As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(06): 25-33, 2023
Copyright © 2023International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0906004
Available online at: http://www.ijmtst.com/vol9issue06.html

A Review on SDN based on Mobilty, Security and Scalability Management

Ganga T G | Dr. J.Gowri

Department of ComputerScience and Applications, Srikrishna Arts and Science college,Coimbatore

To Cite this Article
Ganga T G and Dr. J.Gowri. A Review on SDN based on Mobilty, Security and Scalability Management. International Journal for Modern Trends in Science and Technology 2023, 9(06), pp. 25-33. https://doi.org/10.46501/IJMTST0906003

Article Info
Received: 28 April 2023; Accepted: 24 May 2023; Published: 30 May 2023.

ABSTRACT

In the new, impending era, the Internet hosts all business applications. Nearly all corporate apps went online simultaneously during this pandemic. The COVID-19 epidemic has resulted in a massive bandwidth flood on the Internet. This condition raises concerns for security, load balance, and traffic management. The revolutionary concept of Software Defined Networking (SDN), which is part of the next-generation trend, is developing alongside other network technologies. In SDN, the control and data planes are separated, allowing for the emergence of novel network features like centralized flow management and network programmability. These features promote the introduction of new and improved network functions in an effort to enhance key aspects of network deployment, such as flexibility, scalability, network-wide visibility, and cost-effectiveness. SDN is rapidly evolving, which is transforming it into a significant enabler for implementations in diverse network scenarios, such as datacenters, ISPs, corporate, academic, and home environments. However, the technology is still far from being seen as secure and dependable, which prevents its quick adoption. To decrease the adoption gap for SDN, the scientific community has been drawn to investigate SDN security in recent years. This paper reviews the machine learning techniques that are currently used in SDN for resource management, traffic classification, traffic prediction, routing optimization, and security management.

KEYWORDS:SDN – Traffic Classification and Prediction, Resource management,Security Management, Routing optimization

1. INTRODUCTION

The network architecture known as a legacy network has been used for a very long time. As a result, it is unable to handle problems with contemporary systems. In order to introduce programmability into the conventional network, legacy network mechanisms were investigated in the 1980s, followed by lively networks in the 1990s. According to [1], it is now difficult for the legacy network to manage new, powerful, and traditional systems applications effectively and efficiently [2]. The dynamic application with central/programmable features now performs worse in the conventional network. Software-defined networking (SDN), a new dynamic and scalable technology that has emerged as a revolutionary framework for the impending current Internet, was created to address the shortcomings of the legacy networks design. In order to process, store, and distribute data and applications effectively, the introduction of cloud computing and virtualization in database-centric architecture or data-centric architecture was investigated [3].

The management and setup of internet and ICT (information-centric technology) advancements, such as mobile, cloud, social networking, big data, multimedia, and the trend towards a digital society, have become extremely complex, difficult, and time-consuming. Additionally, having high bandwidth access, being able to expand, and having dynamic control are crucial, specifically when network devices are fully integrated. Therefore, it is recommended to employ a particular group of predefined line commands and an operating system or firmware. By separating the control plane from the data plane, SDN (software-defined networking) is a system created to streamline and improve network management with high flexibility. As a result, network programmability is improved, creating more potential for innovation. Despite being a relatively recent study topic, SDN has caught the interest of many academic and industrial research institutions.

To effectively perform network optimization, data analysis, and automated network service provisioning, machine learning models are trained on historical network data [4]. Recent advances in machine learning offer potential directions for using it in networking, according to the literature. SDN systems benefit from increased performance, effectiveness, and security thanks to machine learning. The performance, effectiveness and security, of the network can all be enhanced through machine learning-based SDN.

STRUCTURE OF PAPER

The paper is organized as follows: In Section 1, the introduction of the paper is provided along with the structure, important terms, objectives and overall description. In Section 2 we discuss machine learning algorithms for SDN. In Section 3 we have the complete information about routing optimization. Section 4 shares information about traffic prediction Section 5 tells us about the resorce management. Section 6 tells us about the security management. Section 7 tells about the future scope and concludes the paper with acknowledgement and references.

2. MACHINE LEARNING ALGORITHMS FOR SDN

SDN controller provides centralized network control and management with a global view of the networks. To add intelligence to SDN, machine learning methods can be employed separately or in conjunction with the various northbound applications of the SDN controller. Machine learning-based SDN controllers analyse and automate network data as well as optimize the network. This section surveys SDN-related machine learning-based research studies. We group the studies into four categories: resource management, route optimization, quality of service (QoS) prediction, and quality of experience (QoE) prediction.

2.1 Traffic Classification

The classification of traffic is essential to network administration. Network administrators can manage and distribute various services thanks to traffic classification. Dynamic port-based methods and machine learning are currently the most popular traffic classification techniques [5]. An OpenFlow-based SDN system is suggested for the data collecting in enterprise networks . The advantage of port-based methods, including deep packet inspection (DPI), is their high categorization accuracy. The categorization of applications based on the availability of patterns and the high processing cost to check network flow is DPI limitations. The traffic that is encrypted is invisible to DPI. As a result, machine learning-based algorithms are employed to analyze encrypted traffic at a minimal computational cost as opposed to classic DPI approaches. Massive amounts of traffic flow data must also be collected, and knowledge must be derived from the traffic data using machine learning techniques.

A two-stage approach with an effective learning cost in SDN is proposed by Xiao et al. [6] for the identification of elephant flow. The first step in separating questionable elephant flow from mic flow is to use a head packet measuring approach. Secondly, to determine if the suspicious traffic is an elephant flow or not, a decision tree classification model is used. To identify applications based on traffic flow, application-aware traffic classification is suggested in the literature.

A behavioral engine for UDP protocol-based application-aware traffic classification was proposed by Rossi et al. [7]. UDP traffic is classified using an SVM-based model with a classification accuracy of more than 90% using its Netflow records. For traffic classification that takes into account mobile applications, TrafficVision, an SDN-enabled edge network, is suggested [8].Traffic Vision Engine is the primary element of Traffic Vision (TV Engine). TV Engine collects data from access devices and end devices and stores it, as well as extracts flow statistics and data for ground truth training. Different applications are classified using a decision tree classifier model. The classification of different sorts of flow, such as video content, audio files, video chats, etc., however, is done using a KNN classifier-based model.

The traffic flow is divided into QoS classes using QoS-aware traffic classification. Various applications are given QoS classes depending on QoS criteria including jitter, latency, and loss rate. The most effective method for traffic flow classification, according to QoS classes, is traffic flow classification. For QoS aware traffic classification, a semi-supervised learning method and DPI-based approach are suggested [9]. The widely used applications are labeled using a DPI method. To categorize apps into known and unknown QoS classes, Laplacian SVM or other semi-supervised learning-based models are trained on the labeled data from DPI.

The SDN controller is subjected to machine learning techniques for the analysis of gathered traffic data. Traffic classification methods based on machine learning, like elephant flow-aware (EF), application-aware and QoS-aware methods. Traffic flow is categorized into elephant flow and mice flow using the EF traffic classification system. Elephant flows are strong, persistent, and bandwidth-hungry, whereas mice flows are weak and delay-intolerant. In data centers, there are 80 mouse flows while the remaining traffic is an elephant flow [10]. Elephant flow identification is crucial in such settings for effectively managing traffic flow. In paper [11], hybrid data center-based traffic flow scheduling difficulties are covered. At the edge, EF traffic classification is implemented using machine learning techniques; these research results are also used by SDN controller-based optimization algorithms for effective traffic flow management. Applications are classified using a variety of machine learning classifiers that have been learned using traffic flow. In paper [12], a hybrid strategy combining a multi-classifier and a DPI-based classifier is suggested for identifying and categorizing apps.

3. ROUTING OPTIMIZATION

The optimal decision, option, or selection with relation to a particular measure, model, or criterion is chosen from a pool of alternatives in mathematical optimization. Optimal route suggestion [13], optimal policy-making [14], and energy optimization [15], to name a few, are only a few of the areas where optimization has been applied. One of a network's main functions is routing; the SDN controller controls this function by altering the flow tables of network devices like switches and routers. A SDN controller may instruct a network device to direct traffic flows along particular paths or may elect to ignore a particular kind of traffic. The optimal decision, option, or selection with relation to a particular measure, model, or criterion is chosen from a pool of alternatives in mathematical optimization. Optimal route suggestion [13], optimal policy-making [14], and energy optimization [15], to name a few, are only a few of the areas where optimization has been applied. One of a network's main functions is routing; the SDN controller controls this function by altering the flow tables of network devices like switches and routers. A SDN controller may instruct a network device to direct traffic flows along particular paths or may elect to ignore a particular kind of traffic. The controller is viewed as an agent in RL-based routing optimization approaches, while the network is viewed as the platform. Network and traffic states make up the state space. The agent rewards are determined based on optimization measures like network delay and throughput, and actions serve as routing solutions. In paper [16], a distributed intelligent routing protocol employing RL is proposed.

A routing optimization approach for SDN-based interdata centre overlay networks is put out in paper [17]. In paper [18], a time-effective QoS aware adaptive routing strategy is given for forwarding the adaptive packet utilizing RL algorithms. The suggested method chooses a routing path with the highest possible QoS-aware reward based on the user apps and traffic kinds. Studies using supervised learning approaches for route optimization are also presented in the literature. The input of a training dataset for supervised learning-based routing optimization includes network and traffic states. The training dataset is thought of as the output of the heuristic algorithm's routing solution. Heuristic-like routing is one of the best routing methods that can result from learning based on supervision. The supervised learning-based dynamic routing method NeuRoute is proposed in [19].

The long short-term memory (LSTM) component of NeuRoute is utilized to predict future traffic. The projected network traffic and network status are utilized as input, and a neural network model receives the output of the heuristic algorithms. These input data and output data are used to train the neural network to forecast outcomes that resemble heuristics.

4. TRAFFIC PREDICTION

Regression modeling is used in the prediction process to determine how likely an outcome will be. Machine learning and artificial intelligence are two fields where predictive modeling is frequently used [20,21]. On the other hand, predictive analytics uses modeling and machine learning techniques using current data to forecast the outcome of yet-to-be-discovered future occurrences. In literature, predictive modeling is employed for prospective real-world applications [22-25]. In the area of routing optimization, traffic forecasting is a crucial research area. Utilizing study of previous traffic data, traffic prediction is used to forecast patterns in network traffic volume [26]. The SDN controller uses the results of traffic prediction to make effective traffic routing decisions in advance and to disseminate dynamic routing policies to data plane devices. Soon, traffic flow routing will be governed by these routing policies.

The SDN controller can avoid traffic congestion, enhance QoS, and proactively provision the network thanks to traffic prediction. A dynamic optimal routing meta-heuristic approach is suggested in the literature [27] for dynamic optical routing. The three stages of these meta-heuristic algorithms are offline scheduling, online routing and offline planning. A neural network is used to forecast network traffic load for the best resource allocation during the offline scheduling phase. Online routing decisions are based on the least expensive routing path. For the purpose of path load optimization, a load balancing technique is suggested [28]. In order to estimate the path load using a neural network model, SDN controllers use four features: packet loss rate, , transmission hop, transmission latency and bandwidth utilization ratio. For the new traffic flows, the path with the least amount of load is chosen. The research proposes the NeuTM LSTM-based framework to forecast the network traffic matrix. Real traffic data from the GEANT backbone network [29] are utilized to train the LSTM model. The performance of LSTM prediction is good for route optimization, according to results from the simulation environment. For evaluating network performance, researchers employ QoS metrics like throughput, latency, loss rate, and jitter. User perception and satisfaction levels are crucial for service providers and network operators. Utilizing user-focused measurements, QoE is utilized to evaluate the network performance. In order to deliver network services to consumers with high customer satisfaction, service providers utilize prediction algorithms to forecast QoS and QoE. For the purpose of predicting QoS and QoE, machine learning methods are used to data and statistics acquired by SDN controllers [30].

By forecasting QoS parameters based on key performance indicators, QoS management can be enhanced (KPIs). Because the values of the QoS metrics are continuous, predicting their values is seen as a regression task. For the prediction of QoS parameters, supervised machine learning-based algorithms such random forest, support vector regression, and ANN-based regression are utilized. Mean opinion score (MOS) is one example of a subjective indicator that QoE identifies across the network [31]. The QoE values are divided into five categories by MOS: excellent, good, fair, poor, and bad. Values for QoE are often derived using a QoS feedback form. Customers give the services a rating of 1 to 10 or 5 stars on a scale of 1 to how good they are. Since QoE depends on QoS factors, the subjective method takes time. To determine how QoS parameters and QoE values relate to one another, machine learning algorithms can be applied. A case study of a video streaming is used in the paper's ref. [32]

QoE prediction experiment. Network factors including delay, bandwidth, jitter, and RTT are used to estimate MoS value. SDN controller can change video settings to enhance user quality of experience. In paper [31], four machine learning algorithms—decision tree, K-NN, ANN, and random forest—are used to estimate QoE values based on video quality characteristics. The performance analysis makes use of the Pearson correlation coefficient and the root mean square error (RMSE).

5. RESOURCE MANAGEMENT

Techniques for resource management are employed by network administrators and service providers to enhance network performance. Utilizing network-based resource management, SDN maximizes resource consumption. Utilizing computing, networking, and caching resources is a part of data plane level resource management. Bandwidth, spectrum, and power are examples of networking resources that are used to meet the QoE and QoS needs of users. Caching strategies to remove data redundancy and save data transmission times by storing the most often requested data at the device end. To improve QoS and QoE, recent technological advances like facial recognition and augmented reality call for high computation at the device end. The gadget resources are unable to complete certain computational tasks due to limited computation and battery capacity. Utilizing EC to deploy computer resources close to end users is one way to offload such computational activities [33].

SDN networks are implemented in single- and multi-tenant settings to manage data plane resources effectively. A logically centralized controller oversees all data plane resources in a single tenancy SDN network. Each tenant's SDN controller maintains their separated resources in a multi-tenancy SDN network where several tenants share data plane layer resources. The paper [34] proposes a framework for software-defined virtualized vehicular ad-hoc networks (VANETs), which improve network performance by dynamically allocating data plane resources. The resource allocation problem is transformed into a multi-objective optimization problem. The issue is resolved and resource allocation strategies are obtained using Deep Reinforcement Learning (DRL) methods. For the case study of smart cities, a multi-objective optimization resource allocation issue solution is suggested [34,35]. C-RAN addresses the issues of multi-tenancy SDN network-based resource allocation in mobile network operators [36]. For this, a non-cooperative game-theoretic resource allocation issue is proposed. In order to tackle the issue, each participant chooses the best possible group of mobile network operators using a learning system based on regret matching. As a non-cooperative game-theoretic problem, the computational offloading problem in mobile edge computing (MEC) is also addressed [37].

The participants are the MEC servers, and each participant can be active or inactive. Each player's optimization objective is to reduce energy usage. Using an RL-based model, each player learns the best course of action. The most recent developments in network virtualization allow multi-tenancy SDN networks to share data plane resources by installing a network hypervisor between the control and data planes. Using a network hypervisor like FlowVisor [38] or OpenVirteX [39], each tenant is responsible for managing its own isolated network resource. Machine learning techniques are used by hypervisors to manage resources effectively. The hvbench CPU consumption measurement tool for hypervisors is suggested in article [40]. A benchmarking programme called Hvbench is used to calculate the control message rate. To determine the relationship between control message rate and CPU usage, three regression models are trained. These trained algorithms are employed to quickly identify network hypervisor overload. The SDN controller location, which has a substantial impact on the SDN network performance, is used in control-plane resource management in SDN. Traffic flows from switches located at various sites are processed by SDN controller. The resource management will take into account the processing time for traffic flows if there is a large distance between network devices and the SDN controller. Heuristic techniques are suggested in the literature to address the issue of controller placement; however these algorithms are computationally expensive. As a result, supervised learning techniques are employed to find the best location for the controller [41, 42]. Traffic distribution data is the input for these supervised learning models, and heuristic algorithms produce a controller placement solution as the output. This hybrid methodology, which combines supervised learning and heuristic algorithms, provides a low-cost, optimal controller placement solution.

6. SECURITY MANAGEMENT

In recent years, data mining and machine learning (ML) techniques have become increasingly important in the identification and categorization of intrusion attacks. The research described in [43-48] use approaches based on network simulation to find malicious traffic in SDN networks. dataset for simulations. In these methods, genuine hosts were set up on the network to produce normal traffic, while other hosts served as "pots" to produce attack traffic. They mimicked DoS assaults using open-source software like Scapy or hping3. The distinguishing characteristics, such as the speed of the source IP address or port, the flow of packets, etc., are taken from the collected traffic for both legitimate and malicious data individually. The row data for the training model are then created by randomly rearranging all of these samples in a.CSV file. Later, the learner model can be used to the SDN platform to classify legitimate and unauthorized packets. It is obvious that these methods compute quickly and require little analysis. It does, however, come with a number of limitations, which are outlined in the discussion that follows.

First, the size of the produced dataset is insufficient to provide reliable results because it is so. Only a few different types of attacks are present in the generated data as well. The variety of oddities that exist on the internet are not accurately represented by these attacks. The lack of diversity in attack types makes it easier for the attacker to understand the typical operation of the detection mechanism and create an attack that mimics it.

Second, the tiny number of recovered features is insufficient to adequately represent the behavior of all attacks, and the number of extracted features is negligible. Additionally, the learner module's features were essentially derived from packet headers without further payload data examination. The header field can be readily changed to resemble other fields. Typically, malicious code can be easily inserted by the attacker within the payload packets to evade detection from Root to Local (R2L) attacks and worm infestations. They consequently provide subpar accuracy for identifying application level threats. Public datasets are used in the work published in [49-54] to detect intrusions inside an SDN system. The evaluation of network intrusion detection systems is significantly impacted by the choice of the appropriate dataset (IDS). Unfortunately, the majority of publicly accessible datasets lack variation in attack types and are not practical in terms of covering all current internet trends. The privacy and legal concerns for service providers to publish their network data are one of the key causes of this shortfall. Because of this, most datasets are not accurate enough to be used with intrusion detection systems.

With the aim of identifying DDoS assaults, in paper [55] proposed the application of machine learning algorithms such as decision trees (DT), random forests (RF), support vector machines (SVM), and multilayer perceptrons (MLP). Entropy-based features are one more method for identifying DDoS attacks. In an SDN simulation environment, a firewall system is also developed to offer a more secure SDN network.

7. CONCLUSION AND FUTURE WORK

In this paper, we discussed the machine learning techniques that are currently used in SDN for resource management, traffic classification, traffic prediction, routing optimization, and security management. The current architecture is insufficient for satisfying the computational requirements of the features, according to research conducted on the papers on SDN. The current architecture also takes up a lot of time because it introduces numerous defects and errors, leaving no time for creating a useful architecture. Although the SDN architecture also has many difficulties, it is still far superior to the current one. Network virtualization, operation, and mobility management present difficulties. While the majority of SDN research focuses on the scalability of solutions, the control plane and data plane, and distributed versus centralized control plane, there is surprisingly little attention paid to the problems. A proper understanding of this emerging area is required if the person wants to address multiple challenges that will involve the software-defined networking process. In our future work, we planned to propose a novel method that solves SDN issues using nature inspired optimization algorithms for better improvement.

Table 1 shows the generalized merits and demerits of SDN using Machine learning algorithms

Sl.No	Applications	Merit	Demerit
1.	Traffic Classification [5-12]	• Improved QoS • Reduced Cost	• Imbalanced training dataset • Concept drift • Scalability in the control plane. • Still lack in performance and accuracy
2	Routing Optimization [13-19]	• Increased throughput • Delay and jitter reduction	• Ignores the load condition, global path lead to the bad impacts • Less utilization of realtime dataset.
3	Traffic Prediction [20-32]	• Predicting possible congestion	• Using historical data • Overburdening of controller
4	Resource Management [33-42]	• Enhanced resource allocation problems	• Need to improve Optimal placement of controller • Cost reduction

5	Security Management [43-55]	• Enhanced network performance • Reduced latency	• Maximizes resource utilization the intelligent entity • Estimating the CPU needs of Virtual network functions • Optimal placement of the nodes • Insufficient dataset

Table 1. Merits and demerits of SDN using ML techniques

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Kumar, S. D., Raihan, U. and Mahbubur, R. (2020).Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach. International Joint Conference on Computational Intelligence, Algorithms for Intelligent.pp.483 494.

[2] Ramkumar, M. P., Emil, S. and Bavani, K. (2020).Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined.International Conference on Advanced Computing & Communication Systems (ICACCS).No. 6.pp. 380 -385.

[3] Jankowski, D. and Marek, A. (2016). On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks. International Journal of Electronics and Telecommunications. VOL. 62, No. 3, pp. 247-252. DOI: 10.1515/eletel-2016-0033.

[4] Xu, G.; Mu, Y.; Liu, J. Inclusion of artificial intelligence in communication networks and services. ITU J. ICT Discov. Spec. 2017, 1, 1–6.

[5] Amaral, P.; Dinis, J.; Pinto, P.; Bernardo, L.; Tavares, J.; Mamede, H.S. Machine learning in software defined networks: Data collection and traffic classification. In Proceedings of the 2016 IEEE 24th International Conference on Network Protocols (ICNP), Singapore, 8–11 November 2016.

[6] Xiao, P.; Qu,W.; Qi, H.; Xu, Y.; Li, Z. NAn efficient elephant flow detection with cost-sensitive in SDN. In Proceedings of the IEEE INISCom'15, Tokyo, Japan, 16 July 2015; pp. 24–28.

[7] Wang, P.; Hao,W.; Jin, Y. Fine-grained traffic flow prediction of various vehicle types via fusison of multisource data and deep learning approaches. IEEE Trans. Intell. Transp. Syst. 2020.

[8] Uddin, M.; Nadeem, T. rafficVision: A case for pushing software defined networks to wireless edges. In Proceedings of the 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Brasilia, Brazil, 10–13 October 2016.

[9] Wang, P.; Lin, S.-C.; Luo, M. A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs. In Proceedings of the IEEE SCC'16, San Francisco, CA, USA, 1 September 2016; pp. 760–765.

[10] Alqahtani, J.; Alanazi, S.; Hamdaoui, B. Traffic Behavior in Cloud Data Centers: A Survey. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 27 July 2020; pp. 2106–2111.

[11] Glick, M.; Rastegarfar, H. Scheduling and control in hybrid data centers. In Proceedings of the 2017 IEEE Photonics Society Summer Topical Meeting Series (SUM), San Juan, PR, USA, 21 August 2017.

[12] Owusu, A.I.; Nayak, A. An Intelligent Traffic Classification in SDN-IoT: A Machine Learning Approach. In Proceedings of the 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 26–29 May 2020; pp. 1–6.

[13] Ahmad, S.; Jamil, F.; Iqbal, N.; Jamil, F.; Kim, D. Optimal Route Recommendation forWaste Carrier Vehicles for EfficientWaste Collection: A Step Forward Towards Sustainable Cities. IEEE Access. 2020, 8, 77875–77887.

[14] Ahmad, S.; Imran; Iqbal, N.; Jamil, F.; Kim, D. Optimal Policy-Making for MunicipalWaste Management Based on Predictive Model Optimization. IEEE Access. 2020, 8, 218458–218469.

[15] Wahid, F.; Fayaz, M.; Aljarbouh, A.; Mir, M.; Amir, M.; Imra. Energy consumption optimization and user comfort maximization in smart buildings using a hybrid of the firefly and genetic algorithms. Energies. 2020, 13, 4363.

[16] Sendra, S.; Rego, A.; Lloret, J.; Jimenez, J.M.; Romero, O. Including artificial intelligence in a routing protocol using software defined networks. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017.

[17] Francois, F.; Gelenbe, E. Optimizing secure SDN-enabled inter-data centre overlay networks through cognitive routing. In Proceedings of the 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), London, UK, 19–21 September 2016

[18] Lin, S.-C.; Akyildiz, I.F.; Wang, P.; Luo, M. QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. In Proceedings of the 2016 IEEE International Conference on Services Computing (SCC), San Francisco, CA, USA, 27 June–2 July 2016

[19] Azzouni, A.; Boutaba, R.; Pujolle, G. NeuRoute: Predictive dynamic routing for software-defined networks. In Proceedings of the 2017 13th International Conference on Network and Service Management (CNSM), Tokyo, Japan, 26–30 November 2017.

[20] Azzouni, A.; Boutaba, R.; Pujolle, G. NeuRoute: Predictive dynamic routing for software-defined networks. IEEE Access. 2020, 8, 46193–46205.

[21] Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. A Novel Blockchain-Based Integrity and Reliable Veterinary Clinic Information Management System Using Predictive Analytics for Provisioning of Quality Health Services. IEEE Access. 2021, 9, 8069–8098

[22] Jamil, F.; Iqbal, N.; Imran; Ahmad, S.; Kim, D. Peer-to-Peer Energy Trading Mechanism based on Blockchain and Machine Learning

for Sustainable Electrical Power Supply in Smart Grid. IEEE Access. 2021, 9, 39193–39217.

[23] Iqbal, N.; Ahmad, R.; Jamil, F.; Kim, D. Hybrid features prediction model of movie quality using Multi-machine learning techniques for effective business resource planning. J. Intell. Fuzzy Syst. 2021, 1–22. [CrossRef]

[24] Khan, A.N.; Iqbal, N.; Ahmad, R.; Kim, D. Ensemble Prediction Approach Based on Learning to Statistical Model for Efficient Building Energy Consumption Management. Symmetry. 2021, 13, 405. [CrossRef]

[25] Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. Toward effective planning and management using predictive analytics based on rental book data of academic libraries. IEEE Access 2020, 8, 81978–81996. [CrossRef]

[26] López-Raventós, Á.; Wilhelmi, F.; Barrachina-Muñoz, S.; Bellalta, B. Combining Software Defined Networks and Machine Learning to enable Self Organizing WLANs. In Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019.

[27] Alvizu, R.; Troia, S.; Maier, G.; Pattavina, A. Matheuristic with machine-learning-based prediction for software-defined mobile metro-core networks. J. Opt. Commun. Netw. 2017, 9, D19–D30. [CrossRef]

[28] Cui, C.-X.; Xu, Y.-B. Research on load balance method in SDN. Int. J. Grid Distrib. Comput. 2016, 9, 25–36.

[29] Michael, S.; Anna, Z.J. An Identity Provider as a Service platform for the eduGAIN research and education community. In Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 8–12 April 2019.

[30] Carner, J.; Mestres, A.; Alarcón, E.; Cabellos, A. Machine learning-based network modeling: An artificial neural network model vs a theoretical inspired model. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017.

[31] Abar, T.; Letaifa, A.B.; El Asmi, S. Machine learning based QoE prediction in SDN networks. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017

[32] Letaifa, A.B. Adaptive QoE monitoring architecture in SDN networks: Video streaming services case. In Proceedings of the IEEE IWCMC 17, Valencia, Spain, 26–30 June 2017; pp. 1383–1388.

[33] Huo, R.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Leung, V.C.M.; Liu, Y. Software defined networking, caching, and computing for green wireless networks. IEEE Commun. Mag. 2016, 54, 185–193.

[34] He, Y.; Yu, F.R.; Zhao, N.; Yin, H.; Boukerche, A. Deep reinforcement learning (DRL)-based resource management in software defined and virtualized vehicular ad hoc networks. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Miami, FL, USA, 13–17 November 2017.

[35] He, Y.; Yu, F.R.; Zhao, N.; Leung, V.C.M.; Yin, H. Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach. IEEE Commun. Mag. 2017, 55, 31–37.

[36] Narmanlioglu, O.; Zeydan, E. Learning in SDN-based multi-tenant cellular networks: A game-theoretic perspective. In Proceedings of the 2017 IFIP IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017.

[37] Ranadheera, S.; Maghsudi, S.; Hossain, E. Mobile edge computation offloading using game theory and reinforcement learning. arXiv 2017, arXiv:1711.09012.

[38] Xiang, Z.; Pandi, S.; Cabrera, J.; Granelli, F.; Seeling, P.; Fitzek, F.H.P. An Open Source Testbed for Virtualized Communication Networks. IEEE Commun. Mag. 2021, 59, 77–83.

[39] Yang, G.; Yu, B.; Jin, H.; Yoo, C. Libera for programmable network virtualization. IEEE Commun. Mag. 2020, 58, 38–44.

[40] Sieber, C.; Basta, A.; Blenk, A.; Kellerer,W. Online resource mapping for SDN network hypervisors using machine learning. In Proceedings of the 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, Korea, 6–10 June 2016.

[41] He, M.; Kalmbach, P.; Blenk, A.; Kellerer, W.; Schmid, S. Algorithm-data driven optimization of adaptive communication networks. In Proceedings of the 2017 IEEE 25th International Conference on Network Protocols (ICNP), Toronto, ON, Canada, 10–13 October 2017.

[42] Blenk, A.; Kalmbach, P.; Kellerer, W.; Schmid, S. CO'zapft is: Tap your network algorithm's big data! In Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks, Los Angeles, CA, USA, 21 August 2017.

[43] A. Prakash and R. Priyadarshini, "An intelligent software defined network controller for preventing distributed denial of service attack," in Proc. Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2018, pp. 585–589.

[44] D. Li, C. Yu, Q. Zhou, and J. Yu, "Using SVM to detect DDoS attack in sdn network," in IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2018, vol. 466, p. 012003.

[45] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," Security and Communication Networks, vol. 2018, 2018.

[46] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (sdn)," Journal of Computer Networks and Communications, vol. 2019, 2019.

[47] T. Hurley, J. E. Perdomo, and A. Perez-Pons, "HMM-based intrusion detection system for software defined networking," in Proc. 15th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2016, pp. 617–621.

[48] 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 Proc. IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016, pp. 27–35.

[49] C. Song, Y. Park, K. Golani, Y. Kim, K. Bhatt, and K. Goswami, "Machine-learning based threat-aware system in software defined networks," in Proc. 26th international conference on computer communication and networks (ICCCN). IEEE, 2017, pp. 1–9.

[50] S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa, and B. Yang, "Predicting network attack patterns in SDN using machine learning approach," in Proc. IEEE Conference on Network

Function Virtualization and Software Defined Networks (NFV-SDN). IEEE, 2016, pp. 167–172.

[51] P. Wang, K-M. Chao, H-C. Lin, W-H. Lin, and C-C. Lo, “An efficient flow control approach for SDN-based network threat detection and migration using support vector machine,” in Proc. IEEE 13th International Conference on e-Business Engineering (ICEBE). IEEE, 2016, pp. 56–63.

[52] L. Barki, A. Shidling, N. Meti, DG Narayan, and M. M. Mulla, “Detection of distributed denial of service attacks in software defined networks,” in Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2016, pp. 2576–2581.

[53] A. Alshamrani, A. Chowdhary, S. Pisharody, D. Lu, and D. Huang, “A defense system for defeating DDoS attacks in SDN based networks,” in Proc. 15th ACM International Symposium on Mobility Management and Wireless Access. ACM, 2017, pp. 83–92.

[54] J. Smith-perrone and J. Sims, “Securing cloud, SDN and large data network environments from emerging DDoS attacks,” in Proc. 7th International Conference on Cloud Computing, Data Science & Engineering- Confluence. IEEE, 2017, pp. 466–469.

[55] Shankaraiah, Shashank, S. (2022). Software-Defined Networking Security System Using Machine Learning Algorithms and Entropy-Based Features. In: Karrupusamy, P., Balas, V.E., Shi, Y. (eds) Sustainable Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies, vol 93. Springer, Singapore. https://doi.org/10.1007/978-981-16-6605-6638