Adaptive Intrusion Detection Model Based on CNN and C5.0 Classifier

Wen-Tao Hao[1], Ye Lu[2], Rui-Hong Dong[3], Yong-Li Shui[3], and Qiu-Yu Zhang[3]
(Corresponding author: Wen-Tao Hao)

Network Information Center of Xi'an Aeronautical University[1]
No.259, West-Second-Ring Road, Xian 710077, China
Email: haowentao811@163.com
School of Computer Science, Baoji University of Arts and Sciences[2]
No. 1, Gaoxin Avenue, Baoji City 721013, China
School of Computer and Communication, Lanzhou University of Technology[3]
No.287, Lan-Gong-Ping Road, Lanzhou 730050, China
(Received Jan. 7, 2022; Revised and Accepted Apr. 28, 2022; First Online May 1, 2022)

Abstract

In order to solve the problems of traditional intrusion detection methods in industrial control networks that are difficult to adaptively respond to dynamic changes in the network environment, extract valid data features, and low detection rates for unknown attacks, an adaptive intrusion detection model based on convolutional neural network (CNN) and C5.0 classifier was proposed. The proposed model first uses the synthetic minority oversampling method (SMOTE) to solve the problem of data type imbalance. Then the middle hidden layer of CNN is used to realize the automatic extraction of network traffic data features. Finally, the C5.0 classifier model is trained using the training set data extracted from CNN. An adaptive online update strategy based on frequent pattern mining is introduced so that the intrusion detection model can adapt to the dynamic changes of the network environment and then obtain the final detection result. The experiment uses KDDCup 99, NSL-KDD, and Gas Pipeline datasets to test the model's validity. Experimental results show that compared with the existing methods, the proposed model can effectively adapt to the dynamic changes of the network environment, and the classification and detection accuracy of various attack behaviors can reach over 98%. In addition, the false alarm rate is less than 2%.

Keywords: Adaptive Intrusion Detection; C5.0 Decision Tree; Convolutional Neural Network; Industrial Control Network; Synthetic Minority Oversampling

1 Introduction

With the continuous integration development of industrialization and informatization, more and more researchers pay attention to the field of network security of industrial control systems. In the industrial control network environment, while responding to traditional functional security threats, industrial control systems are also facing more and more industrial control information security threats such as viruses, Trojan horses, and hackers [7]. There are some malware (such as Stuxnet in 2010, BlackEnergy in 2013, EternalBlue in 2017, etc.) that sounded the alarm for the information security of industrial control networks [26]. Therefore, research on the security of industrial control networks has very important research significance [1].

In view of the security problems of industrial control networks, traditional industrial control security technologies, such as user authentication, firewall, and data encryption, can no longer cope. As the second line of defense of industrial control network information security, intrusion detection technology can effectively make up for the shortcomings of traditional industrial control security technology [24]. Intrusion detection technology extracts data characteristics that reflect system behavior, and classifies attack behavior and normal behavior data through a designed detection algorithm. Due to the continuous improvement of network intrusion technologies and methods, no matter whether it is misuse detection or anomaly detection, satisfactory results can not be obtained [3]. In recent years, scholars have combined intrusion detection technology with the current mainstream algorithms to extend new research directions. They have successively applied mature intrusion detection technologies such as machine learning, data mining, deep learning and so on to the intrusion detection of industrial control networks, and constantly innovating, especially machine learning techniques, such as support vector machines, Bayesian networks, decision trees and other methods [18] have achieved good results. However, due to the

diversification of network intrusions and the imbalance of intrusion data classes, intrusion detection technology cannot detect some new or unknown forms of attacks, cannot adapt to the dynamic changes of the network environment, and cannot achieve the global scope of intrusion detection functions, resulting in low detection efficiency [6, 15, 22]. In addition, with the increase of heterogeneous networks, the network environment has become more and more complex, and the attack behaviors and methods of intruders are constantly evolving and updating. Because of the continuous appearance of unknown intrusions and the dynamic changes of the network environment, the detection rate of the intrusion detection model may be low and the false alarm rate is high. The adaptive intrusion detection technology is an important mechanism for the dynamic changes of the network environment. Which can make the intrusion detection model adapt to the dynamic changes of the network environment and improve the detection rate [19].

In order to reduce the influence of the dynamic changes of the network environment on the accuracy of the intrusion detection model, to better extract effective data features and improve the detection performance of the intrusion detection model, we presents an adaptive intrusion detection model based on CNN and C5.0. The proposed model first preprocesses the dataset. Then, the pooling layer in CNN is used to transform one-dimensional data into multidimensional data, and the optimal features are selected by CNN adaptive. Finally, the optimal features selected by CNN is used to train and detect C5.0 classifier, and an adaptive online update strategy of frequent pattern mining is introduced in the detection process, so that the intrusion detection model can adapt to the dynamic changes of the network environment. The main contributions of this paper are as follows:

1) The hidden layer of CNN is used to realize automatic extraction of network traffic data features. In the process of feature extraction, synthetic minority oversampling is used to solve the problem of data class imbalance.

2) Combining CNN with C5.0 classifier realizes the optimal classification of normal and attack behavior in the intrusion detection model.

3) In the C5.0 classification and detection process, an adaptive online update strategy based on frequent pattern mining is introduced, so that the intrusion detection model can adapt to the dynamic changes of the network environment, and has a high detection rate for known and unknown attacks.

The remaining part of this paper is organized as follows. Section 2 introduces related work. Section 3 introduces related theories in detail. Section 4 describes the proposed adaptive intrusion detection model and related methods. Section 5 gives the experimental results and performance analysis as compared with existing methods. Finally, we conclude our paper in Section 6.

2 Related Work

The dynamic changes of the network environment and the detection of unknown attacks are the main challenges faced by intrusion detection models in current industrial control networks. Therefore, the intrusion detection model that can adapt to the dynamic changes of the network environment and the detection of new intrusion attacks is called an adaptive intrusion detection model. Many researchers at home and abroad have applied mature intrusion detection technologies such as data mining, machine learning, and deep learning into the research of the adaptive intrusion detection model.

Combining data mining with adaptive intrusion detection technology can dig out the deep features of the data, so that intrusion detection has a certain adaptive ability. For example, Ref. [17] used data mining methods to detect abnormal behaviors in incoming datasets, and proposes an intrusion detection system based on self-learning technology. Ref. [21] proposed a knowledge-based intrusion detection strategy for current wireless sensor networks, which is used to detect various forms of attacks under different network structures. Ref. [13] proposed an adaptive network intrusion detection method based on fuzzy rough set feature selection and GA-GOGMM model learning, which can effectively adapt to the dynamic changes of the network environment and can detect various intrusion behaviors in real network connection data in real time.

At present, there have been many related works applying machine learning methods to adaptive intrusion detection. Such as, Ref. [19] proposed an incremental machine learning classifier for intelligent detection and analysis of network data streams. This is an adaptive intrusion detection model (AIDM) based on machine learning technology and feature extraction, which can detect unknowns attack. In order to detect unknown attacks in real-time network traffic, Ref. [2] proposed an adaptive intrusion detection system using multi-layer hybrid support vector machine and extreme learning machine technology to detect and learn unknown attacks in real time. Setareh Roshan et al. [23] proposed an adaptive design method of intrusion detection system based on extreme learning machine, which improved the rapid learning and real-time detection capabilities of intrusion detection system. Ref. [14] proposed an adaptive network intrusion detection (ANID) method based on kernel extreme learning (KELMs) random feature selection integration. This method updates the intrusion detection model according to the dynamic changes of the network environment, guarantees the adaptive ability of the intrusion detection model, and achieves high detection accuracy for both known and unknown attacks, and improves the detection efficiency. In [25], in response to the class imbalance problem in the intrusion data set, the synthetic minority oversampling technique (SMOTE) is used to balance the data set, and then the random forest training classifier is used for intrusion detection.

In recent years, deep learning has been widely used in

the field of intrusion detection and has certain advantages. Ref. [20] proposed an adaptive misuse intrusion detection system combining self-learning and APE-K framework, which can detect unknown attacks by using deep learn-based methods in network environment changes. Chu Ankang et al. [4] proposed an industrial controlled intrusion detection method based on multi-classification long-short memory model, which has good detection accuracy, but cannot accurately detect unknown attacks in high-dimensional and complex changing network environments. Ref. [9] proposed an industrial control detection scheme based on deep learning methods. Deep learning methods can automatically extract key features to achieve accurate attack classification. Ref. [10] proposed an intrusion detection method using multi-CNN fusion method for deep learning, which fully contributes to the data of the Industrial Internet of Things. In [28], for the problem of data class imbalance,put forward the technique of combining SMOTE and the Gaussian mixture model (GMM), and unbalanced processing is combined with a convolutional neural network. Ref. [11] proposed a new feature-level IDS based on convolutional neural networks, and achieved good performance.

Through the above analysis, it can be seen that both data mining and traditional machine learning methods can effectively improve the detection rate, but both have weak adaptability to dynamic changes in the network environment and low detection rate for unknown attacks. Intrusion detection based on deep learning has the advantage of detecting unknown attacks, and can automatically identify different attack characteristics, so as to find potential security threats more efficiently. Therefore, in view of the weak adaptive ability of intrusion detection technology in industrial control networks to dynamic changes in the network environment, difficulty in extracting valid data features, and low detection rate of unknown attacks, this paper proposes adaptive intrusion detection model based on CNN and C5.0 classifiers. The model uses CNN to automatically select the features of the dataset, then uses the C5.0 classifier for training and detection, and introduces an adaptive update strategy for frequent pattern mining.

3 Related Theories

3.1 Convolutional Neural Network Model

CNN [8] generally consists of a convolutional layer part and a fully connected layer part, where the number of convolutional layers and pooling layers of CNNs with different structures is different. CNN uses a back-propagation learning process, that is, input training data in the input layer. Then the predicted value is calculated through the calculation of the convolutional layer, the pooling layer, the fully connected layer and the output layer. Finally, the error function is used to calculate the difference between the real value and the predicted value, so as to achieve the purpose of reverse iteration to update the network weights and thresholds. The structure of CNN is shown in Figure 1.

Convolutional layer: The convolutional layer is the core part of CNN. The feature extraction module in CNN is composed of a combination of multiple convolutional layers. In the convolutional layer, the input feature map and the convolution kernel are convolved and biased, and then a non-linear activation function is used to obtain the feature map of the new layer. The current convolution feature is obtained by the convolution operation of the convolution kernel and the output feature of the previous layer. Its definition is shown in Equation (1):

$$Y_j^a = \sum_i X_i^{a-1} * T_{ij}^{a-1} + b_j^a \tag{1}$$

where Y_j^a represents the input of the jth position in the ath layer feature after the convolution operation, X_i^{a-1} represents the ith input matrix in the a-1 layer, T_{ij}^{a-1} represents the convolution kernel connecting the ith input matrix and the jth position between the ath layer and the a-1th layer, and b_j^a is the offset of the jth position in the features of the ath layer.

After the calculation of Equation (1), the obtained matrix needs to undergo nonlinear activation, which can strengthen the nonlinear expression ability of the network. Commonly used activation functions are Sigmoid, Relu, etc. Pooling layer: The pooling layer is sampled under the output feature map of the convolutional layer. Under the premise of retaining the main features of the data, the data features are reduced in dimensionality, which increases the generalization ability of the neural network and achieves the removal of redundancy. The effect of this also reduces the complexity of the entire network.

Fully connected layer: The fully connected layer acts as a classifier in the entire CNN, that is, after convolution, activation function, pooling and other deep networks, the results are identified and classified through the fully connected layer. The calculation formula is shown in Equation (2):

$$y_j^a = \sum_i K_{ij}^a * x_i^{a-1} + b_j^a \tag{2}$$

where y_j^a is the calculated output result of the jth neuron in the fully connected layer t, K_{ij}^a represents the connection weight value of the ith feature in the a-1th layer and the jth neuron in the ath layer, x_i^{a-1} represents the ith eigenvalue of the features of the a-1 layer, which is the offset of the jth neuron in the fully connected layer a.

After the feature data passing through the convolutional layer and pooling layer pass through the last classification prediction layer, the classification and prediction results can be obtained.

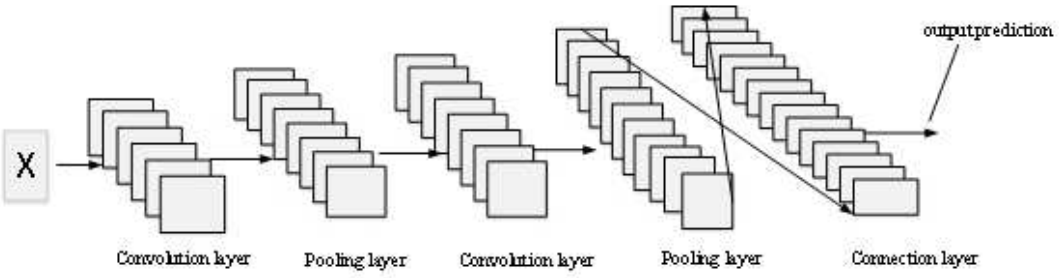


Figure 1: Structure diagram of CNN

3.2 Synthetic Minority Oversampling (SMOTE)

In order to solve the problem of data class imbalance, a synthetic minority oversampling is used to preprocess the training set data. Synthetic minority oversampling [24] is an improved scheme based on random oversampling, because random oversampling is prone to the problem of model overfitting, which makes the information learned by the model too special and not general enough. Synthetic minority oversampling changes the data distribution of the unbalanced dataset by adding the generated minority samples, and synthesizes new samples between two minority samples by linear interpolation, thereby effectively alleviating the overfitting caused by random oversampling problem. The specific process of synthesizing minority oversampling is:

Step 1. Calculate the K-nearest neighbor sample set of each sample V_i of the minority class in the training set.

Step 2. Analyze the proportion of the majority in the sample set, and then judge whether V_i is a boundary sample, if it is, add the boundary sample set; otherwise, put it back into the minority sample set.

Step 3. The boundary sample V_i is oversampled to generate a new minority sample V_new, whose definition is shown in Equation (3):

$$V_{new} = V_i + rand(0,1) \times \mid V_j - V_i \mid \tag{3}$$

where j=1,2,...,n, n represents the number of samples selected randomly according to the sampling ratio, and $rand$(0,1) represents the random number [0,1].

3.3 C5.0 Decision Tree

The C5.0 decision tree [27] classification algorithm is a new classification algorithm that is improved on the basis of the C4.5 classification algorithm. The decision tree construction idea of C5.0 algorithm is consistent with that of C4.5 algorithm, and C5.0 algorithm also includes all the functions of C4.5 algorithm. The difference from the C4.5 algorithm is that the C5.0 algorithm introduces Boosting technology and cost matrix construction technology.

Compared with the C4.5 algorithm, the improvements of the C5.0 decision tree algorithm are: C5.0 runs much faster than the C4.5 decision tree algorithm, C5.0 usually uses less memory than C4.5, and the number of C5.0 trees is less than C4.5.

4 The Proposed Model

4.1 Adaptive Intrusion Detection Model Based on CNN and C5.0

Aiming at the problem of the dynamic changes of the network environment in the industrial control system, in order to improve the adaptability of the intrusion detection model in the dynamic environment, this paper uses a series of algorithms for synthesizing minority oversampling, CNNs, C5.0 decision trees and frequent pattern mining combined, an adaptive intrusion detection model is designed. The model is mainly composed of data preprocessing, classification representation, matching update and attack response. Figure 2 shows the structure of an adaptive intrusion detection model based on CNN and C5.0 classifier.

It can be seen from Figure 2 that the model first uses the hidden layer of the CNN to realize the automatic selection of data features and reduce the dimension of data features. Then use the training set data to train the C5.0 classifier model to obtain the classification of the normal library and the abnormal library. Finally, an adaptive matching update mechanism is introduced, by introducing frequent pattern mining, real-time matching and updating the normal database and abnormal database, to ensure the adaptability of the model, and realize the detection of various attack behaviors, thus improving the network intrusion detection model performance.

The detailed processing steps of the adaptive intrusion detection model are as follows:

Step 1. Data preprocessing. Firstly, the original dataset is preprocessed, the digitized character type in the dataset is integer, and the attribute feature value is normalized. For the problem of data imbalance in the training dataset, a synthetic minority oversampling method is used to deal with it.

Step 2. Feature selection. CNN is used to automatically

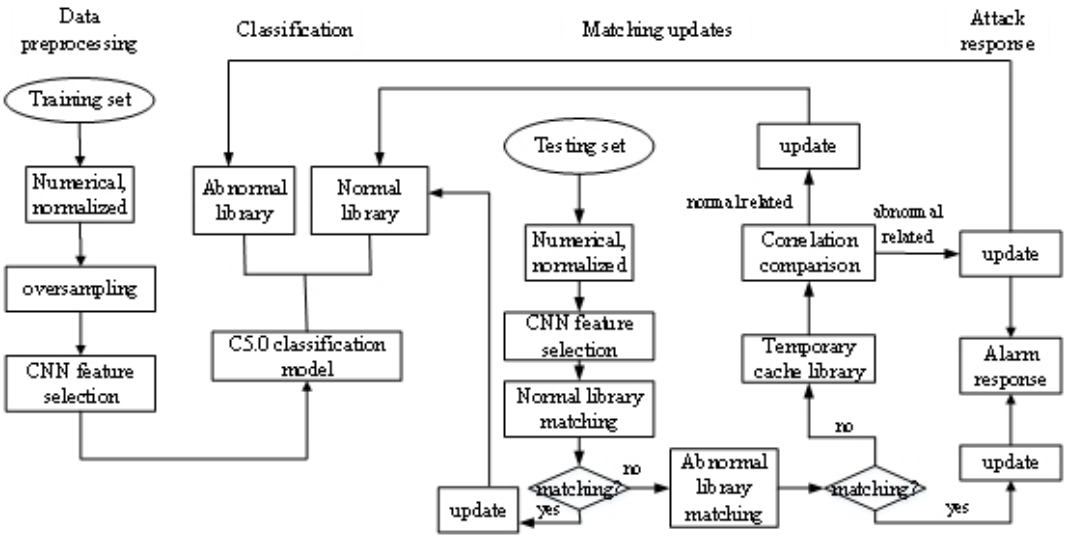


Figure 2: Flow chart of adaptive intrusion detection model processing based on CNN and C5.0 classifier

select data features of the preprocessed data and reduce the dimension of data features.

Step 3. The classification database is formed, and the C5.0 classifier model is trained using the training set data to obtain the normal library and the abnormal library.

Step 4. Matching and update, in view of the dynamic changes of the network environment, in order to improve the adaptability of the intrusion detection model in the dynamic environment, an adaptive matching update mechanism is introduced. By building a temporary cache library, the data that does not match the normal library and the intrusion library is added to the temporary cache library.

A. The test set data M is searching and matching with the normal database. If a type that matches M is found in the normal library, update the data, mark M as normal, and re-execute this step to detect new samples; if it does not match, execute step B.

B. Search and match M in the exception library. If a type that matches M is found, the alarm responds, and the update is performed at the same time, ending the processing of this record, and returning to step A to test the new sample; if it does not match, proceed to the next step.

C. Update the cosine similarity by comparing the cosine similarity with normal and abnormal in the temporary cache library, and mark the high similarity with normal as normal, otherwise, mark as abnormal.

Step 5. Attack response, through the matching update, and the intrusion behavior matching the abnormal library for alarm response. The behaviors that are highly related to intrusions in the temporary cache library also respond to alarms.

4.2 CNN Construction

The CNN network can use the hidden layer to learn the local features of the data layer by layer, and extract the data features in the spatial dimension. The preprocessed network traffic data features are input into the CNN network, and the CNN features are output from the output layer after layer-by-layer learning. Figure 3 shows the CNN model used in this paper.

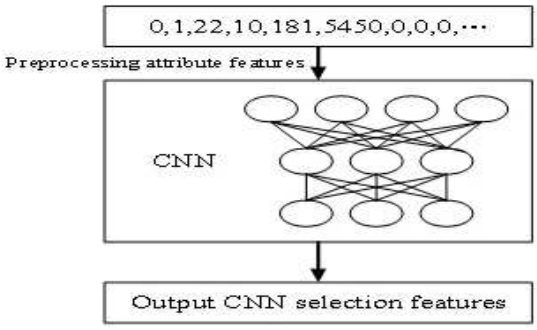


Figure 3: CNN model diagram

4.3 C5.0 Classifier Training

In the C5.0 classifier algorithm, Boosting technology usually stacks multiple C4.5 weak classifiers into one strong classifier. The algorithm inputs the training dataset into the classifier, and trains the weak classifiers one by one in the order of a ladder-like training process. Each time the training set of the weak classifier is transformed according to a certain strategy, and finally the weak classifier is combined into a strong classifier in a certain way.

In the proposed model, the Boosting algorithm is added to the C5.0 algorithm through the C5.0 function. In the C5.0 function, the role of the trials parameter is to control the number of C4.5 decision trees and to enhance the classification performance of the C5.0 model. After building the C5.0 classifier, start training the C5.0 classifier. By adjusting the specific values of parameters such as trials, the model is optimized, so that the model can achieve better classification performance. Figure 4 is a flow chart of C5.0 classifier construction and classification.

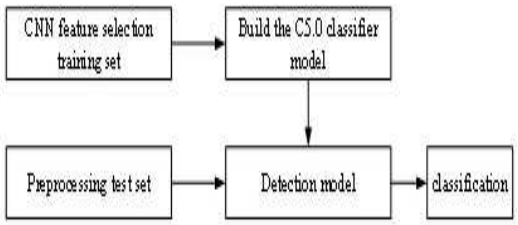


Figure 4: C5.0 classifier construction and classification flow chart

4.4 Adaptive Matching Update Strategy

In order to improve the weak adaptability of the intrusion detection model to the dynamic changes of the network environment, this paper introduces an adaptive matching update strategy. By building a temporary cache library, data that does not match the normal library and the abnormal library is added to the temporary cache library. Each type of data in the temporary cache library has a value, and when a new record matches this type, the value of the type is increased by 1. By analyzing the similarity between the type and the normal type or abnormal type, it is determined to add this type to the normal or abnormal library for dynamic matching and updating. In matching and updating, the cosine similarity is used to measure the similarity between the object to be detected and the corresponding type for matching and updating. The calculation method of cosine similarity is as Equation (4):

$$d(x, y) = x^T y / \| x \| \| y \| \quad (4)$$

where $d(x, y)$ represents the cosine matching degree between the sample x and the type y to be detected. The larger the value, the higher the matching degree (representing the smaller the angle between x and y).

Figure 5 is a flow chart of adaptive matching update strategy processing.

5 Experimental Results and Analysis

The experimental environment of this paper is Intel Core i5-4210U 2.49ghz,8G,Windows 10(64-bit). The programming language is python3 and R, deep learning uses the Keras deep learning framework based on Tensorflow, and data preprocessing uses weka 3.8.3. The experimental dataset selected three datasets: KDDCup 99 [16], NSL-KDD [5] and Gas Pipeline [12].

In the feature selection experiment, in order to prevent the imbalance of data types from causing more false positives, a few synthetic oversampling methods are used for data preprocessing, and then the hidden layer in CNN is used for data feature selection, setting the Dropout rate to 0.5 and hiding in the middle The layer activation function is Relu, and use Root Mean Square Prop (RMSProp) as the optimization function. Since one-hot encoding is not used when digitizing attributes and labels, and numerical encoding is used directly, the model in this paper uses Sparse Categori-Calcrossentropy as the loss function of the network. The initial learning rate of the model is 0.0001. In the classification experiment, for the C5.0 classifier model, set the trial parameter value to 10, and select the default parameters for other parameters. In the model feature learning stage, the most representational feature subset is extracted by constantly adjusting the value of the intermediate feature extraction layer. The adaptive matching updating mechanism is used to integrate the matching updating classification of test set data, judge whether it is abnormal or normal behavior, and divide it into correct classification. In addition, in order to prove the superiority of the intrusion detection performance of this method, the existing four classifiers of RF, SVM, C4.5 and KNN were compared.

5.1 Dataset Description

5.1.1 KDDCup 99 Dataset

KDDcup 99 [16] is one of the most widely used intrusion detection data sets. It contains 4.9 million attack records, which are divided into training sets and test sets. The training set contains one normal type and 22 attack types, while the test set contains another 17 unknown attacks. The included corrected is the test sample set, which includes 17 abnormal types that do not appear in the 10% training set to test the generalization ability of the model.

Each traffic record in the KDDcup 99 dataset consists of 41 feature attributes and 1 class label, containing three main types of features: Attributes 1-10 are the basic features of network connections, attributes 11-22 are the content features of network connections, and attributes 23-41 are the traffic features.

According to the features of the dataset attack, it is divided into the following four types of attacks: denial of service attacks (DoS), probe attacks (Probe), user to root attacks (U2R), root to local attacks (R2L). Some specific types of attacks only appear in the test set, which provides a more realistic theoretical basis for intrusion detection. The specific data information of the KDDcup 99 data set is shown in Table 1.

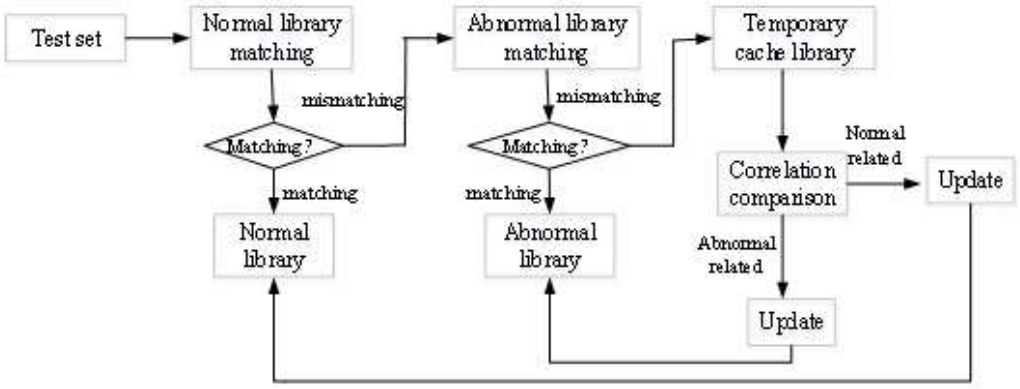


Figure 5: Adaptive matching update policy processing flow

Table 1: KDDcup 99 (10%) experimental dataset attack types and numbers

Classes	Training Data	Testing Data
Normal	97,278	60,593
Dos	391,458	22,985
Probe	4107	4166
R2L	1126	16,189
U2R	52	228

5.1.2 NSL-KDD dataset

The NSL-KDD dataset [5] is an improvement of the KDD99 dataset: (1) The training set of the NSL-KDD dataset does not contain redundant records, so the classifier will not be biased towards more frequent records; (2) There is no duplicate record in the test set of NSL-KDD dataset, which makes the detection rate more accurate; (3) The number of selected records from each difficulty level group is inversely proportional to the percentage of records from the original KDD dataset. The classification rates of different machine learning methods vary over a wider range, making accurate assessments of different learning techniques more effective; (4) The setting of the number of records in training and testing is reasonable, which makes the cost of running the experiment on the whole set of experiments low without having to randomly select a small part.

The specific data information of the NSL-KDD dataset is shown in Table 2.

Table 2: NSL-KDD dataset attack types and numbers

Classes	Training Data	Testing Data
Normal	67,343	9711
Dos	45,927	7458
Probe	11,656	2421
R2L	959	2754
U2R	52	200

5.1.3 Gas Pipeline

The industrial control system intrusion detection dataset Gas Pipeline [12] disclosed by Mississippi State University is a laboratory simulation-scale industrial control system network dataset based on Modbus application layer protocol. The dataset includes 1 type of normal data and 7 types of different attack data. Each record contains 26 traffic features and category labels. The dataset includes network traffic, process control and process measurement features. The dataset is captured by a network data logger, which monitors and stores Modbus traffic information from RS-232C connections, including normal, reconnaissance attack, and Response Injection (RI) attacks and Command Injection (CI) attacks and DoS attacks. This paper selects 80% of the natural gas pipeline dataset as the training set and 20% as the test set. The specific data information of the natural gas pipeline dataset is shown in Table 3.

Table 3: Types and numbers of attacks on the natural gas pipeline dataset

Classes	Training Data	Testing Data
Normal	86,137	128,443
Recon	1519	2268
NMRI	3079	4674
CMRI	5133	7902
MSCI	3044	4856
MPCI	8130	12282
MFCI	1951	2947
DoS	858	1318

5.2 Data Preprocessing

5.2.1 Data Oversampling

Due to the problem of data imbalance in the original dataset used in this paper, the learning algorithm will be biased towards records that appear more frequently. Therefore, this paper adopts the synthetic minority oversampling method to oversampling the minority boundary samples to make the synthesized sample distribution more

reasonable.

5.2.2 Data Transforming

The KDDcup 99 dataset and NSL-KDD dataset have 38 numerical characteristics and 3 non-numerical characteristics, such as protocol type, service, and label. The classification modules of the intrusion detection model all need to calculate the numerical flow features, so non-numerical features must be converted into numerical features. For instance, the protocol_type feature in the NSL-KDD dataset contains three types of protocols, namely TCP, UDP and ICMP, which are replaced by 1, 2, and 3 respectively. As well, the 70 service attributes and 11 flag attributes in the dataset are also numeralized in the same way. The character-type features in the Gas Pipeline dataset are also digitized in the same way.

5.2.3 Data normalization

Data normalization is a process of scaling the value of each attribute to a relatively good range, in order to eliminate the preference for features with larger values from the dataset. Since the KDDcup 99 dataset, NSL-KDD dataset and the Gas Pipeline dataset have data with no fixed upper and lower bounds and continuous values. Therefore, it is necessary to use min-max standardization to map the feature data to the standard range of [0, 1], and each feature is standardized using Equation (5):

$$f(x) = (x - min)/(max - min), x\epsilon[min, max] \quad (5)$$

where x is the feature in the dataset, min and max are the minimum and maximum of feature x. The normalized data can be directly input into the intrusion detection model.

5.3 Evaluation Indexes

To evaluate the performance of the intrusion detection model, Accuracy (Acc), Precision (Precision) andfalse alarm rate (FAR) [5] are used to measure the performance of the model. When evaluating the effectiveness of the model, most commonly used indicators can be calculated from the confusion matrix in Table 4.

Table 4: Confusion matrix

True value	Predictive value	
	Normal	Abnormal
Normal	TP	FN
Abnormal	FP	TN

In Table 4, TP indicates that the true value is a normal sample and is predicted to be the number of normal samples. FN indicates that the true value is a normal sample and is predicted to be the number of abnormal samples. FP indicates that the true value is an abnormal sample and is predicted to be the number of normal samples. TN means that the true value is an abnormal sample and is predicted to be the number of normal samples.

Accuracy (Acc): Accuracy represents the percentage of the dataset that the model correctly classifies the true value of the sample. When the various samples in the dataset are relatively average, this is a good measure. However, when the various types of samples is unbalanced, it cannot reflect the true classification effect of the model. The calculation formula is as follows:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \quad (6)$$

Precision: It represents the probability of actually being a positive sample among all the samples predicted to be positive. The calculation formula is as follows:

$$Precision = TP/(TP + FP) \quad (7)$$

False alarm rate: The false alarm rate is the ratio of the number of false positive records to the total number of normal records, reflecting the proportion of false alarm records in normal records. The formula is as follows:

$$FAR = FP/(FP + TN) \quad (8)$$

5.4 Performance Analysis

5.4.1 Influence of adaptive online update on the model

When adaptive online matching is updated, a frequent pattern threshold needs to be given to determine whether a new sample belongs to a frequent pattern, and then the pattern library is updated. In this paper, the mode attenuation parameter is 0.0001 in the experiment, and different frequent mode thresholds (100, 500, 1000) are selected at the same time to test the influence of different frequent mode thresholds on the model. The experimental results are shown in Figure 6.

As can be seen from Figure 6 that in the experiment, different frequent pattern thresholds have different influences on the accuracy and false alarm rate of the proposed model. The higher frequent threshold in the initial stage has a higher accuracy rate, with the increase of experimental data, the lower the frequent threshold, the higher the accuracy rate. Obviously, the smaller frequent threshold is faster than the adaptive online update strategy, which makes the normal library and abnormal library update more timely, and can ensure a higher intrusion detection accuracy rate. However, some fuzzy and frequent instances will be mistakenly introduced into the unmatched pattern library, which will lead to a high false alarm rate in the proposed model. Therefore, in order to obtain a higher detection rate and a lower false alarm rate, in the initial stage of the experiment, due to the fewer types of abnormal libraries and the large amount of data in the test set, the threshold of frequent patterns was first set to be larger. With the gradual increase in the types of the normal library and the abnormal library,

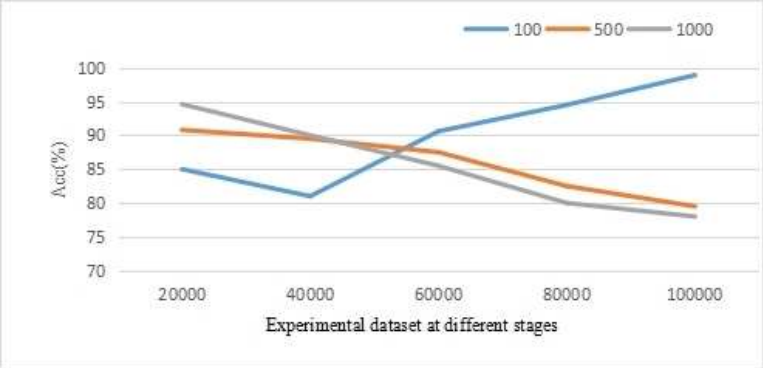


Figure 6: Experimental results of different frequent pattern mining thresholds

the correlation between most data and the normal library and the abnormal library is obviously increased, and the frequent pattern threshold can be automatically reduced according to the decrease in the amount of data in the temporary cache library.

5.4.2 Performance Comparison of CNN Feature + C5.0 Binary Classification Experiment

In order to evaluate the performance of the adaptive intrusion detection model combining the features of the intrusion detection dataset learned by CNN and the C5.0 classifier, ROC curve is used to represent the classification performance of C5.0, RF, SVM, C.4.5 and KNN. On the one hand, it can reflect the representativeness of the CNN selected features, on the other hand, it can also get the classification performance of different classifiers for the same feature. In addition, in the experiment, CNN was used to extract the depth features of three different datasets of KDDcup99, NSL-KDD and Gas Pipeline to illustrate the applicability of the CNN model.

Figure 7 shows the ROC curves of the three different datasets of KDDcup99, NSL-KDD and Gas Pipeline in C5.0, RF, SVM, C.4.5 and KNN.

It can be seen from Figure 7 that the classification AUC values of the C5.0 classifier in the three datasets KDDcup99, NSL-KDD and Gas Pipeline are 99.7%, 92.8% and 98.8%, respectively. In Figure 7(a), there are repeated records and large amount of data in KDDcup99 dataset, which results in the weak performance of KNN classifier. In Figure 7(b), because the NSL-KDD dataset removes redundant data and there are a certain number of unknown attacks, the classification performance of the KNN classifier is weaker than that of other classifiers. In Figure 7(c), the reason for the low AUC value of the SVM and KNN classifiers is that the synthesis minority oversampling methods solves the problem of unbalanced data classes in the Gas Pipeline dataset. The sample classes are combined with close neighbors to affect the SVM and KNN, The nearest neighbor synthesis of sample classes affects the classification performance of SVM and KNN.

Table 5 shows the two-class performance comparison between the method C5.0 and the four machine learning classifiers of RF, SVM, C4.5 and KNN under the three indicators of Acc, Precision and FAR.

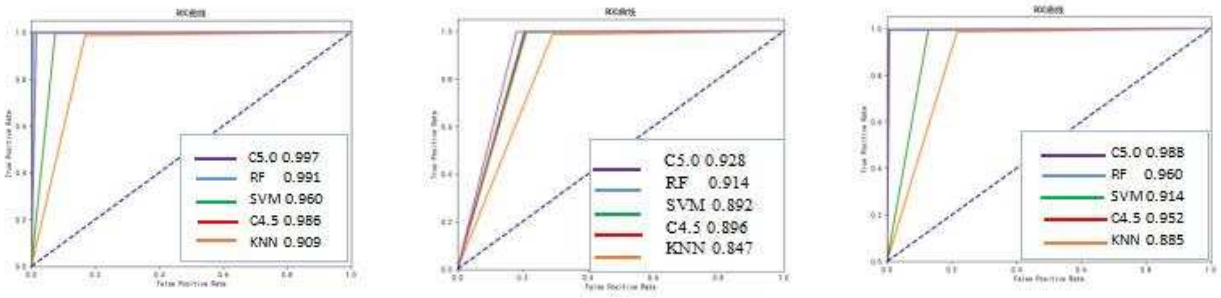
As can be seen from Table 5 that the classification Acc values of the C5.0 classifier used in this paper in the three data sets of KDDcup99, NSL-KDD and Gas Pipeline are 99.87%, 98.23% and 99.80%, respectively, compared with the performance of the other four classifiers optimal. KNN has the lowest classification performance on the KDDcup99 and NSL-KDD datasets and the highest false alarm rate. The SVM classifier has the lowest classification performance on the Gas Pipeline dataset, and the highest false alarm rate is still KNN. Therefore, the performance of the proposed method is the best.

5.4.3 Performance Comparison of CNN Features + C5.0 Multi-classification Experiments

Table 6 shows the detection results of the four different attack types and normal traffic in the KDDcup99 dataset in this paper, and compares them with the Acc of the SMOTE+ENN method [15] and the RTMAS method [2].

It can be seen from Table 6 that the proposed method has achieved 95.42%, 93.29%, 69.23%, and 86.90% for the attack test ACC of Dos, Probe, U2R, and R2L in the KDDcup99 dataset, respectively, and the classification Acc for Normal state reaches 98.69%, compared with the Acc and Normal Acc of the three attacks of Probe, U2R, and R21 obtained in the Ref. [15] are higher, while the proposed method has lower Acc for Dos detection. Compared with the Acc obtained in the Ref. [2], the proposed method has a higher Acc for Normal and Probe, U2R, and R2l attacks, but the detection accuracy rate for Dos attacks is still low, mainly because of the influence of the specific features selected by CNN on the detection accuracy of Dos attack. In some attacks, the similarity between U2R attacks and normal samples is as high as 100%, when the detection rate of normal behavior increases, the detection accuracy of U2R decreases compared to other attacks.

Table 7 shows the detection results of four different attack types and normal traffic in the NSL-KDD dataset by the proposed method, and compares them with the



(a) KDDcup99 (b) NSL-KDD (c) Gas Pipeline

Figure 7: Comparison of ROC curves of different datasets under five classifiers

Table 5: Comparison of the two classification performance of different classifiers with CNN features

Classifier	KDDcup99			NSL-KDD			Gas Pipeline		
	Acc(%)	Precision(%)	FAR(%)	Acc(%)	Precision(%)	FAR(%)	Acc(%)	Precision(%)	FAR(%)
C5.0	99.87	99.87	0.96	98.23	98.0	1.28	99.80	98.63	1.68
RF	98.17	97.69	1.43	96.82	95.96	1.36	97.40	96.67	2.16
SVM	95.62	94.05	2.02	93.14	92.89	2.05	92.53	92.08	3.65
C4.5	97.60	97.41	1.80	97.45	96.40	1.92	96.59	95.86	2.60
KNN	93.72	93.01	3.45	91.06	90.67	2.56	93.28	92.78	3.89

Table 6: The detection accuracy of five classifications based on KDDcup99 dataset

Method	Acc(%)				
	Normal	DoS	Probe	U2R	R2L
The proposed method	98.69	95.42	93.29	69.23	86.90
SMOTE+ENN [15]	98.68	97.23	84.38	55.0	42.02
RTMAS [2]	97.87	99.79	91.86	24.68	35.90

Acc of the AEML method [6] and the CNN method [11].

It can be seen from Table 7 that the proposed method has achieved 98.16%, 96.08%, 86.34%, and 90.18% in the attack test of Dos, Probe, U2R, and R2L in the NSL-KDD dataset, respectively, and the classification Acc for Normal reaches 97.03%. Compared with Acc in Ref. [6], the proposed method has a higher detection accuracy for DoS, Probe, U2R, R2L and Normal. Also compared with the Acc in Ref. [11], the detection accuracy of the proposed method for R2L attacks is 1.64% lower than that of the Ref. [11], and the detection accuracy of the other attacks is higher.

In order to further verify the performance of the proposed model, this paper uses the Gas Pipeline dataset to conduct a verification experiment. Table 8 shows the eight-category Acc detection performance of the proposed method on the Gas Pipeline dataset, and compares it with the detection accuracy of the GoogLeNet-LSTM method [4] and the CNN-BiLSTM method [24].

As can be seen from Table 8, the detection accuracy of the proposed method in NMRI, CMRI, MSCI MPCI, DoS and Normal is significantly higher than that in Ref. [4]. The detection accuracy of the GoogLeNet-LSTM method in Ref. [4] for both Recon and MFCI attacks is 100%, and the detection accuracy of the proposed method is lower than the Acc in Ref. [4]. Also compared with Ref. [24], the detection accuracy rate of the proposed method for NMRI, MSCI, MPCI, DoS, MFCI attacks is higher, while the detection accuracy rate for Normal, Recon and CMRI is slightly lower than that of the Ref. [24].

5.5 Performance Comparison with Existing Methods

In order to further highlight the performance of the proposed method, the performance of the proposed method is compared with the existing method [1, 2, 4, 9, 11, 13, 14, 19, 20, 23, 25], Table 9 and Table 10 are the results of binary classification and multiple classification performance comparison between the proposed method and the existing method on three different datasets: KDDcup99, NSL-KDD and Gas Pipeline.

It can be seen from Table 9 that the Acc value based on the proposed model in the KDDcup99 dataset is higher than AIDM-DL4JMLP [19] and SMOTE-RF [25]. The proposed method is higher than DL-AIDS [20] and CNN [11] in the two-class detection Acc on the NSL-KDD

Table 7: The detection accuracy of five classifications based on NSL-KDD dataset

Method	Acc(%)				
	Normal	DoS	Probe	U2R	R2L
The proposed method	97.03	98.16	96.08	86.34	90.18
AEML [6]	94.93	84.37	87.11	25	55.27
CNN [11]	82.40	92.19	64.32	64.52	91.82

Table 8: The detection accuracy of eight classifications based on Gas Pipeline dataset

Method	Acc(%)							
	Normal	Recon	NMRI	CMRI	MSCI	MPCI	MFCI	DoS
The proposed method	98.45	97.10	96.82	97.64	98.55	99.02	98.90	98.20
GoogLeNet-LSTM [4]	97.83	100	96.50	96.78	96.97	97.21	100	97.33
CNN-BiLSTM [24]	99.8	100	92.2	98.8	93.9	98.0	91.8	98.1

Table 9: Results of two-class classification performance comparison with existing methods

Method	Dataset	Acc(%)	FAR(%)
AIDM-DL4JMLP [19]	KDDcup99	97.9	N/A
SMOTE-RF [25]	KDDcup99	92.57	N/A
DL-AIDS [20]	NSL-KDD	77.99	0.4
CNN [11]	NSL-KDD	85.07	9.71
AEDL-ICS [1]	Gas Pipeline	95.86	N/A
CNN-ICS [9]	Gas Pipeline	99.46	N/A
The proposed method	KDDcup99	99.87	0.96
	NSL-KDD	98.23	1.28
	Gas Pipeline	99.80	1.68

dataset, but the FAR of CNN [11] is better than the proposed method. In the model detection task based on the Gas Pipeline industrial control network data set, the proposed model detection Acc is higher than AEDL-ICS [1] and CNN-ICS [9].

According to the data in Table 10, in the multi-classification task detection, the detection Acc of the proposed method in KDDcup99 dataset is higher than RTMAS-AIDS [2], and FAR lower than RTMAS-AIDS [2], but the detection accuracy and false positives rate of ANID-SEoKELM [14] are both better than that of the proposed method. For the five classification tasks of the NSL-KDD dataset, the detection accuracy of the proposed method is higher than ANID-CELM [23] and GA-GOGMM [13], but the false alarm rate of GA-GOGMM [13] is lower. In the eight-class detection task of the Gas Pipeline industrial control network dataset, the detection accuracy and false alarm rate of the proposed method are better than those of GoogLeNet-LSTM [4], and the detection accuracy of the CNN-ICS [9] model is higher than that of the proposed method. 0.34%.

Based on the above comparison and analysis, it can be seen that the five-class detection Acc on the NSL-KDD dataset is 98.54% higher than the two-class detection Acc 98.23%. The main reason is that when CNN is used to select the features of the NSL-KDD dataset, more features in the five categories are retained, which improves the detection accuracy of the five categories. In addition, compared with other models, the proposed method has higher detection accuracy on the three datasets of KDDcup99, NSL-KDD and Gas Pipeline, mainly because the proposed method uses a synthetic minority oversampling method to solve the problem of data imbalance in the dataset. In response to new attacks, the proposed method uses an online update strategy to ensure the adaptability of the proposed model, thereby improving the overall performance of the proposed model.

6 Conclusions and Future Work

An adaptive intrusion detection model based on CNN and C5.0 classifier is proposed, which improves the adaptability of the intrusion detection model in industrial control network to the dynamic changes of the network environment. The main work is reflected as follows: 1) The problem of data class imbalance is solved by using a few synthetic oversampling methods in industrial control network intrusion detection; 2) The effective data features are extracted by inputting the preprocessed data into the CNN model and adopting C5.0 classifier training and detection; 3) By introducing the adaptive online updating strategy based on frequent pattern mining, the updating of normal library and exception library is realized, which ensures the adaptability of the proposed model and realizes the detection of various attack behaviors. Experimental results show that the proposed method has good detection performance in terms of detection accu-

Table 10: Results of multi-classification performance comparison with existing methods

Method	Dataset	Acc(%)	FAR(%)
RTMAS-AIDS [2]	KDDcup99	95.86	2.13
ANID-SEoKELM [14]	KDDcup99	99.53	0.12
ANID-CELM [23]	NSL-KDD	84	3.03
GA-GOGMM [13]	NSL-KDD	96.52	1.43
GoogLeNet-LSTM [4]	Gas Pipeline	97.56	2.42
CNN-ICS [9]	Gas Pipeline	99.3	N/A
The proposed method	KDDcup99	98.18	1.43
	NSL-KDD	98.54	1.64
	Gas Pipeline	98.96	1.82

racy. The detection accuracy of KDDcup99, NSL-KDD and Gas Pipeline datasets reaches 98.18%, 98.54%, and 98.96%, respectively. At the same time, compared with the latest methods, whether it is two-class or multi-class, the detection accuracy of the proposed method is higher, and it can adapt to changes in the network environment.

The disadvantage is that the proposed method improves the detection accuracy while the false alarm rate is high. Further research will consider reducing the false alarm rate of the adaptive intrusion detection model and the long model training time.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61862041, 61363078), Scientific Research Program of Education Department of Shaanxi Province(No.19JK0040) and Science and Technology Project of Shaanxi Province (No.2020GY-041), The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," *IEEE Access*, vol. 8, pp. 83965–83973, 2020.

[2] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Real-time multi-agent system for an adaptive intrusion detection system," *Pattern Recognition Letters*, vol. 85, pp. 56–64, 2017.

[3] S. T. Bakhsh, S. Alghamdi, and R. A. Alsemmeari, "An adaptive intrusion detection and prevention system for internet of things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, pp. 1–9, 2019.

[4] A. K. Chu, Y. X. Lai, and J. Liu, "Industrial control intrusion detection approach based on multiclassification googlenet-lstm model," *Security and Communication Networks*, vol. 2019, pp. 1–11, 2019.

[5] R. H. Dong, X. Y. Li, Q. Y. Zhang, and H. Yuan, "Network intrusion detection model based on multivariate correlation analysis-long short-time memory network," *IET Information Security*, vol. 14, no. 2, pp. 166–174, 2020.

[6] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, pp. 82512–82521, 2019.

[7] Y. Hu, A. Yang, H. Li, Y. Y. Sun, and L. M. Sun, "A survey of intrusion detection on industrial control systems," *International Journal of Distributed Sensor Networks*, vol. 14, no. 8, pp. 1–14, 2018.

[8] X. Kan, Y. X. Fan, Z. J. Fang, and L. Gao, "A novel iot network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network," *Information Sciences*, vol. 568, pp. 147–162, 2021.

[9] Y. Lai, J. Zhang, and Z. Liu, "Industrial anomaly detection and attack classification method based on convolutional neural network," *Security and Communication Networks*, vol. 2019, no. 9, pp. 1–11, 2019.

[10] Y. Li, Y. Xu, and Z. Liu, "Robust detection for network intrusion of industrial iot based on multi-cnn fusion," *Measurement*, vol. 154, pp. 1–10, 2020.

[11] S. Z. Lin, Y. Shi, and Z. Xue, "Character-level intrusion detection based on convolutional neural networks," in *2018 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, Riode Janeiro, July 2018.

[12] J. Ling, Z. S. Zhu, Y. Lou, and H. Wang, "An intrusion detection method for industrial control systems based on bidirectional simple recurrent unit," *Computers and Electrical Engineering*, vol. 91, pp. 1–10, 2021.

[13] J. Liu, W. Zhang, and Z. Tang, "Adaptive intrusion detection via ga-gogmm-based pattern learning with fuzzy rough set-based attribute selection," *Expert Systems with Applications*, vol. 139, pp. 1–17, 2020.

[14] J. P. Liu, J. Z. He, and W. X. Zhang, "Anid-seokelm: Adaptive network intrusion detection based on selective ensemble of kernel elms with random features,"

Knowledge Based Systems, vol. 177, pp. 104–116, 2019.

[15] T. Lu, Y. P. Huang, W. Zhao, and J Zhang, "The metering automation system based intrusion detection using random forest classifier with smote+enn," in *2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)*, pp. 370–374, Dalian, China, Oct 2019.

[16] Y. Luo, "Research on network security intrusion detection system based on machine learning," *International Journal of Network Security*, vol. 23, no. 3, pp. 490–495, 2021.

[17] B. Mahapatraa and S. Patnaik, "Self adaptive intrusion detection technique using data mining concept in an ad-hoc network," *Procedia Computer Science*, vol. 92, pp. 292–297, 2016.

[18] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 686–728, 2019.

[19] M. R. Mohamed, A. A. Nasr, I. F. Tarrad, and S. R. Abdulmageed, "Exploiting incremental classifiers for the training of an adaptive intrusion detection model," *International Journal of Network Security*, vol. 21, no. 2, pp. 1–15, 2019.

[20] D. Papamartzivanos, F. G. Marmol, G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019.

[21] H. C. Qu, Z. L. Qiu, X. M. Tang, M Xiang, and P Wang, "An adaptive intrusion detection method for wireless sensor networks," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, pp. 27–36, 2017.

[22] P. A. A. Resende and A. C. Drummond, "Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling," *IEEE Communications Surveys and Tutorials*, vol. 1, no. 4, pp. 1–13, 2018.

[23] S. Roshan, Y. Miche, A. Akusok, and A. Lendasse, "Adaptive and online network intrusion detection system using clustering and extreme learning machines," *Journal of the Franklin Institute*, vol. 354, no. 4, pp. 1751–1779, 2018.

[24] L. Y. Shi, H. Q. Zhu, W. H. Liu, and J. Liu, "Industrial control system intrusion detection based on related information entropy and cnn-bilstm," *Journal of Computer Research and Development*, vol. 56, no. 11, pp. 2330–2338, 2019.

[25] X. P. Tan, S. J. Su, and Z. P. Huang, "Wireless sensor networks intrusion detection based on smote and the random forest algorithm," *Sensors*, vol. 19, no. 1, pp. 1–15, 2019.

[26] Y. Yang, H. Xu, L. Gao, Y. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for iec 61850-based scada networks," *IEEE Transactions on Power Delivery*, vol. 32, no. 2, pp. 1068–1078, 2017.

[27] F. Yu, G. Li, H. Chen, and Y. Guo, "A vrf charge fault diagnosis method based on expert modification c5.0 decision tree," *International Journal of Refrigeration*, vol. 92, pp. 106–112, 2018.

[28] H. Zhang, L. Huang, C. Q. Wu, and Z Li, "An effective convolutional neural network based on smote and gaussian mixture model for intrusion detection in imbalanced dataset," *Computer Networks*, vol. 177, pp. 1–10, 2020.

Biography

Hao Wen-tao. received his master's degree in computer science and technology from Lanzhou University of Technology in 2019, is now a teacher at the Network Information Center of Xi'an Aeronautical University, a CCF member. His research interests include network and information security, industrial control network security, intrusion detection, and blockchain, etc.

Lu Ye. Lecturer, Doctoral student, working in the School of Computer Science, Baoji University of Arts and Sciences. The main research direction is network and information security, industrial control network and Internet of things security, blockchain, etc.

Dong Rui-hong. Researcher, worked at school of computer and communication in Lanzhou university of technology. His research interests include network and information security, information hiding and steganalysis analysis, computer network.

Shui Yong-li. received a bachelor's degree in management from Jilin University of Finance and Economics in 2018. Currently, she is studying for a master's degree in Lanzhou University of Technology. The main research directions are network and information security, industrial control network security, intrusion detection, etc.

Zhang Qiu-yu. Researcher/Ph.D. supervisor, graduated from Gansu University of Technology in 1986, and then worked at school of computer and communication in Lanzhou University of Technology. He is vice dean of Gansu manufacturing information engineering research center, a CCF senior member, a member of IEEE and ACM. His research interests include network and information security, information hiding and steganalysis, multimedia communication technology.