Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/86/20241604

Application of deep learning-based Intrusion Detection System (IDS) in network anomaly traffic detection

Fanyi Zhao[1a,*], Hanzhe Li[1b], Kaiyi Niu[2], Jiatu Shi[3], Runze Song[4]

[1a]Computer Science, Stevens Institute of Technology, NJ, USA
[1b]Computer Engineering, New York University, New York, USA
[2]Artificial intelligence, Royal Holloway University of London, Egham, UK
[3]Computer Science, University of Electronic Science and Technology of China, Cheng Du, China
[4]Information System & Technology Data Analytics, California State University, CA, USA

*Corresponding author E-mail: fzhao12@stevens.edu

Abstract. This study discusses the application of deep learning technology in network intrusion detection systems (IDS) and focuses on a new model named CNN-Focal. First, reviewing traditional IDS technology, it analyzes its limitations in dealing with complex network traffic. Then, the design principle of the CNN-Focal model is described in detail, which uses threshold convolution and SoftMax multi-class classification technology to improve abnormal traffic detection's accuracy and efficiency effectively. The experimental results show that CNN-Focal performs well on the open data set, demonstrating the potential and advantages of its application in the natural network environment and providing a new perspective and method for further research of deep learning in the field of network security in the future.

Keywords: Deep learning, Intrusion detection System (IDS), CNN-Focal Model, Abnormal network traffic

1. Introduction

Network intrusion detection is essential in ensuring network security in the digital age. With the popularization of networks and the interconnection of information, network intrusion events occur frequently, which bring severe threats and losses to countries, organizations, and individuals. Therefore, developing an efficient and reliable network intrusion detection system is an urgent task. Network intrusion is a behavior that causes threats and harm to network systems, including unauthorized access, malware attacks, denial of service attacks, and so on. Network intrusion detection becomes an important task to protect network systems' security. Traditional network intrusion detection methods are usually based on rules and statistical models, but these methods are limited by the rules' accuracy and the model's generalization ability [1]. In recent years, deep learning technology has provided new opportunities for network intrusion detection. The classification-based approach turns the network intrusion detection problem into a binary classification problem by training neural networks to distinguish between regular traffic and intrusion behavior. These methods mainly use convolutional

DOI: 10.54254/2755-2721/86/20241604

neural networks, recurrent neural networks, attention mechanisms, and other models to learn features and patterns.

2. Related work

2.1. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) originated from a "computer security threat monitoring and surveillance system" proposed by Anderson et al. [2] in 1980 for processing user audit data. Based on the same principle, Denning proposed to use the user characteristics generated by audit data to identify intrusions, that is, to obtain knowledge of the subject's behavior relative to the object's behavior from audit records and rules for detecting abnormal behavior. As a network security protection technology, IDS can fully use software and hardware to detect malicious activities by monitoring a network or system and issuing alerts in time to provide managers with responsive decisions, thus ensuring network resources' confidentiality, integrity, and availability.

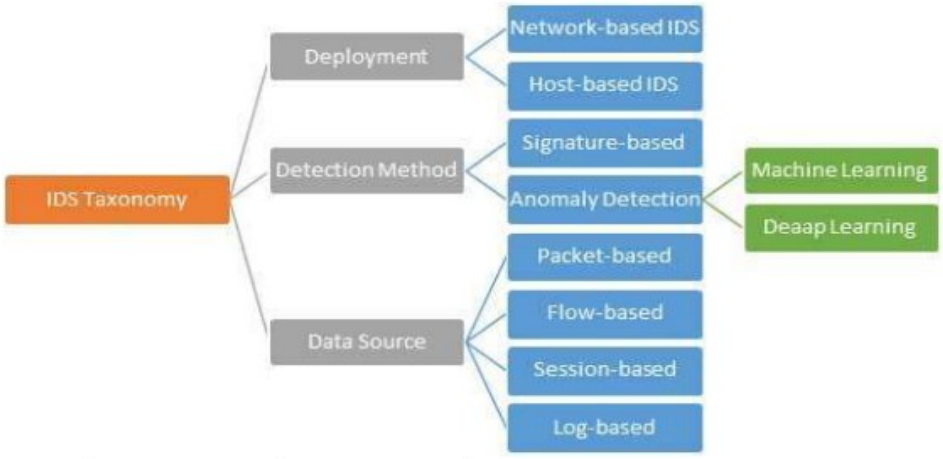

Figure 1. IDS classification

In the realm of cybersecurity, intrusion detection plays a crucial role in safeguarding networks. With the advancement of machine learning technologies, there has been a growing trend towards applying these techniques to intrusion detection research [3]. Deep learning, a subset of machine learning, excels in learning intricate patterns from sample data, making it highly efficient for feature extraction and model construction in detecting network attacks.

This paper begins by summarizing recent research on intrusion detection using machine learning methods. It then delves into a detailed exploration of intrusion detection techniques based on deep learning. Finally, it discusses current challenges and outlines future directions for advancing these technologies. This structured approach provides a comprehensive overview of how machine learning, particularly deep learning, is revolutionizing intrusion detection methods, addressing current capabilities and areas for further development.

2.2. Classification of intrusion detection systems

According to the different sources of detected data, intrusion detection can be divided into host-based intrusion detection and network-based intrusion detection. Host-based intrusion detection (HIDS) [4] collects input data from the hosts monitored by HIDS. Generally, HIDS uses log files as their primary information source and effectively identifies various intrusions by decoding and analyzing log files. The advantages of HIDS are its high-cost performance and low false positive rate. Still, the disadvantages are that only specific programs on the host can be monitored, they need to be installed on each host, and the detection range is limited.

DOI: 10.54254/2755-2721/86/20241604

Anomaly-based intrusion detection (AIDS) [5] usually requires recording everyday activities in the system, determining the characteristics of these activities, and quantitative description; when the user behavior deviates from the regular record, these behavior activities are defined as attacks. Anomaly-based IDS can detect unknown attacks, so it is the focus of scholars' research.

2.3. Intrusion detection technology of traditional machine learning

Traditional machine learning methods are widely used in anomaly-based intrusion detection. These methods typically include supervised learning, unsupervised learning, and semi-supervised learning, and are used to identify abnormal behavior in network traffic. However, while significant progress has been made, there is still room to improve overall detection accuracy. In this context, [6] proposed a network intrusion detection method based on Hidden Markov Model (HMM), focusing on dealing with abnormal traffic. They used principal component analysis (PCA) to extract features from the traffic data and used these features as inputs to the HMM. By analyzing the output probability of HMM, the type of traffic can be determined effectively, and an efficient intrusion detection system can be realized. This method not only performs well in detection rate, but also has significant advantages in processing speed and cost effectiveness [7]. This comprehensive use of machine learning and statistical models not only improves the efficiency of intrusion detection, but also points the way to improve network security technology in the future.

In the realm of intrusion detection systems, two prominent machine learning algorithms stand out: the K-Nearest Neighbor (KNN) [8]algorithm and Support Vector Machine (SVM). KNN is renowned for its precision in multi-classification tasks but faces challenges with high-dimensional network data. Addressing this, employed the tree seed algorithm (TSA) to preprocess data, extracting essential features that optimize KNN's classification performance. This approach, including the improved PKNN variant, demonstrated efficient real-time intrusion detection across datasets like KD99, NSL-KDD, and Kyoto2006+.

SVM, on the other hand, is valued for its ability to handle small sample sizes, nonlinearity, and high-dimensional data in intrusion detection. To enhance efficiency, proposed an SVM model using compressed sampling based on compressed sensing theory. By reducing data dimensionality before SVM classification, this method significantly reduces training and detection times while maintaining robust accuracy, enhancing overall intrusion detection capabilities.

2. Unsupervised machine learning methods

Unsupervised learning mainly deals with the problems in such scenarios as lack of prior knowledge, difficulty in manually labeling categories, or high cost through manual labeling. In intrusion detection, unsupervised learning technology does not need to label data categories but can directly classify network data. Standard unsupervised machine learning methods include k-means, Gaussian mixture model, and principal component analysis.

In the field of intrusion detection and network security, machine learning algorithms such as K-means and Gaussian Mixture Model (GMM) play pivotal roles. [9]K-means, an unsupervised clustering algorithm, identifies anomalies by grouping data points into clusters based on similarity, thus detecting potential intrusions. Researchers enhance its effectiveness by combining K-means with methods like the Classification and Regression Tree (CART), creating hybrid models to improve detection accuracy.

Additionally, advancements include hierarchical, multi-level intrusion detection models that organize data for more efficient analysis and quicker threat identification. On the other hand, GMM models the probability distribution of features to distinguish between normal and malicious data samples in network traffic, particularly effective in detecting unknown attacks when distributions overlap. These approaches highlight the ongoing evolution of machine learning in bolstering network security, addressing emerging threats with precision and scalability.

2.4. Application of deep learning in Intrusion detection systems (IDS)

The application of deep learning in intrusion detection systems (IDS)[10] has been one of the essential development directions in network security in recent years. Traditional IDS methods rely primarily on

DOI: 10.54254/2755-2721/86/20241604

rules and statistical models, which, while effective in specific scenarios, often show limitations in the face of increasingly complex and diverse cyber threats. By constructing multi-layer neural networks, deep learning can automatically learn features and patterns from raw data, thus improving the accuracy and efficiency of the IDS system to detect abnormal network traffic. LSTM can adapt to changing attack patterns and new threats to ensure the security and integrity of financial transactions.

Through these practical cases, the application of deep learning in IDS improves the detection accuracy and efficiency of the system. It expands its ability to deal with complex network environments and new threats. With the advancement of technology and the continuous expansion of application scenarios, deep learning technology will continue to play an essential role in network security, providing strong support for protecting network resources and data security.

3. Methodology

Recent years have seen significant advancements in deep learning, particularly in speech recognition, image recognition, and natural language processing. Deep learning excels in extracting abstract high-level features from raw data, eliminating the need for manual feature selection based on expert knowledge. Given its robust learning capabilities, researchers globally have explored integrating deep learning into network security. This study introduces CNN-Focal, a convolutional neural network-based intrusion detection model. CNN-Focal incorporates threshold convolution and Soft-max within the CNN framework for multi-classification tasks. Moreover, it employs the Focal Loss function to address imbalanced datasets, thereby enhancing intrusion detection accuracy effectively.

3.1. CNN-Focal Intrusion detection model

1. Basic principles of convolutional neural networks

In deep learning, Convolutional Neural Networks (CNNs) have established themselves as powerful and efficient models extensively used across various domains. A typical CNN architecture consists of fundamental layers: an input layer where data is initially fed into the network, followed by convolutional layers that extract intricate patterns from the input data. These convolutional layers are essential for capturing spatial hierarchies in data such as images or sequences.

Following the convolutional layers, pooling layers are often employed to down sample the feature maps, reducing their dimensionality while preserving important features. This alternation between convolutional and pooling layers aids in progressively learning and capturing complex patterns in the data. After several of these layers, fully connected layers are utilized. These layers establish connections between every neuron from the previous layer and every neuron in the subsequent layer, leading up to the output layer, which provides the final classification or prediction.

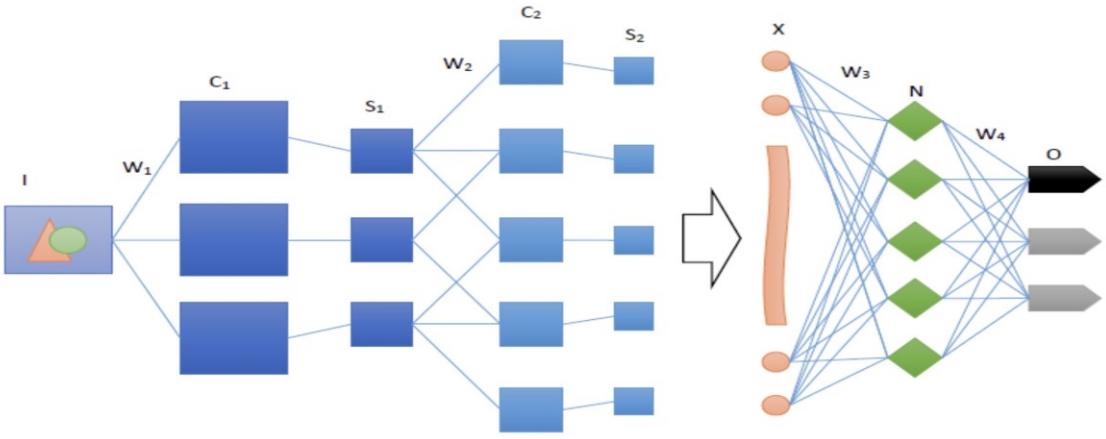

Figure 2. CNN model architecture diagram

DOI: 10.54254/2755-2721/86/20241604

CNNs excel in automatically learning hierarchical representations of data, which is crucial for tasks such as image recognition, where features can vary in scale and position. For instance, in medical image analysis, CNNs have been pivotal in detecting subtle patterns indicative of diseases, enhancing diagnostic accuracy. Moreover, in autonomous driving applications, CNNs process visual input to detect objects, pedestrians, and road signs, contributing to safer navigation. The structured layer arrangement and hierarchical feature learning capabilities of CNNs make them a cornerstone of modern deep learning architectures. Continual advancements in CNN technology drive innovations across artificial intelligence and machine learning applications, pushing the boundaries of what's possible in understanding and leveraging complex data patterns.

The Loss function evaluates the disparity between the predicted value (f(x)) and the actual value (Y) of the model, often denoted as (L(Y, f(x))). It measures the model's robustness; a lower loss function value indicates greater robustness of the model.

3.2. Experimental design

In this paper, the Focal Loss function is applied to the model. To verify the effectiveness of Focal Loss, this paper conducted an experimental comparison between Focal Loss and the cross-entropy loss function commonly used in deep learning; that is, the loss function of the CNN-Focal model was replaced with a cross-entropy loss function, and the model with the changed loss function was recorded as CNN-Cross.

To assess the performance of the models, various metrics such as precision, accuracy, recall rate, and F1 score are selected for evaluation. These metrics comprehensively understand how well the models classify and detect intrusions, considering aspects like true positive rate, false positive rate, and overall prediction accuracy. By comparing these indicators between the CNN-Focal and the comparative models, researchers can gauge the effectiveness and superiority of their proposed approach in detecting network intrusions.

1) Data set introduction. The KDD CUP 99 dataset is the most widely used in intrusion detection research. There are about 5 million records in the training set and about 300,000 in the test set in the KDD CUP 99 data set. The amount of data in this data set has high requirements on the experimental hardware environment. In addition, various statistical analyses show many redundant records in the KDD CUP 99 dataset, which will cause the model to overfit and require more computer resources in the training process, and the model convergence could be faster.

3.3. Data preprocessing

Two data types, nominal and numerical, are generally used. The 41 columns of feature attribute values in the NSL-KDD dataset have both nominal and numerical values. The attribute value types of protocol_ type, service, flag, and label in the data set are nominal, and the rest are numerical. Normalization of data is scaling data to a specific interval to fall from a large interval into a cell. In this paper, the OneHotEncoder in the scleral package is used to one-hot encode the protocol_ type, service, flag, and label four columns of nominal data.

Evaluation index. To evaluate the model, we need a practical and feasible experimental scheme and an evaluation index to measure the model's generalization ability, which is the performance measurement. The most commonly used performance measures in the unbalanced classification task are Accuracy, Precision, Recall, and F1 score.

DOI: 10.54254/2755-2721/86/20241604

3.4. Experimental Result

Table 1. Experimental data result table

Model	Dataset Used	Training Method	Evaluation Metrics	Results Summary
CNN-Focal	NSL-KDD	Train-test split (70%-30%)	Accuracy, Precision, Recall, F1-score	Achieved high accuracy and balanced performance across all metrics. The model effectively addressed class imbalance using Focal Loss.
CNN-Cross	NSL-KDD	70%-30%	Accuracy, Precision, Recall, F1-score	Compared performance with CNN-Focal using Cross Entropy Loss, showing differences in effectiveness in handling class imbalance.
SVM	NSL-KDD	70%-30%	Accuracy, Precision, Recall, F1-score	Provided benchmark for traditional machine learning approach in intrusion detection, showing competitive results.
Random Forest	NSL-KDD	70%-30%	Accuracy, Precision, Recall, F1-score	Demonstrated ensemble learning's effectiveness in handling complex feature relationships.
Decision Tree	NSL-KDD	70%-30%	Accuracy, Precision, Recall, F1-score	Showed basic decision-making capability with moderate performance metrics.

Here are the key conclusions:

1. Model Performance: CNN-Focal outperformed traditional methods like SVM, Random Forest, and Decision Tree regarding accuracy, precision, recall, and F1-score. It showcased robustness in handling the dataset's class imbalance using Focal Loss.

2. Comparison with CNN-Cross: Comparing CNN-Focal with CNN-Cross (using Cross Entropy Loss) showed that Focal Loss significantly enhanced the model's ability to classify minority classes, which is crucial for real-world intrusion detection scenarios.

3. Dataset Suitability: NSL-KDD dataset's partition into training and testing sets facilitated robust evaluation of model performance across different attack types, enhancing model generalization.

4. Future Directions: Future research could explore hybrid models combining CNN architectures with traditional machine learning algorithms for enhanced accuracy and efficiency in intrusion detection.

This conclusion synthesizes the experimental findings, emphasizing CNN-Foal's suitability and superiority in handling intrusion detection tasks compared to traditional methods.

4. Conclusion

With the rapid development of information technology, the issue of network security has increasingly become a focal point of global attention. This paper examines the current landscape and challenges of network security, explores the application of deep learning and artificial intelligence in defense strategies, and proposes future-oriented approaches. This paper proposes an integrated model of deep learning and artificial intelligence for network security defense, forecasting future trends in defense strategies. Future network security defenses will be more intelligent, automated, and adaptable to evolving network environments. As technology advances, new defense technologies will emerge, bolstering network security.

In conclusion, deep learning and artificial intelligence hold immense potential for enhancing network security defenses. Continued optimization and advancement of these technologies will help establish a more secure and reliable digital environment, supporting the growth of the digital economy. Addressing cyber security challenges requires collaborative efforts from governments, enterprises, academia, and other stakeholders to safeguard cyberspace's security and stability. "This revision improves grammar,

DOI: 10.54254/2755-2721/86/20241604

coherence, and logical flow while maintaining the original content's meaning and emphasis on the application of deep learning and artificial intelligence in network security.

References

[1] Sagduyu, Yalin E., Yi Shi, and Tugba Erpek. "IoT network security from the perspective of adversarial deep learning." 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2019.

[2] Alom, M. Z., & Taha, T. M. (2017, June). Network intrusion detection for cyber security using unsupervised deep learning approaches. In 2017 IEEE National Aerospace and Electronics Conference (NAECON) (pp. 63-69). IEEE.

[3] Kumar, C., Bharati, T. S., & Prakash, S. (2021). Online social network security: a comparative review using machine learning and deep learning. Neural Processing Letters, 53(1), 843-861.

[4] Gong Y, Zhu M, Huo S, et al. Utilizing Deep Learning for Enhancing Network Resilience in Finance[C]//2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2024: 987-991.

[5] Uppal, H. A. M., Javed, M., & Arshad, M. (2014). An overview of the intrusion detection system (IDS) and its commonly used techniques and classifications. *International Journal of Computer Science and Telecommunications*, *5*(2), 20-24.

[6] Abbas, S. H., Naser, W. A. K., & Kadhim, A. A. (2023). Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Global Journal of Engineering and Technology Advances*, *14*(2), 155-158.

[7] Pradhan, M., Nayak, C. K., & Pradhan, S. K. (2020). Intrusion detection systems (IDS) and their types. In *Securing the Internet of Things: Concepts, methodologies, tools, and applications* (pp. 481-497). IGI Global.

[8] Tian, J., Li, H., Qi, Y., Wang, X., & Feng, Y. (2024). Intelligent medical detection and diagnosis assisted by deep learning. Applied and Computational Engineering, 64, 121-126.

[9] Borkar, A., Donode, A., & Kumari, A. (2017, November). A survey on the Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS). In *2017 International Conference on Inventive Computing and Informatics (ICICI)* (pp. 949-953). IEEE.

[10] Liu, B., Cai, G., Ling, Z., Qian, J., & Zhang, Q. (2024). Precise positioning and prediction system for autonomous driving based on generative artificial intelligence. Applied and Computational Engineering, 64, 42-49.