International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 380-388

https://doi.org/10.70517/ijhsa46433

Design of Multi-level Intrusion Detection System for Internet of Things Security Based on Support Vector Machines

Dongdong Liu[1,2,*], Fuqiang Li[1] and Shuo Fang[1]
[1] School of Computer and Information Engineering, Fuyang Normal University, Fuyang, Anhui, 236037, China
[2] Anhui Engineering Research Center for Intelligent Computing and Information Innovation, Fuyang Normal University, Fuyang, Anhui, 236037, China
Corresponding authors: (e-mail: 200607017@fynu.edu.cn).

Abstract While hand in hand with the Internet of Things (IoT) to provide people with daily convenience, technologies such as big data are also assisting illegal information to invade and interfere with IoT. In this paper, we take the construction of multi-polar intrusion detection system as the ultimate research goal, design the global search strategy of intrusion, the difference degree detection model and the association rule analysis model to analyze the intrusion information in an all-round way. With this data preparation, support vector machine (SVM) classifier is established and fused with similar cluster-based sample size approximation algorithm to build FSVM model as the detection method of abnormal data. The Gray Wolf Optimization (GWO) algorithm is used for the optimization of support vector machine algorithm parameter selection to form the GWO-SVM algorithm, which in turn proposes an IoT intrusion detection system based on the GWO-SVM algorithm. The designed intrusion detection system shows excellent suitability for IoT security multi-pole intrusion detection with accuracy up to 100.00% and F1 value up to 99.01% in the performance evaluation.

Index Terms FSVM model, GWO-SVM algorithm, internet of things intrusion detection system, association rules

I. Introduction

With the rapid development and application of IoT technology, the security of IoT environment has become an important concern [1], [2]. Intrusion detection system plays a crucial role in IoT environment, which can monitor and detect abnormal behaviors in the network, discover potential attacks in time and take corresponding measures for protection [3]-[5]. Intrusion refers to unauthorized access or activities in the information system, which not only refers to the unauthorized login to the system and use of system resources by non-system users, but also includes the damage to the system caused by the abuse of rights by users within the system, such as illegally stealing other people's accounts, illegally obtaining the rights of the system administrator, and modifying or deleting the system files, etc [6]-[9]. Intrusion detection systems, as an important part of network security, play an important role in preventing malicious attacks and protecting the network environment [10], [11]. However, traditional intrusion detection systems still face some challenges, such as the inability to accurately distinguish real attacks from false alarms, and the limited ability to recognize new attack methods [12], [13]. In contrast, network intrusion detection systems based on support vector machine algorithms have high accuracy and generalization ability and can be applied to various types of network intrusion problems [14]-[16].

Support vector machine is a machine learning algorithm widely used in pattern classification and regression analysis with strong generalization ability and classification effect [17], [18]. It classifies by constructing an optimal hyperplane in a high-dimensional space, which is a very effective classification method and is widely used in the fields of data mining, image recognition, natural language processing and bioinformatics [19]-[21]. Among them, the support vector machine algorithm has also shown excellent ability in network intrusion detection, but due to the variability of the network environment, the multilevel intrusion detection system for IoT security based on support vector machines also needs to be improved and optimized continuously [22]-[25].

In this paper, we first describe the mathematical construction process of the intrusion data source distribution model as a big data analysis method for intrusion information in the IoT environment. Then, under the representation of Support Vector Machine (SVM) classifier model, it elucidates the computational formulas of low-dimensional feature data, kernel function, and objective function. And design the process of acquiring data near the decision boundary based on the sample size approximation algorithm of heterogeneous classes, combined with the K-means algorithm, to construct the FSVM model. Subsequently, the global search method of Gray Wolf Optimization (GWO) algorithm is resolved, and the specific steps of the GWO algorithm to optimize the parameter selection of the support vector machine, so as to comprehensively build the IoT intrusion detection

system based on GWO-SVM. The system is trained for RBM feature extraction performance and parameters for fast scoring of intrusion data are defined. Finally, the overall performance of the designed IoT intrusion detection system is carried out on the UNSW-NB20 dataset.

II. GWO-SVM Based Intrusion Detection System for IoT

II. A.Big data analysis of intrusion information

Adopting the method of knapsack decision-making to realize the construction of the objective function in the process of industrial interconnection AI intrusion detection, based on the method of multidimensional scale decomposition to realize the spatial feature sampling and information search of industrial interconnection AI intrusion, and to obtain the formula of the global search strategy of the industrial interconnection AI intrusion as in Eq. (1):

$$C = \frac{\left(X_{new}^{*} - X\right)r}{X_h} + lB \tag{1}$$

In the above equation, X_{new}^{*} is the new solution of industrial interconnection AI intrusion search, X is the current solution, r is the random number that represents the industrial interconnection AI intrusion detection, and its value is within $(0,1)$, X_h is the optimal solution of the industrial interconnection AI intrusion detection, and l is the dynamic factor. The backpack detection method is used to establish the difference degree detection model of industrial interconnection AI intrusion, and the transfer function is obtained as Eq. (2):

$$D = \frac{N(z)}{C} \tag{2}$$

In the above equation, $N(z)$ is the characteristic function of industrial interconnection AI intrusion. The fuzzy information fusion method is used for the big data fusion analysis of industrial interconnection AI intrusion in IoT environment, and at the extreme value point z, the global information exchange method is used to analyze the intrusion anomaly node $u(x)$, and the associated feature quantity of the industrial interconnection AI intrusion signals in the IoT environment is extracted, so that the subspace of the industrial interconnection AI information is obtained as equation (3):

$$E = \frac{u(x) - z}{D} + \frac{u_1(\tilde{x})}{u_2(\tilde{x})} \times D \tag{3}$$

In the above equation, $u_1(\tilde{x})$ is the autocorrelation feature quantity, and $u_2(\tilde{x})$ is the mutual correlation feature quantity.

The autocorrelation matching method is used to realize the correlation rule analysis model for AI intrusion in industrial interconnection network, and the expression is Eq. (4):

$$G = Ep - \frac{u_1(\tilde{x})}{u_2(\tilde{x})} \tag{4}$$

In the above equation, the selection of the associated feature quantity p should satisfy $2a \le p \le b-1$. Combined with the interference filtering method, the filtering analysis of industrial interconnection network AI intrusion in IoT environment is carried out, and the cross term of industrial interconnection AI intrusion output is obtained as Eq. (5):

$$g = aG + b/p \tag{5}$$

In the IoT environment, the industrial Internet AI intrusion data source distribution model is established, and the discrete distribution form of the industrial Internet AI intrusion signal is obtained as equation (6):

$$H = \frac{1}{s}\sum_{j=1}^{m}\frac{\left|\rho G - g\right|}{td_j} \tag{6}$$

In the above equation, t is the anomalous data phase eigenvalue of industrial Internet AI intrusion, ρ is the set average statistic of industrial Internet AI intrusion, and s is the autocorrelation function scale parameter. The design of intrusion detection is realized by weighting and analyzing the root node of industrial interconnection network AI intrusion in IoT environment.

II. B.FSVM model

II. B. 1) SVM Classifier

In order to solve the nonlinear classification problem, Gaussian kernel function is used in the model to solve the sub-linear classification problem of the model.SVM converts the low-dimensional data into the high-dimensional space representation when calculating the maximum spacing hyperplane as in Eq. (7), and the low-dimensional vector x is converted into the high-dimensional space representation through the mapping function, at this time, the classifier model is represented as in Eq. (8), because there is the inner product form of the high-dimensional vectors in the Eq. , which can be converted to low-dimensional feature data through the kernel function is calculated as Eq. (9). The Gaussian function is chosen as the kernel function in the model as in Eq. (10), therefore, the objective function of the model is as in Eq. (11).

$$x \to \phi(x) \tag{7}$$

$$W(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j (\phi(x_i) \cdot \phi(x_j)) \tag{8}$$

$$g(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1,j=1}^{n} \alpha_i \alpha_j y_i y_j k(x_i, x_j) \tag{9}$$

$$k(x_i, x_j) = e^{-\frac{\|x_i - x_j\|^2}{2\sigma^2}} \tag{10}$$

$$g(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1,j=1}^{n} \alpha_i \alpha_j y_i y_j e^{-\frac{\|x_i - x_j\|^2}{2\sigma^2}} \tag{11}$$

II. B. 2) Sample size normalization algorithm based on similar clusters

In the process of training SVM using sample data, it is the sample data near the decision boundary and on the interval boundary in the sample, i.e., the support vectors, that determine the classification hyperplane. So before training the SVM model using sample data, the sample data is screened to get the sample data near the decision boundary. The network sample data can be categorized into two classes, i.e., normal data and abnormal data. First, the model performs clustering operation on normal data and abnormal data separately by optimized K-mean algorithm, and then obtains clusters that are similar to the dissimilar data in normal data and abnormal data respectively. The data in this cluster is returned as the input sample of the classification model, and the operation flow of sample size approximation based on similar clusters is shown in Fig. 1.

The detailed flow of the algorithm is as follows:

(1) Perform the following clustering operation on the normal data in the sample data, randomly select a data from the normal sample set as a cluster center and put it into the set A_{core}, set the value of the cluster radius r, traverse the normal sample set, and put samples whose similarity with the center of the clusters in the set A_{core} is less than R into the corresponding cluster. When there is a sample that does not belong to any of the known clusters, set that sample data as a new cluster center and put it into A_{core}, and continue traversing the normal sample set until all the sample data have found their respective clusters, obtaining the set of clusters A, where the i th element, denoted as a_i, is a cluster, and its corresponding cluster center is ac_i.

(2) Repeat the operation of step (1) for the anomalous data in the sample data to obtain the set B of clusters, where the j th element, denoted as b_j, is a cluster whose corresponding cluster center is bc_j.

(3) Perform the Cartesian product operation $(A \times B)$ on A and B as shown in Eq. (12), and compute the similarity $l_{i,j}$ between the cluster centers ac_i and bc_j for each element (a_i, b_j) in the set $(A \times B)$.

(4) Categorize the elements in $(A \times B)$ with a_i as the classification basis, sort the elements in each category according to the similarity $l_{i,j}$ obtained in step (3) from smallest to the largest, set the number of similar clusters n, and select the first n elements in each category to generate the set C. Remove all b_j elements in C and perform the concatenation operation to generate a new sample set BB.

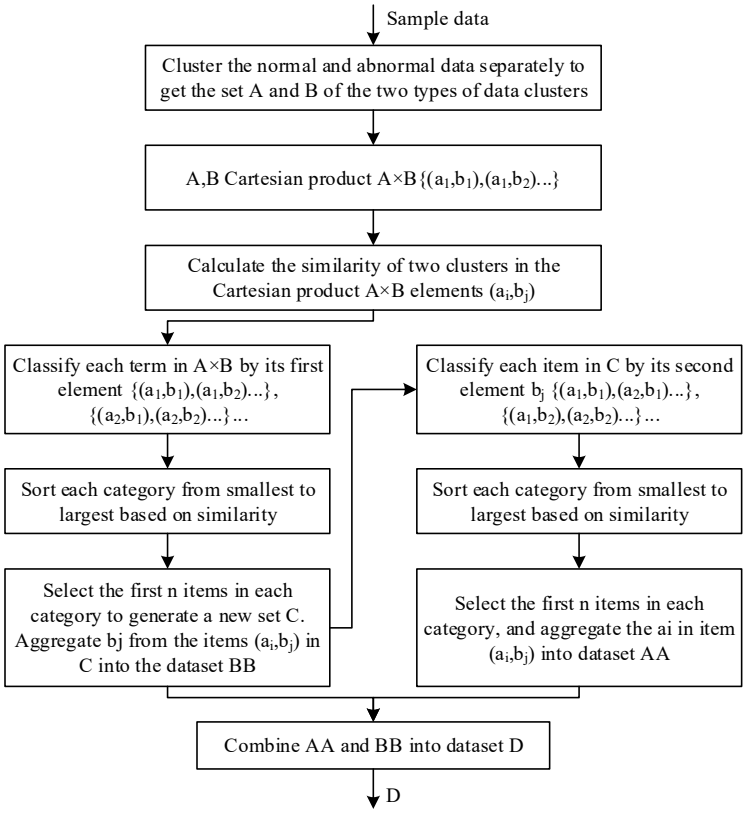

Figure 1: The operation process of sample size reduction based on similar clusters

(5) Repeat the operation of step 4 for the set C, categorize the elements in it with b_j as the categorization basis, sort the similarity of elements in each category $l_{i,j}$ from smallest to the largest, select the first n elements, and take out the a_i elements from this n elements to perform the concatenation operation to generate a new sample set AA.

(6) Merge the sample sets AA and BB to generate a new sample set D, and use D as the original input samples of SVM.

The formula for the Cartesian product operation is equation (12):

$$A \times B = \{(a_1, b_1), (a_1, b_2) \cdots (a_1, b_n), (a_2, b_1), \cdots (a_i, b_j)(a_n, b_m)\} \tag{12}$$

In Equation (12), n and m are the number of elements in the cluster sets A and B, respectively, a_i is the i th element in A, and b_j is the j th element in B.

II. C.Gray Wolf Optimization Algorithm

In the gray wolf optimization algorithm, each gray wolf represents one potential solution for the population. The algorithm simulates the gray wolf social hierarchy as α-wolf, β-wolf, δ-wolf, and ω-wolf, which represent the optimal, superior, suboptimal, and candidate solutions, in that order. Where α, β and δ lead the search and ω follows.

II. C. 1) Surrounding prey

Let the number of wolves be N and the dimension of the search space be M, then the location of the i th wolf is defined as equation (13):

$$X_{i,j} = \left(X_{i,1}, X_{i,2}, \cdots, X_{i,m}\right) \tag{13}$$

where $i = 1, 2, \cdots, n$. Then the encircling prey is defined as in Eqs. (14)-(15):

$$D = \left| C \cdot X_p(t) - X(t) \right| \tag{14}$$

$$X(t+1) = X(t) - A \cdot D \tag{15}$$

where t is the current iteration number. A and C are coefficient vectors. X_p is the prey position, X is the gray wolf position, and D denotes the distance between the gray wolf and the prey. The vectors A and C are calculated as in Eqs. (16)-(18):

$$A = 2a \cdot r_1 - a \tag{16}$$

$$C = 2 \cdot r_2 \tag{17}$$

$$a = 2 - 2\left(t / \left(\max\_t\right)\right) \tag{18}$$

where the component of a decreases linearly from 2 to 0 during the iteration. r_1 and r_2 are random numbers in $[0,1]$.

The random values of $|A| > 1$ are utilized in the GWO algorithm to force the searching wolf to stay away from the prey, which facilitates the global search. The C provides random weights for the prey, which helps to show a more random behavior throughout the optimization process, facilitating the search and avoiding falling into a local optimum.

II. C. 2) Hunting

During the hunting process, α wolves, β wolves and δ wolves have more information about the prey, so the 3 optimal solutions are kept during each iteration, forcing the other ω wolves to update their own search positions based on these 3 optimal solutions, as shown in Eqs. (19)-(21):

$$\begin{cases} D_\alpha = \left| C_1 \cdot X_\alpha - X \right| \\ D_\beta = \left| C_2 \cdot X_\beta - X \right| \\ D_\delta = \left| C_3 \cdot X_\delta - X \right| \end{cases} \tag{19}$$

$$\begin{cases} X_1 = X_\alpha - A_1 \cdot D_\alpha \\ X_2 = X_\beta - A_2 \cdot D_\beta \\ X_3 = X_\delta - A_3 \cdot D_\delta \end{cases} \tag{20}$$

$$X\left(t+1\right) = \frac{X_1 + X_2 + X_3}{3} \tag{21}$$

Eq. (19) obtains the distance of the individual gray wolf from the three wolves α, β, and δ, and Eqs. (20) and (21) determine the location where the individual gray wolf moves.

II. D.GWO Optimization SVM Parameter Selection

The classification effect of SVM is affected by the penalty coefficient C and the radius of the RBF kernel function σ, and it is difficult to guarantee the classification effect only based on the empirical values, so the purpose of optimization is to find suitable parameters. There have been studies using various swarm intelligence optimization algorithms to improve the parameter selection of SVM. In this paper, based on the previous research, GWO is used to optimize these two important parameters of SVM algorithm to improve the accuracy of the classification model on the one hand, and take into account the generalization ability of the model on the other hand. Finally, the classification model is applied to the IoT security intrusion detection system.The working process of GWO-SVM algorithm is shown in Figure 2.

The specific steps of GWO-SVM algorithm are as follows:

(1) Do preprocessing on the sample data, including character feature numericalization and normalization. Divide the training dataset and test dataset to prepare for subsequent SVM model fitting and validation.

(2) Initial gray wolf population size and iteration number, set the parameters C and σ of SVM as the position vector of individual gray wolves, i.e., Eq. (22):

$$X_{i,j} = \left(C_{i,1}, \sigma_{i,2}\right) \tag{22}$$

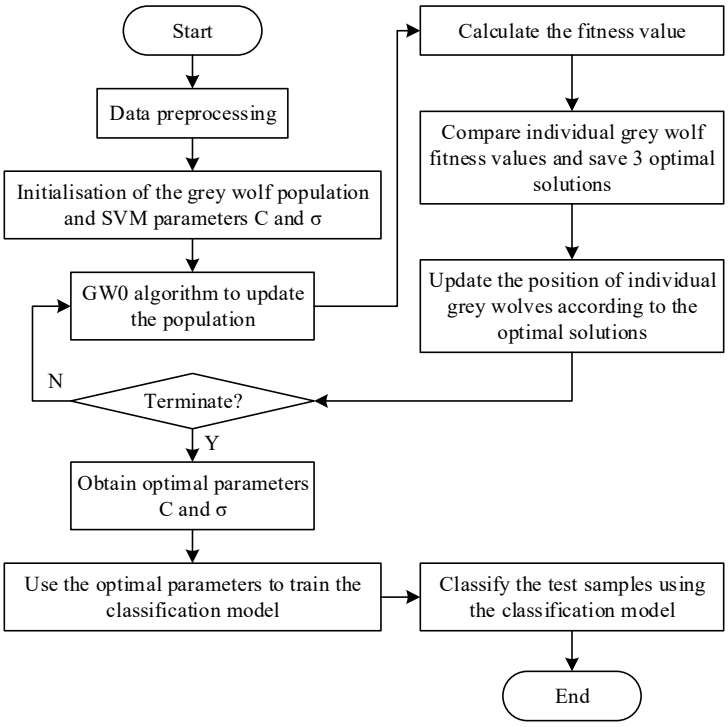

Figure 2: Workflow of the GWO-SVM Algorithm

(3) Calculate the fitness value, the classification accuracy of SVM is taken as the fitness value, and the formula is shown in equation (23):

$$fitness = TP/Total \times 100\% \tag{23}$$

where TP denotes the number of all correctly predicted samples and $Total$ denotes the total number of samples.

(4) Save the optimal top 3 fitness values and the gray wolf location.

(5) Update the parameters a, A and C in the GWO.

(6) Update the position of ω wolves based on the fitness.

(7) Determine whether the algorithm satisfies the end condition, if so, go to (8). Otherwise go to (3) to continue iteration.

(8) Obtain SVM optimal parameters $(C、\sigma)$.

(9) Train the classification model using the optimal parameters.

(10) Apply the classification model to classify the test samples.

III. Training and Application Evaluation of IoT Intrusion Detection Systems

III. A. System training and feature selection

III. A. 1) Training for RBM feature extraction

RBM is an energy-based probability distribution function, and the extraction and training of its features are of great significance in the practical application of IoT intrusion detection system. The CD algorithm is selected as the training algorithm for unsupervised learning of the detection system of this paper, which helps the detection system of this paper to obtain the internal features of the dataset. Multiple iterations training optimal $\theta = \{W, a, b\}$. The training of the detection system of this paper is divided into three parts: forward propagation, back propagation and error comparison. By comparing the predicted probability and the true distribution of the data, the KL scatter is used to measure the similarity of the two distributions, and the optimal parameters are obtained by iteratively minimizing the KL scatter.

In this simulation, the number of input neurons of the detection system is set to 45, and the number of output neurons of the system is 36, 27, 18, and 9, respectively. The reconstruction error is shown in Fig. 3, and a small reconstruction error is achieved through one sampling, which is based on the momentum gradient descent method of selecting the generation of searching for the optimal, and the reconstruction error is finally reduced to about 0.46

in the 36-dimensional reconstruction error. It can be seen that the system network in this paper can effectively extract the data features at the same time as the dimensionality reduction, to ensure that the data processed by the system network in this paper can well retain the feature information. The Y-axis is the reconstruction error of the data reduced to 9, 18, 27 and 36 dimensions, respectively, and the lower the dimensions reduced, the larger the reconstruction error.

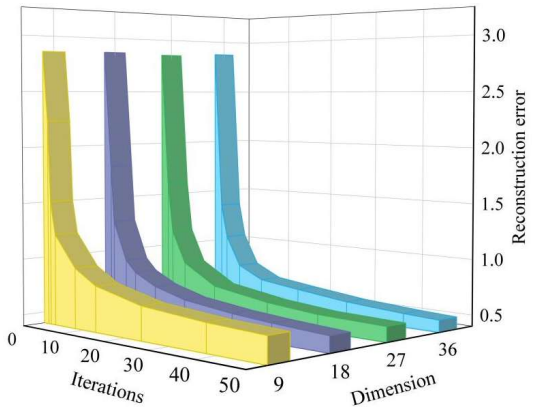

Figure 3: Reconstruction error

III. A. 2) Parameter definitions for rapid scoring

The parameters of the algorithm are many and have different roles, the meanings of some of the main parameters are as follows:

(1) Iterations: the maximum number of decision trees, default is 500.

(2) depth: the depth of the tree, the default is 6, the maximum is 16.

(3) learning_rate: the learning rate, the smaller its value indicates that the number of iterations required for training is more, the default is 0.03.

(4) loss_function: loss function, for two classification is usually used CrossEntropy or LogLoss, multi-classification when using MultiClass, the default is LogLoss.

(5) 12 leaf_reg: 12 regular parameters, default value is 3.0.

III. A. 3) Feature selection and comparison of results

In the experiments, feature selection is performed on the original intrusion information dataset in order to filter the features that contribute less to the experimental results and may even negatively affect the results. The 13 features spkts, dttl, dtcpb, synack, is_sm_ips_ports, ct_ftp_cmd, is_ftp_login, ct_state_ttl, trans_depth, swin, dwin, stcpb, dtcpb are removed from dataset A. The features are selected from the original intrusion information dataset. In order to verify the effectiveness and necessity of feature selection, experiments were conducted on dataset A with binary classification as an example, and the experimental results before and after feature selection were compared in Table 1, where “(b)” represents before feature selection. In addition to the GWO-SVM modeling algorithm designed in this paper, the modeling algorithms selected for comparison are SVM, KNN, NB, and RF.

Table 1: The experimental results before and after feature selection on dataset A

Model	Recall rate (%)	Accuracy rate (%)	Precision rate (%)	F1 value (%)	AUC (%)	Time (s)
SVM	97.81	59.21	57.98	72.72	54.53	687
SVM(b)	90.88	61.88	60.25	71.34	53.88	953
KNN	85.01	75.07	74.03	79.13	73.94	57
KNN(b)	83.9	74.23	74.88	76.9	73.9	60
NB	66.94	75.33	84.97	74.87	76.27	75
NB(b)	68.09	74.24	77.68	75.86	72.08	81
RF	97.41	85.33	79.24	87.37	83.64	114
RF(b)	83.37	80.11	76.4	83.99	83.37	127
GWO-SVM	97.97	87.46	85.14	89.73	86.33	235
GWO-SVM(b)	83.13	84.75	88.38	83.71	83.12	259

From the table, it can be seen that the experimental effect of each method has been improved after feature selection, in which the GWO-SVM model has a more significant improvement in all the evaluation indexes, and it has a significant improvement relative to that before no feature selection, which assists the GWO-SVM model in 97.97% recall, 87.46% accuracy, 85.14% precision, 89.73% F1 value, 86.33% AUC value, and all of them are the highest among the five model algorithms.NB model, KNN model, SVM model in the five model algorithms are the highest. 85.14%, F1 value to 89.73%, and AUC value to 86.33%, and all of them reach the highest among the five modeling algorithms.The NB model, KNN model, and SVM model are also improved in most of the evaluation metrics.

It is worth noting that due to the removal of redundant features, the running time of all the models is reduced, especially SVM, a model that originally had a long running time, the running time is reduced substantially. From the experimental results, it can be seen that feature selection on the original dataset can significantly improve the classification accuracy of the models.

III. B. System performance

One of the features of the UNSW-NB20 dataset is that it contains multiple types of network intrusion behavior and normal traffic. It includes nine different attack categories: Generic, Exploits, Fuzzers, DoS, Reconnaissance, Analysis, Backdoor, Shellcode, Worms, and other intrusion behaviors, making it possible to perform comprehensive evaluation and testing of intrusion detection systems. In addition, the dataset provides a rich set of features, including features based on transport, network and application layers. These features can be used to build intrusion detection models and provide in-depth analysis of network traffic.

The comparison results of the IoT intrusion detection system based on the GWO-SVM algorithm for different attack categories in the UNSW-NB20 dataset are shown in Table 2. It can be seen that the designed intrusion detection system has a precision of up to 100.00% on Analysis evaluation metrics, an F1 value of up to 99.01% on Generic evaluation metrics, and a Normal evaluation metric of Recall is as high as 99.87%. It shows that the IoT intrusion detection system based on the GWO-SVM algorithm is able to quickly recognize and detect multiple attack categories, resist the multi-polar intrusion of illegal information sources, and maintain the operation and data security of IoT.

Table 2: Textual method comparison of different attack categories in the dataset

Attack category	Precision	F1 value	Recall rate	Number
Analysis	1	0.1787	0.1076	800
Backdoor	0.618	0.0944	0.0611	706
DoS	0.5257	0.5861	0.6629	4212
Exploits	0.8338	0.79	0.7507	11255
Fuzzers	0.7383	0.818	0.9177	6185
Generic	0.9823	0.9901	0.9916	18994
Normal	0.9898	0.9869	0.9987	37123
Reconnaissance	0.9266	0.8944	0.8644	3619
Shellcode	0.6978	0.7058	0.7139	501
Worms	0.8805	0.5772	0.4325	56

IV. Conclusion

In this paper, by designing the data analysis method for IoT intrusion information to obtain the data features of the intrusion information, constructing the FSVM model to identify the abnormal data information in IoT, and combining with the GWO-SVM algorithm, we propose the IoT intrusion detection system. The system is trained with RBM feature extraction as well as feature selection, and the reconstruction error is reduced to about 0.46, and the recall (97.97%), accuracy (87.46%), precision (85.14%), F1 value (89.73%), and AUC value (86.33%) are all the best in the same category of systems. In terms of overall performance, the precision of Analysis evaluation index is as high as 100.00%, the F1 value of Generic evaluation index is as high as 99.01%, and the recall rate of Normal evaluation index is as high as 99.87%.

Funding

This work was supported by Natural Science Research Project for Anhui Universities (KJ2018A0336, KJ2021A0682, 2022AH051324, 2023AH050403, 2023AH050406, 2024AH051466), Fuyang Normal University

Open Project of Anhui Intelligent Computing and Information Innovation Application Engineering Research Center (ICII202307), Scientific Research Project of Fuyang Normal University(Analysis of Security Protocol for IoT Perception Layer Based on RFID), Fuyang Normal University Quality Engineering Project (2023JYXMSZ09, 2024XTTZTD03), Anhui Province Quality Engineering Project (2022jyxm1172, 2023jyxm0528, 2023yjshhsfkc036).

References

[1] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67, 423-441.
[2] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.
[3] Choudhary, V., Tanwar, S., & Choudhury, T. (2024). Evaluation of contemporary intrusion detection systems for internet of things environment. Multimedia Tools and Applications, 83(3), 7541-7581.
[4] Gopi, R., Sheeba, R., Anguraj, K., Chelladurai, T., Alshahrani, H. M., Nemri, N., & Lamoudan, T. (2023). Intelligent Intrusion Detection System for Industrial Internet of Things Environment. Computer Systems Science & Engineering, 44(2).
[5] Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 160, 165-191.
[6] Rebbah, M., Rebbah, D. E. H., & Smail, O. (2017, December). Intrusion detection in Cloud Internet of Things environment. In 2017 International Conference on Mathematics and Information Technology (ICMIT) (pp. 65-70). IEEE.
[7] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.
[8] Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. Sensors, 19(9), 1977.
[9] Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC, 2(04), 190-199.
[10] Guezzaz, A., Benkirane, S., & Azrour, M. (2022). A novel anomaly network intrusion detection system for internet of things security. In IoT and smart devices for sustainable environment (pp. 129-138). Cham: Springer International Publishing.
[11] Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), 1-20.
[12] Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). A deep study of novel intrusion detection systems and intrusion prevention systems for Internet of Things networks. Procedia Computer Science, 210, 94-103.
[13] Liang, C., Shanmugam, B., Azam, S., Jonkman, M., De Boer, F., & Narayansamy, G. (2019, March). Intrusion detection system for Internet of Things based on a machine learning approach. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-6). IEEE.
[14] Alqarni, A. A. (2023). Toward support-vector machine-based ant colony optimization algorithms for intrusion detection. Soft Computing, 27(10), 6297-6305.
[15] Shams, E. A., & Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24, 1821-1829.
[16] Bhati, B. S., & Rai, C. S. (2020). Analysis of support vector machine-based intrusion detection techniques. Arabian Journal for Science and Engineering, 45(4), 2371-2383.
[17] Gaye, B., Zhang, D., & Wulamu, A. (2021). Improvement of support vector machine algorithm in big data background. Mathematical Problems in Engineering, 2021(1), 5594899.
[18] Ding, S., Zhu, Z., & Zhang, X. (2017). An overview on semi-supervised support vector machine. Neural Computing and Applications, 28, 969-978.
[19] Tan, X., Yu, F., & Zhao, X. (2019). Support vector machine algorithm for artificial intelligence optimization. Cluster Computing, 22, 15015-15021.
[20] Sakr, M. M., Tawfeeq, M. A., & El-Sisi, A. B. (2019). Network intrusion detection system based PSO-SVM for cloud computing. International Journal of Computer Network and Information Security, 13(3), 22.
[21] Alghushairy, O., Alsini, R., Alhassan, Z., Alshdadi, A. A., Banjar, A., Yafoz, A., & Ma, X. (2024). An efficient support vector machine algorithm based network outlier detection system. IEEE Access, 12, 24428-24441.
[22] Jama, A. M., Khalifa, O. O., Subramaniam, N. K., & Kumar, N. (2021). Novel approach for IP-PBX denial of service intrusion detection using support vector machine algorithm. Int. J. Commun. Netw. Inf. Secur, 13, 249-257.
[23] Osanaiye, B. S., Ahmad, A. R., Mostafa, S. A., Mohammed, M. A., Mahdin, H., Subhi, R., & Obaid, O. I. (2019). Network data analyser and support vector machine for network intrusion detection of attack type. REVISTA AUS, 26(1), 91-104.
[24] Tally, M. T., & Amintoosi, H. (2021). A hybrid method of genetic algorithm and support vector machine for intrusion detection. International Journal of Electrical & Computer Engineering (2088-8708), 11(1).
[25] Zou, L., Luo, X., Zhang, Y., Yang, X., & Wang, X. (2023). HC-DTTSVM: A network intrusion detection method based on decision tree twin support vector machine and hierarchical clustering. IEEE Access, 11, 21404-21416.