






Research on Intrusion Detection Technology for Naval Ship Networks

Wenliang Xu  and Luhui Yang  

Jiangsu Automation Research Institute, Lianyungang 222061, Jiangsu, China
yangluhui005@foxmail.com

Abstract. To deal with the security threats faced by naval ship networks, this paper proposes an intrusion detection model, constructs a naval ship networks intrusion detection dataset by combining the business features of the naval ship networks, and validates the detection effect of the model. First, combined with the characteristics of the ship's network service, the data characteristics were analyzed. Based on the result of feature analysis, an intrusion detection model based on a deep belief network feature dimensionality reduction method and multi-class support vector machine is proposed. The intrusion detection dataset is constructed by collecting data in a simulated naval ship network. The model is validated based on the collected dataset. The experimental results denote that the proposed intrusion detection model can effectively identify the intrusive behaviors of the naval ship network with an accuracy of 97.15%.

Keywords: Naval ship networks · Intrusion detection · SVM

1 Introduction

The naval ship networks, as the core of information transmission of naval ship equipments, has gradually developed from a small system network to an integrated network of the whole ship, or even a formation integrated network of the naval fleet.

The naval ship networks have also gradually developed from a local, single closed network to a global, fully open network. While ensuring the interaction of information equipment on surface ships and submarines, the naval ship networks face various security threats from within and outside the naval ship networks, and once the naval ship networks are successfully attacked by the enemy, in minor cases it can lead to the leakage of internal information, and in serious cases, it can lead to the illegal interception, tampering, and forgery of target intelligence and operational instructions, thus causing incalculable losses. Therefore, the development of safe and efficient naval ship intrusion detection technology is of great significance for ensuring the safety of the naval ship networks.

Network attacks on naval ship networks are usually well-designed and the intrusion detection rules are not included in security software, such as 0-day attacks. Traditional rule-based intrusion detection methods have a low detection rate for such intrusions, with a high false alarm and leakage rate. Moreover, the general intrusion detection technology does not combine the business characteristics of naval ship networks and cannot

effectively improve the accuracy of ship network intrusion detection [1–4]. To improve the intrusion detection capability of naval ship networks, this paper determines the data features for naval ship networks intrusion detection based on the business characteristics of naval ship networks, based on the results of the feature analysis, this paper proposes a naval ship networks intrusion detection model based on deep belief network which could reduce the feature dimensionality and multi-classification support vector machine. Based on the collected naval ship networks intrusion detection dataset, the training and testing of the naval ship networks intrusion detection models are completed. The results show that the intrusion detection model proposed in this paper can effectively identify the intrusive behaviors of the naval ship networks, and the detection accuracy can reach 97.15%, which is better than the comparison algorithm.

2 Business Characteristics of Naval Ship Networks

There are significant differences between naval ship networks and the Internet in terms of device connectivity, message types, and communication cycles. The intrusion detection model applicable to the Internet cannot achieve optimal intrusion detection metrics in naval ship networks, so it is necessary to analyze the differences between naval ship networks and the Internet. In this paper, based on an in-depth study of the operational characteristics of the naval ship networks in terms of time system equipment, navigation equipment, communication equipment, early warning and detection equipment, command, and control equipment, weapon equipment, the following characteristics of the naval ship networks have been identified.

2.1 The Limited Number of Network Devices

As a closed LAN, the naval ship networks are not interconnected with the Internet, but only with the military's LAN through a limited number of channels. The number of network devices mounted on the naval ship networks is limited, so to better monitor the network posture of each device, each device can be numbered, and the device number and its interconnection relationship can be used as a dimensional feature of network communication.

2.2 The Limited Number of Message Types

The number of network devices in the naval ship networks is limited, and the network services between the various network devices are simple and clear. Each device in the naval ship networks needs to send only a limited number of network message types, and each device sends a different message type. Therefore, the message types can be numbered and the message types can be used as data characteristics.

2.3 Some Network Messages Are Cyclical

Some of the network traffic in the naval ship networks has a defined communication period, so the period of sending messages in the naval ship networks can be used as a feature for analysis.

2.4 Some Network Messages Are Time-Sensitive

According to the naval ship networks message protocol, some messages in the naval ship networks are sent in a certain time sequence. For example, device *A* sends a command to device *B*. After completing the command, device *B* replies to device *A* that it has completed the command. Device *B* cannot send a reply without receiving a request from device *A*. Therefore, the temporal relationship of communication in a naval ship network can be analyzed as a feature.

By analyzing the business characteristics of the above naval ship networks, based on the KDD CUP99 dataset, intrusion detection data characteristics of the naval ship networks were determined. These include 41 data features such as connection duration, protocol type, and network service type of the target host contained in the KDD CUP99 dataset, as well as the naval ship networks device number, message type number, the most recent interval between sending the same message, the average interval between sending the same message, and whether a command message has been sent in the last 0.3 s.

3 Naval Ship Networks Intrusion Detection Model

3.1 Detection Model

This paper proposes a naval ship networks intrusion detection model, the architecture of the model is shown in Fig. 1. The model is divided into a data collection and pre-processing module, a feature dimensionality reduction module, and an intrusion detection module. The data collection and pre-processing module is responsible for collecting network data to construct the dataset and pre-processing the dataset. The feature dimensionality reduction module is responsible for reducing the dimensionality of the dataset and reducing the computational complexity. The Intrusion Detection module is responsible for detecting network intrusions and outputting intrusion detection results.

The intrusion detection model training and testing process are as follows.

1. Real-time collection and pre-processing of intrusion detection data from the naval ship networks.
2. Reducing the dimensionality of the dataset using feature reduction algorithms.
3. The reduced-dimensional training dataset is fed into the detection algorithm to adjust the algorithm parameters, and the reduced-dimensional test dataset is fed into the intrusion detection algorithm to obtain intrusion detection results and calculate the model intrusion detection performance.

Where data pre-processing of the naval ship networks includes string data digitization and feature data normalization. There are some string data in the naval ship networks intrusion detection dataset, which cannot be directly calculated, and all strings need to be converted into numbers. In this paper, one-hot encoding [5] is used to convert the string data into numbers as shown in Table 1.

Because of the different units of each data feature, it is necessary to standardize the data of different data features to reduce the influence between the dimensions of each

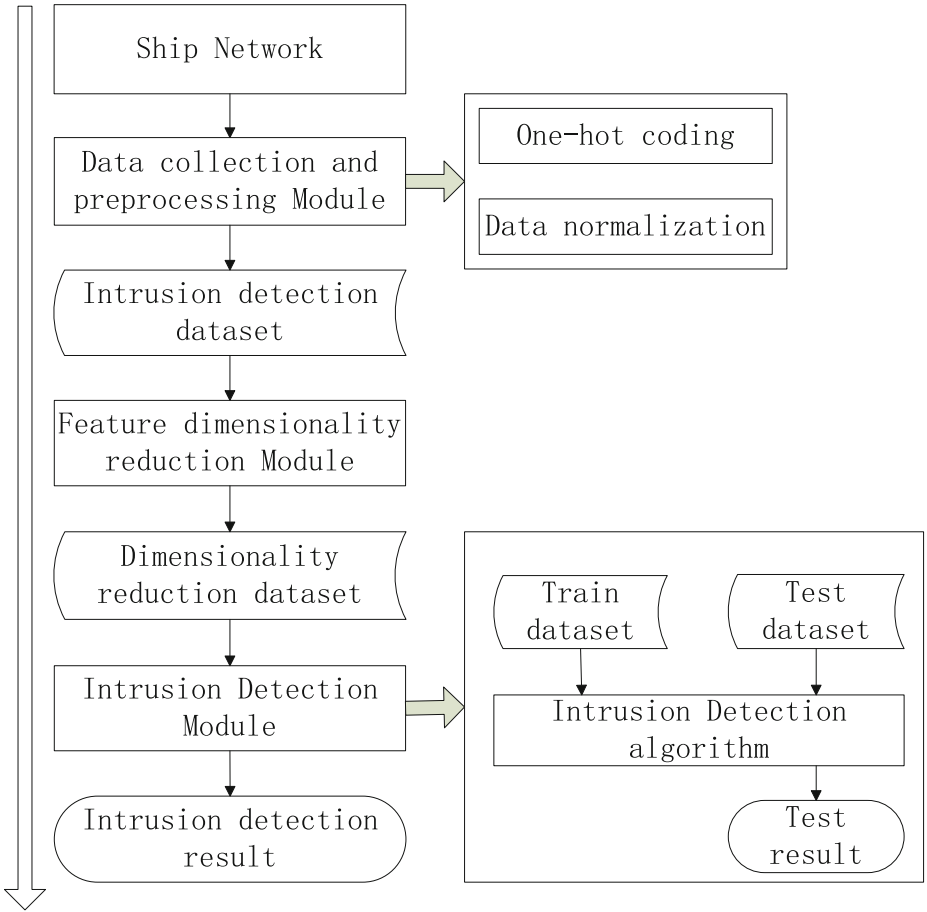


Fig. 1. Naval ship networks intrusion detection model

data feature. In this paper, the data is normalized by the following data normalization formula.

$$x' = \frac{x - MIN}{MAX - MIN} \tag{1}$$

Among them: x is the feature value, MIN is the minimum value of all data for that feature, and MAX is the maximum value of all data for that feature.

3.2 Feature Dimensionality Reduction Module Based on DBN

The number of features in the naval ship networks proposed in this paper is large, and when classifying based on the features, the high dimensionality of the data will lead to a large amount of intrusion detection computation, long detection time, and prone to dimensional disasters, which will affect the detection accuracy. Therefore, there is a need

Table 1. One-hot encoding converts strings to numbers

String data	Conversion results
“TPC”	[1,0,0]
“UDP”	[0,1,0]
“ICMP”	[0,0,1]
“Normal”	[1,0,0,0,0]
“Probe”	[0,1,0,0,0]
“DoS”	[0,0,1,0,0]
“U2R”	[0,0,0,1,0]
“R2L”	[0,0,0,0,1]

to reduce the dimensionality of the data to reduce the computation time and improve the detection accuracy [6].

Deep Belief Network [7, 8] is a typical neural network, widely used in the field of feature dimensionality reduction, which can learn and analyze data, adjust its parameters and establish a mapping from high-dimensional airborne to low-dimensional space to achieve the purpose of data dimensionality reduction.

To obtain dimensionality reduction data requires training DBN, first, input part of the training dataset into DBN, and the DBN will train each RBM from the bottom to the top in a layer-by-layer training method. Then, the DBN will be trained by a supervised learning method, the pre-processed intrusion detection data will be input to the DBN to get the output data, and then the back propagation algorithm will be used to propagate the error between the output data and the actual data layer by layer to adjust the DBN parameters to the optimal [9]. Finally, the pre-processed intrusion detection data is input to the DBN, and the dimensionality reduction data is obtained in the final hidden layer of the DBN.

3.3 Intrusion Detection Module Based on Multi-class SVM

The naval ship networks intrusion detection algorithm purposed in this paper is used to classify the input naval ship networks data into normal data and various types of intrusion data. However, the structure of naval ship network data is complex and simple classifiers such as the K-nearest neighbor algorithm and decision tree algorithm are not effective in classifying normal network behavior and network intrusion behavior. In this paper, Support Vector Machine (SVM) [10, 11] is used to classify the data, and the training dataset is used to find the classification hyperplane, which can make the separation interval of the naval ship networks data as large as possible and can identify the network intrusion more accurately.

SVM can only classify the input data into 2 categories and cannot accurately distinguish between normal network behavior, Probe intrusion, Dos intrusion, U2R intrusion, and R2L intrusion. In this paper, a multi-class SVM is used to differentiate between normal network behavior and various types of network intrusions. In this paper, we

construct a multi-class SVM (see Fig. 2).The classification functions of each SVMs are shown in Table 2.

Table 2. The classification functions of each SVMs

The ID of SVM	Classification type	Possible types on the left	Possible types on the right
SVM1	Normal, R2L	Normal, Probe, Dos, U2R	Probe, Dos, U2R, R2L
SVM2	Normal, U2R	Normal, Probe, Dos	Probe, Dos, U2R
SVM3	Probe, R2L	Probe, Dos, U2R	Dos, U2R, R2L
SVM4	Normal, Dos	Normal, Probe	Probe, Dos
SVM5	Probe, U2R	Probe, Dos	Dos, U2R
SVM6	Dos, R2L	Dos, U2R	U2R, R2L
SVM7	Normal, Probe	Normal	Probe
SVM8	Probe, Dos	Probe	Dos
SVM9	Dos, U2R	Dos	U2R
SVM10	U2R, R2L	U2R	R2L

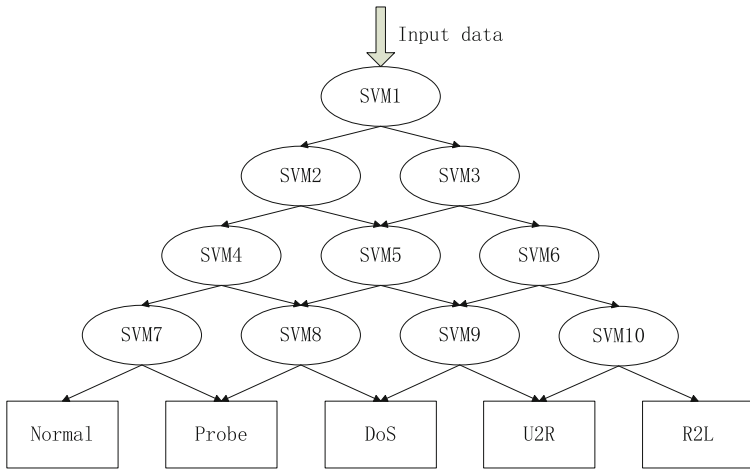


Fig. 2. Multi-class SVM

4 Naval Ship Networks Intrusion Detection Experiments

4.1 Intrusion Detection Evaluation Indicators

The main performance evaluation indicators for intrusion detection are intrusion detection Accuracy, False Alarm Rate, Missing Rate, etc. Among them, Accuracy represents

the ratio of the number of samples with correct intrusion detection results to the number of all samples; the False Alarm Rate represents the ratio of the number of normal network behaviors flagged as network intrusions by the intrusion detection system to the number of normal network behaviors; the Missing Rate represents the ratio of the number of network intrusions flagged as normal by the intrusion detection system to the total number of network intrusions.

Network intrusion detection Accuracy calculation formula.

$$A_{CC} = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

Network intrusion detection Missing Rate calculation formula.

$$M_R = \frac{FP}{FP + TN} \quad (3)$$

Network intrusion detection False Alarm Rate calculation formula.

$$F_A = \frac{FN}{TP + FN} \quad (4)$$

Among them, TP represents the number of normal network behaviors judged as normal network behaviors; TN represents the number of intrusions behaviors judged as network intrusions behaviors; FP represents the number of intrusions behaviors judged as normal network behaviors; FN represents the number of normal network behaviors judged as network intrusions behaviors.

4.2 Naval Ship Networks Intrusion Detection Dataset

The intrusion detection model for naval ship networks used in this paper uses machine learning algorithms that require large amounts of data as learning samples. We simulate a network attack in a simulated naval ship network while collecting a large amount of data according to the data characteristics described in Chap. 2. The dataset is randomly divided into a training dataset and a testing dataset in a 4:1 ratio for naval ship networks intrusion detection. The amount of data for each type of network behavior in the dataset is shown in Table 3.

Table 3. The quantity of various data in the naval ship networks intrusion detection dataset

Types of network behavior	Training set (10,000 entries)	Test set (10,000 entries)
Normal	640.94	159.95
Probe	28.23	6.67
DoS	80.12	20.38
U2R	24.52	6.76
R2L	26.31	6.44

4.3 Naval Ship Networks Intrusion Detection Experiments and Analysis of Results

To test the performance of the naval ship networks intrusion detection model mentioned in Chap. 3, this paper verifies the accuracy, false alarm rate, and missed alarm rate of the model in naval ship networks intrusion detection through experiments. When the SVM is used as the classifier, the Gaussian radial basis kernel function is selected, the parameter gamma of the kernel function is set to 3, and the penalty factor of the SVM is set to $C = 316$, DBN will adopt a 7-layer network structure, and the number of neurons in each layer of DBN is 200, 143, 106, 85, 53, 25, and 5 from the bottom to the top.

This paper also compares the effect of using the DBN dimensionality reduction algorithm with the PCA dimensionality reduction algorithm and not using the dimensionality reduction algorithm on the intrusion detection results, as shown in Table 4. The results show that using DBN dimensionality reduction achieves the best detection results, with an accuracy rate of 97.15% and false alarm and missed alarm rates of only 2.59% and 3.88%, the detection results are significantly better than the use of PCA and no dimensionality reduction algorithm result.

Table 4. Feature dimensionality reduction algorithm comparison

Dimensionality reduction algorithms	Accuracy (%)	False alarm rate (%)	Missing rate (%)
DBN	97.15	2.59	0.87
PCA	90.42	8.12	2.98
Not use	95.27	3.94	1.84

The multi-classification results of the algorithm in this paper for the different types of intrusions as shown in Table 5. Table cell data is expressed as the number of recognized results (column labels) of actual network behaviors (row labels), in units of 10,000. The results show that the algorithm in this paper achieves good detection results for each type of intrusion.

Table 5. Intrusion detection identification results

Real	Result				
	Normal	Probe	DoS	U2R	R2L
Normal	155.8	1.31	0.81	1.42	0.61
Probe	0.13	6.32	0.07	0.06	0.09
DoS	0.12	0.19	19.84	0.14	0.09
U2R	0.04	0.09	0.12	6.44	0.07
R2L	0.06	0.09	0.14	0.06	6.09

The comparison of the experimental results shows that the dimensionality reduction algorithm based on DBN and the multi-class SVM algorithm can effectively identify various types of network intrusions, with high Accuracy and low False Alarm Rate and Missing rates. Confirmed the feasibility of the naval ship networks intrusion detection model in this paper.

5 Conclusion

In this paper, the intrusion detection technology of naval ship networks is studied to meet the needs of naval ship network security protection. The data characteristics of the naval ship networks intrusion detection dataset are proposed by analyzing the business characteristics of the naval ship networks. A ship network intrusion detection model based on the DBN dimensionality reduction algorithm and multi-class SVM algorithm is proposed. The network data is collected in a simulated naval ship network, a naval ship networks intrusion detection dataset is constructed and experiments are conducted to verify the feasibility of using DBN for naval ship networks data dimensionality reduction and multi-class SVM for intrusion detection.

In terms of intrusion detection data features of the naval ship networks, this paper only adds a small number of data features based on the existing feature set in the KDD CUP99 dataset. It is necessary to further analyze more dimensional business characteristics of naval ship networks, and at the same time provide for naval ship networks intrusion detection High-quality dataset. At the same time, this article adopts an offline and post-event detection method. To improve the efficiency of intrusion detection, an online and real-time detection method suitable for the massive data of the naval ship networks will be studied.

References

1. Benedetto, M.S., Anastasija, C., Niels, A.N.: Training guidance with KDD cup 1999 and NSL-KDD data sets of ANIDINR: anomaly-based network intrusion detection system. *Procedia Comp. Sci.* **175**, 560–565 (2020)
2. Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J., Bayne, E., Bellekens, X.: Utilising deep learning techniques for effective zero-day attack detection. *Elect.* **9**(10), 1684 (2020)
3. Hausken, K., Welburn, J.W.: Attack and defense strategies in cyber war involving production and stockpiling of zero-day cyber exploits. *Inf. Syst. Front.* **23**(6), 1609–1620 (2020). <https://doi.org/10.1007/s10796-020-10054-z>
4. Wang, Z., Xu, Z., He, D., Chan, S.: Deep logarithmic neural network for Internet intrusion detection. *Soft. Comput.* **25**(15), 10129–10152 (2021). <https://doi.org/10.1007/s00500-021-05987-9>
5. Okada, S., Ohzeki, M., Taguchi, S.: Efficient partition of integer optimization problems with one-hot encoding. *Scient. Reports* **9**(1), 13036–13036 (2019)
6. Femi, E.A., Sakinat, O.F., Adebayo, A., Abayomi, A., Adebola, O.A., Joseph, B.A.: Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. *Inform. Security J.: A Glob. Perspect.* **29**(6), 267–283 (2020)
7. Sützen, A.A.: Developing a multi-level intrusion detection system using hybrid-DBN. *J. Ambient. Intell. Humaniz. Comput.* **12**(2), 1913–1923 (2020). <https://doi.org/10.1007/s12652-020-02271-w>

8. Velliangiri, S., Karthikeyan, P., Vinoth, K.: Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *J. Exp. Theoret. Artif. Intell.* **33**(3), 405–424 (2020)
9. Metawa, N., Pustokhina, I.V., Pustokhin, D.A., Shankar, K., Elhoseny, M.: Computational intelligence-based financial crisis prediction model using feature subset selection with optimal deep belief network. *Big Data* **9**(2), 100–115 (2021)
10. Xiaolong, L., Jinxiang, Y., Yifan, F., Mengxing, X., Xin, Q., Huiming, L.: Rapid monitoring of heavy metal pollution in lake water using nitrogen and phosphorus nutrients and physicochemical indicators by support vector machine. *Chemosphere* **280**, 130599–130599 (2021)
11. Yizhang, W., Tingting, G., Muhammad, H., Qiang, L., Sa, H., You, Z.: A feature extraction based support vector machine model for rectal cancer T-stage prediction using MRI images. *Multimedia Tools Appl.* **80**(20), 30907–30917 (2021)