IJICTR
International Journal of Information & Communication Technology Research

Volume 14- Number 2 – 2022 (1 -13)

A Review on Internet Traffic Classification Based on Artificial Intelligence Techniques

Mohammad Pooya Malek
Telecommunications Department
Broadcast University (IRIBU)
Tehran, Iran
pooyamalek@iribu.ac.ir

Shaghayegh Naderi*
ICT Research Institute (ITRC)
Tehran, Iran
Naderi@itrc.ac.ir

Hossein Gharaee Garakani
ICT Research Institute (ITRC)
Tehran, Iran
gharaee@itrc.ac.ir

Received: 8 April 2022 – Revised: 18 May 2022 - Accepted: 20 June 2022

Abstract—**Almost every industry has revolutionized with Artificial Intelligence. The telecommunication industry is one of them to improve customers' Quality of Services and Quality of Experience by enhancing networking infrastructure capabilities which could lead to much higher rates even in 5G Networks. To this end, network traffic classification methods for identifying and classifying user behavior have been used. Traditional analysis with Statistical-Based, Port-Based, Payload-Based, and Flow-Based methods was the key for these systems before the 4th industrial revolution. AI combination with such methods leads to higher accuracy and better performance. In the last few decades, numerous studies have been conducted on Machine Learning and Deep Learning, but there are still some doubts about using DL over ML or vice versa. This paper endeavors to investigate challenges in ML/DL use-cases by exploring more than 140 identical researches. We then analyze the results and visualize a practical way of classifying internet traffic for popular applications.**

Keywords: Internet Traffic Classification; Network Traffic Analysis; DL; ML; Artificial intelligence.

Article type: Research Article

Publisher: ICT Research Institute

I. Introduction

One of the challenges in telecommunication systems has always been optimizing data transmission systems. In today's world, where a massive amount of information is transferred via the internet, some vital and sensitive information necessitates real-time communication, while others necessitate larger bandwidth and high reliability. This category is prevalent even in cellular networks, where achievement is possible through something known as QoS. Tracking the evolution of cellular networks from 1G to 5G and even 6G reveals that they all have the same goal, and that is to provide users with the best quality of services. Several approaches were used to improve customer service delivery. Upgrade system infrastructures in high-population areas, identify communication protocols, and exchange traffic to transfer information through specific infrastructures in different regions based on priority, necessity, and security. In this survey, we attempt to examine the traffic of viral applications, which can include messengers, games, and social media, which are following the users' appetites. Accordingly, network traffic is adjusted so that the user obtains the highest satisfaction by using those applications by providing the appropriate infrastructure facilities.

* Corresponding Author

[DOI: 10.52547/itrc.14.2.1]

To this end, by comprehensively studying more than 140 authoritative articles and journals, we tried to find ways to solve these challenges. Among these, traditional methods were also examined. There were four approaches to traditional identification methods, but none of them works in today's world, lonely. These approaches include 1- Statistical methods which use packet length, average packet time, and other parameters to determine traffic type. This method is both costly and prone to errors due to the use of human labor. 2- Port-based methods are ineffective today due to the use of dynamic ports, changing and updating port numbers, and the use of tunnels. 3- Payload-based methods are also ineffective due to frequent updates, high costs, and encrypted data for information transfer. 4- Flow-based methods that employ a large number of packets in a timely manner. To solve the problems resulting from the high probability of error in each of these approaches, a combination of the above-mentioned methods with artificial intelligence is a useful solution for increasing accuracy, lowering costs, and improving user satisfaction. Machine learning and deep learning are examples of artificial intelligence. Features are extracted manually or using third-party software in a machine learning algorithm. In contrast, in Deep learning methods, the features in the data are automatically extracted inside the network's model, and the network itself is responsible for extracting and selecting the appropriate features. It should be noted that deep learning is a subset of machine learning and artificial intelligence, but in this article, we have treated them as separate categories due to the stated characteristics. In some cases, these new methods combine all four approaches or selected features under the subsections of each method combined with artificial intelligence; the features in the datasets include a combination of statistical features, port, IP features, or features in packets or flow traffics. [1] demonstrated that ISPs could use bandwidth and event duration as a feature to make resource allocation, routing, and QoS policies. However, when these features are combined with AI techniques, they can improve QoS performance. The key is AI structures and methods, which we will elaborate on later. This paper focuses on Network Traffic Analysis research, surveying AI-based methods in recent years, detailing their observations, and comparing their applications. Furthermore, this paper describes the limitations of ML/DL methods and briefly introduces future trends. The remainder of this paper is as follows: Section II introduces some AI-based network traffic Analysis methods, as well as classes and datasets; Section III will reveal different papers and the frequency of each ML/DL method; Section IV will be about Model Evaluations; Section V will show a general pipeline for training AI-based network traffic classification models. Conclusions are drawn in section VI.

II. Network Traffic Analysis Methods

To solve traffic classification problems, machine learning algorithms and deep learning models have been widely used. However, the structure and architecture of these models differ greatly, and training such models necessitates a large amount of labeled data (dataset). In the process of creating a dataset, data tagging (labeling) is frequently a laborious and time-consuming task. The type and number of output classes are also important for data collection and network training. In some cases, the granularity of a specific application, such as WhatsApp, must be checked, which can include Voice calls, Video calls, Chat, File Sharing, and Voices, among others. In many cases, simply checking the application type, such as Map, is sufficient. Relevant solutions and outcomes will be discussed in this section.

A. Artificial Intelligence

As opposed to traditional methods, AI-based methods are used to automate the process of traffic classification and have demonstrated undeniable performance in Bigdata and high-speed connections. Traditional classification methods were primarily used for a specific application that could not be generalized, but using AI allowed for greater accuracy than superhumans. AI-based architectures benefit from model iterations for different batches of data rather than hand-crafted features extracted by humans' knowledge and expertise, which typically contain far more errors. Whereas traditional software is purposefully programmed line by line to perform a task, an AI-based algorithm is programmed to learn how to perform the task. The convergent analysis is one of the most significant advances in modern science, utilizing heterogeneous technologies from multiple and independent domains/sources to analyze and classify large amounts of data. Compared to traditional classification methods, AI is the key enabler and makes it a truly distinguishable feature. Furthermore, due to recent privacy concerns and the massive growth of connected devices, we can no longer process and classify traffic using traditional methods with the assistance of humans, and thus the best way to solve this problem is to use robots or artificial intelligence techniques for this field. One of the most substantial steps in traffic classification/identification is to use the appropriate artificial intelligence model. To solve a traffic Classification problem, we generally have two choices: one is to use machine learning methods, and the other is to use deep learning methods. As mentioned above, Deep learning is considered a subset of Machine learning. So based on that, Machine learning approaches are divided into four categories: supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning. With the studies conducted, reinforcement learning includes a very small proportion of research and practical implementation in this subject. Since we do not deal with continuous data for traffic analysis, among the subsets of **Supervised Learning** methods, which are Regression and Classification, we only explore classification methods. In [2], which is a supervised machine learning method, they firstly filter the Ip address and Protocol type of the game traffic to reduce background noise as much as possible. Then, to remove irrelevant and redundant features, the Pearson correlation coefficient and information gain ratio are used as feature selection criteria. They then analyze the traffic using the SVM algorithm. The main purpose of [3] was to introduce new traffic features to identify applications. They have Proposed a set of statistical

[DOI: 10.52547/itrc.14.2.1]

characteristics of traffic flow such as the number of packets in each flow, the size and time of each flow, the type of distribution in the burst, and the ideal time between different bursts, … that can be used for C5.0 decision tree method to achieve higher accuracy in classifying web-based software traffic. As mentioned, DPI[1] is a real-time separation (filtering) method that uses packet payload to further analyze traffic alongside packet header, and it is a network traffic analysis technology. DFI[2] is the latest packet filtering technique that uses flow statistical features such as TBF[3] and RCF[4] and DF[5] and APBF[6], etc., to detect traffic types. it is worth noting that their work would cause a microsecond delay between exact service execution and packet capture time, which is not significant but should be considered. To the best of our knowledge, defining a value such as ϵ, epsilon, which is an arbitrary small sub_second value for compensating the delay, would be helpful to increase the overall accuracy, whereas the statistical features would be compromised without the delay compensation!

According to [4,] P2P applications such as Facebook, WhatsApp, BitTorrent, and others generate 60-80 percent of traffic. They compared the performance of three machine learning algorithms: decision trees, SVM, and Bayesian networks with DPI and DFI. Some articles have also conducted thorough research on encrypted data. Many applications combine symmetric and asymmetric cryptography. Secure Socket Layer (SSL) and Transfer Layer Security (TLS), two encryption protocols designed to provide secure communications over the Internet, are common examples of such dual systems. SSL protocols are now deemed insecure and will be phased out. TLS protocols, on the other hand, are secure and widely used by major browsers. While their work contains a wealth of useful information, it contains some flaws, such as the effect of DPI classification over DFI classification. They did not take into account this effect in their work, and as a result, some accuracy degradation happened.

Authors in [5] believe that different encrypted software leaves distinct Footprints. So, they used a sequence of randomly selected bits by the application as a feature. They proved that when randomly generated data is encrypted in different ways, these obtained features can be used for training machine learning models to achieve acceptable accuracy in classifying the network traffic. Decision tree methods, Gaussian Naïve Bayes, SVM, and Adaboost, have been used for this purpose. A mobile device with an Asus RT-3200AC as a wireless router was required to perform such a test. It was claimed that by using specific bit sequences for each software and the aforementioned machine learning methods, achieving an average accuracy of about 95 percent was easily accessible. An important note about potential software updates or new network changes that may arise for any application is mentioned in [6]. They examined the impact of packet length changes that may occur primarily to improve a program or security issues. Various supervised machine learning algorithms were used to investigate this issue. The Random Forest, Bagged Trees, and XGBoost algorithms achieved 90% accuracy on the original data. Increasing the length of packets (padding) reduces the accuracy of SGD and SVM algorithms but does not affect Bayesian-based network algorithms. Recall reduction is more affected by packet length change in the random forest than in Google Chrome, Google Drive, One Drive, OneNote, Spotify, and WhatsApp. Despite using one of the best-boosting algorithms to classify the traffic, they did not consider the newly generated fake data for watermarking or concealing information inside other apps' data using Autoencoders or GANs. As a result, in the case of Steganography, this method would be inaccurate. We believe that boosting the model with synthetic data requires combining their techniques with some more advanced techniques.

Two methods were explored in [7], one related to MLP, and the other was LSTM. Instead of Softmax for the last layer, which is commonly used, they defined a threshold to determine the classes. If the class probability falls below that threshold, the traffic is recognized as a VPN; if it goes above that threshold, the traffic is classified as a normal flow. This technique, known as "the distance from the class center," has the potential to improve model accuracy. A hybrid method for network router traffic classification is introduced in [9]. It uses a combination of flow-based methods with XGboost algorithms to train a model and then use it as a classifier. The method begins by sampling the original data, then classifying it using packet-based methods. The categorization process is then aided by flow-based and deep packet inspection methods. If the traffic does not fit within the available information and classes, the RULES will be updated to achieve the best results. Incoming traffic goes through the router for routing policy based on Class Aware or RULEs. In addition, Flow-Based and DPI-Based classifiers are given a mirror of incoming traffic to label Packets/Flows based on their characteristics. Gradient boosted tree models such as XGBoost and LightGBM were used to design and implement an updated packet-based routing policy for the router to improve Class Aware classification on time, which is a must.

[11] studies Unsupervised Learning methods. As you may know, unsupervised methods are used only for clustering. They discussed definitions and issues related to the scope of traffic analysis in the first part and techniques for unsupervised learning methods such as data clustering, hidden variable models, and dimensional reduction in the second part. Finally, unsupervised learning applications were indexed in cases such as Internet Traffic Classification, Anomaly/Intrusion Detection, Network Operations/optimization & Analysis, Dimensionality Reduction & Visualization. Three different algorithms in [12], including K-Means, Fuzzy C Means, and Expectation Maximization, were considered as part of the proposed classification and network error detection solution. The methods attempted to improve the quality of guaranteed services by automatically preventing errors or detecting error points. Due to the increasing

[1] Deep Packet Inspection
[2] Deep Flow Inspection
[3] Total Byte of Flow
[4] Packet Count of Flow
[5] Duration of each Flow
[6] Average Packet Byte of Flow

[DOI: 10.52547/itrc.14.2.1]

growth of applications, especially messengers and SuperApp [7], Various communication services and protocols had used within an application. this is only for Android traffic, but one of the concerns about this method is that it requires knowledge of a user's PII (Hardcoded identifiers) to work on, which has some privacy implications that should be taken seriously.

In [13], a study of performance and detection of granularity using the MIMD techniques, a set selector for the optimal feature selection was conducted. This is helpful and differentiable to feature selection. Using RCC, a type of K-Means could achieve in-app traffic clustering. They evaluated this on WeChat, WhatsApp, and Facebook and gained considerable accuracy.

[14] Is a **Semi-supervised Learning** approach. They come up with new ideas for classifying applications such as YouTube, Netflix, BitTorrent, Skype, DropBox, GDrive, 8 ball Pools, Treasure Hunter, Outlook, and more. They used 17-Tuple Bidirectional NetFlow Records to categorize network traffic. To accomplish this, the traffic was clustered using K-mean, and the classification was obtained using the C5.0 decision tree algorithm. Video Streaming, Video Chat/Voice, p2p Torrent, Cloud Storage, Online Gaming, and Email Clients are examples of clusters.

Deep Learning has emerged as one of the most effective methods for overcoming challenges in a variety of domains in recent years. If a large amount of data is available and also powerful processors are accessible, acceptable accuracy can be achieved through these models. An innovative method for traffic analysis was presented in [16]. According to the authors, Deep Packet is the first deep learning-based traffic classification system that could identify the application and traffic using CNNs[8] and SAE[9]. Five fully connected layers of 50 to 400 neurons were used in the SAE structure. The system described in this study first receives incoming PCAP files before performing preprocessing operations such as removing the data link layer, modifying the transport layer header, deleting irrelevant packets, truncating, normalizing, and IP masking. The output is then fed into CNN and SAE, and the expected output is displayed in the form of a specific label. It is also worth noting that they compared the results of their work with four different machine learning methods t demonstrate the promising results of deep learning models. [17] perused data collection methods and identified about 140 widely used applications using CNN, SAE, and LSTM networks. They also studied the accuracy of convolutional neural network models by increasing the number of input payload bytes, which is much higher by using the initial 300 bytes of the subsequent payloads compared to using a smaller number of payloads. They also used the Tanh activation function for SAE with the ReLU activation function for CNN & LSTM, and Adam optimization is used in all of these models. In [18], NTMA Techniques associated with network traffic analysis and monitoring were scrutinized. It delves into four broad categories of deep learning traffic classification, traffic prediction, fault management, and network security. They looked at two common types of NTMA techniques for obtaining network information: 1- Active methods, such as traffic probe generation and injection within the network, to learn and understand how it works. The sampling is mostly done on a regular and scheduled basis. 2- Passive methods, which use logs and post-events to improve monitoring capability, error tolerance, and problem elimination, but can result in computationally expensive network traffic analysis. They also mentioned some issues with DPI-based traffic analysis methods that could jeopardize user data. Full-packet processing requires more processing capabilities than traditional methods, and they are unusable in some types of networks, such as Virtual Private Networks(VPNs). To this end, they switched to Flow-based strategies with nearly identical temporal and statistical characteristics for each App/Service and their capability to manage encrypted/normal traffic.

[15] is an online traffic classification system for network flow identification that combines CNN and DPIs to detect network traffics such as RDP, BitTorrent, SSH, eDonkey, etc. They claimed that by receiving 10 packets of each traffic stream, classes of these protocols could be identified. The idea of using a system that can extract the pattern in the packets and the patterns in the data flows using LSTM was suggested in [19]. They identified 80 applications using a laboratory dataset collected by popular tools like Wireshark and tcpdump. They only considered the payload and statistical features of the first few packets of a flow, but as previously discussed, in the case of encrypted traffic that conceals the payload, their work will not accurately classify the traffic.

Software-Defined Networks are now considered an alternative to traditional networks. Among the reviewed articles on traffic analysis for software defined-based networks, [22] addressed traffic classification using the Mininet controller and OpenVSwitch. Various machine learning methods such as decision trees, support vector machines, simple Bayesian, and deep learning methods such as AE, NN, and RNN were used to overcome some of the challenges. Federated Learning was used in [23], which is a new framework based on decentralized datasets that allow collaborative model training. This learning approach enables the use of deep learning algorithms in resource-constrained appliances as the training data is distributed among all participants use a shared model. As a result, even with limited memory and computational resources, the entire system can achieve promising results, but none of them could happen if they acted friendlessly. For this type of dataset, a new GAN-based method was used. As a result, we have a set of local servers that communicate with FOG servers, and these FOGs communicate with a central coordinator. Each of these local servers receives the data, categorizes it, and then passes it to the FOGs. There are now two options. The first possibility is that these FOGs act as discriminators while the coordinator acts as a generator. In this case, the generator generates data, and FOG attempts to distinguish between real and fake data. If the generated data looks genuinely like the true data, the discriminator

[7] That allows a user to access several services from a single app.
[8] Convolutional Neural Networks
[9] Stacked Auto Encoders

[DOI: 10.52547/itrc.14.2.1]

is fooled, and the data is considered real. In the second possibility, generation and discrimination are done within both the FOGs and Coordinators. This decentralized method reduces security concerns, and the new data can be generated with a small dataset, so a large amount of labeled traffic is not required.

The Internet of Things (IoT), which is expected to support approximately 21 billion devices in the upcoming years, is the communication structure of devices that send and receive data. [25] introduces a new method for converting traffic flow data into video and categorizing and managing traffic flow based on the analysis of this video for IoT traffic data. The combination of CNN and LSTM was used to extract spatial and temporal information from the stream and then convert this information into a video so that they could apply Time Distributed Feature Learning with MLP to achieve 95% accuracy. They discovered that the combination of TD and MLP aids in understanding semi-temporal properties which could not be detected by LSTM. They compared the CNN + LSTM + TD + MLP structure to the CNN + LSTM + MLP structure, which is an obvious trade-off between 41 times the parameters (about 115 thousand) for a 10% increase in accuracy. It should be noted that the cost was doubling the training time. In [26], the performance of AI-based systems, including the ML and DL methods for classifying encrypted traffic has been examined while Adversarial Evasion Attacks are conducted. Adversarial Evasion attacks are a method in which noise is added to the original data in such a way that it misdiagnoses the decision boundary between normal data and manipulated data which makes traffic classification difficult. In this method, traffic generation and evaluation were performed using Zeroth Order Optimization (ZOO), Projected Gradient Descent (PGD), and DeepFool to investigate the classification performance of various algorithms for encrypted traffic. The performance had measured with and without attack, and it has shown that DL models performed better than ML in non-attack environments. In attack time, depending on the type of attack, the superiority of DL over ML models could be different. In [31], the problems of conventional AI methods for analyzing network traffic classification were addressed, and an optimal model called iCarl + was introduced. The iCarl+ algorithm was inspired by the iCarl algorithm, which is widely used in machine vision tasks for continuous learning. To add a new class or category of traffic using traditional methods, two steps must be taken: 1- Create new training data or improve and expand on existing data 2- Create a new network model from scratch using new data. However, incremental (continuous) learning methods were proposed, eliminating the need for retraining from scratch, saving time and money, and improving performance. A network that benefits from continuous or incremental learning is always looking for new ways to update the models' weights to adapt to new information needed for the best classification performance. In this case, combining the knowledge gained from previous information and available classes with the addition of new classes can result in much higher accuracy. Then they worked to resolve iCarl's ambiguities and improve the network. NMC was replaced with SoftMax, and the output layer was dynamically expanded instead of a fixed predefined output layer size, allowing it to be compatible with new classes while improving performance without affecting error. The model consists of 1D-CNN with about 200,000 parameters.

B. Datasets and tools

As you may know, data plays a very essential and critical role in the accuracy and performance of artificial intelligence methods. Deep learning algorithms are data-hungry, which means that the more data they hit, the better their performance and accuracy will be. In the network traffic analysis field, due to the possibility of misusing data for specific purposes, the number of articles that provide up-to-date and valid data to the public for free is practically low. For this reason, the data used in this field are mainly related to the university environment (campus) or obsolete data. Of course, as shown in TABLE. I, many dataset names are no longer usable; only about 10-20 are publicly available and valid to be used for today's development. Some of the most available prominent datasets can be pointed out as follows: IP Network Traffic Flows Labeled with 75 Apps [38], Moore [39], ISCX [40], ANSM [41], ISCXVPN [52], Labeled Network Traffic Flows-141 Applications [53], USTC-TFC[54], UNIBS: Data sharing[59]. On the other hand, there are articles about dataset collection and construction, including [55], which provide tips on how to collect data for the training and test dataset. It also explains how to place the probes correctly. Are the training and test data collected from the same networks (cellular networks, home networks, or public networks)? Is the training and testing data from the same layer (L7, L3, L2)? How was the information gathered (online or offline)? A rich dataset can be collected by observing and applying these notes to achieve high-performance accuracy.

Another influential topic in dataset collection that should be considered is tools. Wireshark and Netmate were used for this purpose in [143]. NetFlow, SoftFlow, and TCPdump are mostly open-source tools used by [144], a system for detecting anomalies. By the way, some commercial tools, such as PACE, Libprotoident, and NBAR, ... that can be used in both the data collection as well as classification phases, are studied in [65]. It is also important to note in [19], which was mentioned earlier, that if you want to generate a dataset, you must pay attention to ambient traffic. According to the authors, each application generates some ambient traffic (obscure traffic) in addition to normal traffic. Shared modules between applications, such as ad-related traffic or a shared web API, can generate this traffic. They also attempted to detect this type of traffic. However, it should be noted that this type of traffic can have a similar pattern while being delivered from different apps. They also perused the effects of categorizing traffic using adjacent flows. As a result, they believe that examining ambiguous packets generated by one application may not have a distinct pattern from other applications; however, they were able to achieve sufficient accuracy by leveraging nearby traffic as well as the LSTM algorithm (the LSTM uses time-series processing so that it can manage few packets around the engaging packets). Preprocessing can cause higher accuracy and better performance in all AI-related studies. [60] examines and categorizes Anomaly traffic class, and they believe in such a manner. They pointed out that preprocessing methods have not received enough attention, and many implementations have been done without paying much attention to these methods, even though simple items like raw data aggregation, Data Cleaning, Data Transformation, Data Normalization, and under-sampling can boost data quality and thus model accuracy. They used Under Sampling to reduce the unbalanced difference between data classes to increase the number of Benign samples from approximately 13 million to roughly one million. The main focus of [61] was on Deep Learning-based methods for studying various issues in network traffic classification and identification. However, they initially stated that the complexity of the deep learning model and training time would be increased due to the numerical dispersion of training samples for each software, operating system, device, and software version. They also grouped deep learning classes into four broad categories, including Single / Multiple Input Modalities (SM / MM) and Single / Multiple Classification Task.

C. Classes

Numerous works in network traffic analysis have been completed, ranging from intrusion detection to identifying social media, games, and messengers. Each of these includes several categories based on the dataset and the researchers' intentions. For example, [29] discusses the traffic classification of social networks such as WhatsApp, WeChat, Facebook, and Weibo. Alternatively, in [33], traffic is classified as HTTP, BitTorrent DNS, SSL, etc. Convolutional neural networks were used in [8] to classify Emails, file transfers, chat, streaming, and VoIP traffic. They obtained promising results, but they were only considered ideal for classifying the majority classes and focused on improving the performance of the model structure because their approaches lacked rebalancing strategies and thus failed to classify minority classes. The full results of these studies can be seen in TABLE I. In [3], which was mentioned earlier, the output classes include Facebook, Google, YouTube, Gmail, Amazon, BBC News, and Bing, which are considered from a very general perspective. Also, in [19], 80 applications from different contexts were categorized. I.e., Social media's subcategories include traffic detection on Instagram, WhatsApp, Telegram, LinkedIn, Skype, Twitter, etc. Other contexts such as Download, Store, Maps, News, and Music have also been studied. The classes used in [60] related to IDS include Benign, BruteForce, DDos, Web Attack, and Infiltration, built using a model based on LightGBM.

III. Findings

After numerous and time-consuming studies, more than 140 articles in which at least one artificial intelligence method was used had studied, and the results have shown in TABLE I.

The Table starts with the name of the article's author, the reference number, and the publication year. The columns that follow are about Machine Learning or Deep Learning methods, and the last two columns are about Datasets and Classes. In ML algorithms, If the exact header, such as Bayesian Networks, was used and no details were provided, the green checkbox would be present as the possible article methods. If the exact method of Baysian Networks was mentioned in their articles, that is written in the Table. For example, [5] compares their self-collected datasets using gaussian bayesian networks with other ML methods. As mentioned earlier, the majority of the articles collected their datasets (written as Self-collected), while the others used public datasets. The classes cover a wide range of use-cases, such as encrypted traffic, VPNs, social media, and various protocols such as FTP, TCP, UDP, SCTP, and so on.

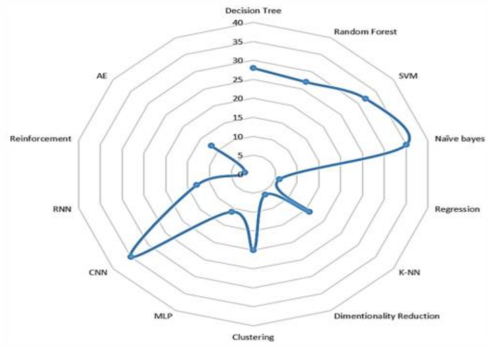

Figure 1. Most Frequently used AI/ML Techniques in reviewed Network Traffic Classification papers

According to studies and investigations, the frequency of methods is shown in Fig.1. As can be seen, if we consider the left side of the figure as deep learning models and the right side of the figure as machine learning-based algorithms, it can be argued that for machine learning methods, algorithms based on Bayesian networks are at the forefront and they are the most widely used machine learning algorithms for traffic analysis. Also, convolutional neural networks or a combination of convolutional networks with other networks such as LSTM are known as the most widely used type of implementation for models based on deep learning.

IV. Model Evaluation

After we've trained our model on a dataset, it's time to see how accurately it can classify unknown data. The "Confusion Matrix" concept will be conducted when the accuracy of predicting a category is more important than the accuracy of the overall diagnosis. Each data point will eventually be assigned to one of these Classes. Therefore, each data sample contains four candidates:

- The data is a member of a Positive category and predicted to be a member of the same Class (TP)
- The sample is a member of the Positive Class, but the model predicts it as a Negative Class (FN)
- The sample is a member of a Negative class and predicted to be a member of the same Class (TN)
- Finally, the sample is a member of the Negative Class, but the model has predicted to Positive Class (FP)

[DOI: 10.52547/itrc.14.2.1]

TABLE I. COMPREHENSIVE REVIEW ON MORE THAN 140 PAPERS ON NETWORK TRAFFIC CLASSIFICATIONS FOR ML/DL TECHNIQUES, CLASSES AND DATASETS

Name/Algorithm	Reference	Year	Decision Tree	Random Forest	SVM	Regression	Baysian Networks	KNN	Dimentionality Reduction	Clustering	Deep Learning	Dataset	Classes
Shahbaz	1	2020									CNN	QUIC Dataset. ISCX VPN-nonVPN Dataset	VPN/non-VPN, GoogleDoc (1251 flows),GoogleDrive (1664 flows),Google Music (622 flows), Youtube (1107 flows),Google Search (1945 flows).
Yuning	2	2018			√							Self Collected	GAME: Fantasy Westward Journey, against the war, furnace stone legend, LOL, DOTA2 and DOTA
Hussein	3	2019	√									Self Collected	
Satadal	5	2019	√	√	√	Logistic	Gaussian	√			MLP	Self Collected	Encrypted TLS, Ciphering Algorithms, ARP, DNS, IGMP, ICMP, NTP, DB-LSP-DISC
Sina	6	2019	Bagged Trees, Decision Trees	√	√		Adaboost, Bernoulli NB, Gaussian NB, XGBoost				MLP	Self Collected: The total generated dataset consists of about 11 million TCP packets	Google Chrome, Google Drive, Microsoft One Drive, WhatsApp, Microsoft Onenote, and Spotify.
D. Li	7	2017									MLP ,VAE	Self Collected :IMTD17	Alipay, Baidu, Bilibili, CNTV, JD, Kugou, QQ, QQMail, QQMusic, Taobao, Wechat, Weibo
Ali Safari	8	2019	√	√		ridge regression	Bernoulli, Multinomial, Complement, Linear	√				UNB2015, NIMS2018	Web Browsing Firefox and Chrome mail SMPTS, POP3S and IMAPS Chat ICQ, AIM, Skype, Facebook and Hangouts , Video Vimeo and Youtube, File Transfer Skype, FTP over SSH (SFTP) and FTP over SSL (FTPS) , VoIP Facebook, Skype and Hangouts voice calls , P2P uTorrent
L. Vu, C. T. Bui	9	2017									GAN	NIMS	SSH services as Shell login; X11; Local tunneling; Remote tunneling; SCP and SFTP, DNS, HTTP, FTP, P2P (limewire),and telnet
Yuantian	10	2018		RF, BOF-RF						Kmeans		ISP	Protocols :BT, DNS, EBUDDY, EDON-KEY, FTP, HTTP, IMAP, MSN, POP3, RSP, RTSP, SMB, SMTP, SSH, SSL2, SSL3, XMPP, and YAHOOMSG
A. Le	12	2015			Linear SVM							self Collected	HTTP and HTTPS , VPN,Non VPN, Entertainment , Media & Video, Social, Music & Audio, Communication, News & Magazines, System, Travel & Local, Other
H. F. Alan	13	2016					Guassian & Multinomial					Self Collected	HTTP/HTTPS, run time app identification
Taimur	14	2016	C 4.5	j 48			√			K means		Self Collected using Netflow	Video streaming YouTube,Netflix,Dailymotion. Video chat/VoIP Skype,Gtalk,Facebook Messenger. P2P torrent VUZE, BitTorrent. Cloud storage Dropbox,Google Drive, OneDrive. Online games 8-Ball Pool , Treasure Hunt. Email client Thunderbird, Outlook.
Qing	15	2019					√				CNN, RNN, FC	UNIBS traces, UPC traces	"RDP", "BitTorrent", "Web", "SSH", "eDonkey" and "NTP"
Mohammad	16	2019									CNN,SAE	UNB ISCX VPN-nonVPN	AIM chat, Email, Facebook, FTPS, Gmail, Hangouts, ICQ, Netflix, SCP, SFTP, Skype, Spotify, Torrent, Tor,VoipBuster, Vimeo,YouTube
Xin	17	2020									SDAE,CNN,RNN, LSTM	Self Collected: Used NetLog	TLS encryption. WeChat, JingDong
SHAHBAZ	19	2019		√							CNN + LSTM	Self Collected: Our dataset is comprised of 80 apps from a wide range of categories, including streaming, messaging, news, navigation, etc.	Google Map, Google Music, Hangouts, Gmail, Google Earth, YouTube, and Google Play, Google Common, Google Analytics, Google Search, Google Adsense, TCP Connect, HTTP, and HTTPS.
Giuseppe	20	2018	cart	Tay_RF	Tay_SVC		Multinomial NB, Her_Pure, Her_TF				CNN, LSTM	dataset collected by a global mobile solutions provider. Due to NDA with the provider we can not report its name, details of its network, detailed information on the data set, nor release the data set.	encrypted protocols, QQ, Sayhi,googleplay,hotspotshield, 6rooms, pureVPN, QQReader, HidemanVPN, Baidu, google+, 80sMovie, googleMaps, private Tunnel VPN, GoogleAllo, Hangouts, Intervoipe, NetTalk, Fsecure VPN, Shadowsocks, Smart Voip, 360 Security, Google Photos, Hidemyass, Minecrafts
Yu-ning	21	2017	c4.5	√	√		√	√			MLP	Asymmetric standard definition videos Asymmetric high definition videos HTTP-download HTTP-download videos QQ Interactive video communication class Xunlei P2P video data sharing Sopcast Network live TV	
Ays¸e	22	2019	√	√	√	Linear, Polynomial	√	√		K-means	SAE,CNN,RNN, LSTM	MIT KDD 1999	SDN
Vincent	24	2017	√	√	√						Reinforcement Learning	5 Self Collected Dataset using different devices	SSL/TLS, HTTP/HTTPS
Bogdan	27	2014			√	logestic	√					Wikipedia, World Bank data	Social Media, StockMarket
Lizhi	28	2015	NBTree	√	√	Logistic	NaiveBayes, BayesNet, AdaBoost, Bagging					UNIBStraces.UJNtraces,AucklandIItraces	ftp, ftp-data, http,imap, pop3, smtp, ssh, telnet, bittorrent, edonkey, http, imap,pop3, skype,smtp, ssh, Webbrowser,Chat, Cloud disk, Liveupdate, Streammedia,Mail,P2P
Zhen	29	2018	c4.5	√			Adaboost, Bagging				NN	Self Collected	Social WeChat, Weibo, Facebook, WhatsApp Streaming Youku, Mi Video, Web Browser, AppStore, VipShop Service Downloads, Mail Yahoo mail, QQ mail, Gmail
Zhen	30	2018		√						√		Self Collected	
Gerard	32	2016	c4.5					√				Self Collected	Web Browsing Firefox and Chrome, Email SMPTS, POP3S and IMAPS, Chat ICQ, AIM, Skype, Facebook and Hangouts, Streaming Vimeo and Youtube, File Transfer Skype, FTPS and SFTP using Filezilla and an external service, VoIP Facebook, Skype and Hangouts voice calls (1h), P2P uTorrent and Transmission (Bittorrent)
Lei	33	2017		j48		logestic	√					Self Collected	HTTP, BitTorrent, DNS, SSL, ICMP, Apple, HTTP Proxy, Quic, and DCE-RPC
Brendan	35	2016			multi-class support vector machine							Netscope Dataset	News & Politics, Personal Health, Social, Dating, Travel & Local, Shopping,Communication, Media Streaming
Anish	36	2019		√	Linear, RBF, Polynomial		XGBoost	√				CTU-13, The Malware Capture Facilityproject	Benign, Malware
Yaru	37	2019		√			Adaboost, XGBoost					Self Collected: using wieshark	instant messaging apps,WeChat and WhatsApp.Alipay app.Tik Tok, Weibo, Taobao, Weishi
per	42	2015	C 4.5		√		√	√		√	Reinforcement Learning	Not Mentioned	WEB, P2P, DATA:FTP, Network Management, Mail, Chat, Streaming and Gaming, Skype, QQ, SSH, SSL,MSN, IMAP, POP3, SMTP, Telnet,Bittorent, IPSEC
Muhammad	43	2016	C 4.5		√		√					Self Collected : from WEKA	WWW, DNS, FTP, P2P, FTP Data, FIP, SSH, Telnet, SMTP, DNS, HTTP, POP3, NTP, SNMP, WoW
Q. Liao	45	2019					√				CNN	UNIBS traces, UPC traces	RDP, BitTorrent, Web, SSH, eDonkey
Yang	46	2019			√		Bayes Network	√				Self Collected	Video Streaming :Youku SD, Youku HD, Youku CD
BONFIGLIO	47	2007					√					CAMPUS, ISP	Skype, Voip
Y. Dong	48	2019						√			Not DL But Inf. Gain Ration was their Alg. for classification (new Alg)	-	Live video(e.g. Cbox1), Web browsing (e.g. Baidu), Online audio (QQMusic), Web browsing (sina), Voice chat (skype), Video Streaming (Youku)
Giuseppe Aceto	50	2019									MLP, CNN, LSTM		
Jan	51	2018		√			√					Self Collected	FORENSICS
Hamza	55	2016			√							DARPA99 traces	WWW, Skype
Zhang	57	2012	c4.5				√	√				WEKA	Yahoo Mahjong, Globulos, QQ Game, Club Marian, and FashionDash
Kandaraj	58	2019	√	√	Linear, RBF, Polynomial and Sigmoid			√		K means		IP Network Traffic Flows, Labeled 75 Apps Kaggle	SDN
Ruolong	62	2017									CNN	Self Collected	SSL , SSH , SMTP , HTTP ,GVSP , FTP ,DNS ,SKYPE ,WOW ,POP3 ,MSN ,BITTORRENT , MYSQL
Shuang	63	2019		√								Self Collected	Wechat,TencentVideo, BILIBILI, Sougou Pinyin, TaoBao, BaiDu Browser, QQ,
Zhanyi	66	2015									CNN, Deep Belief Networks (DBN) and Stacked, SAE	Self Collected	SSL, HTTP_Proxy, MySQL, SMB, HTTP_Connect,Whois-DAS , Redis, SSH , Apple, Kerberos,DCE_RPC, NetBIOS, FTP_CONTROL,DNS,Skype,LDAP,AppleiCloud,AppleiTunes,MSN,Gmail,BitTorrent,TDS,IMAPS,SMTP,RSYNC
Hongtao	67	2018	C 4.5		√		√				Recurrent Neral Networks, CNN, Deep Belief Networks	Cambridge and UNIBS	WWW http, https MAIL imap, pop2/3, smtp FTP-CONTROL ftp control FTP-PASV ftp passive mode ATTACK Internet worm and virus attacks P2P KaZaA, BitTorrent, GnuTella FTP-DATA ftp data DATABASE Postgres, sqlnet oracle, ingres MULTIMEDIA Windows Media Player, Real SERVICES X11, dns, ident, Idap, ntp
Z. A. Qazi	68	2013	C5.0									self Collected	web, P2P vs. VoIP
Q. Wang	70	2015		√								self Collected	Browsing Chrome(CH) Loading text, pictures and streaming Gaming Boom Beach(BB) Gaming action Multimedia YouTube (UTB), Songza(SON) Streaming Online, Chatting Facebook Messenger (FBM), Tecent QQ (QQ), Snapchat (SN) Sending and receiving text, pictures Social Network Facebook (FB), Twitter (TW) Posting, messaging, adding contact, loading text, pictures, Dating Tinder (TD) Loading pictures Financial Mint (MT) Configuring account, loading text, pictures Medical CDC News (CDC), Medscape (MED) Loading text, pictures
Mongkolluksamee	72	2016		√								Self Collected	FaceBook, Line,Skype, Youtube,web
E. Serkani	73	2019	C5.0		LS-SVM							KDD Cup 99, d UNSW-NB15	
Z. Fadlullah	74	2017									Neural Network	Self Collected	SDN
E. Hodo, X. Bellekens	75	2017									NeuralNetwork	KDD Cup '99	Introsion Detection :DoS, Probe, U2R,DoS-Prob, R2L
H. Gharaee	76	2018			√							KDD CUP 99,UNSW-NB15	
W. Wang	77	2017									CNN	KDD CUP1999 & NSL-KDD	BitTorrent P2P Outlook Email/WebMail Facetime Voice/Video Skype Chat/IM FTP Data Transfer SMB Data Transfer Gmail Email/WebMail Weibo Social NetWork MySQL Database WorldOfWarcraft Game
M. Yousefi-Azar	78	2017									AutoEncoder	NSL-KDD	Intrusion Detection
X. Xie	79	2017									RNN (LSTM)	Self Collected	IOT traffic
M. Adda	80									K-means		NSL-KDD	Intrusion Detection
A. Vl˘adut¸u	81	2017								Dissimilarity Based clustering		Self Collected	SSH or HTTPS,FTPm POP, IMAP, and SMTP , HTTP Video Enterprise, HTTP Enterprise, SSH Enterprise, Oracle Enterpris, Raw UDP Enterprise, Raw Enterprise, BitTorrent Enterprise, Flash Enterprise, HTTPS Simulated Enterprise, SMB Enterprise, SMTP Enterprise, PPLive Enterprise, FTP Enterprise, YouTube Enterprise
J. Liu, Y	82	2017								K-means		Self Collected	Wechat Whatsapp Facebook
T. Wiradinata	83	2016							PCA			3 different dataset from http://www.cl.cam.ac.uk/research/srg/netos/nprobe/data/pap	WWW , MAIL, FTP-CONTROL (FC) , FTP-PASV (FP), ATTACK, P2P, DATABASE (DB, FTP-DATA (FD) , MULTIMEDIA(MM) , SERVICES(SRV) , INTERACTIVE(INT), GAMES (GM)
H. Shi	84	2017							PCA			D_20_15	VOIP, P2P-UPD, SMTP, WWW, P2P, IM and HTTP+FLASH , TLS1, TLS2, TLS3, TLS4 and TLS5
S. Liu	85	2016							Mixture Distribution			Self Collected	WWW , MAIL, FTP-CONTROL (FC) , FTP-PASV (FP), ATTACK, P2P, DATABASE (DB, FTP-DATA (FD) , SERVICES(SRV) ,
J. Cao	86	2017			√				PCA			Andrew Moore	WWW Mail FTP control FTP pasv Attack P2P Database FTP data Multimedia Services, HTTP and HTTPS Pop2/3, smtp, and imap FTP FTP worm and virus Kazaa, BitTorrent, and Gnutella Postgres, sqlnet, oracle, and ingres FTP Voice and video streaming X11, dns, ident, and ntp
S. Rajendran	87	2017							t-SNE		RNN (LSTM)	RadioMl	Signal Detector WFM, TETRA, DVB, RADAR, LTE, GSM

[DOI: 10.52547/itrc.14.2.1]

L. Yingqiu	88	2007								K-means		Moore	WWW, MAIL, P2P, FTP-CONTROL, FTP-PASV, ATTACK, DATABASE, FTP-DATA, SERVICES, INTERACTIVE, MULTIMEDIA, and GAMES
J. Zhang	89	2013									Non- parametric Neural Network	ISP, WIDE	BT, DNS, eBuddy, FTP, HTTP, IMAP, MSN, POP3, RSP, SMTP, SSH, SSL, XMPP, and YahooMsg
A. McGregor	90	2004								EM Based		Self Collected	IMAP,HTTP, DNS, SMTP, FTP
J. Erman	91	2006								EM Based		Auck-Ivsub	http, smtp, dns, socks, irc, ftp (control), pop3, limewire, ftp (data)
T. J. O'Shea, J. Corgan	94	2016									Convolutional AutoEncoder	Self Collected	Radio Communication
Eswaradass A	95	2006									MLP , Neural Network	NSF TeraGrid dataset	Bandwidth predictor
Chen Z	96	2016									RNN (LSTM)	Network traffic volume and flow count collected every 5 min over a 24 week period (public)	AR,ARMA,ARIMA,FARIMA
Haffner P	97	2005					Naïve bayes, Adaboost					Proprietary	FTP, SMTP, POP3, IMAP, HTTPS, HTTP, SSH
Ma J, Levchenko K	98	2006							HCA			Proprietary:U.cambridge, UCSD	FTP, SMTP, HTTP, HTTPS, DNS, NTP, NetBIOS, SrvLoc
Finamore A	99	2010			√							Tstat;NAPA-WINE; Proprietary:ISP network	eMule, BitTorrent, RTP, RTCP, DNS, P2P-TV (PPLive, Joost, SopCast, TVAnts), Skype, Background
Schatzmann D	100	2010			√							Proprietary; ISP network	Mail, Non-Mail
Bermolen P	101	2011			√							Proprietary:campus network, ISP network	PPLive, TVAnts, SopCast, Joost
Roughan M	102	2004						√				Proprietary: univ. networks, streaming service	Telnet, FTP-data, Kazaa, RealMedia Streaming, DNS, HTTPS
Zhang J	103	2013					BOF-NB					WIDE. Proprietary:ISP network	BT, DNS, FTP, HTTP, IMAP, MSN, POP3, SMTP, SSH, SSL, XMPP
Zhang J	104	2015					BOF-NB			K means		KEIO, WIDE, proprietary:ISP network	FTP, HTTP, IMAP, POP3, RAZOR, SSH, SSL, UNKNOWN / ZERO-DAY (BT, DNS, SMTP)
Este A	105	2009			√							LBNI, CAIDA,proprietary campus network	HTTP, SMTP,POP3, HTTPS, IMAPS, BitTorrent, FTP, MSN, eDonkey, SSL, SMB, Kazaa, Gnutella, NNTP, DNS, LDAP, SSH
Jing	106	2011			TF-SVM							proprietary	BULK, INTERACTIVE, WWW, MAIL, SERVICES, P2P, ATTACK, GAME, MULTIMEDIA, OTHER
Wang	107	2006			multiclass SVM, Binary SVM							proprietary:univ.network	BitTorrent, eDonkey, Kazaa, pplive
Liu	108	2007								Kmeans		Proprietary:campus network	WWW, MAIL, P2P, FTP (CONTROL, PASV, DATA), ATTACK, DATABASE, SERVICES, INTERACTIVE, MULTIMEDIA, GAMES
Zander	109	2005					AutoClass					NLANR	AOL Messenger, Napster, Half-Life, FTP, Telnet, SMTP, DNS, HTTP
Erman	110	2006					AutoClass					Univ.Auckland	HTTP, SMTP, DNS, SOCKS, IRC, FTP (control, data), POP3, LIMEWIRE, FTP
Erman	111	2006								Density Based		Univ.Auckland, proprietary: Univ.Calgary	HTTP, P2P, SMTP, IMAP, POP3, MSSQL, OTHER
Erman	112	2007								K means		proprietary:univ.network	(control, data),Web, EMAIL, DB, P2P, OTHER, CHAT, FTP, STREAMING
Bernaille et al.	113	2006								K means		Proprietary: univ.network	POP3, LIMEWIRE, eDonkey, FTP, HTTP, Kazaa, NNTP, POP3, SMTP, SSH, HTTPS
TIE	114	2011	Random Tree	j48			√	√			MLP	Proprietary: Univ. Napoli campus network	FTP, BitTorrent, SMTP, Skype2Skype, POP, HTTP, SOULSEEK, NBNS, QQ, DNS,SSL, RTP, EDONKEY
Nguyen et al.	115	2012	C 4.5				√					Proprietary: home network, univ.network, game server	Enemy Territory (online game), VoIP, Other
Li et al.	116	2007	C 4.5				AdaBoost					Proprietary	WEB, MAIL, BULK, Attack, P2P, DB, service, Interactive
Alshammari	117	2009	C 4.5		√		AdaBoost, Naïve bayse					AMP MAWI, DARPA99, Univ. Dalhousie	SSH, Skype
Shbair et al	118	2016	C 4.5	√								Synthetic trace	Service Provider (number of services): Uni-lorraine.fr, Google.com , akamihd.net Googlevideo.com , Twitter.com , Youtube.com , Facebook.com , Yahoo.com, Cloudfront.com
He et al	119	2016	√	√	Linear SVM, Radial SVM		AdaBoost, Naïve bayse	√			MLP	KDD	Attack tyoes
Wang et al.	120	2016			Laplacian SVM							Proprietary: univ network	voice/video conference, streaming, bulk data transfer, interactive
El Khayat et al.	121	2005	Boosting DT	√				√			MLP-Neural Network	Synthetic data: Simulation in: ns-2, BRITE 0>1K random topologies Data distribution: Training=25k Testing=10K	Congestion loss, Wireless loss
Hyun-Kyo	122	2019									CNN+LSTM	Self Collected	RDP, SSH, Skype, BitTorrent, Facebook,Wikipedia, Google, and Yahoo ,Remote Desktop Protocol (RDP), Skype, SSH, BitTorrent, HTTP-Facebook, HTTP-Google, HTTP-Wikipedia, HTTP-Yahoo
P. Wang	123	2018									MLP, SAE, CNN	ISCX2012	HTTPS, SSH, SSL,AIM, Email, Netflix, Facebook, Gmail, hangout, scp, skype, youtube,vimo,tor, twitter, spotify
M. Lotfollahi	124	2017									MLP, SAE, CNN	ISCX2012 , VPN-nonVPN	AIM chat Email Facebook FTPS, Gmail, Hangouts, ICQ, Netflix, SCP, SFTP, Skype, Spotify, Torrent, Tor, Voipbuster, Vimeo ,YouTube
W.Wang	125	2017									CNN	ISCX2012	Email/Gmail (SMPT, POP3,IMAP) VPN-Email Chat ICQ, AIM, Skype, Facebook, Hangouts VPN-Chat Streaming Vimeo, Youtube, Netflix, Spotify VPN-Streaming File transfer Skype, FTPS, SFTP VPN-File transfer VoIP Facebook, Skype, Hangouts, Voipbuster VPN-VoIP P2P uTorrent, Bittorrent VPN-P2P
M. Lopez-Martin	126	2017									CNN , LSTM	RedIRIS	HTTP, SIP, DNS, Youtube, QUIC, Google, Apple, NTP, Telnet, SMTP
G. Aceto, D. Ciuonzo	127	2018									CNN, LSTM, SAE, MLP	ISCX VPN-nonVPN	360Security ,Rooms 80sMovie,9YinZhenJing,,Anghami, BaiDu ,Crackle, EFood , FrostWire, FSecureVPN, Go90 , Google+ , GoogleAllo, GoogleCast, GoogleMaps, GooglePhotos ,GooglePlay ,GroupMe ,Guvera ,Hangouts ,HidemanVPN ,Hidemyass,Hooq ,HotSpot , IFengNews ,InterVoip, LRR ,MeinO2 ,Minecraft ,Mobily , Narutom , NetTalk ,NileFM , Palringo, altalkScene ,PrivateTunnelVPN ,PureVPN , QQ ,QQReader,QianXunYingShi ,RaidCall ,Repubblica, RiyadBank ,Ryanair, SayHi ,Shadowsocks ,SmartVoip, Sogou ,eBay
S. Rezaei and X. Liu	128	2018									SAE,CNN	QUIC Dataset, Ariel Dataset	Google drive, Youtube, and Google music
V. Tong	129	2018		√							CNN	QUIC dataset	voice call (VC), chat (C), video streaming (VS), Google play music, (GPM) and file transfer (FT),Google Hangout Chat, Hangout Voice Call, YouTube, File transfer, Google play music
H. Zhou	130	2017									CNN	Moore	WWW, MAIL, FTP-DATA,FTP-PASV , FTP-CONTROL, SERVICES, DATABASE, P2P, ATTACK, MUITIMEDIA, INTERACTIVE,GAME
Z. Chen	131	2017									CNN	2 different dataset but private	FTP, HTTP, SSH, TFTP, TLSV, Instagram Skype Facebook Wechat Youtube
Antonello	133	2015	Random Tree	√	√						MIN MAX algorithm	Self Collected	HTTP,FTP-C(controlsessionofFTP),POP3,SSH,Emule, Bittorrent, IMAP-thunderbird, Skype-skype
Jing	134	2017									GSAE,LSTM,LSAE	China Mobile dataset	
Zhanyi	135	2014									CNN,SAE	Self Collected	
Peng Li	136	2018									Bayesian auto-encoder	MAWI, DARPA99, SYNDATA	FTP SSH TELNET MAIL DNS HTTP
P. Xiao	137	2015	√									wide data set, data center data set	web, ftp, DNS, Hadoop, Vmware
J. Su´arez-Varela	138	2018	√									-	SMTP, SSH, , Netflix, Facebook, SSL/TLS
L. He	139	2016	√	√			Adaboost					KDD dataset	YouTube streaming, OpenFlow Traffic, Distributed Denial-of-Service (DDoS) attacks
Z. Fan	140	2017			√					K-means		Moore	WWW Web MAIL SMTP, POP3, IMAP GAMES WOW BULK FTP SERVICES DNS, X11, NTP P2P BitTorrent, eDonkey DATABASE Mysql, Oracle MULTIMEDIA Windows Media Player ATTACK Virus, Worm INTERACTIVE TELNET, SSH
A. S. da Silva	141	2016			√					K-means		Self collected	streaming flows, VLC player, Port scanning, DDoS attack,
P. Wang	142	2016			Laplacian SVM					Kmeans		Self Collected	Voice: GoogleVoice • Video conference: Skype, GoogleTalk • Streaming: USstream, Sopcast • Bulk data transfer: FTP, Mega • Interactive data: SSH, Telnet

Following the implementation of the classification algorithm, according to the mentioned explanations and definitions, the classifier's performance can be examined using a table as shown Fig. 2.

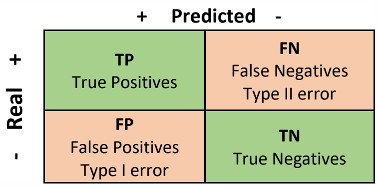

Figure 2. Confusion Matrix

The Confusion Matrix displays classification results based on the currently available information. The Confusion Matrix can be used to define various evaluation criteria such as Accuracy, Precision, Recall, Specificity, and F1-score. Accuracy is the most common, fundamental, and straightforward criterion for assessing prediction quality. This parameter represents the number of patterns that were correctly predicted and formulated as

$$\textbf{Accuracy} = (TP+TN) / (TP+FN+FP+TN) \qquad (1)$$

Precision or Positive Predictive Value expresses the "ratio of correct replies in each category." it shows what percentage of the data has truly categorized as the Positive class and is formulated as follows:

$$\textbf{Precision (PPV)} = TP / (TP+FP) \qquad (2)$$

[DOI: 10.52547/itrc.14.2.1]

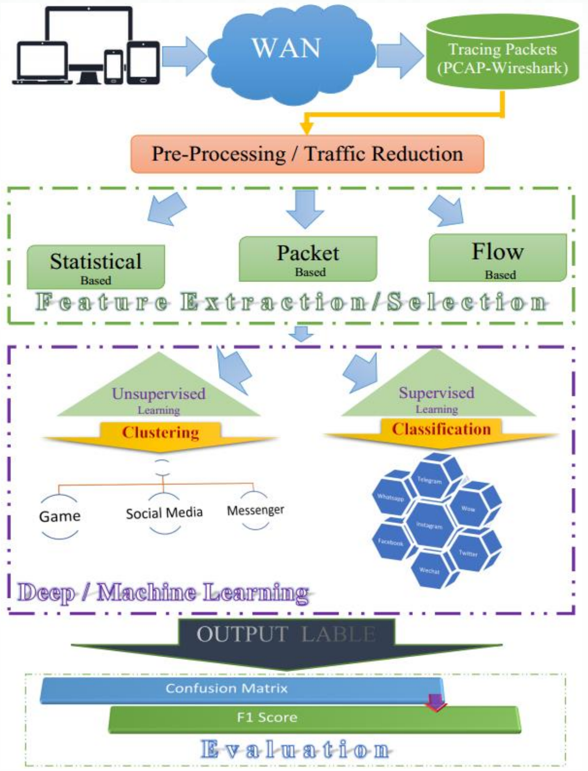

Figure 3. General Perspective of Network Traffic Classification system based on different Methodologies

privacy (encrypted payload contents) while providing promising quality of service. The data rates, packet sizes, and delays remain unchanged while the payload is encrypted. As a result, we can use this information to classify traffic without having to inspect the payload of the packets. We also believe that using correlations between neighbor flows could be an important feature to extract to gain a few percent accuracies.

We discovered that many of the techniques investigated paid little attention to the balance of the dataset or the enrichment of its classes. The emphasis was primarily on providing a new model with various features. It is necessary to improve and enrich the dataset regardless of whether you are using ML-based models or DL techniques, especially when part of the traffic can be generated by new or unconventional methods such as DeepFool, where deep learning techniques generate the traffic, and they are not real. However, they look like real data to fool the model by not accurately learning features from the ground truth. The use of cloud computing for data processing and analysis, as well as edge processing, has gained traction and enabled low-cost training using a vast majority of devices and testbeds with varying devices, operating systems, topology, and protocols, and this is an open challenge to have a better and more accurate classifier even though heterogeneity and decentralized processing and traffic transfers are two of the domain's most difficult challenges.

V. General Perspective

In the previous sections, disassembled information about the classification of network traffic was pointed out. Fig. 3 shows the general operational structure of a system in which the traffic of connected devices to the WAN network is first captured by Wireshark or other network traffic tracking tools. The traffic is then subjected to preprocessing operations such as Datalink Header Removal, Transport Header Modification, Irrelevant Packet Rejection, Byte Conversion, Truncation, Normalization, and IP Masking, among others. Machine learning algorithms are then utilized to select and extract features using statistical-based, packet-based, and flow-based approaches (this step for DL is done automatically within the model). Now it's time to pick an artificial intelligence learning type. At this point, extracted features can be used to train the network using Supervised Learning, Unsupervised Learning, or Semi-supervised Learning. Clustering is a subcategory of Unsupervised Learning. Some of these clusters include Games, Social Media, Messenger, and so on. Furthermore, WhatsApp, Facebook, and Telegram, among others, can be categorized as Supervised Learning algorithms in network traffic classification. After training the network, various evaluation criteria, such as the Confusion Matrix, can be used to calculate Accuracy, Recall, Precision, Specificity, etc. Other criteria, such as the F1 Score, are also computable. Following model evaluation, various techniques such as dropout can be conducted to improve the final model's result and performance. Nowadays, the majority of internet traffic transmitted via satellites/lane lines/cellular networks is encrypted to protect the user's

VI. Conclusion and Future Works

A Comprehensive Comparison of AI techniques was needed to determine which methods were frequently used and which are the most suitable for different datasets of varying sizes and features. To this end, we investigated some of the limitations of DL and ML-based algorithms used to classify internet traffic for over 140 identical state-of-the-art Algorithms and articles. The routing policies can be updated to make the best/most effective use of resources by classifying the internet traffic. Knowing the best method would also enable us to apply it to the telco infrastructure/industry to ensure that users receive promising QOS and QOE. The traffic Classification algorithm can also be used in 5G network slicing to provide eMBB, MMTC, or URLLC slices to users and IoT devices.

We believe that Machine Learning algorithms are far better than Deep Learning Methods for Datasets with low sparsity in Classes and low volume of Data, while deep learning methods are better for the high volume of normalized data and a wide variety of classes in the Network Traffic Classification Domain. Considering network growth and rapid security/feature updates for various applications (e.g., social media, games, ...), the new continuous learning approaches based on deep learning, which can learn through inference time, are more efficient in all aspects. After all, we analyzed different approaches to find the best/most suitable workflow for using AI in network traffic classification (Fig. 3).

Although there are some other novel approaches to Internet traffic classification, artificial intelligence has

[DOI: 10.52547/itrc.14.2.1]

gained tremendous popularity in the modern era. Recent advances in Computer Vision / Deep Learning research, such as Attention Networks or Capsule networks, may draw attention to internet traffic classification in the coming years.

ACKNOWLEDGMENT

A special thanks to Rahimi, SamieZade, Noureddini, Madani, Banad, and Abolghasemi. This work was supported in part by ITRC. Any opinions, findings, and conclusions in this paper are those of the authors only and do not necessarily reflect the views of our sponsors.

REFERENCES

[1] Rezaei, S., & Liu, X. (2020). Multitask Learning for Network Traffic Classification. 2020 29th International Conference on Computer Communications and Networks (ICCCN). doi:10.1109/icccn49398.2020.9209652

[2] Dong, Y., Zhang, M., & Zhou, R. (2018). Classification of Network Game Traffic Using Machine Learning. Communications in Computer and Information Science, 134–145. https://doi.org/10.1007/978-981-13-0893-2_15

[3] Oudah, H., Ghita, B., Bakhshi, T., Alruban, A., & Walker, D. J. (2019). Using Burstiness for Network Applications Classification. Journal of Computer Networks and Communications, 2019, 1-10. doi:10.1155/2019/5758437

[4] Argha Ghosh, Dr.A.Senthilrajan (2019), Classifying network traffic using DPI and DFI

[5] Sengupta, S., Ganguly, N., De, P., & Chakraborty, S. (2019). Exploiting Diversity in Android TLS Implementations for Mobile App Traffic Classification. The World Wide Web Conference on - WWW 19. doi:10.1145/3308558.3313738

[6] . Fathi-Kazerooni, S., Kaymak, Y., & Rojas-Cessa, R. (2019, May). Identification of User Application by an External Eavesdropper using Machine Learning Analysis on Network Traffic. In the 2019 IEEE International Conference on Communications Workshops (ICC Workshops) IEEE.

[7] D. Li, Y. Zhu, and W. Lin, ``Traf_c identi_cation of mobile apps based on variational autoencoder network,'' in Proc. 13th Int. Conf. Comput. Intell. Secure. (CIS), Dec. 2017.

[8] Khatouni, A. S., & Heywood, N. Z. (2019). How much training data is enough to move a ML-based classifier to a different network? Procedia Computer Science, 155, 378–385.

[9] L. Vu, C. T. Bui, and U. Nguyen, ``A deep learning based method for handling imbalanced problem in network traf_c classi_cation,'' in Proc. 8th Int. Symp. Inf. Commun. Technol., 2017, pp. 333_339.

[10] Miao, Y., Pan, L., Rajasegarar, S., Zhang, J., Leckie, C., & Xiang, Y. (2018). Distributed Detection of Zero-Day Network Traffic Flows. Communications in Computer and Information Science Data Mining, 173-191.

[11] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K.-A., Elkhatib, Y., Hussain, A., & Al-Fuqaha, A. (2019). Unsupervised Machine Learning for Networking: Techniques, Applications, and Research Challenges. IEEE Access, 7, 65579–65615.

[12] A. Le, J. Varmarken, S. Langhoff, A. Shuba, M. Gjoka, and A. Markopoulou, “AntMonitor: A system for monitoring from mobile devices,” in Proceedings of the 2015 ACM SIGCOMM Workshop on Crowdsourcing and Crowdsharing of Big (Internet) Data, ser. C2B(1)D ’15. New York, New York, USA: ACM, 2015, pp. 15–20.

[13] H. F. Alan and J. Kaur, “Can Android applications be identified using only TCP/IP headers of their launch time traffic?” in Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec ’16. New York, New York, USA: ACM, 2016, pp. 61–66

[14] Bakhshi, T., & Ghita, B. (2016). On Internet Traffic Classification: A Two-Phased Machine Learning Approach. Journal of Computer Networks and Communications, 2016.

[15] Liao, Q., Li, T., & Zhang, W. (2019). An Online Network Traffic Classification Method Based on Deep Learning. 2019 IEEE 2nd International Conference on Electronic Information and Communication Technology (ICEICT).

[16] Lotfollahi, M., Siavoshani, M. J., Zade, R. S., & Saberian, M. (2019). Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Computing, 24(3).

[17] Wang, X., Chen, S., & Su, J. (2020). Real Network Traffic Collection and Deep Learning for Mobile App Identification. Wireless Communications and Mobile Computing, 2020, 1-14.

[18] Abbasi, M., Shahraki, A. and Taherkordi, A., 2021. Deep learning for network traffic monitoring and analysis (ntma): A survey. Computer Communications.

[19] Rezaei, S., Kroencke, B., & Liu, X. (2019). Large-scale mobile app identification using deep learning. IEEE Access, 8, 348-362.

[20] Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2018). Multi-classification approaches for classifying mobile app traffic. Journal of Network and Computer Applications, 103, 131-145. doi:10.1016/j.jnca.2017.11.007

[21] Dong, Y., Zhao, J., & Jin, J. (2017). Novel feature selection and classification of Internet video traffic based on a hierarchical scheme. Computer Networks, 119, 102-111.

[22] Mohammed, A. R., Mohammed, S. A., & Shirmohammadi, S. (2019). Machine Learning and Deep Learning Based Traffic Classification and Prediction in Software Defined Networking. 2019 IEEE International Symposium on Measurements & Networking (M&N). doi:10.1109/iwmn.2019.8805044

[23] Xu, C., Xia, R., Xiao, Y., Li, Y., Shi, G., and Chen, K.C., 2021. Federated Traffic Synthesizing and Classification Using Generative Adversarial Networks. arXiv preprint arXiv:2104.10400.

[24] Taylor, V. F., Spolaor, R., Conti, M., & Martinovic, I. (2018). Robust Smartphone App Identification via Encrypted Network Traffic Analysis. IEEE Transactions on Information Forensics and Security, 13(1), 63-78. doi:10.1109/tifs.2017.2737970

[25] Manjunath, Y.S.K., Zhao, S. and Zhang, X.P., 2021, June. Time-Distributed Feature Learning in Network Traffic Classification for Internet of Things. In 2021 IEEE 7th World Forum on Internet of Things (WF-IoT) (pp. 674-679). IEEE.

[26] Maarouf, R., Sattar, D. and Matrawy, A., 2021. Evaluating Resilience of Encrypted Traffic Classification Against Adversarial Evasion Attacks.

[27] Batrinca, B., & Treleaven, P. C. (2014). Social media analytics: A survey of techniques, tools and platforms. Ai & Society, 30(1), 89-116. doi:10.1007/s00146-014-0549-4

[28] Peng, L., Yang, B., & Chen, Y. (2015). Effective packet number for early stage internet traffic identification. Neurocomputing, 156, 252-267.

[29] Liu, Z., Wang, R., & Tang, D. (2018). Extending labeled mobile network traffic data by three levels traffic identification fusion. Future Generation Computer Systems, 88, 453-466.

[30] Liu, Z., Wang, R., Japkowicz, N., Cai, Y., Tang, D., & Cai, X. (2019). Mobile app traffic flow feature extraction and selection for improving classification robustness. Journal of Network and Computer Applications, 125, 190-208.

[31] Bovenzi, G., Yang, L., Finamore, A., Aceto, G., Ciuonzo, D., Pescape, A. and Rossi, D., 2021. A First Look at Class Incremental Learning in Deep Learning Mobile Traffic Classification. arXiv preprint arXiv:2107.04464.

[32] Draper-Gil, G., Lashkari, A.H., Mamun, M.S., & Ghorbani, A.A. (2016). Characterization of Encrypted and VPN Traffic using Time-related Features. ICISSP.

[33] Ding, L., Liu, J., Qin, T., & Li, H. (2017). Internet traffic classification based on expanding vector of flow. Computer Networks, 129, 178-192. doi:10.1016/j.comnet.2017.09.015

[34] Haffey, M., Arlitt, M., & Williamson, C. (2018). Modeling, Analysis, and Characterization of Periodic Traffic on a Campus Edge Network. 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS).

[35] Saltaformaggio, B., Choi, H., Johnson, K., Kwon, Y., Zhang, Q., Zhang, X., ... & Qian, J. (2016). Eavesdropping on fine-grained user activities within smartphone apps over encrypted network traffic. In 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16).

[DOI: 10.52547/itrc.14.2.1]

[36] Shekhawat, A. S., Di Troia, F., & Stamp, M. (2019). Feature analysis of encrypted malicious traffic. Expert Systems with Applications, 125, 130-141.

[37] Wang, P., Chen, X., Ye, F., & Sun, Z. (2019). A survey of techniques for mobile service encrypted traffic classification using deep learning. IEEE Access, 7, 54024-54033.

[38] "IP Network Traffic Flows Labeled with 75 Apps", *Kaggle.com*. [Online]. Available: https://www.kaggle.com/jsrojas/ip-network-traffic-flows-labeled-with-87-apps. [Accessed: 07- Jan- 2022].

[39] "Moore | Datasets Master", *Kaggle.com*. [Online]. Available: https://www.kaggle.com/imoore/datasets. [Accessed: 07- Jan- 2022].

[40] "Datasets – ISCX", Available: http://www.iscx.ca/datasets/ *Iscx.ca*. [Online]. [Accessed: 07- Jan- 2022].

[41] HOMOLIAK, I., MALINKA, K. and HANACEK, P., ASNM Datasets: A Collection of Network Traffic Data for Testing of Adversarial Classifiers and Intrusion Detectors.

[42] P. Velan, M. Cermak, P. Celeda and M. Drasar, "A survey of methods for encrypted traffic classification and analysis", International Journal of Network Management, vol. 25, no. 5, pp. 355-374, 2015.

[43] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, and F. Abdessamia, "Network traffic classification techniques and comparative analysis using machine learning algorithms", Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC), pp. 2451-2455, Oct. 2016.

[44] Dainotti, A., de Donato, W., Pescapé, A.: TIE: A Community-Oriented Traffic Classification Platform. In: Papadopouli, M., Owezarski, P., Pras, A. (eds.) TMA 2009. LNCS, vol. 5537, pp. 64–74. Springer, Heidelberg (2009)

[45] Q. Liao, T. Li, and W. Zhang, "An Online Network Traffic Classification Method Based on Deep Learning," 2019 IEEE 2nd International Conference on Electronic Information and Communication Technology (ICEICT), Harbin, China, 2019, pp. 34-39, DOI: 10.1109/ICEICT.2019.8846395.

[46] Yang LY, Dong YN, Tian W, Wang ZJ (2019) The study of new features for video traffic classification. Multimed Tools Appl 78(12):15839–15859

[47] BONFIGLIO, D., MELLIA, M., MEO, M., ROSSI, D., AND TOFANELLI, P. Revealing Skype Traffic: When Randomness Plays with You. In Proc. ACM SIGCOMM (2007)

[48] Y. Dong, R. Cao, and M. Zhang, "A Multi-Objective Evolutionary Algorithm for Multimedia Traffic Classification," 2019 IEEE 21st International Conference on High-Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 2019, pp. 2804-2810, DOI: 10.1109/HPCC/SmartCity/DSS.2019.00393.

[49] Zhang, Jun & Chen, Xiao & Xiang, Yang & Zhou, Wanlei & Wu, Jie. (2014). Robust Network Traffic Classification. IEEE/ACM Transactions on Networking. 23. 1-1. 10.1109/TNET.2014.2320577, 2014.

[50] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Mobile encrypted traffic classification using deep learning: Experimental evaluation lessons learned and challenges", IEEE Trans. Netw. Service Manager., vol. 16, no. 2, pp. 445-458, Feb. 2019.

[51] Jan Pluskal, Ondrej Lichtner, and Ondřej Ryšavý. 2018. Traffic Classification and Application Identification in Network Forensics. In IFIP International Conference on Digital Forensics. Springer, 161--181.

[52] "VPN 2016 | Datasets | Research | Canadian Institute for Cybersecurity | UNB", *Unb.ca*. [Online]. Available: https://www.unb.ca/cic/datasets/vpn.html. [Accessed: 07- Jan- 2022].

[53] "Labeled Network Traffic flows - 141 Applications", *Kaggle.com*. [Online]. Available: https://www.kaggle.com/jsrojas/labeled-network-traffic-flows-114-applications. [Accessed: 07- Jan- 2022].

[54] "GitHub - yungshenglu/USTC-TFC2016: Traffic dataset USTC-TFC2016", *GitHub*. [Online]. Available: https://github.com/yungshenglu/USTC-TFC2016. [Accessed: 07- Jan- 2022].

[55] Ibrahim, H. A., Zuobi, O. R., Al-Namari, M. A., Mohamedali, G., & Abdalla, A. A. (2016). Internet traffic classification using machine learning approach: Datasets validation issues. 2016 Conference of Basic Sciences and Engineering Studies (SGCAC). doi:10.1109/sgcac.2016.7458022

[56] Che, X., & Ip, B. (2012). Packet-level traffic analysis of online games from the genre characteristics perspective. Journal of Network and Computer Applications, 35(1), 240-252. doi:10.1016/j.jnca.2011.08.005

[57] Z.Q.X.W. (Ed.). (2013). Research on Online Game Traffic Classification Based on Machine Learning (Vol. 49). ipder.

[58] Reza, M., Javad, M., Raouf, S., & Javidan, R. (2017). Network Traffic Classification using Machine Learning Techniques over Software Defined Networks. International Journal of Advanced Computer Science and Applications, 8(7). doi:10.14569/ijacsa.2017.080729

[59] "UNIBS: Data sharing", *Netweb.ing.unibs.it*. [Online]. Available: http://netweb.ing.unibs.it/~ntw/tools/traces/. [Accessed: 07- Jan- 2022].

[60] Hua, Y., 2020, May. An efficient traffic classification scheme using embedded feature selection and lightgbm. In 2020 Information Communication Technologies Conference (ICTC) (pp. 125-130). IEEE.

[61] Aceto, G., Ciuonzo, D., Montieri, A. and Pescapé, A., 2020. Toward effective mobile encrypted traffic classification through deep learning. Neurocomputing, 409, pp.306-315.

[62] Ma, R., & Qin, S. (2017). Identification of unknown protocol traffic based on deep learning. 2017 3rd IEEE International Conference on Computer and Communications (ICCC).

[63] Zhao, S., Chen, S., Sun, Y., Cai, Z., & Su, J. (2019). Identifying Known and Unknown Mobile Application Traffic Using a Multilevel Classifier. Security and Communication Networks, 2019, 1-11. doi:10.1155/2019/9595081

[64] Aceto, G., Ciuonzo, D., Montieri, A., & Pescape, A. (2018). Mobile Encrypted Traffic Classification Using Deep Learning. 2018 Network Traffic Measurement and Analysis Conference (TMA). doi:10.23919/tma.2018.8506558

[65] Bujlow, Carela-Español, Barlet-Ros, T. V. P. (2013, June). Comparison of Deep Packet Inspection(DPI) Tools for traffic classification. Department of Computer Architecture (DAC).

[66] Wang, Z. (2015). The applications of deep learning on traffic identification. BlackHat USA, 24(11), 1-10.

[67] Shi, Hongtao, et al. "An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification." Computer Networks 132 (2018): 81-98.

[68] Z. A. Qazi, J. Lee, T. Jin, G. Bellala, M. Arndt, and G. Noubir, “Application- awareness in SDN,” in Proceedings of the 2013 Annual Conference of the ACM Special Interest Group on Data Communication. SIGCOMM ’13. New York, New York, USA: ACM, 2013, pp. 487–488

[69] Chen, K., Jiang, J., Huang, P., Chu, H., Lei, C., & Chen, W. (2008). Identifying MMORPG Bots: A Traffic Analysis Approach. EURASIP Journal on Advances in Signal Processing, 2009(1). doi:10.1155/2009/797159

[70] Q. Wang, A. Yahyavi, B. Kemme, and W. He, “I know what you did on your smartphone: Inferring app usage over encrypted data traffic,” in Proceedings of the 2015 IEEE Conference on Communications and Network Security, ser. CNS ’15. New York, New York, USA: IEEE Communications Society, 2015, pp. 433–441.

[71] Chiu, S. (2006). Online Interactive Game Traffic: A Survey & Performance Analysis on 802.11 Network.

[72] S. Mongkolluksamee, V. Visoottiviseth, and K. Fukuda, “Combining communication patterns & traffic patterns to enhance mobile traffic identification performance,” Journal of Information Processing, vol. 24, no. 2, March 2016.

[73] Serkani, E., Gharaee Garakani, H. and Mohammadzadeh, N., 2019. Anomaly detection using SVM as classifier and decision tree for optimizing feature vectors. *The ISC International Journal of Information Security*, *11*(2), pp.159-171.

[74] Z. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, “State-of-the-art deep learning: Evolving machine intelligence toward tomorrow’s intelligent network traffic control systems,” IEEE Communications Surveys & Tutorials, 2017.

[DOI: 10.52547/itrc.14.2.1]

[75] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," arXiv preprint arXiv:1701.02145, 2017.

[76] Gharaee, H., Fekri, M. and Hosseinvand, H., 2018. Intrusion Detection System Using SVM as Classifier and GA for Optimizing Feature Vectors. *Journal of Information and Communication Technology Research*, *10*(1), pp.26-35.

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

[78] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in Neural Networks (IJCNN), 2017 International Joint Conference on, pp. 3854–3861, IEEE, 2017.

[79] X. Xie, D. Wu, S. Liu, and R. Li, "IoT data analytics using deep learning," arXiv preprint arXiv:1708.03854, 2017.

[80] M. Adda, K. Qader, and M. Al-Kasassbeh, "Comparative analysis of clustering techniques in network traffic faults classification," International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 4, pp. 6551–6563, 2017.

[81] A. Vl˘adut¸u, D. Com˘aneci, and C. Dobre, "Internet traffic classification based on flows' statistical properties with machine learning," International Journal of Network Management, vol. 27, no. 3, 2017.

[82] J. Liu, Y. Fu, J. Ming, Y. Ren, L. Sun, and H. Xiong, "Effective and real-time in-app activity analysis in encrypted internet traffic streams," in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 335–344, ACM, 2017.

[83] T. Wiradinata and A. S. Paramita, "Clustering and feature selection technique for improving internet traffic classification using k-nn," 2016.

[84] H. Shi, H. Li, D. Zhang, C. Cheng, and W. Wu, "Efficient and robust feature extraction and selection for traffic classification," Computer Networks, vol. 119, pp. 1–16, 2017.

[85] S. Liu, J. Hu, S. Hao, and T. Song, "Improved em method for internet traffic classification," in Knowledge and Smart Technology (KST), 2016 8th International Conference on, pp. 13–17, IEEE, 2016.

[86] J. Cao, Z. Fang, G. Qu, H. Sun, and D. Zhang, "An accurate traffic classification model based on support vector machines," Journal of Network Management, vol. 27, no. 1, 2017.

[87] S. Rajendran, W. Meert, D. Giustiniano, V. Lenders, and S. Pollin, "Distributed deep learning models for wireless signal classification with low-cost spectrum sensors, 2017.

[88] L. Yingqiu, L. Wei, and L. Yunchun, "Network traffic classification using K-Means clustering," in Second International Multi-Symposiums on Computer and Computational Sciences (IMSCCS), 2007., pp. 360– 365, IEEE, 2007.

[89] J. Zhang, Y. Xiang, Y. Wang, W. Zhou, Y. Xiang, and Y. Guan, "Network traffic classification using correlation information," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 1, pp. 104–117, 2013.

[90] A. McGregor, M. Hall, P. Lorier, and J. Brunskill, "Flow clustering using machine learning techniques," in Passive and Active Network Measurement, pp. 205–214, Springer, 2004.

[91] J. Erman, A. Mahanti, and M. Arlitt, "Qrp05-4: Internet traffic identification using machine learning," in Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE, pp. 1–6, IEEE, 2006.

[92] E. I. Oyman and C. Ersoy, "Multiple sink network design problem in large scale wireless sensor networks," in Communications, 2004 IEEE International Conference on, vol. 6, pp. 3663–3667, IEEE, 2004.

[93] T. J. O'Shea and J. Hoydis, "An introduction to machine learning communications systems," arXiv preprint.

[94] T. J. O'Shea, J. Corgan, and T. C. Clancy, "Unsupervised representation learning of structured radio communication signals," in Sensing, Processing and Learning for Intelligent Machines (SPLINE), 2016 First International Workshop on, pp. 1–5, IEEE, 2016.

[95] Eswaradass A, Sun XH, Wu M. Network bandwidth predictor (nbp): A system for online network performance forecasting. In: Proceedings of 6th IEEE International Symposium on Cluster Computing and the Grid (CCGRID). IEEE; 2006.

[96] Chen Z, Wen J, Geng Y. Predicting future traffic using hidden markov models. In: Proceedings of 24th IEEE International Conference on Network Protocols (ICNP). IEEE; 2016.

[97] Haffner P, Sen S, Spatscheck O, Wang D. Acas: automated construction of application signatures. In: Proceedings of the 2005 ACM SIGCOMM workshop on Mining network data. New York: ACM; 2005. p. 197–202.

[98] Ma J, Levchenko K, Kreibich C, Savage S, Voelker GM. Unexpected means of protocol inference. In: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. 2006. p. 313–26.

[99] Finamore A, Mellia M, Meo M, Rossi D. Kiss: Stochastic packet inspection classifier for UDP traffic. IEEE/ACM Trans Netw. 2010;18(5):1505–15.

[100] Schatzmann D, Mühlbauer W, Spyropoulos T, Dimitropoulos X. Digging into https: Flow-based classification of webmail traffic. In: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement; 2010. p. 322–27.

[101] Bermolen P, Mellia M, Meo M, Rossi D, Valenti S. Abacus: Accurate behavioral classification of P2P-tv traffic. Comput Netw. 2011;55(6): 1394–411.

[102] Roughan M, Sen S, Spatscheck O, Duffield N. Class-of-service mapping for qos: a statistical signature-based approach to ip traffic classification. In: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. ACM; 2004a. p. 135–148.

[103] Zhang J, Chen C, Xiang Y, Zhou W, Xiang Y. Internet traffic classification by aggregating correlated naive bayes predictions. IEEE Trans Inf Forensic Secur. 2013;8(1):5–15.

[104] Zhang J, Chen X, Xiang Y, Zhou W, Wu J. Robust network traffic classification. IEEE/ACM Trans Netw (TON). 2015;23(4):1257–70.

[105] Este A, Gringoli F, Salgarelli L. Support vector machines for TCP traffic classification. Comput Netw. 2009; 53(14): 2476–90.

[106] Jing N, Yang M, Cheng S, Dong Q, Xiong H. An efficient SVM-based method for multi-class network traffic classification. In: Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International. IEEE; 2011. p. 1–8.

[107] Wang R, Liu Y, Yang Y, Zhou X. Solving the app-level classification problem of p2p traffic via optimized support vector machines. In: Intelligent Systems Design and Applications, 2006. ISDA'06. Sixth International Conference on, IEEE, vol 2; 2006. p. 534–9.

[108] Liu Y, Li W, Li YC. Network traffic classification using k-means clustering: IEEE; 2007. pp. 360–5.

[109] Zander S, Nguyen T, Armitage G. Automated traffic classification and application identification using machine learning. IEEE; 2005, pp. 250–7.

[110] Erman J, Mahanti A, Arlitt M. Internet traffic identification using machine learning. In: Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE. IEEE; 2006b. pp. 1–6.

[111] Erman J, Arlitt M, Mahanti A. Traffic classification using clustering algorithms. In: Proceedings of the 2006 SIGCOMM workshop on Mining network data. ACM; 2006a. p. 281–6.

[112] Erman J, Mahanti A, Arlitt M, Williamson C. Identifying and discriminating between web and peer-to-peer traffic in the network core. In: Proceedings of the 16th international conference on World Wide Web. ACM; 2007b. p. 883–92.

[113] Bernaille L, Teixeira R, Akodkenou I, Soule A, Salamatian K. Traffic classification on the fly. ACM SIGCOMM Comput Commun Rev. 2006a;36(2):23–6.

[114] Dainotti A, Pescapé A, Sansone C. Early classification of network traffic through multi-classification. In: International Workshop on Traffic Monitoring and Analysis. Springer; 2011. p. 122–35.

[115] Nguyen TT, Armitage G, Branch P, Zander S. Timely and continuous machine-learning-based classification for

interactive IP traffic. IEEE/ACM Trans Netw (TON). 2012;20(6):1880–94.

[116] Li W, Moore AW. A machine learning approach for efficient traffic classification. In: Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 2007. MASCOTS'07. 15th International Symposium on. IEEE; 2007. p. 310–7.

[117] Alshammari R, Zincir-Heywood AN. Machine learning based encrypted traffic classification: Identifying ssh and skype. In: Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on. IEEE; 2009. p. 1–8.

[118] Shbair WM, Cholez T, Francois J, Chrisment I. A multi-level framework to identify HTTP services. In: IEEE/IFIP Network Operations and Management Symposium (NOMS) 2016. p. 240–8.

[119] He L, Xu C, Luo Y. vtc: Machine learning based traffic classification as a virtual network function. In: Proceedings of the 2016 ACM International Workshop on Security in SDN & Network Function Virtualization. ACM; 2016. p. 53–56.

[120] Wang P, Lin SC, Luo M. A framework for qos-aware traffic classification in sdns. In: Services Computing (SCC), 2016 IEEE International Conference on. IEEE; 2016. p. 760–5.

[121] El Khayat I, Geurts P, Leduc G. Improving TCP in Wireless Networks with an Adaptive Machine-Learning Classifier of Packet Loss Causes. Berlin, Heidelberg: Springer Berlin Heidelberg; 2005, pp. 549–60.

[122] Lim, Kim, Kim, Hong, & Han. (2019). Payload-Based Traffic Classification Using Multi-Layer LSTM in Software Defined Networks. Applied Sciences, 9(12), 2550.

[123] P. Wang, F. Ye, X. Chen, and Y. Qian, ``DataNet: Deep learning based encrypted network traf_c classi_cation in SDN home gateway,'' IEEE Access, vol. 6, pp. 55380_55391, 2018.

[124] M. Lotfollahi, R. S. H. Zade, M. J. Siavoshani, and M. Saberian. (2017). ``Deep packet: A novel approach for encrypted traf_c classi_cation using deep learning.'' [Online].

[125] W.Wang, M. Zhu, J.Wang, X. Zeng, and Z. Yang, ``End-to-end encrypted traf_c classi_cation with one-dimensional convolution neural networks,'' in Proc. IEEE Int. Conf. Intell. Secure. Inform. (ISI), Jul. 2017, pp. 43_48.

[126] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, ``Network traf_c classi_er with convolutional and recurrent neural networks for Internet of Things,'' IEEE Access, vol. 5, pp. 18042_18050, 2017.

[127] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, ``Mobile encrypted traf_c classi_cation using deep learning,'' in Proc. Netw. Traf_c Meas. Anal. Conf. (TMA), Jun. 2018, pp. 1_8.

[128] S. Rezaei and X. Liu, ``How to achieve high classi_cation accuracy with just a few labels: A semi-supervised approach using sampled packets,'' CoRR, Dec. 2018.

[129] V. Tong, H.-A. Tran, S. Souihi, and A. Mellouk, ``A novel QUIC traf_c classi_er based on convolutional neural networks,'' 2018, pp. 1_6.

[130] H. Zhou, Y. Wang, X. Lei, and Y. Liu, ``A method of improved CNN traf_c classi_cation,'' in Proc. 13th Int. Conf. Comput. Intell. Secure. (CIS), Dec. 2017, pp. 177_181.

[131] Z. Chen, K. He, J. Li, and Y. Geng, ``Seq2img: A sequence-to-image based approach towards IP traf_c classi_cation using convolutional neural networks,'' in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2017, pp. 1271_1276.

[132] Tongaonkar, A., Torres, R., Iliofotou, M., Keralapura, R., & Nucci, A. (2015). Towards self-adaptive network traffic classification. Computer Communications, 56, 35-46.

[133] Rizzi, A., Iacovazzi, A., Baiocchi, A., & Colabrese, S. (2015). A low complexity real-time Internet traffic flows neuro-fuzzy classifier. Computer Networks, 91, 752-771.

[134] Jing Wang, Jian Tang, Zhiyuan Xu, Yanzhi Wang, Guoliang Xue, Xing Zhang, and Dejun Yang. Spatiotemporal modeling and prediction in cellular networks: A big data-enabled deep learning approach. In Proc. 36th Annual IEEE International Conference on Computer Communications (INFOCOM), 2017.

[135] Zhanyi Wang. The applications of deep learning on traffic identification. BlackHat USA, 2015.

[136] Peng Li, Zhikui Chen, Laurence T. Yang, Jing Gao, Qingchen Zhang, and M. Jamal Deen. An Improved Stacked Auto-Encoder for Network Traffic Flow Classification. IEEE Network, 32(6):22–27, 2018

[137] P. Xiao, W. Qu, H. Qi, Y. Xu, and Z. Li, "An efficient elephant flow detection with cost-sensitive in sdn," in 2015 1st International Conference on Industrial Networks and Intelligent Systems (INISCom). IEEE, 2015, pp. 24–28.

[138] J. Suarez-Varela and P. Barlet-Ros, "Sbar: Sdn flow-based monitoring and application recognition," in Proceedings of the Symposium on SDN Research. ACM, 2018, p. 22.

[139] L. He, C. Xu, and Y. Luo, "Vtc: Machine learning based traffic classification as a virtual network function," in Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, 2016, pp. 53–56.

[140] Z. Fan and R. Liu, "Investigation of machine learning based network traffic classification," in 2017 International Symposium on Wireless Communication Systems (ISWCS). IEEE, 2017, pp. 1–6.

[141] A. S. da Silva, J. A. Wickboldt, L. Z. Granville, and A. Schaeffer-Filho, "Atlantic: A framework for anomaly traffic detection, classification, and mitigation in sdn," in NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016, pp. 27–35.

[142] P. Wang, S.-C. Lin, and M. Luo, "A framework for QoS-aware traffic classification using semi-supervised machine learning in sdns," in 2016 IEEE International Conference on Services Computing (SCC). IEEE, 2016, pp. 760–765.

[143] Shafiq, M., Yu, X., Bashir, A. K., Chaudhry, H. N., & Wang, D. (2018). A machine learning approach for feature selection traffic classification using security analysis. The Journal of Supercomputing, 74(10), 4867-4892.

[144] Sharma, R., Singla, R., & Guleria, A. (2018). A New Labeled Flow-based DNS Dataset for Anomaly Detection: PUF Dataset. Procedia Computer Science, 132, 1458-1466.

Mohammad Pooya Malek received a B.A.Sc. in Engineering from IRIB University. He subsequently continued on to the IRIBU University in Tehran, Iran, to pursue his M.Sc. degree in Electrical and Telecommunications Engineering. 5G Cellular Networks, Artificial Intelligence, Deep Learning, QoS, QoE, Networking, and Digital Signal Processing are among his research interests.

Shaghayegh Naderi is an Assistant Professor at ICT Research Institute, since 2015. She received M.Sc. and Ph.D. degrees in Computer Engineering from Tarbiat Modares University (TMU), Tehran, Iran in 2003 and 2012 respectively. Her research interests include Biometrics, Image Enhancement, Intrusion Detection Systems, Machine Learning, and Knowledge-Based Systems.

Hossein Gharaee received B.Sc. degree in Electrical Engineering from K.N. Toosi University, of Technology in 1998, M.Sc. and Ph.D. degree in Electrical Engineering from Tarbiat Modares University, Tehran, Iran, in 2000 and 2009 respectively. Since 2009, he has been with the Department of Network Technology at ICT Research Institute (ITRC). He is currently Associate Professor at ITRC. His research interests include VLSI with emphasis on Basic Logic Circuits for Low-Voltage Low-Power Applications, DSP, Crypto Chip, and Intrusion Detection and Prevention Systems.

[DOI: 10.52547/itrc.14.2.1]