Abnormal Traffic Detection in Industrial Control Networks Using a CNN-LSTM Fusion Model

Dinghui Lyu[1,2,*]
[1]Puyang Vocational and Technology College, Puyang, Henan 457000, China
[2]Puyang Institute of Technology, Henan University, Puyang, Henan 457000, China
E-mail: ldinghuidh@hotmail.com
[*]Corresponding author

Keywords: Industrial control network, abnormal traffic, CNN, LSTM

Received: October 30, 2025

This paper used a combination of two neural network models, convolutional neural network (CNN) and long short-term memory (LSTM), to detect abnormal traffic in industrial control networks. The performance of the support vector machine (SVM), traditional back-propagation neural network (BPNN), gated recurrent unit, and the CNN-LSTM algorithms were compared using the natural gas pipeline dataset from the University of Mississippi and the public KDDCUP99 dataset. Moreover, ablation experiments were conducted on the proposed algorithm. Finally, the performance of the four algorithms was evaluated in a laboratory-built industrial control network. The results showed that the CNN-LSTM algorithm was highly effective in detecting abnormal traffic. For the natural gas pipeline dataset, this algorithm achieved an accuracy of 0.998 ± 0.014, a false alarm rate of 0.010 ± 0.011, and a precision of 0.994 ± 0.012. For the KDDCUP99 dataset, its accuracy, false alarm rate, and precision were 0.995 ± 0.011, 0.004 ± 0.013, and 0.997 ± 0.011, respectively. Moreover, both the CNN and LSTM parts contributed to the overall performance.

Povzetek: Članek pokaže, da kombinacija CNN in LSTM učinkovito zaznava anomalije v industrijskih omrežjih ter dosega zelo visoko natančnost in nizko stopnjo lažnih alarmov.

1 Introduction

With industrial development and the advancement of the "Internet Plus Advanced Manufacturing" strategy, traditional industrial control systems are gradually evolving toward a more open industrial Internet [1]. This transformation has not only enhanced production efficiency and enabled remote monitoring and intelligent decision-making but also broken down the original physical isolation barriers of industrial control systems. As a result, industrial networks are now exposed to cybersecurity threats. Once an industrial network is compromised, it can lead to significant economic losses and pose risks to personal safety, environmental safety, and even national security [2]. Compared with traditional information technology networks, an industrial control network (ICN) utilizes proprietary communication protocols. Data transmission in ICNs is characterized by periodicity, low rates, and determinism. Traditional methods for detecting abnormal traffic in networks include rule-based, statistics-based, and early machine learning approaches. However, rule-based detection methods are difficult to deal with unknown attacks and can be troublesome to maintain. Statistics-based detection methods have difficulty dealing with non-linear data. Early machine learning algorithms often present complexities in feature processing and lack generalization [3]. Deep learning algorithms have the ability to perform nonlinear fitting and automatic data feature extraction; therefore, they can effectively handle data with complex features. The relevant research is shown in Table 1. Some studies focus on detecting abnormal behaviors in ICNs, others on identifying internal files, and some use firewalls to counter abnormal traffic in ICNs. This paper, however, focuses on the detection of abnormal traffic in ICNs. It combines two neural network algorithms, a convolutional neural network (CNN) and a long short-term memory (LSTM). The CNN is used to extract the characteristics of ICN traffic, while the LSTM is used to identify the characteristics extracted by CNN according to the time series to determine whether the traffic is abnormal.

In order to accurately detect abnormal traffic in ICNs, this paper combines the strength of two deep learning models, CNN and LSTM, to improve the accuracy in detecting abnormal traffic. Moreover, simulation experiments demonstrate that the CNN-LSTM algorithm exhibits superior accuracy, lower false alarm rates, and higher precision compared to traditional methods.

Table 1: Related works

Author	Research content	Research results
Chen et al. [4]	They proposed a multi-branch convolutional fusion neural network	This method could maintain a higher processing accuracy while

	method to improve the accuracy and efficiency of abnormal behavior detection in Internet of Things industrial control systems.	maintaining a high processing speed.
Yin et al. [5]	They proposed a MapReduce anomaly data mining and detection algorithm based on Hadoop distributed file system and deep neural network.	The algorithm can control the missed detection rate and the number of wrongly detected folders through the segmentation detection strategy.
Zhou et al. [6]	They optimized the industrial firewall whitelist using the genetic algorithm-support vector machine algorithm to enable it to learn rules independently.	This algorithm had a high detection accuracy and a short detection time for abnormal industrial control data.

2 Abnormal traffic detection based on an improved neural network model

Traditional techniques for detecting ICN traffic data are difficult to deal with unknown attacks and have poor performance in recognizing data with nonlinear characteristics. In contrast, deep learning algorithms have the ability of nonlinear fitting and can effectively deal with nonlinear feature data, suggesting good generalization [7]. CNNs use convolutional structures to extract local features from data, combine local features into overall abstract features, and then determine the type of ICN traffic data based on the extracted features. LSTM networks, an extension of recurrent neural networks, accounts for both current and past inputs during computational processing, thus effectively capturing time series features within traffic data [8]. Both CNN and LSTM have unique advantages when it comes to detecting ICN traffic data. CNNs can fully extract the spatial state features from current network traffic to identify current abnormal states, while LSTMs can extract the connection features from the time series of the network traffic data to predict possible future abnormal states [9, 10].

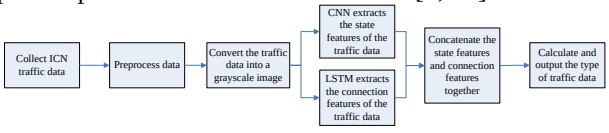

Figure 1: The process of an improved neural network for detecting the ICN traffic data

The process of an improved neural network for detecting ICN traffic data is shown in Figure 1.

① The traffic data is collected from the ICN, which is represented as:

$$\begin{cases} P = \{q^1, q^2, \cdots q^i\} \\ q^i = (x^i, l^i, t^i) \\ f^j = (x^j, l^j, d^j, t^j) \\ F = \{f^1, f^2, \cdots f^j\} \end{cases}, \quad (1)$$

where P is the collection of all data packets in the traffic data, q^i is the i-th packet in the traffic data, x^i is the five-tuple information (origin, destination IP, origin, destination port, transport protocol) of q^i, l^i is the byte length of q^i, t^i is the transmission time of q^i, f^j is the j-th unidirectional flow of the traffic data after collation, x^j is the five-tuple information of the data packets in unidirectional flow f^j, l^j is the total byte length of all data packets in the unidirectional flow, d^j is the duration of all data packets in the unidirectional flow, i.e., the time interval between the earliest and latest data packets sent out, f^1 is the time when the earliest data packet in the unidirectional flow is sent out, and F is the collection of all unidirectional flows.

② The collected traffic data is preprocessed. First, any incomplete or duplicate packets are cleaned up. The data within the traffic data packets is trimmed to the same byte length [11], the first 900 bytes of the data packets.

③ The traffic data is converted to grayscale images. Each byte in the data packet is used as a grayscale pixel value. If the data within the data packet is less than 900 bytes, additional 0x00 bytes are appended to the end to ensure it reaches the full 900-byte length. After cropping the data packet, 900 grayscale pixels can be obtained. These pixels are arranged in the order of bytes to form a 30×30 grayscale image.

④ This grayscale image is input into the CNN for feature extraction. In the convolutional layer, convolution kernels are employed to extract convolutional features from the input image [12]:

$$H_i = \sigma(H_{i-1} \otimes \omega_i + b_i), \quad (2)$$

where H_i and H_{i-1} are the feature map of outputs in the i-th and $i-1$-th layers, ω_i is the weight in the i-th layer structure, b_i is the bias in the i-th layer structure, and $\sigma(\cdot)$ is the activation function. The pooling layer compresses the convolutional features extracted from the convolutional layer, and max-pooling is employed in this paper. The global pooling layer compresses each convolutional feature map output by the previous layer to a size of 1 × 1. Finally, convolutional features after global pooling [13] are output in the output layer.

⑤ The byte matrix corresponding to the grayscale image is input into the LSTM for forward computation [14].

⑥ The spatial feature vectors and connection feature vectors extracted by the CNN and LSTM are then concatenated. Forward computation is performed in the fully connected layer to obtain the fusion vector.

⑦ The fusion vector uses the softmax function [15] to calculate the probability distribution of various types of abnormalities in the traffic data in the output layer. Ultimately, the abnormality type with the highest probability is output.

3 Simulation experiment

3.1 Experimental environment

The basic architecture of the ICN built in a laboratory during the simulation experiment is shown in Figure 2. For ease of setup and subsequent simulation experiments, only one server was used as the ICN server, connected to a programmable logic controller (PLC), Ethernet bus coupler, and camera via a router. The PLC used the hyper text transfer protocol (HTTP), the Ethernet bus coupler used the transmission control protocol (TCP), and the camera used the file transfer protocol (FTP). In addition, to simulate the scenario of abnormal traffic attacking the ICN, a second server was established to connect to the router and function as a third-party attacker. The maximum transmission rate of the built ICN was 100 MB/s, and the maximum delay was 20 ms.

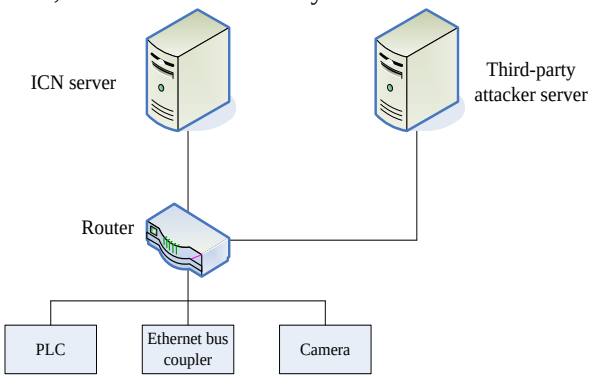

Figure 2: Basic architecture of the ICN in the simulation experiment

3.2 Experimental project

(1) Performance testing of the abnormal traffic detection algorithm

The abnormal traffic detection algorithm based on an improved neural network was simulated first. The datasets used in the tests were from the public industrial control system network dataset provided by the University of Mississippi and the public KDDCUP99 dataset. From the natural gas pipeline dataset at the University of Mississippi public dataset, 20,000 data points were selected, including eight types of attacks. Specifically, there were 2,500 data points for each attack type, of which 1,500 pieces were used as the training set and the remaining 1,000 pieces as the test set. Similarly, 20,000 data points were selected from the KDDCUP99 dataset, including five types of attacks, with 4,000 data points for each attack type, of which 2,500 were used as the training set and the remaining 1,500 as the test set.

Table 2: Relevant parameters of the abnormal traffic detection algorithm based on the improved neural network.

Structure	**Parameter setting**	**Structure**	**Parameter setting**
CNN input layer	30×30	Convolutional layer 1	32 convolution kernels (2×2), a step size of 1, the ReLU activation function
Pooling layer 1	2×2 max-pooling, a step size of 2	Convolutional layer 2	64 convolution kernels (2×2), a step size of 2, the ReLU activation function
Pooling layer 2	4×4 max-pooling, a step size of 4	Convolutional layer 3	128 convolution kernels (1×1), a step size of 1, the ReLU activation function
Global pooling layer	Max pooling	LSTM input layer	30×30
LSTM hidden layer	28 nodes, ReLU activation function	Fully connected layer	1,024 nodes, the ReLU activation function
Output layer	Softmax activation function	Learner	Adam
Learning rate	0.01	Times of learning	500

Note: ReLU: rectified linear unit

The relevant parameters of the abnormal traffic detection algorithm based on the improved neural network are shown in Table 2. In addition, to verify the performance of this algorithm for detecting abnormal traffic in ICN, it was compared with three other algorithms, namely the SVM algorithm, the traditional BPNN algorithm, and the gated recurrent unit (GRU) algorithm. In the SVM, the sigmoid kernel function and a penalty parameter of 1 were used. The relevant parameters of the BPNN were set as follows: 16 nodes in the input layer, 32 nodes in the hidden layer, and eight nodes in the output

layer; the ReLU activation function was used in the hidden layer. The relevant parameters of the GRU algorithm were as follows: there were 16 nodes in the input layer, 28 nodes in the hidden layer, and 8 nodes in the output layer, and the ReLU activation function was also used in the hidden layer. When training the above three algorithms, the same training set as that of the proposed algorithm was used, and the same test set was used during testing.

(2) Ablation experiments for the CNN-LSTM abnormal traffic detection algorithm

The abnormal traffic detection algorithm, which is based on the improved neural network, identifies abnormalities by combining the traffic data features extracted by the CNN and LSTM algorithms. To evaluate the contribution of the CNN and LSTM parts to the overall algorithm's performance, ablation experiments were conducted on the improved neural network model. In the ablation experiment, the CNN and LSTM parts were eliminated respectively, while the structure and parameters of the remaining parts remained unchanged. The performance of the algorithm in detecting abnormal traffic after eliminating a part of the structure was then tested and compared to that of the complete algorithm.

(3) Application of the abnormal traffic detection algorithm in ICN

The CNN-LSTM algorithm was tested in an ICN established in the laboratory. During the test, the PLC, Ethernet bus coupler, and camera within the ICN sent normal data to the ICN server via a router, while the third-party attacker server sent abnormal data to the ICN server. The types of abnormal data included remote-to-local (R2L), user-to-local (U2L), Probing, and denial of service (DoS).

3.3 Evaluation Indicators

The performance of the algorithm was measured by accuracy, false alarm rate, and precision. The calculation formulas are:

$$\begin{cases} ACC = \dfrac{TP + TN}{TP + TN + FP + FN} \\ FAR = \dfrac{FN}{TP + FN} \\ DR = \dfrac{TP}{TP + FP} \end{cases}, \quad (3)$$

where ACC, FAR, DR represent accuracy, false alarm rate, and precision, respectively, TP is the number of attack data classified as attack, TN is the number of normal data classified as normal, FP is the number of attack data classified as normal, and FN is the number of normal data classified as attack.

3.4 Experimental results

The SVM, traditional BPNN, GRU, and CNN-LSTM algorithm were evaluated using the natural gas pipeline dataset and the KDDCUP99 dataset. The results are shown in Table 3. It can be seen that the CNN-LSTM algorithm outperformed the others in identifying abnormal flow data in both datasets.

Table 3: Detection performance of the four algorithms

Algorithm	Dataset	Data type	ACC	FAR	DR
SVM	Natural gas pipeline dataset	Normal	0.423 ± 0.012	0.079 ± 0.013	0.483 ± 0.010
		NMRI	0.543 ± 0.013	0.126 ± 0.014	0.507 ± 0.014
		CMRI	0.441 ± 0.014	0.086 ± 0.012	0.550 ± 0.016
		MSCI	0.532 ± 0.011	0.099 ± 0.010	0.428 ± 0.013
		MPCI	0.521 ± 0.010	0.137 ± 0.013	0.438 ± 0.014
		MFCI	0.489 ± 0.014	0.132 ± 0.010	0.511 ± 0.012
		DoS	0.575 ± 0.013	0.088 ± 0.014	0.464 ± 0.011
		RECO	0.443 ± 0.012	0.054 ± 0.013	0.541 ± 0.012
		Overall	0.496 ± 0.011	0.100 ± 0.012	0.490 ± 0.013
	KDDCUP99 dataset	Normal	0.468 ± 0.010	0.101 ± 0.013	0.451 ± 0.014
		R2L	0.514 ± 0.013	0.100 ± 0.010	0.498 ± 0.016
		U2L	0.568 ± 0.011	0.044 ± 0.012	0.529 ± 0.013
		Probing	0.515 ± 0.013	0.159 ± 0.011	0.461 ± 0.012
		DoS	0.544 ± 0.013	0.068 ± 0.010	0.428 ± 0.011
		Overall	0.522 ± 0.012	0.094 ± 0.013	0.473 ± 0.013
BPNN	Natural gas pipeline dataset	Normal	0.719 ± 0.014	0.054 ± 0.012	0.782 ± 0.012
		NMRI	0.777 ± 0.015	0.078 ± 0.014	0.723 ± 0.010
		CMRI	0.710 ± 0.010	0.020 ± 0.010	0.775 ± 0.011
		MSCI	0.784 ± 0.011	0.063 ± 0.012	0.722 ± 0.012
		MPCI	0.757 ± 0.014	0.115 ± 0.011	0.735 ± 0.014

		MFCI	0.778 ± 0.021	0.068 ± 0.013	0.756 ± 0.011
		DoS	0.786 ± 0.013	0.059 ± 0.011	0.723 ± 0.013
		RECO	0.701 ± 0.014	0.039 ± 0.012	0.763 ± 0.012
		Overall	0.752 ± 0.011	0.062 ± 0.014	0.747 ± 0.010
	KDDCUP99 dataset	Normal	0.726 ± 0.022	0.030 ± 0.016	0.730 ± 0.014
		R2L	0.770 ± 0.013	0.054 ± 0.012	0.735 ± 0.012
		U2L	0.786 ± 0.018	0.021 ± 0.014	0.777 ± 0.013
		Probing	0.739 ± 0.016	0.074 ± 0.015	0.712 ± 0.011
		DoS	0.777 ± 0.011	0.037 ± 0.012	0.699 ± 0.012
		Overall	0.760 ± 0.012	0.043 ± 0.011	0.731 ± 0.013
GRU	Natural gas pipeline dataset	Normal	0.714 ± 0.013	0.059 ± 0.013	0.787 ± 0.010
		NMRI	0.771 ± 0.011	0.077 ± 0.012	0.725 ± 0.011
		CMRI	0.717 ± 0.011	0.021 ± 0.011	0.774 ± 0.011
		MSCI	0.789 ± 0.013	0.064 ± 0.010	0.726 ± 0.012
		MPCI	0.757 ± 0.011	0.116 ± 0.010	0.737 ± 0.013
		MFCI	0.771 ± 0.011	0.069 ± 0.011	0.754 ± 0.014
		DoS	0.787 ± 0.012	0.054 ± 0.013	0.726 ± 0.016
		RECO	0.703 ± 0.013	0.037 ± 0.014	0.765 ± 0.012
		Overall	0.758 ± 0.015	0.063 ± 0.015	0.749 ± 0.013
	KDDCUP99 dataset	Normal	0.729 ± 0.016	0.031 ± 0.016	0.737 ± 0.014
		R2L	0.774 ± 0.014	0.058 ± 0.012	0.731 ± 0.012
		U2L	0.782 ± 0.013	0.026 ± 0.014	0.779 ± 0.013
		Probing	0.737 ± 0.011	0.077 ± 0.013	0.714 ± 0.014
		DoS	0.775 ± 0.012	0.035 ± 0.013	0.698 ± 0.012
		Overall	0.761 ± 0.016	0.044 ± 0.011	0.739 ± 0.013
The CNN-LSTM algorithm	Natural gas pipeline dataset	Normal	0.996 ± 0.011	0.003 ± 0.010	0.993 ± 0.014
		NMRI	0.998 ± 0.015	0.003 ± 0.010	0.994 ± 0.012
		CMRI	0.999 ± 0.014	0.002 ± 0.011	0.993 ± 0.011
		MSCI	0.998 ± 0.012	0.001 ± 0.011	0.999 ± 0.013
		MPCI	0.999 ± 0.011	0.021 ± 0.013	0.992 ± 0.012
		MFCI	0.997 ± 0.013	0.012 ± 0.012	0.993 ± 0.011
		DoS	0.998 ± 0.015	0.011 ± 0.011	0.995 ± 0.010
		RECO	0.999 ± 0.014	0.023 ± 0.012	0.994 ± 0.013
		Overall	0.998 ± 0.014	0.010 ± 0.011	0.994 ± 0.012
	KDDCUP99 dataset	Normal	0.994 ± 0.013	0.002 ± 0.010	0.995 ± 0.014
		R2L	0.995 ± 0.012	0.001 ± 0.016	0.997 ± 0.012
		U2L	0.998 ± 0.010	0.003 ± 0.014	0.996 ± 0.013
		Probing	0.994 ± 0.010	0.011 ± 0.012	0.998 ± 0.014
		DoS	0.993 ± 0.011	0.004 ± 0.011	0.997 ± 0.010
		Overall	0.995 ± 0.011	0.004 ± 0.013	0.997 ± 0.011

To test the effectiveness of the CNN and LSTM parts in the proposed algorithm, ablation experiments were conducted, and the results are shown in Figure 3 and Table 4. It can be seen that removing either the CNN or the LSTM component led to a decrease in the algorithm's performance in detecting abnormal traffic. The algorithms that excluded the CNN part and the LSTM part exhibited similar performance in detecting abnormal traffic.

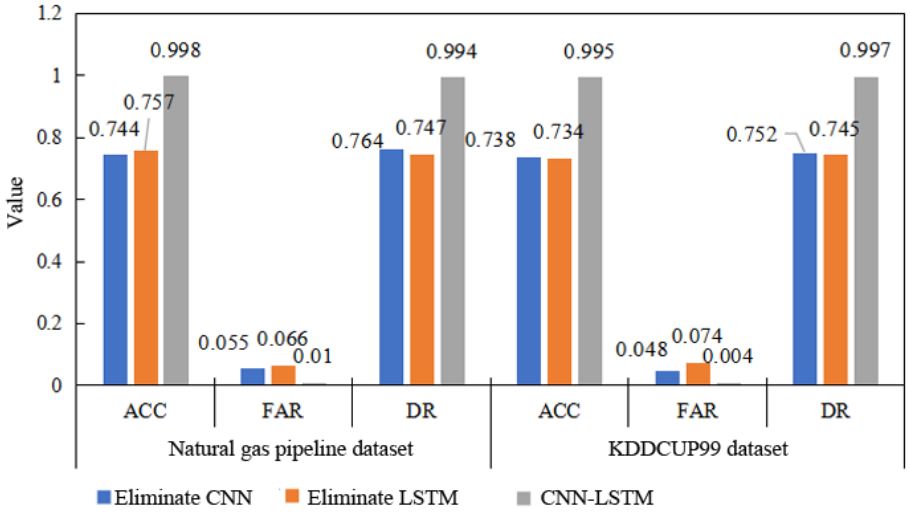

Figure 3: The ablation experiment results

Table 4: The ablation experiment results of the CNN-LSTM algorithm

Algorithm	Dataset	Data type	ACC	FAR	DR
The algorithm with the CNN part eliminated	Natural gas pipeline dataset	Normal	0.737 ± 0.011	0.027 ± 0.012	0.780 ± 0.013
		NMRI	0.700 ± 0.012	0.025 ± 0.013	0.759 ± 0.012
		CMRI	0.714 ± 0.013	0.061 ± 0.012	0.759 ± 0.011
		MSCI	0.767 ± 0.012	0.077 ± 0.011	0.788 ± 0.012
		MPCI	0.764 ± 0.011	0.083 ± 0.012	0.737 ± 0.014
		MFCI	0.711 ± 0.012	0.044 ± 0.014	0.750 ± 0.012
		DoS	0.780 ± 0.014	0.054 ± 0.012	0.764 ± 0.011
		RECO	0.782 ± 0.012	0.066 ± 0.011	0.777 ± 0.011
		Overall	0.744 ± 0.011	0.055 ± 0.011	0.764 ± 0.013
	KDDCUP99 dataset	Normal	0.747 ± 0.011	0.069 ± 0.013	0.779 ± 0.011
		R2L	0.707 ± 0.013	0.016 ± 0.011	0.729 ± 0.012
		U2L	0.750 ± 0.011	0.026 ± 0.012	0.774 ± 0.014
		Probing	0.747 ± 0.012	0.082 ± 0.014	0.755 ± 0.012
		DoS	0.738 ± 0.014	0.047 ± 0.012	0.722 ± 0.013
		Overall	0.738 ± 0.012	0.048 ± 0.013	0.752 ± 0.011
The algorithm with the LSTM part eliminated	Natural gas pipeline dataset	Normal	0.735 ± 0.013	0.051 ± 0.011	0.694 ± 0.012
		NMRI	0.771 ± 0.011	0.068 ± 0.012	0.765 ± 0.013
		CMRI	0.776 ± 0.012	0.079 ± 0.013	0.758 ± 0.015
		MSCI	0.747 ± 0.013	0.099 ± 0.015	0.725 ± 0.012
		MPCI	0.705 ± 0.015	0.046 ± 0.012	0.769 ± 0.013
		MFCI	0.761 ± 0.012	0.028 ± 0.013	0.766 ± 0.012
		DoS	0.776 ± 0.013	0.080 ± 0.012	0.721 ± 0.013
		RECO	0.784 ± 0.012	0.080 ± 0.013	0.776 ± 0.014
		Overall	0.757 ± 0.013	0.066 ± 0.014	0.747 ± 0.013
	KDDCUP99 dataset	Normal	0.751 ± 0.014	0.090 ± 0.013	0.736 ± 0.015
		R2L	0.703 ± 0.013	0.077 ± 0.015	0.769 ± 0.014
		U2L	0.775 ± 0.015	0.024 ± 0.014	0.772 ± 0.012
		Probing	0.712 ± 0.014	0.090 ± 0.012	0.725 ± 0.014
		DoS	0.729 ± 0.012	0.087 ± 0.014	0.725 ± 0.013
		Overall	0.734 ± 0.014	0.074 ± 0.013	0.745 ± 0.014
The CNN-	Natural gas	Normal	0.996 ± 0.013	0.003 ± 0.014	0.993 ± 0.011

LSTM algorithm	pipeline dataset	NMRI	0.998 ± 0.014	0.003 ± 0.011	0.994 ± 0.012
		CMRI	0.999 ± 0.011	0.002 ± 0.012	0.993 ± 0.011
		MSCI	0.998 ± 0.012	0.001 ± 0.011	0.999 ± 0.010
		MPCI	0.999 ± 0.011	0.021 ± 0.010	0.992 ± 0.014
		MFCI	0.997 ± 0.010	0.012 ± 0.014	0.993 ± 0.012
		DoS	0.998 ± 0.014	0.011 ± 0.012	0.995 ± 0.013
		RECO	0.999 ± 0.012	0.023 ± 0.013	0.994 ± 0.011
		Overall	0.998 ± 0.013	0.010 ± 0.011	0.994 ± 0.010
	KDDCUP99 dataset	Normal	0.994 ± 0.011	0.002 ± 0.010	0.995 ± 0.012
		R2L	0.995 ± 0.010	0.001 ± 0.012	0.997 ± 0.013
		U2L	0.998 ± 0.012	0.003 ± 0.013	0.996 ± 0.011
		Probing	0.994 ± 0.013	0.011 ± 0.011	0.998 ± 0.011
		DoS	0.993 ± 0.011	0.004 ± 0.011	0.997 ± 0.012
		Overall	0.995 ± 0.011	0.004 ± 0.012	0.997 ± 0.013

The four detection algorithms were tested in the ICN set up in the laboratory, and their performance in detecting abnormal traffic for different industrial equipment is shown in Table 5. It can be seen that the CNN-LSTM algorithm showed the best performance in identifying abnormal traffic data, whether it was in PLC, Ethernet bus coupler, or camera.

Table 5: The detection performance of four algorithms for abnormal traffic in the actual ICN

Algorithm	**Dataset**	**Data type**	**ACC**	**FAR**	**DR**
SVM	PLC	Normal	0.486 ± 0.013	0.081 ± 0.011	0.512 ± 0.014
		R2L	0.464 ± 0.011	0.107 ± 0.013	0.479 ± 0.012
		U2L	0.436 ± 0.010	0.106 ± 0.011	0.477 ± 0.011
		Probing	0.459 ± 0.012	0.073 ± 0.012	0.466 ± 0.013
		DoS	0.505 ± 0.013	0.148 ± 0.011	0.441 ± 0.015
		Overall	0.470 ± 0.011	0.103 ± 0.012	0.475 ± 0.012
	Ethernet bus coupler	Normal	0.545 ± 0.010	0.103 ± 0.013	0.556 ± 0.014
		R2L	0.431 ± 0.011	0.096 ± 0.014	0.531 ± 0.011
		U2L	0.499 ± 0.012	0.090 ± 0.012	0.482 ± 0.012
		Probing	0.491 ± 0.014	0.070 ± 0.013	0.453 ± 0.013
		DoS	0.551 ± 0.011	0.161 ± 0.011	0.511 ± 0.011
		Overall	0.503 ± 0.012	0.104 ± 0.011	0.507 ± 0.014
	Camera	Normal	0.487 ± 0.013	0.116 ± 0.012	0.482 ± 0.012
		R2L	0.514 ± 0.011	0.133 ± 0.013	0.437 ± 0.011
		U2L	0.511 ± 0.012	0.113 ± 0.012	0.491 ± 0.011
		Probing	0.430 ± 0.013	0.145 ± 0.011	0.403 ± 0.012
		DoS	0.494 ± 0.011	0.143 ± 0.012	0.518 ± 0.013
		Overall	0.487 ± 0.011	0.130 ± 0.013	0.466 ± 0.012
BPNN	PLC	Normal	0.717 ± 0.013	0.036 ± 0.014	0.775 ± 0.011
		R2L	0.695 ± 0.014	0.085 ± 0.015	0.727 ± 0.013
		U2L	0.719 ± 0.012	0.043 ± 0.013	0.713 ± 0.012
		Probing	0.756 ± 0.013	0.031 ± 0.011	0.757 ± 0.015
		DoS	0.761 ± 0.011	0.063 ± 0.012	0.700 ± 0.012
		Overall	0.730 ± 0.013	0.052 ± 0.011	0.734 ± 0.014
	Ethernet bus coupler	Normal	0.770 ± 0.012	0.068 ± 0.011	0.779 ± 0.013
		R2L	0.718 ± 0.014	0.021 ± 0.012	0.752 ± 0.011

		U2L	0.738 ± 0.010	0.022 ± 0.013	0.771 ± 0.011
		Probing	0.756 ± 0.011	0.022 ± 0.014	0.742 ± 0.012
		DoS	0.772 ± 0.012	0.110 ± 0.012	0.772 ± 0.010
		Overall	0.751 ± 0.013	0.049 ± 0.013	0.763 ± 0.010
	Camera	Normal	0.716 ± 0.012	0.078 ± 0.011	0.739 ± 0.011
		R2L	0.751 ± 0.013	0.068 ± 0.013	0.731 ± 0.012
		U2L	0.783 ± 0.014	0.088 ± 0.012	0.757 ± 0.013
		Probing	0.726 ± 0.012	0.091 ± 0.014	0.699 ± 0.011
		DoS	0.762 ± 0.011	0.079 ± 0.012	0.750 ± 0.015
		Overall	0.748 ± 0.012	0.081 ± 0.011	0.735 ± 0.011
GRU	PLC	Normal	0.714 ± 0.013	0.059 ± 0.013	0.787 ± 0.010
		R2L	0.771 ± 0.011	0.077 ± 0.012	0.725 ± 0.011
		U2L	0.717 ± 0.011	0.021 ± 0.011	0.774 ± 0.011
		Probing	0.789 ± 0.013	0.064 ± 0.010	0.726 ± 0.012
		DoS	0.757 ± 0.011	0.116 ± 0.010	0.737 ± 0.013
		Overall	0.771 ± 0.011	0.069 ± 0.011	0.754 ± 0.014
	Ethernet bus coupler	Normal	0.787 ± 0.012	0.054 ± 0.013	0.726 ± 0.016
		R2L	0.703 ± 0.013	0.037 ± 0.014	0.765 ± 0.012
		U2L	0.758 ± 0.015	0.063 ± 0.015	0.749 ± 0.013
		Probing	0.729 ± 0.016	0.031 ± 0.016	0.737 ± 0.014
		DoS	0.774 ± 0.014	0.058 ± 0.012	0.731 ± 0.012
		Overall	0.782 ± 0.013	0.026 ± 0.014	0.779 ± 0.013
	Camera	Normal	0.737 ± 0.011	0.077 ± 0.013	0.714 ± 0.014
		R2L	0.775 ± 0.012	0.035 ± 0.013	0.698 ± 0.012
		U2L	0.761 ± 0.016	0.064 ± 0.011	0.739 ± 0.013
		Probing	0.724 ± 0.013	0.059 ± 0.013	0.777 ± 0.010
		DoS	0.761 ± 0.011	0.047 ± 0.012	0.735 ± 0.011
		Overall	0.737 ± 0.011	0.031 ± 0.011	0.764 ± 0.011
CNN-LSTM	PLC	Normal	0.998 ± 0.011	0.003 ± 0.014	0.993 ± 0.012
		R2L	0.991 ± 0.012	0.002 ± 0.013	0.992 ± 0.011
		U2L	0.997 ± 0.013	0.008 ± 0.011	0.999 ± 0.013
		Probing	0.992 ± 0.011	0.004 ± 0.012	0.991 ± 0.012
		DoS	0.997 ± 0.012	0.011 ± 0.011	0.994 ± 0.011
		Overall	0.995 ± 0.013	0.006 ± 0.012	0.994 ± 0.012
	Ethernet bus coupler	Normal	0.995 ± 0.012	0.006 ± 0.012	0.992 ± 0.014
		R2L	0.991 ± 0.011	0.002 ± 0.011	0.998 ± 0.010
		U2L	0.997 ± 0.010	0.001 ± 0.012	0.992 ± 0.011
		Probing	0.998 ± 0.012	0.003 ± 0.013	0.998 ± 0.012
		DoS	0.998 ± 0.011	0.011 ± 0.011	0.998 ± 0.011
		Overall	0.996 ± 0.013	0.005 ± 0.012	0.996 ± 0.013
	Camera	Normal	0.992 ± 0.012	0.005 ± 0.011	0.993 ± 0.012
		R2L	0.997 ± 0.011	0.007 ± 0.010	0.996 ± 0.012
		U2L	0.999 ± 0.011	0.011 ± 0.012	0.998 ± 0.011
		Probing	0.993 ± 0.010	0.005 ± 0.012	0.993 ± 0.010
		DoS	0.998 ± 0.013	0.007 ± 0.013	0.996 ± 0.011
		Overall	0.996 ± 0.012	0.007 ± 0.014	0.995 ± 0.012

4 Discussion

With the development of Internet technology, industrial control systems are rapidly evolving toward networking, intelligence, and openness. ICNs are gradually connected to the Internet to achieve remote monitoring, data acquisition, and collaborative optimization. However, while connecting ICNs to the Internet improves production efficiency, it also expands the attack surface, making ICNs more vulnerable to network security threats. Detecting abnormal traffic in ICNs is the first line of defense for ensuring industrial control systems. Different from traditional information technology networks, the communication of industrial control systems has characteristics of strong real-time performance, protocol exclusivity, highly periodic traffic patterns, and extreme sensitivity to false alarms, making conventional intrusion detection algorithms difficult to apply directly. Traditional statistical-based identification methods can only target a single type of abnormal traffic. Against this background, deep learning technology provides a new approach for detecting abnormal traffic in ICNs. In deep learning technology, CNN is good at extracting local spatial features and is suitable for analyzing keyword patterns in the packet header or payload, while LSTM can effectively model long time series and is suitable for capturing temporal behaviors such as instruction streams and state transitions. By combining CNN and LSTM in this paper, it is possible to extract both spatial and temporal characteristics of the traffic in ICNs, thus better identifying abnormal traffic.

In this paper, a basic framework of the ICN was built in the laboratory, and simulation experiments were carried out. Firstly, the natural gas pipeline dataset from the University of Mississippi and the public KDDCUP99 dataset were used to test the CNN-LSTM algorithm. The algorithm was compared with SVM, BPNN, and GRU algorithms. Then, an ablation experiment was conducted. Finally, the abnormal traffic of three devices, namely PLC, Ethernet bus coupler, and camera, was tested in the built ICN. The experimental results showed that compared with the other three algorithms, the CNN-LSTM algorithm had superior performance in detecting abnormal traffic. The results of the ablation experiment showed that after removing the CNN part or the LSTM part, the detection performance of abnormal traffic decreased, indicating that both parts are very important for the algorithm. The reason is that the CNN part can effectively extract the spatial features of traffic data, and the LSTM part can analyze the temporal features of traffic data. Combining them can more accurately identify the abnormal traffic.

The innovation of this paper lies in combining CNN and LSTM, enabling the algorithm to integrate the spatial and temporal characteristics of traffic data. This allows for more accurate identification of abnormal traffic, providing an effective reference for ICN security protection. One of the limitations of this paper is that the spatial and temporal characteristics of traffic data, the algorithm were not extracted simultaneously. Moreover, the sample data used for training and testing was limited, which resulted in limited generalization ability of the algorithm. Additionally, there were only a limited number of indicators for evaluating the algorithm's performance. Therefore, the future research directions are to attempt parallel processing of the spatial and temporal characteristics of traffic data, expand the variety of training samples to enhance the generalization ability of the algorithm, and extend the performance evaluation indicators.

5 Conclusions

This paper combined two neural network models, CNN and LSTM, to detect abnormal traffic in ICN. In subsequent simulation experiments, the natural gas pipeline dataset from the University of Mississippi and the public KDDCUP99 dataset were chosen to compare the performance of the SVM, traditional BPNN, and CNN-LSTM algorithms. Ablation experiments were also conducted. Finally, the SVM, traditional BPNN, GRU, and CNN-LSTM algorithms were compared in the ICN built in the laboratory. It was found that the CNN-LSTM algorithm demonstrated the best performance in identifying abnormal traffic data for both the natural gas pipeline dataset and the KDDCUP99 dataset. Moreover, whether the CNN part or the LSTM part was eliminated, the performance of the algorithm decreased. Whether it is the abnormal traffic data from PLC, Ethernet bus coupler, or camera, the CNN-LSTM algorithm always performed best.

References

[1] Yan Q, Yu FR, Gong Q, Li J (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) Attacks in cloud computing environments: a survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, 18(1), pp. 602–622. https://doi.org/10.1109/COMST.2015.2487361.

[2] Kolias C, Kambourakis G, Stavrou A, Voas J (2017). DDoS in the IoT: Mirai and Other botnets. *Computer*, 50(7), pp. 80–84. https://doi.org/10.1109/MC.2017.201.

[3] Osanaiye O, Choo KKR, Dlodlo M (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network & Computer Applications*, 67(may), pp. 147–165. https://doi.org/10.1016/j.jnca.2016.01.001.

[4] Chen J, Liu B, Zuo H (2024). Abnormal behavior detection in industrial control systems based on CNN. *Alexandria Engineering Journal*, 107, pp. 643–651. https://doi.org/10.1016/j.aej.2024.08.109.

[5] Yin C, Pan C, Zhang P (2020). Deep neural network combined with MapReduce for abnormal data mining and detection in cloud storage. *Journal of Ambient Intelligence and Humanized Computing*, 2020(8), pp. 1–12. https://doi.org/10.1007/s12652-020-01996-y.

[6] Zhou X, Shi W (2024). Research on the optimisation of whitelisting technology for network firewall in

industrial control system using genetic algorithm. *International Journal of Communication Networks and Distributed Systems: IJCNDS*, 30(1), pp. 30–41. https://doi.org/10.1504/IJCNDS.2024.10060170.

[7] Saranya V, Umagandhi R (2017). A Comparative study of outlier detection in large-scale data using data mining algorithms. *International Journal of Data Mining and Emerging Technologies*, 7(1), pp. 10–15. https://doi.org/10.5958/2249-3220.2017.00002.7.

[8] Chaabene NEHB, Bouzeghoub A, Guetari R, Ghezala HHB (2022). Deep learning methods for anomalies detection in social networks using multidimensional networks and multimodal data: a survey. *Multimedia Systems*, 28(6), pp. 2133–2143. https://doi.org/10.1007/s00530-020-00731-z.

[9] Lishchytovych A, Pavlenko V, Shmatok A, Finenko Y (2020). Comparative analysis of system logs and streaming data anomaly detection algorithms. *Information Systems and Technologies Security*, 1(2), pp. 5–7. https://doi.org/10.17721/ists.2020.1.50-59.

[10] Wen H (2017). A new algorithm based on artificial intelligence to realize rapid detection and recognition of mass data abnormal point. *Boletin Tecnico/Technical Bulletin*, 55(6), pp. 364–371.

[11] Gugelmann D, Gasser F, Ager B, Lenders V (2015). Hviz: HTTP(S) traffic aggregation and visualization for network forensics. *Digital Investigation*, 12, pp. S1–S11. https://doi.org/10.1016/j.diin.2015.01.005.

[12] Liu C, Liu C, Liu C (2025). An abnormal traffic detection method for chain information management system network based on convolutional neural network. *Frontiers in Physics*, 13(13), pp. 1–12. https://doi.org/10.3389/fphy.2025.1592975.

[13] Chen L, Zhang T, Ma Y, Chen M (2024). Abnormal network traffic detection algorithm based on improved convolutional neural network. *2024 Proceedings of International Conference on Interactive Intelligent Systems and Techniques (IIST)*, IEEE, New York, pp. 733–739. https://doi.org/10.1109/iist62526.2024.00098.

[14] Beri M, Gill KS, Chauhan R, Pokhariyal HS (2024). Enhancing cybersecurity through anomaly detection in network traffic using convolutional neural networks: a sustainable development approach. *Proceedings of 2024 4th Asian Conference on Innovation in Technology (ASIANCON)*, IEEE, New York, pp. 1–5. https://doi.org/10.1109/asiancon62057.2024.10838103.

[15] Song J, Wang X, He M, Jin L (2023). CSK-CNN: network intrusion detection model based on two-layer convolution neural network for handling imbalanced dataset. *Information*, 14(2), pp. 17. https://doi.org/10.3390/info14020130.