Network traffic monitoring based on CNN-SVM

Qian Wu

Department of Computer Science and Software Engineering, School of Hebei University of Technology, 300401 Tianjin, China

Abstract. In a modern complex network, network monitoring and measurement have become increasingly important. The traditional network traffic monitoring methods face the challenge of efficiency and accuracy when dealing with massive data. The proposed hybrid model in this study uses convolutional neural networks (CNNs) and support vector machines (SVMs) to address these concerns and increase the effectiveness of network traffic monitoring. This paper uses CNN to extract features from network traffic data. CNN has the ability to recognize intricate patterns in the data and automatically extract valuable characteristics from the raw data. The SVM classifier receives the retrieved characteristics and uses them to further classify the data in order to distinguish between normal and abnormal traffic. By doing this, this paper may more successfully combine the benefits of SVM for classification with CNN's advantages for feature learning, enhancing traffic monitoring's precision and resilience. According to the experimental data, the hybrid model performs far better in network traffic categorization tasks than the standard techniques, with a reduced false positive rate and higher accuracy. This research shows that CNN-SVM model is an effective network traffic monitoring tool, which can provide high quality detection results while ensuring high efficiency.

1. Introduction

The task of safeguarding computer networks from illegal use has become more pressing for governments, corporations, and regular people in recent times. According to Morgan (2016), the cybersecurity industry was expected to grow by more than twofold, from $75 billion in 2015 to $170 billion by 2020 [1]. The development of network traffic detection technology has gone through many stages. Initially, signature-based detection and basic traffic analysis tools such as Wireshark were widely used. In order to increase inspection efficiency and accuracy, cutting-edge techniques like deep packet inspection (DPI) and machine learning are being deployed.

Contemporary approaches to network traffic monitoring include a range of approaches, from passive monitoring (capturing and analyzing traffic data without changing the operation of the network) to active monitoring (injecting synthetic traffic to detect network health). The complexity of the Internet has made designing scalable tools and applications for network traffic monitoring and analysis (NTMA) a crucial approach [2].

Corresponding author: 225813@stu.hebut.edu.cn

CNNs are a key deep learning model that have produced amazing results in voice recognition, image processing, and other areas thanks to their strong feature extraction capabilities. CNN is the most well-known algorithm among the several deep learning algorithms [3]. In order to extract local features from the raw input, a CNN needs the convolution layer. In the field of network traffic monitoring, CNN can automatically extract high-level feature representations from the original network traffic data, which are of great significance to distinguish normal traffic from abnormal traffic. However, a single CNN model may be troubled by overfitting and poor generalization ability in classification tasks [4]. In order to overcome these problems, this paper proposes a method that combines CNN with SVMs, namely CNN-SVM method. CNN-SVM classification model will achieve more accurate network traffic monitoring. In order to obtain more accurate network traffic monitoring, the SVM is utilized as a classifier and the deep learning model as a feature learner [5].

This paper aims to explore the network traffic monitoring method based on CNN-SVM, and show the advantages and potential of this method by analyzing the basic principles of CNN and SVM and their applications in network traffic monitoring in detail. This article will first outline the history, importance, and present demands of network traffic monitoring. It will also discuss the issues that the field is now facing. The CNN-SVM based network traffic monitoring method's implementation procedure, including data pretreatment, feature extraction, classification, and other crucial phases, will then be thoroughly explained in this study. Finally, the CNN-SVM model's prediction accuracy will be demonstrated in this study by comparing it to the CNN-SVM model.

2. Principle of classification model based on CNN-SVM

Image and time series data are processed particularly effectively by CNN, a deep learning model that can automatically extract features from raw input. In network traffic detection, CNN identifies patterns and abnormal behaviors in traffic data through its convolutional layer and pooling layer. The convolution layer identifies local features through sliding Windows (convolution cores), while the pooling layer is used to reduce feature dimensions while preserving important information. These operations allow CNN to extract features from complex network traffic data that help with classification. SVMs are grouped together as similar supervised learning techniques that are used for regression and classification [6]. The objective is to create a decision limit between two classes that enables label forecasting with one or more feature vectors [7]. SVM is particularly adept at handling high-dimensional data, and by employing kernel techniques, it can efficiently handle nonlinearly separable data. When it comes to network traffic detection, SVM uses CNN-extracted features as input and bases its classification judgments on them.

The essential characteristics of both classifiers are combined in the CNN-SVM model. CNN is used to extract features automatically and SVM is used to classify binary data in the hybrid model suggested [8]. The pre-processed CNN+SVM architecture is more accurate, efficient, and loss-free than alternative combinations and single classifiers [9]. The convolutional layer and pooling layer of the CNN model have powerful computing capabilities, which can reduce the loss rate of images in the translation process, and thus greatly reduce the influence of feature vectors. The size of the feature vector in the fitting process may be decreased and the model's ability to fit successfully managed by using various convolution and pooling layers. Based on the kernel function idea, SVM takes nonlinear mapping as the theoretical basis to map high-dimensional space from nonlinear to linearly separable, and then seeks the optimal classification hyperplane (classification function) with the aim of maximizing classification interval.

The CNN-SVM model uses CNNs as feature extractors. CNN automatically learns the characteristics of network traffic data through multiple convolutional layers and pooling layers. These layers capture local connection patterns and hierarchies in the data, generating feature maps that represent important features of the input data. This feature of CNNS makes them well suited for handling network traffic data, which often contains complex, high-dimensional information. The output of CNN is used as the input of SVM to make the final classification decision. SVM is known for its ability to maximize classification intervals, distinguishing between different classes by finding the optimal decision boundary. To process data that is both linear and nonlinear, SVM utilizes kernel techniques and maps it to a high-dimensional space, resulting in a better decision boundary.

After the CNN component of the model is first trained, the backpropagation approach improves the convolution kernel parameters to extract meaningful information. The SVM classifier is then trained using the characteristics that were retrieved. In the training process, the performance of the model on the training data is gradually improved through continuous iterative optimization. The SVM method has a benefit over the standard SVM method because it directly converts binary classification problems into two multi-classification problems with short time and fast speed. The output of all classifiers determines the final classification result when dealing with multiple classification problems. SVM uses a one-to-many (OvR) strategy to train a classifier for each class [10].

3. Experiment

3.1 Experimental settings

The experiment used the publicly available dataset USTC-TF2016. The USTC-TF2016 dataset is derived from actual network traffic and contains a large amount of network data for both normal and malicious traffic. The experiment stipulated that the test set made up 30% of the total data and the training set accounted for the remaining 70%, in accordance with the usual machine learning allocation ratio. The experimental data was used in the ten classification experiment of the two models to compare the accuracy of the two models.

3.1.1 Experimental configuration

This experiment uses Keras as the front-end deep learning framework and Tensor Flow as the back-end framework. CNN model is utilized as a feature extractor, while SVM is utilized as a classification tool. The experimental configuration is shown in Table 1.

Table 1. Three Scheme comparing

Experimental configuration	
Name	Model
Operating System	64-bit Windows 11
CPU	13th Gen Intel(R) Core(TM) i7-13620H
Memory	16GB
Graphics Card	NV GTX 1 070

3.1.2 Experimental indexes

The experiment included the following four experimental indices: F1 Score, Precision, Accuracy, and Recall.

By calculating the harmonic mean of accuracy and recall, the F1 Score metric ensures a balance between accuracy and recall.

$$\mathrm{F1\,Score} = 2 \times \frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}} \quad (1)$$

The percentage of samples that are precisely classified as positive when all samples are projected to be positive is referred to as precision.

$$\mathrm{Precision} = \frac{\mathrm{True\,Positive}}{\mathrm{True\,Positives} + \mathrm{False\,Positives}} \quad (2)$$

Accuracy is defined as the ratio between the number of properly recognized samples and all samples.

$$\mathrm{Accuracy} = \frac{\mathrm{True\,Positives} + \mathrm{True\,Negatives}}{\mathrm{Total\,Samples}} \quad (3)$$

Recall refers to the proportion of positive samples that are correctly classified compared to all genuine positive samples.

$$\mathrm{Recall} = \frac{\mathrm{True\,Positives}}{\mathrm{True\,Positives} + \mathrm{False\,Negatives}} \quad (4)$$

3.2 Analysis of experimental results

In order to compare the CNN-SVM classification model's performance with the CNN model alone, the tests aimed to confirm the model's validity in network traffic classification situations.

Ten categories were used to categorize the data set in order to conduct the experiment. The test findings demonstrate that the CNN model and CNN-SVM model can achieve recall rates and recognition accuracy of over 90% over a wide range of data. Furthermore, the CNN-SVM model's 95% accuracy is greater than the CNN model's 93% accuracy. The difference between the CNN and CNN-SVM models is seen in Fig. 1.

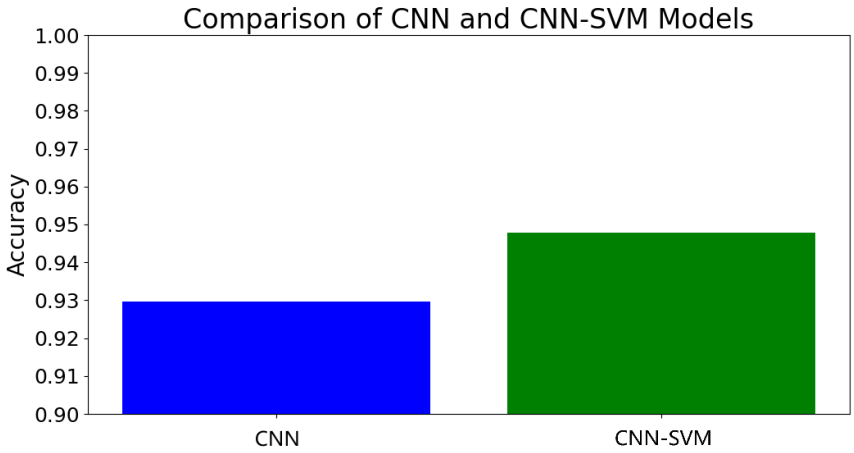

Fig. 1. Comparison of CNN and CNN-SVM Models

According to the results, the CNN-SVM model is superior to the CNN model in terms of test accuracy. This implies that further SVM classification might be able to offer higher accuracy for particular workloads. CNN-SVM blends the strengths of SVM's robust feature classification in high-dimensional feature spaces with CNN's benefits in feature extraction.

The features extracted by CNN are classified by SVM. This combination may improve the classification performance, because SVM performs well in processing complex features and small sample data.

The Classification report of CNN-SVM shows that some categories (such as 2, 4, 5, 7, 8, 9, 10) have very high F1-score, indicating that SVM has excellent classification performance in these categories. SVM can make use of the features extracted by CNN for more accurate classification. However, the classification performance of CNNS may be low in some categories, especially when dealing with complex patterns or features. Table 2 displays the CNN-SVM categorization report.

Table 2. CNN-SVM Classification Report

CNN-SVM test accuracy: 0.95				
CNN test accuracy: 0.93				
CNN-SVM classification report:				
	Precision	Recall	F1-Score	Support
0	0.75	0.45	0.56	240
1	1.00	0.97	0.98	159
2	1.00	1.00	1.00	1845
3	0.72	0.60	0.65	260
4	1.00	1.00	1.00	394
5	1.00	1.00	1.00	1755
6	0.48	0.78	0.59	232
7	0.99	1.00	0.99	184
8	1.00	1.00	1.00	264
9	1.00	1.00	1.00	256
10	1.00	0.99	1.00	316

The experimental results show that CNN may not be as accurate as SVM in processing some complex features. By separating feature extraction and classification tasks, CNN-SVM enables SVM to classify in higher-dimensional, finer feature Spaces, which may improve the overall performance of the model.

In addition, as can be seen from the confusion matrix, CNN-SVM classification is more accurate on most categories, especially on complex categories, and performs better. However, the confusion matrix of CNN may show more confusion in some categories, which may be due to the loss of some important information in the process of feature extraction. The confusion matrix is shown in Figs. 2 and 3.

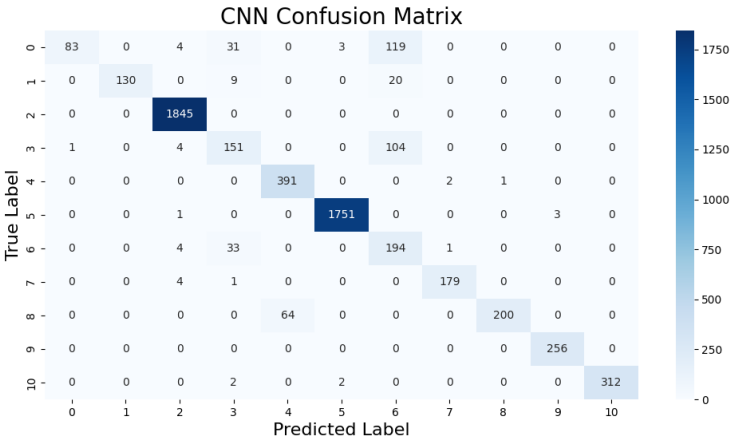

Fig. 2. CNN confusion matrix

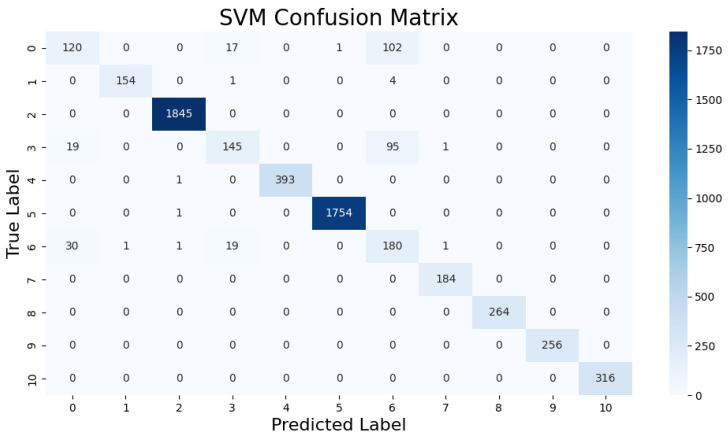

Fig. 3. CNN-SVM confusion matrix

CNN-SVM may reduce the confusion between categories through the fine classification capability of SVM, thus improving the classification accuracy. SVM's ability to classify features may help reduce some classification errors of CNN.

The experimental findings and data suggest that the CNN-SVM model is more accurate in test accuracy than the CNN model, which suggests that SVM is better at handling the characteristics extracted by CNN. CNN-SVM integrates the benefits of both CNN and SVM in feature extraction to optimize feature space use and enhance classification efficacy. CNN-SVM performs better in classifying most categories, especially when dealing with complex or unevenly distributed features.

4. Conclusion

This study describes a CNN and SVM-based network traffic monitoring technique and uses several tests to demonstrate its superiority and efficacy. In order to create an effective network traffic monitoring model, this experiment effectively combines the potent feature extraction capabilities of CNN with the effective classification performance of SVM. The model surpasses conventional network traffic monitoring techniques in terms of testing speed,

training duration, and accuracy. It also considerably increases the efficiency and accuracy of network anomaly identification. These findings are supported by comparative studies. This accomplishment offers network managers a more dependable tool in addition to fresh perspectives for network security research.

In conclusion, the network traffic monitoring method based on CNN-SVM can achieve high precision. It is predicted that this method will play a more significant role in network security with continuous exploration and optimization, guaranteeing the safe and stable operation of the network.

References

1. R. Vogel, Closing the cybersecurity skills gap. Salus J. **4**, 32-64 (2016)
2. P. Casas, AD. Alconzo, T. Zseby, M. Mellia, Big-DAMA: big data analytics for network traffic monitoring and analysis, in Proceedings of the 2016 workshop on Fostering Latin-American Research in Data Communication Networks, Association for Computing Machinery, August 22 (2016) 1-3
3. R. Yamashita, M. Nishio, RKG. Do, K. Togashi, Convolutional neural networks: an overview and application in radiology. Insights Imaging. **9**, 611-629 (2018)
4. Y. Yang, J. Jin, H. Zheng, Y. Li, M. Xu, Y. Chen, Learn Generalization Feature via Convolutional Neural Network: A Fault Diagnosis Scheme Toward Unseen Operating Conditions. IEEE. **8**, 91103-91115 (2020)
5. MC. Laskowski, Vapnik-Chervonenkis Classes of Definable Sets. J Lond Math Soc. **2**, 377-384 (1992)
6. H. Bhavsar, MH. Panchal, A review on support vector machine for data classification. IJARCET. **1**, 185-189 (2012)
7. WS. Noble, What is a support vector machine?. Nat Biotechnol. **24**, 1565-1567 (2006)
8. S. Ahlawat, A. Choudhary, Hybrid CNN-SVM classifier for handwritten digit recognition. Procedia Comput Sci. **167**, 2554-2560 (2020)
9. R. Sharma, A. Sungheetha, An efficient dimension reduction based fusion of CNN and SVM model for detection of abnormal incident in video surveillance. JSCP. **3**, 55-69 (2021)
10. G. Qin, X. Huang, Y. Chen, Nested One-to-One Symmetric Classification Method on a Fuzzy SVM for Moving Vehicles. Symmetry. **9**, 48 (2017)