safety of electric power industrial control network is increasingly prominent. Abnormal traffic detection is one of the important tasks in network security. To detect anomalous traffic quickly and accurately, the sine-cosine function and Levy flight are introduced into the locust algorithm to optimize its reduction factors. The improved locust algorithm is used to optimize the parameters of the anomalous network traffic model built on the basis of long short-term memory networks. Meanwhile, the optimized model is applied to the electric power industrial control system. The results showed that the accuracy of both the test and training sets was above 90%, proving that the designed model achieved good generalization capability and robustness. In the Dos attack type, the detection rate of the designed model reaches 98.15%, which is about 6% and 10% higher than that of other algorithms, which proves its high accuracy. These results prove the high efficiency and accuracy of the designed model in detecting network traffic attacks. The above results prove that the designed model can effectively identify anomalous flow and contribute to maintaining the safety of the power grid.

Keywords: abnormal network traffic detection; grasshopper optimization algorithm; levy flight; long short-term memory networks; reduction factor

1 INTRODUCTION

As the boost of information technology and the advancement of industrial automation, the power industry control network poses an essential influence on the Power System (PS) [1]. However, the power industry control network also suffers from the increasing network security threats, such as network attacks, malicious software, and data leakage. These challenges not only have a serious impact on the operational stability and reliability of the PS, but also lead to damage to power equipment and data loss. Therefore, the detection of abnormal power industrial control network traffic becomes crucial. In the field of power industrial control networks, traditional methods for detecting abnormal traffic include Bayesian belief networks, Naive Bayes classifiers, Support Vector Machines, k-nearest neighbor algorithms, etc. However, power industrial control networks have a large amount of data, and as the data volume increases, these traditional methods often reduce performance and scalability. So, it is necessary to explore a detection method that performs better in the face of large-scale data and can adapt to different attack scenarios [2]. As the boost of Deep Learning (DL) algorithms, the application of these methods in abnormal power industrial control Network Traffic Detection (NTD) gradually receives attention. The DL algorithm, as a machine learning method based on artificial neural networks, has strong feature extraction and pattern recognition capability. In the detection of abnormal power industrial control network traffic, the DL algorithm can automatically graph representative features by learning a large amount of power network traffic data and identify normal and abnormal traffic through training models. DL algorithms can help achieve real-time monitoring and timely response to abnormal network traffic in the power industry control network, which improves the security and reliability of PS [3, 4]. Therefore, the application of DL algorithms in abnormal power industrial control NTD has important significance and development potential. In view of this, this study first designed an abnormal NTD model based on Long Short-Term Memory (LSTM). Meanwhile, the reduction factors of Grasshopper Optimization Algorithm (GOA) were optimized through sine cosine function and Levy flight. Then, the optimized GOA was utilized for optimizing the parameters of LSTM for improving the performance of the abnormal NTD model. This model can more accurately detect unknown attack behaviors and improve the security and reliability of PS compared to the traditional detection methods.

The innovation of this article lies in the first combination of the improved Grasshopper Optimization Algorithm (GOA) and Long Short Term Memory Network (LSTM) for anomaly detection of traffic in power industrial control networks. Through innovative optimization of GOA reduction factors using sine and cosine functions and Levy flight strategy, the accuracy and efficiency of LSTM parameter adjustment are effectively improved.

The contribution of this article lies in the selection of important features through a hybrid feature selection method, building an LSTM neural network as an anomaly detection model, and introducing an improved GOA algorithm to optimize the hyperparameters of the LSTM neural network. The design method can quickly detect various attacks in the network, thereby better perceiving the current network security situation and improving the security and reliability of the network.

2 RELATED WORKS

Abnormal NTD is an essential network security issue. Traditional detection methods are usually based on rules and statistical analysis. Recently, DL algorithms achieve significant results in some aspects, so many researchers begin to apply them to abnormal NTD. Dong S. et al. designed an optimization method for abnormal traffic detection based on semi-supervised dual depth Q network to improve the speed of data annotation during abnormal traffic detection. An automatic encoder was used for reconstructing traffic characteristics and a deep neural network was utilized as a classifier. The results indicated that this method had certain advantages in terms of time complexity [5]. Chen M. and other scholars designed a network traffic classification model based on metric learning for enhancing the network traffic classification.

This model integrated metric learning into convolutional neural networks and mapped traffic samples of different networks separately. The results showed that the model performed well in both network traffic classification and open set [6]. Researchers such as Alshammari A. designed a machine learning-based intrusion detection system for detecting malicious network traffic. This system extracted various attack features for training machine learning models through it. The results showed that the system improved the quality of malicious detection of network traffic [7]. Cvitić I. et al. designed a distributed denial of service traffic detection method based on a conceptual network model to detect abnormal network traffic generated by IoT devices. This method detected illegal network traffic through conceptual networks based on IoT devices. The results indicated that the calculation ability of this method was good [8]. Scholars such as Xiao F designed an abnormal tolerant network traffic estimation method based on a noise immune time matrix complete model to apply NTD methods to complex noise distributions. This method utilized the inherent low rank and time characteristics of the traffic matrix for simultaneously estimating network traffic and detecting network anomalies. The outcomes showcased that this method outperformed other methods [9]. Phan T. V. researchers designed a fine-grained deep reinforcement learning network to achieve efficient abnormal NTD. It learned a traffic strategy that maximized traffic granularity through a dual deep Q network, while actively protecting the network data plane from overload. The outcomes showcased that the network markedly enhanced the network attack detection [10].

Song H. M. et al. designed a network self-supervised abnormal detection method using noisy-pseudo normal data to solve the problem that most supervised learning relied on training datasets. This method consisted of two DL models, which were used to generate noisy-pseudo normal data and detect anomalies, respectively. The outcomes showcased that the detection accuracy of this method was significantly enhanced [11]. Scholars such as Ma W. designed an abnormal traffic detection method based on generative adversarial networks and feature optimization selection to enhance the NTD. This method utilized information between generative adversarial network adversarial training and classification network supervised training to learn shared feature distributions. The results indicated that the method had high robustness [12]. Researchers such as Dandil E. designed a hybrid network traffic abnormal detection model based on artificial immune algorithms to accurately detect and prevent abnormal changes in network traffic. This model detected abnormal network traffic data by monitoring changes in the activated detectors. The outcomes showcased that the classification accuracy of this method was high [13]. Duan L. et al. designed an NTD method based on self-coding and decision trees to detect and control botnets. This method utilized an automatic encoding neural network for feature selection. The results indicated that this method had good botnet detection performance [14]. Xia B. and other researchers designed an abnormal traffic classification model based on ResNet and Inception convolutional neural networks to protect the security of cloud computing and outsourced data. This model learned more traffic features through Inception units and eliminated network degradation through the direct mapping of unit ResNet. The outcomes showcased that the model had a high recognition rate [15]. Yang J. and other scholars designed an encrypted network malicious traffic detection model based on DL and reinforcement learning to accurately capture malicious traffic in network traffic. This model automatically extracted malicious traffic from encrypted networks and distinguished between normal and abnormal encrypted network traffic. The outcomes illustrated that the accuracy of this method was high [16]. Nguyen H. C. et al. designed an attack detection algorithm based on multi-layer perceptron, inference, and graph convolutional network to improve the detection accuracy of advanced persistent threat abnormal traffic in the network. It combines various data mining techniques to calculate the relationship and correlation between advanced persistent threat attack behaviors in the network. The results show that the algorithm reduces false positives to the maximum efficiency [17]. Shi G. and other scholars have designed a deep anomaly network traffic detection model to address the real-time changes in actual industrial control networks. The model utilizes deep convolutional autoencoders to extract effective high-order features and employs generative adversarial networks as a data augmentation strategy to enrich anomaly data. The results show that the model can effectively ensure the security of the network [18]. Fortino G. et al. designed a detection method based on labeled time point processes and neural networks to more accurately identify threats in industrial control networks. The method uses deep learning theory to improve the ability to learn arbitrary and unknown event distributions, and the results show that the method has high accuracy and recall rate [19].

In summary, the application of DL algorithms in abnormal power industrial control NTD has potential. However, these DL algorithms still face some challenges in practical application, some methods require a long training time, the detection process is also complex, some methods are prone to overfitting, classification accuracy is low, and some methods have limited effect in complex industrial control system environment, and need to consume a lot of computing resources when processing large sample data sets. Therefore, based on the characteristic of LSTM neural network being able to handle sequence data well, an abnormal network traffic model was constructed on the basis of LSTM. At the same time, an improved GOA algorithm was used to optimize the parameters of the model to improve the performance and efficiency of abnormal network traffic detection, thereby achieving effective detection of abnormal traffic.

3 RESEARCH METHODS

In the abnormal NTD of power industry control, two key issues have received much attention, namely processing high-dimensional and multi-feature network traffic data and constructing efficient detection models. Network traffic often has certain temporal and correlation. In the network, traffic is influenced by factors such as data transmission, user behavior, and application activity

during the previous time period. Therefore, this study chooses a recurrent neural network LSTM suitable for processing temporal data for detecting abnormal network traffic. At the same time, since the neural network is largely affected by its hyperparameters in the training process, in order to solve the problem of neural network hyperparameter combination, the GOA algorithm is used to optimize the LSTM neural network's hyperparameters, improve the training efficiency of the neural network, improve the accuracy of the anomaly detection model and other indicators, so as to realize the effective detection of abnormal traffic.

3.1 Construction of Abnormal NTD Model Based on LSTM

Due to the large scale of network traffic, there may be some redundant features in its original feature set, which will consume resources and reduce the efficiency during training. Therefore, feature selection is necessary for network traffic data. Extra Tree (ET), XGBoost, and Pearson Correlation Coefficient (Pcc) are combined into a hybrid feature selection algorithm in this study to reduce error in feature selection and make the resulting feature evaluation more objective. The algorithm is shown in Fig. 1.

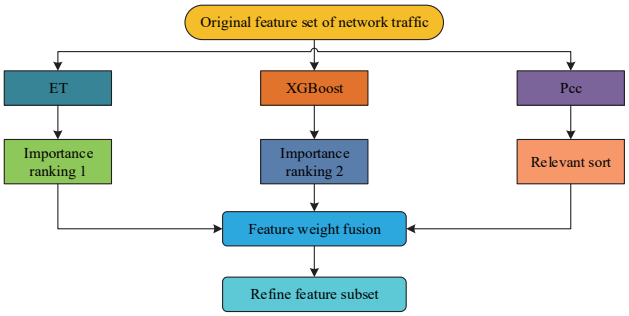

Figure 1 Hybrid feature selection algorithm

First, ET and XGBoost are used to score the importance of the original characteristics of network traffic, and their weights are calculated in the two feature selection algorithms. Meanwhile, Pcc is used to calculate the correlation coefficient between the original features of network traffic and category labels. The magnitude of this coefficient reflects the correlation between the features and subsequent detection results. Then, the correlation coefficients are ranked to obtain the third importance weight. Finally, the three feature weights are fused to obtain the final mixed feature weights. The calculation is demonstrated in Eq. (1).

$$\begin{cases} \omega_e = \sum_{i=1}^{k}[\frac{n}{N}(1-\sum_{y}^{Y}P_{ny})^2 - \frac{n_{sl}}{N}(1-\sum_{Y}^{y}P_{ny})^2 - \frac{n_{sr}}{N}(1-\sum_{Y}^{y}P_{ny})^2] \\ \omega_x = \frac{1}{2}[\frac{G^2_{j\in L_1}}{H_{j\in L_1}+\lambda} + \frac{G^2_{j\in L_2}}{H_{j\in L_2}+\lambda} - \frac{G^2_{j\in L}}{H_{j\in L}+\lambda}] - \gamma \\ \omega_p = \frac{E(XY)-E(X)E(Y)}{\sqrt{E(X^2)-E^2(X)}\sqrt{E(Y^2)-E^2(Y)}} \\ \omega = \omega_e + \omega_x + \omega_p \end{cases} \quad (1)$$

In Eq. (1), ω_e serves as the importance score of ET. ω_x represents the importance score of XGBoost. ω_p serves as the importance score of Pcc. n represents the n-th node of the extremely random tree. N serves as the total quantity of samples. y represents the category. Y represents the total categories. P_{ny} represents the proportion of category y in node n. n_{sl} serves as the quantity of samples on the left side of the current node. n_{sr} serves as the quantity of samples on the right side of the current node. G_j serves as the accumulation of the first-order partial derivatives of all samples at node j in XGBoost. H_j represents the accumulation of second-order partial derivatives of all samples at node j. L_2 represents the quantity of left nodes after the dataset is split. L_1 represents the quantity of right nodes after the dataset is split. L serves as the total nodes in the dataset. λ serves as the penalty coefficient. γ represents the control factor for the number of nodes. E represents the expectation of Pcc. X represents a feature [20]. The next step is for constructing an abnormal NTD model. The obtained features with higher mixed weight values are used as input values. The LSTM training network traffic characteristics are shown in Fig. 2.

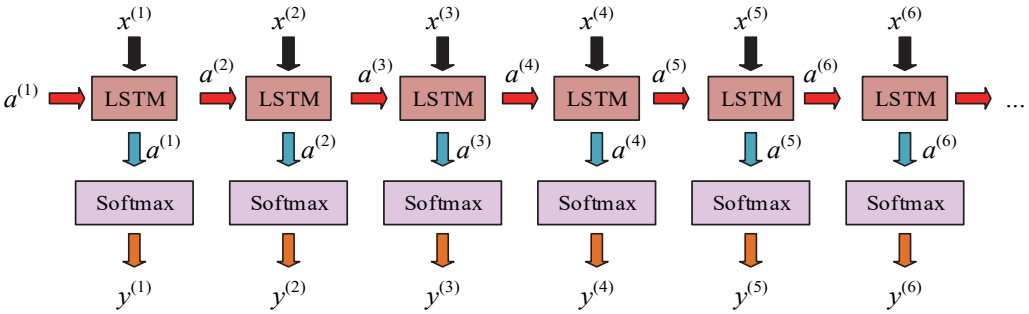

Figure 2 Training process of network traffic characteristics

In Fig. 2, the LSTM neural network consists of multiple feedforward neural networks. The feedforward neural network networks at different times transmit dependency relationships through hidden layer neurons. Each layer of feedforward neural network is divided into three layers, namely the input layer containing 12 neuron nodes, the hidden layer containing 64 neuron nodes, and the output layer containing 12 neurons. Because of the possibility of overfitting during the training process, Dropout is introduced into LSTM and network traffic is classified and detected using the Sigmoid and Softmax functions, respectively. Then, the probabilities of different categories are calculated. The formula and derivative of the Sigmoid function are shown in Eq. (2).

$$\begin{cases} S(x)=\dfrac{1}{1+e^{-x}} \\ S(x)'=\dfrac{e^{-x}}{(1+e^{-x})^2} \end{cases} \tag{2}$$

In Eq. (2), $S(x)$ serves as the Sigmoid function. $S(x)'$ serves as the derivative of the Sigmoid function. e represents the base of the natural logarithmic function. The input values are mapped to a range of 0-1 through the Sigmoid function. The threshold is set to 0.5, the features less than 0.5 are set to normal traffic, and features greater than 0.5 are set to abnormal traffic. The loss function for classification is showcased in Eq. (3).

$$F(L)=-\frac{1}{n}\sum_{x}[y\ln a+(1-y)\ln(1-a)] \tag{3}$$

In Eq. (3), $F(L)$ represents loss. The next step is to use a Softmax classifier for detection and classification. Assuming that the training set for abnormal network traffic features is $\{(x_1,y_1),...,(x_m,y_m)\}$ and the category label is $y\in\{1,2,3,...,k\}$, the probability assumption function is shown in Eq. (4).

$$h_\theta(x_i)=p(y_i=k\,|\,x_i;\theta)=\frac{1}{\sum_{j=1}^{k}e^{\theta_j^T x_i}} \tag{4}$$

In Eq. (4), θ serves as the parameters. $\theta_j^T x_i$ serves as the input of the Softmax classifier. $\dfrac{1}{\sum_{j=1}^{k}e^{\theta_j^T x_i}}$ represents normalization. The loss function of Softmax classifier is showcased in Eq. (5).

$$J(\theta)=-\frac{1}{m}\left[\sum_{i=1}^{m}\sum_{j=1}^{k}1\{j=y_i\}\log\frac{e^{\theta_l^T x_i}}{\sum_{l=1}^{k}e^{\theta_l^T x_i}}\right] \tag{5}$$

In Eq. (5), $J(\theta)$ represents the loss function of the Softmax classifier. $1\{j=y_i\}$ represents $y_{ij}=1$ when data i is j, $j=1,2,...,k$. The probability formula for classification in Softmax classifier is shown in Eq. (6).

$$P(y_i=j\,|\,x_i;\theta)=\frac{e^{\theta_l^T x_i}}{\sum_{l=1}^{k}e^{\theta_l^T x_i}} \tag{6}$$

In Eq. (6), P represents the probability. Finally, the minimum value of the loss function for Softmax classification is calculated using the gradient descent method, where the gradient descent calculation is showcased in Eq. (7).

$$\nabla_{\theta_j}J(\theta)=-\frac{1}{m}\sum_{i=1}^{m}[x_i(1\{y_i=j\}-P(y_i=j|x_i;\theta))] \tag{7}$$

In Eq. (7), $\nabla_{\theta_j}J(\theta)$ serves as the gradient differentiation of $J(\theta)$. The update formula for minimizing $J(\theta)$ is showcased in Eq. (8).

$$\theta_j'=\theta_j-\nabla_{\theta_j}J(\theta) \tag{8}$$

In Eq. (8), θ_j' serves as the updated parameter value. θ_j represents the current parameter value. The relevant structure based on LSTM is shown in Fig. 3.

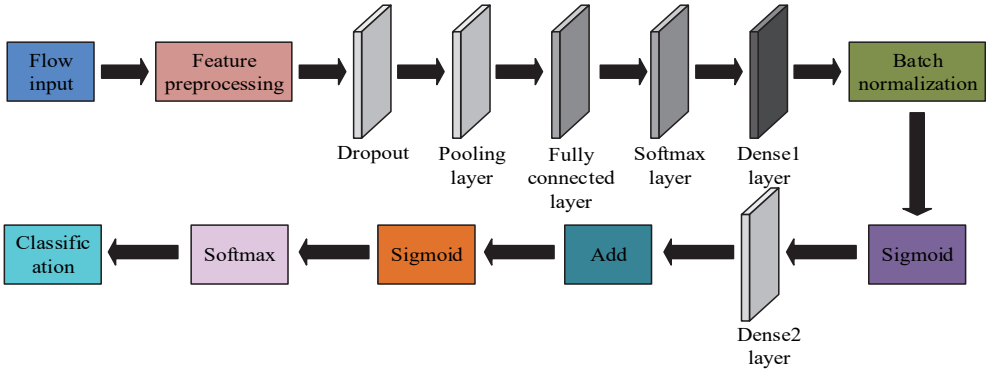

Figure 3 Structure of abnormal traffic detection model based on LSTM

3.2 Parameter Optimization Design of LSTM Abnormal Detection Model Based on Improved GOA

In the LSTM abnormal detection model, there are many parameters that need to be adjusted, such as learning rate, hidden layer neurons, iterations, etc. [21]. Among them, the learning rate is the step size of the control model to adjust the parameters in each update. If it is too small, the training will be too slow, and if it is too large, the convergence may not be possible. The selection of the number of hidden layer neurons depends on the complexity of the dataset and the capacity of the model. When the dataset is large or the problem is complex, the number of hidden neurons can be appropriately increased to improve the fitting ability of the model. However, if the number of hidden layer neurons is too large, it may lead to overfitting. The number of iterations refers to the number of iterations in the entire training process. The more iterations, the more

fully the model will learn from the data, but it may also lead to overfitting. Therefore, the GOA in this study is used to optimize the parameters of the LSTM abnormal detection model, quickly find the global optimal solution, and improve model performance and prediction accuracy. The relevant details are showcased in Fig. 4.

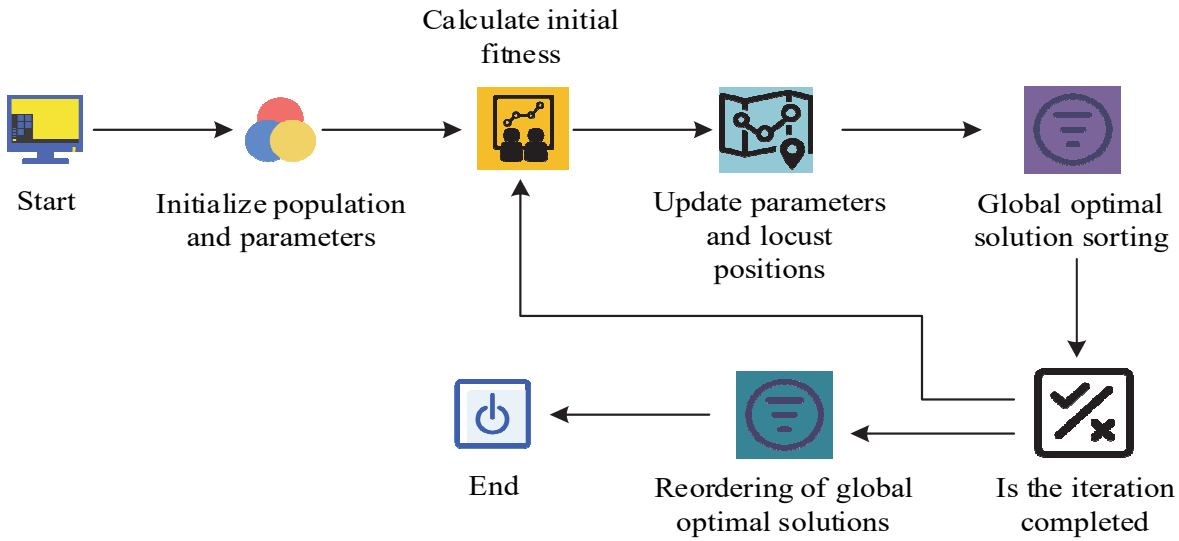

Figure 4 Structure of abnormal traffic detection model based on LSTM

The GOA is a natural heuristic optimization method that seeks the optimal solution by simulating the predatory behavior of locusts [22, 23]. In GOA, it is first necessary for initializing the population as well as allocating the initial positions of individuals in the population, while assigning initial parameter values to each individual. Next, the fitness values are calculated for each individual's current position and parameter values. Then, it updates by changing the parameter values and positions of each individual. Next, all individuals are sorted to find the current global optimal solution. Finally, it determines whether the iteration conditions are met. If the conditions are met, the iteration stops and the global optimal solution is outputted. Otherwise, it returns the calculated fitness value and continues the iteration. In the calculation of GOA, assuming the number of populations is N, the relevant formula is showcased in Eq. (9).

$$X_i = S_i + G_i + A_i \tag{9}$$

In Eq. (9), Xi represents the position of the i-th locust. S_i represents the mutual influence in individual locusts. G_i serves as the gravity on the i-th locust. A_i represents the wind force on i locusts. Among them, the mutual influence between individual locusts possesses the most excellent influence on the position of locusts, and its relevant detail is showcased in Eq. (10).

$$S_i = \sum_{j=1, j=i}^{N} s(d_{ij})\hat{d}_{ij} \tag{10}$$

In Eq. (10), d_{ij} represents the distance between individual locusts. $\hat{d}_{ij}$ represents the unit vector between individual locusts. The expressions for d_{ij} and $\hat{d}_{ij}$ are shown in Eq. (11).

$$\begin{cases} d_{ij} = \left| X_j - X_i \right| \\ \hat{d}_{ij} = \dfrac{\left| X_j - X_i \right|}{d_{ij}} \end{cases} \tag{11}$$

In Eq. (11), X_j serves as the position of the j-th individual locust. The determining formula for the mutual influence in locust individuals is shown in Eq. (12).

$$s(r) = f^{e^{\frac{-r}{m}}} - e^{-r} \tag{12}$$

In Eq. (12), f represents the mutual influence in individuals. m represents the scale of influence between individuals. When $s(r) < 0$, individuals are mutually exclusive. When $s(r) = 0$ is present, individuals neither repel nor attract each other. When $s(r) > 0$, individuals attract each other. Due to the application of GOA in the detection of abnormal network traffic, the influence of gravity on individuals is not considered. The direction of wind force on individuals remains unchanged. The next step is to introduce a reduction factor for enhancing the local and global search capabilities of the GOA to improve the detection efficiency. The expression is showcased in Eq. (13).

$$\mu = \mu_{\max} - l \times \frac{\mu_{\max} - \mu_{\min}}{L}, \mu \in [0.00004, 1] \tag{13}$$

In Eq. (13), μ represents the reduction factor. $\mu_{\max}$ serves as the maximum value of the reduction factor. $\mu_{\min}$ serves as the minimum value of the reduction factor. l serves as the current quantity of iterations. L serves as the total iterations. The calculation method for locust individuals after introducing reduction factors is shown in Eq. (13).

$$X_i^d = \mu(\sum_{j=1, j\neq i}^{N} \mu \frac{\mu b_d - l b_d}{2} s(\left|X_j^d - X_i^d\right|) \frac{X_j - X_i}{d_{ij}}) + \hat{T}_d \quad (14)$$

In Eq. (14), μ represents the introduced reduction factor. μb_d represents the upper bound of the population in the d-dimensional space. lb_d represents the lower bound of the population in the d-dimensional space. $\hat{T}_d$ represents the optimal solution obtained after each iteration. The reduction factor is used for adjusting the size of the search space and enhancing the convergence speed. Meanwhile, this factor can adjust the values of different influence regions among locust individuals, guiding them to move towards the direction of the optimal solution. However, the algorithm still suffers from issues of insufficient global search and being prone to falling into local optima. The reduction factors are optimized through sine cosine function and Levy flight to avoid these phenomena. The distribution of sine cosine and Levy flight functions is shown in Fig. 5.

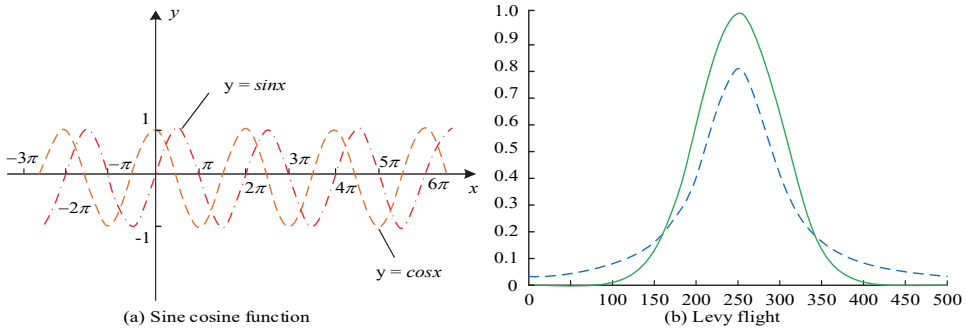

Figure 5 The distribution of sine and cosine functions and Levy's flight functions

The introduced sine and cosine functions can adjust the reduction factor, so that there is a small increase stage before the reduction factor decreases. In the early stage of the algorithm, if the original reduction factor decreases too quickly, it will limit the search space of locusts, resulting in insufficient global search. The small increase of the reduction factor can effectively avoid the situation of insufficient search space in the early stage of locusts to a certain extent. Levy flight is a random flight strategy that simulates the random flight behavior of animals during the search, using random steps and directions for searching. Unlike traditional random walks, the Levy distribution is used to generate step sizes, which has a larger scale range and stronger long-tail characteristics and can better search for space. The study introduces the Levy flight strategy by combining the characteristics of local search in the GOA algorithm. Levy flight can provide a random walk with a step size that conforms to the Levy distribution. During each iteration of the GOA algorithm, Levy flight can be used to make random unknown adjustments for individual locusts in the search unit. This not only expands the search range of the search unit, but also enhances the randomness of local optimization. The calculation method for the optimized reduction factor is shown in Eq. (15).

$$\mu' = R \times ((\mu_{\max} - l \times \frac{\mu_{\max} - \mu_{\min}}{L}) \cos(\pi \times \frac{l}{L}) \sin(\pi \times \frac{l}{L})) \quad (15)$$

In Eq. (15), μ' represents the optimized reduction factor. R represents a uniformly distributed random number. The position relationship of optimized locust individuals is shown in Eq. (16).

$$X_i^{d'} = X_i^d + X_i^d \cdot \omega_s \cdot L(\theta) \quad (16)$$

In Eq. (16), $X_i^{d'}$ represents the position of the optimized locust individual. ω_s represents the control weight when generating step sizes through the Levy distribution. $L(\theta)$ represents the function of Levy flight. Finally, the optimized parameters are input into the LSTM abnormal NTD model for testing. The process of LSTM abnormal NTD based on improved GOA is shown in Fig. 6.

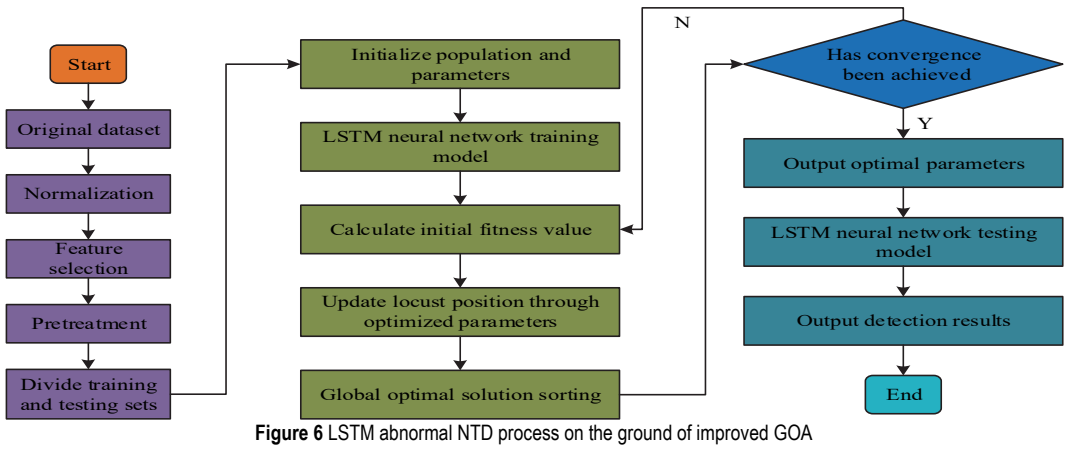

Figure 6 LSTM abnormal NTD process on the ground of improved GOA

The study is conducted in an experimental environment with motherboard parameters of X10DRG-O+- CPU, Intel (R) i5-7200U CPU, 200 GB hard disk memory, and 16 GB running memory. The dimension d = 3 is set, and the iterations are 200. First, various parameters are input, including the locusts, batch size, and maximum iteration. Then, the locust population is initialized, the fitness values of locusts in the population are calculated. The current best individual is retained. The neural network based on the current best individual is trained and the loss function is calculated. Next, the search location of individual locusts is updated to obtain the current population. In the next step, the optimized parameters are updated and the Levi flight strategy is used to update the locust position. All the obtained solutions are sorted. Finally, whether the population completed iteration and convergence is determined.

4 RESULT

4.1 Performance Analysis of LSTM Anomalous NTD Model Based on Improved GOA

First, the optimized GOA was tested to verify the designed LSTM abnormal NTD model based on improved GOA. Its optimization ability was tested through Spherical, Rastigin, Ackley, and Schwefel functions. The dimensions were compared with traditional GOA. The relevant outcomes are showcased in Fig. 7.

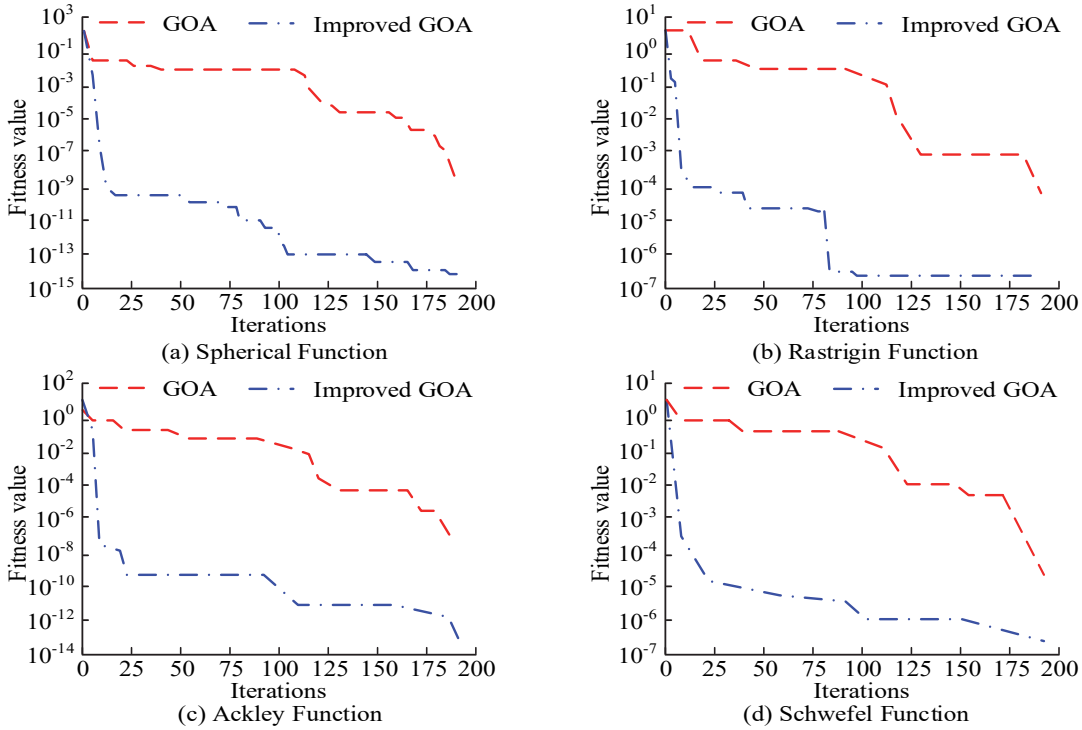

Figure 7 Optimization curve of Improved GOA algorithm in four test functions

Fig. 7 shows that among the four test functions. As the iterations increased, the fitness curve of the improved GOA reduced significantly faster than that of the traditional GOA. This meant that when reaching the iterations, the improved GOA was more effective in finding the global optimal solution than the traditional GOA. Specifically, the improved GOA transformed the reduction factor from linear to nonlinear, enhancing the global search capability of the algorithm. Meanwhile, it increased the randomness by Levy flight, thereby improving the local search ability. The above outcomes showcased that the improved GOA had better optimization ability. The next step was to validate the accuracy, recall, and F1 score of the designed abnormal NTD model in the NSL-KDD dataset, and it was compared with the three indicator values of decision tree, random forest, K-nearest neighbor, and autoencoder algorithms. Calculate the confidence intervals for each indicator, and based on a normal distribution, set the standard normal score for the 95% confidence interval to 1.96. Meanwhile, compared with the LSTM algorithm optimized using traditional GOA and bottle sea sheath swarm algorithm, the relevant outcomes are showcased in Tab. 1.

Table 1 Accuracy, recall, and F1 score of abnormal NTD model

Detection model	Precision Rate	95% CI for Precision	F1-score	95% CI for F1-score	Recall	95% CI for Recall
IGOA-LSTM	0.93	(0.891, 0.968)	0.95	(0.923, 0.976)	0.98	(0.954, 1.006)
Decision Tree Algorithm	0.68	(0.643, 0.712)	0.80	(0.766, 0.836)	0.96	(0.933, 0.983)
PSO	0.89	(0.852, 0.924)	0.74	(0.707, 0.776)	0.60	(0.562, 0.634)
K-nearest neighbor algorithm	0.84	(0.804, 0.875)	0.87	(0.832, 0.906)	0.91	(0.886, 0.932)
Auto encoder algorithm	0.77	(0.738, 0.802)	0.87	(0.834, 0.906)	0.97	(0.943, 0.991)
GOA-LSTM	0.92	(0.884, 0.953)	0.94	(0.913, 0.966)	0.95	(0.922, 0.973)
SSA-LSTM	0.91	(0.871, 0.947)	0.93	(0.905, 0.956)	0.92	(0.896, 0.942)

In Tab. 1, the accuracy of the model based on the decision tree was 0.68, with a higher recall rate and F1 score of 0.96 and 0.80. The recall rate and F1 score based on the random forest algorithm were 0.60 and 0.74, respectively, indicating that the model might miss some abnormal samples when detecting abnormal traffic. The accuracy of the model based on K-nearest neighbor algorithm was 0.84, and the recall rate and F1 score were 0.91 and 0.87. The accuracy of the model based on auto encoder was 0.77, with a higher recall rate and F1 score of 0.97 and 0.87. The performance of the LSTM model based on traditional GOA was similar to that of the LSTM model based on the bottle sea sheath group, with accuracy rates of 0.92 and 0.91, recall rates of 0.95 and 0.92, and F1 score of 0.94 and 0.93. Compared with the above models, the accuracy, recall, and F1 score values of the LSTM abnormal NTD model based on improved GOA were 0.93, 0.98, and 0.95, respectively, with 95% confidence intervals of (0.891, 0.968), (0.923, 0.976), and (0.954, 1.006), respectively. Its comprehensive performance was significantly superior to other models in abnormal NTD, demonstrating its superiority in abnormal NTD. This designed abnormal NTD model was tested with and without Dropout, respectively, to further validate its accuracy. The accuracy and loss curves are shown in Fig. 8.

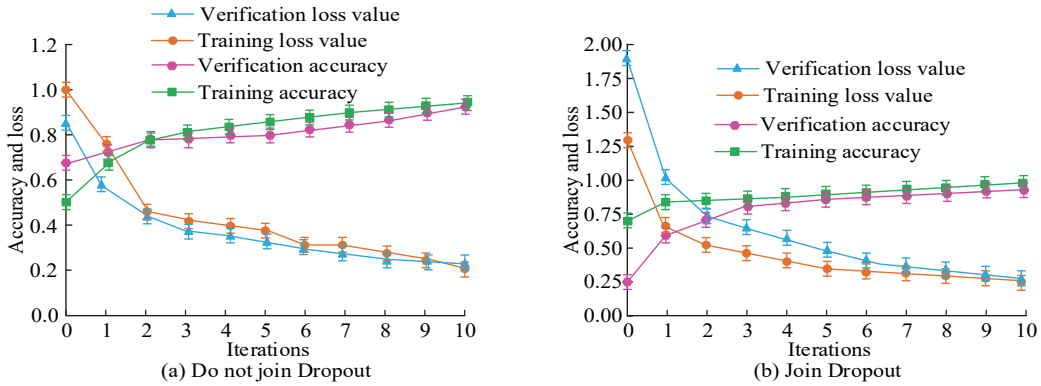

Figure 8 Accuracy and loss curve with and without dropout

In Fig. 8, when Dropout was not added, the accuracy of the training set of the designed abnormal NTD model was 94%, with a loss of 0.21. The accuracy of the test set reached 92%, with a loss value of 0.23. The average accuracy reached 93%, and the average loss reached 0.22. When Dropout was added, the accuracy of the training set reached 99%, the accuracy of the test set reached 97%, and the average accuracy reached 98%. The loss of the training set reached 0.26, the loss of the test set reached 0.30, and the average loss reached 0.28. The above results indicated that adding Dropout effectively prevented overfitting of the model during training, thereby improving the model's generalization ability and robustness. The above results indicate that adding Dropout effectively prevents overfitting of the model during training, thereby improving the model's generalization ability and robustness. In order to verify the computational complexity of the abnormal network traffic detection model, training was conducted on the NSL-KDD dataset, KDD99 dataset, and DARPA dataset, and the detection time was calculated. The results were compared with decision tree algorithm, random forest algorithm, K-nearest neighbor algorithm, methods in references [24] and [25], and the results are shown in Tab. 2.

Table 2 Comparison of inspection time for different algorithms in different data sets

Model	Testing time / s		
	NSL-KDD	KDD99	DARPA
Decision Tree Algorithm	0.483	0.714	0.437
Random forest algorithm	0.572	0.821	0.584
Reference [24]	0.338	0.538	0.373
Reference [25]	0.264	0.487	0.356
Improved GOA-LSTM	0.147	0.340	0.235

From Tab.2, it can be seen that the detection time of the designed anomaly network traffic detection model is 0.147 seconds in the NSL-KDD dataset, 0.340 seconds in the KDD99 dataset, and 0.235 seconds in the DARPA dataset. It can be observed that the detection time of the designed model on different datasets is significantly lower than that of other models, indicating that its computational speed is faster and proving that the computational complexity of the designed model is lower [26].

4.2 Analysis of the Actual Effect of LSTM Anomalous NTD Model Based on Improved GOA

Multi-classification detection was conducted using three attack types: Dos, R2L, and U2R to test the effectiveness of the industrial control network abnormal traffic detection model in practical applications. Firstly, the time for abnormal traffic detection was calculated and compared with other models. The results are shown in Fig. 9.

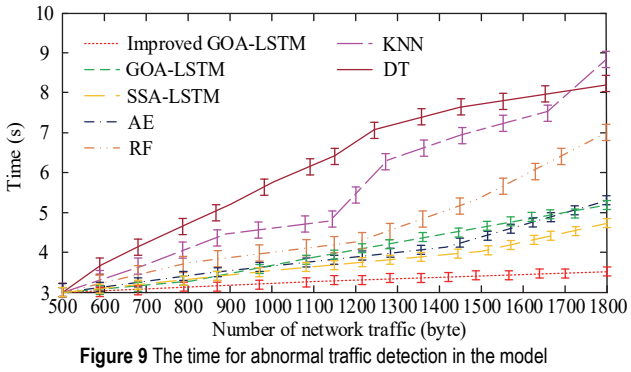

Figure 9 The time for abnormal traffic detection in the model

In Fig. 9, as network traffic increased, the detection time of each model gradually increased. When the network

traffic was 1800 bytes, the detection time of the improved GOA-based LSTM network abnormal traffic detection model was 3.52 seconds, while the detection time of the traditional GOA-based LSTM network abnormal traffic detection model was 5.25 seconds. The detection time of the LSTM model based on the group of bottle sea squirts, the model based on auto encoder, the model based on random forest, the model based on K-nearest neighbor, and the model based on decision tree was 4.87 s, 5.28 s, 7.02 s, 8.96 s, and 8.14 s, respectively. The above results indicated that the designed LSTM network abnormal traffic detection model based on improved GOA had high recognition efficiency. This model quickly and effectively detected various attack types such as Dos, R2L, U2R, etc., which was beneficial to industrial control network security. The detection rate refers to the number of alarms when a unit of valid tags passes through different positions in the detection area in different directions. False alarm rate refers to the probability of a system mistaking correct behavior for an attack. The unknown attack detection rate represents the model's ability to identify unknown attack types. These indicators can comprehensively reflect the performance of the network anomaly traffic detection model. The next step was to calculate the detection, false alarm, and unknown attack detection rates of NTD. This model was compared with the LSTM model based on GOA and the K-nearest neighbor model. The outcomes are illustrated in Tab. 3 [27].

Table 3 The detection, false alarm, and unknown attack detection rates of NTD (%)

Attack Type	Improved GOA-LSTM			GOA-LSTM			K-nearest neighbor algorithm		
	Detection rate	False alarm rate	Unknown attack detection rate	Detection rate	False alarm rate	Unknown attack detection rate	Detection rate	False alarm rate	Unknown attack detection rate
Dos	98.15	3.16	94.85	92.48	8.16	91.05	88.73	10.87	89.95
R2L	95.52	4.15	95.29	91.87	9.04	90.50	87.60	10.48	87.58
U2R	96.48	3.37	94.96	93.15	9.12	91.68	89.14	8.14	88.74

In Tab. 3, the designed model had a detection rate of 98.15% for the Dos attacks, which was nearly by 6% exceeding the GOA-LSTM model as well as by nearly 10% exceeding the K-nearest neighbor algorithm. In the R2L attack type, the detection rate of the designed model was 95.52%, which was nearly 4% exceeding the GOA-LSTM model and nearly 8% exceeding the K-nearest neighbor algorithm. For U2R attacks, the detection rate of the designed model reached 96.48%, which was nearly 3% exceeding the GOA-LSTM model and nearly 7% exceeding the K-nearest neighbor algorithm. Meanwhile, the designed model had a lower false alarm rate than other models. The designed model performed best in terms of unknown attack detection rate. The above outcomes illustrated that the designed model possessed high efficiency and accuracy in detecting network traffic attacks [28]. Finally, the detection effect of the design method was further verified through the working characteristic curve of the subjects, and the outcomes made comparison with other models as shown in Fig. 10.

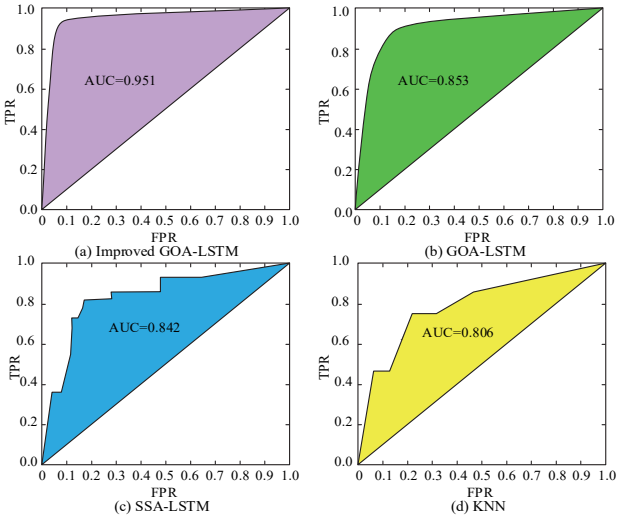

Figure 10 The time for abnormal traffic detection in the model

In Fig. 10, the AUC value of the LSTM model based on improved GOA was 0.951. The AUC value of the LSTM model based on GOA was 0.853. The AUCA value of the LSTM model based on the group of bottle sea squirts was 0.842. The AUC value of the K-nearest neighbor-based model was 0.806. These results indicated that the LSTM model based on improved GOA had high accuracy and reliability in identifying network traffic attacks, providing an efficient and reliable solution for network security.

5 DISCUSSION

With the progress of the Internet, the network environment becomes more and more complex. At the same time, more network attacks and threats appear on the Internet. Network security is the foundation of national security, which not only receives high attention from the state, but also sparks intense discussions in the academic community. In response to the large amount of network traffic data, this study improved the GOA and optimized the hyperparameters of LSTM through the improved GOA. An LSTM abnormal detection algorithm based on improved GOA parameter optimization was proposed. The results showed that in the NSL-KDD dataset, the F1 value of the designed algorithm was 0.95, which was significantly higher than other models. This conclusion was consistent with the conclusions drawn by Thanh N. N. T. and Nguyen Q. H. The model designed by Thanh N. N. T. achieved an F1 value of 99.97% on the CICIDS2017 dataset [23]. These results proved the effectiveness of the design algorithm. The accuracy of the design algorithm in the training set reached 99%, which was consistent with the conclusion drawn by Han D. et al. Han D. et al. proposed a lightweight abnormal NTD model for the Internet of Things in 2023, and an accuracy of 99.98% was achieved on the AWID dataset [24]. It was proved that the abnormal traffic detection model based on design algorithms had

stable performance and high robustness, which better detected and discriminated network traffic. The detection rate of the designed model on Dos, R2L, and U2R attacks reached 98.15%. The model proposed by Li Y. et al. in 2023 achieved a maximum detection rate of 99.98% in intrusion detection [25]. Therefore, this research obtained similar conclusions as Li Y. and other researchers, proving the accuracy and reliability of the design method. The above results indicated that the designed algorithm identified the types of abnormal traffic, provided users with further attack information, enabled effective defense and risk avoidance when dealing with network attacks, and improved the security index of the network environment. In summary, although the research only conducted experiments on known types of attacks, with the advancement of technology, more unknown attacks will emerge, and the proposed model will inevitably face these challenges. However, it has a high detection rate in detecting abnormal network traffic and performs excellently in indicators such as accuracy, recall, and F1 score. Design can improve the security and reliability of the entire power industrial control network, which has a positive impact on the sustainable development of the entire power industry.

6 CONCLUSION

With the development and intelligent process of power industry control systems, the security issues of power industry control networks attract people's attention. This study designed an LSTM-based abnormal NTD model to detect abnormal traffic in the network in a more timely manner. Meanwhile, the sine cosine function and Levy flight optimization were introduced for reducing the factors based on the GOA. The parameters of the model were optimized through the improved GOA. The results showed that among the four test functions, the fitness curve of the improved GOA decreased faster than that of the traditional GOA, indicating its good optimization ability. In the calculation of accuracy, recall, and F1 score, the LSTM abnormal NTD model based on improved GOA had three values of 0.93, 0.98, and 0.95, which were superior to other algorithms and demonstrated its superiority in abnormal NTD. In the calculation of subject performance curve, the AUC value of the LSTM model based on improved GOA was 0.951, which was higher than the 0.853, 0.842, and 0.806 of the other three models. This proved that the LSTM model based on improved GOA had high reliability and accuracy in identifying network traffic attacks. The designed algorithm not only enhances the optimization ability of the model, but also improves the accuracy of abnormal traffic detection. At the same time, it can improve the stability and safety of power industry control systems, which is of positive significance for promoting technological progress in related fields. However, the research mainly focuses on training for known specific types of attacks and has not attempted to apply it to the detection of unknown types of attacks. In future research, we will further explore its ability to detect new types of attacks in real network environments.

7 REFERENCES

[1] Garg, S., Kaur, K., Kumar, N., & Rodrigues, J. J. (2019). Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective. *IEEE Transactions on Multimedia*, *21*(3), 566-578. https://doi.org/10.1109/TMM.2019.2893549

[2] Guezzaz, A., Asimi, Y., Azrour, M., & Asimi, A. (2021). Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection. *Big Data Mining and Analytics*, *4*(1), 18-24. https://doi.org/10.26599/BDMA.2020.9020019

[3] Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2020). CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet of Things Journal*, *8*(5), 3242-3254. https://doi.org/10.1109/JIOT.2020.3002255

[4] Bukya, R., Madhu Mohan, G., & Kumar Swamy, M. (2025). Artificial intelligence role in optimizing electric vehicle charging patterns, reduce costs, and improve overall efficiency: A review. *Journal of Engineering, Management and Information Technology, 2*(3), 129–138. https://doi.org/10.61552/JEMIT.2024.03.004

[5] Dong, S., Xia, Y., & Peng, T. (2021). Network abnormal traffic detection model based on semi-supervised deep reinforcement learning. *IEEE Transactions on Network and Service Management*, *18*(4), 4197-4212. https://doi.org/10.1109/TNSM.2021.3120804

[6] Chen, M., Wang, X., He, M., Jin, L., Javeed, K., & Wang, X. (2020). A network traffic classification model based on metric learning. *CMC-computers Materials & Continua*, *64*(2), 941-959. https://doi.org/10.32604/cmc.2020.09802

[7] Alshammari, A., & Aldribi, A. (2021). Apply machine learning techniques to detect malicious network traffic in cloud computing. *Journal of Big Data*, *8*(1), 1-24. https://doi.org/10.1186/s40537-021-00475-1

[8] Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2021). Novel approach for detection of IoT generated DDoS traffic. *Wireless Networks*, *27*(3), 1573-1586. https://doi.org/10.1007/s11276-019-02043-1

[9] Xiao, F., Chen, L., Zhu, H., Hong, R., & Wang, R. (2019). Anomaly-tolerant network traffic estimation via noise-immune temporal matrix completion model. *IEEE Journal on Selected Areas in Communications*, *37*(6), 1192-1204. https://doi.org/10.1109/JSAC.2019.2904347

[10] Phan, T. V., Nguyen, T. G., Dao, N. N., Huong, T. T., Thanh, N. H., & Bauschert, T. (2020). DeepGuard: Efficient anomaly detection in SDN with fine-grained traffic flow monitoring. *IEEE Transactions on Network and Service Management*, *17*(3), 1349-1362. https://doi.org/10.1109/TNSM.2020.3004415

[11] Song, H. M. & Kim, H. K. (2021). Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. *IEEE Transactions on Vehicular Technology*, *70*(2), 1098-1108. https://doi.org/10.1109/TVT.2021.3051026

[12] Ma, W., Zhang, Y., Guo, J., & Li, K. (2021). Abnormal traffic detection based on generative adversarial network and feature optimization selection. *International Journal of Computational Intelligence Systems*, *14*(1), 1170-1188. https://doi.org/10.2991/ijcis.d.210301.003

[13] Dandıl, E. (2020). C-NSA: a hybrid approach based on artificial immune algorithms for anomaly detection in web traffic. *IET Information Security*, *14*(6), 683-693. https://doi.org/10.1049/iet-ifs.2019.0567

[14] Duan, L., Zhou, J., Wu, Y., & Xu, W. (2022). A novel and highly efficient botnet detection algorithm based on network traffic analysis of smart systems. *International Journal of Distributed Sensor Networks*, *18*(3), 182459-182476. https://doi.org/10.1177/15501477211049910

[15] Xia, B., Han, D., Yin, X., & Na, G. (2022). RICNN: A ResNet & Inception convolutional neural network for intrusion detection of abnormal traffic. *Computer Science and Information Systems*, *19*(1), 309-326. https://doi.org/10.2298/csis210617055x
[16] Yang, J., Liang, G., Li, B., Wen, G., & Gao, T. (2021). A deep-learning-and reinforcement-learning-based system for encrypted network malicious traffic detection. *Electronics Letters*, *57*(9), 363-365. https://doi.org/10.1049/ell2.12125
[17] Nguyen, H. C., Xuan, C. D., Nguyen, L. T., Nguyen, L. T., & Nguyen, H. D. (2023). A new framework for APT attack detection based on network traffic. *Journal of Intelligent & Fuzzy Systems*, *44*(3), 3459-3474. https://doi.org/10.3233/JIFS-221055
[18] Shi, G., Shen, X., Xiao, F., & He, Y. (2023). DANTD: A deep abnormal network traffic detection model for security of industrial internet of things using high-order features. *IEEE Internet of Things Journal*, *10*(24), 21143-21153. https://doi.org/10.1109/JIOT.2023.3253777
[19] Fortino, G., Greco, C., Guzzo, A., & Ianni, M. (2023). Identification and prediction of attacks to industrial control systems using temporal point processes. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 4771-4783. https://doi.org/10.1007/s12652-022-04416-5
[20] Nimrah, S. & Saifullah, S. (2022). Context-Free Word Importance Scores for Attacking Neural Networks. *Journal of Computational and Cognitive Engineering*, *1*(4), 187-192. https://doi.org/10.47852/bonviewJCCE2202406
[21] Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2020). Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4519-4530. https://doi.org/10.1109/TITS.2020.3027390
[22] Wang, W., Wang, Z., Zhou, Z., Deng, H., Guo, Y., Wang, C., & Zhao, W. (2021). Anomaly detection of industrial control systems based on transfer learning. *Tsinghua Science and Technology*, *26*(6), 821-832. https://doi.org/10.26599/TST.2020.9010041
[23] Thanh, N. N. T. & Nguyen, Q. H. (2023). Detection of Abnormal Network Traffic Using Bidirectional Long Short-Term Memory. *Computer Systems Science and Engineering*, *46*(1), 491-504. https://doi.org/10.32604/csse.2023.032107
[24] Han, D., Zhou, H. X., Weng, T. H., Wu, Z., Han, B., Li, K. C., & Pathan A. S. K. (2023). LMCA: a lightweight anomaly network traffic detection model integrating adjusted mobilenet and coordinate attention mechanism for IoT. *Telecommunication Systems*, *84*(4), 549-564. https://doi.org/10.1007/s11235-023-01059-5
[25] Li, Y., Han, D., Cui, M., Yuan, F., & Zhou, Y. (2023). RESNETCNN: An abnormal network traffic flows detection model. *Computer Science and Information Systems*, *20*(3), 997-1014. https://doi.org/10.2298/CSIS221124004L
[26] Sarp, S., Kuzlu, M., Zhao, Y., Cetin, M., & Guler, O. (2022). A Comparison of Deep Learning Algorithms on Image Data for Detecting Floodwater on Roadways. *Computer Science and Information Systems*, *19*(1), 397-414. https://doi.org/10.2298/CSIS210313058S
[27] Xia, B., Han, D., Yin, X., & Gao, N. (2022). RICNN: A ResNet & Inception Convolutional Neural Network for Intrusion Detection of Abnormal Traffic. *Computer Science and Information Systems*, *19*(1), 309-326. https://doi.org/10.2298/CSIS210617055X
[28] Ibrahim, J. & Gajin, S. (2022). Entropy-based Network Traffic Anomaly Classification Method Resilient to Deception. *Computer Science and Information Systems*, *19*(1), 87-116. https://doi.org/10.2298/CSIS201229045I

Contact information:

Liming LIN
(Corresponding author)
State Grid Information & Telecommunication Group Co., Ltd.,
Beijing, 102200, China
E-mail: xwypapers@163.com

Ang XIA
State Grid Information & Telecommunication Co., Ltd.,
Beijing, 100032, China
E-mail: xiaang@sgcc.com.cn

Fangfang DANG
State Grid Henan Information & Telecommunication Company (Data Center),
Zhengzhou, Henan, 450000, China
E-mail: songzet123@sina.com

Qin YIN
State Grid Information & Telecommunication Group Co., Ltd.,
Beijing, 102200, China
E-mail: yinqinhouse@163.com

Xirong LV
Xiamen Great Power Geo Information Technology Company Ltd.,
Xiamen, Fujian, 361000, China
E-mail: zhiqingshunxie@126.com