Hindawi
Security and Communication Networks
Volume 2022, Article ID 5448647, 8 pages
https://doi.org/10.1155/2022/5448647

Research Article

Intelligent Intrusion Detection Method of Industrial Internet of Things Based on CNN-BiLSTM

Aichuan Li[1] **and Shujuan Yi**[2]

[1]*College of Information and Electrical Engineering, Heilongjiang Bayi Agricultural University, Daqing, Heilongjiang 163319, China*
[2]*Engineering Research Center of Processing and Utilization of Grain By-products, Ministry of Education, Heilongjiang Engineering Technology Research Center for Rice Ecological Seedlings Device and Whole Process Mechanization, Daqing, Heilongjiang 163319, China*

Correspondence should be addressed to Shujuan Yi; yishujuan@byau.edu.cn

Received 15 February 2022; Revised 9 March 2022; Accepted 11 March 2022; Published 4 April 2022

Academic Editor: Irshad Azeem

Aiming at the problems of fuzzy detection characteristics, high false positive rate and low accuracy of traditional network intrusion detection technology, an improved intelligent intrusion detection method of industrial Internet of Things based on deep learning is proposed. Firstly, the data set is preprocessed and transformed into 122 dimensional intrusion data set after one-hot coding; Secondly, aiming at the problem that convolution network cannot deal with data with long-distance attributes, Bidirectional long short-term memory (BiLSTM) is used to mine the relationship between data features; At the same time, the Batch Normalization mechanism is introduced to speed up the training of deep neural network. After the activation function performs nonlinear transformation on the input data of the previous layer, it is normalized to ensure the trainability of the network. The experimental results on NSL-KDD data set show that the accuracy of the proposed CNN-BiLSTM model is 96.3%, the detection rate is 97.1%, and the performance is the best.

1. Introduction

So far, the Internet of Things has been applied to various fields [1–3]. In the process of its development, it has introduced technologies such as Internet, advanced computing, analysis and sensing, and completed the integration of industrial production system, industrial monitoring system and industrial management system. Through the analysis and processing of industrial data, the production cost can be effectively reduced [4–8].

With the wide application of industrial Internet of Things technology, more and more open network connections make industrial control systems vulnerable to intrusion [9–12]. Since the development of the Internet of Things, incidents based on industrial Internet of Things security have occurred frequently at home and abroad. For intruders, attacking industrial Internet of Things systems can attract more attention or obtain more benefits than attacking Internet of Things systems in other industries [13, 14].

According to the current security vulnerabilities and structural characteristics of the domestic industrial Internet of Things, the information security risks can be divided into three categories. The first is due to the structural characteristics of the industrial Internet of Things, the second is the non-technical penetration based on social engineering, and the third is the external network risk brought by the combination with the Internet. In short, there are several reasons for the threat of industrial Internet of Things [15–17]:

(1) The operation environment of industrial network is complex

(2) Rapid growth of mobile Internet malware

(3) Information space network attacks, such as destroying data integrity, tampering with data packets, etc.

(4) System attack: violate the definition of data packet format in the protocol, or illegally command to destroy the field equipment, such as tampering with data to make it out of range, resulting in an attack

(5) Process attack: although the command conforms to the protocol specification, it violates the production logic, and security vulnerabilities and system defects threaten the user's privacy

Therefore, in order to ensure the security of network information, data integrity, confidentiality, effectiveness, operability and non-repudiation are required. At present, the research on security technology of industrial Internet of Things mainly focuses on authentication technology, encryption technology, access control technology and intrusion detection technology [18].

Aiming at the problems of fuzzy detection characteristics, high false positive rate and low accuracy of traditional network intrusion detection technology, an improved intelligent intrusion detection method of industrial Internet of Things based on deep learning is proposed. The BiLSTM network is used to mine data features, and the batch normalization is introduced to speed up the training and maintain the consistency of input data distribution. The BiLSTM network is integrated into CNN, which not only solves the problem of parameter explosion, but also improves the ability of intrusion detection system to process characteristic data with long-distance attributes and time series.

2. Related Works

The role of industrial Internet of Things network intrusion detection is to find unauthorized malicious behavior, which is essentially a data classification problem [19, 20]. In recent years, the research results of some scholars show that the performance of deep learning method in two classification and multi classification of network intrusion detection data sets is better than that of traditional methods. Literature [21] adopts the greedy multilayer deep belief network (DBN) model. Firstly, the limited Boltzmann machine is used to eliminate the negative impact of noise and abnormal data on the network, and then the back propagation algorithm is used to fine tune the DBN to realize the classification task. Literature [22] uses the depth automatic encoder (DAE) model. In order to avoid over fitting and local optimization, greedy layered training is adopted layer by layer. Literature [23] proposed ensemble learning based on trestle sparse self-coding network and phased sampling algorithm. Multi classification ensemble learning weighted fusion can have good detection ability in the early stage of intrusion virus. Literature [24] proposed an IICS anomaly detection technology based on deep learning model. Literature [25] uses BiLSTM-RNN to detect industrial Internet of Things attacks. The multilayer deep neural network is trained with the new UNSWNB15 data set, and the BiLSTM-RNN model achieves an accuracy of more than 95% in attack detection. Literature [26] uses RBM based on contrast divergence algorithm to train data and fine tune it through BP algorithm. The experimental results on nsl-kdd data set show that the classification accuracy is 95.25%, which can effectively detect attacks. In order to protect Internet of Things devices, Literature [27] combined feature-based intrusion detection and anomaly based intrusion detection system, proposed a method combining C5 classifier and support vector machine. Literature [28] uses the deep learning model to predict network security attacks, and proposes a prediction model based on sparse evolutionary training (set) to analyze and detect such as denial of service, malicious operation, data type detection, espionage, scanning, intrusion detection, violence, network attacks and error settings. Literature [29] proposed a model based on improved genetic algorithm and deep trust network by adaptively generating the number of neurons by genetic algorithm. The traditional deep learning model has limited ability of feature extraction and learning. When facing large-scale data sets, it cannot form an effective nonlinear mapping of data distribution.

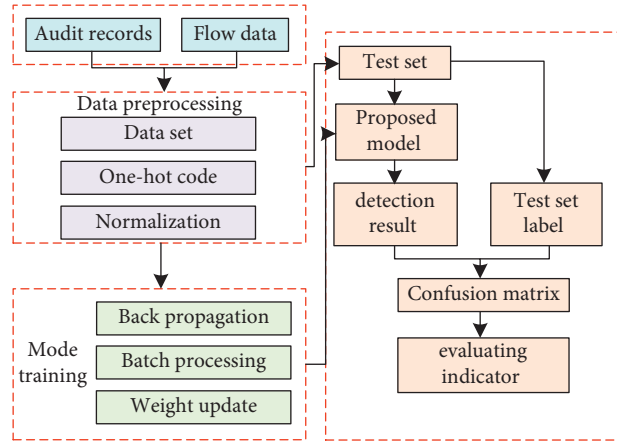

Figure 1: Intrusion detection model framework of industrial Internet of Things.

3. Internet of Things Intrusion Detection Based on Deep Learning

3.1. Industrial Internet of Things Intrusion Detection Model Framework. The industrial Internet of Things connects with devices and the Internet, so a network intrusion monitoring system should be set up in the environment of the industrial for security protection. In the industrial Internet of Things network flow, there are usually multiple characteristic attributes. These attributes jointly represent each data flow, which has the characteristics of high dimension and huge amount of data. Therefore, this paper uses the characteristics of deep learning and self-learning to build an intrusion detection model. The overall architecture is shown in Figure 1. The intrusion detection model of industrial Internet of Things based on deep learning is mainly divided into: data preprocessing module and data conversion module, training and testing module of deep learning network, and decision

Table 1: Label types of NSL-KDD dataset.

Attack category	Label	Attack classification
Normal	0	Normal
Dos	1	Apache2, back, land, mailbomb, neptune, pod, processtable, smurf, teardrop, udpstorm (10)
Probe	2	ipsweep, mscan, nmap, portsweep, saint, satan (6)
R2L	3	Fpt_write, guess passwd, nmap, multihop, named, phf, sendmail, snmpgetattack, snmpguess, spy, warezmaster, worm, xlock, xsnoop (15)
U2R	4	Buffer_overflow, httytunnel, loacmodule, perl, ps, rootkit, sqlattack, xterm (8)

output module. Therefore, using the characteristics of deep learning and self-learning, this paper constructs the intrusion detection model of industrial Internet of Things. The overall architecture is shown in Figure 1. The data preprocessing and data conversion module realizes standardized input, the deep learning network training and testing module carries out model training and optimization, and the decision output module uses Softmax for prediction.

(1) Data preprocessing. The data in this paper adopts the intrusion detection feature data set NSL-KDD covering the industrial Internet of Things. Firstly, the data is one-hot coded, transformed into 122 dimensional intrusion data set, and normalized to the range of [0, 1] to eliminate the influence of different dimensional differences.

(2) Model building. This paper constructs the intrusion detection model of industrial Internet of Things based on the combination of BiLSTM and CNN, and carries out feature extraction through deep learning network.

(3) Output. Softmax classifier is used to output the classification results and get the intrusion detection results.

3.2. Experimental Data Set and Preprocessing. NSL-KDD is collected by Lincoln Laboratory during the intrusion detection project. It collects data of many different users, different network traffic and attack means in the simulated real environment. The label attributes of NSL-KDD dataset are divided into one Normal identification class and one exception identification class, in which the exception identification data is divided into four categories: DOS, Probe, R2l and U2R. There are 39 attack modes, representing four types of network attacks that may be encountered by the industrial Internet of Things. The detailed attack types are shown in Table 1.

First, the NSL-KDD data set should be preprocessed. The first step is to convert symbolic data into numerical data. What needs to be numerically is protocol_type, flag and service. Where protocol_type contains three symbol types: TCP, UDP and ICMP. The numerical method adopted in this paper is to replace them with values 1, 2 and 3 respectively. In the same way, 70 values from 1 to 70 are used to represent 70 symbol types of service, and 11 values from 1 to 11 are used to represent 11 symbol types in flag. Finally, the five values 01, 02, 03, 04 and 05 are used to represent the five states of Normal, DOS, Prob, U2R and R2L respectively. After all features are converted into numerical type, they need to be normalized to keep the numerical value range of all features in the same order of magnitude. The normalization method adopted is

$$x = \frac{x - \max}{\max - \min}, \tag{1}$$

where x is the normalized value, max and min represent the maximum and minimum value of this feature in the data set, respectively.

3.3. Improved BiLSTM Model. This paper takes BiLSTM as the core of the model, which can well complete the extraction of data features. In LSTM, C_t and C_{t-1} are the memory units of the current time and the previous time respectively, h_t and h_{t-1} are the hidden units of the current time and the previous time respectively, i_t is the input gate of the current time, f_t is the forget gate, o_t is the output gate, and X_{nmt} is the value of n characteristic vector in the m time period of the t day (others, and so on). The LSTM network status is updated as follows:

$$\begin{aligned}
C_t &= f_t * C_{t-1} + i_t * C_t', \\
C_t' &= \tanh\left(W_c\left[h_{t-1}, X_{nm(t-1)}\right] + b_c\right), \\
f_t &= \sigma\left(W_f\left[h_{t-1}, X_{nmt}\right] + b_f\right), \\
i_t &= \sigma\left(W_i\left[h_{t-1}, X_{nmt}\right] + b_i\right), \\
o_t &= \sigma\left(W_o\left[h_{t-1}, X_{nmt}\right] + b_o\right), \\
h_t &= o_t * \tanh\left(C_t\right), \\
\sigma(\cdot) &= \frac{1}{1 + e^{-(\cdot)}},
\end{aligned} \tag{2}$$

where W_c, W_f, W_i and W_o are the weights of memory unit, forget gate, input gate and output gate respectively, and b_c, b_f, b_i, b_o are the corresponding bias coefficients. Since the LSTM uses sigmoid function (i.e. σ function) as excitation, the input of $(-\infty, +\infty)$ is mapped to the [0, 1] interval, which is equivalent to determining the weight coefficient between each unit in the LSTM. In other words, when the weight coefficient is 0, all information of the unit will be discarded and not input to other units connected to it; When

the weight is 1, all information of the unit will be fully retained and input to other units.

BiLSTM is an improved version of LSTM, which can carry out high-level abstraction and nonlinear transformation of intrusion data, analyze two-way data information, and provide more fine-grained computing. The calculation process is as follows:

$$\begin{aligned}\overrightarrow{h}_t &= f\left(\overrightarrow{W}\cdot x_t + \overrightarrow{W}\cdot \overrightarrow{h}_{t-1} + \overrightarrow{b}\right),\\ \overleftarrow{h}_t &= f\left(\overleftarrow{W}\cdot x_t + \overleftarrow{W}\cdot \overleftarrow{h}_{t-1} + \overleftarrow{b}\right),\\ y_t &= g\left(U\cdot\left[\overleftarrow{h};\overrightarrow{h}\right]+c\right),\end{aligned} \tag{3}$$

where $\overrightarrow{W}$ and $\overleftarrow{W}$ represent the network hidden layer parameters, x_t represents the input data, h_t and $\overrightarrow{h}_t$ represent the output results of the two LSTM layers at time t, $\overrightarrow{b}$ and b represent the offset value, and y_t represents the output of BiLSTM. The BiLSTM structure is shown in Figure 2.

After analyzing the data with BiLSTM, the data distribution may change in the neural network. In order to solve the inconsistency of data distribution when training deep neural network, Batch Normalization mechanism is introduced. Batch normalization can speed up the training of deep neural networks. It normalizes the input data of the previous layer after the nonlinear transformation of the activation function, which can ensure the trainability of the network, and enable the neural network to continuously maintain the consistency of the input data distribution, so as to reduce the large change of the node distribution in the network. Batch normalization mechanism can accelerate the convergence speed of the network and maintain the representation ability of the neural network. $B = \{x_{1\ldots m}\}$ represents the activation value in a batch, α and β represent the parameters to be learned. The calculation process of batch normalization in each layer of neural network is as follows:

$$\begin{aligned}u_\beta &= \frac{1}{m}\sum_{i=1}^{m} x_i,\\ \sigma_\beta^2 &= \frac{1}{m}\sum_{i=1}^{m}\left(x_i-\mu_\beta\right)^2,\\ x_i' &= \frac{x_i-\mu_\beta}{\sqrt{\sigma_\beta^2+\varepsilon}},\\ y_i &= \alpha x_i' + \beta,\end{aligned} \tag{4}$$

where x_i' represents the value after normalization, and y_i represents the value after batch normalization transformation.

3.4. Intrusion Detection Model Based on CNN-BiLSTM. Many information flows in the industrial Internet of Things often have strong local correlation, and some of these information even have direct correlation with the information with a long span. The BiLSTM neural network can effectively deal with these time sequential data by screening the valuable and useless information in the data through the algorithm. Therefore, based on CNN, this paper integrates BiLSTM network to improve the detection ability of the detection system. Figure 3 shows the proposed industrial Internet of Things intrusion detection model of CNN-BiLSTM.

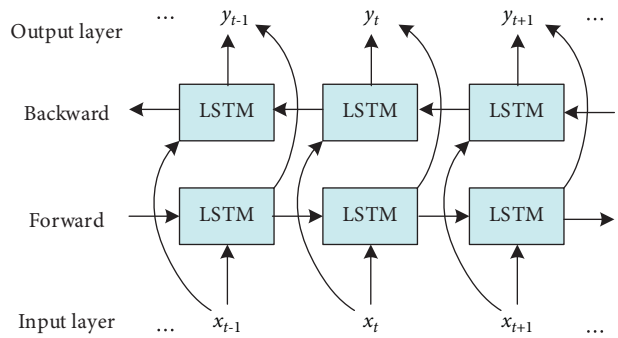

Figure 2: BiLSTM structure.

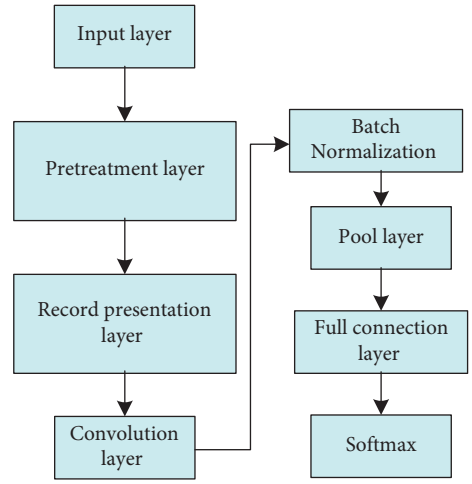

Figure 3: Intrusion detection model of industrial Internet of Things based on CNN-BiLSTM.

In the first step of the detection model, the original data set needs to be preprocessed. First, all the data are transformed into numerical data, and then standardized and normalized. The processed data enters the record representation layer. The record presentation layer adopts embedded representation for each piece of data after preprocessing. When the features of all data are convoluted by convolution check, the output feature formula is as follows:

$$H^d = \left[h_1^d, h_2^d, \ldots, h_{n-d_r+1}^d\right]. \tag{5}$$

All the features $\underset{H}{d}$ obtained by convolution are superimposed to obtain the feature sequence, and the formula is as follows:

$$H_s = \left[h_1, h_2, \ldots, h_{n-d_r+1}\right]. \tag{6}$$

After the convolution processing of the convolution layer to obtain the feature map, the convolution layer transmits it to the pooling layer. The pooling layer then pools

the feature sequences respectively. Using maximum pooling, first divide the input $\frac{d}{H}$ into M blocks, then take the maximum value respectively, and splice all the results together to obtain the eigenvector. The length of the eigenvector is M, and the final result is

$$P_S = \left[p_{m_1}, p_{m_2}, \ldots, p_{m_n}\right], \tag{7}$$

where $\frac{m_i}{P}$ is the vector obtained by the pooling layer after the pooling operation on the block m_i.

After the data is pooled in the pooling layer, the obtained feature sequence is input into the BiLSTM layer. The long short-term memory layer is composed of two LSTM modules in different directions, and multiple weights between them are shared together. The BiLSTM module selects and removes all data in turn.

CNN- BiLSTM network obtains the data features after processing the data. A full connection layer is used to integrate these feature sequences, and the results obtained from the full connection layer are input into the softmax classifier. Finally, the classification results of each information are obtained.

4. Experiment and Analysis

The experiment is implemented using the Keras framework. The integrated development environment used is Pychar, and the experimental data set is NSL-KDD data set. The Keras framework can build neural network more simply. The framework supports two environments: CPU and GPU, and the CPU is Intel core i5- 7500@3.40 GHz, with 8 GB RAM.

4.1. Evaluating Indicator. This paper uses accuracy (P_1), precision (P_2), detection rate (P_3) and false positive rate (P_4) to evaluate the performance of the algorithm. Accuracy rate indicates the number of samples with correct classification, but when the positive and negative classes of the data set are unbalanced, this index can not accurately reflect the performance of the model, and other indexes are needed to judge together. Detection rate and accuracy are also called recall rate and precision rate. These two indicators will affect each other. Usually, one is high and the other is relatively low. The calculation method of these four indicators is shown in formulas (8)–(11).

$$P_1 = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}, \tag{8}$$

$$P_2 = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}, \tag{9}$$

$$P_3 = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}, \tag{10}$$

$$P_4 = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}, \tag{11}$$

where TP refers to the true positive, that is, the aggressive behavior judged as an intrusion; FP refers to the normal behavior judged as intrusion behavior; FN refers to the aggressive behavior judged as normal behavior; TN refers to the normal behavior judged as normal behavior.

4.2. Convergence Detection. In the hybrid model, the optimizer adopts Adam optimizer, and the sparse classification cross entropy algorithm is used to calculate the loss value. The changes of the loss value and recognition rate of the training set and the test set are shown in Figure 4. Train_Loss and test_Loss represents the change curve of loss value of training set and test set respectively. Train_Accuracy and test_Accuracy represents the change curve of recognition rate of training set and test set respectively. From the figure, the recognition rate of training set and test set is 99.78%.

4.3. Comparison with Other Methods. In order to verify the performance of the proposed method, the methods of literature [28], literature [29] and the proposed method are used for comparative tests, and their effects are tested respectively. The results are as follows:

As can be seen from Figure 5, the detection accuracy and detection rate of the intrusion detection system in literature [28] are the lowest, and the accuracy and detection rate are only 83.2% and 86.4% respectively. Literature [29] iteratively generated the optimal number of hidden layers and neurons per layer based on genetic algorithm, which improved the accuracy and detection rate of intrusion detection, reaching 87.2% and 91.9% respectively. The accuracy of the proposed CNN-BiLSTM model is 96.3%, the detection rate is 97.1%, and the performance is the best. This is because the proposed CNN-BiLSTM model can carry out high-level abstraction and nonlinear transformation of network intrusion data, can well analyze two-way data information and provide more fine-grained computing. However, the methods of literature [28] and literature [29] do not extract the data deeply, so the accuracy and detection rate are slightly low.

As can be seen from Figure 6, the accuracy rate of the proposed CNN-BiLSTM model is 98.9%, while the accuracy rate of the method in literature [28] is 97.9%, and in literature [29] is 98.5%. The false positive rate of the methods in literature [28] and literature [29] is higher than 1.9% of the proposed model, because the comparison method focuses on the type of attack and the optimization of network structure, ignoring the extraction of intrusion data features. By integrating BiLSTM network into CNN, the proposed method not only solves the problem of parameter explosion, but also improves the ability of intrusion detection system to process characteristic data with long-distance attributes and time series.

Confusion matrix can quickly help analyze the misclassification of each category, so as to analyze and adjust the experiment. In order to more intuitively observe the performance of the model, Normal samples are coded as [1, 0, 0, 0 ,0], abnormal samples are divided into four categories, Dos is coded as [0, 1, 0, 0, 0], Probe is coded as [0, 0, 1, 0, 0], R2L is coded as [0, 0, 0, 1, 0], and U2R is set as [0, 0, 0, 1]. The confusion matrix of the model on the NSL-KDD dataset is shown in Table 2.

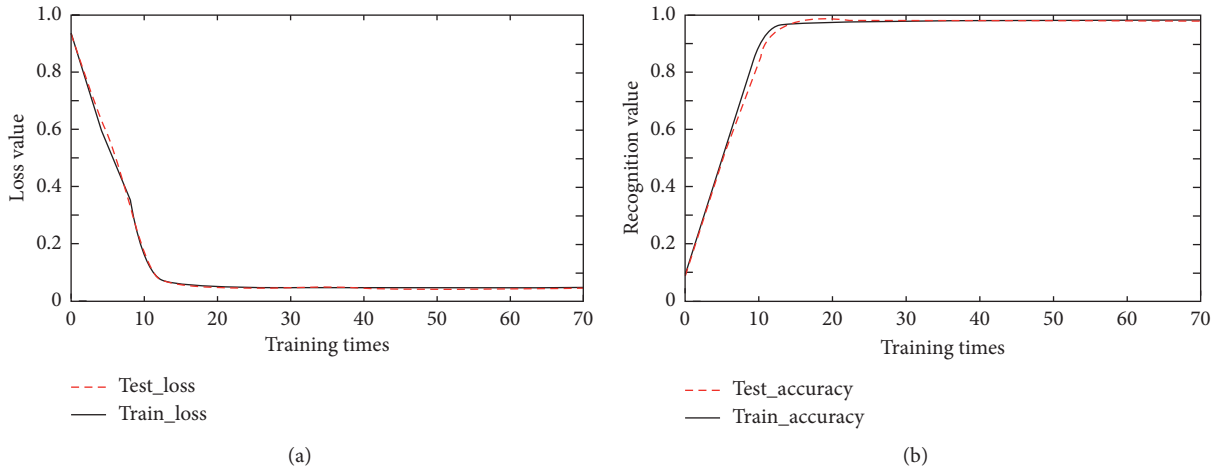

Figure 4: The loss value and recognition rate change curve of the proposed method. (a) Loss value variation curve of the proposed model. (b) Change curve of recognition rate of the proposed model.

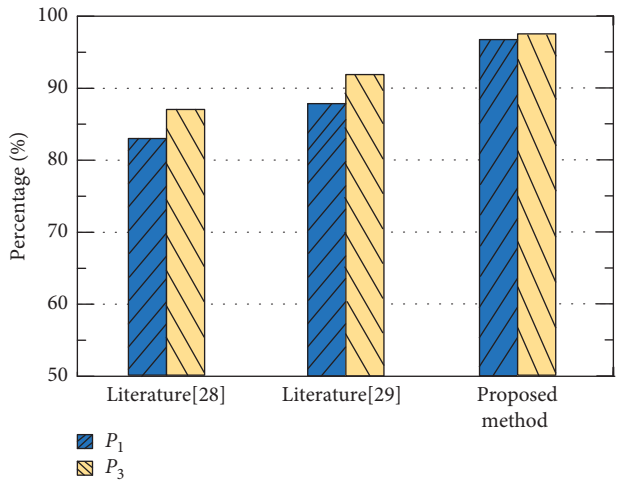

Figure 5: Accuracy and detection rate of different methods.

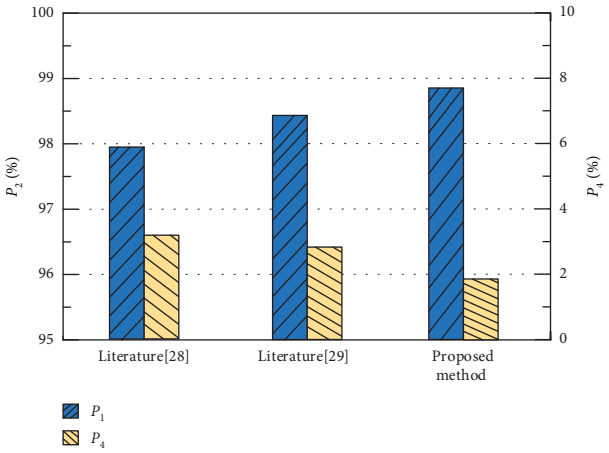

Figure 6: Precision and false positive rate of different methods.

Table 2: Confusion matrix of NSL-KDD test set.

	Normal	Dos	Probe	R2L	U2R
Normal	9534	156	120	96	6
Dos	74	7523	15	1	0
Probe	5	20	2264	0	0
R2L	226	0	8	540	0
U2R	51	0	12	0	641

5. Conclusion

Aiming at the problems of fuzzy detection characteristics, high false positive rate and low accuracy of traditional network intrusion detection technology based on deep learning, an improved intelligent intrusion detection method of industrial Internet of Things based on deep learning is proposed. The innovations of the proposed method are described as follows:

(1) BiLSTM neural network is used to deal with the dependence between data features, and batch normalization mechanism is introduced to speed up the training speed of deep neural network. The input data is normalized after nonlinear transformation to ensure the trainability of the network and maintain the consistency of the distribution of the input data.

(2) The proposed model uses CNN-BiLSTM model to deal with the dependencies between data features, and can mine more association rules.

Due to the time relationship and the limited ability of the author, there are inevitably many deficiencies in the paper. There are some deficiencies in the analysis and research of industrial Internet of Things network attack. In the future, the combination training can be combined with more efficient algorithms to improve the accuracy of the model and

optimize the algorithm. Although the data set used in this paper is relatively reasonable, it can not completely replace the existing network environment. Although the training and test set data is sufficient, the performance in the existing network environment needs to be further verified. In the later stage, the existing network data can be processed, trained and tested to further verify the feasibility of the model.

Data Availability

The data included in this paper are available without any restriction.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Central Government Directs Special Projects for the Development of Local Science and Technology (no. ZY20B05), Heilongjiang Agricultural Reclamation Administration's Projects (no. HKKY190201-02), Heilongjiang Innovative Talent Project (no. CXRC2017014), and the University's Talent Research Program (no. XDB201813).

References

[1] L. H. Son, S. Jha, R. Kumar, J. M. Chatterjee, and M. Khari, "Collaborative handshaking approaches between internet of computing and internet of things towards a smart world: a review from 2009-2017," *Telecommunication Systems*, vol. 70, no. 4, pp. 617–634, 2019.

[2] A. Wang, P. Wang, X. Miao, L. Xiangming, and L. Yun, "A review on non-terrestrial wireless technologies for Smart City Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, pp. 155–163, 2020.

[3] X. Li and L. Da Xu, "A review of Internet of Things—resource allocation," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1000–1009, 2020.

[4] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of things: a review of surveys based on context aware intelligent services," *Sensors*, vol. 16, no. 7, pp. 1069–1074, 2016.

[5] R. F. Sari, L. Rosyidi, B. Susilo, and M. Asvial, "A comprehensive review on network protocol design for autonomic internet of things," *Information*, vol. 12, no. 8, pp. 292–299, 2021.

[6] M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of nano-things, things and everything: future growth trends," *Future Internet*, vol. 10, no. 8, pp. 68–76, 2018.

[7] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," *IEEE Software*, vol. 33, no. 1, pp. 112–116, 2015.

[8] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: industry 4.0, IoT, blockchain, and business analytics," *Journal of Industrial Integration and Management*, vol. 5, no. 6, pp. 165–180, 2020.

[9] S. Albishi, B. Soh, A. Ullah, and F. Algarni, "Challenges and solutions for applications and technologies in the internet of things," *Procedia Computer Science*, vol. 124, no. 3, pp. 608–614, 2017.

[10] P. Pico-Valencia and J. A. Holgado-Terriza, "A gentification of the Internet of Things: a systematic literature review," *International Journal of Distributed Sensor Networks*, vol. 14, no. 10, pp. 2002–2010, 2018.

[11] S.-T. Deng and C. Xie, "Research based on data processing technology of industrial internet of things," in *Proceedings of the International Conference on Industrial IoT Technologies and Applications*, pp. 53–60, Springer, Wuhu, China, March 2017.

[12] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2020.

[13] M. Sheikhan and H. Bostani, "A hybrid intrusion detection architecture for internet of things," in *Proceedings of the 2016 8th International Symposium on Telecommunications (IST)*, pp. 601–606, IEEE, 2016.

[14] S. H. Jafier, "Utilizing feature selection techniques in intrusion detection system for internet of things," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, pp. 1–3, Tehran, Iran, September 2018.

[15] X. Liu, C. Zhang, P. Liu, W. Baojia, and Z. Jianyong, "Application of temperature prediction based on neural network in intrusion detection of IoT," *Security and Communication Networks*, vol. 2018, no. 4, 167 pages, Article ID 1635081, 2018.

[16] M. Rebbah, D. E. H. Rebbah, and O. Smail, "Intrusion detection in cloud internet of things environment," in *Proceedings of the International Conference on Mathematics and Information Technology (ICMIT)*, pp. 65–70, IEEE, Adrar, Algeria, December 2017.

[17] F. Angiulli, L. Argento, and A. Furfaro, "Effectiveness of content spatial distribution analysis in securing IoT environments," in *Proceedings of the 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 41–46, IEEE, Barcelona, Spain, August 2018.

[18] S. Choudhary and N. Kesswani, "Detection and prevention of routing attacks in internet of things," in *Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering*, pp. 1537–1540, IEEE, New York, NY, USA, August 2018.

[19] L. Liu, B. Xu, X. Zhang, and W. Xianjun, "An intrusion detection method for internet of things based on suppressed fuzzy clustering," *EURASIP Journal on Wireless Communications and Networking*, vol. 18, no. 1, pp. 1–7, 2018.

[20] L. Santos, C. Rabadao, and R. Gonçalves, "Intrusion detection systems in Internet of Things: a literature review," in *Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–7, IEEE, Caceres, Spain, June 2018.

[21] B. Yan and G. Han, "Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system," *IEEE Access*, vol. 6, no. 8, pp. 41238–41248, 2018.

[22] C. M. Hsu, H. Y. Hsieh, S. W. Prakosa, and Z. A. Muhammad, "Using long-short-term memory based convolutional neural networks for network intrusion detection," in *Proceedings of the International wireless internet conference*, pp. 86–94, Springer, Taipei, Taiwan, October 2018.

[23] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, no. 1, pp. 52843–52856, 2018.

[24] A. L. H. Muna, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of Information security and applications*, vol. 41, no. 3, pp. 1–11, 2018.

[25] B. Roy and H. Cheung, "A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network," in *Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–6, IEEE, Sydney, NSW, Australia, November 2018.

[26] T. Aldwairi, D. Perera, and M. A. Novotny, "An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection," *Computer Networks*, vol. 144, no. 7, pp. 111–119, 2018.

[27] A. Khraisat, I. Gondal, P. Vamplew, K. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *Electronics*, vol. 8, no. 11, pp. 1210–1217, 2019.

[28] R. V. Mendonça, J. C. Silva, R. L. Rosa, S. Muhammad, R. D. Zegarra, and F. Ahmed, "A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithm," *Expert Systems*, vol. 4, no. 5, pp. 2008–2013, 2021.

[29] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, no. 3, pp. 31711–31722, 2019.