International Journal of Information Technologies and Systems Approach
Volume 16 • Issue 2

Security Detection Design for Laboratory Networks Based on Enhanced LSTM and AdamW Algorithms

Guiwen Jiang, Guangxi Technological College of Machinery and Electricity, China*

ABSTRACT

With the addition of multimedia big data, the diversification of network data types becomes more prominent, the proportion of unstructured data increases sharply, and the requirements of data application show the characteristics of rapid change. Laboratory servers hold a large amount of core experimental data, which is at risk of being compromised in the event of a cyberattack, and the rapid pace of information technology has made cyberattacks complex. In the face of the great challenges posed by continuously changing networks to network security, this paper proposes a network exception detection approach that combines an improved inception module incorporating an attention mechanism and a Bi-LSTM. The inception module with the attention mechanism enhances the adaptability of the neural network to different spatial feature scales in the network stream, weakens irrelevant non-critical features, and exploits the advantages of the Bi-LSTM in terms of temporal features of the network stream to effectively improve the accuracy of the detection of network attacks.

KEYWORDS

Attention Mechanisms, Inception, Network Security, Sustainable Development of Network

INTRODUCTION

The era of multimedia big data makes has complicated the network environment as network functions become enriched and the characteristics of network security change (Xing et al., 2022). First, the era of big data causes the phenomenon of data scale to increase. Second, it opens the curtain to changes in data application requirements (Jin et al., 2022).

Structured data, unstructured data, and semi-structured data intersect within the network space. Network attacks exist in network flows, aiming to destroy the availability, confidentiality, integrity, and other critical attributes of network devices. In a group's lab, most of the core experimental data is stored on the lab's server. The server must be connected to the network to download or update relevant software during set up or maintenance (Alwageed, 2022). If a cyber-attack were to occur during this time, the core experimental data of the laboratory would be at risk of being leaked. An attack on the server could bring down the entire system, affecting research and threatening cyber security.

DOI: 10.4018/IJITSA.319721 *Corresponding Author

Therefore, malicious network traffic must be watched during network monitoring to immediately detect malicious network traffic and help defenders target relevant defense strategies in the face of network attacks (Jia, 2022). Hence, the ability to accurately detect vicious attack traffic in the network is critical to enhancing the capabilities and reliability of the network.

As traffic data continues to grow, researchers have introduced machine learning methods to classify and predict large-scale traffic data. This, in turn, enables traffic anomaly detection (Agrawal & Affijulla, 2022). Researcher-based traffic anomaly detection has used traditional machine learning methods via a single classifier or the fusing of multiple classifiers for detection (Sornsuwit & Jaiyen, 2015; Syarif et al., 2012). However, there have been unsatisfactory outcomes in finding the results of traffic anomaly detection based on traditional approaches. In addition, their detection performance was feature dependent. Most emphasize feature engineering and feature selection, as well as present a high false alarm rate.

This article investigates the network traffic anomaly detection model. The proposed network traffic anomaly detection model is obtained by incorporating an improved inception module that incorporates an attention mechanism in combination with Bi-LSTM. Local and long-range sequence features of network traffic data is retrieved using a modified inception module, including an attention mechanism and Bi-LSTM. An effective attention mechanism was incorporated into the inception module, focusing on features that impact classification and improve detection rates for a small number of attack categories. To improve model performance, the AdamW was chosen as the optimizer of the model in the training phase.

RELATED RESEARCH

The changing pattern of cyber-attacks has increased the difficulty of detecting network traffic anomalies. Based on the enabling effect of artificial intelligence, cyberspace security faces new risks, which include increasingly intelligent cyber-attacks, more frequent large-scale attacks, more covert cyber-attacks, more adversarial gaming of cyber-attacks, and increasing vulnerability to the theft of important data. Maintaining network security is both an offensive and defensive game. Network traffic anomaly detection, as a prerequisite for ensuring network security, is receiving more attention because it can identify unknown network attacks. Therefore, it is key to understand how to build an intelligent and efficient network anomaly traffic detection model.

Machine learning shows good performance in describing non-linear application problems. It is self-organizing and adaptive, with infinite approximation capabilities. This, in turn, leads to several machine learning-based research results for malicious network traffic detection (Shi et al., 2019). Sahani et al. (2018) proposed the application of the C4.5 decision tree algorithm to malicious network traffic detection and the classification of attacks. Tan et al. (2019) proposed a random forest (RF)-based method for detecting malicious network traffic, improving the detection performance of the model by using the synthetic minority oversampling technique (SMOTE) to alleviate class inequality in the dataset. Assiri (2021) then used a genetic algorithm to find the optimal parameters of the RF model to increase the classification accuracy of normal and abnormal network traffic by optimizing the classifier. Although the traditional methods can achieve good classification results when applied to malicious network traffic detection, they cannot learn the deeper features of network traffic. This creates a poor generalization ability of the model. It cannot handle more complex classification problems.

The deep neural network (DNN) can learn the deeply hidden features in the data. It can also train a classifier with high accuracy, which can improve the overall performance of the malicious network traffic detection model. In the field of deep learning, auto-encoder (AE), as a classical unsupervised learning model, facilitates the discovery of potential security threats. AE has efficient feature extraction capabilities and provides more possibilities to solve complex malicious network attack detection problems (Lai et al., 2021). Ustebay et al. (2019) and Awotunde et al. (2021), on the other hand, fed the data features of the network traffic extracted by the self-encoder directly into the DNN structure for training, resulting in better accuracy of the detection model. Recurrent neural

networks (RNNs) and convolutional neural networks (CNNs) are types of deep learning models commonly used for malicious network traffic detection. Khan et al. (2019) proposed to concatenate CNN models and long-short term memory (LSTM) to detect malicious network traffic. Zhang et al. (2020) used multi-scale CNNs and LSTM to extract spatiotemporal information of malicious network traffic for classification. This achieved good experimental results.

For deep learning approaches, the choice of the optimizer is related to the contract performance of the model for network traffic anomaly detection. As a classical optimization algorithm, the Adam algorithm (Kingma & Ba, 2014) has been used in computer vision and other fields. With the Adam algorithm, the weight of the neural network is iteratively updated based on training data. However, after many practical applications and research, researchers found that its convergence was not effectively guaranteed. They also identified problems with non-convergence or slow convergence.

TRAFFIC ANOMALY DETECTION METHOD BASED ON ATTENTION MECHANISM AND INCEPTION-BILSTM

Traffic Anomaly Detection Framework

The goal of this article is to design a traffic anomaly detection method that achieves superior detection performance on traffic data with a small number of traffic samples. In this regard, the proposed traffic anomaly detection method combines data resampling techniques and deep learning network models (Liao & Li, 2022). The overall detection structure of the approach is shown in Figure 1. It is made up of three main modules: (1) data pre-processing module; (2) traffic anomaly detection module; and (3) classification and evaluation module. The data pre-processing module is concerned with the quantification, normalization, and resampling of the training data from the raw traffic feature data. Quantization and normalization enable the data to meet the input format requirements of the deep learning model. This is more conducive to the training and detection of the model. Data resampling balances the traffic data, reducing the impact and bias of the original data category imbalance on the detection results.

Traffic Anomaly Detection Model Based on Attention Mechanism and Inception-BiLSTM

Traffic data can be seen as sequence data with backward and forward correlation. The traffic feature data has significant backward and forward sequence dependency and correlation between different features of the same sequence (Guo et al., 2021).

To enhance the detection rate of minority attack traffic, this article designs a traffic anomaly discovery model based on attention mechanism and Inception-BiLSTM. This helps to learn the traffic feature data and extract deep complex features. In this model, the BiLSTM network is used to implement the long-range sequence feature learning. The inception module with attention mechanism is used to broaden the network structure and increase the weight of features related to traffic categories. Thus, the model tends to pay attention to features that are more important for anomalous traffic detection. The detailed structure of the prototype is shown in Figure 2.

The input of the model is a processed grayscale map of the network traffic. The output is the category to which the network traffic belongs. The model consists of a convolutional layer, pooling layer, two inception modules with attention mechanisms, two LSTM layers, a fully connected layer, and Softmax. The two inception modules with attention mechanisms are introduced to pick up space features of network stream data. The LSTM modules are used to pick up time features in network stream data.

Inception Module With an Attention Mechanism

Figure 3 shows the primitive structure of the inception block. The aim is to aggregate multiple convolutional layers with 3×3 pooling layers, which improves the adaptability of the model to feature scales. However, this poses problems like high channel count dimensionality and inadequate feature

Figure 1.
Flow anomaly detection framework

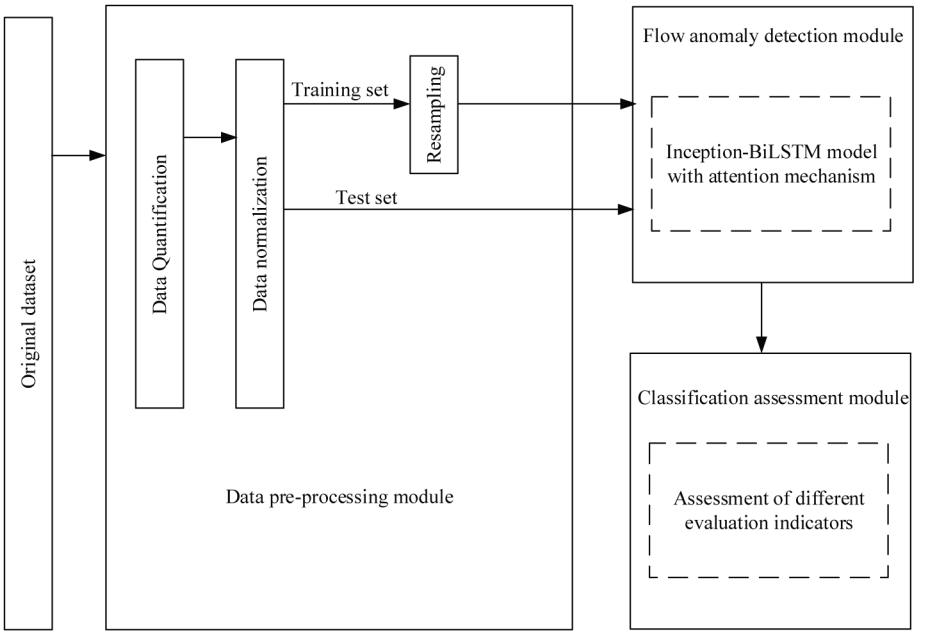


Figure 2.
Inception-BiLSTM structure with attention mechanism

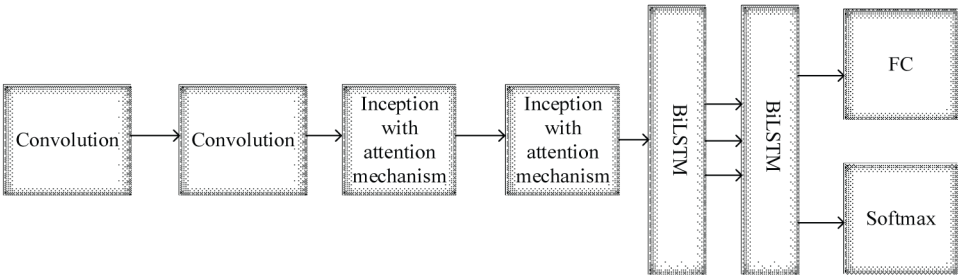
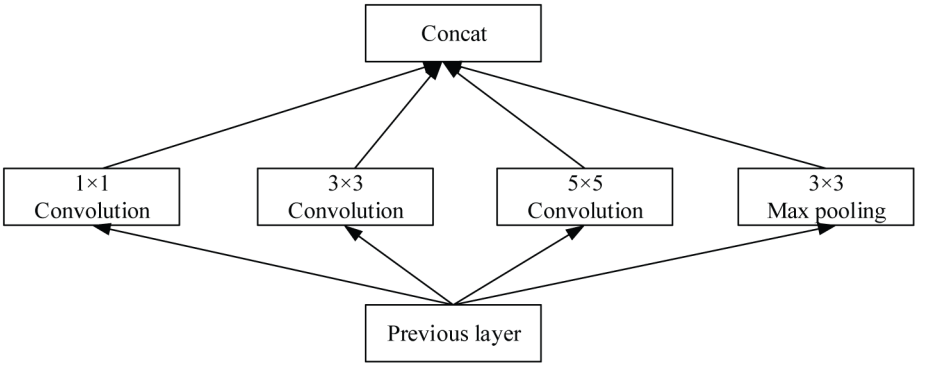


Figure 3.
Original structure of Inception module



extraction. Regarding the principle of the attention mechanism, when presented with a large amount of information, the limited attention resources are focused on a few key pieces of information. In addition, any useless and irrelevant information is ignored as the more critical information is extracted by features. Incorporating an attention mechanism that assigns corresponding weights to the different traffic features used to detect attacks is more beneficial to improving the detection rate of a small number of attack samples.

This article introduces the attention mechanism in the inception module. First, the number of channels is reduced by 1×1 convolution. Then, the attention mechanism is incorporated into the convolution to perform feature extraction at different scales and pooling to obtain information at multiple scales. Finally, the results are cascaded. The output and processing process is shown in equations (1)-(3). The structure of the improved inception module is shown in Figure 4:

$$e_t = u\tanh(w_t h_t + b) \tag{1}$$

$$a_t = \frac{\exp(e_t)}{\sum_{j=1}^{t}\exp(e_j)} \tag{2}$$

$$s_t = \sum_{t=1}^{t} a_t h_t \tag{3}$$

Bi-LSTM

BiLSTM is an LSTM variant. First, it has the long-range sequence learning capability of the LSTM model. Second, it improves LSTM by being able to learn the association relationship between the forward and reverse of sequence data. This makes the model more advantageous for classification problems [12].

This article uses the input traffic data to train the forward LSTM and reverse LSTM of BiLSTM. Its structure, as shown in Figure 5, contains an input layer, forward hidden layer, reverse hidden layer, and output layer. The forward LSTM extracts the forward features of the input deep traffic feature

Figure 4.
Structure diagram of the improved Inception module

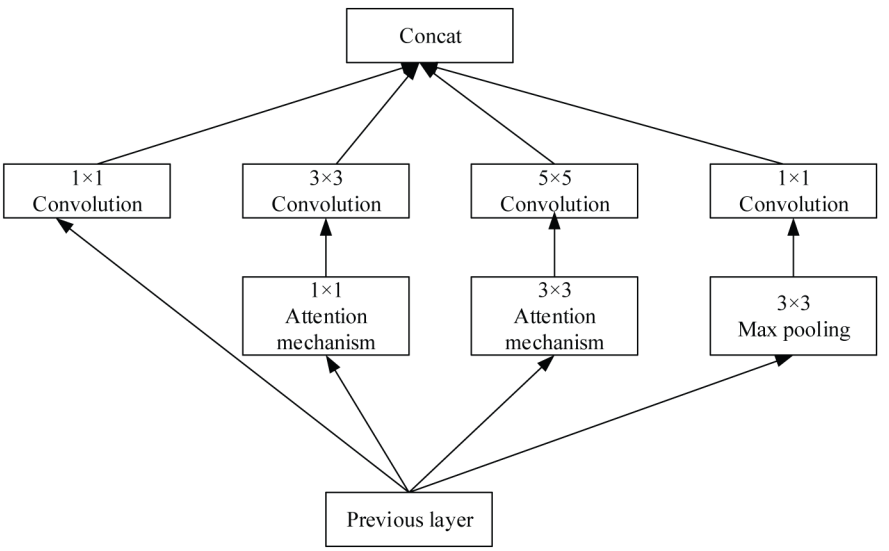
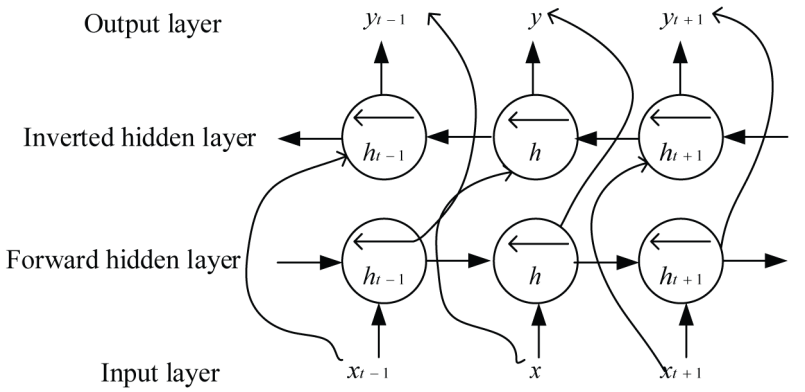


Figure 5.
Structure diagram of BiLSTM



sequence. The reverse LSTM, in contrast, extracts the reverse features of the deep traffic feature sequence from backward to forward. The output layer integrates the output data of both. The output vector calculation formula for the time step is shown in equation (4):

$$H_t = W'_{hf}h' + W''_{hb}h'' + b_h \tag{4}$$

AdamW Optimization Algorithm

The Adam algorithm, a modified neural network parameter optimization algorithm, has been used in a range of domains [11]. The Adam optimization algorithm is efficient and uses low memory expenditure, which makes it suitable for solving optimizations with a significant range of parameters. The optimization process of the Adam algorithm is as follows:

Establish the preliminary parameters.
α: The learning rate is generally taken as 0.001, which can be adjusted to suit the actual situation.
$\beta_1, \beta_2 \in (0,1)$: The current estimated exponential decay rate is generally taken as 0.9.
ε: prevent division by 0, generally taking 10^{-8}.
$f(\theta)$: Loss function under parameter θ.
Initialize the parameter vector θ_0, $m_0 = 0$, $v_0 = 0$, $t = 0$.
Repeat the following equation until θ_t converges:

$$t = t + 1 \tag{5}$$
$$g_t = \Delta_t f_t(\theta_t - 1) \tag{6}$$
$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t \tag{7}$$
$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g^2{}_t \tag{8}$$
$$\bar{m}_t = \frac{m_t}{1 - \beta_1^t} \tag{9}$$
$$\bar{v}_t = \frac{v_t}{1 - \beta_2^t} \tag{10}$$

$$\theta_t = \theta_{t-1} - \frac{\alpha \overline{m}_t}{\sqrt{\overline{v}_t} + \varepsilon} \tag{11}$$

Equations (7) and (8) are the weighted averages of the momentum exponents. Equations (9) and (10) are the deviation correction of the weighted average of the exponents.

Upon completion of the study, it is found that the convergence of the Adam algorithm is not effectively guaranteed. In addition, there is the problem of non-convergence or slow convergence. To address the convergence problem of the Adam algorithm, researchers have proposed many kinds of improvement methods, including theAdamW algorithm. The AdamW algorithm adds a weight decay factor to the parameter update, which is generally taken as 0.01. Other training parameters and methods are the same as the Adam algorithm,. The AdamW algorithm tends to have smaller losses on the training and test sets, yielding better generalization performance.

EXPERIMENT ANALYSIS

The article's experiments were made on a desktop computer with 32G of RAM, an Intel Core i7-8700 3.20 GHz CPU, and an Nvidia GeForce GT 730 GPU. It was programmed in Python 3.5 and evaluated on the NSL-KDD and CICIDS2017 datasets for detection of multiple classic and modern attacks effectiveness.

The NSL-KDD dataset is used for traffic anomaly detection. There are other updated datasets; however, it is still used for performance evaluation by state-of-the-art traffic anomaly detection literature. It removes redundant records from the dataset. It also contains normal samples and four attack samples with attack categories containing DoS, Probe, U2R, and R2L. The dataset contains 41-dimensional traffic features and 1-dimensional category labels. In the experiments, KDDTrain+_20Percent is used as the training set and KDDTest+ is the test set. The CICIDS2017 dataset is a traffic dataset with complex modern attack types. The dataset contains 3,119,345 network transmission samples, 78-dimensional traffic characteristics, and 1-dimensional category labels. These contain normal samples and 14 types of attack samples.

Second Classification Experiment

This section conducts binary classification experiments on traffic anomaly detection methods based on the NSL-KDD and CICIDS2017 datasets. The NSL-KDD and CICIDS2017 datasets were pre-processed by numerically labeling and normalizing the attribute data in both datasets. The network is sensitive to unbalanced data; therefore, it is necessary to ensure that the number of samples of BENIGN type and ATTACK type data are equal. The BENIGN class is downsampled using random downsampling. Several classes of the ATTACK class are upsampled using the SMOTE algorithm. To verify the detection performance of the models in this article, the experiments first compare the detection performance of three typical machine learning classification methods and three popular models that have better detection results on the category imbalance problem on the NSL-KDD dataset. Three machine learning methods are multilayer perceptron, RF, and 1DCNN- BiLSTM. Three classification models are CNN, BiLSTM, and DTNB+MOEFS model, respectively. Accuracy, precision, and detection rate (DR) factors are used to assess the detection performance of the model. The evaluation metrics are calculated as follows:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{12}$$

$$Precision = \frac{TP}{TP + FP} \tag{13}$$

$$DR = \frac{TP}{TP + FN} \tag{14}$$

TP is the number of samples correctly predicted as attack, TN is the number of samples correctly predicted as normal, and FP is the number of samples incorrectly predicted as attack. The sample size correctly predicted as normal, FP is the number of samples incorrectly predicted as attack, and FN is the number of incorrectly predicted normal samples. The experimental results are shown in Table 1. As can be seen in Table 2, when the anomalous traffic samples are less than the benign traffic samples, the method in this article achieves an accuracy rate of 93.4%, an accuracy rate of 93.52%, a detection rate of 94.55%, and an F1 score of 94.03% for the attack traffic. The false positive rate of the method in this article is 8.64%, which is only 0.69% more than the lowest false positive rate in other models. This indicates that the detection performance of this article's method for the NSL-KDD dataset is better than other methods in the case of imbalance between normal and abnormal traffic. This verifies the effectiveness of the article's method in facing an imbalance between normal and abnormal data in classical traffic dataset.

Validation of the detection performance of this article's comparison of different models is conducted on the CICIDS2017 dataset to evaluate the efficacy of the ability to detect novel modern attack samples. Due to the large data volume of the CICIDS2017 dataset, benign samples account for 80.30% and attack samples account for 19.70%. To improve the efficiency of the experiment, 10% of the data is extracted as the experimental data. The training set and test set are divided according to the ratio of 7:3. The experimental results are shown in Table 2. As can be observed from Table 2, the traffic anomaly detection accuracy of the proposed model in this article is improved by 2.11%

Table 1.

Model Name	Accuracy	Precision	Detection Rate	False Positive Rate	F1
MLP	79.92	93.26	71.02	6.72	79.82
RF	80.88	90.18	74.53	10.73	81.61
CNN	84.20	91.69	78.96	8.87	84.91
BiLSTM	87.01	92.54	83.96	7.95	88.04
DTNB+MOEFS	87.57	88.49	86.20	13.30	87.33
1DCNN+BiLSTM	89.06	88.42	88.92	10.34	88.67
Ours moudle	93.17	93.52	94.55	8.64	94.03

Table 2.
Dichotomous detection results based on the CICIDS2017 dataset (%)

Model Name	Accuracy	Precision	Detection Rate	False Positive Rate	F1
MLP	94.01	86.94	93.00	5.61	89.87
CNN	95.68	91.36	93.43	3.29	92.38
BiLSTM	98.14	92.86	96.85	3.74	94.81
RF	96.61	93.28	94.20	3.51	93.74
DTNB+MOEFS	96.80	97.40	96.70	3.70	97.05
Ours moudle	98.65	97.21	99.77	3.07	98.47

compared to the RF model, 4.94% compared to the MLP model, 3.10% compared to the deep CNN model, 0.52% compared to the BiLSTM model, and 1.91% compared to the DTNB+MOEFS model. The detection effect is significantly improved. The precision, detection rate, and F1-score of the proposed model are higher than other methods. The false positive rate is smaller than other methods. This provides additional validation of the effectiveness of the article's approach in detecting unbalanced traffic samples in novel datasets.

Multiclassification Experiments

Regarding the detection performance of the article's traffic anomaly detection method in distinguishing between attack types, the experiments are based on the NSL-KD dataset to evaluate the performance of the model's multiple classifications. The experiments compare the typical machine learning algorithms (MLP, RF) and three existing models (CNN, LSTM, and BiLSTM). These are more effective in facing the traffic data category imbalance problem. The detection performance of different models is shown in Figures 6 through Figure Supplement 9.

Figure 6 shows the comparison of the detection rate of the six methods. The colors indicate the detection rate of each model for normal traffic, DoS attack traffic, probe attack traffic, U2R attack traffic, and R2L attack traffic, respectively. According to Figure 6, the detection rate of the method in this article is slightly smaller than other algorithms. Its detection rate is 92.07%, which is 5.46% lower than the highest RF algorithm. However, regarding DoS attack traffic and U2R and R2L attack traffic with smaller sample sizes, this method achieves the highest detection rate compared with other methods (93.66%, 83.00%, and 84.66%, respectively). The detection rate of U2R attack traffic is improved by at least 13.70% as compared with other methods. The detection rate of R2L attack traffic is improved by at least 9.78% as compared with other methods. This result shows that the method can improve the detection rate for each attack sample with a smaller sample size. Additionally, it has a better ability to identify a few classes of attack samples compared to the baseline classifier.

Figure 7 shows the comparison of the detection accuracy of the six methods. Each color indicates the precision of the model for the category of traffic, class, and U2R attack traffic. A smaller sample size achieved the highest precision of 95.47% and 79.05%, respectively. For the normal class and four attack classes, the detection accuracy is more stable as compared with other methods. This indicates that the detection accuracy of the method in this article is good for all types of samples.

Figure 8 shows the comparison of the false positive rate of multi-category detection for six methods. Each color indicates the false positive rate of the model for each category of traffic. According to Figure 8, this article's method achieves the lowest false positive rate for normal class and DoS class (3.30% and 0.84%, respectively). The false positive rate for Probe, U2R, and R2L is

Figure 6.
Multi-classification detection rate based on NSL-KDD dataset

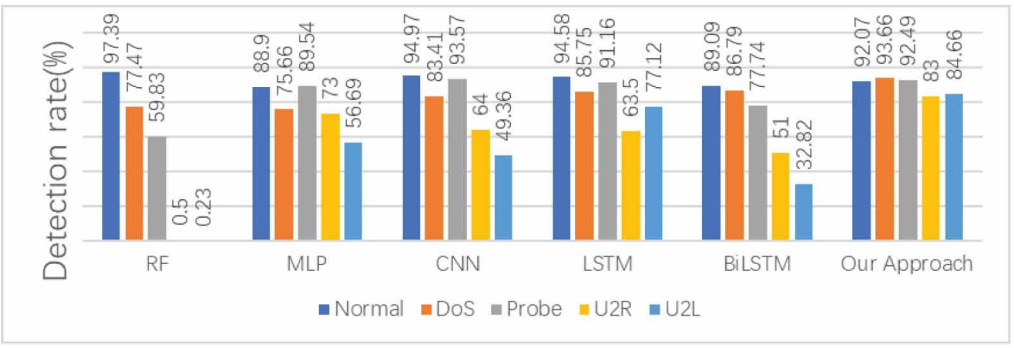


Figure 7.
Precision of multiclassification detection based on NSL-KDD data set

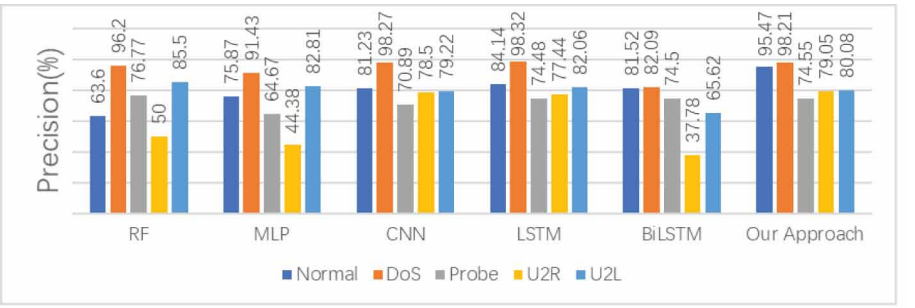
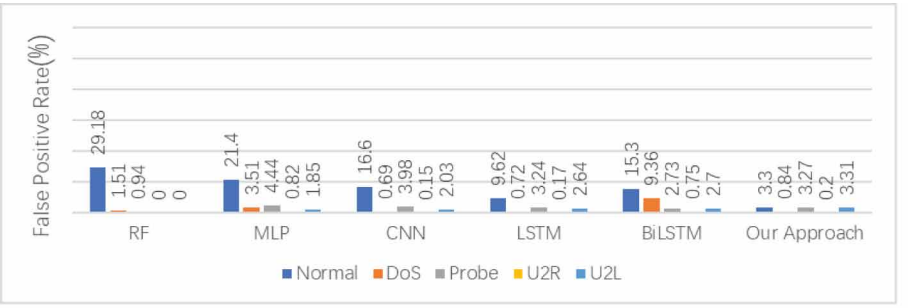


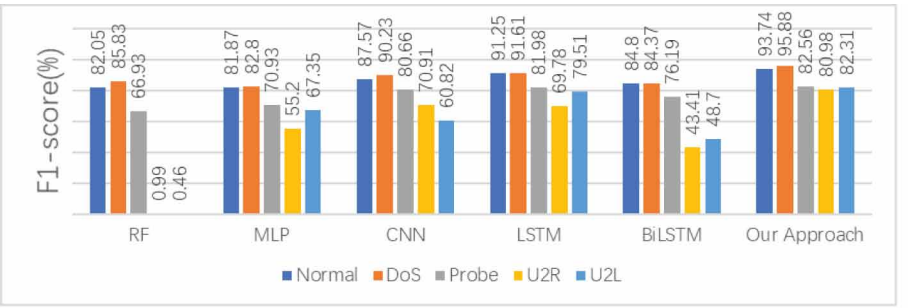
Figure 8.
False Positive Rate of multiclassification detection based on NSL-KDD data set



slightly higher than the individual models. The amount of normal class and DoS attack traffic data is misclassified, resulting in a slightly higher false positive rate. However, the false positive rate of the article's method for the five classes of data is smaller, none of which exceeds 4%.

Figure 9 shows the F1-score comparison of the six methods. Each color indicates the F1 score of the model for each category of traffic. F1-score is more reflective of the overall detection performance of the model. The F1-scores are 93.74%, 95.88%, 82.56%, 80.98%, and 82.31% for normal, DoS,

Figure 9.
F1-score of multiclassification detection based on NSL-KDD data set



Probe, U2R, and R2L attack traffic, respectively. This indicates that the method improves the detection rate of the few attack traffic data while ensuring precision.

From the comparison of performance parameters in Figure 6 through Figure supplement 9, it can be seen that the model in this article is better in each detection performance index for normal traffic and DoS, probe attack traffic with larger sample size, and U2R and R2L attack traffic with smaller sample size. However, it is slightly worse than other classes in the single evaluation index, it is the best in the detection rate of a few attack traffic and another performance, compared with other typical models have obvious improvement. This verifies the effectiveness and superiority of the method in this article for the multi-classification task of unbalanced traffic data.

CONCLUSION

To cope with the risk that laboratories may be subject to network attacks, as well as considering that the category imbalance trouble in traffic anomaly detection affects the detection accuracy of attack traffic data and the detection rate of a few attack classes of traffic, this article proposes a traffic anomaly detection model based on the attention mechanism and Inception-BiLSTM. The method can extract local features and long-range sequence features of traffic data, improve learning in the before-and-after correlation relationship of traffic feature data, and assign weights to the features according to their importance. In turn, it provides full play to the role of important features in traffic anomaly detection and improves detection accuracy and detection rate.

This article uses NSL-KDD and CICIDS2017 datasets for training and testing. The experimental results show that, in contrast to some existing typical and more popular machine learning algorithms, the method in this article achieves good results in various performance evaluation metrics for both binary and multivariate classification. This validates the effectiveness of the method in detecting unbalanced attack traffic. In the future, we will consider how to better exploit the features in the network to improve the accuracy of traffic anomaly detection, while minimizing the number of parameters to improve the efficiency of the model.

ACKNOWLEDGMENT

The author would like to thank the anonymous reviewers who provided valuable comments on this publication.

CONFLICTS OF INTEREST

The authors declare there is no conflict of interest.

FUNDING AGENCY

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Agrawal, A., & Affijulla, S. (2022). A concept for discrimination of electrical fault from cyber attack in smart electric grid. *Journal of Electrical Engineering*, *73*(4), 299–304. doi:10.2478/jee-2022-0039

Alwageed, H. S. (2022). Detection of cyber attacks in smart grids using SVM-boosted machine learning models. *Service Oriented Computing and Applications*, *16*(4), 313–326. doi:10.1007/s11761-022-00349-1

Assiri, A. (2021). Anomaly classification using genetic algorithm-based random forest model for network attack detection. *Computers Materials & Continua*, *66*(1), 767–778. doi:10.32604/cmc.2020.013813

Awotunde, J. B., Abiodun, K. M., Adeniyi, E. A., Folorunso, S. O., & Jimoh, R. G. (2021, November). A deep learning-based intrusion detection technique for a secured IoMT system. In *International Conference on Informatics and Intelligent Applications* (pp. 50–62). Springer.

Chou, H. H., & Tsai, F. S. (2022). Technology-enabled mobilization in the emergence of a value co-creating ecosystem. *Journal of Organizational and End User Computing*, *34*(1), 1–17. doi:10.4018/JOEUC.312855

Guo, S., Liu, Y., & Su, Y. (2021, September). Network traffic anomaly detection method based on CAE and LSTM. *Journal of Physics: Conference Series*, *2025*(1), 012025. doi:10.1088/1742-6596/2025/1/012025

Jia, X. (2022). Security control of cyber-physical systems with cyber attacks and mixed time-delays. *Journal of Electronics and Information Science*, *7*(3), 6–15.

Jin, Z., Ma, M., Zhang, S., Hu, Y., Zhang, Y., & Sun, C. (2022). Secure state estimation of cyber-physical system under cyber attacks: Q-learning vs. SARSA. *Electronics (Basel)*, *11*(19), 3161. doi:10.3390/electronics11193161

Khan, M. A., Karim, M. R., & Kim, Y. (2019). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry*, *11*(4), 583. doi:10.3390/sym11040583

Kingma, D. P., & Ba, J. (2014). *Adam: A method for stochastic optimization.* arXiv preprint arXiv:1412.6980.

Lai, J., Wang, X. D., & Xiang, Q. (2021). Overview of self-encoders and their applications. *Journal of Communication*, *42*(09), 218–230.

Liao, N., & Li, X. (2022). Traffic anomaly detection model using K-means and active learning method. *International Journal of Fuzzy Systems*, *24*(5), 1–19. doi:10.1007/s40815-022-01269-0

Morales, Y. N., & Suárez-Rocha, J. (2022). Management model for university-industry linkage based on the cybernetic paradigm: Case of a Mexican university. *International Journal of Information Technologies and Systems Approach*, *15*(1), 1–18. doi:10.4018/IJITSA.304812

Sahani, R., Rout, C., Chandrakanta Badajena, J., Jena, A. K., & Das, H. (2018). Classification of intrusion detection using data mining techniques. In *Progress in computing, analytics and networking* (pp. 753–764). Springer. doi:10.1007/978-981-10-7871-2_72

Shi, L. Y., Liu, J., & Liu, W. H. (2019). A review of cybersecurity situational awareness research. *Computer Engineering and Applications*, *55*(24), 1–9.

Sornsuwit, P., & Jaiyen, S. (2015, October). Intrusion detection model based on ensemble learning for U2R and R2L attacks. In *2015 7th international conference on information technology and electrical engineering (ICITEE)* (pp. 354–359). IEEE. doi:10.1109/ICITEED.2015.7408971

Syarif, I., Prugel-Bennett, A., & Wills, G. (2012, April). Unsupervised clustering approach for network anomaly detection. In *International conference on networked digital technologies* (pp. 135–145). Springer. doi:10.1007/978-3-642-30507-8_13

Tan, X., Su, S., Huang, Z., Guo, X., Zuo, Z., Sun, X., & Li, L. (2019). Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. *Sensors (Basel)*, *19*(1), 203. doi:10.3390/s19010203 PMID:30626020

Ustebay, S., Turgut, Z., & Aydin, M. A. (2019, June). Cyber attack detection by using neural network approaches: shallow neural network, deep neural network and autoencoder. In *International Conference on Computer Networks* (pp. 144–155). Springer. doi:10.1007/978-3-030-21952-9_11

Xing, S., Sun, W., & Deng, F. (2022). Event-triggered control for uncertain stochastic systems under triple network attacks. *Journal of the Franklin Institute*, *359*(16), 8869–8894. doi:10.1016/j.jfranklin.2022.08.025

Yang, Y., Siau, K., Xie, W., & Sun, Y. (2022). Smart health: Intelligent healthcare systems in the metaverse, artificial intelligence, and data science era. *Journal of Organizational and End User Computing*, *34*(1), 1–14. doi:10.4018/JOEUC.308814

Zhang, J., Ling, Y., Fu, X., Yang, X., Xiong, G., & Zhang, R. (2020). Model of the intrusion detection system based on the integration of spatial-temporal features. *Computers & Security*, *89*, 101681. doi:10.1016/j.cose.2019.101681