Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047543

ARTICLE

Cluster Detection Method of Endogenous Security Abnormal Attack Behavior in Air Traffic Control Network

Ruchun Jia[1], Jianwei Zhang[1,*], Yi Lin[1], Yunxiang Han[1] and Feike Yang[2]

[1]College of Computer Science, Sichuan University, Chengdu, 610065, China

[2]Equipment Management and Unmanned Aerial Vehicle College of Air Force Engineering University, Air Force Engineering University, Xi'an, 710051, China

*Corresponding Author: Jianwei Zhang. Email: zhangjianwei@scu.edu.cn

Received: 08 November 2023 Accepted: 13 March 2024 Published: 15 May 2024

ABSTRACT

In order to enhance the accuracy of Air Traffic Control (ATC) cybersecurity attack detection, in this paper, a new clustering detection method is designed for air traffic control network security attacks. The feature set for ATC cybersecurity attacks is constructed by setting the feature states, adding recursive features, and determining the feature criticality. The expected information gain and entropy of the feature data are computed to determine the information gain of the feature data and reduce the interference of similar feature data. An autoencoder is introduced into the AI (artificial intelligence) algorithm to encode and decode the characteristics of ATC network security attack behavior to reduce the dimensionality of the ATC network security attack behavior data. Based on the above processing, an unsupervised learning algorithm for clustering detection of ATC network security attacks is designed. First, determine the distance between the clustering clusters of ATC network security attack behavior characteristics, calculate the clustering threshold, and construct the initial clustering center. Then, the new average value of all feature objects in each cluster is recalculated as the new cluster center. Second, it traverses all objects in a cluster of ATC network security attack behavior feature data. Finally, the cluster detection of ATC network security attack behavior is completed by the computation of objective functions. The experiment took three groups of experimental attack behavior data sets as the test object, and took the detection rate, false detection rate and recall rate as the test indicators, and selected three similar methods for comparative test. The experimental results show that the detection rate of this method is about 98%, the false positive rate is below 1%, and the recall rate is above 97%. Research shows that this method can improve the detection performance of security attacks in air traffic control network.

KEYWORDS

Air traffic control network; security attack behavior; cluster detection; behavioral characteristics; information gain; cluster threshold; automatic encoder

1 Introduction

With the continuous rapid development of China's national economy and a series of advances in the aviation field, the development of the air transport industry has entered a new development field [1]. In order to meet the rapid development of the aviation market, more aviation enterprises have been established, and the operation capacity of major airlines has also been rapidly improved. Aviation enterprises continue to launch new routes and maintain close ties with international routes. It can be said that the development of air traffic has achieved a steady rise [2]. The air traffic control department bears important responsibilities as an important guarantor of aviation safety operations. Air traffic control department managers can quickly dispatch and improve air routes and air traffic flow according to the air network, which is the key to the safe and stable operation of aviation enterprises. The effective control of air traffic control network is an important task in air traffic control operation system. The network structure is obviously different from the general network, and it is more critical [3]. If the ATC network suffers from security attack, it will lead to irreversible disaster. Therefore, the safety of air traffic control network is an important support for the steady-state development of the aviation industry. Air traffic control network will also have security attacks in operation, which will seriously affect the safety of air traffic control network [4]. Therefore, the detection and early warning of air traffic control network security attacks is particularly critical. Therefore, researchers in this field have designed many methods for the detection of security attacks on air traffic control networks and have achieved certain results.

In machine learning and deep learning methods, reference [5] points out that due to the continuous expansion of network scale, the network environment is faced with diversification and more and more intrusion attacks, which threaten network security. The application of machine learning and deep learning methods significantly improves the performance of network attack detection. Although this method improves the detection accuracy, it is complicated and has some limitations in the application of machine learning algorithms. In Fourier transform and entropy methods, reference [6] argues that one problem that automated attack tools cannot solve is the inevitable repetition or periodicity of traffic data, which is an important feature of effective attack detection. Several researchers have proposed to detect attacks by analyzing the frequency domain information or information entropy of network communication signals or network packets. This method is more convenient, faster, and more widely applicable. In the perfect Bayes-Nash equilibrium method, reference [7] replaces the solution of the Nash equilibrium problem with the benefit (reward) maximization problem through the deep combination of the subgame perfect Nash equilibrium (NE) of the dynamic game with complete information and the Bayesian Nash equilibrium (BNE) of the static game with incomplete information. Reference [8] studied a dynamic kernel convolutional neural network optimized based on a multi-population genetic algorithm to identify their malicious intentions and effectively detect malicious behavior in the cloud environment to achieve higher accuracy. Reference [9] proposes a grouped convolutional neural network model based on feature correlation for learning and reconstructing security data to deal with the network threat detection problem in the Internet of Things, and proves the advantages of this method in dimension reduction and performance. In addition, in order to evaluate the effectiveness of this method, a representative signal game with a specific value is investigated theoretically. The effectiveness of this method is proved from the practical point of view. However, this method does not carry out further detection according to specific attack behavior in the attack behavior detection, and needs further improvement.

The data generated by the ATC network is huge and diverse, including network traffic, log records, alert information, etc. These data have a high dimension and contain a large number of features, such as source Internet Protocol (IP) address, target IP address, protocol type, port number, etc., which make the processing and analysis of data become complex. At present, there is little research on ATC network security performance. Therefore, to improve the security performance of air traffic control networks, this paper proposes a novel clustering detection method for the security attack behavior of air traffic control networks. This study aims to improve the clustering detection method for air traffic control network security attacks, in order to address the current problems in the field of air traffic control network security. Firstly, in feature extraction, a recursive feature addition method is introduced to extract more representative and discriminative network security attack features by training a model on a large amount of existing data. Secondly, in data feature preprocessing, the original features are optimized by combining the expected information gain and entropy values with the data dimensionality reduction algorithm to reduce data interference and improve the accuracy and efficiency of the subsequent clustering analysis. Finally, in the process of clustering detection, an unsupervised learning algorithm is used to cluster and group the network security attack behavior data according to the cluster threshold. Based on the results of the clustering analysis, the objective function is computed to further identify potentially unknown attack types. Through the above improvements, the aim is to improve the detection accuracy of air traffic control network security attacks, enhance the security protection capabilities of the air traffic control network, and effectively respond to the constantly evolving network security threats. The specific structure of this paper includes:

(1) The feature set of air traffic control network security attack behavior is obtained by recursive feature addition method, and the feature extraction of air traffic control network security attack behavior is realized by determining the key degree of the feature;

(2) The automatic encoder in the artificial intelligence algorithm is introduced to encode and decode the characteristics of ATC network security attack behavior to achieve dimensionality reduction processing of ATC network security attack behavior data;

(3) Through the design of an unsupervised learning algorithm for the cluster detection of air traffic control network security attack behavior, the cluster detection of air traffic control network security attack behavior is completed;

(4) The performance of the proposed method was verified through experiments, and relevant conclusions were drawn.

2 Materials & Methods

2.1 Feature Extraction

In the cluster detection of the security attack behavior of ATC networks, the characteristics of the security attack behavior are key to reflect all anomalous behaviors. Therefore, we should first determine the characteristics of different attack behaviors [10]. Subsequent cluster detection studies are then performed based on the obtained features. Air traffic control network security attack behavior refers to the behavior of interfering with the air traffic control network system during its operation and endangering the stability and integrity of the network. The appearance of this kind of behavior is a destructive behavior carried out by external intruders with the help of a series of malicious behavior codes. The general network security attack behavior intrusion form [11–13] is similar to the ATC network security attack behavior, but its network security attack behavior is still quite different. Therefore, in order to ensure the safe and stable operation of the air traffic control network, this paper first extracts the characteristic data of air traffic control network security attack behavior, and on this basis, carries out more in-depth research.

In feature extraction for ATC network security attack behavior, recursive feature addition is used to extract the attack behavior. This algorithm is an iterative feature extraction algorithm, which is fast in feature extraction and can capture the most core features. An example of the implementation of this algorithm for feature extraction is shown in Fig. 1:

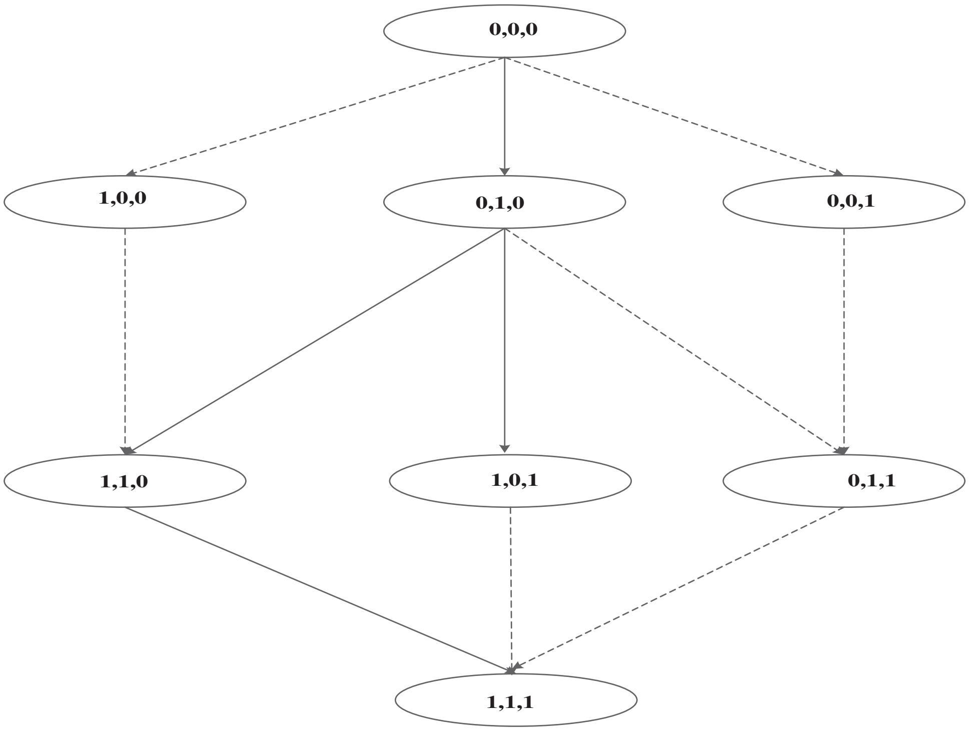


Figure 1: Example diagram of recursive feature addition and feature extraction

As shown in Fig. 1, the numbers 0 and 1 in the figure respectively represent the two states that a feature of ATC network security attack behavior is not selected and selected, and the solid line and dotted line in the figure respectively represent the critical degree and non critical degree of the feature. Considering that the attack behavior is highly dynamic, attackers constantly change attack strategies and means to avoid detection and defense measures [14–16]. Therefore, it is assumed that there is a certain feature dataset of ATC network security attack behavior, and the three features of the feature dataset are denoted as 0 or 1. Define the characteristics of ATC network security attacks in the ATC collection, and set the status of relevant characteristics. The obtained characteristics of ATC network security attack behavior are represented as:

$$\mathrm{D} = \{d_1, d_2, \ldots d_n\} \tag{1}$$

In formula (1), D represents the feature set of air traffic control network security attack behavior, $d_1, d_2, \ldots d_n$ represents the composition of characteristics of ATC network security attack behavior, and n represents the number of feature vectors [17–19].

Set the characteristic state of air traffic control network security attack behavior in this set, and the obtained characteristic state set:

$$\mathrm{D}\left(\mathrm{s}\right) = \left\{d_1\left(s\right), d_2\left(s\right), \ldots d_n\left(s\right)\right\} \tag{2}$$

In formula (2), s represents the set characteristic state value

Based on the above settings, the result of feature extraction for this attack behavior through recursive feature addition:

$$F(s) = \sum D \sum_{s}^{s \in D} (d_n(s)) \tag{3}$$

In formula (3), $F(s)$ stands for the network security attack behavior characteristics of air traffic control stored in the empty set.

After extracting the feature data of the security attack behavior of ATC networks, the criticality of the features is mainly determined by the correlation analysis of the features of the security attack behavior. In the detection of the correlation between the characteristic data of the ATC network security attack behavior, the cross correlation test index is used to study the correlation of the characteristics, and the correlation is set to 0.3 as the standard to determine whether the characteristic data of ATC network security attack behavior is the key characteristic data. When the correlation value of characteristic data of network security attack behavior is larger, it reflects that the extracted characteristics are more critical [20–22]. After adding the recursive features, the optimal features for the secure attack behavior of the ATC network are extracted step by step. Set the characteristic correlation coefficient of ATC network security attack behavior as V. when calculating the characteristic correlation coefficient, calculate its correlation through the Eta coefficient. The results are as follows:

$$\mathrm{V} = \sqrt{\frac{x^2}{N(k-1)}} \tag{4}$$

$$\mathrm{Eta} = \frac{\sum (\mathrm{y} - \bar{\mathrm{y}})^2 - \sum (\mathrm{y} - \bar{\mathrm{y}}_{\mathrm{i}})^2}{\sum (\mathrm{y} - \bar{\mathrm{y}})^2} \tag{5}$$

In the above formula, x^2 represents the chi square statistic, k represents the smaller actual characteristic value of air traffic control network security attack behavior, $\overline{y}$ represents the mean of all characteristic variables of air traffic control network security attack behavior, and $\overline{y_i}$ represents the mean value of all data corresponding to the characteristic variable i of network security attack behavior [23].

According to the above calculation, the correlation coefficient between the characteristics of air traffic control network security attack behavior:

$$\mathrm{C_i} = \left\{ \begin{matrix} V & y \in \text{symbol features} \\ Eta & y \in \text{Numerical characteristics} \end{matrix} \right\} \tag{6}$$

In formula (6), $\mathrm{C_i}$ represents the correlation coefficient result between the characteristics of air traffic control network security attack behavior.

Finally, based on the above analysis, the key feature code set of the air traffic control network security attack behavior extracted is shown in Table 1:

Table 1: Key feature set of air traffic control network security attack behavior

Feature name	Characteristic number	Continuous state
dst_bytes	1	Continuous
src_bytes	5	Continuous
service	3	Dispersed
num_root	15	Continuous
rerror_tate	23	Dispersed

2.2 Research on Data Feature Preprocessing of Air Traffic Control Network Security Attack Behavior

Based on the extracted features of the air traffic control network security attack behavior data, further research is needed to pre-process the features of the air traffic control network security attack behavior data due to the large amount of extracted feature data and different attributes. Before preprocessing, the information gained from the feature data is calculated to determine the most relevant feature in the data of air traffic control network security attack behavior [24–26]. This can reduce the interference of similar feature data and reduce the difficulty and complexity of subsequent detection.

Set the annotated feature sample dataset of air traffic control network security attack behavior data as A. If the features in this dataset share *m* categories, the expected information gain of the feature data in that category is calculated using the following formula:

$$G_i = -\sum_{i=1}^{m} \frac{s_i}{s} \log_2 \frac{s_i}{s} \tag{7}$$

In formula (7), s_i represents the number of samples in Class i, and G_i represents the expected information gain value.

Assuming that the value contained in the characteristics of ATC network security attack behavior data is fixed, it can be divided into training sets. At this time, it is necessary to determine the entropy value of the characteristics of ATC network security attack behavior data, and its calculation formula:

$$E(A) = \sum_{j=1}^{n} \frac{s_{1j} + s_{2j} + \dots s_{mj}}{s} \times \left(s_{1j} + s_{2j} + \dots s_{mj}\right) \tag{8}$$

In formula (8), $E(A)$ represents the entropy value of the obtained air traffic control network security attack behavior data features, and s_j represents the j class value in the feature category [27].

Based on the above calculations, the information gain result of the final data characteristics of air traffic control network security attack behavior is determined as:

$$Gain(E) = G_i - E(A) \tag{9}$$

In formula (9), $Gain(E)$ represents the information gain of the data characteristics of air traffic control network security attacks. Through the gain result, the continuous variable Discretization in the extracted feature data can be determined, that is, the correlation degree of each type of feature can be obtained to avoid the interference of similar feature data, which is also a processing method in feature data preprocessing.

After calculating the information gain of the ATC network security attack behavioral data features, the relevance of each type of feature is effectively determined and the interference of similar feature data is reduced. Based on this, the dimensionality of ATC network security attack behavior is higher due to the large difference between the characteristic data and the general data. Further dimensionality reduction processing is required during preprocessing to improve the efficiency of subsequent clustering detection [28–30]. Therefore, in this paper, we introduce an autoencoder for Artificial Intelligence (AI) algorithms to reduce the dimensionality of the characteristics of air traffic control network security attacks. The automatic encoder can gradually convert specific features into abstract features, and can well realize the nonlinear conversion from high-dimensional data to low-dimensional data. In the dimensionality reduction process, this is achieved by two steps of encoding and decoding. The specific implementation process is as follows:

(1) The encoding execution from the input layer to the hidden layer involves inputting the sample data of air traffic control network security attack behavior characteristics into the input layer and hidden layer of the automatic encoder for encoding, namely:

$$f(x) = h_f(w_1 x + b_1) \tag{10}$$

In formula (10), $f(x)$ represents the coded Activation function model, h_f represents the input initial feature sample set, w represents the feature weight parameter, and b represents the offset value.

(2) Further input the above feature data into the output layer to complete the decoding work, namely:

$$g(x) = h_f(w_2 x + b_2) \tag{11}$$

In formula (11), $g(x)$ represents the decoder decoding function model.

(3) Reconstruct the characteristic error of air traffic control network security attack behavior. When performing dimensional processing, the automatic encoder minimizes the difference between the input sample vector and the output result vector. During its dimensionality reduction process, it trains the characteristic data of air traffic control network security attack behavior and conducts reasonable parameter search to make the dimensionality reduced characteristic data closer to a reasonable value [31–33]. Therefore, the error of its reconstruction can be defined as:

$$p(x) = \frac{1}{n}\sum_{x\in h}^{n} L\{(x, g(x)[f(x)])\} \tag{12}$$

In formula (12), $p(x)$ represents the reconstruction error, and L represents the difference parameter.

(4) Realize dimension reduction feature processing of automatic encoder. The automatic encoder completes the dimensionality reduction processing by inputting and outputting the reconstruction error of the security attack behavior characteristics [34–36]. After determining its dimensionality reduction objective function, it further iterates and updates the weights with the help of the gradient descent method to realize the dimensionality reduction processing of the security attack behavior characteristics of air traffic control network. The final results are shown as follows:

$$U(x) = -\sum_{i=1}^{m}\left[x_i \log p(x) + (1 - x_i)/y_i \log(1 - p(x))\right] \tag{13}$$

In formula (13), $U(x)$ represents the objective function of dimensionality reduction, x_i represents the i-th feature vector of the input feature dimension sample, and y_i represents the i-th feature vector of the output dimensionality reduced feature sample.

The preprocessing process of data characteristics for air traffic control network security attack behavior is shown in Fig. 2:

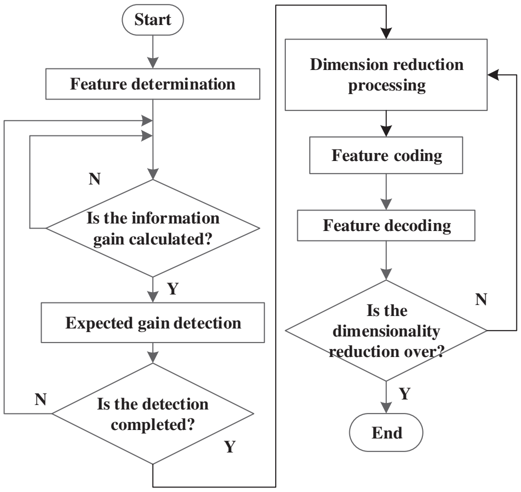

Start
Feature determination
N
Is the information gain calculated?
Y
Expected gain detection
N
Is the detection completed?
Y
Dimension reduction processing
Feature coding
Feature decoding
N
Is the dimensionality reduction over?
Y
End

Figure 2: Pre processing process of data characteristics for air traffic control network security attack behavior

2.3 Implementation of Clustering Detection for Security Attack Behaviors in Air Traffic Control Networks

As one of the important subjects of aviation security, air network security is the key to control the safe and stable operation of air routes, and has become an important research object of aviation risk. Air traffic control network security attack is a kind of behavior that deviates from the normal network state. When it is attacked, the deviation is more serious. Therefore, on the basis of attack behavior feature extraction and preprocessing [37,38], the attack behavior feature data is used as the basic data for clustering detection of ATC network security attack behavior.

Clustering detection of ATM network security attack behavior aims at aggregating several data objects with the same characteristics into the same cluster, which is a key way to quickly detect ATM network security attack behavior based on the similarity between its characteristics. Differences between different data categories can be obtained through clustering detection results. This algorithm is an unsupervised learning algorithm. In the detection process, it does not require prior access to data object labels. By employing a specific algorithm, this approach can directly establish the correlation between the characteristic data of ATC network security attack behavior, facilitating conclusive research on detection outcomes. The implementation steps are as follows:

Step 1: Determine the distance between clusters of security attack behavior characteristics [39–43]. Assuming that each cluster is a sample set of ATC network security attack behavior characteristic data, when calculating the distance between clusters, it is necessary to determine the distance between the set characteristic data, including the minimum distance, the maximum distance and the average distance. The calculation formula of these distances is as follows:

The minimum distance calculation formula:

$$D_{\min}\left(d_i, d_j\right) = \min_{x \in d_i, y \in d_j} dist\left(x, y\right) \tag{14}$$

The maximum distance calculation formula:

$$D_{\max}\left(d_i, d_j\right) = \max_{x \in d_i, y \in d_j} dist\left(x, y\right) \tag{15}$$

The formula for calculating the average distance:

$$D_{avg}\left(d_i, d_j\right) = \frac{1}{\left|d_i\right| \left|d_j\right|} \sum\nolimits_{x \in d_i, y \in d_j} dist\left(x, y\right) \tag{16}$$

In the above formula, d_i/d_j represents the set clustering cluster, and $dist\left(x, y\right)$ represents the set cardinality.

Based on the distance between clusters of air traffic control network security attack behavior characteristics determined above, the impact of all feature data in the cluster on the distance between clusters can be comprehensively measured, which is more suitable for improving the robustness of cluster detection [44–46]. This helps to improve the clustering detection effect of security attack behavior, make it more adaptable to the complex and changeable network environment, and enhance the detection and response ability to potential threats. The schematic diagram of cluster distance variation is shown in Fig. 3:

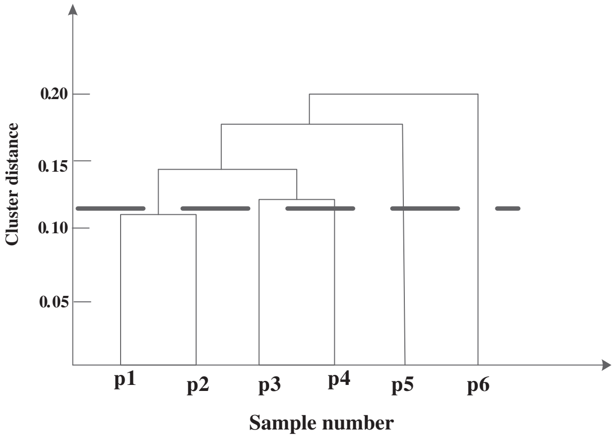


Figure 3: Schematic diagram of distance changes in clustering clusters of air traffic control network security attack behavior characteristics

Step 2: Calculate the clustering threshold for security attack behavior features of the air traffic control network. By calculating its threshold, the frequency of non feature matching attack behavior data in cluster detection can be reduced, and the accuracy of cluster detection can be improved [47,48]. The calculation formula for this threshold is:

$$r_i = \frac{1}{n} \sum e_i\left(k\right) / t_i, k = 1, 2, \ldots n \tag{17}$$

In formula (17), r_i represents the fixed threshold value of the feature clustering cluster, e_i represents the relevant feature matrix, t_i represents the number of clustering times, and k represents the number of times the clustering threshold is determined.

Step 3: Construct the initial clustering center of the cluster to which the characteristic data of air traffic control network security attack behavior belongs. Set the feature data set of air traffic control network security attack behavior as $B = \{b_1, b_2, \ldots, b_m\}$, randomly select feature data objects from this set to form their clustering centers, and obtain the following results:

$$Q_i = \{x_i \,| d\left(x_i, b_i\right) \leq d\left(x_i, b_i\right), i \neq l|\} \tag{18}$$

In formula (18), Q_i represents the initial clustering center point, and x_i/b_i represents the randomly selected feature data.

Step 4: Recalculate the new mean of all feature objects in each cluster as the new cluster center point. Due to the interference of multiple data in determining the initial cluster center point, the cluster center taste changes [49]. In order to ensure the stability of the cluster center point, a new cluster center point was determined, and the results obtained were:

$$V_i = \frac{1}{|Q_i|} \sum\nolimits_{x_i \in Q_i} x_i \tag{19}$$

Step 5: All objects in the cluster of ATC network security attack behavior feature data are traversed and the cluster detection of ATC network security attack behavior is completed by the objective function computation. The traversal result can be expressed as:

$$\varphi_i = dist\left(x_i, x_j\right) \sum V_i \tag{20}$$

In formula (20), φ_i represents the traversal result [50,52].

The calculation formula for the objective function of clustering detection is expressed as:

$$\zeta = \sum_{i=1}^{n} \sum_{j=1}^{m} \varphi_i \left(x_i, x_j\right)^2 \int \delta \tag{21}$$

In formula (21), ξ represents the clustering detection result of air traffic control network security attack behavior, and δ represents the interference term in the clustering detection. Based on the above content, the overall technical flowchart can be obtained as shown in Fig. 4.

Complete the clustering detection of air traffic control network security attack behavior through the process shown in Fig. 4, in order to improve the detection performance of air traffic control network security attack behavior.

3 Results

3.1 Experiment Programme

To validate the feasibility of clustering detection of air traffic control network security attacks in this paper, a specific scheme is implemented for the experiment. The experimental analysis is conducted using data on air traffic control network attacks within a certain airline over the past six months.

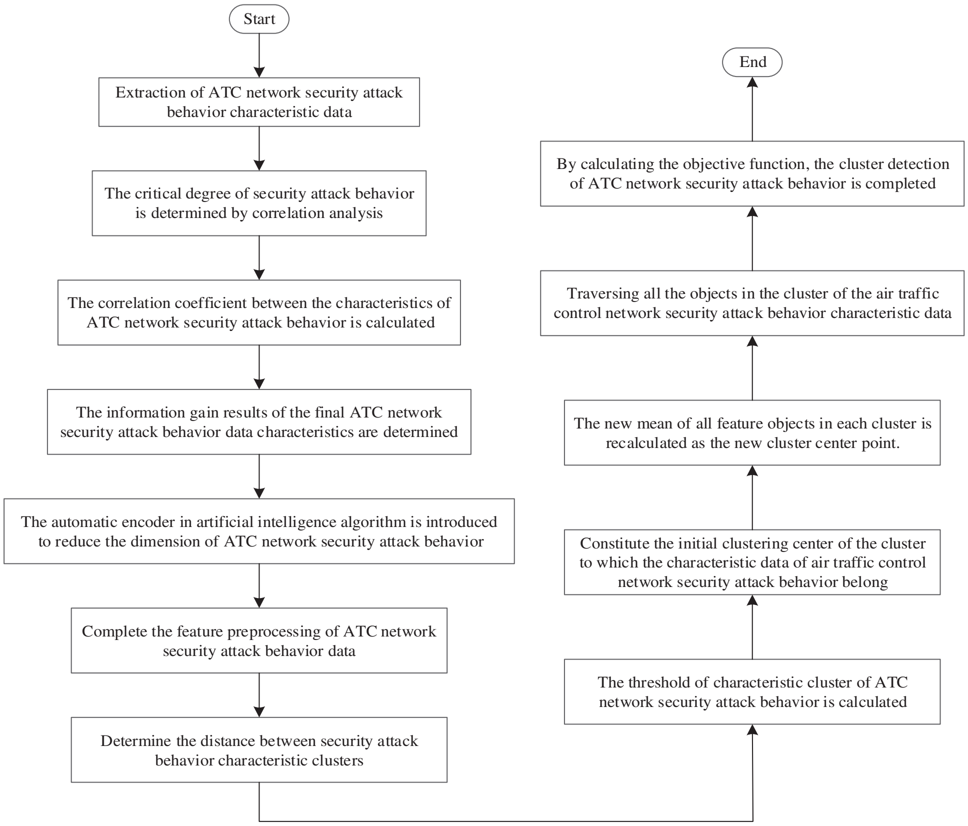

Start
Extraction of ATC network security attack behavior characteristic data
The critical degree of security attack behavior is determined by correlation analysis
The correlation coefficient between the characteristics of ATC network security attack behavior is calculated
The information gain results of the final ATC network security attack behavior data characteristics are determined
The automatic encoder in artificial intelligence algorithm is introduced to reduce the dimension of ATC network security attack behavior
Complete the feature preprocessing of ATC network security attack behavior data
Determine the distance between security attack behavior characteristic clusters
The threshold of characteristic cluster of ATC network security attack behavior is calculated
Constitute the initial clustering center of the cluster to which the characteristic data of air traffic control network security attack behavior belong
The new mean of all feature objects in each cluster is recalculated as the new cluster center point.
Traversing all the objects in the cluster of the air traffic control network security attack behavior characteristic data
By calculating the objective function, the cluster detection of ATC network security attack behavior is completed
End

Figure 4: Overall technical flowchart

(1) Experimental environment

The experimental environment is as follows: The operating system is win7, the air traffic control network programming environment is Microsoft Studio Ultimate 2018, and the language is visual c++. The programming language in this experiment is combined with database technology, which is SQL 2016. In order to ensure the feasibility of the experiment, the processor of this experiment is inter core i7-2670qm 2.2 GHz, with 32 g memory and 500 g hard disk.

(2) Experimental dataset

The data of ATC network security attack behavior selected in this experiment comes from the database SQL 2016. This experiment is a simulation experiment, and three groups of experimental attack behavior data sets are selected, respectively. Three sets of experimental attack behavior data sets are respectively (1) nsl-kdd data set: Nsl-kdd data set is a kind of data set for network intrusion detection research (https://www.unb.ca/cic/datasets/nsl.html), which is an improvement of KDD cup 1999 data set. It contains network traffic data from different types of attacks, including normal traffic and a variety of attack behaviors, such as DOS, r2l, u2r and probing. (2) Unsw-nb15 dataset: Unsw-nb15 (https://ieeedataport.org/documents/unswnb15-dataset). This data set collects traffic data from UNSW network and contains different types of attacks, such as DOS, probing, malware, etc. (3) Cicids2017 data set (https://www.unb.ca/cic/datasets/ids-2017.html): Cicids2017 data set is based on the network traffic data set collected by the Canadian Research Center for communication and information security (CIC). The data set contains the simulated network traffic data of industrial control system, and contains a variety of attacks, such as DOS, DDoS, brute force, etc.

The data selected in the experiment is a sampling data set. In order to avoid the contingency of cluster detection of ATC network security attack behavior in a single experimental data set, 10 data sets were selected from the selected attack behavior data set for 10 experiments before each group of experiments. Among them, the attack behavior data in the data set contains several unknown attack behaviors of corresponding categories, which are masked by known attack behavior data to verify the effectiveness of the detection method. The data set in the experiment is shown in Table 2:

Table 2: Experimental dataset details

Normal air traffic control network data/piece	Security attack behavior data/piece	Attack behavior/class
100	100	3
200	200	5
300	300	6
400	400	8
500	500	10
600	600	11
700	700	13
800	800	14
900	900	15
1000	1000	16

3.2 Experimental Indicator Setting

The experimental indicators selected in this article are the detection rate, false detection rate, and recall rate of air traffic control network security attacks. The calculation formula for specific experimental indicators:

(1) Detection rate: The ratio of the sum of the air traffic control network security attack behavior data correctly identified by this indicator to the total data. The higher the detection rate, the better the performance of the algorithm detection. The calculation formula:

$$\tau_{\mathrm{i}} = \frac{P_i + N_i}{P_i + N_i + F_i + N_j} \tag{22}$$

(2) Misdetection rate: This indicator reflects the ratio of the amount of data for air traffic control network security attacks that have been misjudged to the total amount of data for journey behavior. The lower the detection rate, the better the detection performance of the method. The calculation formula:

$$\tau_j = \frac{F_i}{N_i + F_i} \tag{23}$$

(3) Recall rate: This indicator refers to the ratio of the amount of correctly detected attack behavior data to the total amount of attack behavior. The higher the value, the stronger the detection ability.

The calculation formula for this indicator:

$$R_i = \frac{P_i}{P_i + F_i} \tag{24}$$

In the above formula, N_i represents the amount of data that correctly identifies normal air traffic control network security behavior as security attack behavior data, P_i represents the amount of network data that correctly identifies air traffic control network security attack behavior as the corresponding attack type, F_i represents the amount of data that misjudges the behavior of air traffic control network security tools as normal behavior data, and F_j represents the amount of data that misjudges normal behavior data as a certain type of security attack behavior.

3.3 Experimental Process

Based on the analysis of the content in the introduction, it can be seen that the hybrid DBN-LSTM detection method (reference [5] method), the detection method based on Fourier transform and entropy (reference [6] method), the perfect Bayesian Nash equilibrium detection method (reference [7] method), Malicious behavior detection method using self-optimized dynamic nuclear Convolutional neural network (reference [8] method) and network threat detection method based on CNN privacy protection (reference [9] method) have achieved good research results in the field of network attack detection. Therefore, the above method will be used as a comparison method for the proposed method, and experiments will be conducted on the same experimental data set. The specific experimental process is as follows:

(1) Detection rate: During the experiment, 8 sets of experimental dataset samples were selected for analysis and judgment based on known true case labels, and the detection rate index was obtained according to formula (22).

(2) Misdetection rate: Attack three datasets 50 and 100 times, respectively, use the above method for classification and judgment, and obtain the misdetection rate indicator according to formula (23).

(3) Recall rate: During the experiment, 8 sets of experimental dataset samples were selected for classification and judgment using the above method, and the recall rate index was obtained according to formula (24).

3.4 Experimental Results

In the experiment, the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method) were used for experimental analysis on the same experimental data set. Firstly, the detection rates of four methods for air traffic control network security attack behavior in the experimental dataset were analyzed, and 10 data detection rates were analyzed in this experimental set. The obtained results are shown in Fig. 5.

From the results in Fig. 5, it can be seen that there are certain differences in the detection rate of air traffic control network security attacks using the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method). From the curve in the figure, it can be seen that the detection rate of the proposed method is relatively high and stable at around 98%, while the detection rates of the other three methods fluctuate to some extent and are lower than the proposed method, thus verifying the feasibility of the proposed method.

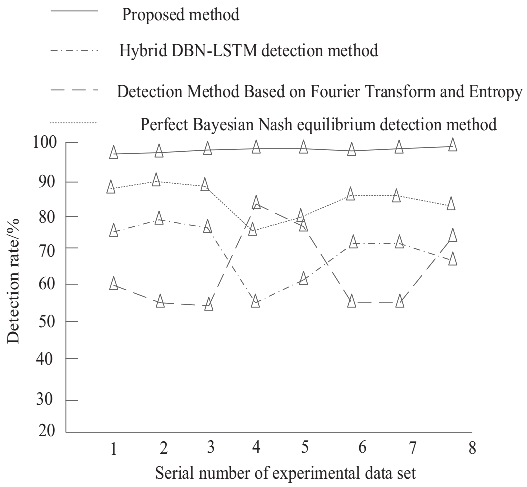


Figure 5: Comparison results of detection rates for air traffic control network security attack behaviors

The proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method) were used for clustering detection on three datasets. The clustering accuracy results were described in Table 3.

Table 3: Clustering accuracy of different methods (%)

Attack category	Proposed method		Hybrid DBN-LSTM detection method		Detection Method Based on Fourier Transform and Entropy		Perfect Bayesian Nash equilibrium detection method	
	Attack 50 times	Attack 100 times	Attack 50 times	Attack 100 times	Attack 50 times	Attack 100 times	Attack 50 times	Attack 100 times
NSL-KDD dataset	97	98	93	91	94	94	94	95
UNSW-NB15 Dataset	97	97	93	92	93	92	94	93
CICIDS2017 Dataset	98	98	92	91	91	90	92	94

Analysis of Table 3 shows that there are certain differences in the clustering accuracy of air traffic control network security attack behaviors using the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method). Among them, the clustering accuracy of the proposed method is relatively high and stable at around 97%, while the clustering accuracy of the other three methods is lower than that of the proposed method, which verifies the feasibility of the proposed method.

The experiment used the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method) to detect the error detection rates of four methods on the same experimental data set. The results obtained are shown in Fig. 6:

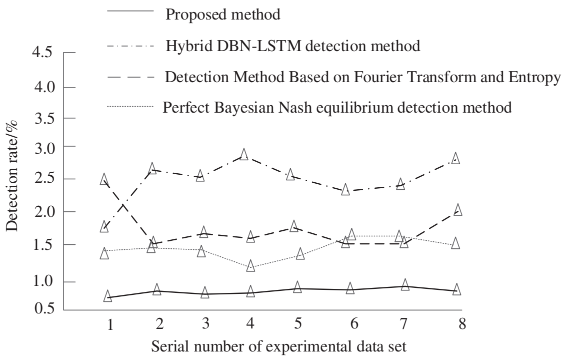


Figure 6: Comparison results of misdetection rate of air traffic control network security attack behavior

Analyzing the test results in Fig. 6, it can be seen that the false positives of four methods were detected on the same experimental data set. From the results, it can be seen that the false detection rate of the proposed method for air traffic control network security attacks remains below 1%. Although the detection rate of the other three methods shows a certain downward trend, the overall level is still higher than the proposed method. This also shows that the detection error rate of the proposed method is lower, verifying the feasibility of this method.

The experiment used the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), perfect Bayesian Nash equilibrium detection method (reference [7] method), malicious behavior detection method using self-optimized dynamic nuclear Convolutional neural network (reference [8] method) and network threat detection method based on CNN privacy protection (reference [9] method) to detect the recall rates of four methods on the same experimental data set. The results obtained are shown in Table 4.

Table 4: Comparison of recall rates for air traffic control network security attack behavior detection (%)

Experimental data set number	Proposed method	Hybrid DBN-LSTM detection method	Detection Method Based on Fourier Transform and Entropy	Perfect Bayesian Nash equilibrium detection method	Malicious behavior detection method using self-optimized dynamic kernel convolutional neural networks	Network threat detection method based on CNN privacy protection
1	99	91	93	92	95	94
2	99	91	91	91	95	96
3	99	92	91	93	94	93

(Continued)

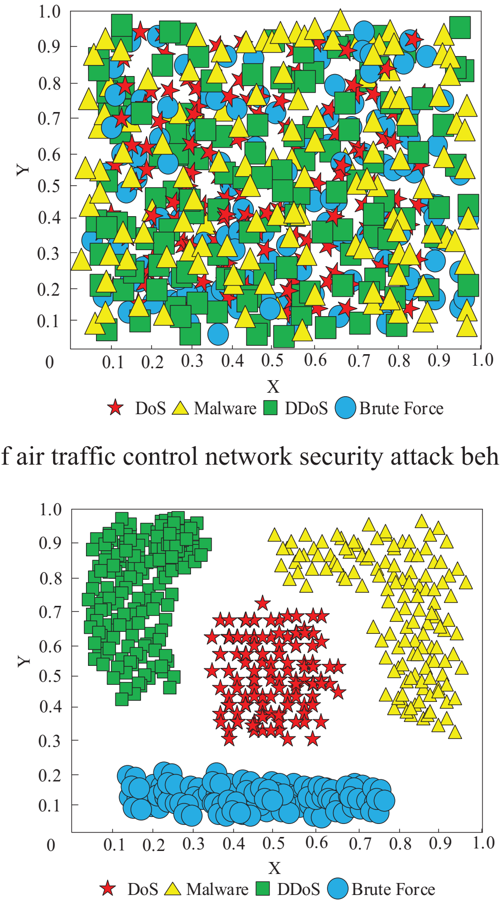
Table 4 (continued)

Experimental data set number	Proposed method	Hybrid DBN-LSTM detection method	Detection Method Based on Fourier Transform and Entropy	Perfect Bayesian Nash equilibrium detection method	Malicious behavior detection method using self-optimized dynamic kernel convolutional neural networks	Network threat detection method based on CNN privacy protection
4	98	90	90	90	94	94
5	98	90	90	90	94	96
6	98	91	89	90	95	92
7	97	92	91	92	93	93
8	98	90	92	91	94	91
9	98	90	91	93	92	90
10	97	91	90	92	91	92

By analyzing the data in Table 4, we can see that in the same experimental data set, the recall rate of the six methods is maintained at a relatively high level, higher than 90% as a whole, indicating that these six methods can detect the air traffic control network security attacks. However, the comparison of recall rates on each set shows that the recall rate of the proposed method is higher than that of the other four methods, which is higher than 97%. This is because the proposed method determines the most relevant features in the ATC network security attack behavior data by calculating the information gain of the feature data before pre-processing, thus reducing the interference of similar feature data and making the proposed method have strong detection performance.

Using the method presented in this article, four types of air traffic control network security attack behaviors, DoS, Malware, DDoS, and Brute Force, were clustered from the experimental dataset to obtain a set of air traffic control network security attack behaviors. The clustering results are shown in Fig. 7.

According to Fig. 7a, it can be seen that the behavior of air traffic control network security attacks is relatively scattered. According to Fig. 7b, it can be seen that the air traffic control network security attack behavior after clustering using the method in this article consists of four clear categories, with each category having a relatively long distance, clear boundaries, and no confusion. Experimental results have shown that the method proposed in this paper can accurately cluster air traffic control network security attack behaviors, obtaining a set of four different types of air traffic control network security attack behaviors, and the clustering effect is relatively good.



(a) Distribution of air traffic control network security attack behavior before clustering

(b) Cluster results

Figure 7: Clustering results of air traffic control network security attack behavior

To verify the advantages of the proposed method in the field of attack behavior recognition, experiments were conducted using the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method), malicious behavior detection method using self-optimized dynamic nuclear Convolutional neural network (reference [8] method) and network threat detection method based on CNN privacy protection (reference [9] method). The accuracy, false alarm rate, and false alarm rate during the recognition of attack behavior were shown in Table 5.

According to Table 5, the accuracy rate, omission rate and false alarm rate of the proposed method are better to the other five methods. This is because the method of automatic encoder dimension processing, keep the input sample vector and minimize the difference between the output of the vector, in the process of its dimension reduction of air traffic control network security behavior characteristic data training, and the reasonable search parameters, make the characteristics of dimension reduction data closer to the reasonable value. Therefore, the proposed method has shown favorable results in terms of checking accuracy, omission rate, and false alarm rate in the clustering detection of ATC network security attack behavior.

Table 5: Comparison of recognition performance between different methods

Comparison item	Proposed method	Hybrid DBN-LSTM detection method	Detection method based on Fourier transform and entropy	Perfect Bayesian Nash equilibrium detection method	Malicious behavior detection method using self-optimized dynamic kernel convolutional neural networks	Network threat detection method based on CNN privacy protection
Accuracy/%	97.61	94.12	93.11	93.62	93.85	94.62
Misreporting rate/%	0.23	2.81	3.61	3.21	0.52	1.72
False alarm rate/%	0.03	1.96	0.71	1.34	0.21	0.18

The DCP (Detection Cost per Point) value experiment is an indicator used to evaluate the performance of clustering detection methods. The DCP value can be used to measure the cost required for clustering detection methods to discover real attack behavior, the cost of reducing false detection rate while achieving a certain recall rate. Table 6 shows the comparison of DCP values between the proposed method and the comparison method in detecting attack behavior.

Table 6: Comparison of DCP values between different methods

Number of samples	Proposed method	Hybrid DBN-LSTM detection method	Detection method based on Fourier Transform and entropy	Perfect Bayesian Nash equilibrium detection method
100	0.041	0.054	0.052	0.071
200	0.043	0.057	0.053	0.075
300	0.046	0.061	0.055	0.078
400	0.047	0.065	0.057	0.082
500	0.047	0.067	0.058	0.086
600	0.051	0.069	0.062	0.090
700	0.052	0.073	0.066	0.097
800	0.054	0.076	0.073	0.104
900	0.056	0.078	0.080	0.111
1000	0.059	0.081	0.088	0.154

Analysis of Table 6 shows that as the number of samples increases, the DCP values of different methods in detecting the attack behavior of the research object all increase. The proposed method has a maximum DCP value of 0.059%, which is significantly reduced compared to the three comparison methods of 0.081%, 0.088%, and 0.154%, indicating that the proposed method has lower energy consumption in practical applications.

Shorter detection time allows for faster detection and response to security threats. Therefore, based on the single detection task time as an indicator, the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method) were used in the experiment to conduct detection time experiments on the same experimental data set. The time of a single detection task refers to the time from the start of network traffic data analysis and detection to the final detection results. This includes the time spent on preprocessing data, feature extraction, clustering algorithm operation, result analysis, and other processes. Take the average of the experimental results, as shown in Fig. 8:

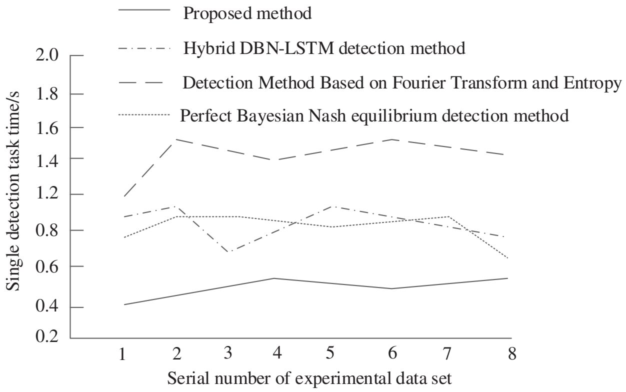


Figure 8: Comparison results of single detection task time detection for air traffic control network security attack behavior

Analyzing the test results in Fig. 8, it can be seen that the single detection task time of four methods was detected on the same experimental data set. From the results, it can be seen that the maximum average detection time of a single detection task for the proposed method's air traffic control network security attack behavior is 0.45 s. The maximum average detection time for a single detection task of Hybrid DBN-LSTM detection method, Detection Method Based on Fourier Transform and Entropy, and Perfect Bayesian Nash equilibrium detection method is 1.02, 1.46, and 0.86 s. From this it can be seen that the proposed method has a faster single detection task time for air traffic control network security attacks, verifying the feasibility of this method.

To further explore the clustering detection performance of different methods, SSB was used as an indicator for testing. Determine the clustering errors of the proposed method, mixed DBN-LSTM detection method (reference [5] method), detection method based on Fourier transform and entropy (reference [6] method), and perfect Bayesian Nash equilibrium detection method (reference [7] method) for six attacks: R2L, U2R, Probing, DoS, DDoS, and Brute Force. The smaller the SSB value, the higher the similarity between samples within the cluster, and the more accurate the clustering results. The experimental results are shown in Fig. 9.

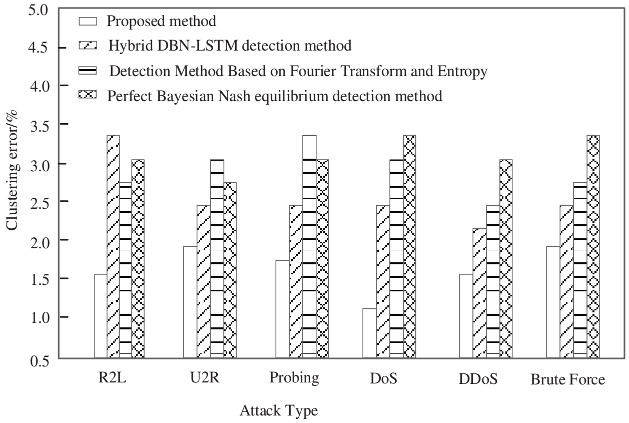


Figure 9: Comparison results of SSB values

Analyzing the test results in Fig. 9, it can be seen that the SSB value of the proposed method for air traffic control network security attack behavior is less than 2%. The minimum SSB values for Hybrid DBN-LSTM detection method, Detection Method Based on Fourier Transform and Entropy, and Perfect Bayesian Nash equilibrium detection method are 2.2%, 2.4%, and 2.7%. From this it can be seen that the proposed method has a smaller SSB value and better clustering detection performance for air traffic control network security attack behavior.

4 Discussion

According to the experimental results, the proposed method performs well in testing indicators such as detection rate, clustering accuracy, false detection rate, and recall rate. The detection rate remains around 98%, clustering accuracy remains at 97%, false detection rate remains below 1%, and recall rate is above 97%. However, the experimental results also have some limitations and uncertainties, and possible sources of error and influencing factors are as follows.

Firstly, the reliability of the experimental results is influenced by the selection and quality of the dataset. In this experiment, three sets of experimental attack behavior datasets were used as test subjects, but these datasets may not fully represent various attack behavior situations in the real world. Therefore, the generalization ability and applicability of the experimental results have certain limitations.

Secondly, there may be differences in the comparison methods used in the experiment. Although three similar methods were selected for comparative testing, the specific implementation and parameter settings of these methods may be different. Therefore, these differences may have a certain impact on the experimental results. In addition, other factors that were not considered, such as the complexity of the algorithm, the quantity and quality of training data, may also have an impact on the experimental results.

In addition, there are potential sources of error in the experiment. For example, there may be errors or biases in the data preprocessing process, which may affect the experimental results. In addition, the selection of evaluation indicators in the experiment may also have an impact on the results, as different evaluation indicators have different focuses on measuring algorithm performance.

Finally, the experimental results may also be limited by experimental settings and environmental conditions. For example, the hardware devices, software tools, and experimental procedures used in the experiment may have an impact on the experimental results. In addition, there may be other factors that were not considered in the experiment, such as noise during data collection, bias of specific data samples, etc., all of which may introduce errors.

In summary, although the experimental results show that the proposed method performs well on multiple indicators, it is still necessary to pay attention to the limitations and uncertainties of the experiment. Further research can consider expanding the size of the dataset, increasing the number and diversity of comparison methods, optimizing the experimental process and the selection of evaluation indicators to evaluate the performance and robustness of the proposed methods more comprehensively.

5 Conclusion

Aiming at the problem of air traffic control network security attacks, this paper designs a solution based on the cluster detection method. The experimental results show that this method can improve the security level of networks and information systems by extracting the characteristics of air traffic control network security attack behavior and using unsupervised learning methods to accurately identify and classify the attack. From an academic point of view, this study provides a new approach for research in the field of aggressive behavior detection to solve this problem. The advantages and limitations of attack behavior detection algorithms are better understood by comparing the performance of different methods. In terms of practical application, the research provides an effective tool and method for the field of network security, which can be used for practical defense and monitoring of attack behavior. This is of great significance to enterprises, organizations, and individuals, and can help improve the level of network security protection.

Future research can further explore the characteristics and behavior patterns of new network attacks, and develop corresponding clustering detection methods to deal with these new threats. At the same time, in the field of air traffic control network security, multi-source data, such as network traffic data, log records, and user behavior, can be integrated and analyzed to improve the accuracy and robustness of clustering detection methods.

Acknowledgement: I want to thank all those who helped me in writing this article. I would like to express my deepest gratitude to my supervisor, Professor Jianwei Zhang, for his continuous encouragement and guidance to me, and to Professor Yi Lin and Professor Yunxiang Han for their guidance. He led me through all the writing stages of this article. Without his consistent and enlightening guidance, this paper would not have been completed so quickly.

Funding Statement: This work was supported by National Natural Science Foundation of China (U2133208, U20A20161); National Natural Science Foundation of China (No. 62273244); Sichuan Science and Technology Program (No. 2022YFG0180).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Ruchun Jia, Yunxiang Han, Feike Yang; data collection, analysis and interpretation of results: Yi Lin, Ruchun Jia; draft manuscript preparation: Ruchun Jia, Jianwei Zhang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Due to the nature of this research, participants of this study did not agree for their data to be shared publicly, so supporting data is not available.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Perboli, M. Gajetti, S. Fedorov, and S. L. Giudice, "Natural language processing for the identification of human factors in aviation accidents causes: An application to the SHEL methodology," *Expert. Syst. Appl.*, vol. 186, no. 7, pp. 115694, 2021. doi: 10.1016/j.eswa.2021.115694.

[2] C. S. Stonesifer, D. E. Calkin, M. P. Thompson, and E. J. Belval, "Is this flight necessary? The aviation use summary (AUS): A framework for strategic, risk-informed aviation decision support," *Forests*, vol. 17, no. 8, pp. 1208–1221, 2021. doi: 10.3390/f12081078.

[3] J. M. Mateu, P. M. Fernández, and R. I. Franco, "Setting safety foundations in the Hyperloop: A first approach to preliminary hazard analysis and safety assurance system," *Saf. Sci.*, vol. 14, no. 2, pp. 1503–1512, 2021. doi: 10.1016/j.ssci.2021.105366.

[4] E. P. Paraschi, A. Georgopoulos, and M. Papanikou, "Safety and security implications of crisis-driven austerity HRM practices in commercial aviation: A structural equation modelling approach," *Saf. Sci.*, vol. 14, no. 13, pp. 1055–1067, 2022. doi: 10.1016/j.ssci.2021.105570.

[5] A. Chen, Y. Fu, X. Zheng, and G. Lu, "An efficient network behavior anomaly detection using a hybrid DBN-LSTM network," *Comp. Secur.*, vol. 114, no. 11, pp. 1–11, 2022. doi: 10.1016/j.cose.2021.102600.

[6] Z. Liu, C. Hu, and C. Shan, "Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method," *Comp. Secur.*, vol. 109, no. 10, pp. 102392, 2021. doi: 10.1016/j.cose.2021.102392.

[7] L. Liu, L. Zhang, S. Liao, J. Liu, and Z. Wang, "A generalized approach to solve perfect Bayesian Nash equilibrium for practical network attack and defense," *Inf. Sci.*, vol. 577, no. 1, pp. 245–264, 2021. doi: 10.1016/j.ins.2021.06.078.

[8] A. M. Alajlan and M. M. Almasri, "Malicious behavior detection in cloud using self-optimized dynamic kernel convolutional neural network," *Trans. Emerg. Telecomm. Technol.*, vol. 33, no. 5, pp. 4449–4475, 2022. doi: 10.1002/ett.4449.

[9] Y. Xu *et al.*, "Network threat detection based on group CNN for privacy protection," *Wirel. Commun. Mob. Comput.*, vol. 17, no. 2, pp. 1–20, 2021. doi: 10.1155/2021/3697536.

[10] Y. Xiao *et al.*, "A multitarget backdooring attack on deep neural networks with random location trigger," *Int. J. Intell. Syst.*, vol. 37, no. 3, pp. 2567–2583, 2022. doi: 10.1002/int.22785.

[11] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, "A novel approach for detection of APT malware using multi-dimensional hybrid Bayesian belief network," *Int. J. Inf. Secur.*, vol. 22, no. 1, pp. 119–135, 2023. doi: 10.1007/s10207-022-00631-5.

[12] S. Gavini, B. A. Vinaya, and M. Divya, "Improved security in cloud using sandpiper and extended equilibrium deep transfer learning based intrusion detection," *Cluster Comput.*, vol. 25, no. 5, pp. 3129–3144, 2022. doi: 10.1007/s10586-021-03516-9.

[13] X. Liu, J. Ren, H. He, Q. Wang, and X. Song, "Low-rate DDoS attacks detection method using data compression and behavior divergence measurement," *Computers & Security*, vol. 100, no. 21, pp. 102107, 2021. doi: 10.1016/j.cose.2020.102107.

[14] S. Wan and Y. Liu, "A security detection approach based on autonomy-oriented user sensor in social recommendation network," *Int. J. Distrib. Sens. Netw.*, vol. 18, no. 3, pp. 2017–2461, 2022. doi: 10.1177/15501329221082415.

[15] Z. Zhang, Y. Zhang, J. Niu, and D. Guo, "Unknown network attack detection based on open-set recognition and active learning in drone network," *Trans. Emerg. Telecomm. Technol.*, vol. 33, no. 3, pp. 4212, 2021. doi: 10.1002/ett.4212.

[16] Y. Li and X. Li, "Research on multi-target network security assessment with attack graph expert system model," *Sci. Program.*, vol. 2021, no. 3, pp. 1–11, 2021. doi: 10.1155/2021/9921731.

[17] C. Do, D. Duong, and D. Hoang, "A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic," *J. Intell. Fuzzy Syst.*, vol. 40, no. 6, pp. 2465–2472, 2021. doi: 10.3233/JIFS-20246.

[18] M. R. Aliabadi, M. Seltzer, M. V. Asl, and R. Ghavamizadeh, "An efficient intrusion detection technique for resource-constrained cyber-physical systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 33, no. 1, pp. 100430, 2021. doi: 10.1016/j.ijcip.2021.100430.

[19] C. D. Xuan, "Detecting APT attacks based on network traffic using machine learning," *J. Web Eng.*, vol. 20, no. 1, pp. 171–190, 2021.

[20] F. Folino, G. Folino, M. Guarascio, F. S. Pisani, and L. Pontieri, "On learning effective ensembles of deep neural networks for intrusion detection," *Inf. Fusion*, vol. 72, no. 1, pp. 48–69, 2021. doi: 10.1016/j.inffus.2021.02.007.

[21] L. Duan, J. Zhou, Y. Wu, and W. Xu, "A novel and highly efficient botnet detection algorithm based on network traffic analysis of smart systems," *Int. J. Distrib. Sens. Netw.*, vol. 18, no. 3, pp. 182459–182476, 2022. doi: 10.1177/15501477211049910.

[22] G. Zheng, B. Gong, and Y. Zhang, "Dynamic network security mechanism based on trust management in wireless sensor networks," *Wirel. Commun. Mob. Comput.*, vol. 12, no. 3, pp. 1–10, 2021. doi: 10.1155/2021/6667100.

[23] X. Yin, Y. Zhu, and J. Hu, "A sub-grid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 1957–1967, 2021. doi: 10.1109/TII.2021.3102332.

[24] B. Hussain., Q. Du., B. Sun, and Z. Han, "Deep learning-based DDoS-attack detection for cyber-physical system over 5G network," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 860–870, 2021. doi: 10.1109/TII.2020.2974520.

[25] K. D. Lu, G. Q. Zeng, and X. Luo, "Evolutionary deep belief network for cyber-attack detection in industrial automation and control system," *IEEE Trans. Ind. Inform.*, vol. 17, no. 11, pp. 7618–7627, 2021. doi: 10.1109/TII.2021.3053304.

[26] U. Ahmed, C. W. Lin, and G. Srivastava, "Mitigating adversarial evasion attacks of ransomware using ensemble learning," *Comp. Electr. Eng.*, vol. 100, no. 114, pp. 1–16, 2022. doi: 10.1016/j.compeleceng.2022.107903.

[27] Y. Alharbi, A. Alferaidi, K. Yadav, G. Dhiman, and S. Kautish, "Denial-of-service attack detection over IPv6 network based on KNN algorithm," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, pp. 1–6, 2021. doi: 10.1155/2021/8000869.

[28] S. R. Isaac and J. Jasper, "A secure routing scheme to mitigate attack in wireless adhoc sensor network," *Comp. Secur.*, vol. 103, no. 2, pp. 102197, 2021. doi: 10.1016/j.cose.2021.102197.

[29] M. Marvi, A. Arfeen, and R. Uddin, "An augmented K-means clustering approach for the detection of distributed denial-of-service attacks," *Int. J. Netw. Manag.*, vol. 31, no. 6, pp. 1–23, 2021. doi: 10.1002/nem.2160.

[30] R. Sahay, G. Geethakumari, and B. Mitra, "A novel network partitioning attack against routing protocol in internet of things," *Ad Hoc Netw.*, vol. 121, no. 10, pp. 1–11, 2021. doi: 10.1016/j.adhoc.2021.102583.

[31] S. Sambangi, L. Gondi, and S. Aljawarneh, "A feature similarity machine learning model for DDoS attack detection in modern network environments for Industry 4. 0," *Comp. Electr. Eng.*, vol. 100, no. 10, pp. 107955–107983, 2022. doi: 10.1016/j.compeleceng.2022.107955.

[32] Y. Y. Chen, B. Xu, and J. Long, "Information security assessment of wireless sensor networks based on bayesian attack graphs," *J. Intell. Fuzzy Sys.*, vol. 41, no. 4, pp. 1–7, 2021. doi: 10.3233/JIFS-189711.

[33] A. Mairaj and A. Y. Javaid, "Game theoretic solution for an unmanned aerial vehicle network host under DDoS attack," *Comp. Netw.*, vol. 211, no. 5, pp. 1–15, 2022. doi: 10.1016/j.comnet.2022.108962.

[34] O. Yousuf and R. N. Mir, "DDoS attack detection in internet of things using recurrent neural network," *Comp. Electr. Eng.*, vol. 101, no. 14, pp. 1–14, 2022. doi: 10.1016/j.compeleceng.2022.108034.

[35] J. T. Wang and Z. X. Liu, "An active detection of compromised nodes based on en-route trap in wireless sensor network," *Int. J. Distrib. Sens. Netw.*, vol. 17, no. 8, pp. 102–114, 2021. doi: 10.1177/15501477211040367.

[36] S. Koksal, Y. Dalveren, B. Maiga, and A. Kara, "Distributed denial-of-service attack mitigation in network functions virtualization-based 5G networks using management and orchestration," *Int. J. Commun. Syst.*, vol. 34, no. 9, pp. 1–16, 2021. doi: 10.1002/dac.4825.

[37] X. Zhang, F. Zhu, J. Zhang, and T. Liu, "Attack isolation and location for a complex network cyber-physical system via zonotope theory," *Neurocomputing*, vol. 469, no. 16, pp. 239–250, 2022. doi: 10.1016/j.neucom.2021.10.070.

[38] Z. Liu, Y. Fang, C. Huang, and J. Han, "GraphXSS: An efficient XSS payload detection approach based on graph convolutional network," *Comp. Secur.*, vol. 114, no. 11, pp. 167–173, 2022. doi: 10.1016/j.cose.2021.102597.

[39] D. Han, Z. Wang, Y. Zhong, W. Chen, and X. Yin, "Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2632–2647, 2021. doi: 10.1109/JSAC.2021.3087242.

[40] J. Yang, Y. Guo, C. Guo, Z. Chen, S. Wang and B. Jiang, "A robust active distribution network defensive strategy against cyber-attack considering multi-uncertainties," *IET Gener. Transm. Distrib.*, vol. 16, no. 8, pp. 1–9, 2022. doi: 10.1049/gtd2.12443.

[41] Y. Chen, H. Zhang, Y. Wang, Y. Yang, X. Zhou and Q. M. J. Wu, "MAMA Net: Multi-scale attention memory autoencoder network for anomaly detection," *IEEE Trans. Med. Imag.*, vol. 40, no. 3, pp. 1032–1041, 2021. doi: 10.1109/TMI.2020.3045295.

[42] Z. Li, C. Lang, J. H. Liew, Y. Lia, and J. Feng, "Cross-layer feature pyramid network for salient object detection," *IEEE Trans. Image Process.*, vol. 30, pp. 4587–4598, 2021. doi: 10.1109/TIP.2021.3072811.

[43] M. P. Karpowicz, "Adaptive tuning of network traffic policing mechanisms for DDoS attack mitigation systems," *Eur. J. Control*, vol. 61, no. 9, pp. 101–118, 2021. doi: 10.1016/j.ejcon.2021.07.001.

[44] X. Xian, T. Wu, Y. Liu, W. Wang, and Y. Xiao, "Towards link inference attack against network structure perturbation," *Knowl. Based Syst.*, vol. 218, no. 2, pp. 106674, 2021. doi: 10.1016/j.knosys.2020.106674.

[45] C. Natalino, A. Udalcovs, L. Wosinska, O. Ozolins, and M. Furdek, "Spectrum anomaly detection for optical network monitoring using deep unsupervised learning," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1583–1586, 2021. doi: 10.1109/LCOMM.2021.3055064.

[46] L. Grbi, L. Kranjevi, and S. Drueta, "Machine learning and simulation-optimization coupling for water distribution network contamination source detection," *Sens.*, vol. 21, no. 4, pp. 1157, 2021. doi: 10.3390/s21041157.

[47] G. Li, Z. Liu, M. Chen, Z. Bai, and H. Ling, "Hierarchical alternate interaction network for RGB-D salient object detection," *IEEE Trans. Image Process.*, vol. 30, no. 5, pp. 3528–3542, 2021. doi: 10.1109/TIP.2021.3062689.

[48] N. Wang, Y. Gao, J. T. He, and J. Yang, "Robustness evaluation of the air cargo network considering node importance and attack cost," *Reliab. Eng. Syst. Saf.*, vol. 217, no. 1, pp. 594–608, 2022. doi: 10.1016/j.ress.2021.108026.

[49] K. Wang, Z. Hu, Q. Ai, Q. Liu, and Y. Cong, "Membership inference attack with multi-grade service models in edge intelligence," *IEEE Netw.*, vol. 35, no. 1, pp. 184–189, 2021. doi: 10.1109/MNET.011.2000246.

[50] J. Wang and X. Liu, "Cascading attack on trusted-relay quantum key distribution networks," *Commun. Theor. Phys.*, vol. 73, no. 6, pp. 1–5, 2021. doi: 10.1088/1572-9494/abeedc.

[51] X. J. Xu and H. L. Chang, "Automatic detection of security vulnerabilities in multi-thread interactive learning software system," *Comp. Simul.*, vol. 39, no. 4, pp. 335–340, 2022.

[52] H. J. S. Niu, "Flow-based attack detection and accommodation for networked control systems," *Int. J. Control*, vol. 94, no. 3, pp. 109–118, 2021. doi: 10.1080/00207179.2019.1621384.