Journal of Theoretical and Applied Information Technology
31st January 2023. Vol.101. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MACHINE LEARNING TECHNIQUE IN QOS MANAGEMENT NETWORK

ZHUNUSSOV A.[1], BAIKENOV A.[2], ZHELTAYEV T.[3], SERIKOV T.[4], ZIYEKENOV T.[5]
[1,2,3,5] Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Kazakhstan

[4] Kazakh Agrotechnical University named after S.Seifullina, Nur-Sultan, Kazakhstan

E-mail: [1]jarmale@mail.ru, [2] a.baikenov@aues.kz, [3]zheltayev@gmail.com, [4]tansaule_s@mail.ru. [5]toktalyk@mail.ru.

ABSTRACT

Modern telecommunication systems and data transmission networks generate large volumes of heterogeneous traffic. In such networks, traditional network management methods for monitoring and analyzing data have some problems in terms of accuracy and efficient processing of big data in real time. The purpose of the study is to show how the value of the number of PPPoE PADT session break packets sent by the router indicates the presence of packet loss along the way. The PPPoE protocol works on the client-server principle, which is mainly used in broadband networks, by encapsulating PPP frames within an Ethernet frame. Using the PPPoE protocol, operators can control the access and operation of subscriber connections, as well as manage a large number of connections at one point in the network. It is proposed to use a machine learning method that will automate the process of tracking the quality of services provided using information from PPPoE sessions in a specific VLAN at specified time intervals. The article analyzes statistics from PPPoE sessions collected in 8 directions of VLANs providing various types of services. Found and fixed problems in the direction of VLAN112, which were associated with signal distortion in the section of the radio relay link along the route. Based on the test results, the proposed method makes it possible to identify a malfunction without involving additional technological resources. To store statistics, you need to allocate memory on the server for each direction and configure PPPoE.

Keywords: *QoS management, PPPoE, PADT, VLAN, Machine learning, Monitoring*

1. INTRODUCTION

In modern networks, traditional QoS methods for monitoring and analyzing data have some problems, such as accuracy and efficient processing of big data in real time. Machine learning is effectively used to facilitate the analysis and identification of problems in systems with a large amount of data to recognize hidden and complex patterns [1]. To help make an informed decision on the choice of the appropriate learning algorithm to meet the specific requirements of the application, it is necessary to know the advantages and disadvantages of machine learning algorithms in terms of their application [2], [3].

In our time, the bulk of traffic falls on the use of the Internet. This causes exponential growth in data and traffic over the Internet. Classification of Internet traffic is a very popular tool in relation to information discovery systems. Although so many methods have been developed to effectively classify Internet traffic, machine learning methods are the most popular among them [4]-[8]. IoT devices are driving the generation of large amounts of data in real time. IoT devices have become ubiquitous, such as sensors and actuators. This has led to what is an attractive target for using ML systems. Deploying machine learning systems on edge computing devices removes problems with high latency, increased communication costs and privacy, allowing calculations to be performed near data sources [9].

Machine learning can also be applied in traffic analysis and software failure prediction. In [10], a comparison was made between the performance of machine learning and statistical methods based on Software Fault Prediction models. This empirical study and analysis shows that the predictive ability of machine learning methods to classify a class/module as error-prone/non-error-prone is better than classical statistical models. The performance of machine learning based SFP methods in terms of failure susceptibility is higher than for conventional statistical purposes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Traffic analysis in a data network has many purposes, such as evaluating the performance and security of network operations and management. Therefore, network traffic analysis is considered vital to improve the performance and security of networks. The application of machine learning methods in the field of traffic analysis demonstrates effective possibilities in solving network problems [11]. An interdisciplinary combination of IP network methods and data mining makes it possible to conduct a qualitative analysis of existing IP networks and identify bottlenecks [12].

In the field of mobile technologies, machine learning methods are already being explored [13], aimed at providing optimal configurations, optimizing mobile communications, computing and resource allocation [14]. The paper [15] proposes the concept of machine learning strategies for solving wireless sensor network design problems.

If the implementation of third-party software modules in traditional networks is a difficult task, then the use of machine learning in software-defined SDN networks makes it possible to predict and provide the quality of service specified by the customer and reduce the load on network equipment by reducing the amount of signal traffic in the network [16]-[21]. Moreover, machine-learning algorithms are used to identify and classify conflicting flows. As a result, several machine learning algorithms are presented in [22], which include a decision tree (DT), a support vector machine (SVM), an extremely fast decision tree (EFDT) and a hybrid (DT -SVM) to detect and classify conflicting streams in SDN. The proposed EFDT and hybrid DT-SVM algorithms demonstrate the high ability of SDN applications to provide fast detection and classification of conflict flows. Accurate classification of traffic over SDN is fundamental to many other network operations, from monitoring security to accounting and from QoS to providing operators with useful predictions for long-term service delivery [23], [24]. For SDN, one of the security concerns is a DDoS attack. A DDoS attack poses a threat to the Internet. To prevent a DDoS attack, you can use the machine-learning algorithm [25]-[28].

With SDN as the leading technology for enabling 5G mobile communication systems, the focus is on reducing operating costs while improving QoS by taking advantage of queuing and multipath forwarding in OpenFlow, providing the operator networks with support for SDN efficient distribution of network resources, taking into account mobility and reducing or even eliminating the need for overprovisioning [29].

The idea of machine learning demonstrates the fact that a computer can improve itself over time. The study [30] showed that machine-learning strategies in terms of a computer are controlled, unsupervised and semi-supervised. The most recent applications of machine learning are object detection, object classification, and extracting relevant information from images, graphics documents, and videos.

Based on this review, we can say that the use of machine learning methods today is a relevant direction, as network monitoring is becoming more and more complex due to the growth of traffic requirements. By introducing these methods in various fields of science and technology, you can come to faster and better solutions. In this article, a machine learning method has been developed that provides a search for bottlenecks in a telecommunications network when monitoring the quality of services [31]-[36]. According to a review of publications, it can be concluded that the PPPoE protocol has been explored more in terms of customization for different software, and has been used by service providers as an auxiliary mechanism to distinguish between end hosts connected via Ethernet and access device. Normally, PPP uses the LCP protocol to close the PPP link. However, the PPPoE specification allows you to disable the connection using a special PADT packet. The client will recognize this packet and will properly terminate the session if it receives a request to terminate the PPP session. Either the client or the server may terminate an established PPPoE session at any time by sending this packet. The PADT package setting is disabled by default. Ending a session can be for various reasons and not always a successful session. Previously, little importance was attached to the study of this type of packet in terms of information about the presence of a malfunction. For example, a PADT message for a broadband access network on loss of connection with a client may indicate a loss of DSL synchronization on the corresponding subscriber line. Moreover, it can be said that the use of machine learning methods in the study of this issue has not been deeply studied in foreign and domestic publications. The proposed method involves the use of data on the router about the end of the PPPoE session of PADT type values, which indirectly indicate the presence of bottlenecks, which was first proposed by the authors of this publication at the conference [37]. The novelty of the proposed method in this article lies in

Journal of Theoretical and Applied Information Technology
31st January 2023. Vol.101. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the fact that machine learning technology is used to automate the collection of statistics on PPPoE sessions of PADT values. 8 VLAN destinations are being explored providing different types of services. The machine learning-based method monitors the state of the PPPoE session along the VLAN route, collects data from the router at specified time intervals and sends it to the server, where the collected data from the tables is analyzed. The result obtained in the form of diagrams shows in which direction it is necessary to diagnose the service.

2. METHOD

The PPPoE protocol works on the client-server principle, which is mainly used in broadband networks, by encapsulating PPP frames within an Ethernet frame. Using the PPPoE protocol, operators can control the access and operation of subscriber connections, as well as manage a large number of connections at one point in the network. The principle of operation is that when the system is initialized, the PPPoE client establishes a session with the access server by exchanging a series of packets [38]:

1) A PPPoE Active Discovery Initiation (PADI) packet initiates communication with the server and contains a service request.

2) The server responds to the PADI request by sending a PPPoE Active Discovery Offer (PADO) packet containing the server name and the service being offered.

3) In response to PADO, the client sends a PPPoE Active Discovery Request (PADR) packet to accept the service. If a client receives PADO from multiple servers, it selects one based on the name or type of service offered.

4) When the server receives a PADR packet, it sends a PPPoE Active Discovery Session-confirmation (PADS) packet, which confirms the connection.

5) At any point in the session, the server or client MAY send a PPPoE Active Discovery Termination (PADT) packet to end the session.

Since telecom operators usually allocate a separate VLAN for each type of service, therefore, each VLAN is registered along its own path, starting from the router to the client. The scheme under study is shown in Figure 1 and consists of 8 main services allocated in VLAN.

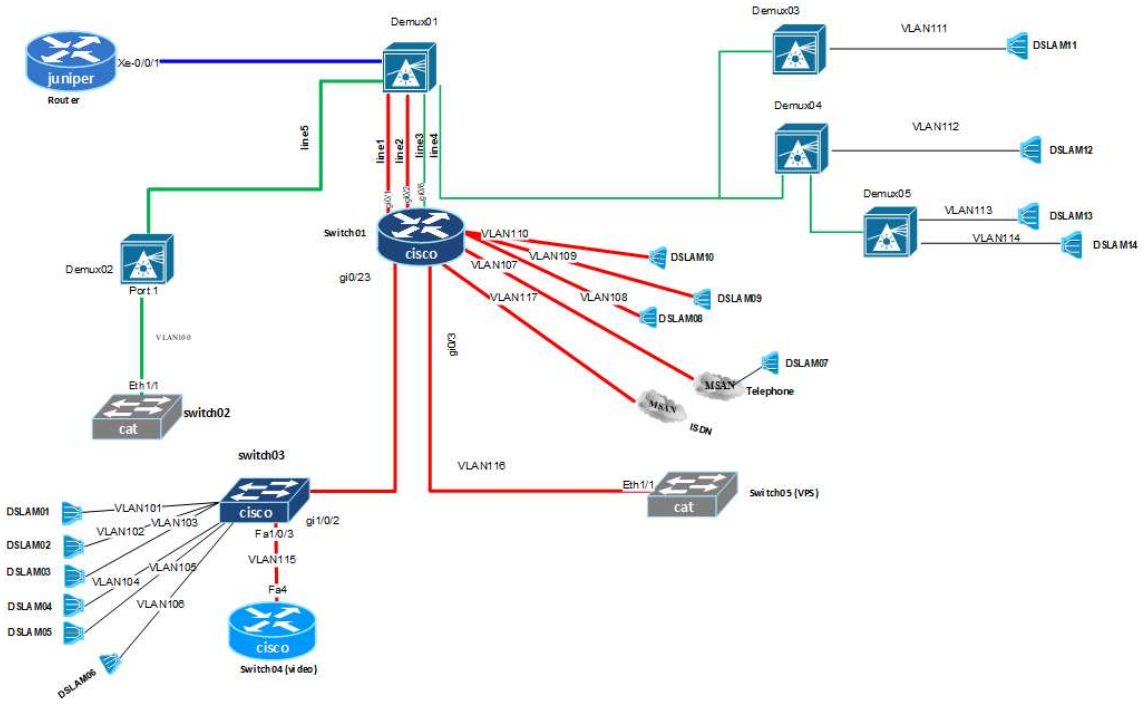

Figure 1: PPPoE network architecture

Statistics will be collected within 2 weeks for 8 dedicated services [39]. Considering the fact that PADT packets will be dropped on one path during peak hours, one can say that there is a

Journal of Theoretical and Applied Information Technology
31st January 2023. Vol.101. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

bottleneck in this direction of service provision. To understand the growth trend of dropped packets in the direction, it is necessary to calculate the ratio of dropped packets using the formula:

$$K = (PADT2 – PADT1) / S, \quad (1)$$

where K is the rate of dropped packets,

PADT2 - value of sent PADT packets during polling t2,

PADT1 - value of sent PADT packets during polling t1,

S is the arithmetic mean of the total number of sessions in the time interval (t2-t1).

The packet drop rate reveals the percentage of failed authorization attempts [39], [40].

To optimize the collection of PADT package statistics and search for bottlenecks, it is proposed to use machine learning techniques. For this, a Python script was developed that allows you to collect data from the router at specified time intervals and send it to the server, where the collected data from tables is converted into charts. For visual convenience, the ratio is measured as a percentage.

How the crypt works:

Step 1: Start collecting statistics every 5 minutes for each PPPoE VLAN from all network routers in selected directions.

Step 2: Formation of PADT data tables.

Step 3: Calculation of the packet drop rate based on the sent PADTs.

Step 4: Comparison of the coefficient calculation data with the norm.

Step 5: In case of compliance with the norm, go to step 8.

Step 6: If the values deviate from the norm, the route and the list of equipment for testing are detected.

Step 7: The specified parameters are checked along the VLAN route:

a. CRC and Reset errors on the physical interfaces of routers and switches.

b. Speed, bandwidth and MTU.

c. The presence of a wireless network and RRL in the route.

d. CPU load and processes on the equipment along the track.

Step 8: Static data is collected in the database and the counters are updated.

Step 9: Displaying the results of checks and alerting by coincidence.

The advantage of tracking the quality of services provided in a telecommunications network using the analysis of PPPoE packet statistics is the absence of additional financial costs for technological resources. The disadvantages include the mandatory availability of free space on the server for each direction, as well as the mandatory configuration of the PPPoE protocol.

3. RESULTS AND DISCUSSION

8 directions were chosen for collecting statistics. Figure 2 shows the values of the rate of dropped packets in the period under consideration (2 weeks) for 8 VLAN directions, formed as a result of the script.

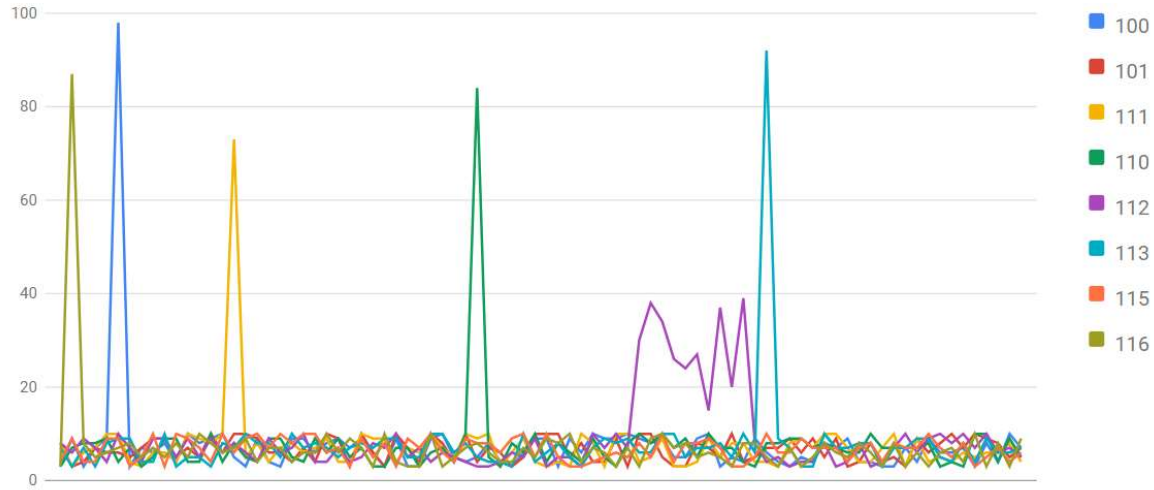

Figure 2: PPPoE Packet Statistics

Journal of Theoretical and Applied Information Technology
31st January 2023. Vol.101. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As can be seen from the graph, in the directions of VLAN116, VLAN100, VLAN111, VLAN110, VLAN112, VLAN113 there were single bursts that lasted a short period of time. For direction VLAN112, there was a period when the value of the packet drop rate exceeded 8% longer than other directions. Following the hypothesis put forward in the article, the deviation from the norm of the values of the packet loss coefficient indicates the presence of problems in this direction. Therefore, we conclude that in the direction of VLAN112 it is necessary to carry out troubleshooting. To do this, first select the track and the list of equipment for testing. In our case, the following route is defined: router - demultiplector - demultiplexer - concentrator - subscriber. Next, PADT packet statistics are collected. Table 1 shows statistics for one session.

Table 1. Active PPPoE sessions: 289

Packet Type	Sent	Received
PADI	0	10431298
PADO	258974	0
PADR	0	210422
PADS	208596	0
PADT	**75786**	**1592062**

PPPoE packet statistics for VLAN112 shows that the session is frequently initiated, which indirectly indicates that there are problems in this direction.

Further, according to the principle of the script, the specified parameters are checked along the VLAN route. It was found that there is a wireless network and radio relay line (RRL) on the subscriber side, CRC and Reset errors on the physical interfaces of routers and switches are within normal limits, speed, bandwidth and MTU are within normal limits, CPU load and processes on equipment along the route are also within normal limits.

According to the analysis, a problem with a distorted signal was detected on a section of the radio relay communication line along the VLAN112 route. After the problem was fixed, the drop rate for VLAN112 decreased to normal (Figure 3).

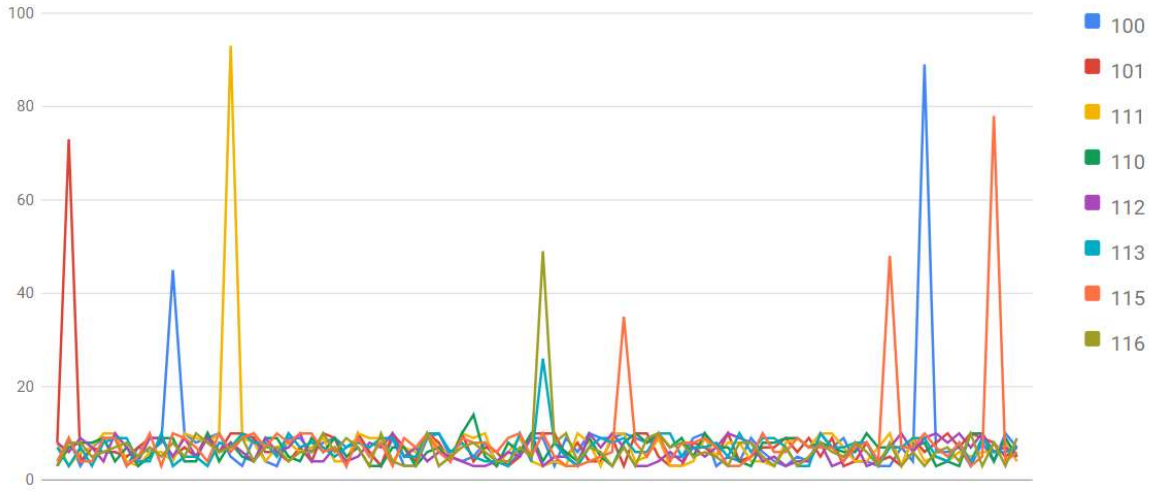

Figure :. PPPoE Packet statistics after troubleshooting in VLAN112 direction

In the course of monitoring the working telecommunications network of the country's largest provider, confirmation of the hypothesis put forward was obtained. The data collected for 2 months with a frequency of 5 minutes for eight VLANs occupied 98 megabytes of memory on the server.

4. CONCLUSION

The results of research show that one of the ways to ensure QoS can be the setting of a structure that allows you to classify traffic and guarantee compliance with service levels by monitoring traffic. The parameter selected for this monitoring is the tracking of packet values from sessions of the PPPoE protocol type PADT for broadband network access and is implemented using machine learning tools.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The studies carried out in this work demonstrate the possibility of including the QoS mechanism in the architectural protocol PPPoE without changing the standard protocol. PPPoE is quite stable and has proven itself well in practice. 8 VLAN destinations were explored that provide different types of services. Found and fixed problems in the direction of VLAN112, which were associated with a distorted signal on a segment of the radio relay link along the path. Based on the test results, the proposed method makes it possible to detect a malfunction without involving additional technological resources. In the future, it is planned to use a deep learning model, increase the variety of fault tracking parameters, and discuss the effectiveness and performance of the method.

REFERENCES

[1] M. Abbasi, A. Shahraki, A. Taherkordi. Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey. Computer Communications, vol. 170, Mar. 2021, pp. 19-41, doi: 10.1016/j.comcom.2021.01.021.

[2] S. Ray. Quick Review of Machine Learning Algorithms. Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019, India, pp. 36-39, 2019, doi: 10.1109/COMITCon.2019.8862451.

[3] M. L. O. de Andres, A. Poniszewska-Maranda, L. A. Hernandez Gomez. (2020). Towards the Machine Learning Algorithms in Telecommunications Business Environment. Lecture Notes in Business Information Processing 402, doi: 10.1007/978-3-030-63396-7_6.

[4] N. Namdev, S. Agrawal, S. Silkari. Recent advancement in machine learning based internet traffic classification. Procedia Computer Science, vol. 60, pp. 784-791, 2015, doi: 10.1016/j.procs.2015.08.238.

[5] F. Pacheco, E. Exposito, M. Gineste. A framework to classify heterogeneous Internet traffic with Machine Learning and Deep Learning techniques for satellite communications. Computer Networks, vol. 173. doi: 10.1016/j.comnet.2020.107213.

[6] V. Labayen, E. Magana, D. Morato, M. Izal. Online classification of user activities using machine learning on network traffic. Computer Networks, vol. 181, 2020, doi: 10.1016/j.comnet.2020.107557.

[7] S. Suthaharan. Big data classification: Problems and challenges in network intrusion prediction with machine learning. Performance Evaluation Review, vol. 41, no. 4, pp.70-73, 2014, doi:10.1145/2627534.2627557.

[8] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, F. Abdessamia. Network Traffic Classification techniques and comparative analysis using Machine Learning algorithms. 2nd IEEE International Conference on Computer and Communications, ICCC 2016 – Proceedings, pp. 2451-2455, 2016, doi: 10.1109/CompComm.2016.7925139.

[9] M. G. Sarwar Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan, F. Hussain. Machine Learning at the Network Edge: A Surve. ACM Computing Surveys, vol. 54, no. 8, pp. 1-37, Nov. 2022, doi: 10.1145/3469029.

[10] S. K. Pandey, R. B. Mishra, Tripathi, A. K. Machine learning based methods for software fault prediction: A survey. Expert Systems with Applications, vol.172, 2021, Art. no. 114595, doi:10.1016/j.eswa.2021.114595.

[11] N. Alqudah, Q. Yaseen. Machine Learning for Traffic Analysis: A Review. Procedia Computer Science, vol.170, pp.911-916, 2020, doi: 10.1016/j.procs.2020.03.111.

[12] T. T. T. Nguyen, G. Armitage. A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys and Tutorials, vol. 10, no 4, pp.56-76, 2008, doi: 10.1109/SURV.2008.080406.

[13] A. Nacef, A. Kaci, Y. Aklouf, D. L. C. Dutra. Machine learning based fast self optimized and life cycle management network. Computer Networks, vol. 209, 2022, doi: 10.1016/j.comnet.2022.108895.

[14] O. Nassef, W. Sun, H. Purmehdi, M. Tatipamula, T. Mahmoodi. A survey: Distributed Machine Learning for 5G and beyond. Computer Networks, vol. 207, 2022, doi: 10.1016/j.comnet.2022.108820.

[15] Z. A. Khan, A. Samad. A Study of Machine Learning in Wireless Sensor Network. International Journal of Computer Networks and Applications, vol. 4, no.4, 2017, doi: 10.22247/ijcna/2017/49122.

[16] C. Wang, L. Yuan, M. Medvetskyi, M. Beshley, A. Pryslupskyi, H. Beshley. Machine Learning-Enabled Software-Defined Networks for QoE Management.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2021 IEEE 4th International Conference on Advanced Information and Communication Technologies, AICT 2021 – Proceedings, 2021, doi: 10.1109/AICT52120.2021.9628961.

[17] Y. Zhao, B. Yan, D. Liu, Y. He, D. Wang, J. Zhang. SOON: self-optimizing optical networks with machine learning. Optics Express, vol. 26, no. 22, 2018, doi: 10.1364/oe.26.028713.

[18] W. S. Saif, M. A. Esmail, A. M. Ragheb, T. A. Alshawi, S. A. Alshebeili. Machine Learning Techniques for Optical Performance Monitoring and Modulation Format Identification: A Survey. IEEE Communications Surveys and Tutorials, vol. 22, no. 4, 2020, doi: 10.1109/COMST.2020.3018494.

[19] S. Ayoubi, N. Limam, M. A. Salahuddin, N. Shahriar, R. Boutaba, F. Estrada-Solano, O. M. Caicedo. Machine Learning for Cognitive Network Management. IEEE Communications Magazine, vol. 56, no. 1, Jan. 2018, doi: 10.1109/MCOM.2018.1700560.

[20] T. Serikov, A. Zhetpisbayeva, S. Mirzakulova, K. Zhetpisbayev, Z. Ibrayeva, Soboleva L. Application of the NARX neural network for predicting a one-dimensional time series. Eastern-European Journal of Enterprise Technologies, vol. 5, no. 4 (113), pp. 12-19, 2021. doi: https://doi.org/10.15587/1729-4061.2021. 242442.

[21] Zhumazhanov, B., Zhetpisbayeva, A., Zhetpisbayev, K., Nauryz, K., Kussainova, K. Modeling the Method for Determining the Stimulated Brillouin Scattering Threshold in a Single-Mode Optical Fiber. Eastern-European Journal of Enterprise Technologies, vol. 1, no. 5 (115), pp. 6-13, 2022. doi: https://doi.org/10.15587/1729-4061.2022.253390

[22] M. H. H. Khairi, S. H. S. Ariffin, N. M. A. A. Latiff, K. M. Yusof, M. K. Hassan, F. T. Al-Dhief, M. Hamdan, S. Khan, M. Hamzah. Detection and Classification of Conflict Flows in SDN Using Machine Learning Algorithms. IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3081629.

[23] M. Reza, M. Javad, S. Raouf, R. Javidan. Network Traffic Classification using Machine Learning Techniques over Software Defined Networks. International Journal of Advanced Computer Science and Applications, vol. 8, no. 7, Jan. 2017, doi: 10.14569/ijacsa.2017.080729.

[24] Z. Xiong, N. Zilberman. Do switches dream of machine learning?: Toward in-network classification. HotNets 2019 - Proceedings of the 18th ACM Workshop on Hot Topics in Networks, Nov. 2019, doi: 10.1145/3365609.3365864.

[25] A. Banitalebi Dehkordi, M. R. Soltanaghaei, F. Z. Boroujeni. The DDoS attacks detection through machine learning and statistical methods in SDN. Journal of Supercomputing, vol. 77, no. 3, pp. 2383-2415, Jun. 2021, doi: 10.1007/s11227-020-03323-w.

[26] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, P. Chinnasamy. Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques. 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, doi: 10.1109/ICCCI50826.2021.9402517.

[27] I. F. Kilincer, F. Ertam, A. Sengur. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, vol. 188, 2021, doi: 10.1016/j.comnet.2021.107840.

[28] O. Manankova, M.Yakubova, A. Baikenov. Cryptanalysis the SHA-256 Hash Function using Rainbow Tables. Indonesian Journal of Electrical Engineering and Informatics (IJEEI), vol. 10, no. 4, 2022. doi: 10.52549/ijeei.v10i4.4247

[29] M. Bagaa, D. L. C. Dutra, T. Taleb, K. Samdanis. On SDN-Driven Network Optimization and QoS Aware Routing Using Multiple Paths. IEEE Transactions on Wireless Communications, vol. 19, no. 7, 2020, doi: 10.1109/TWC.2020.2986408.

[30] A. I. Khan, S. Al-Habsi. Machine Learning in Computer Vision. Procedia Computer Science, vol. 167, pp. 1444-1451, 2020, doi: 10.1016/j.procs.2020.03.355.

[31] F. Liu, T. Xie, Y. Feng, D. Feng. On the security of PPPoE network. Security and Communication Networks, vol. 5, no. 10, pp. 1159-1168, 2012, doi: 10.1002/sec.512.

[32] T.Z. Teshabaev, M.Z. Yakubova, O.A. Manankova. Analysis, research and simulation of a multiservice network based on the Packet Tracer software package to determine the value of delays to increasing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

value size of ICMP packet. in International Conference on Information Science and Communications Technologies (ICISCT 2020), 2020, Art. no. 20486756, doi: 10.1109/ICISCT50599.2020.9351479.

[33] M.Z.Yakubova, O.A. Manankova, K.A. Tashev, G.S. Sadikova. Methodology of the determining for Pearson's criterion based on researching the value of delays in the transmitting of information over a multiservice network. in International Conference on Information Science and Communications Technologies (ICISCT 2020), 2020, Art. no. 20486776.

[34] A.Solochshenko, A.Baikenov, V.Tikhvinskiy, and J.Caiko. Research of Self – Organizing Networks (SON) Algorithms Efficiency Applying on Fourth – Generation Mobile Networks. Transport and Telecommunication Journal, vol.22, no.4, pp.444-452, 2021.

[35] O.A. Manankova, B.M. Yakubov, T.G. Serikov, M.Z. Yakubova, A.K. Mukasheva. Analysis and research of the security of a wireless telecommunications network based on the IP PBX Asterisk in an Opnet environment. Journal of Theoretical and Applied Information Technology, Vol.99, No.14, 2021, pp. 3617-3630.

[36] S.V. Konshin, M.Z.Yakubova, T.N. Nishanbayev, O.A. Manankova. Research and development of an IP network model based on PBX asterisk on the opnet modeler simulation package. International Conference on Information Science and Communications Technologies (ICISCT 2020), Article no. 20486746, doi: 10.1109/ICISCT50599.2020.9351405.

[37] A. Zhunussov, A. S. Baikenov, D. Ilieva. Monitoring the quality of services provided in a telecommunication network by analyzing the statistics of PPPoE packets. 2020 7th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE), 2020, pp. 1-4, doi: 10.1109/EEAE49144.2020.9279089.

[38] L. Mamakos, K. Lidl, J. Evarts. A Method for Transmitting PPP over Ethernet (PPPoE). RFC 2516 (Informational), 1999, https://www.ietf.org/rfc/rfc2516.txt, (accessed Mar. 8, 2019).

[39] S. Bradner. Benchmarking Terminology for Network Interconnection Devices. RFC 1242, 1991, https://www.ietf.org/rfc/rfc1242.txt (accessed Mar. 8, 2019).

[40] A. Morton. Round-Trip Packet Loss Metrics. RFC6673, https://ietf.org/rfc/rfc6673.txt (accessed Mar. 10, 2019).