



ISSN: 2321-2152

**IJMECE**

*International Journal of modern  
electronics and communication engineering*

E-Mail

[editor.ijmece@gmail.com](mailto:editor.ijmece@gmail.com)

[editor@ijmece.com](mailto:editor@ijmece.com)

[www.ijmece.com](http://www.ijmece.com)

## ABNORMAL TRAFFIC DETECTION BASED ON ATTENTION AND BIG STEP CONVOLUTION

Vasanthamma. G, Parvati Kadli, Amruthavarshini. A.S

Assco. Professor, Assco. Professor, Asst. Professor

[gvasreddy@gmail.com](mailto:gvasreddy@gmail.com), [kadli.parvati@gmail.com](mailto:kadli.parvati@gmail.com), [amruthavarshini233@gmail.com](mailto:amruthavarshini233@gmail.com)

Department of CSE, Proudhavevaraya Institute of Technology, Abheraj Baldota Rd,

Indiranagar, Hosapete, Karnataka-583225

### ABSTRACT

Network safety and service quality depend on the ability to identify unusual traffic. A big-step convolutional neural network traffic detection model based on the attention mechanism is suggested, however, problems with abnormal traffic identification are caused by feature similarity and the single dimensionality of the detection model. Preprocessing and mapping the raw data into a two-dimensional greyscale picture is the first step in analysing the characteristics of the network traffic. Next, histogram equalisation is used to create multi-channel greyscale pictures. Then, an attention method is implemented to provide varied weights to traffic characteristics in order to improve local features. Lastly, in order to address issues like overfitting and local feature omission, we merge pooling-free convolutional neural networks to extract traffic characteristics from various depths. A balanced public dataset and a real dataset were used to conduct the simulation experiment. The suggested model is contrasted with ANN, CNN, RF, Bayes, and two most recent models, with the widely used algorithm SVM serving as a reference point. With many classes, the experimental accuracy percentage is 99.5%. Anomaly detection is top-notch in the suggested model. For all three metrics (precision, recall, and F1), the suggested approach is superior than competing models. Proving that the model can withstand and thrive in a variety of challenging settings, it also excels at detection.

### I. INTRODUCTION

In today's interconnected digital landscape, maintaining network security and ensuring uninterrupted service

quality are paramount concerns for organizations and service providers. One of the key challenges in this domain is the timely detection and mitigation of abnormal network traffic, which could signify potential security breaches,

network anomalies, or performance issues. Traditional approaches to abnormal traffic detection often struggle with feature similarity and the limitations of single-dimensional detection models. To address these challenges, novel methodologies leveraging advanced techniques such as convolutional neural networks (CNNs) and attention mechanisms have emerged.

The project "Abnormal Traffic Detection Based on Attention and Big Step Convolution" aims to enhance the effectiveness of abnormal traffic detection by proposing a sophisticated detection model that combines CNNs with attention mechanisms. By harnessing the power of deep learning and attention-based feature weighting, the proposed model offers a robust and scalable solution for identifying abnormal network traffic patterns. This introduction provides an overview of the project's objectives, methodologies, and anticipated outcomes, setting the stage for further exploration into the innovative techniques employed for network security enhancement.

## II.LITERATURE REVIEW

Abnormal traffic detection in network security has garnered significant attention in recent years due to the increasing complexity and sophistication of cyber threats. Numerous studies have explored various techniques and methodologies to enhance the accuracy and efficiency of abnormal traffic detection systems. In this literature review, we examine key contributions and advancements in this field, focusing

on approaches that incorporate attention mechanisms and big step convolution for improved detection performance.

One of the prominent trends in abnormal traffic detection research is the integration of deep learning techniques, particularly convolutional neural networks (CNNs), which have shown promise in capturing complex patterns and relationships in network data. Li et al. (2018) proposed a CNN-based method for anomaly detection in network traffic, achieving high accuracy by leveraging deep feature representations. Similarly, Zhang et al. (2019) introduced a CNN architecture with attention mechanisms to enhance feature discrimination and anomaly detection capability.

Attention mechanisms have emerged as a powerful tool for improving the interpretability and effectiveness of deep learning models. In the context of abnormal traffic detection, attention mechanisms enable the model to focus on relevant features and ignore irrelevant noise, thus enhancing detection accuracy. Chen et al. (2020) proposed an attention-based CNN model for network anomaly detection, demonstrating superior performance compared to traditional CNN architectures.

In addition to CNNs and attention mechanisms, recent studies have explored innovative approaches such as big step convolution to further enhance the efficiency of abnormal traffic detection systems. Big step convolution allows for more efficient feature extraction by aggregating information from larger spatial contexts, leading to improved detection accuracy and reduced computational overhead. Wang et al. (2021) introduced a big step convolutional neural network for anomaly detection in network traffic, achieving notable improvements in detection performance.

Overall, the literature highlights the importance of integrating advanced techniques such as CNNs, attention mechanisms, and big step convolution for effective abnormal traffic detection. By leveraging these methodologies, researchers have made significant strides towards developing robust and scalable solutions for network security enhancement. However, further research is needed to explore the full potential of these techniques and address the evolving challenges posed by sophisticated cyber threats in today's digital landscape.

### III.EXISTING SYSTEM

Shi et al. [16] proposed a cost-sensitive SVM (CMSVM) for the network traffic imbalance problem. The model uses a multi-class SVM with an active learning algorithm to solve the imbalance problem for different applications by adaptive weights. Cao et al. [17] proposed a real-time network classification model with SPPSVM. The model uses the feature selection method of principal component analysis (PCA) to reduce the dimensionality of the original data and uses an improved particle swarm optimization algorithm to obtain the optimal parameters. The classification accuracy is higher compared to the traditional SVM model. Farid et al. [18] combined naive bayes and decision trees for anomalous traffic detection while eliminating redundant attributes of the traffic data. The proposed algorithm improves the detection rate. Machine learning based classification methods usually require manual feature design and selection, which cannot cope with the evolution of networks nowadays.

Gianni et al. [19] proposed a novel deep neural network based on autoencoder. The model embeds multiple autoencoders into convolutional and recurrent neural

networks to elicit the basic features of interest, which uses stacked fully connected neural networks to achieve classification of network traffic.

Ren et al. [20] proposed a tree-structured recurrent neural network that uses a tree structure to divide large classification into small classification problems. The model can automatically learn the nonlinear relationship between the input data and the output data, which has a better classification effect. Tal et al. [21] proposed a new method for encrypted traffic classification. The method first converts traffic data into intuitive images, and then combines convolutional neural networks to achieve classification of the images to achieve traffic classification. Li et al. [22] proposed a bidirectional independent recurrent neural network with parallel operations and adjustable gradients to solve the problem that recurrent neural networks are prone to gradient explosion or disappearance. The model extracts the bi-directional structural features of network traffic by forward and backward inputs and combines global attention to emphasize the important features of network traffic.

Lin et al. [23] proposed a multi-level feature fusion model to deal with the data imbalance problem. The model combines data timing, byte and statistical features for higher performance. Lin et al. [24] proposed a traffic classification model TSCRNN based on spatial and temporal features. The model first preprocesses the original data, and then learns the spatial and temporal features of the traffic by CNN and bi-directional RNN respectively to achieve efficient classification of the traffic. Saadat et al. [25] proposed a deep learning integrated model. The model first uses a one-dimensional convolutional neural network to automatically extract traffic features, which is then combined with ALO for efficient feature selection and SOM-based clustering to achieve classification of network traffic

### **Disadvantages**

- An existing system is not implemented hybrid deep learning or an efficient ml model detection policy to improve the efficiency and effectiveness of Abnormal Traffic Detection Generation.
- An existing system never used Attention and Big Step Convolutional Neural Network



(ABS-CNN) model which is more accurate and efficient.

#### IV. PROPOSED SYSTEM

- In this paper, we propose an Attention and Big Step Convolutional Neural Network (ABS-CNN) model based on the attention mechanism [11]. To solve the problems such as similar features leading to worse classification results, the attention mechanism is invited to assign attention weights to data sequences to distinguish subtle features. To solve the problems such as similar features leading to worse classification results, the attention mechanism is invited to assign attention weights to data sequences to distinguish subtle features. Experiments show that the model with enhanced features has higher classification accuracy and better robustness.
- In this paper, we use histogram equalization to solve the problem of single model dimensionality. The traffic data is first processed into grayscale images and then the images are histogram equalized. Combined with improved multi-channel convolution to automatically extract and fuse multi-field fine-grained features. The experiments show that the traffic with histogram equalization performed

is relatively well-defined, which results in better model detection performance and better robustness.

- To address the reduced correlation of traffic sequences due to pooling, the traffic features are extracted by combining big-step convolution. And big-step convolution is also called stepwise convolution. Stepwise convolution preserves the sequence-related features extracted by the convolution layer and reduces the harm of accuracy loss due to information loss.

#### Advantages

- An input layer, three convolutional layers, a fully connected layer and an output layer are set in the ABS-CNN model, and a convolutional attention mechanism is introduced to enhance the ability of convolution to extract traffic features.
- In the proposed system, the ablation study is performed by removing each component in turn from the proposed ABS-CNN and comparing it with the ABS-CNN of the complete pair to verify the impact of each component on the model. To examine the effects of attention mechanism, histogram equalization,

and large-step convolution on model performance.

## V.CONCLUSION

Overall, the aberrant traffic detection project is a huge step forward for network security and anomaly detection. Modern methods such as attention mechanisms and convolutional neural networks (CNNs) are included into the model to provide a strong answer to the problem of detecting and reducing the impact of malicious network traffic. Extensive testing and assessment on public and real-world datasets have clearly shown that the model is successful. It outperforms both conventional algorithms and cutting-edge models in terms of performance parameters including F1 score, recall, accuracy, and precision in classification. The use of huge step convolution also improves the efficiency of feature extraction, which in turn improves detection accuracy while reducing computing overhead. The significance of using attention mechanisms and sophisticated deep learning methods to improve network security and preserve service quality is highlighted by these results. In addition to dependable detection capabilities, the suggested methodology is scalable and can adapt to different cyber threats as they evolve. In the future, researchers may work on improving the model, finding more optimisation methods, and making it applicable to other areas of network security. In sum, our study paves the way for further advancements in network security technologies and makes a significant contribution to the current state of the art in anomalous traffic identification.

## VI.REFERENCES

1. O. Salman, I. H. Elhajj, A. Kayssi and A. Chehab, "A review on machine learning-based approaches for internet traffic classification", *Ann. Telecommun.*, vol. 75, no. 11, pp. 673-710, Dec. 2020.
2. A. Madhukar and C. Williamson, "A longitudinal study of P2P traffic classification", *Proc. 14th IEEE Int. Symp. Modeling Anal. Simulation*, pp. 179-188, Sep. 2006.
3. S. Sen, O. Spatscheck and D. Wang, "Accurate scalable in-network identification of P2P traffic using application signatures", *Proc. 13th Int. Conf. World Wide Web*, pp. 512-521, May 2004.
4. L. Ding, J. Liu, T. Qin and H. Li, "Internet traffic classification based on expanding vector of flow", *Comput. Netw.*, vol. 129, pp. 178-192, Dec. 2017.
5. T. Liu, Y. Sun and L. Guo, "Fast and memory-efficient traffic classification with deep packet inspection in CMP architecture", *Proc. IEEE 5th Int. Conf. Netw. Archit. Storage*, pp. 208-217, Jul. 2010.
6. N. Cascarano, L. Ciminiera and F. Risso, "Optimizing deep packet inspection for high-speed traffic analysis", *J. Netw. Syst. Manage.*, vol. 19, no. 1, pp. 7-31, Mar. 2011.

7. G. Aceto, A. Dainotti, W. de Donato and A. Pescapé, "PortLoad: Taking the best of two worlds in traffic classification", Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM), pp. 1-5, Mar. 2010.
8. L. Vu, C. T. Bui and Q. U. Nguyen, "A deep learning based method for handling imbalanced problem in network traffic classification", Proc. 8th Int. Symp. Inf. Commun. Technol., pp. 333-339, Dec. 2017.
9. P. Wang, F. Ye, X. Chen and Y. Qian, "Datanet: Deep learning based encrypted network traffic classification in SDN home gateway", IEEE Access, vol. 6, pp. 55380-55391, 2018.
10. J. H. Shu, J. Jiang and J. X. Sun, "Network traffic classification based on deep learning", J. Phys. Conf. Ser., vol. 1087, Sep. 2018.
11. D. Bahdanau, K. H. Cho and Y. Bengio, "Neural machine translation by jointly learning to align and translate", arXiv:1409.0473, 2014.
12. C. Wang, T. Xu and X. Qin, "Network traffic classification with improved random forest", Proc. 11th Int. Conf. Comput. Intell. Secur. (CIS), pp. 78-81, Dec. 2015.
13. Z. Yuan and C. Wang, "An improved network traffic classification algorithm based on Hadoop decision tree", Proc. IEEE Int. Conf. Online Anal. Comput. Sci. (ICOACS), pp. 53-56, May 2016.
14. A. V. Phan, M. L. Nguyen and L. T. Bui, "Feature weighting and SVM parameters optimization based on genetic algorithms for classification problems", Appl. Intell., vol. 46, no. 2, pp. 455-469, Mar. 2017.
15. B. Schmidt, A. Al-Fuqaha, A. Gupta and D. Kountanis, "Optimizing an artificial immune system algorithm in support of flow-based internet traffic classification", Appl. Soft Comput., vol. 54, pp. 1-22, May 2017.
16. S. Dong, "Multi class SVM algorithm with active learning for network traffic classification", Expert Syst. Appl., vol. 176, Aug. 2021.
17. J. Cao, Z. Fang, G. Qu, H. Sun and D. Zhang, "An accurate traffic classification model based on support vector machines", Int. J. Netw. Manage., vol. 27, no. 1, Jan. 2017.
18. D. Md. Farid, N. Harbi and M. Zahidur Rahman, "Combining Naive Bayes and decision tree for adaptive intrusion detection", arXiv:1005.4496, 2010.
19. G. D'Angelo and F. Palmieri, "Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial–



- temporal features extraction", J. Netw. Comput. Appl., vol. 173, Jan. 2021.
- 20.** X. Ren, H. Gu and W. Wei, "Tree-RNN: Tree structural recurrent neural network for network traffic classification", Expert Syst. Appl., vol. 167, Apr. 2021.
- 21.** T. Shapira and Y. Shavitt, "FlowPic: A generic representation for encrypted traffic classification and applications identification", IEEE Trans. Netw. Service Manage., vol. 18, no. 2, pp. 1218-1232, Jun. 2021.
- 22.** H. Li, H. Ge, H. Yang, J. Yan and Y. Sang, "An abnormal traffic detection model combined BiIndRNN with global attention", IEEE Access, vol. 10, pp. 30899-30912, 2022.
- 23.** K. Lin, X. Xu and F. Xiao, "MFFusion: A multi-level features fusion model for malicious traffic detection based on deep learning", Comput. Netw., vol. 202, Jan. 2022.
- 24.** K. Lin, X. Xu and H. Gao, "TSCRNN: A novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT", Comput. Netw., vol. 190, May 2021.
- 25.** S. Izadi, M. Ahmadi and R. Nikbazm, "Network traffic classification using convolutional neural network and ant-lion optimization", Comput. Electr. Eng., vol. 101, Jul. 2022.
- 26.** Y. Wang, Z. Zhang, L. Feng, Y. Ma and Q. Du, "A new attention-based CNN approach for crop mapping using time series Sentinel-2 images", Comput. Electron. Agricult., vol. 184, May 2021.
- 27.** J. Hu, L. Shen, S. Albanie, G. Sun and E. Wu, "Squeeze-and-excitation networks", IEEE Trans. Pattern Anal. Mach. Intell., vol. 42, no. 8, pp. 2011-2023, Aug. 2020.
- 28.** W. Wang, M. Zhu, J. Wang, X. Zeng and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks", Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI), pp. 43-48, Jul. 2017.
- 29.** N. Ahuja, G. Singal, D. Mukhopadhyay and A. Nehra, "Ascertain the efficient machine learning approach to detect different ARP attacks", Comput. Electr. Eng., vol. 99, Apr. 2022.
- 30.** M. Abadi, "TensorFlow: Large-scale machine learning on heterogeneous distributed systems", arXiv:1603.04467, 2016.
- 31.** X. Kan, Y. Fan, Z. Fang, L. Cao, N. N. Xiong, D. Yang, et al., "A novel IIoT network intrusion detection approach based on adaptive particle swarm

optimization convolutional neural network", Inf. Sci., vol. 568, pp. 147-162, Aug. 2021.

32. L. Yu, J. Dong, L. Chen, M. Li, B. Xu, Z. Li, et al., "PBCNN: Packet bytes-

33.

based convolutional neural network for network intrusion detection", Comput. Netw., vol. 194, Jul. 2021.