IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 4, Ser. 2 (Jul. – Aug. 2024), PP 23-29
www.iosrjournals.org

Network Traffic Classification Schemes: A Review

[1]Abhishek Kumar Dubey*, [2]Arvind Kumar Jain, [3]Dharmendra Narayan Jha, [4]Abhijit Dwivedi, [5]Anuj Kumar Pal, [6]Rohit Bansal

[1]Assistant Professor, Department of Computer Science and Engineering-Internet of Things, Sagar Institute of Science,Technology & Engineering, Bhopal, (M.P.) India
[2-6]Assistant Professor, Department of Computer Science & Engineering, Sagar Institute of Science,Technology & Research, Bhopal, (M.P.) India
**Corresponding Author: information.dubey.abhishek@gmail.com*

Abstract
The major purpose of technique of classifying the network traffic is to identify various kinds of applications or traffic data. The analysis of received data packets is performed due to its necessity in communication networks nowadays. There are diverse phases to classify the network traffic such as to pre-process the data, extract the attributes and perform the classification. The dataset is utilized for the input in the classification stage. This paper studies diverse ML techniques in order to classify the network traffic.

Keywords
Network Traffic, Machine learning, Feature Extraction

Date of Submission: 02-07-2024 Date of Acceptance: 12-07-2024

I. Introduction

Network traffic classification is the process of identifying specific applications or activities within network traffic, which is essential for effective network management and security. This technique is foundational for recognizing various applications and protocols within a network, allowing for tasks such as prioritizing different applications based on available bandwidth in Quality of Service (QoS) control methods [1]. Both industry and academia have devoted significant attention to traffic classification over the past decade, with techniques typically falling into categories such as payload-based, port-based, and flow statistics-based methods. The traditional port-based method relies on inspecting commonly used ports associated with popular programs. However, its reliability is compromised because not all modern applications adhere to standard ports, and some may even use established ports of other programs to hide their identity. To overcome this limitation, the payload-based approach offers a solution by searching for the application's signature within the payload of IP packets, making it more adaptable to contemporary applications. However, this approach often falls short with encrypted traffic [2]. In recent academic research, there has been substantial interest in applying machine learning techniques to the flow statistics-based approach. Unlike deep packet inspection (DPI), the statistical approach doesn't require examining the packet contents and relies solely on flow statistical data, such as interpacket time. This method has garnered attention as an alternative that can be effective even in the absence of DPI, presenting a promising direction for traffic classification.

1.1 Machine Learning in Network Traffic Classification

The proliferation of network applications has drastically expanded today's networks, creating a vast and complex system [3]. This growth brings significant management challenges, underscoring the need for intelligent traffic analysis-based network management. Network traffic classification plays a crucial role in this management, enabling the differentiated handling of various network traffic types and serving as the basis for developing subsequent network protocols. Additionally, it aids in identifying network attacks and managing flow in network security. Machine learning techniques are instrumental in identifying and analyzing traffic data packets by examining the statistical characteristics of specific application traffic. Two primary types of machine learning techniques exist: supervised and unsupervised learning. In unsupervised learning, the classifier does not pre-label the training set; instead, it forms clusters based on sample similarities. Representative clustering techniques include expectation-maximization (EM) and K-means clustering. Conversely, supervised learning, which is aware of the actual traffic categories [4], proves advantageous for constructing application-oriented network traffic classification models. In supervised learning, classification models and parameters are developed based on historical data. Methods such as Bayesian, C4.5 decision trees, and K-NN are utilized, employing classifiers or

classification models grounded in pattern recognition approaches, though they may encounter local optimization challenges.

On the other hand, ensemble learning is a technique that combines multiple simple classifiers to make collective decisions. Common basic classifiers include Bayesian models, random forests, and decision trees [5]. However, the effectiveness of ensemble learning algorithms and their ability to generalize can be significantly influenced by dependencies between the fundamental classifiers and the number of basic classifiers involved. Deep learning, characterized by its reliance on learning from data, utilizes neural networks with multiple layers for pattern recognition and feature extraction. While deep learning requires a substantial amount of training data for optimal performance, fine-tuning the hyperparameters of deep neural networks poses a challenging task.

1.2 Machine Learning based Network Traffic Classification Model

To overcome the limitations of traditional traffic classification methods, there has been a recent surge in the popularity of machine learning (ML)-based approaches [6]. These methods operate under the premise that different types of protocols or applications exhibit distinct statistical properties in their network traffic flows, such as packet length distribution and packet inter-arrival time. Leveraging these statistical characteristics, ML-based approaches differentiate between various applications [7]. Their primary goal is to classify different applications or group traffic flows based on shared patterns. ML-based methods excel in identifying encrypted traffic and offer a computational advantage over DPI-based solutions by eliminating the need for packet payload inspection. Figure 1 illustrates the architecture of a network traffic classification system based on supervised machine learning.

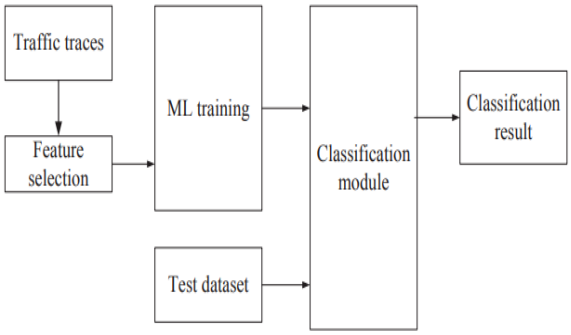

Figure 1: NTC based on Supervised ML

ML-based approaches involve several phases. Initially, features such as packet lengths, flow durations, or inter-packet arrival times are extracted by analyzing numerous packets within flows [8]. Feature selection methods are often employed to further refine these features whenever possible. Subsequently, a pre-trained ML model is utilized to generate classification rules, and the ML algorithm is applied to classify unknown traffic flows. Typically, a unique flow is defined by five tuples of information, including the IP source, IP destination, source port, destination port, and transport layer protocol. Traffic flow features can be broadly categorized into two classes based on how they are observed: flow-level features and packet-level features [9]. Flow-level characteristics, such as the number of packets, flow time, and mean packet size, are typically computed once the flow has concluded. In contrast, the early stages of a flow provide packet-level information, encompassing details like packet length, inter-arrival time, and the packet direction of the initial few packets within the flow. The rationale behind packet-level features is that the initial packets serve as descriptive features, constituting the negotiation stage of the application.

In recent years, early-stage classification of traffic has become increasingly prominent [10]. Unlike waiting for the flow to conclude, a timely classifier aims to use as few packets as possible to arrive at a conclusion. The quality of features significantly influences the performance of the ML algorithm. The use of redundant features can reduce accuracy and potentially increase the computational cost of the system. Therefore, selecting the optimal combination of features to convey essential information about the classes of interest and characterize various traffic types is crucial [11]. Feature selection algorithms fall into two categories: wrapper and filter methods. Various feature selection methods, including principal component analysis (PCA), information gain (IG), fast correlation-based feature selection (FCFS), correlation-based feature selection (CFS), and others, have been widely employed. Machine learning algorithms fall into three categories: semi-supervised, unsupervised, and supervised [12]. In supervised learning, models classify new examples into pre-existing classes. The process of supervised learning involves two stages: the training phase, where the algorithm analyzes a training dataset (instances with characteristics and ground truth of classes) to create a classification model, and the testing (or classifying) phase, where the developed model is used to categorize new occurrences.

1.2 ML algorithms for NTC

Various classification models are available, each employing a distinct mathematical model to classify data. As a result, the outcomes of each model may differ [13]. While some models perform well in certain scenarios, others may be more suitable for improvement. Therefore, it is recommended to train and evaluate multiple classification models to determine which is best suited for the specific project. Below are brief explanations of commonly used models:

Support Vector Machine (SVM): The SVM (Support Vector Machine) algorithm trains the model using labeled data in a supervised learning approach. It establishes decision boundaries, also known as hyperplanes, between labeled data points. The SVM model determines these hyperplanes by identifying extreme points that are close to them [14]. To optimize these decision boundaries, the algorithm establishes margins between hyperplanes. Various kernels, including Sigmoid, Polynomial, RBF (Radial Basis Function), and Linear, are employed to optimize these decision boundaries. SVM can handle both one-dimensional and multidimensional real-world data, and it is not restricted to linearly separable datasets. The linear kernel, in particular, is versatile, capable of handling linearly separable datasets and transforming nonlinear datasets into linear ones. Apart from its memory efficiency, SVM (Support Vector Machine) performs effectively with multi-dimensional datasets.

Decision Tree: Another supervised learning approach is the decision tree, which utilizes the dataset's entropy to classify data based on information gain. The decision tree graphically represents all circumstances and choices within the dataset. The root node is determined by the highest information gain entropy in the dataset, and the tree is expanded by splitting branches accordingly. Each internal node functions as an attribute test, with branches indicating the result, while a leaf represents a class label. Decision trees are versatile, accommodating both numerical and categorical data for classification tasks, and they can capture nonlinear correlations between features [15].

Random Forest: Random Forest is among the most potent supervised learning algorithms, adept at tackling both regression and classification problems. It harnesses the power of multiple decision tree methods, and its accuracy tends to increase with the number of trees employed. Functioning akin to an ensemble of decision trees, Random Forest aggregates the predictions of individual trees to arrive at a final decision. This collective decision is typically determined by the majority vote of the outcomes. Notably, Random Forest excels in handling large datasets and effectively managing missing values.

K Nearest Neighbor (KNN): KNN (K-Nearest Neighbors) is a supervised learning algorithm that follows an instance-based approach. In the KNN model, the parameter “k” represents the number of neighbors considered for classification. By examining the labels of these neighbors, the model selects the majority label to assign to the target instance [16]. When “k” is an odd number, a definitive decision can be made. KNN is a robust model that performs effectively with larger training datasets and is adept at handling noisy data. However, it may encounter challenges in multidimensional datasets, which can result in decreased accuracy and efficiency.

II. Literature Review

Z. X. Wang, et.al (2024) suggested model to classify network traffic for smart home networks in which Federated Learning (FL) was employed for protecting traffic data privacy [17]. In this, the model was locally trained and inference of TC models was considered. First of all, a DPI-based traffic labeling (DTL) technique was presented on edge home gateways as FL nodes for helping these nodes to assign labels on data in order to protect data privacy. After that, an auto-encoder (AE)-based semi-supervised (SS) framework was put forward for alleviating the dependence of model on labeled traffic samples. In the end, an XAI-based technique was adopted for interpreting the model which ensured that the suggested model was explainable. The ISCX VPN2016 and self-built datasets were executed for computing the suggested model. The experimentation demonstrated that the suggested model was performed well on a small amount of samples for classifying traffic when the data privacy was protected, and the model was made more reliable.

Z. Chen, et.al (2023) introduced a new traffic graphical expression (TGE) framework known as Weaved Flow Fragment (WFF) for converting a packet sequence into a graph to illustrate the inner relationship of packet sequence [18]. The co-evolution and the cross-direction change association was taken in account in the bidirectional flow to overcome the drawback of considering only adjacent Markov properties in tensor-like length sequence (TLS). Afterward, the graph convolutional networks (GCN), gated graph neuron networks (GGNN), and capsule graph neural networks (CGNN) were utilized to deploy the introduced framework in classifying traffic. Besides, the ensemble GNN model was developed using diverse ensemble methods for mitigating the possibility of error occurred due to overfitting. The experimental results depicted the supremacy of introduced framework over other method. The F1-score of this framework was counted 99.25% and its model size was mitigated up to 99.1% in an open-world scenario.

M. Seydali, et.al (2023) developed an encrypted traffic classification (ETC) method depending upon deep learning (DL) called CBS to classify traffic [19]. The encrypted traffic was classified at 2 levels in which 1D-CNN, attention-based Bi-LSTM, and SAE deep network algorithms were implemented. This method was

assisted in classifying traffic kinds and applications on the basis of a comprehensive set of session and packet-level attributes. Furthermore, the spatial, temporal, and statistical attributes after extracting them from packet content, temporal relations among packets in a session, and statistical features of a work session, were employed for distinguishing traffic classes. A GAN network-based traffic data augmentation (TDA) method was adopted for alleviating the impact of data imbalance on traffic classes. The ISCX VPN-Non VPN 2016 dataset was executed for simulating the developed method. The experimental results indicated that the developed method was effective and accurate to recognize applications and classify encrypted traffic. This method led to enhance precision up to 21.3%, accuracy up to 13.1%, recall up to 18.11%, and F1 score up to 19.79%.

Y. Jang, et.al (2022) projected a traffic classification (TC) technique in a software-defined network (SDN) for classifying network traffic using a Variational Auto-Encoder (VAE) [20]. The k-flow similarity scores taken in comparison of the distributions were summarized to verify the service class of query flow. The projected technique was focused on training VAE based on 6 statistical attributes, and extracting the distributions of latent features for the flows in every service class. Additionally, this technique was helped in classifying the query traffic. The projected technique was trained and tested on statistical features of network flows taken from real-time domestic and overseas Internet services. The simulation results exhibited that the projected technique was more effective and offered an average accuracy up to 89% as compared to other techniques.

F. Zola, et.al (2022) formulated a three-fold technique which classified the network traffic [21]. At first, temporal dissection was employed to extract graph-based information. Due to the impact of class imbalance on resultant graphs, two new graph data-level preprocessing (GDLP) methods, namely R-hybrid and SM-hybrid were presented to deploy relevant graph sub-structures. At last, a comparative analysis was conducted on Neural Network (NN) and two Graph Convolutional Network (GCN) models while classifying node behavior. The experiments confirmed that the temporal dissection metrics laid impact on performance, and the presented methods were useful to alleviate class imbalance and classify the supervised node behavior more effectively. Generally, the initial model was performed better as compared to other 2 models. The formulated technique was effective to classify traffic and detect malicious attack in network traffic data.

X. Yan, et.al (2024) presented a High-speed Encrypted Traffic Classification (HETC) technique to classify traffic in 2 phases [22]. Initially, for effectively detecting the encryption of traffic, the arbitrarily sampled short flows were considered and chi-square test features were employed to extract aggregation entropies for computing diverse patterns of the byte composition and distribution. Subsequently, the features were presented based on the earlier features. Additionally, these payload features were integrated with a Random Forest (RF) algorithm to classify traffic. The experiments validated that the presented technique offered F-measure of 94% to detect encrypted flows and 85%-93% to classify fine-grained flows on a 1-KB flow-length dataset and consumed average time around 2 or 16 ms for processing every flow while classifying traffic.

X. Jing, et.al (2022) designed a traffic granularity-based cryptographic traffic classification (TG-CTC) technique, known as Granular Classifier (GC) [23]. A new Cardinality-based Constrained Fuzzy C-Means (CCFCM) algorithm was adopted for dealing with the issue related to restricted training traffic. Thereafter, an original illustration format of traffic was put forward on the basis of granular computing, called Traffic Granules (TG), for defining the traffic structure. For this, the dispersion of diverse traffic attributes was captured. Every granule was a compact set having same data with a refined boundary from which the outliers were excluded. The TG was considered to develop GC for classifying traffic on the basis of multi-level attributes. The real-time data was employed to compute the designed technique. The experiments proved that the designed technique was more effective to classify encrypted traffic on restricted sized training traffic and in dynamic network circumstances.

A. M. Eldhai, et.al (2024) focused on deploying a stream learning (SL) method for enhancing efficacy to classify traffic after selecting applicable Feature Selection (FS) [24]. Firstly, an FS technique known as Boruta was suggested to classify traffic. Secondly, three streaming-based TC techniques, namely Hoeffding adaptive trees (HAT), adaptive random forest (ARF), and k-nearest neighbor with adaptive sliding window detector (KNN-ADWIN) were projected. These techniques were capable of handling concept drift and tackling the issue related to memory and time consumption at least overhead. Thirdly, the suggested technique was evaluated on real and synthetic traffic traces. The results depicted that the suggested technique and projected techniques offered an average accuracy (ACC) of 95% and 85%, and precision, recall, and f-score of 87% and 62-88% respectively. Moreover, the projected approaches offered kappa of 78% and consumed lower time of 15s and memory of 105KB.

J. Koumar, et.al (2024) introduced a new extended IP flow called Network Time Series Analyzed (NetTiSA) flow, when the time series of packet sizes was analyzed [25]. Twenty-five diverse tasks were tested to prove that the introduced flow was applicable and effective. Its features were employed to expand sizes of flows which were taken in account for practically deploying this approach. Moreover, an analysis was conducted on their computation in the flow exporter. These novel features consumed least cost and higher performance. These features were employed to train the machine learning (ML) methods which performed better than the traditional techniques. The introduced flow was assisted in bridging gap and offered universal, small-sized, and computational cost-effective features to classify traffic for enhancing wide monitoring infrastructures. Moreover,

this flow provided ML even with100 Gbps backbone lines. Hence, the introduced flow was proved universal and discriminative.

S. Ahn, et.al (2021) recommended a technique which explained the working mechanism of deep learning (DL)-based technique called XAI based on a genetic algorithm (GA) to classify traffic [26]. Afterward, a DL-based method was put forward on the basis of ResNet algorithm to illustrate the recommended technique. A dominant feature selection (FS) technique was presented relied on GA for generating an optimal mask to select features. Moreover, the GA was helped in producing a mask to select significant features in the whole feature set. The experiments indicated that the recommended technique was effective to classify traffic at 97.24% accuracy. Furthermore, the significance of every feature was provided at the dominance rate.

2.1 Table

Author	Year	Technique Used	Dataset	Parameters	Results	Limitations
Z. X. Wang, et.al	2024	Federated Learning (FL)	ISCX VPN2016 and self-built dataset	Precision, Recall, F1-score, and Acc	The experimentation demonstrated that the suggested model was performed well on a small amount of samples for classifying traffic when the data privacy was protected, and the model was made more reliable.	The data was distributed by every sub-node inconsistently. Besides, the communication resources and data amount on every edge device were varied due to which training time was extended.
Z. Chen, et.al	2023	Weaved Flow Fragment (WFF)	ISCX VPN-nonVPN dataset	Precision rate, recall rate, training time, and prediction time	The experimental results depicted the supremacy of introduced framework over other method. The F1-score of this framework was counted 99.25% and its model size was mitigated up to 99.1%	This framework was not applicable to compress the features and classify multi-flow traffic.
M. Seydali, et.al	2023	CBS	ISCX VPN-Non VPN 2016 dataset	Accuracy, precision, recall, and F1 score	The experimental results indicated that the developed method led to enhance precision up to 21.3%, accuracy up to 13.1%, recall up to 18.11%, and F1 score up to 19.79%.	Statistical features were not useful in real-time and this method was unable to classify stream data in the real time.
Y. Jang, et.al	2022	Variational Autoencoder (VAE)	ISCX VPN-nonVPN dataset	Accuracy	The simulation results exhibited that the projected technique was more effective and offered an average accuracy up to 89%.	The significant information related to network flow was extracted in manual way.
F. Zola, et.al	2022	A graph-based method	UNSW-NB15	AUC-ROC, F1-Score, TP, FP	The formulated technique was effective to classify traffic and detect malicious attack in network traffic data.	This technique was unable to detect attacks in case the entities were mixed with other classes.
X. Yan, et.al	2024	High-speed Encrypted Traffic Classification (HETC)	DoHBrw-2020, Wireshark capture and ISCX VPN2016	F-measure and average time	The experiments validated that the presented technique offered F-measure of 94% to detect encrypted flows and 85%-93% to classify fine-grained flows on a 1-KB flow-length dataset and consumed average time around 2 or 16 ms.	The efficiency of this technique was mitigated in the presence of diverse traffic types and more heterogeneous traffic distributions.
X. Jing, et.al	2022	Granular Classifier (GC)	ISCXTor, UNIBS and USTC	Accuracy, precision and F-measure	The experiments proved that the designed technique was more effective to classify encrypted traffic on restricted sized training traffic and in dynamic network circumstances.	This technique had consumed longer time to generate information related to traffic.

A. M. Eldhai, et.al	2024	Boruta	TOR and SDN datasets	Accuracy, kappa, precision, recall, and f-score	The results depicted that the suggested technique and projected techniques offered an average accuracy (ACC) of 95% and 85%, and precision, recall, and f-score of 87% and 62-88% respectively.	This method was not suitable to meet the requirements of varied traffic.
J. Koumar, et.al	2024	Network Time Series Analyzed (NetTiSA)	CESNET-based datasets	Accuracy, precision, recall and F1-score	This flow provided ML even with100 Gbps backbone lines. Hence, the introduced flow was proved universal and discriminative.	Due to the deployment of standard datasets, only a minority of classification classes were obtained.
S. Ahn, et.al	2021	XAI based on a genetic algorithm	ISCX VPN-nonVPN, MACCDC, and WRCCDC datasets	Accuracy, convergence speed	The experiments indicated that the recommended technique was effective to classify traffic at 97.24% accuracy.	The convergence speed of GA was found lower in real time.

III. Conclusion

Three kinds of methods are utilized to classify the network traffic such as port-based, payload-based and flow statistics-based techniques. Various types of applications or traffic data are recognized by classifying the network traffic. The recognition of the received data packets is required in the communication networks of real world. The standard ports are considered in the traditional port-based mechanism. Various phases are executed to classify the network traffic in which pre-processing is done, features are extracted and classification is done. This paper analyses different ML algorithms to classify the network traffic.

References

[1]. L. Garcia, G. Bartlett, S. Ravi, H. Ibrahim, W. Hardaker and E. Kline, "Explaining Deep Learning Models for Per-packet Encrypted Network Traffic Classification," 2022 IEEE International Symposium on Measurements & Networking (M&N), Padua, Italy, 2022, pp. 1-6, doi: 10.1109/MN55117.2022.9887744.

[2]. L. Garcia, G. Bartlett, S. Ravi, H. Ibrahim, W. Hardaker and E. Kline, "Explaining Deep Learning Models for Per-packet Encrypted Network Traffic Classification," 2022 IEEE International Symposium on Measurements & Networking (M&N), Padua, Italy, 2022, pp. 1-6, doi: 10.1109/MN55117.2022.9887744.

[3]. J. Zhang, F. Li and F. Ye, "Sustaining the High Performance of AI-Based Network Traffic Classification Models," in IEEE/ACM Transactions on Networking, vol. 31, no. 2, pp. 816-827, April 2023, doi: 10.1109/TNET.2022.3203227.

[4]. R. Ghanavi, B. Liang and A. Tizghadam, "Generative Adversarial Classification Network with Application to Network Traffic Classification," 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 2021, pp. 1-6, doi: 10.1109/GLOBECOM46510.2021.9685899.

[5]. P. Khandait, N. Hubballi and B. Mazumdar, "Efficient Keyword Matching for Deep Packet Inspection based Network Traffic Classification," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 567-570, doi: 10.1109/COMSNETS48256.2020.9027353.

[6]. G. Lv, R. Yang, Y. Wang and Z. Tang, "Network Encrypted Traffic Classification Based on Secondary Voting Enhanced Random Forest," 2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 2020, pp. 60-66, doi: 10.1109/CCET50901.2020.9213165.

[7]. Y. Guo and D. Wang, "FEAT: A Federated Approach for Privacy-Preserving Network Traffic Classification in Heterogeneous Environments," in IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1274-1285, 15 Jan.15, 2023

[8]. T. Shapira and Y. Shavitt, "FlowPic: A Generic Representation for Encrypted Traffic Classification and Applications Identification," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1218-1232, June 2021

[9]. F. Li and F. Ye, "Adaptive and Lightweight Network Traffic Classification for Edge Devices," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 4, pp. 2003-2014, Dec. 2022

[10]. X. Ma, W. Zhu and R. Wang, "EETC: An extended encrypted traffic classification algorithm based on variant resnet network", Computers & Security, vol. 128, pp. 125-135, 8 March 2023

[11]. A. Telikani, A. H. Gandomi, K. -K. R. Choo and J. Shen, "A Cost-Sensitive Deep Learning-Based Approach for Network Traffic Classification," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 661-670, March 2022

[12]. Z. Diao, G. Xie and M. Qiao, "EC-GCN: A encrypted traffic classification framework based on multi-scale graph convolution networks", Computer Networks, vol. 224, pp. 12-30, 10 February 2023

[13]. W. Chen, F. Lyu, F. Wu, P. Yang, G. Xue and M. Li, "Sequential Message Characterization for Early Classification of Encrypted Internet Traffic," in IEEE Transactions on Vehicular Technology, vol. 70, no. 4, pp. 3746-3760, April 2021

[14]. S. -J. Xu, G. -G. Geng, X. -B. Jin, D. -J. Liu and J. Weng, "Seeing Traffic Paths: Encrypted Traffic Classification With Path Signature Features," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2166-2181, 2022

[15]. X. Xiao, W. Xiao, R. Li, X. Luo, H. Zheng and S. Xia, "EBSNN: Extended Byte Segment Neural Network for Network Traffic Classification," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3521-3538, 1 Sept.-Oct. 2022

[16]. J. Dai, X. Xu, H. Gao, X. Wang and F. Xiao, "SHAPE: A Simultaneous Header and Payload Encoding Model for Encrypted Traffic Classification," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1993-2012, June 2023

[17]. Z. X. Wang, Z.Y. Li and P. Wang, "Network traffic classification based on federated semi-supervised learning", Journal of Systems Architecture, vol. 149, pp. 23-30, 17 February 2024

[18]. Z. Chen, G. Cheng, D. Niu, X. Qiu, Y. Zhao and Y. Zhou, "WFF-EGNN: Encrypted Traffic Classification Based on Weaved Flow Fragment via Ensemble Graph Neural Networks," in IEEE Transactions on Machine Learning in Communications and Networking, vol. 1, pp. 389-411, 2023
[19]. M. Seydali, F. Khunjush, B. Akbari and J. Dogani, "CBS: A Deep Learning Approach for Encrypted Traffic Classification With Mixed Spatio-Temporal and Statistical Features," in IEEE Access, vol. 11, pp. 141674-141702, 2023
[20]. Y. Jang, N. Kim and B.-D. Lee, "Traffic classification using distributions of latent space in software-defined networks: An experimental evaluation", Engineering Applications of Artificial Intelligence, vol. 119, pp. 63-70, 21 December 2022
[21]. F. Zola, L. Segurola-Gil and R. Orduna-Urrutia, "Network traffic analysis through node behaviour classification: a graph-based approach with temporal dissection and data-level preprocessing", Computers & Security, vol. 115, pp. 123-130, 29 January 2022
[22]. X. Yan, L. He and G. Xie, "High-speed encrypted traffic classification by using payload features", Digital Communications and Networks, vol. 1, pp. 6374-6382, 28 February 2024
[23]. X. Jing, J. Zhao and X. Li, "Granular classifier: Building traffic granules for encrypted traffic classification based on granular computing", Digital Communications and Networks, vol. 6, pp. 10-19, 30 December 2022
[24]. A. M. Eldhai et al., "Improved Feature Selection and Stream Traffic Classification Based on Machine Learning in Software-Defined Networks," in IEEE Access, vol. 12, pp. 34141-34159, 2024
[25]. J. Koumar, K. Hynek and T. Čejka, "NetTiSA: Extended IP flow with time-series features for universal bandwidth-constrained high-speed network traffic classification", Computer Networks, vol. 240, pp. 69-76, 3 January 2024
[26]. S. Ahn, J. Kim, S. Y. Park and S. Cho, "Explaining Deep Learning-Based Traffic Classification Using a Genetic Algorithm," in IEEE Access, vol. 9, pp. 4738-4751, 2021