International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

Classification of Software Defined Network Traffic to provide Quality of Service

Sarika Nyaramneni[1], Bodepudi Narasimha[2], Nimma Harshitha[3], Pujari Rakesh[4], Thatishetti Shiva [5]

[1] *Assistant Professor,* Dept. *of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology Hyderabad, India*

[2, 3, 4, 5] *Student ,*Dept. *of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology Hyderabad, India*

Abstract - *Accurate traffic classification is of fundamental importance to numerous network activities, from security monitoring to accounting, and from Quality of Service to providing operators with useful forecasts for long-term provisioning. The initial stage in analysing and classifying the various types of applications running via a network is network traffic classification. This method allows network operators or internet service providers to control the overall performance of a network. We apply machine learning models to categorize traffic by application. This can be done by extracting the features of the traffic. This classified data can be used to stop unnecessary traffic and allow only user required traffic. Basically we prioritize the network traffic based on the features extracted during the classification. Features related to OTT are identified and we try to restrict them in the network for reducing the traffic in the network for providing better quality of service. We intend to stop traffic from Over-the-top(OTT) platforms like Netflix, Prime Videos, etc. Hence, by this the quality of service can be improved for user required applications.*

Key Words*: *Software-defined networks, Quality of service, Network traffic, classification, Over-the-top platforms.

1. INTRODUCTION

Network traffic is categorized in a variety of ways of extreme interest for both internet service providers and also network operators. It helps to classify the types of data flowing and link each one to the apps that produce it. This information is crucial for many purposes, including network monitoring, applications behavior and network security, and to improve Quality of Service(QoS).

The term "Software-defined networking" (SDN) refers to a method of networking where traffic on a network is controlled by application programming interfaces (APIs) or software-based controllers that communicate with the underlying hardware infrastructure This architecture is distinct from traditional networks, which employ specialized hardware to regulate network traffic (such as switches and routers). SDN can manage traditional hardware or create and manage virtual networks through software. Although software-defined networking provides a fresh way to control how data packets are routed through a single server, network virtualization enables organizations to segment different virtual networks within a single physical network or to connect devices on different physical networks to create a single virtual network. Compared to traditional networking, SDN is far more versatile since the control plane is software-based. Without adding extra hardware, it enables administrators to manage the network, alter configuration options, supply resources, and boost network capacity from a single user interface.

By providing a knowledge basis for identifying the performance levels required by applications, classification is a critical mechanism for traffic treatment. Deep Packet Inspection (DPI) and port-based classification are the two most used approaches for traffic classification. As more communication is encrypted and more apps use dynamic ports and ports for other well-known applications, these techniques are becoming outdated [1]. Machine Learning (ML), an alternate approach for traffic classification, employs the statistical characteristics of network traffic flows to address the basic issues with DPI and port-based categorization for encrypted flows.

Network traffic classification is a crucial component for managing infrastructure and ensuring the QoS for various applications. In reality, a thorough traffic classification process enables the effective management of already-available network resources, enabling more precise and reliable resource allocation systems [2].

The classification of network traffic can be carried out using the features related to the OTT platforms. The feature extraction is a process of recognising features and

attributes that often represent video streaming platforms or OTT platforms.

2. RELATED WORK

According to Meenaxi M Raikar et al. [3], accurate traffic classification is critical in network operations such as accounting for network consumption, security monitoring, and separating multiple network services' Quality of Service (QoS) components. The many basic network traffic classification (NTC) approaches have failed to achieve consistent accuracy. The machine learning (ML) and software defined network (SDN) architecture technologies were created to solve this problem. Naive Bayes (NB),Nearest Centroid (NC), and Support Vector Machine (SVM), were three supervised learning models that are used to categorize data traffic depending on applications. The NTC workflow includes data gathering, pre-processing of data, data labeling, model construction, data validation and prediction Flow characteristics are created from the network traffic traces and provided to the classifier for prediction. The nearest centroid (NC) is 90.12%, NB is 95.99%, and the accuracy for the SVM is 91.4%.

Yoshinobu Yamada et al. [4] have conducted a traffic prediction, which may be loosely divided into two categories: time-series analysis and machine learning(ML). They implemented a prioritizing technique for predicting mobile traffic [29] that enables us to use less traffic log data while retaining a satisfactory level of accuracy. The "important" traffic log data collects each base station and provides more crucial information to the server with a greater priority using this method. Both the prediction approach and the mechanism for determining the significance of each data entry were done using Random Forest. This study's disadvantage was the lack of use of additional machine learning (ML) techniques like DNN to increase prediction accuracy.

Kourosh Ahmadi et al. [5] have conducted an SDN controller that incorporates a fuzzy logic control system (FLCS) [30] to enhance QoS for various service flows. The path weight for a specific communication line is determined by the FLE-SDN controller using a fuzzy logic control mechanism after it continually gathers all communication's QoS measurements channels between different networks. The process ends with the determination of the best path for a specific service flow, after which forwarding devices are given instructions to modify their flow forwarding strategies. Particularly for real-time applications like audio and video, the FLE-SDN approach has a proven track record of assisting SDN controllers in trying to improve the architecture of various service flows and providing greater QoS. The limitation of this study was designing service flows with the goal of providing improved QoS, this technique has not been implemented on SDN controllers.

Rajat Chaudhary et al. [6] have developed an SDN-based QoS-aware traffic flow management system. The plan is broken down into three parts, each of which aims to speed up reaction time for incoming traffic. To eliminate inter-packet dependence, the incoming packets are first arranged linearly. By doing this, the packets won't have to wait at their destination. The sorted packets are then classified in the second stage based on the application type, packet size, and priority. The third step establishes a priority-based queuing system to control packet waiting times. This queuing model also incorporates queue migration and priority shifting algorithms to solve the issues of congestion and starvation. The obtained results clearly show the effectiveness of the suggested system with regard to several QoS criteria. The limitation of this study was compared to previous methods, the suggested plan displays less delay.

Thomas Favale et al. [7] analyzed modifications to the traffic patterns coming from the Politecnico di Torino (PoliTO) campus, where the Italian university is located. They focus on usage of the collaborative and remote working platforms, the acceptance of online learning, and campus traffic while also keeping an eye out for any changes in undesired or harmful communications. For all of the second semester's classes, which were due to begin on March 2, PoliTO decided to create an internal e-learning solution based on the BigBlueButton framework.. During the first week of March, the platform was created, set up, and tested before going live the following week to kick off the online semester. We take advantage of this special vantage point to monitor alterations in campus traffic and services.

Yang peng et al. [8] researched a reliable and effective technique for detecting network traffic anomalies. They start by creating an all-encompassing architecture that spells out how each stage, from data gathering to finalize the detection of anomaly and application, should work. Next, motivated by the precise and effective identification of large amounts of data, They propose a parallel subagging GRU-based method for detecting network traffic anomalies. They employ Spark platform to increase detection effectiveness, utilizing GA to enhance the training process and GRU to handle the long-term reliance that traffic data inevitably entails. They also seamlessly integrate subagging into GRU to lower the MSE and variance of every order term and broaden the applicability of their model. They carry out numerous rounds of comparison trials to confirm the effectiveness of their

suggested strategy. The experiment's findings demonstrate that PSB-MSE GRU's is enhanced and that it outperforms RNN approaches in terms of detection accuracy, reaching a level of up to about 99.8%. In addition, PSB-GRU provides larger efficiency gains as compared to the nonparallel approach.

Yanan Wanget al. [9] put forward a model for predicting network traffic based on intuitionistic fuzzy time series. In the realm of traffic forecasting, intuitionistic fuzzy time series models are utilized because of the abundance of complex and dynamic variables found in network traffic. The IFTS theory does a good job of describing the cloudy and unpredictable nature of data flow in networks. It is established what a long-term intuitionistic fuzzy time series is. (p−q) A model for forecasting an intuitionistic fuzzy time series with many inputs and outputs is called IFTS. This model significantly reduces the computational complexity. IFCM clustering is a technique that is enhanced during the training phase, and the clustering centroid similarity measure method is proposed. In place of the conventional absolute cluster centroid distance, the vector distance of the fuzzy time series with intuition is employed. The clustering centroid of their model has been demonstrated. This model is implemented on four distinct time scales using traffic information gathered by the WIDE project's MAWI working group from the Pacific Ocean backbone. To mimic trace flow collecting, the Wireshark network traffic analysis programme is used. The experiment shows that this model is more accurate, as evidenced by its reduced RMSE and AFER compared to other pertinent models. The LT-IFTS model is a useful and efficient tool for predicting network traffic.

Ren-hung Hwang et al. [10] introduced the D-PACK framework, an innovative early hazardous traffic detection system based on traffic auto-profiling (CNN), traffic sampling, and an unsupervised DL model (autoencoder).Their system can drastically minimize the amount of traffic that has to be processed by focusing on reviewing the fewest packets and most bytes from each packet. The evaluation's findings demonstrate that, even with only two packets from each flow and 80 bytes from each packet being assessed, D-PACK can identify malicious traffic with an accuracy rate of 99%+ and less than 1% FNR and FPR. Furthermore, because fewer packets and bytes are being examined, it is expected to take significantly less time than earlier efforts to pre-process and detect flows .So, this framework's main benefit is that it makes detection quicker.

Damian Jankowski et al. [11] recognized malicious activities in software defined networks by using flow features. They processed flow features for the effective classification of the traffic. It was considered that in order to achieve an adequate degree of malicious traffic detection, extra and basic flow characteristics must be integrated with data of the application layer. The feature and its corresponding weight are used to recognize the malicious attack.

In the process to increase the Quality of Service for a network, M.A.Ridwan et al. [12] suggests two Machine Learning based predictive routing algorithms that use classification and regression techniques. Their research compares the network performance of the routing algorithms based on regression and classification, respectively, known as RgRoute and ClassRoute. They suggested regression-based routing, according to their simulation findings, reduces the time approximately by 52% when compared with approach based on classification.

Yuyang Zhou et al. [13] introduced a novel intrusion detection system that is centered on ensemble learning and feature selection approaches. In the first stage, a heuristic strategy named CFS(Clustered File System)-BA for dimensionality reduction is presented which selects an optimal subset which relies on correlation among the extracted features. Afterwards, they developed an ensemble method that integrates the Random Forest, C4.5 and Forest by Penalizing Attributes algorithms. Finally, the voting mechanism was utilized for merging the probability distributions of training sets for the recognition of the attack. Their experimental findings for the dataset(NSL-KDD) is remarkable, with accuracy in classification of 99.81%, 0.08% FAR and 99.8%DR along with accuracy in classification of 99.52% and 0.15% FAR for the subsets consisting only 10 and 8 features respectively.

Muhammad Shafiq et al. [14] suggested a feature selection metric method which was termed as CorrAUC, and then they developed and designed Corrauc, which is a new algorithm for feature selection that depends on the wrapper strategy to properly filter the features and pick up useful features from Bot-IoT dataset for the chosen MachineLearning algorithm by utilizing AUC(Area Under roc Curve) metric. Then, using a bijective soft set as a foundation, they combined TOPSIS and Shannon entropy for evaluating a set of characteristics for detecting fraudulent traffic in an IoT network. They used 4 different ML algorithms and experimental findings showed the proposed method is effective and may often provide outcomes of >96%.

Gianni D'Angelo et al. [15]suggested a model that begins with statistical characteristics (basic features), taken from traffic flows over a predetermined time period, and

creates additional features that explain the correlations between the features (spatial features), as well as changes in those features over time (temporal features). They suggested a deep architecture made up of neural networks based on autoencoders (AEs). The autoencoder's encode-decode function contains various combinations of recurrent and convolutional network layers in order to extract such information. The following combinations were looked into: CNN, LSTM, ConvLSTM, CNN-LSTM, and Stacked-CNN-LSTM. The LSTM recurrent network was used to extract temporal features, while the convolutional network was utilized to extract spatial features.

A model that utilizes a novel strategy for relaxing the hypothesis of independence between the Naive Bayes algorithm's attributes was put out by Klenilmar Lopes Dias et al. [16]. Their report claims that by 2022, video streaming apps would account for more than 60% of all Internet traffic, with predictions that this percentage will continue to rise. But very few studies make an effort to comprehend the network properties of this traffic. These studies [18] include one that looks into the network properties of the two most widely used streaming services, Netflix and YouTube.

Dmitri Bekerman et al. [17] put forth a supervised end-to-end method for identifying malware using network traffic analysis. The suggested technique pulls 972 behavioral characteristics from various network levels and protocols. The most important characteristics are then determined, and the data dimensionality is decreased to a manageable level using a feature selection approach. To identify malicious network traffic and find new risks, multiple supervised algorithms are assessed. their analysis of the timeline reveals that several cases of unknown malware might have been discovered at least one month earlier their static criteria were added to Snort or Suricata systems.

Shi Dong et al. [19] introduced the cost-sensitive Support Vector Machine (CMSVM) method, an upgraded version of the support vector machine technique, to address the imbalance issue in network traffic detection. CMSVM uses an active learning multi-class SVM algorithm that dynamically weights applications. Models of various learning methods were developed and their performances were compared using the MOORE SET and NOC SET datasets. The suggested algorithm's effectiveness in comparison to the other three algorithms is demonstrated by performance analysis using the SVM, ROS, and RUS algorithms.

Pedro Amaral et al. [20] In this paper control plane software was implemented in Software Defined Networks along with implementing the OpenFlow method's built-in data collecting techniques for the applications under machine learning control. They said something about a straightforward architecture used in a corporate network which uses the OpenFlow protocol to acquire traffic statistics. Their results demonstrate that supervised learning techniques could be utilized with such an architecture and indeed the data it gathers with high degrees of accuracy for classification.

Deep-Full-Range, developed by Yi Zeng et al. [21], is a lightweight system for classified encrypted communication and intrusion detection (DFR). They introduced the Deep-Full-Range (DFR) framework, which combines three deep learning algorithms: Convolutional Neural Network [22], Stacked Auto-Encoder (SAE) [24] and Long Short-Term Memory (LSTM) [23] to classify network encrypted traffic and identify intrusions. They employed CNN to extract characteristics from the raw traffic's spatial distribution. The time-related aspect's properties are learned using LSTM.

Anderson Santos da Silva et al. [25] presented an architecture in this study to gather, expand, and choose flow characteristics for traffic classification in networks based on OpenFlow. It provides a wide range of flow characteristics that may be examined, improved, and evaluated to discover the best subset of information to categorize various traffic flow patterns. As comparing to classification accuracy achieved with the whole collection of flow characteristics, the subset of flow features identified either by the PCA(Principal Component Analysis) or GA(Genetic algorithm) provides for a much more accurate traffic categorization in all circumstances. The experiment results of their idea reveals that several aspects stand out as significant and take the top spots for the categorization of various experimental scenarios' unique flows.

To categorize network traffic, Isadora P. Possebon el al. [26] presented a comparison of individual classifiers and meta learning strategies. They looked into and assessed several meta learning strategies, such as boosting, bagging, stacking, and voting. Based on real-world tools and data, meta-learning algorithms clearly outperformed their base classifiers, primarily due to the base classifiers having low correlation. The frequency of false positives was decreased because of the ensemble learners, excluding stacking because of the information it gains on its initial level.

3. PROPOSED METHODOLOGY

This section provides specifics on the suggested method for building a network classifier that can exploit the features specific to OTT platforms [31]. The feature extraction is the paramount section of the project. It can be done by extracting the features related to OTT platforms.

A helpful tool for file analysis and network traffic monitoring is packet capture (PCAP). Utilizing tools for packet collection, like Wireshark, you may capture network traffic and transform it into a format that is readable by humans. For a variety of reasons, networks are viewed by PCAP [32]. Some of the most typical ones include tracking bandwidth use, identifying malicious DHCP servers, spotting malware, DNS resolution, and incident response. In order to study the network properties, PCAP files are utilized. By using these qualities, features that will be utilized for categorization will be extracted. By utilizing their unique qualities, we hope to identify network traffic coming from OTT services. In comparison to earlier articles, we intend to employ more features for classifications. This results in higher accuracy rates.

The bulk of the known models employ convolutional neural networks, long-short term neural networks, and other machine learning techniques like Naive Bayes, Random Forest, Forest PA, C4.5, Support Vector Machine, etc. We suggest an ensemble model for classification. An ensemble model is an approach that combines more than one machine learning model in the classification process. We intend to use Random Forest, C4.5 and SVM(Support Vector Machine) to form an ensemble model.

After classifying network traffic to its application, in the deployment state, traffic from OTT platforms will be restricted and we prioritize the network traffic specific to the application. We prioritize the network traffic based on the features extracted during the classification. Features related to OTT are identified and we try to restrict them in the network for reducing the traffic in the network for providing better quality of service.

4. CONCLUSION

In this study, we conducted extensive research on network classification and examined numerous research papers on various classification models. Many papers presented feature extraction algorithms for classifying network traffic to its application. A significant amount of work is required to extract specific features of OTT platforms. We intend to restrict network traffic from OTT platforms. This lessens traffic and raises quality of service as a result.

REFERENCES

[1] H. Shi, H. Li, D. Zhang, C. Cheng, W. Wu, Efficient and robust feature extraction and selection for traffic classification, Comput. Netw. 119 (2017) 1–16.

[2] M. Finsterbusch, C. Richter, E. Rocha, J.-A. Muller, K. Hanssgen, A survey of payload-based traffic classification approaches, IEEE Commun. Surv. Tut. 16 (2) (2014) 1135–1156 doi: https://doi.org/10.1016/j.media.2020.101813

[3] Meenaxi M Raikara, Meena S Mb, Mohammed Moin Mullac, Nagashree S Shetty, Meghana Karanandie,Data Traffic Classification in Software Defined Networks (SDN) using supervised-learning,ScienceDirect 171 (2020) 2750–2759

[4] Yoshinobu Yamada, Ryoichi Shinkuma, Takehiro Sato, and Eiji Oki Graduate School of Informatics, Kyoto University Yoshida-honmachi, Sakyo-ku, Kyoto, 606-8501, Japan, Feature-selection based data prioritization in mobile traffic prediction using machine learning , 978-1-5386-4727-1/18/$31.00 ©2018 IEEE

[5] Amirhossein Moravejosharieh ,Kourosh Ahmadi ,Saghir Ahmad , A Fuzzy Logic Approach To Increase Quality of Service in Software Defined Networking, Communication Control and Networking (ICCC 2018)

[6] Gagangeet Singh Aujla,Rajat Chaudhary,Neeraj Kumar, An Ensembled Scheme for QoS-aware Traffic Flow Management in Software Defined Networks, 978-1-5386-3180-5/18/$31.00 ©2018 IEEE

[7] Thomas Favale, Francesca Soroa , Martino Trevisana, Idilio Drago b, Marco Mellia, Campus traffic and e-Learning during COVID-19 pandemic.Computer Networks 176 (2020) 107290.

[8] Xiaoling Tao, Yang Peng, Feng Zhao, Changsong Yang, Baohua Qiang, Yufeng Wang, Zuobin Xiong, Gated recurrent unit-based parallel network traffic anomaly detection using subagging ensembles.Ad Hoc Networks 116 (2021) 102465.

[9] Xiaoshi Fana, Yanan Wang , Mengyu Zhang. Network traffic forecasting model based on long-term intuitionistic fuzzy time series Information Sciences 506 (2020) 131–147.

[10] REN-HUNG HWANG, (Senior Member, IEEE), MIN-CHUN PENG, CHIEN-WEI HUANG, PO-CHING LIN, AND VAN-LINH NGUYEN, (Member, IEEE). An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection.Digital Object Identifier 10.1109/ACCESS.2020.2973023

[11] D. Jankowski and M. Amanowicz, "A study on flow features selection for malicious activities detection in software defined networks," 2018 International Conference on Military Communications and Information Systems (ICMCIS), 2018, pp. 1-9, doi: 10.1109/ICMCIS.2018.8398697.

[12] Ridwana, M. A., N. A. M. Radzib, and F. Abdullah. "Quality-of-Service Performance Comparison: Machine Learning Regression and Classification-Based Predictive Routing Algorithm." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.14 (2021): 2808-2817.

[13] Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai,Building an efficient intrusion detection system based on feature selection and ensemble classifier,Computer Networks,Volume 174,2020,107247,ISSN1389-1286, https://doi.org/10.1016/j.comnet.2020.107247.

[14] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March 1, 2021, doi: 10.1109/JIOT.2020.3002255.

[15] Gianni D'Angelo, Francesco Palmieri, Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial–temporal features extraction, Journal of Network and Computer Applications, Volume 173, 2021, 102890, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102890.

[16] Klenilmar Lopes Dias, Mateus Almeida Pongelupe, Walmir Matos Caminhas, Luciano de Errico, An innovative approach for real-time network traffic classification, Computer Networks, Volume 158, 2019, Pages 143-157, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2019.04.004

[17] D. Bekerman, B. Shapira, L. Rokach and A. Bar, "Unknown malware detection using network traffic classification," 2015 IEEE Conference on Communications and Network Security (CNS), 2015, pp. 134-142, doi: 10.1109/CNS.2015.7346821.

[18] A. Rao, A. Legout, Y.-s. Lim, D. Towsley, C. Barakat, W. Dabbous, Network characteristics of video streaming traffic, in: Proceedings of the Seventh Conference on Emerging Networking Experiments and Technologies, ACM, 2011, pp. 1–12

[19] Shi Dong, Multi class SVM algorithm with active learning for network traffic classification, Expert Systems with Applications, Volume 176, 2021, 114885, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2021.114885.

[20] P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares and H. S. Mamede, "Machine Learning in Software Defined Networks: Data collection and traffic classification," 2016 IEEE 24th International Conference on Network Protocols (ICNP), 2016, pp. 1-5, doi: 10.1109/ICNP.2016.7785327.

[21] Y. Zeng, H. Gu, W. Wei and Y. Guo, "Deep-Full-Range : A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework," in IEEE Access, vol. 7, pp. 45182-45190, 2019, doi: 10.1109/ACCESS.2019.2908225.

[22] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in Advances in neural information processing systems, 2012, pp. 1097–1105.

[23] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural computation, vol. 9, no. 8, pp. 1735–1780, 1997.

[24] P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P.-A. Manzagol, "Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion," Journal of machine learning research, vol. 11, no. 12, pp. 3371–3408, 2010.

[25] A. Santos Da Silva, C. C. Machado, R. V. Bisol, L. Z. Granville and A. Schaeffer-Filho, "Identification and Selection of Flow Features for Accurate Traffic Classification in SDN," 2015 IEEE 14th International Symposium on Network Computing and Applications, 2015, pp. 134-141, doi: 10.1109/NCA.2015.12.

[26] Erman, Jeffrey & Arlitt, Martin & Mahanti, Anirban. (2006). Traffic Classification Using Clustering Algorithms. Proceedings of the 2006 SIGCOMM Workshop on Mining Network Data, MineNet'06. 2006. 281-286. 10.1145/1162678.1162679.

[27] Li, Wei & Moore, Andrew. (2007). A Machine Learning Approach for Efficient Traffic Classification. 310 - 317. 10.1109/MASCOTS.2007.2.

[28] I. P. Possebon, A. S. Silva, L. Z. Granville, A. Schaeffer-Filho and A. Marnerides, "Improved Network Traffic Classification Using Ensemble Learning," 2019 IEEE Symposium on Computers and Communications (ISCC), 2019, pp. 1-6, doi: 10.1109/ISCC47284.2019.8969637.

[29] Diala Naboulsi, Student Member, IEEE, Marco Fiore, Member, IEEE, Stephane Ribot, Razvan Stanica, Member, IEEE ,Large-scale Mobile Traffic Analysis: a Survey,1553-877X (c) 2015 IEEE

[30] D. A. Rutherford and G. A. Carter , Fuzzy Logic in Control Systems: Fuzzy Logic Controller, 0018-9472/90/0300-0404$01.00 2019 IEEE

[31] Syazwina Binti Alias, Selvakumar Manickam, Mohammed M. Kadhum, A Study on Packet Capture Mechanisms in Real Time Network Traffic, 978-1-4799-2758-6/13 $31.00 © 2013 IEEEDOI 10.1109/ACSAT.2013.95