Abnormal Traffic Classification Based on Deep Learning Technique

Naseer Abdulhussein Lafta

Islamic Azad University, Isfahan Khorasgan Branch, Iran, Salhelalinasseer@gmail.com

In this paper, we propose a deep-learning framework for Abnormal traffic classification. There has been a huge increase in Abnormal traffic in recent years which poses a serious security threat to financial institutions, businesses, and individuals. To combat this, new classifications are essential to quickly classify traffic so that their behavior can be analyzed. This study presents a deep learning framework for Convolutional Neural Networks (CNN), a recent deep learning technique that has demonstrated better performance than classical learning algorithms, particularly in image classification applications. Inspired by this achievement, we suggest a CNN-based traffic classification architecture. This approach shows that our performance outperforms the state-of-the-art. On the Malimg datasets, the suggested technique obtains an accuracy of 98.80%, respectively.

Keywords: Traffic Classification, Convolutional Neural Network, deep learning.

1. Introduction

As computer networks have been more widely used and developed—particularly mobile internet—they have become ingrained in every area of peoples lives. Because of this, there are an increasing number of network applications, which in turn cause a wide variety of network traffic types to be generated throughout the information transfer and communication process. The administration and security of networks are greatly challenged by the variety of network traffic. Consequently, there is an increasing need to classify network traffic, identify various types of communication or encrypted traffic [1], detect malicious traffic [2], find network assaults or intrusions [3], and increase the efficiency of network operation. They are necessary for network operation, administration, and security [4].

Both domestically and internationally, network traffic categorization research has been steadily advancing. Numerous types of categorization studies are emerging, ranging from conventional methods based on port number and deep packet inspection to machine learning methods like Support Vector Machine (SVM) and decision trees. Additionally, some studies compare and analyze various traffic classification techniques.

Classification techniques based on recurrent neural networks (RNN) and convolution neural networks (CNN) have become more popular with the advent of deep learning. There are now a large number of articles on the categorization of network traffic, most of which use machine learning and conventional classification techniques. Additionally, a number of publications regarding various deep learning algorithms as well as studies about enhancing performance and deep learning algorithm performance have been published. To the best of our knowledge, there aren't many review publications on deep learning-based traffic classification, though [5].

1.1 Evaluation Criteria

Before comparing and analyzing various categorization techniques, it is important to select appropriate assessment criteria. The classification results are often assessed using the classification accuracy and error rate [6] [9–10]. However, performance measurements like accuracy and recall will also be utilized because of the uneven distribution of certain samples or the consideration of multi-angle assessment of the classification results [11]. These are the descriptions of the assessment criteria.

As stated in formula (1), accuracy is equal to the number of samples properly detected divided by the total number of samples.

The accuracy (ACC) may be defined as follows given the training set D= {(x1,y1), (x2,y2), …, (xm,ym)}, where xi∈(x1,xm) is the sample to be categorized, yi∈(y1,ym) is its real classification, and f is the classifier.

Let TP represent the proportion of samples that are both class-labeled and really belong to a class. Let FP represent the number of samples that are labeled as belonging to a class but are not in fact in that class. Let FN represent the number of samples that are genuinely members of the class but are not labeled as such.Let TN represent the total number of samples that are neither in the class nor have a class label. Formula (2) and formula independently (3) may be used to express the accuracy (PRE) and recall (REC).

Simultaneously, an effective traffic categorization system should possess high recall, precision, and accuracy [7]. Nonetheless, there are instances where the recall and accuracy rates conflict. If you are unable to take into account both, you should choose which is more crucial based on the specifics of the application. The recall rate might be given additional weight when discussing the coverage of test findings. However, accuracy is given more weight when discussing the veracity of test results.

1.2 Traffic Classification Based on Deep Learning

SVM and decision trees are examples of machine learning algorithms that are fundamentally shallow algorithms. When dealing with small data samples, the graph featuring several hidden layers [8]. It can suit complicated functions better due to the number of layers, and each layer can extract distinct characteristics that can be combined to generate higher-level features. When it comes to accuracy and dependability, feature extraction outperforms professional manual extraction. The algorithm's ralization ability is low, and it can't even represent extremely complicated non-linear functions [9].

A perceptron network with many hidden layers is used in deep learning [8]. It can suit complicated functions better due to the number of layers, and each layer can extract distinct characteristics that can be combined to generate higher-level features. When it comes to accuracy and dependability, feature extraction outperforms professional manual extraction.

In contrast to traditional machine learning-based classification methods that rely on artificial feature extraction, deep learning-based classification allows the neural network to learn how to extract traffic features on its own, achieving end-to-end traffic classification, where the input is the raw network traffic and the output is the classification of traffics or related services and applications.

1.3 Traffic Classification Based on Convolution Neural Network

An early version of the convolutional neural network was proposed by Yann LeCun, one of the troikas of artificial intelligence and recipient of the 2018 Turing Award, the highest prize in the world of computers. The network's excellent performance was confirmed by handwritten numeral recognition tests. It offers three main advantages over regular neural networks: pooling, weight sharing, and local connections [10].

Due to their extensive connectivity, artificial neural networks require a lot of time to train. Inspired by the real nervous system, convolutional neural networks minimize this by only establishing connections between a single node and its neighbouring nodes. Filtering, also known as weight sharing, lowers the number of parameters required for training by allowing each neuron to connect with the one before it. Pooling enhances data size, decreases over-fitting, and lessens the influence of noise and interference while dividing feature maps into smaller sections.

Convolutional neural network traffic classification uses training and learning to select features from input traffic data, determining model weights and parameters. Pre-processing is necessary for raw data .

Convolutional neural networks may be categorized into one-, two-, and three-dimensional varieties based on the various items that need to be processed. Text and audio are examples of temporal data that are often processed by 1D-CNN. While 3D-CNN is capable of processing three-dimensional data, including stereo pictures and video, 2D-CNN is often used to process images as well as audio and video data represented in the time- and frequency-domains. The majority of convolutional neural network-based traffic classification techniques employ 2D-CNN [11], while some also use 1D-CNN and 3D-CNN [12].

2. Related Work

Using different network models, deep learning has achieved some noteworthy successes in the identification of malicious traffic. For instance, the authors in [13] presented a unique approach to network-based anomaly identification that leverages deep autoencoders to identify aberrant network traffic originating from hacked Internet of Things devices by extracting behavior snapshots of the network. Commercial IoT devices infested with real botnets, including BASHLITE and Mirai, are used to test the methodology. However, the work's success mostly depends on several artificial data sets that the author constructed, which might not provide as much variation in data interchange. In a different study [2], the authors suggested a CNN-based malware traffic categorization technique that treats traffic data as pictures.

In [14] study proposes a method to speed up packet-level detection in intrusion detection systems (IDSs) using word embedding and the LSTM model, enabling efficient classification of incoming packets as malicious or legitimate, thereby reducing detection latency.

There are now a number of additional cutting-edge, pertinent research, including [15]. These kinds of works are primarily characterized by their reliance on the flow or session-based method, which indexes traffic according to the flow.

3. Methodology

3.1 Model Overview

Convolution Neural Networks (CNNs) are what we employ to classify traffic. An picture of traffic is the input for our network, and the output is a set of scores for different traffic classifications. The class with the highest score is then chosen to represent our prediction for the given traffic.

3.2 Dataset

The Malimg Dataset has been used to train and assess the suggested model. 9,339 malware grayscale photos from 25 malware types make up the Malimg Dataset [16].

4. Results

Table 1. Validation accuracy on Malimg dataset.

Method	**Accuracy of method**
Method in [17]	97.18%
GIST+SVM [18]	93.23%
2D-CNN [18]	98.52%
Proposed method	98.80%

Table 1 presents a comparison of several approaches' validation accuracy using the Malimg dataset. Among all earlier methods, our model's accuracy (98.80%) was the greatest. Nevertheless, the accuracy only reached 97.18% with the Method in [15], 93.23% with GIST+SVM [16], and 98.52% with 2D-CNN [16].

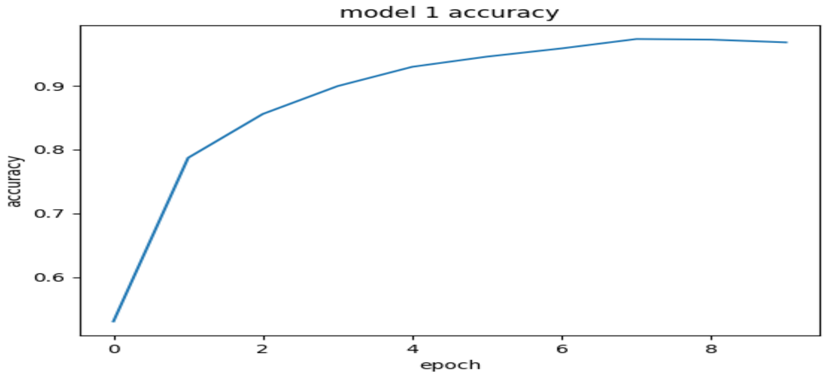

Figure. 1. shows the learning curve of accuracy of proposed model.

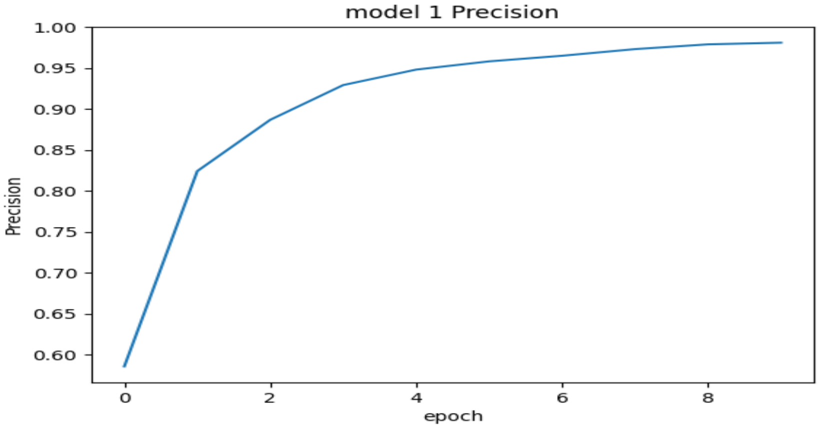

Figure 2. shows the learning curve of recall of proposed model.

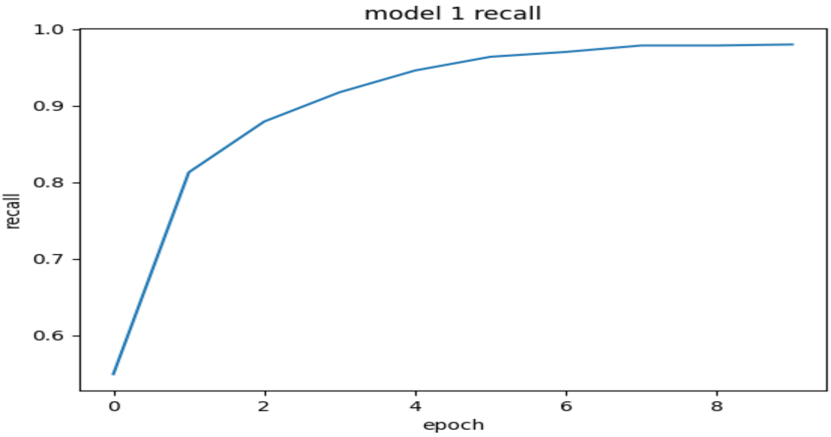

Figure 3. shows the learning curve of precision of proposed model.

5. Conclusions

Traffic classification is becoming more and more crucial as network traffic grows more sophisticated. In this paper, we suggested a CNN for traffic classification, and we assessed the model's performance using the Malimg Dataset. The suggested solution is significantly less time-consuming and more adaptable to any future development in malware because it does not involve features engineering. Network traffic classification presents both benefits and problems as deep learning advances further, and there is still much space for improvement. We anticipate that traffic classification will advance further and that we can offer a more thorough knowledge of network traffic classification based on deep learning and reference for network planning, network management, and network security.

References

1. G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescape, “Mobile Encrypted Traffic Classification Using Deep Learning,” in 2018 Network Traffic Measurement and Analysis Conference (TMA), IEEE, Jun. 2018, pp. 1–8. doi: 10.23919/TMA.2018.8506558.
2. Wei Wang, Ming Zhu, Xuewen Zeng, Xiaozhou Ye, and Yiqiang Sheng, “Malware traffic classification using convolutional neural network for representation learning,” in 2017 International Conference on Information Networking (ICOIN), IEEE, 2017, pp. 712–717. doi: 10.1109/ICOIN.2017.7899588.
3. P. Ducange, G. Mannara, F. Marcelloni, R. Pecori, and M. Vecchio, “A novel approach for internet traffic classification based on multi-objective evolutionary fuzzy classifiers,” in 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), IEEE, Jul. 2017, pp. 1–6. doi: 10.1109/FUZZ-IEEE.2017.8015662.
4. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.
5. “Network Traffic Classification Based on Deep Learning,” KSII Trans. Internet Inf. Syst., vol. 14, no. 11, Nov. 2020, doi: 10.3837/tiis.2020.11.001.
6. G. He, M. Yang, J. Luo, and X. Gu, “A novel application classification attack against Tor,” Concurr. Comput. Pract. Exp., vol. 27, no. 18, pp. 5640–5661, Dec. 2015, doi: 10.1002/cpe.3593.
7. 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. 18042–18050, 2017, doi: 10.1109/ACCESS.2017.2747560.
8. F. Ertam and E. Avcı, “A new approach for internet traffic classification: GA-WK-ELM,” Measurement, vol. 95, pp. 135–142, Jan. 2017, doi: 10.1016/j.measurement.2016.10.001.
9. P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares, and H. S. Mamede, “Machine Learning in Software Defined Networks: Data collection and traffic classification,” in 2016 IEEE 24th International Conference on Network Protocols (ICNP), IEEE, Nov. 2016, pp. 1–5. doi: 10.1109/ICNP.2016.7785327.
10. Y. Dong, J. Zhao, and J. Jin, “Novel feature selection and classification of Internet video traffic based on a hierarchical scheme,” Comput. Networks, vol. 119, pp. 102–111, Jun. 2017, doi: 10.1016/j.comnet.2017.03.019.
11. O. Avci, O. Abdeljaber, S. Kiranyaz, and D. Inman, “Structural Damage Detection in Real Time: Implementation of 1D Convolutional Neural Networks for SHM Applications,” 2017, pp. 49–54. doi: 10.1007/978-3-319-54109-9_6.
12. M. Stevanovic and J. M. Pedersen, “An analysis of network traffic classification for botnet

detection," in 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, Jun. 2015, pp. 1–8. doi: 10.1109/CyberSA.2015.7361120.

13. Y. Meidan et al., "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.

14. R.-H. Hwang, M.-C. Peng, V.-L. Nguyen, and Y.-L. Chang, "An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level," Appl. Sci., vol. 9, no. 16, p. 3414, Aug. 2019, doi: 10.3390/app9163414.

15. J. Cui, J. Long, E. Min, and Y. Mao, "WEDL-NIDS: Improving Network Intrusion Detection Using Word Embedding-Based Deep Learning Method," 2018, pp. 283–295. doi: 10.1007/978-3-030-00202-2_23.

16. V. Moussas and A. Andreatos, "Malware Detection Based on Code Visualization and Two-Level Classification," Information, vol. 12, no. 3, p. 118, Mar. 2021, doi: 10.3390/info12030118.

17. L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images," in Proceedings of the 8th International Symposium on Visualization for Cyber Security, New York, NY, USA: ACM, Jul. 2011, pp. 1–7. doi: 10.1145/2016904.2016908.

18. M. Kalash, M. Rochan, N. Mohammed, N. D. B. Bruce, Y. Wang, and F. Iqbal, "Malware Classification with Deep Convolutional Neural Networks," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, Feb. 2018, pp. 1–5. doi: 10.1109/NTMS.2018.8328749.