Encrypted Network Traffic Identification Based on 2D-CNN Model

Yan Zhou, Huiling Shi*, Yuhan Zhao, Wei Gao and Wei Zhang*
Shandong Provincial Key Laboratory of Computer Networks,
Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan, Shandong, China
zy_qlu@163.com; shihl,yhzhao@sdas.org; wgao0917@163.com; wzhang@sdas.org

***Abstract*—Rapid development of the Internet has enabled explosive growth of various network traffic. How to classify and identify different categories of network traffic among these huge network traffic for cyberspace security has always been a hot research topic. In our study, we found that the composition structure of data frames and grayscale maps in the original traffic is very similar. Combined with recent research of deep learning in image processing, this paper proposes a 2D-CNN model-based network traffic recognition algorithm, while transforming traffic to grayscale maps for recognition. To validate the effectiveness of our proposed model, we use the public network dataset ISCX-VPN-NonVPN-2016 and USTC-TF2016. Experimental results prove that the average accuracy is 98.7% in regular encrypted traffic identification and 97.6% for malicious traffic identification. Our method provides new solutions for network traffic identification.**

***Index Terms*—Network security, traffic identification, network monitoring, deep learning**

I. Introduction

Works on network traffic identification through deep learning have continued to be popular in recent years. With the rapid growth of network traffic transmission volume and network structure complexity, it puts higher demands on network traffic monitoring and management. On the one hand, fields of network security need to identify the intrusion traffic; on the other hand, more accurate network traffic identification and classification can be better for traffic monitoring and resource allocation to guarantee network QoS [1]. How to accurately classify different traffic types has become a key problem to improve network service quality.

In this paper, we propose a method for identifying network traffic using image processing, using grayscale maps instead of traditional samples for network traffic data identification, converting the network traffic packet (Pcap) format to grayscale map format in the data input module kind, and automatically filling the content data to be identified as images for saving. By converting specific traffic data bit streams into images, a cross-fertilization study between network traffic recognition techniques and object vision recognition techniques is conducted. In our study, we found that the hexadecimal network traffic data stored in the Pcap data file is converted to decimal and takes values in the range of $0 \rightarrow 255$, which exactly corresponds to the range of each pixel point in the grayscale map.

Experiments are conducted separately for different classes of network traffic in our work. We chose the network public dataset ISCX-VPN-NonVPN-2016 (ISCX) [2] dataset with USTC-TFC2016-master (USTC) [3] dataset experiments including two classification experiments, nine classification experiments and eighteen classification experiments, for network traffic identification experiment.

Overall, contributions of our work are listed as followed:

1) We design a convolutional neural network based 2D-CNN model for identifying network traffic data, with optimal parameters of the model for network traffic identification through various tests.
2) Compared with traditional network traffic recognition algorithms, higher training accuracy is achieved with a shorter training time period.
3) By converting specific traffic data bit streams into images, a cross-fertilization study between network traffic recognition techniques and object vision recognition techniques is conducted.

The rest of the paper is organized as follows. Section II describes the related work. Section III describes the data preprocessing module we used and the 2D-CNN convolutional neural network approach. Section IV focuses on the experimental results and analysis. Section V presents future work with possible improvements.

II. Related Works

The traditional network traffic classification methods include clustering, support vector machine, C4.5 and so on Anshu Priya et. al. [4] proposed to analyze real-time network data traffic situation in universities using KMeans clustering algorithm. Wang et. al. [5] used C4.5 for describing application behavior features to classify p2p traffic. Coull et. al. [6] proposed to classify p2p traffic by analyzing packet features to propose traffic analysis of encrypted messaging services:Apple iMessage and other message classification. Mauro et. al. [7] proposed to reveal encrypted WebRTC traffic by machine learning tools, using the random forest approach.

This work was supported by Natural Science Foundation of Shandong Province (No.ZR2019LZH013 and No.ZR2020LZH010) and the National Natural Science Foundation of China (No.61802233).

Wang et. al. in [3] [8] took two dimensions of CNN (1D and 2D CNN) for feature extraction of raw traffic data after pre-processing. The authors verified the superiority of these two methods by observing the accuracy rates in the experimental evaluation metrics, etc., and achieved a large surpassing relative to the traditional network traffic classification techniques. Lopez et. al. [9] combined CNNs and RNNs for network traffic classification. The two dimensions of the network input data are the flow statistical features selected by the authors (source port number, destination port number, packet direction, number of load bytes, TCP window size, etc.) and the packet sequence number, respectively. The authors achieved excellent results in their study of combinatorial networks by keeping the feature vector dimension constant in the output of the CNN and flattening the other two dimensions as the temporal dimension needed for the RNN, and using the matrix thus constructed as the input to the neural network. Lotfollahi et. al. [10] proposed Deep packet: a new method for cryptographic traffic classification using deep learning Zou et. al. [11]. propose a method for cryptographic traffic classification based on convolutional long and short term memory neural networks.

We transform the problem of network traffic classification into the problem of data traffic image classification by combining the field of traffic visualization and computer vision, so as to better solve the problem of traffic identification and classification.

III. Scheme Design

In this section, we analyze the factors affecting the network traffic recognition problem, address the proposed optimization modules about transforming traffic characteristics to grayscale map and convolutional neural network based traffic recognition. And finally, we establish the traffic recognition optimization model.

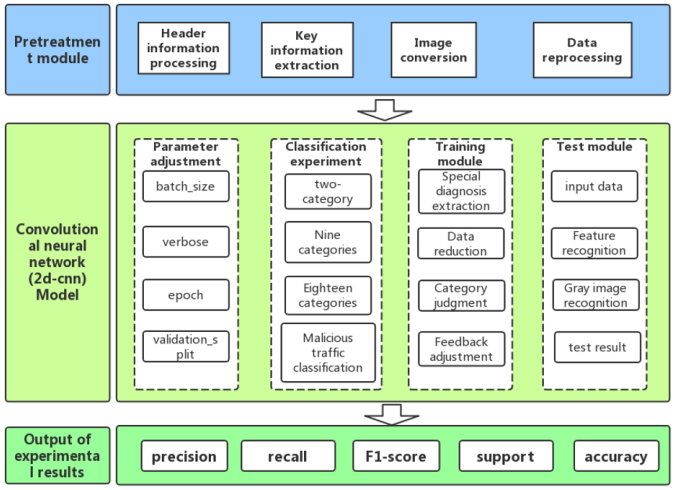


Fig. 1: System framework of model classification

A. System Framework

As shown in Fig.1,the data preprocessing module includes four steps: header information processing, key information extraction, image conversion and data reprocessing. The convolutional neural network module includes feature extraction, data refinement, category determination, feedback adjustment and other methods to train the convolutional neural network model. The test data was input into the test module containing the trained convolutional neural model.

B. Data pre-processing

In the pretreatment module of this article, we will in the packet header information as to eliminate redundant information, only to extract the pcap packets of information namely in pcap data, remove the 24B the pcap file header information and pcap 16B information in baotou Before we study found now n packets, packet of effective length of about $50 \rightarrow 1480$ Bytes. Therefore, in this paper, packets smaller than 1024 Bytes are padded with zero with the limit M(1024 Bytes), and packets larger than 1024 Bytes are clipped to the size of the first 1024 Bytes.

Step 1:The Pcap Header data and Packet Header data in the Pcap file are eliminated for redundancy. In the network traffic classification identification, this $24B+16B$ data is considered as redundant data in this paper.

Step 2:The obtained remaining data frame hexadecimal data such as: (e8, e7, 32, 3c, 65 ...) are converted to decimal representation as (232, 231, 50, 60, 101 ...) . Convert one byte of eight bits of binary data in the packet into a value from 0 to 255, which exactly corresponds to the value of the pixel points in the grayscale image.

Step 3: Arrange the one-dimensional sequence data in bytes according to the order in the data packet, and then convert the one-dimensional sequence data into a two-dimensional array $M = m^2$ of size 32×32 $(m \times m)$ and save it as a grayscale image file.

The range of each byte in the data frame is 0 to 255 that corresponds with the values of each pixel in the grayscale map. Hence, feature extraction is performed via grayscale map instead of the byte stream format of traditional network traffic recognition, after taking the results of convolutional neural network for image processing direction into consideration.

C. Convolutional Neural Network Model

1) Analysis: Workflow of the convolutional neural network (2D-CNN) is based on network traffic recognition method. By converting the pre-processed Pcap file mentioned above to grayscale images, the generated grayscale image will be used as input to the model. After processing by multiple convolutional layers and pooling layers, the recognition process is completed in accordance with the category of traffic or applications.

2) Model introduction: We deployed a convolutional neural network model in our study. And in our attempts to experiment on the 2D-CNN model using grayscale images, we found out that tests run smoothly under the simple convolutional neural network model. Compared with brief descriptions for 1D-CNN and 2D-CNN models in the study of Wei Wang [5],

TABLE I: 2D-CNN model structure

Layer	Operation	Input	Filter	Stride	Padding	Output
1	Conv2D +ReLU	32*32	3*3	1	Same	32*30*30
2	2D max pool	32*30*30	2*2	2	Same	32*15*15
3	Con2D +ReLU	32*15*15	3*3	1	Same	64*13*13
4	2D max pool	64*13*13	2*2	2	Same	64*6*6
5	Conv2D +ReLU	64*6*6	3*3	1	Same	64*4*4
6	Flatten	64*4*4	Null	Null	None	1024
7	Full connect	1024	Null	Null	None	2/9/18
8	Softmax	2/9/18	Null	Null	None	2/9/18

we concluded that the processing process in our paper is more in-line with the input of the model.

We used a similar LeNet-5 convolutional neural network [12] to build a 2D-CNN for the network traffic identification work. But the feature acquisition method and scale size are different in the convolutional layer. There are eight layers in our model as we can see in the table above.

IV. Experimental Results

In this section, experiments are conducted using the network public dataset ISCX dataset with the dataset USTC. The ratio of the training set test is set to 9:1, and a specific description of the sample sets used for each experiment is introduced followed.

A. Evaluation Metrics

We judged the accuracy based on the cumulative true positives, false positives, true negatives and false negatives of all data sets. The final evaluation metrics are Accuracy, Precision, Recall and F1-score.

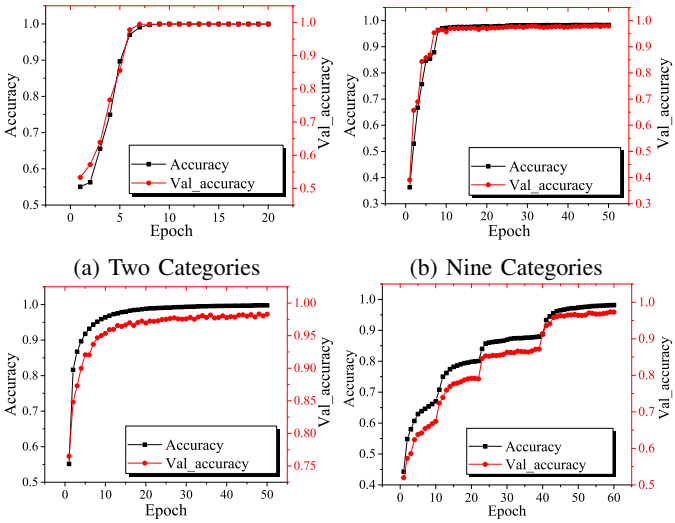
B. Environment

The ISCX dataset published by Draper et. al.. [2] and the UTSC dataset published by Wang et al. [3], both include stream features and raw traffic (pcap format). In our experiments, some small samples of traffic data were removed because their sample size was much smaller than the 5000 samples required in the preprocessing stage, so we selected 9 categories with sufficient data samples in the final traffic category selection. In the UTSC dataset, we use 7+3 malicious and non-malicious traffic categories, to identify the model's ability to identify malicious traffic.

C. Result Analysis

1) ISCX-VPN-NonVPN-2016: The experimental results of network traffic identification on the dataset ISCX are divided into three groups including: two categories, nine categories, and eighteen categories, respectively.

In our paper, the goal of the binary classification experiments is to identify two different types of traffic, regular



(a) Two Categories (b) Nine Categories

(c) Eighteen Categories (d) Malicious and Non-Malicious Results

Fig. 2: Experimental Results

encrypted traffic and VPN protocol encapsulated traffic. Ten different traffic data samples are used in the binary classification experiment, 10 types of regular encrypted traffic and the corresponding 10 types of VPN protocol encapsulated traffic, each with 1000 samples, for a total of 20,000 samples. The experiments were conducted for 20 iterations. In the nine-classification experiment, we use the ISCX dataset to classify aim, facebook, email, netflix, hangouts, youtube, skype, vimeo, and spotify, in order to identify nine types of regular encrypted traffic respectively. A maximum of 5000 samples are taken for each type of traffic. The experiment is performed for 50 iterations. The aim of this experiment is to enable the model to predict nine types of traffic.

In the eighteen classification experiments, we use the nine classifications (nine common types of encrypted traffic and nine corresponding types of VPN encapsulated traffic), taking a maximum of 5000 samples for each type of traffic.

2) USTC-TFC2016-master: In the USTC dataset, we use $7 + 3$ categories, i.e., identify seven types of normal traffic and three types of malicious traffic, with normal traffic using BitTorrent, Facetime, Gmail, MySQL, WorldofWarcraft, Weibo, and Skype. Malicious traffic includes Nsis-ay, Virut, Zeus.

As shown in Fig.3, in each experiment all encrypted traffic and vpn encapsulated traffic experimental metrics are in the range of 0.976 to 1. This shows that the model in this paper has great advantages in network traffic identification work, and our model is compared with the traditional model below.

D. Summary

Accuracy of 2 categories, 9 categories (Non-VPN), 18 categories, and malicious, non-malicious traffic classification by distribution experiments reaches 100%, 97.8%, 98.5%, and 97.6%, respectively.

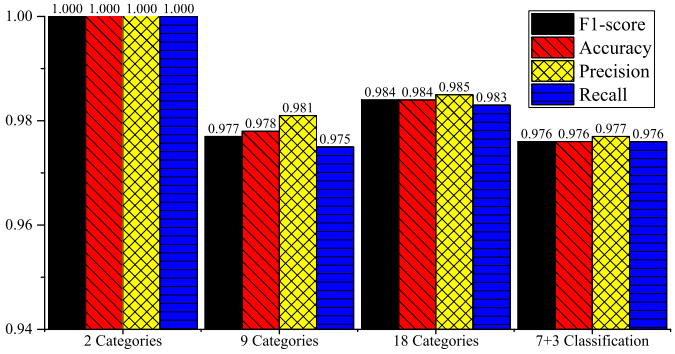


Fig. 3: List of experimental results

TABLE II: Accuracy of malicious traffic identification

	Precision	Recall	F1-score
Zeus	97.9%	98.7%	98.3%
Virut	94.5%	96.7%	95.6%
Nsis-ay	97.4%	94.3%	95.9%

Our method has the ability to detect the traffic flow for regular encrypted traffic and VPN encapsulated traffic. Wang et. al.. [5] use the C4.5 machine learning approach to select the used traffic feature dataset using manual feature extraction. So they both do not have features for early detection. In contrast, this paper uses the original traffic dataset and our method can extract features automatically.

TABLE III: Comparison with two categories model testing

	Non-VPN		VPN	
	Precision	Recall	Precision	Recall
C4.5	89.0%	92.0%	90.6%	88.8%
2D-CNN	100%	100%	100%	100%
Improvement	11.0%	8.0%	9.4%	11.2%

TABLE IV: Comparison with Multi-categories testing

	Non-VPN		VPN	
	Precision	Recall	Precision	Recall
C4.5	84%	87.6%	89%	85.5%
2D-CNN	98.5%	98.3%	98.1%	97.5%
Improvement	14.4%	10.7%	9.1%	12%

The experimental results show that this paper can get higher accuracy by 2D-CNN convolutional neural network, due to the use of grayscale graph image classification method in dataset selection. Coull et.al. [6] and Mauro et al. [7] used packet features and stream features respectively, which makes their ideas limited by the extraction of dataset features. Finally, because only the first 1024 Bytes of each session are used in the data processing stage of this paper, some malicious traffic will be disguised in the format of normal data traffic, which leads to a less accurate analysis of them, which also provides ideas and directions for the next experimental analysis.

V. Conclusion

This paper analyzes the problem of network traffic identification using convolutional neural networks, proposes to process network traffic data overlooking redundant information in the data pre-processing stage, and proposes a 2D-CNN algorithm based on convolutional neural networks. It performed 9.1% higher in non-VPN data identification accuracy reaching 98.1%, compared to C4.5. In VPN protocol encapsulated traffic, it also achieved 14.4% higher results than C4.5, reaching 98.5%. For malicious traffic identification, the accuracy of this model reached 97.6%.

Acknowledgment

Thanks to Qilu University of Technology (Shandong Academy of Sciences) Science, Education and Industry Integration Innovation Pilot Project ”Supercomputer Internet Key Technology Research and Application Demonstration. Huiling Shi and Wei Zhang are the corresponding authors.

References

[1] K. Yu, L. Tan, X. Wu, and Z. Gai, “Machine learning driven network routing,” in *2019 6th International Conference on Systems and Informatics (ICSAI)*, pp. 705–712. IEEE, 2019.

[2] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, “Characterization of encrypted and vpn traffic using time-related,” in *Proceedings of the 2nd international conference on information systems security and privacy (ICISSP)*, pp. 407–414, 2016.

[3] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, “End-to-end encrypted traffic classification with one-dimensional convolution neural networks,” in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 43–48. IEEE, 2017.

[4] A. Priya, S. Nandi, and R. Goswami, “An analysis of real-time network traffic for identification of browser and application of user using clustering algorithm,” in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 441–445. IEEE, 2018.

[5] D. Wang, L. Zhang, Z. Yuan, Y. Xue, and Y. Dong, “Characterizing application behaviors for classifying p2p traffic,” in *2014 International Conference on Computing, Networking and Communications (ICNC)*, pp. 21–25. IEEE, 2014.

[6] S. E. Coull and K. P. Dyer, “Traffic analysis of encrypted messaging services: Apple imessage and beyond,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 5–11, 2014.

[7] M. Di Mauro and M. Longo, “Revealing encrypted webrtc traffic via machine learning tools,” in *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, vol. 4, pp. 259–266. IEEE, 2015.

[8] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” in *2017 International Conference on Information Networking (ICOIN)*, pp. 712–717. IEEE, 2017.

[9] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, “Network traffic classifier with convolutional and recurrent neural networks for internet of things,” *IEEE Access*, vol. 5, pp. 18 042–18 050, 2017.

[10] M. Lotfollahi, M. J. Siavoshani, R. S. H. Zade, and M. Saberian, “Deep packet: A novel approach for encrypted traffic classification using deep learning,” *Soft Computing*, vol. 24, no. 3, pp. 1999–2012, 2020.

[11] Z. Zou, J. Ge, H. Zheng, Y. Wu, C. Han, and Z. Yao, “Encrypted traffic classification with a convolutional long short-term memory neural network,” in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 329–334. IEEE, 2018.

[12] Y. LeCun, L. D. Jackel, L. Bottou, C. Cortes, J. S. Denker, H. Drucker, I. Guyon, U. A. Muller, E. Sackinger, P. Simard *et al.*, “Learning algorithms for classification: A comparison on handwritten digit recognition,” *Neural networks: the statistical mechanics perspective*, vol. 261, no. 276, p. 2, 1995.