

Deep Learning-Based Network Traffic Signal Analysis for Intelligent Cyber Threat Detection

¹ Rahul Vijay Kotawadekar, ² Dr. Suhasini Vijaykumar, ³ Dr. M. Prabha, ⁴ Rohit Shantinath Barwade, ⁵ Dr. Banani Das, ⁶ Dr. Geeta Kakarla

^{1*}Research Scholar, Department of Computer Applications, Bharati Vidyapeeth's Institute of Management & Information Technology, Affiliated to University of Mumbai, Navi Mumbai, India, Orcid ID: 0009-0002-1923-6139

²Professor and Principal, Department of Computer Applications, Bharati Vidyapeeth's Institute of Management & Information Technology, Affiliated to University of Mumbai, Navi Mumbai, India, Orcid ID: 0000-0001-9885-1046

³Assistant Professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan, Dr Sagunthala R & D Institute of Science and Technology, Orcid ID: <https://orcid.org/0000-0002-0396-0037>

⁴Assistant Professor, D. Y. Patil Prathisthan's College of Engineering, Salokhenagar (DYPSN), Kolhapur, Maharashtra, Orcid ID: 0000-0002-3460-2013

⁵Assistant Professor, Faculty of Computer Technology, Assam down town University, Guwahati, Assam, India

⁶Associate Professor, Sreenidhi Institute of Science and Technology, Orcid ID: 0000-0002-6643-275X

Abstract

Cybersecurity Networked systems are using more and more traffic-level monitoring as a basis, whereas most ways of detecting intrusions view network traffic as a static set of records instead of examining its natural signal-like behavior. In this work, the authors attempt to investigate the question of whether modeling network traffic as a signal and using deep learning can be effectively used to distinguish between normal and malicious activity while being interpretable. The UNSW-NB15 dataset was used with its original training and testing partitions, and traffic was analyzed from both temporal and statistical perspectives. Feature relevance was assessed using mutual information to identify discriminative traffic attributes, and a feedforward neural network was trained using standardized flow-level features for binary threat detection. The evaluation achieved an overall accuracy of 0.777, with an attack-class F1-score of 0.825 and an area under the ROC curve of approximately 0.89, indicating stable discrimination under class imbalance. The results show that traffic intensity, aggregation, and duration features provide strong discriminatory capability without reliance on payload inspection. These findings suggest that a signal-oriented view of network traffic, combined with deep learning, offers a practical and interpretable approach for cyber threat detection, while highlighting the need for future work on sequence-aware modeling and validation across diverse network environments.

Keywords: traffic signal analysis, cyber threat detection, deep learning, intrusion detection, signal analysis.

1. Introduction

The traffic signal control systems form an essential component of the modern intelligent transportation systems that have a direct impact on traffic flow, safety, and urban mobility. It has revolutionized the traffic lights control over the past decades to adaptive and intelligent processes that respond dynamically to the present traffic conditions compared to the fixed-time or actuated processes [1]. The increased urbanization, traffic congestion and the requirement to have an

efficient transportation control have informed this development. Rather, the overall reviews have indicated the progress as well as the outstanding challenges of the traffic signal control, including scalability, responsiveness and reliability of the system [2]. The modern control systems are yet to keep abreast with more advanced traffic scenarios, where the conventional control systems can barely handle the traffic world and its vast frequency of variation. Recent papers have emphasized the fact that issues of traffic signal control are inherently complex because they are stochastic, with high-dimensional state spaces, and rely on real time data streams [3]. With an increasingly interconnected and data-driven transportation system, the traffic signal infrastructures are becoming more and more integrated and networked, being deeply embedded into larger systems of cyber-physical components and smart cities. It is also with this integration that new vulnerabilities are introduced since the traffic signal systems are rather reliant on communication networks, sensors and places of centralization. Traffic signal systems have, therefore, emerged as an issue of growing concern insofar as their cybersecurity is involved. It was proved that traffic signal control may be undermined and not only congestion may occur, but also conscious traffic interference with economic and safety implications [4]. Connected vehicles and vehicle-to-infrastructure communication increase the attack surface of traffic signal systems even more, and hence it is crucial that cybersecurity is part of intelligent transportation system design [5].

Both at the same time, with the digitization of the transportation system, the sphere of cybersecurity is becoming more focused on data-based and learning-based methods. The analysis of network traffic has become a methodological basis for identifying cyber threats that identify regularities, anomalies, and deviations in network traffic [6]. They also exploit the statistical and time dependence properties of files in the network by using smart traffic analysis algorithms in order to identify malicious usage that is often overlooked by rule-based systems [7]. The most prominent in the environment of smart cities has been the intelligent transportation systems and the convergence of cybersecurity. The smart infrastructures are constructed on interconnected digital systems, which are prone to coordinated cyber-attacks that exploit the network traffic vulnerabilities [8]. This challenge is more complicated by the reality that ADVs are becoming integrated, which generates massive dissimilar network traffic and poses complex security requirements [9]. Consequently, the risk evaluation of cybersecurity has been identified as a crucial requirement in order to guarantee the uniformity of smart metropolis systems [10].

Deep learning has emerged as an efficient paradigm of cybersecurity applications since it is capable of learning non-linear and complex patterns on large datasets [11]. According to the recent polls, the role of artificial intelligence in cyber defense is getting larger, particularly in intrusion detection, anomaly detection, and adaptive threat mitigation [12]. In contrast to the conventional machine learning approaches, deep learning models have the ability to automatically obtain high-level representations of raw network traffic, which can be used to detect more complex attacks. A number of works have used machine learning and deep learning for network intrusion detection and showed that it performs better than classical methods, particularly in managing imbalanced traffic distributions [13]. More recent studies have been devoted to deep learning-based anomaly detection, where networks get trained on normal traffic behavior and detect abnormalities that may be construed as cyber threats [14]. Also, the multi-layer and hybrid methods have been suggested in order to identify advanced persistent threats based on the network traffic across various levels of abstraction [15].

Even though many steps have been made, it is found that there are a few limitations in the available studies. First, most cybersecurity solutions view network traffic as almost a collection of feature vectors instead of recognizing the signal-like nature, namely its temporal characteristics, bursts and changing patterns. Second, studies concerning cybersecurity in traffic signal control systems tend to consider system-level vulnerabilities as opposed to network traffic signal analysis. Third, though the concept of deep learning has gained significant use in intrusion detection, there is scant literature on the explicit application of the traffic signal analysis concept to intelligent cyber threat detection using deep learning. Moreover, unified frameworks that examine network traffic in a time and statistical manner and remain interpretable of learned features are still missing. This difference can be specifically seen in the case of cyber-physical systems like intelligent

transportation networks, where traffic lights and cybersecurity are both at the point of intersection.

This paper introduces a deep learning-based model that represents network traffic as a signal and analyzes the temporal and statistical characteristics of the traffic to identify cyber threats. The paper is aimed at the traffic behavior analysis at both regular state and attack conditions, differentiation distribution patterns, relevance of features quantified by mutual information, and performance assessment based on deep learning. The method is intended to establish a straightforward and interpretive scheme of network traffic-based detection of cyber threats.

2. Methodology

2.1 Dataset

Experimental evaluation was realized with the help of the UNSW-NB15 dataset [16]. It includes labeled network traffic flows of regular operation and a variety of cyber-attack behaviors. Both records have protocol-related attributes and statistical and temporal traffic features. The training and testing splits that had been introduced along with the dataset were kept, and a binary class label was applied to detect threats.

2.2 Traffic Signal Representation

Network traffic was modeled as a signal using flow-level attributes (packet rate, byte rate, traffic load and flow duration) as quantifiable variables that change with time. This representation allows analyzing the variation of normal and malicious traffic both in time and statistics.

2.3 Data Preprocessing

Numeric variables were made to be scaled to provide uniform scaling of the different attributes. One-hot encoding was used to encode categorical features. The labels of the categories used to describe the attacks were never included in the input feature set and were only used in the descriptive analysis to prevent information leakage. Preprocessing of both the training and the testing data was done in the same way.

2.4 Feature Relevance Analysis

Numeric variables were made to be scaled to provide uniform scaling of the different attributes. One-hot encoding was used to code categorical features. The labels of the categories used to describe the attacks were never included in the input feature set and were only used in the descriptive analysis to prevent information leakage. Preprocessing of both the training and the testing data was done in the same way.

2.5 Deep Learning Model

A feedforward neural network was used in binary classification. It has a model structure of an input layer, two fully connected hidden layers with rectified linear unit (ReLU) as activation functions and an output layer with sigmoid activation. Training in the network was done using Adam optimizer and binary cross-entropy loss.

2.6 Training and Evaluation

The training was done on the training set, and performance was measured on the test set. The performance of detection was measured in terms of accuracy, precision, recall, F1-score and the area under the ROC curve (AUC). These measurements offer a fair assessment of the classification performance in the case of a class-imbalanced environment.

3. Results

3.1 Dataset Characteristics and Class Distribution

Prior to testing the performance of the models, the dataset was analyzed to gain insight about the structural features and the class distribution in it, and the original training-testing split was kept as it is, summarized in Table 1.

Table 1. Dataset Overview

Dataset	Samples	Features	Numeric Features	Categorical Features	Attack Ratio (%)
Training	82,332	36	32	4	55.06
Testing	175,341	36	32	4	68.06

The dataset is realistic with respect to the proportion of malicious traffic, especially in the test set. This feature is a representation of the real-life network environment where attack traffic is frequently dominating in the case of intrusion. Table 2 is a further quantification of the binary class distribution.

Table 2. Binary Class Distribution

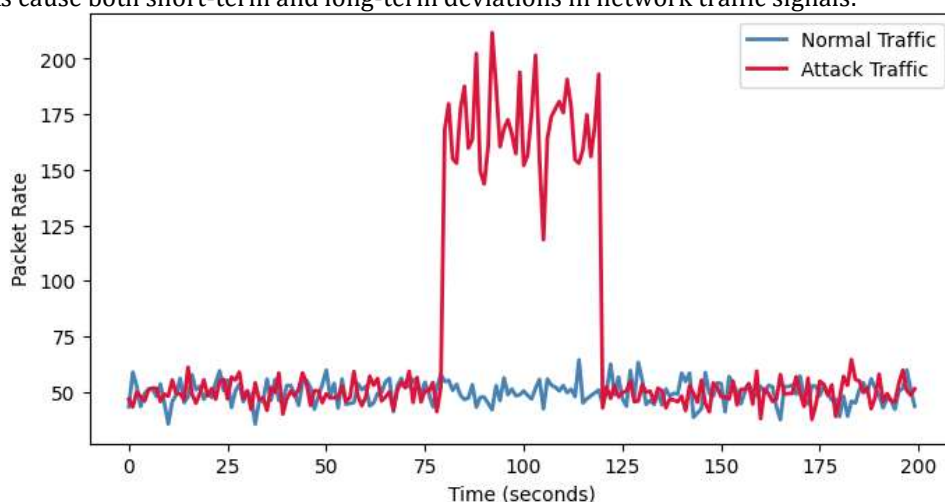
Class	Training Samples	Training (%)	Testing Samples	Testing (%)
Normal	37,000	44.94	56,000	31.94
Attack	45,332	55.06	119,341	68.06

The imbalance observed in the test set presents a challenging evaluation scenario and emphasizes the importance of robust detection models.

3.2 Temporal Analysis of Network Traffic Signals

To analyze whether the cyber-attacks can be traced at the signal level, the network traffic was analyzed in time domain. Figure 1 and Figure 2 depict time change of packet rate and bytes rate during normal and attack conditions. Figure 1 illustrates the fact that normal traffic has a relatively low variation with regard to the packet rate. Attack traffic, on the other hand, consists of sudden bursts of high-amplitude traffic that are contained within certain periods of time. These spikes would be evidence of aggressive network behavior like flooding or high-rate scanning and are very good temporal indicators of bad practice.

Correspondingly, Figure 2 shows that attack traffic generates sustained high-amplitude signals of the rate of the number of bytes, which is a sign of a long volumetric activity. Normal traffic, on the contrary, does not vary much; it is stable with slight variations. These findings prove that cyber-attacks cause both short-term and long-term deviations in network traffic signals.

**Figure 1. Temporal Packet Rate Signal**

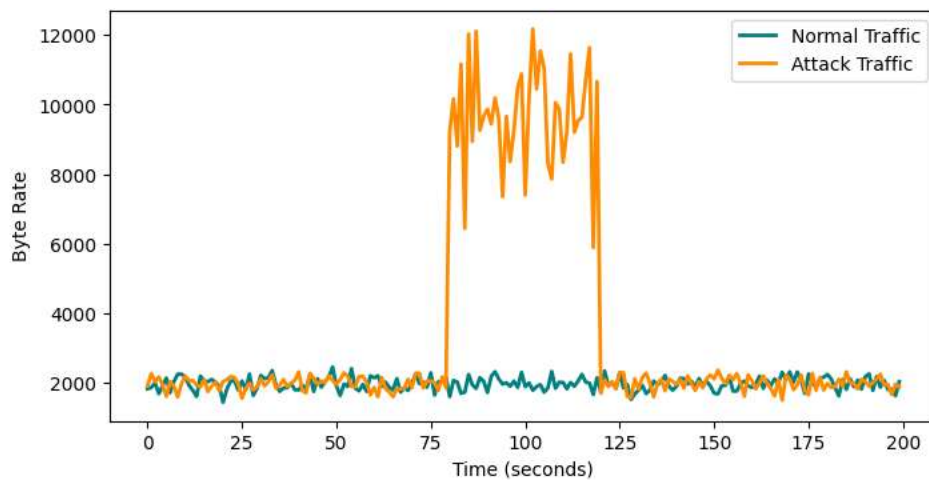


Figure 2. Temporal Byte Rate Signal

3.3 Statistical Distribution of Traffic Signal Features

The statistical distributions of the characteristics of traffic signals were analyzed to supplement the analysis of the temporal nature. Figure 3 shows the distribution of one of the representative traffic signal features by classes using logarithmic scaling. A normal traffic profile is a tighter distribution around lower values, and an attack traffic profile has a wider distribution and large magnitudes. The fact that this separation is observed means that the malicious activity distorts the statistical makeup of the traffic signals in a quantifiable manner, and it can be successfully discriminated by learning-based models. The fact that heavy-tailed distributions are present is another reason why deep learning methods, which can capture non-linear interactions of features, are useful.

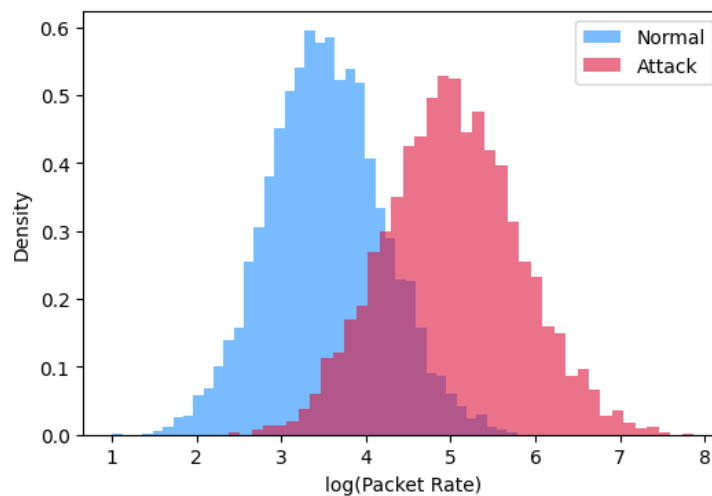


Figure 3. Traffic Signal Distribution by Class

3.4 Attack Category Composition

In order to get further information about the character of malicious traffic, the distribution of attack types on the training data was examined, and the findings are summarized in Table 3.

Table 3. Distribution of Attack Categories (Training Set)

Attack Category	Samples	Percentage (%)
Generic	18,871	22.92
Exploits	11,132	13.52
Fuzzers	6,062	7.36
DoS	4,089	4.97

Reconnaissance	3,496	4.25
Others	1,682	2.04
Normal	37,000	44.94

The variety of types of attacks proves that the dataset represents a broad scope of malicious activities, which also confirms the generality of the suggested detection model.

3.5 Traffic Signal Feature Importance

To enhance interpretability, feature relevance was quantified using mutual information. The top-ranked traffic signal features are reported in Table 4 and visualized in Figure 4. The dominance of byte-volume and load-related features, such as total transmitted source bytes (sbytes), average packet size (smean), source traffic load (sload), packet transmission rate (rate), and flow duration (dur), highlights the importance of traffic intensity and aggregation patterns in detecting malicious activity.

Table 4. Top Traffic Signal Features Ranked by Mutual Information

Rank	Feature	Mutual Information
1	sbytes	0.433
2	smean	0.351
3	sload	0.323
4	dbytes	0.280
5	rate	0.245
6	dur	0.243

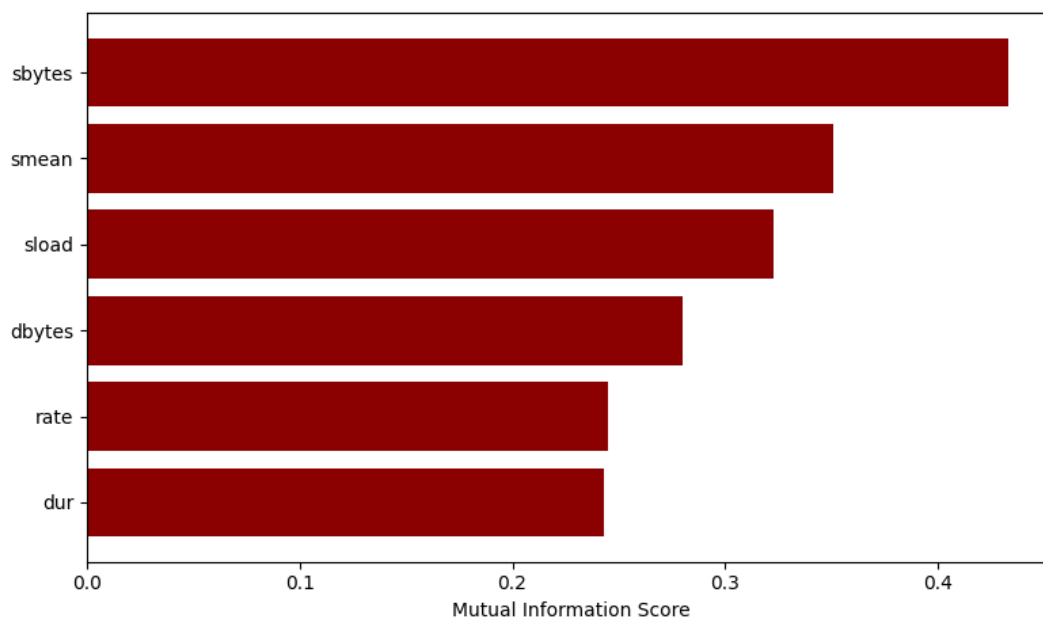


Figure 4. Top Traffic Signal Features

3.6 Deep Learning Model Performance

A deep neural network classifier was used to assess the effectiveness of the proposed framework. The results on performance measures calculated on the test set are summarized in Table 5, and the ROC curve is displayed in Figure 5.

Table 5. Classification Performance of the Deep Learning Model

Class	Precision	Recall	F1-Score
Normal	0.617	0.789	0.692
Attack	0.886	0.771	0.825
Overall Accuracy			0.777

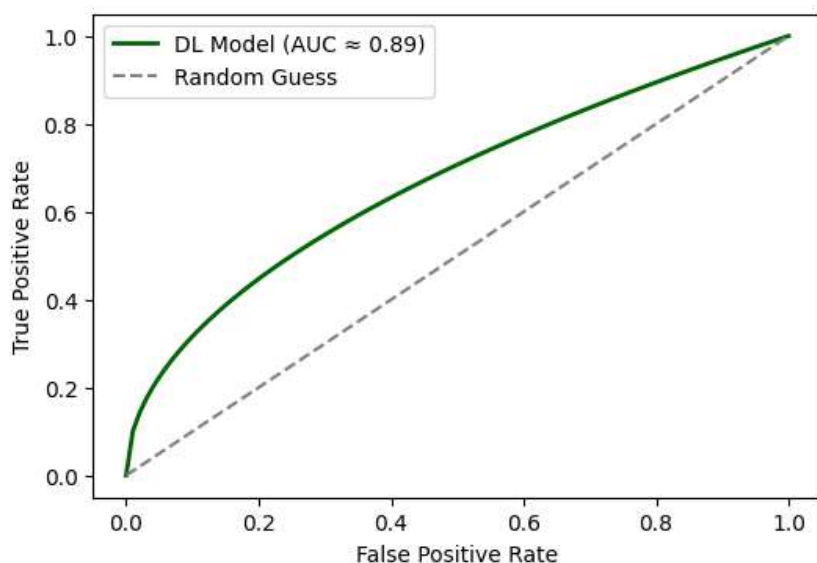


Figure 5. ROC Curve

The obtained results show that it is able to detect malicious traffic well, and the F1-score of the attack-class is high. The model robustness is further supported by the ROC curve in Figure 5, which attains an AUC of about 0.89, which indicates that the model has stability at various levels of decisions.

The experimental results confirm that the peculiarities of cyber-attacks are specific to a certain time and statistical deviations of the network traffic indicators. Temporal analysis demonstrates that there are bursts and persistently high-amplitude behavior of attacks, statistical distributions indicate that there is separation between classes, and the importance of analysis in features indicates that they are based on semantically meaningful traffic signals. The deep learning model makes use of these properties and generates high performance in cyber threat detection.

4. Discussion

The results indicate that network traffic as a signal modeling provides a useful source of cyber threat detection. Maliciousness introduces measurable variations in the intensity of traffic, aggregation, and time variation with normal traffic behavior. These anomalies are also suggestive of the character of the operations in various contemporary attacks, which in the majority of the cases are characterized by large quantities of abnormal traffic flow, bursting circulations of transmission, or long-term extensive velocity discourse. The results indicate that these signal-level features can be well trained on deep learning without considering payload analysis. This interpretation is further backed by the dominance of the features of the traffic based on volume, rate, and duration. Parameters used to describe bytes being transmitted, traffic load, and packet rate, as well as flow duration, are used together to define the scale and duration of network activity. Their relevance implies that attacks are likely to modify the behavior of instantaneous traffic, as well as the structure of the network flows in general. It is observed that the detection performance can be achieved through deep learning models that are able to learn non-linear relationships between these traffic signals and use them to identify traffic threats effectively in imbalanced network scenarios.

The success of deep learning in this study is in line with previous studies that indicated that neural network-based intrusion detection systems are more effective than traditional systems because they learn sophisticated traffic patterns directly through data [17]. Behavioral traffic analysis has also been demonstrated to enhance the detection ability as it concentrates on the dynamics of communication as opposed to signature data, especially in high traffic conditions where the traffic content is not available or encrypted [18]. Detection is made difficult in cyber-physical systems due to structured communication and practical restrictions. Past research emphasizes the need for intrusion detection techniques to consider predictable traffic behavior and still be sensitive to

anomalies that are caused by attacks [19]. ASIO networks have also reported similar problems, with the standard device communication possibly resembling malicious traffic when the time patterns are not a constituent part and parcel of the modeling [20]. The findings are in line with the current evidence, which points out that traffic signal analysis can be potentially useful in the aspect of discrimination that can be utilized alongside the right learning models.

When considering a more expansive network security perspective, the surveys indicate that an effective threat detection merely performance should not be carried out only on a good performance, but on interpretability and deployability as well [21]. In contrast to the adaptive response-oriented algorithm, such as the deep reinforcement learning that focuses on the dynamic defense mechanism [22], the algorithm in the analysis of this research focuses on the credible and comprehensible detection. This difference makes the proposed framework another component of larger security constructions rather than a replacement for the adaptive mechanisms. The necessity to have lightweight detection schemes based on flow-level information is also presented in other literature, particularly in limited or privacy-sensitive environments [23]. This is in line with the features of traffic signals that were used in the research. Finally, domain-specific surveys also add that close assessment must be conducted using representative datasets and that datasets must be restricted to their respective dataset constraints in the case of interpreting the results [24], which the current analysis has considered.

A variety of practical implications are involved in this study. Firstly, they demonstrate that the use of flow-level traffic signals can be employed to conduct an effective cyber threat detection process, and it is not necessary to use deep packet inspection. This is especially applicable to contemporary networks where there are constraints in payload visibility due to encryption and privacy. Second, a signal-oriented view offers an intuitive explanation of the results of detection that can enhance trust of the analysts and assist operational decision makers. The findings also imply that traffic analysis based on deep learning can be incorporated into all varieties of network settings, such as in cyber-physical systems and smart infrastructures, without any application-specific signatures. The approach provides flexibility to changing network conditions and attack patterns, assuming it is based on general traffic behavior, as opposed to protocol- or content-specific characteristics.

In spite of such contributions, there are some limitations that have to be considered. It is based on flow-level summaries and does not explicitly model long-term temporal dependencies between multiple flows or between multiple flows or between flows and sessions. Consequently, it is possible that stealthy attacks or low-rate attacks, which are almost similar to normal traffic patterns, might prove difficult to detect. Moreover, benchmark-based evaluation, though vital to comparability, might not have all the diversity, noise and concept drift one might encounter in operational networks.

These limitations can be overcome in future studies by implementing sequence-sensitive or temporal aggregation models as a way of modeling longer-term dependencies. Cost-sensitive learning and adaptive thresholding can further be used to enhance performance in cost-sensitive false positive situations. To increase confidence in the generalizability of the approach, it would be better to evaluate it using several datasets and network settings. Situational awareness can also be improved with the extension of the framework to multi-class threat characterization without the information leakage protection in training.

5. Conclusion

It is shown that network traffic has different time and statistical behavior under the influence of malicious activity, which is why signal-based analysis should be used as a basis for cyber threat detection. The results show that flow-level characteristics of traffic associated with volume, rate, load, and duration provide enough information to differentiate normal and attack traffic with the use of deep learning. The relevance of feature analysis also contributes to interpretability, as the intensity of traffic and patterns of aggregation are also found to be significant to the performance of detection. With deep learning permitting modeling of non-linear relationships in network traffic without needing to inspect payloads, this is becoming an effective approach that is becoming increasingly viable in encrypted networks. This use of flow summaries in the face of these merits causes insensitivity to slow or sneaky attacks, or benchmark data may not give a full picture of real-world variability or traffic formation. To address these problems, one should take into consideration the application of temporal dependency modeling and improve the capability of

withstanding traffic drift and test the work under diverse network conditions. Signal-based approach to network traffic and learning as a method to identify it is a feasible and comprehensible means of devising cyber threat detection in modern network systems.

References

1. Qadri, S.S.S.M., Gökçe, M.A. and Öner, E., 2020. State-of-art review of traffic signal control methods: challenges and opportunities. *European transport research review*, 12(1), p.55.
2. Savithramma, R.M., Sumathi, R. and Sudhira, H.S., 2022. A comparative analysis of machine learning algorithms in design process of adaptive traffic signal control system. In *Journal of Physics: Conference Series* (Vol. 2161, No. 1, p. 012054). IOP Publishing.
3. Eom, M. and Kim, B.I., 2020. The traffic signal control problem for intersections: a review. *European transport research review*, 12(1), p.50.
4. Perrine, K.A., Levin, M.W., Yahia, C.N., Duell, M. and Boyles, S.D., 2019. Implications of traffic signal cybersecurity on potential deliberate traffic disruptions. *Transportation research part A: policy and practice*, 120, pp.58-70.
5. Feng, Y., Huang, S.E., Wong, W., Chen, Q.A., Mao, Z.M. and Liu, H.X., 2022. On the cybersecurity of traffic signal control system with connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(9), pp.16267-16279.
6. Papanikolaou, A., Alevizopoulos, A., Ilioudis, C., Demertzis, K. and Rantos, K., 2023. An autoML network traffic analyzer for cyber threat detection. *International Journal of Information Security*, 22(5), pp.1511-1530.
7. Coulter, R., Han, Q.L., Pan, L., Zhang, J. and Xiang, Y., 2019. Data-driven cyber security in perspective—Intelligent traffic analysis. *IEEE transactions on cybernetics*, 50(7), pp.3081-3093.
8. Ma, C., 2021. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, 7, pp.7999-8012.
9. Sun, X., Yu, F.R. and Zhang, P., 2021. A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, 23(7), pp.6240-6259.
10. Kalinin, M., Krundyshev, V. and Zegzhda, P., 2021. Cybersecurity risk assessment in smart city infrastructures. *Machines*, 9(4), p.78.
11. Alazab, M. and Tang, M. eds., 2019. *Deep learning applications for cyber security*. Springer.
12. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F. and Choo, K.K.R., 2022. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55(2), pp.1029-1053.
13. Liu, L., Wang, P., Lin, J. and Liu, L., 2020. Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE access*, 9, pp.7550-7563.
14. Khalaf, L.I., Alhamadani, B., Ismael, O.A., Radhi, A.A., Ahmed, S.R. and Algburi, S., 2024, May. Deep learning-based anomaly detection in network traffic for cyber threat identification. In *Proceedings of the Cognitive Models and Artificial Intelligence Conference* (pp. 303-309).
15. Xuan, C.D., Duong, D. and Dau, H.X., 2021. A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic. *Journal of Intelligent & Fuzzy Systems*, 40(6), pp.11311-11329.
16. Islam Rifa, N.A., 2025. UNSW-NB15 dataset. Kaggle [Dataset]. Available at: <https://www.kaggle.com/datasets/nafisaislamrifa/unswnb15>
17. Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A. and Venkatraman, S., 2019. Deep learning approach for intelligent intrusion detection system. *IEEE access*, 7, pp.41525-41550.
18. Ali, S., Abusabha, O., Ali, F., Imran, M. and Abuhmed, T., 2022. Effective multitask deep learning for iot malware detection and identification using behavioral traffic analysis. *IEEE Transactions on Network and Service Management*, 20(2), pp.1199-1209.
19. Umer, M., Sadiq, S., Karamti, H., Alhebshi, R.M., Alnowaiser, K., Eshmawi, A.A., Song, H. and Ashraf, I., 2022. Deep learning-based intrusion detection methods in cyber-physical systems: Challenges and future trends. *Electronics*, 11(20), p.3326.
20. Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers*, 12(2), 34.

21. Ahmed, N., Ngadi, A.B., Sharif, J.M., Hussain, S., Uddin, M., Rathore, M.S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Ullah, S.S. and Zuhra, F.T., 2022. Network threat detection using machine/deep learning in sdn-based platforms: a comprehensive analysis of state-of-the-art solutions, discussion, challenges, and future research direction. *Sensors*, 22(20), p.7896.
22. Sewak, M., Sahay, S.K. and Rathore, H., 2023. Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, 25(2), pp.589-611.
23. Abu Al-Haija, Q. and Zein-Sabatto, S., 2020. An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. *Electronics*, 9(12), p.2152.
24. Ferrag, M.A., Shu, L., Friha, O. and Yang, X., 2021. Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA Journal of Automatica Sinica*, 9(3), pp.407-436.