A Novel IoT Intrusion Detection Model Using 2dCNN-BiLSTM

Ruihan XIANG [1], Sishan LI [2], Julong PAN [1]

[1] College of Information Engineer, China Jiliang University, 310018, Hangzhou, China
[2] Committee of Mengzi Economic and Technological Development Zone (Honghe Comprehensive Bonded Zone), 661100, Yunnan, China

s21030812010@cjlu.edu.cn, lisishan1@outlook.com, pjl@cjlu.edu.cn

Submitted January 3, 2024 / Accepted March 24, 2024 / Online first April 19, 2024

Abstract. *With the continuous advancement of Internet of Things (IoT) intelligence, IoT security issues have become more and more prominent in recent years. The research on IoT security has become a hot spot. A lightweight IoT intrusion detection model fusing a convolutional neural network, bidirectional long short-term memory network is proposed. It aims to improve processed data security and attack detection accuracy. First, sampling is performed by a hybrid sampling algorithm fusing SMOTE and ENN. Its aim is to minimize the impact of imbalanced-data and ensure data quantity in the process. Then, the data features are extracted by 2-dimensional convolutional neural network (2dCNN), and the effect of useless information is reduced by mean pooling and maximum pooling, so it can be adapted to the demanding resource environment of the IoT. On this basis, long-range dependent temporal features are extracted using bidirectional long short-term memory (BiLSTM), which aims to fully extract data features to improve detection accuracy in the limited resource environment. Finally, the algorithm is validated on the UNSW_NB15 dataset, and the results of the experiments reaches 93.5% at Accuracy, 86.4% at Precision, 85.3% at Recall and 85.8% at F1-Score. According to the results, the proposed algorithm can generate higher-quality samples, achieve higher detection rate with faster inference time and spend lower memory costs.*

Keywords

Internet of Things (IoT), convolutional neural network (CNN), bidirectional long short-term memory (BiLSTM), intrusion detection

1. Introduction

Currently, Internet of Things (IoT) devices are becoming smarter and are used in a diversity of fields, such as intelligent homes, education, entertainment and energy distribution, simplifying the way people live and work in their daily lives [1]. However, the general public is still paying little attention to IoT security [2], which may endanger IoT users and even lead to an imbalance in the ecosystem. In response, researchers have introduced continuously upgraded intrusion detection systems [3], [4] into IoT security, which has become a key technology for defending against IoT security threats.

With the growing complexity and diversity of intrusion methods in recent years [5], traditional intrusion detection systems that rely on simple pattern recognition and feature selection can no longer adapt to today's booming IoT environment, resulting in an awful exactitude and high misreporting rate of intrusion detection systems. As a new research direction of machine learning, deep learning can combine the low-level features from human-screened and prepared training samples into higher-level potential features that can characterize the sample data [6], and its powerful learning and classification capabilities have led to extensive research and applications in computer image and vision, natural language processing, and network security. For example, Yang et al. [7] proposed the LM-BP intrusion detection algorithm and finished the optimization of the performance of the IoT intrusion detection system. Chen et al. [8] addressed the large-scale IoT traffic problem by converting its data samples into grayscale maps and using ResNet and BiLSTM network memory fusion model for classification.

An important prerequisite for the excellent application of the above deep learning algorithms in the IoT domain is to have sufficient training samples with balanced class distribution. The main function of an IDS is to differentiate between regular traffic and aggressive traffic. In daily life, attacks on IoT devices are small probability events, so IoT intrusion detection is essentially a classification problem in the case of data imbalance. Data imbalance refers to the number of samples of each category varies greatly in the dataset, there is a large difference in the distribution of data categories, which affects the evaluation of classification methods. Therefore, it is of great importance to improve the detection rate of a few attack sample types or unknown attack types effectively on the basis of data with unbalanced class distribution.

DOI: 10.13164/re.2024.0236

The current mainstream solution targeting the data imbalance problem is to reduce or eliminate the imbalance by readjusting the sample distribution of the training set from the data perspective, and the commonly used methods are oversampling, undersampling, and the mixture of both oversampling and undersampling [9–11], but all the above methods are prone to overfitting or loss of potentially useful information [12], and the improvement of the model classification performance is more limited [13]. GAN presented by Goodfellow in 2014 [14] is a subclass of generative models that estimate the potential distribution of existing data samples and construct a model that can match the data distribution and thus generate new data samples. Because the generated data types are very broad and the model has some self-learning capability, it can be applied in semi supervised learning [15]. In recent years, GAN has made some impressive progress in computer vision [16], text [17], audio [18], and reinforcement learning [19].

Aiming at the abovementioned problems, an intrusion detection model that incorporates the SMOTE, ENN, 2dCNN and BiLSTM is proposed. This paper contributes in the following two areas.

(1) Proposing a scheme that balances intrusive detection and data generation for IoT. In the process of generating data, the SMOTE algorithm and ENN is applied to realize the balance of the dataset. It can provide sufficient data for the next stage of IoT intrusion detection;

(2) A lightweight intrusion detection model incorporating convolutional neural networks and bidirectional long and short-term memory networks using deep learning concepts is designed. It can fully capture the characteristics of the processed data, achieving high detection rate;

The remaining sections of this paper are as follows: In Sec. 2, we conduct a detailed discussion of the model components used, the mathematical inference methods, and the evaluation criteria. The suggested solution is presented in Sec. 3. The simulation results and discussion are included. The last section concludes and discusses the future direction of this study.

2. Methodology

2.1 Data Purging

The best method for using raw data as input is by purging, labeling and annotating. We use the function of LabelEncoder to transforming the abstract features into digital features, and then facilitate 2dCNN-BiLSTM model to learn intrinsic features.

Regularization can minimize the variability of the features within a certain range and decrease the effect of abnormal value. We employ the standardization of minmax function [20] as shown in (1) to standardize the characteristics to values between 0 and 1, in which $h_{i,j}$ represents the eigenvalues in the i-th row and j-th column of the dataset:

$$h_{i,j} = \frac{h_{i,j} - \min(h_{i,j})}{\max(h_{i,j}) - \min(h_{i,j})}. \tag{1}$$

2.2 SMOTEEN Sampling

The SMOTE method uses linear interpolation to synthesize the new minority sample between the minority class and the K-nearest neighbor samples, which solves the information redundancy caused by random oversampling to some extent. However, it tends to cause problems such as sample overlap and noisy samples in the synthesized samples. SMOTEEN is a deep cleaning of the data generated by the latter using the ENN method based on SMOTE. The method has been shown to generally outperform other classical sampling methods on several standard datasets [21].

2.3 Evaluation Criteria

The estimation index mainly includes 4 indices as shown in (2)–(5). All results must be divided into 4 categories: TP, TN, FP and FN. TN means the model judges the data as attack class, which is actually also abnormal data. TP denotes the model judges the data as the regular, which is actually also the regular class, so the result is right. FN means the system recognizes the sample as anomalous, but it is normal class in reality, which leads to an incorrect classification result. FP means the system recognizes the sample as normal, while the actual data are abnormal, which leads to an incorrect classification result. Table 1 shows the detailed categorization results.

Classification	Prediction positive class	Prediction positive class
Actual positive class	TP	FN
Actual negative class	FP	TN

Tab. 1. Confusion matrix.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}, \tag{2}$$

$$precision = \frac{TP}{TP + FP}, \tag{3}$$

$$recall = \frac{TP}{TP + FN}, \tag{4}$$

$$F_1 - score = \frac{2 \times recall \times precision}{recall + precision}. \tag{5}$$

3. Materials and Methods

Conventional IoT intrusion detection models consider more of their features in space during the detection of attacks and ignore the features in time series. Converting the original one-dimensional traffic data into a two-dimensional grayscale map by 2dCNN can extract richer characteristics of the data effectively and avoid the gradient explosion; however, it has poor ability to extract information

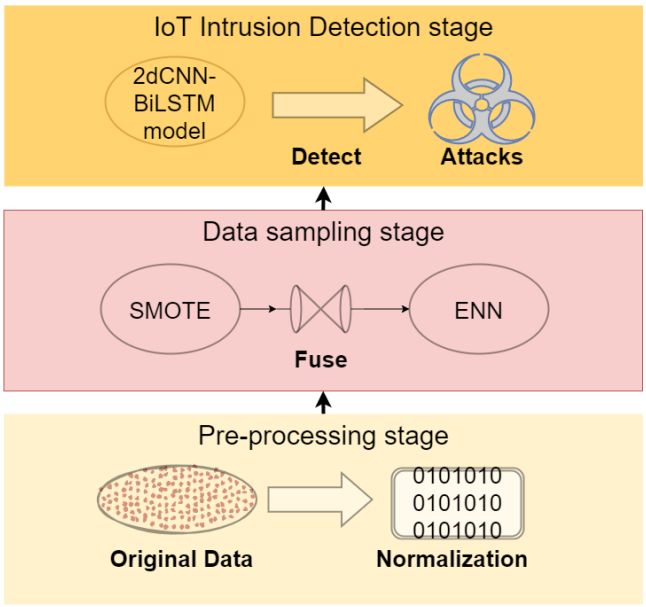

Fig. 1. IoT intrusion detection model architecture diagram.

over long distances and will increase model complexity. BiLSTM is more capable of capturing long-distance characteristics and maintaining a long memory during the process. Nevertheless, BiLSTM is more complex than LSTM in model composition. Therefore, fusing the advantages of the above two models and fully extracting multi-dimensional features to achieve better model performance.

The IoT intrusion detection model that combines the SMOTEEN, 2dCNN and BiLSTM has 3 main parts in Fig. 1: the first stage, we use the functions of LabelEncoder and Minmax to convert the original data into digital characteristics and then normalizing; second, balancing the dataset by the hybrid sampling method of SMOTE and ENN, and then converting the one-dimensional data in the original dataset into two-dimensional data; third, the balanced data are trained by extracting features through 2dCNN-BiLSTM and then classified by the softmax function.

3.1 Data Preprocessing

According to Fig. 2, the data preprocessing process in this section consists of 3 stages. In the Data Cleaning stage, we convert the nonnumerical characteristics in the primitive data into digital characteristics and standardize them. In the SMOTE sampling stage, the preprocessed training set is input into the SMOTE algorithm for pre-generation. The few minority samples in the dataset are augmented to reach a certain size, so as to facilitate the subsequent ENN sampling to be able to fully extract the data features. Finally, the balanced datasets are converted into grayscale maps in Fig. 3.

3.2 Model Structure

The most important advantage of CNN over conventional models is that it can learn the best filters by itself, it can accept directly input images, and then combine feature learning with mass regression in the training process. 2dCNN has the advantage of fewer parameters and fewer computations and is suitable for intrusion detection with temporal data features in harsh resource environments. BiLSTM effectively prevents gradient explosion and gradient disappearance. It is good at capturing longer distance dependent feature information. To enhance the representativeness and sufficiently capture the information in the classification process under the limited resources of the IoT, we propose a lightweight 2dCNN-BiLSTM model with the structure shown in Fig. 4.

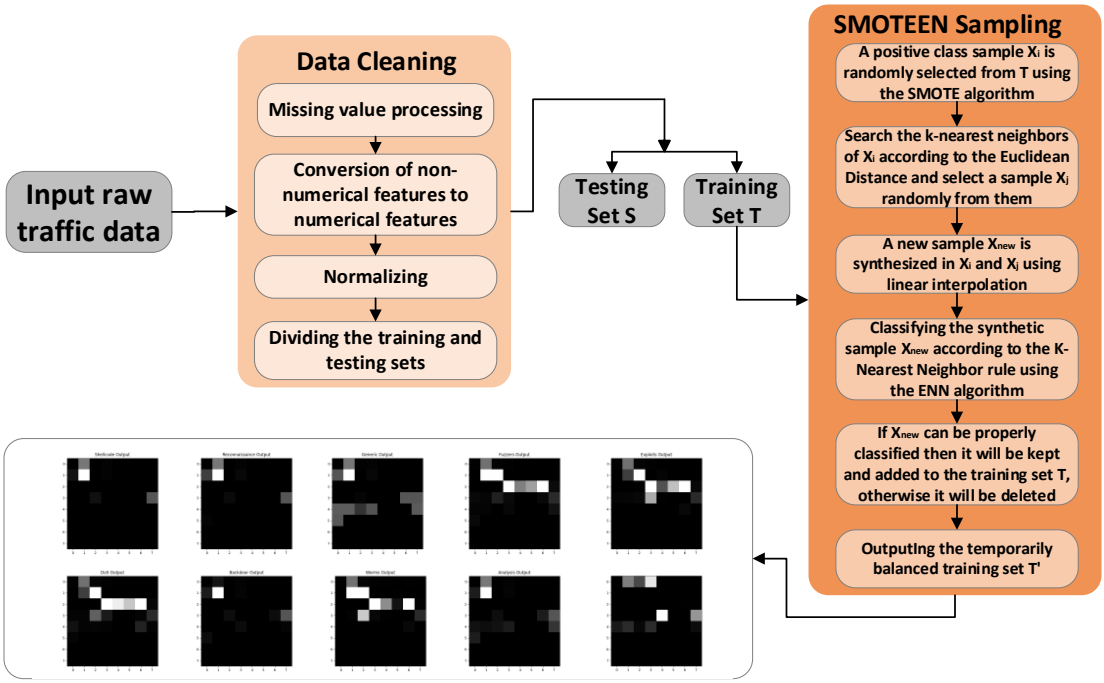

Fig. 2. Preprocessing flow chart.

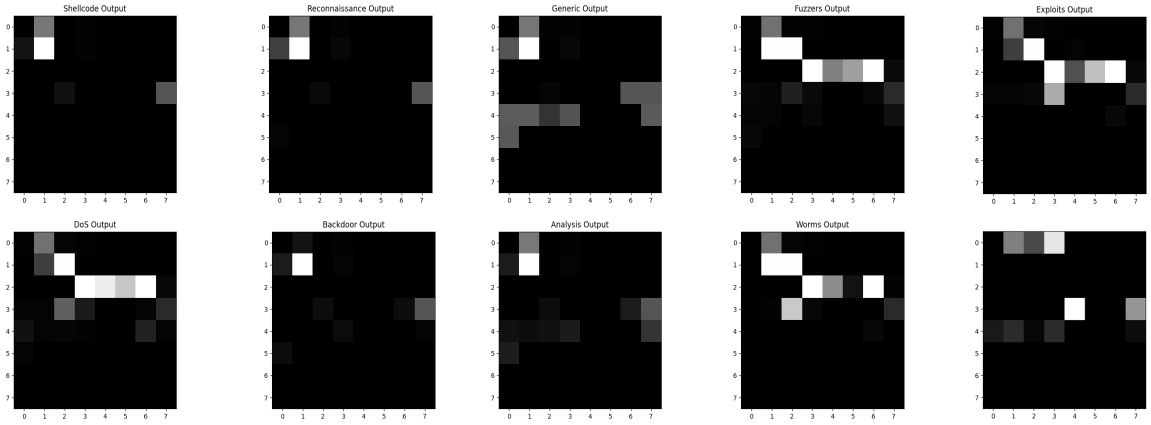

Fig. 3. Converted grayscale map.

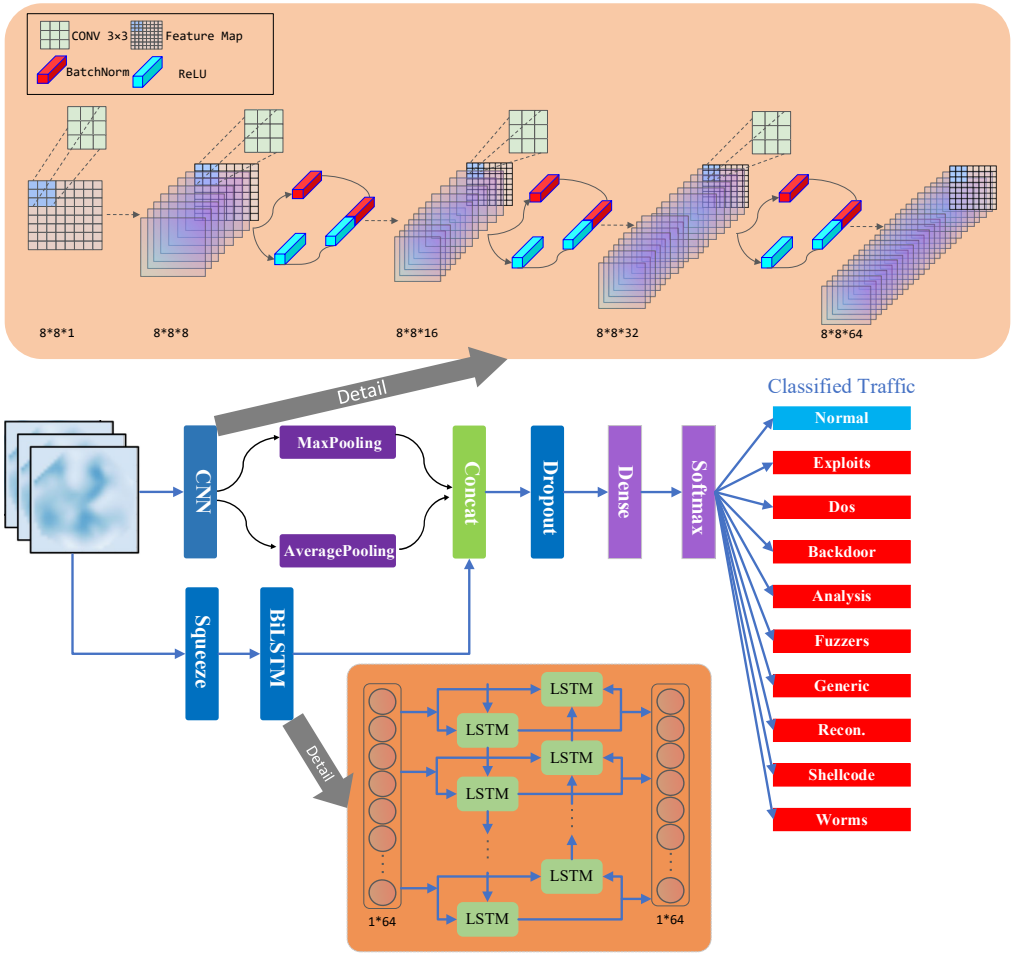

Fig. 4. IoT intrusion detection model structure.

As shown in Fig. 4, firstly, the data features are extracted from different channels after the data are input by convolution, and normalization and activation are performed for each feature map to speed up the convergence and lift current network representation to adapt to complex and changing environment of IoT.

Secondly, the features of each channel are maximally pooled or averaged to remove as much redundant information from the convolutional extraction as possible, and the features are compressed to reduce the computations and memory consumption to fit the limited resources of IoT terminals.

Finally, the quantity of convolutional channels, output channels of BiLSTM and the output channels of the final dense module are manually modified to reduce the total parameters between layers and simplify the complexity of

the network while ensuring the stability of the corresponding indicators and achieve lightweighting. To decrease the model complexity, the quantity of channels of the first conv-layer is modified from 32 to 8, the quantity of channels of the second conv-layer is modified from 64 to 16, the quantity of channels of the third conv-layer is modified from 128 to 32, the quantity of channels of the fourth conv-layer is modified from 256 to 64, and each of the above layers is accompanied by a standardization-layer and an activation-layer. To fuse features of convolution output, the quantity of output channels of BiLSTM is modified from 128 to 32. The final dense layer is modified from (16,640, 128) to (4160, 32) at the beginning. So far, we can eliminate the parameters of redundant neurons between the convolutional layers and the parameters of redundant units of the BiLSTM and increase the fit time in training process, thus reducing the size from the initial 10 MB to approximately 660 KB, theoretically compressing the model by 16 times, reducing the inference time from 59 seconds to approximately 11 seconds, and decreasing the inference time by 4 times theoretically, achieving the purpose of lightweighting. Additionally, to some extent, this model can meet real-time detection requirements in the IoT environment.

4. Experiments and Analysis

4.1 Experimental Setup

All the studies were performed on the device of 64-bit Windows Intel(R) Core (TM) i7-7700HQ CPU (2.80 GHz) with 16 GB RAM and a Python-based Nvidia GeForce GTX 1050ti GPU (4 GB). The model is tested in PyTorch environment in Python 3.8. To test the performance of the proposed models, the experimental parameters are set to the base settings of the optimizer choosing the stochastic gradient descent algorithm, the learning rate is set to 0.001, and the cross-entropy loss function is chosen. The batch size and the number of training rounds are 128 and 300, respectively. All the parameter selection processes mentioned above have been subjected to a series of experiments and considerations. Given the simplicity of the selection process, we have chosen not to elaborate further.

There have been numerous datasets related to intrusion detection over the years, including the UNSW_NB15 dataset [22], the KDDCUP_99 dataset [23], and the NSL_KDD dataset [24]. The UNSW_NB15 dataset [22] is the primary evaluation dataset for its abundance of data and comprehensiveness of attack types, and the KDDCUP_99 dataset [23] and the NSL_KDD dataset [24] are used as the secondary validation datasets.

The UNSW_NB15 dataset is a dataset generated in 2015 by the Cyber Range Laboratory of the Australian Center for Cyber Security (ACCS) using the IXIA PerfectStorm tool to simulate a realistic cyber environment.

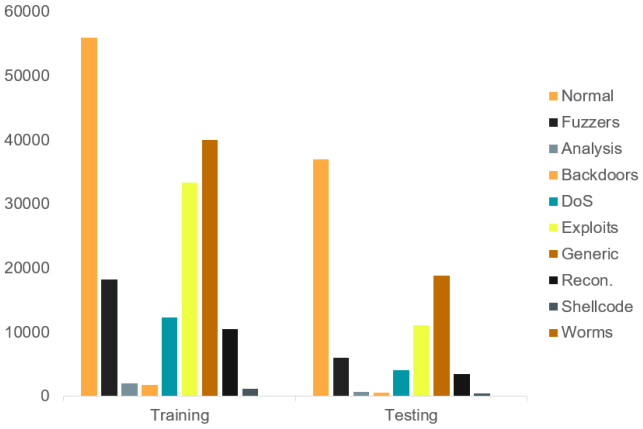

Fig. 5. Distribution of different classes in the dataset.

The UNSW_NB15 dataset [22] comprises 47 attribute features and 9 attacks as shown in Fig. 5. The divided training set and testing set are used to examine the performance of the model.

4.2 Experiments and Analysis

4.2.1 Experiments on Different Sampling

To address problem that most of the attack classes in the dataset are unbalanced compared to the normal classes, we use the sampling method of SMOTEEN to balance the dataset for preprocessing. This section is conducted to different sampling ways for comparison experiments: 4 different methods of SMOTE [25], ADASYN [25], random undersampling [25] and random oversampling [25] are used to deal with the unbalanced dataset.

Figure 6 shows in contrast to many different sampling methods, the processing results of the proposed SMOTEEN method are more stable. The reason is that the singular over-sampling models cannot effectively differentiate the noisy data, and tend to generate a large amount of noisy data during processing, which in turn leads to the decline of the model categorization results. Singular undersampling models tend to lose the critical messages, which causes the decline of results. SMOTEEN, which samples most samples and few samples respectively.

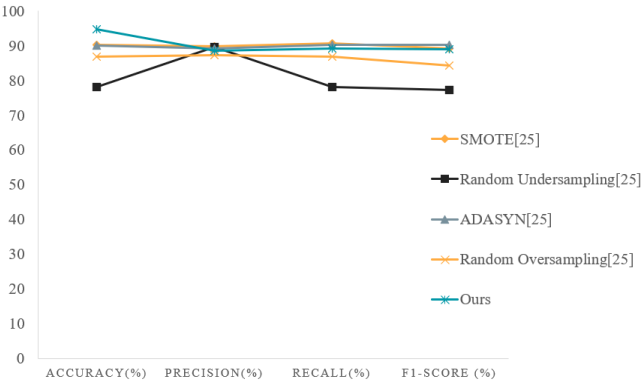

Fig. 6. Comparison of different sampling methods.

In the SMOTEEN process stage, minority class samples are generated using the SMOTE algorithm, and then the overlapping samples are processed using the data cleaning technique ENN. The majority of the minority samples in the dataset are augmented to obtain a balanced dataset.

From Fig. 6, it can be clearly seen that compared with the performance of using a single sampling method, the performance of the fusion sampling method proposed in this paper is better. In addition to avoiding the loss of critical messages, it also reduces the influence of noisy data on the filters, and therefore achieves better effects.

4.2.2 Experiments on Different Modules

To verify the validity of the proposed model, experiments were conducted to analyze the performance of the intrusion detection model: the CNN [26], CNN-LSTM [27] and 2dCNN-BiLSTM were tested through the UNSW_NB15 dataset as main standard.

From Fig. 7, it is observed that the model of 2dCNN and BiLSTM occupies the largest area compared to CNN [26] and CNN-LSTM [27], and the accuracy rate is 93.5%, recall rate is 85.3%, precision rate is 86.4% and F1-score rate is 85.8%. It indicates that the 2dCNN-BiLSTM model combines the advantages of the above two models to achieve effective multi-dimensional feature learning, and therefore achieves better results.

The reason why we can achieve good performance is that the CNN [26] structure is better at extracting spatial structure features. After reconstructing the balanced dataset into 2d gray map data, we can better utilize the advantages of the CNN [26] structure to extract the latent spatial features in the dataset compared with the traditional 1d data. 4-layer 2d convolutional structure can cover the whole dataset well, and the number of filters and the size of convolution kernel of each layer can also extend the sense of the wildness to each piece of data very well.

BiLSTM structure is good at extracting temporal features, and some obvious temporal relationships also exist in the dataset. Considering the harsh resource environment of IoT, we use 1 layer of BiLSTM structure to extract temporal features, which is able to maximize the information extraction while reducing the network parameters.

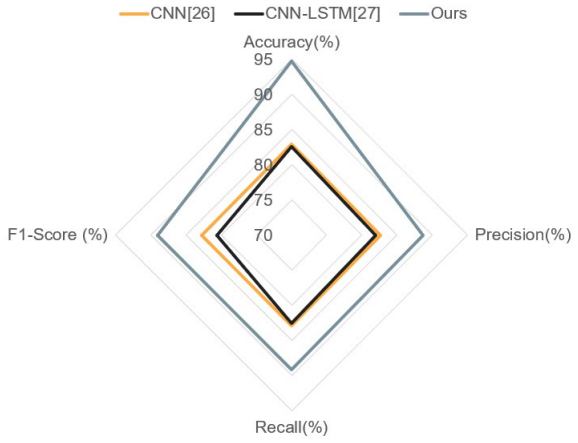

Fig. 7. Comparison between the single model and hybrid model.

From Fig. 7, it can be seen that compared with a single network structure, the 2dCNN-BiLSTM network structure is able to perform better in the subsequent detection after fusing spatial and temporal features.

4.2.3 Experiments on Performance Analysis and Comparison of Different Models

To further validate the effectiveness of the intrusion detection model, performance comparison experiments are conducted in this section: machine learning functions and deep learning functions are applied to the UNSW_NB15 dataset [22] under the same experimental conditions.

Table 2 shows that our model achieves more stable results on the above four evaluation metrics compared to other models. The reason why we can achieve stable performance is that our model learns more comprehensive characteristics by fusing the advantages of multivariate models, and combines the ground-level characteristics to develop a more abstracted representation.

In contrast to the traditional machine learning methods of XGboost [28] and LightGBM [29] models, although the 2dCNN-BiLSTM model did not exhibit optimal performance across the aforementioned four metrics, the gap between its performance and the optimal benchmarks was maintained within a 5% margin. Furthermore, in comparison to traditional machine learning approaches, the architecture of the 2dCNN-BiLSTM model is notably more flexible, facilitating a more convenient training process. Additionally, this model architecture contributes to an enhanced generalization capability, thereby offering significant advantages in various application contexts.

In contrast to PSO-LightGBM [30], AlexNet [31], CWGAN-CSSAE [32] and MSCNN-LSTM [33], the 2dCNN-BiLSTM intrusion detection model extracts and learns a more comprehensive set of features at the same time with better results. There are two reasons for this: (1) SMOTEEN sampling method makes a high-quality expansion for the dataset, thus providing good data support for the current detection model training; (2) the structure and parameter settings used in our model are more suitable for the characteristics of the data in the UNSW_NB15 dataset. Our model construction and parameter selection are more in line with the characteristics of the data that have more

Model	Accuracy	Precision	Recall	F1-Score
LightGBM [28]	92.1	84.8	82.5	83.3
XGboost [29]	94.8	89.1	88.4	88.7
PSO-LightGBM [30]	70.5	-	-	-
AlexNet [31]	89.9	87.6	-	88.4
CWGAN-CSSAE [32]	93.3	92.6	-	92.9
MSCNN-LSTM [33]	89.0			
Ours	93.5	86.4	85.3	85.8

Tab. 2. Comparison of different models.

spatial than temporal features. Therefore, we use more convolutional layers than LSTM layers in the construction process. And we also fully consider the harsh resource environment of IoT in the selection of filters and convolutional kernel sizes, adopting a heuristic selection method for parameter setting. Combining the above two reasons, the 2dCNN-BiLSTM model is able to improve intrusion detection capability effectively.

4.2.4 Experiments on Different Models on Different Datasets

To illustrate the generalization of our model, which can be adapted to the harsh resource conditions in various IoT devices, the experiments take some models in Tab. 2 and our model applied on the UNSW_NB15 dataset [22], KDD_CUP99 dataset [23] and NSL_KDD dataset [24] for comparison experiments.

As seen in Tabs. 3–5, our model shows the overall best performance with the above three datasets. In the UNSW_NB15 [22] dataset, although our model does not get the best performance on the criteria of Accuracy, Precision and Memory, the gap from the optimal criteria for each of the above four criteria is so small that it is almost negligible. In the memory capacity, the most important criteria, our model occupies only about 0.6 MB, which is suitable for the limited resource environment of the IoT. In the KDD_CUP99 dataset [23] and NSL_KDD dataset [24], although our model does not have the best performance in all metrics, the difference between the indicators of this paper and the optimal model can be almost ignored from the viewpoint of accuracy.

Model	Accuracy (%)	Precision (%)	Memory (MB)
LightGBM [28]	92.1	84.8	0.7
XGboost [29]	94.8	89.1	2.8
CWGAN-CSSAE [32]	93.3	92.6	-
MSCNN-LSTM [33]	89.0	-	-
Ours	93.5	86.4	0.6

Tab. 3. Comparison of different models on UNSW_NB15.

Model	Accuracy (%)	Precision (%)	Memory (MB)
LightGBM [28]	99.2	99.3	0.4
XGboost [29]	99.9	99.8	1.3
Decision Tree [34]	98.5	95.2	-
LSTM-FCNN [35]	98.5	98.9	-
Ours	98.1	98.2	0.7

Tab. 4. Comparison of different models on KDD_CUP99.

Model	Accuracy (%)	Precision (%)	Memory (MB)
LightGBM [28]	99.0	98.6	0.3
XGboost [29]	99.8	99.7	1.2
OCNN-HMLSTM [36]	90.6	86.7	-
LOGNN [37]	98.7	98.4	-
Ours	97.6	97.5	0.7

Tab. 5. Comparison of different models on NSL_KDD.

The reason why it can achieve above performance is that we used a heuristic structured pruning method during model training, which focuses on the number of convolutional channels, layers and convolutional kernels. At first, the parameter magnitude of each layer is ranked. Then, the layer with the largest parameter magnitude is selected for pruning the above three aspects. Lastly, the pruning is done by manual modification. After pruning, the size of the model was significantly reduced, from the initial 10.1 MB to about 660 KB now, and the parameters of the model were compressed by 16 times. Under the setting of keeping the same training parameters, the accuracy on UNSW_NB15, KDD_CUP99 and NSL_KDD datasets after 300 theories training is tested at 93.5%, 98.1% and 97.6% on Accuracy, respectively.

In summary, our model can show good generalization performance in different IoT environments, which can theoretically be adapted to the harsh resource environment of the IoT to some extent.

4.2.5 Experiments on Different Class

To further illustrate the detection rate of the proposed model for minority classes, experiments on multi-classification are conducted in this section using the 2dCNN-BiLSTM model on the UNSW_NB15, KDD_CUP99 and NSL_KDD datasets.

As can be seen from Figs. 8–10, the 2dCNN-BiLSTM model performs better in the 10 classes in the UNSW_NB15 dataset. Except for the AUC area of Normal and DoS reach about 90%, and the AUC area of the remaining 7 classes is around 94% or even higher. The reason for this is that the above 2 classes have the least amount of data in the original dataset, and after SMOTEEN sampling, the amount of data has been expanded to a certain extent, and the accuracy has been greatly improved compared to that before sampling. Therefore, in terms of the comprehensive accuracy, the 2dCNN-BiLSTM model can achieve the ideal accuracy for different attack types. Among the five categories in the KDD_CUP99 dataset, all

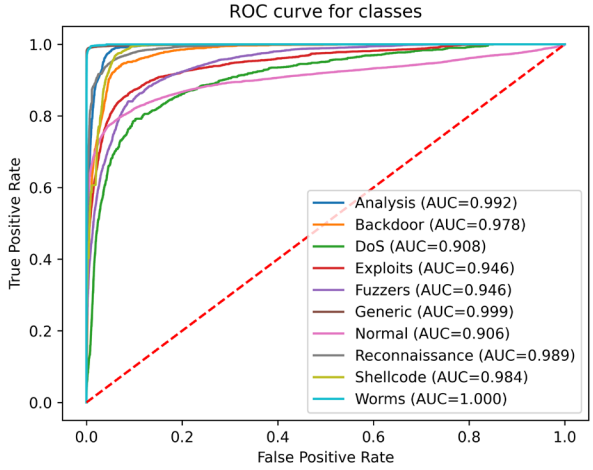

Fig. 8. ROC curve tested on UNSW_NB15.

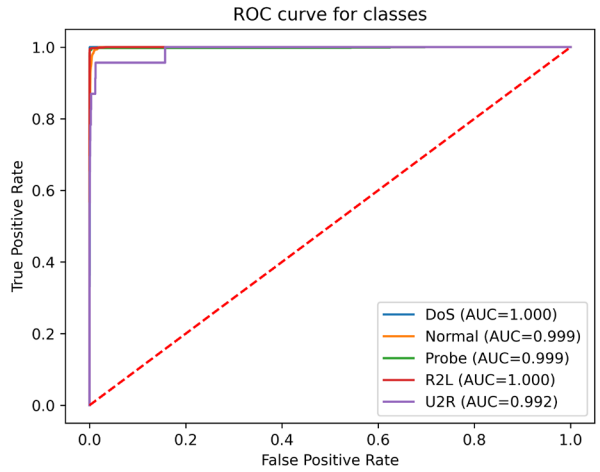

Fig. 9. ROC curve tested on KDD_CUP99.

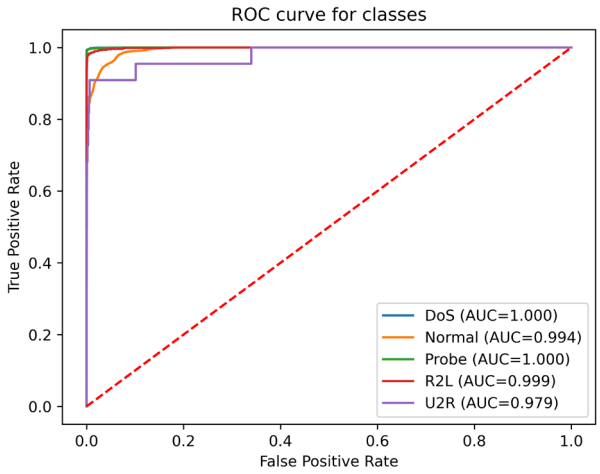

Fig. 10. ROC curve tested on NSL_KDD.

the 5 categories perform strongly. It shows that the structure and parameters of the model proposed in this paper can fit the characteristics of this dataset well. Similarly, in the NSL_KDD dataset, the AUC area of the 5 categories is all beyond 97%, which fully demonstrates that the generalization performance of the model proposed in this paper is very good and can adapt to different data in different IoT environments.

5. Conclusion

With the advancement of 5G, IoT has been further developed, and its wide range of use and increasing importance have made it an obvious target for hackers to attack. As a large-scale functional network for endpoints, once attacked, it may cause immeasurable losses. Therefore, it is extremely important to study the network intrusion detection methods for IoT. Regarding the existing IoT security field, an intrusion detection scheme is proposed.

Firstly, in order to realize the balance between data availability and data richness, we design a fusion of SMOTE and ENN model. It solves the data imbalance on the one hand, and greatly enhance the data richness on the other hand. Secondly, in order to fully extract the detailed features of the data after perturbation, we convert the one-dimensional data into a two-dimensional grayscale map, which greatly improves the detection accuracy at the later stage. Furthermore, to facilitate the operation in the harsh resource environment of IoT, a deep learning model fusing 2dCNN and BiLSTM is designed, and the model is light-weighted so that it can take both detection accuracy and faster inference time into account. Finally, we conducted some comparative experiments. The experimental results indicate that on the UNSW_NB15-based dataset, with reasonable parameter configurations, the accuracy rate is 93.5%, the inference time is 11.91 s, and the model size is 0.68 MB, which indicates that the proposed model can achieve good performance in IoT environments while maintaining a great detection performance. Compared with the existing techniques, it can realize high detection rate in IoT's real-time environment.

On the whole, the proposed scheme can be applied to many IoT's scenarios, such as smart homes. However, facing the current huge network system, the resource consumption and communication overhead of the actual deployment on IoT devices is a problem that must be considered. In the future we will focus on the deployment of the model in real IoT environments, do the detection of real-time data and test.

Acknowledgments

We sincerely thank our teammates and professors for their help in this study. They provided us with the tools that we needed to choose the right direction and insightful feedback.

Data Availability

The data that support the findings of this study are available from the first author, upon reasonable request.

References

[1] WORTMANN, A. F., FLÜCHTER, K. Internet of things. *Business & Information Systems Engineering*, 2015, vol. 57, no. 3, p. 221–224. DOI: 10.1007/s12599-015-0383-3

[2] CHAHID, Y., BENABDELLAH, M., AZIZI, A. Internet of things security. In *Proceedings of 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*. Fez (Morocco), 2017, p. 1–6. DOI: 10.1109/WITS.2017.7934655

[3] KRISHNAN, P., JAIN, K., ACHUTHAN, K., et al. Software-defined security-by-contract for blockchain-enabled MUD-aware industrial IoT edge networks. *IEEE Transactions on Industrial Informatics*, 2022, vol. 18, no. 10, p. 7068–7076. DOI: 10.1109/TII.2021.3084341

[4] NASIR, M. H., KHAN, S. A., KHAN, M. M., et al. Swarm intelligence inspired intrusion detection systems a systematic

literature review. *Computer Networks*, 2022, vol. 205, no. 3, p. 1–29. DOI: 10.1016/j.comnet.2021.108708

[5] XU, L. J., WANG, B. L., YANG, M. H., et al. A multi-mode attack detection and anomaly state evaluation method for industrial control networks. (in Chinese) *Computer Research and Development*, 2021, vol. 58, no. 11, p. 1–17. DOI: 10.7544/issn1000-1239.2021.20210598

[6] WONGSUPHASAWAT, K., SMILKOV, D., WEXLER, J., et al. Visualizing dataflow graphs of deep learning models in tensorflow. *IEEE Transactions on Visualization and Computer Graphics*, 2017, vol. 24, no. 1, p. 1–12. DOI: 10.1109/TVCG.2017.2744878

[7] YANG, A., ZHUANSUN, Y., LIU, C., et al. Design of intrusion detection system for internet of things based on improved BP neural network. *IEEE Access*, 2019, vol. 7, p. 106043–106052. DOI: 10.1109/ACCESS.2019.2929919

[8] CHEN, H. S., CHEN, J. J. Construction and optimization of IoT intrusion detection classification model based on ResNet and bi-directional LSTM fusion. *Journal of Hunan University: Natural Science Edition*, 2020, vol. 47, no. 8, p. 1–8.

[9] CHAWLA, N. V., BOWYER, K. W., HALL, L. O., et al. SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 2002, vol. 16, no. 1, p. 321–357. DOI: 10.1613/ jair.953

[10] HAN, H., WANG, W. Y., MAO, B. H. Borderline-SMOTE: A new over-sampling method in imbalanced data sets learning. In *Lecture Notes in Computer Science (International Conference on Intelligent Computing ICIC 2005)*, 2005, vol. 3644, p. 878–887. DOI: 10.1007/11538059_91

[11] HE, H., BAI, Y., GARCIA, E. A., et al. ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In *Proceedings of 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*. Hong Kong, 2008, p. 1322–1328. DOI: 10.1109/IJCNN.2008.4633969

[12] ZHANG, J. J. Research on credit risk assessment of listed companies based on category imbalance data. (in Chinese) *Hefei University of Technology*, 2021.

[13] LI, Y. X., CHAI, Y., HU, Y. Q., et al. A review of imbalance data classification methods. *Control and Decision Making*, 2019, vol. 34, no. 4, p. 673–688. ISSN 1001-0920

[14] GOODFELLOW, I., POUGET-ABADIE, J., MIRZA, M., et al. Generative adversarial nets. *Advances in Neural Information Processing Systems*, 2014, p. 2672–2680. DOI: 10.3156/JSOFT.29.5_177_2

[15] ODENA, A. *Semi-Supervised Learning with Generative Adversarial Networks*. 2016, p. 1–3. [Online] Cited 2024-03-10. DOI: 10.48550/arXiv.1606.01583

[16] LIU, M. Y., BREUEL, T., KAUTZ, J. Unsupervised Image-to-Image Translation Networks. In *31st Conference on Neural Information Processing Systems (NIPS 2017)*. Long Beach (CA, USA), 2017, p. 1–11. DOI: 10.48550/arXiv.1703.00848

[17] RAJESWAR S., SUBRAMANIAN S., DUTIL F., et al. Adversarial generation of natural language. In *Proceedings of Meeting of the Association for Computational Linguistics*. Canada, 2017, p. 1–11. DOI: 10.18653/V1/W17-2629

[18] DONG, H. W., HSIAO, W. Y., YANG, L. C., et al. *MuseGAN: Multi-track Sequential Generative Adversarial Networks for Symbolic Music Generation and Accompaniment*. 2017, p. 1–13. [Online] Cited 2024-03-10. DOI: 10.48550/arXiv.1709.06298

[19] YU, L., ZHANG, W., WANG, J., et al. *SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient*. 2017, p. 1–11. [Online] Cited 2024-03-10. DOI: 10.48550/arXiv.1609.05473

[20] BRECK, E., CAI, S., NIELSEN, E., et al. The ML test score: A rubric for ML production readiness and technical debt reduction. In *Proceedings of 2017 IEEE International Conference on Big Data (Big Data)*. Boston (MA, USA), 2017, p. 1123–1132. DOI: 10.1109/BigData.2017.8258038

[21] YAN, Y. T., DAI, T., ZHANG, Y. W., et al. Neighborhood-aware oversampling method for unbalanced data sets. *Small Microcomputer Systems*, 2021, vol. 42, no. 7, p. 1–11.

[22] ZHANG, H., LI, X. J. L., LIU, M., et al. Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection. *Future Generation Computer Systems,* 2021, vol. 122, p. 130–143. DOI: 10.1016/j.future.2021.03.024

[23] LIPPMANN, R., HAINES, J. W., FRIED, D. J., et al. The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks*, 2000, vol. 34, no. 4, p. 579–595. DOI: 10.1016/S1389-1286(00)00139-0

[24] TAVALLAEE, M., BAGHERI, E., LU, W., et al. A detailed analysis of the KDD CUP 99 data set. In *Proceedings of 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*. Ottawa (Canada), 2009, p. 1–6. DOI: 10.1109/CISDA.2009.5356528

[25] JIA, S. W. *Intrusion Detection Based on Imbalanced Classification* (in Chinese). Tianjin University of Technology, 2023.

[26] XIAO, Y., XING, C., ZHANG, T., et al. An intrusion detection model based on feature reduction and convolutional neural networks. *IEEE Access,* 2019, vol. 7, p. 42210–42219. DOI: 10.1109/ACCESS.2019.2904620

[27] WANG, W., SHENG, Y., WANG, J., et al. HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, 2018, vol. 6, p. 1792 to 1806. DOI: 10.1109/ACCESS.2017.2780250

[28] KE, G., MENG, Q., FINLEY, T., et al. LightGBM: A highly efficient gradient boosting decision tree. In *Proceedings of 31st Conference on Neural Information Processing Systems (NIPS 2017)*. Long Beach (CA, USA), 2017, p. 3149–3157. ISBN 9781510860964

[29] CHEN, T., GUESTRIN, C. XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. San Francisco (CA, USA), 2016, p. 785–794. DOI: 10.1145/2939672.2939785

[30] LIU, J., YANG, D., LIAN, M., et al. Research on intrusion detection based on particle swarm optimization in IoT. *IEEE Access*, 2021, vol. 9, p. 38254–38268. DOI: 10.1109/ACCESS.2021.3063671

[31] LIU, L., WANG, P., LIN, J., et al. Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE Access*, 2020, vol. 9, p. 7550–7563. DOI: 10.1109/ACCESS.2020.3048198

[32] ZHANG, G., WANG, X., LI, R., et al. Network intrusion detection based on conditional Wasserstein generative adversarial network and cost-sensitive stacked autoencoder. *IEEE Access*, 2020, vol. 8, p. 190431–190447. DOI: 10.1109/ACCESS.2020.3031892

[33] ZHANG, J., LING, Y., FU, X., et al. Model of the intrusion detection system based on the integration of spatial temporal features. *Computers & Security*, 2020, vol. 89, no. 2, p. 1–9. DOI: 10.1016/j.cose.2019.101681

[34] SHARMA, N. V., YADAV, N. S. An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers. *Microprocessors & Microsystems,* 2021, no. 85, p. 1–11. DOI: 10.1016/J.MICPRO.2021.104293

[35] SAHU, S. K., MOHAPATRA, D. P., ROUT, J. K., et al. A LSTM-FCNN based multi-class intrusion detection using scalable

framework. *Computers and Electrical Engineering,* 2022, vol. 99, p. 1–19. DOI: 10.1016/j.compeleceng.2022.107720

[36] KANNA, P. R., SANTHI, P. Unified deep learning approach for efficient intrusion detection system using integrated spatial-temporal features. *Knowledge-Based Systems*, 2021, no. 226, p. 1–12. DOI: 10.1016/j.knosys.2021.107132

[37] WANG, Z., XU, Z., HE, D., et al. Deep logarithmic neural network for internet intrusion detection. *Soft Computing*, 2021, no. 25, p. 10129–10152. DOI: 10.1007/s00500-021-05987-9

About the Authors …

Ruihan XIANG was born in 1997. She received the Bachelor of Engineering (2021) in Computer Science and Technology from the China Jiliang University, Hangzhou, China. She is pursuing the Master of Engineering from the China Jiliang University, Hangzhou, China.

Sishan LI (corresponding author) graduated from the Northeast Normal University in 2017. Currently, he is the Head of Information Technology in Honghe Comprehensive Bonded Zone of Mengzi Economic and Technological Development Zone, Yunnan Province, China. His research interests are network information security and network terminal security.

Julong PAN (corresponding author) was born in 1965. He received his Bachelor's Degree and Ph.D. from Zhejiang University, China in 1987, and 2011. Now he is a Professor at the College of Information Engineering, China Jiliang University, Hangzhou, China. His main research interests are machine learning, wireless sensor network security and mobile computing.