Grenze International Journal of Engineering and Technology, June Issue

Review of AI/ML in Software Defined Network from Past to Present

Dr. Raghavendra Kulkarni
Department of Computer Science, School of Science
Gandhi Institute of Technology & Management (GITAM) Deemed to be University
Hyderabad, Telangana, India.
Email: raghavendra.kulkarni82@gmail.com

***Abstract*— Software-Defined Networks (SDN) technology disrupts the traditional network architecture's tight link between the data plane and the control plane, enabling network resource economy, security, and controllability. In this study, we carried out a systematic analysis with a specific focus on the application of AI/ML algorithms to enhance SDN functions. Artificial intelligence (AI) or Machine learning (ML) will have significant potential in fields such as route planning, network resource management, traffic scheduling, network security and fault detection, when paired with SDN architecture. Networks have become more complicated and challenging to configure, manage, and monitor as a result of these demands. Researchers and operators recommended using software tools that can monitor and configure networks on-demand to make networks more manageable and controllable. From the perspective of ML algorithms, this study focuses on the applications of traditional AI/ML algorithms in SDN-based networks. Finally, a discussion and analysis of the potential future development of SDN concepts in ML algorithms is addressed. We present a summary of the state-of-the-art after reviewing 1450 publications. Researchers from various domains will find this study useful and essential in fully understanding the fundamental concerns.**

***Index Terms*— Artificial Intelligence, Machine Learning, Quality of Service, Software-Defined Networks, Systematic Literature Review.**

I. INTRODUCTION

The necessity for novel and effective network architectures is made clear by the rising service heterogeneity and consumption. To ensure quality of service (QoS) and to achieve Service-Level Agreements (SLAs), modern networks are configured with complicated static rules. The complexity of administration and configuration procedures tends to rise in multi-vendor setups. The problems with conventional network-centric architectures are intractable. Consequently, with SDN and network programmability and automation, network-centric paradigms give way to application-centric paradigms [1]. In order to grant access to and control over the network resources, the SDN controller hosts APIs. However, these APIs require the applications to effectively optimize network speed and security, and machine learning (ML) and artificial intelligence (AI) algorithms can support this effort. There have been numerous systematic reviews of SDN studies conducted by academics and business professionals. The authors of [2] describe different SDN load balancing methods, some of which use AI algorithms. Using SDN designs, Ray et al. proposed an examination of IoT devices in [3]. In addition, [4] discusses the difficulty of applying AI/ML in SDNs.

Grenze ID: 01.GIJET.9.2.337
© Grenze Scientific Society, 2023

Network management is made easier with the advent of SDN, which also makes it possible to configure networks efficiently through programming [5]. Through streamlined hardware, software, and management, SDN can accommodate while having lower operational costs [6]. Hardware limits on the network design will be eliminated.

Applications for SDN enable centralized management of network policies and regulations. Additionally, they include a range of features that let administrators use ML techniques to successfully resolve network issues. In parallel, the SDN architecture implements network management and traffic control based on ML techniques. From a comprehensive network perspective, controlling network traffic is simple since the controller has access to all data regarding physical networks and their operational needs. According to our findings, network traffic categorization research has been a hot area for a while. This study is crucial for choosing the best route configurations, managing network resources, meeting QoS standards, etc. One of the crucial applications that cannot be underestimated is network security.

Although these studies offer some extremely intriguing viewpoints and a thorough examination of the subject, none of them discuss how AI/ML might be used to SDNs as a whole, instead concentrating primarily on particular features like load balancing and intrusion detection systems. Furthermore, no studies that used a rigid and open selection process in conjunction with a systematic literature review technique could be located. Therefore, the focus of the current work is on how AI/ML may enhance performance and address unique challenges in SDNs.

II. Methodology

The objective of this study is to compile a collection of publications and analyze them in order to address different research issues. The following are the research questions:

RQ1. What kind of AI/ML mechanisms are applied to SDN?

RQ2. Can Performance of SDNs be improved by AI/ML?

RQ3. What are the main limitations of using AI/ML in SDNs with respect to Quality of Service (QoS)?

We gathered a number of publications for analysis. An initial batch of papers is assessed using inclusion/exclusion criteria at the beginning of the procedure. In a subsequent iteration, references and citing articles from the individuals listed are acquired and examined.

Our search was conducted using the terms "Software Defined Networks," "Artificial Intelligence," and "Machine Learning," as well as their respective acronyms: ("SDN" OR "Software Defined Network" AND ("Artificial Intelligence" OR "AI" OR "Machine Learning" OR "ML")

A. Start Set and Criteria

We submitted the search query into the IEEE Xplore, Google Scholar and Core, search engines in order to build the start set. The first five papers from each group were then chosen.

The following acceptance standards were established before the articles were examined:

- Publication date between 2011 and 2022 (OpenFlow's release date);
- Published in first- or second-quartile peer-reviewed articles (Scimago ranking);
- Written in English;
- Focus on the current themes, such as SDN and AI/ML applications;
- Articles with access that the authors have been given.

With the help of the approval criteria, we selected a collection of articles that directly examine AI/ML in SDNs from reputable sources. Only six of the prospective beginning set's fifteen articles ultimately complied with the requirements: [7–12]. A total of 344 were omitted based on the year of publication, 112 were excluded because they were not published in conferences or journals with high enough rankings, 14 were unavailable, 296 were duplicates, 4 were not articles, and 582 did not directly address the issues at hand. 98 articles were chosen from this process, which was conducted between August and September 2022.

III. Discussion

The primary objectives of this part are to present our findings, discuss them, and provide an overview of existing and emerging trends.

A. Application of AI/ML algorithms

The application of AI/ML algorithms in the publications is displayed in Table 1. The ranking shows that supervised learning algorithms are second in prevalence to neural networks (NNs) methods. Other mechanisms,

such as self-organizing maps, have been discussed in a number of studies but have not received as much attention.
The popularity neural networks and of deep learning, as well as RF and DT algorithms, can be used to explain why supervised learning techniques are preferred over the others. Unsupervised learning discovers patterns from unlabeled data, whereas supervised learning uses labelled data to adjust model parameters.

TABLE I. SDN-CONCEPT NETWORK PERFORMANCE ANALYSIS AND APPLICATIONS OF AI/ML ALGORITHMS

References	AI/MI Algorithm	Application	Performance analysis
[13]	K-Nearest Neighbours (KNN)	Predis: detects various attacks in addition to DDoS attacks.	Easily accessible, highly accurate; incapable of recognizing extremes; Calculate features easily; Suitable for multiclass classifications; Time consuming for large datasets
[14]	Random Forest (RF)	using regression to model one VNF's latency distribution.	High accuracy
[15], [16]	Decision Tree (DT)	Packet classification; LCD: optimize the ASP; Flow classification; Inductive inference;	Simple to comprehend and implement; Data preparation is easy or not required; High-speed; Too many categories may lead to higher error growth.
[17]-[19]	Neural Network (NN)	Collaborative intrusion prevention; Predicting the performance of SDN; Load balancing	Due to its simple and parallel computational capabilities, it achieved a low overhead; Achieved low mean squared error (MSE); improved efficiency and a 19.3% reduction in network latency.
[20], [21]	Reinforcement Learning (RL)	Cognitive network management	Manage networks efficiently;
[22]	Deep RL	Adaptive multimedia traffic control mechanism leveraging	Dynamic coordination of computational, networking, and caching resources
[23],[24]	Deep Q-Learning	Q value-action function approximation	Promote resilience and scalability
[25] [26], [27]	SVM	Predict link failure; Detect DDoS attack;	Reduces the start-up time for identification and classification recognition; lowers the rate of false alarms
[28]	Laplacian SVM	Traffic classification on the real Internet data	Similar applicability to supervised learning; only tested in a lab environment; processes synthetic data

In this context, it appears that supervised learning can be used more readily to enhance network decision-making in areas like routing and QoS. RL and unsupervised learning algorithms are outperformed by supervised learning algorithms, which are distinguished by a peak in 2017 and an erratic drop in the years that followed. It's interesting to note that RL has been rising gradually. In IoT, 5G access networks and automotive networking—dynamic situations recognized by RL to perform unsupervised and supervised learning methods—this suggests a possible application for SDNs. Based on these findings, it is predicted that the usage of RL to train networks and SDN processors would have to adapt to variations in resource demand and traffic, especially with the introduction of SDNs in increasingly complicated networks.

B. Artificial Intelligence in SDN

Numerous issues, resource allocation and admission control, [29], have been successfully solved using AI and ML methodologies. However, in the SDN era, AI's function was greatly expanded due to the significant efforts made by the business sectors. Many researchers have revealed a significant trend in the scientific community's application of AI methods in SDNs.

C. ML Methods In SDN-Concept Networks

The reinforcement learning, the semi-supervised, the unsupervised, the supervised learning method are the four kinds of ML approaches. A mathematical model is created by supervised learning algorithms using a labelled training sample. Algorithms for unsupervised learning gain information derived from test results that were not labelled. Additionally, when some of the sample input lacks labels, semi-supervised learning approaches are used to build mathematical models using sparse training data. Numerous classification and prediction issues have been successfully solved by the application of ML methods [30]. In this section, we will continue our work from an algorithmic perspective by providing many traditional ML techniques used in SDN also listed in Table I for greater understanding.

1) Supervised Learning in SDN-Concept Networks

Nowadays, Numerous various applications, including spam detection, object and speech recognition, commonly use supervised learning [31]. Predicting the value of results obtained from the values of a vectors of input variable is the objective. In the context of regression approaches, the SDN architecture uses a regression to predict [32].The key performance indicator (KPI) for the application and the network metrics are additionally related using multiple linear regressions [33]. Regression algorithm usage in SDN is currently uncommon on the whole. We focus on introducing the categorization techniques in SDN. The Logistic Regression, SVM, Decision Trees, KNN, Naive Bayesian algorithms are some of the most frequently used classification methods.

a) K-Nearest Neighbours (KNN) In SDN-Concept Networks

KNN is categorized by calculating the distance between various feature values. The categorization outcomes actually depend on a relatively limited set of nearby samples. KNN is appropriate for multiclass classifications which has been extensively utilized as a classifier in many different fields.

Predis, a computationally straightforward and effective KNN method, was proposed by Zhu et al. [13] as its detection technique. Because of its better efficiency design, it can accurately identify a variety of other forms. The algorithm takes a long time when the training dataset is huge. KNN, one of the most straightforward ML algorithms, is simple to use, estimates features accurately, and works well for multiclass classifications. When used to huge datasets, the algorithm takes a long time.

b) Support Vector Machine (SVM) in SDN-Concept Networks

Generalized linear classifiers include SVM that uses supervised learning to carry out binary classification. Because both structural and empirical risk minimizations are taken into consideration in the optimization problem, SVM is stable.SVM only works for binary classification tasks, it should be mentioned. Multiple classification tasks will therefore be broken down into a number of binary questions. The technology uses SVM embedded in the controller to identify DDoS attacks in [26]&[27]. It can identify the distinction between flow entries created by DDoS attack traffic that are malicious and flow entries created by normal traffic that are benign. In terms of binary classification problems, SVM has a lower rate of false alarms. Effectively cutting down on the time needed to start classification recognition and assault detection is the detection strategy. Since SVM is established at the SDN controller stage, the effectiveness of the SDN system is not significantly impacted by its complexity.

c)Neural Networks (NN) in SDN-Concept Networks

According to the testing findings, CIPA is more effective than [35] at identifying DDoS flooding attacks. CIPA also has success finding outbreaks of the Witty, Slammer, and Conficker worms. Due to its parallel and straightforward processing capabilities, the system achieved little computational and communication overhead. A multi-label classification method was suggested by He et al. [36] to estimate global network allocations. The neural network approach outperformed decision trees and logistic regression and reduced algorithm runtime by up to two-thirds. In order to estimate traffic demands off-line for a mobile network operator, Alvizu et al. [34] employed a neural network technique, which reduced the optimality gap between 0.2% and 0.45%. Additionally, the next configuration time point was predicted off-line using a NN technique.

A system for intrusion detection for SDN built on NN technique was proposed by Abubakar et al. [37]; it made use of the NSL KDD dataset to obtain a high reliability of 97.3%.

d)Decision Tree (DT) in SDN-Concept Networks

DT is a prediction model that illustrates the relationship among both object values and characteristics. It is a tree data structure where leaf nodes signifies a category and branch route denotes a potential parameter value, and internal node in the tree indicates an object. DT is frequently used in data mining to examine data for prediction. Packet classification is its primary use in networks. These are well-known methods, such as Hyper Cuts [38], Hi Cuts [39], Cut Split [40] or Effi Cuts [41], Partition Sort [42], which incorporates the advantages of DTs and TSS (Tuple Space Search), is proposed in light of the significantly increased dimensionality and dynamism in SDN. A least cost disruptive (LCD) decision tree was developed to resolve trade-offs between good delivery of services, adaption costs, and users disruptive level variables [43].The DTs were employed in the work in [44] as a technique of solving the Flow Table Congestion Problem (FTCP). The main advantage of DT over KNN and SVM is that it can be easily implemented, and that preparation of data is either trivial or not even necessary. However, when there are too many categories, errors could increase more frequently.

e)Ensemble Learning in SDN-Concept Networks

The objective of the supervised learning method is to develop a stable model that excels in all situations, although the facts aren’t quite obvious. In order to create a stronger, more complete strong supervision model, multiple weak supervised models are combined through ensemble learning. A particular approach is used to merge a group of individual learners after they have first been formed. Bagging and boosting are two of the main ensemble learning algorithms. Despite the fact that these methods are used less frequently than traditional methods. RF (Random Forest) creates bagging integration and uses it in numerous settings using DT as the foundation learner. The indoor localization generated by the model in [45] has a high efficiency of 98.3% and performs best when using SVM, NN and KNN. It trains itself using RF-based cross validation (Neural Networks). To effectively describe the latency distribution of a single VNF, Lei et al. [46] suggest using a random-forest regression prediction approach. Ensemble learning is more accurate than the conventional methods mentioned above, but comes with a high level of complexity.

2) Unsupervised Learning in SDN-Concept Networks

The training samples' labels are unknown in unsupervised learning techniques. Analyzing training samples without labels that adds another layer of support for data analysis, the objective is to discover the fundamental characteristics and laws governing the data. The most popular technique is "clustering," and K-means is the most basic and well-known algorithm[48]. In an SDN-based WAN design, a controller placement problem is solved using a hierarchical K-means algorithm [49]. There are also algorithms that contrast or combine supervised learning and unsupervised learning. Understanding each algorithm's benefits and drawbacks is the goal of the comparison. Different supervised and unsupervised learning methods, including Naive Bayes, KNN, K-medoids and K-means, are used by Barki et al. [47] to categorize the traffic as abnormal or normal. Compared to Bayes and KNN, K-means and K-mediods are faster but less accurate. For traffic categorization, the two ML techniques unsupervised K-means clustering and supervised SVM are investigated [50].

3) Semi-Supervised Learning in SDN-Concept Networks

Generally, unsupervised and supervised learning are the two main subcategories of machine learning technology. While unsupervised learning only utilizes unlabeled sample sets, supervised learning only employs labelled sample sets. However, because labelling data is so expensive, there are sometimes far more unlabeled data available in real issues than there are labelled data. As a result, semi-supervised learning methods that may be applied to both labelled and unlabeled samples quickly developed. A combination of unsupervised and supervised learning is used in this learning strategy. By employing a large amount of unlabeled samples and small amount of labelled data and it primarily focuses on how to build and categorize models. The same applications as supervised learning utilize semi-supervised learning [36]. Semi-supervised learning has only been evaluated in the lab and has historically been used to handle synthetic data, whereas [51] has done studies to achieve accurate traffic classification of real Internet data. To re route effectively and accomplish the objectives of resource, the QoS parameters may be used. The QoS classifier also uses semi-supervised machine learning to handle traffic from unidentified applications. Its practical importance has not been adequately represented, relative speaking. Additionally, more study is needed to determine the practical benefits of semi-supervised learning.

4) Reinforcement Learning (RL) in SDN-Concept Networks

Through trial and error and rewards from interactions, an agent learns the reward-guiding activity referred as RL. In SDN-concept networks [52], [53], RL delivers path selection or route optimization and is often used to support reliability and scalability [20]. When delay reduction and throughput maximization are employed as the primary operational and maintenance method for DROM [54], the resulting network performance, routing services, and convergence are all significantly improved. The Internet of Vehicles (IoV) environment can be sensed and learned from to give an optimal routing policy adaptively. SDCoR [55] is the first study to do this and outperforms numerous common IoV protocols. Reduce the number of distinct pathways used for contiguous data frames in order to address the primary challenge of high jitter [52]. It is suggested to mix certain innovative RL research with other technologies for improved performance. To discover the best overlay paths with the least amount of monitoring overhead, for instance, Random NN with RL are constructed [21]. For making auto-scaling policy decisions, SRSA [56], an RL-based auto-scaling decision mechanism, was investigated. Furthermore, due to the complex and dynamic network environment, RL with architecture changes are considered.

To effectively manage networks with SON (Self-Organizing Networks) capabilities, Daher et al. [57] presented a scalable strategy based on distributed RL. By combining DL with RL, Deep Reinforcement Learning (DRL) accelerates learning and enhances the effectiveness of RL algorithms. DRL has produced outstanding outcomes in both theory and practice. In particular, the Google Deep Mind team's DRL-based Alpha Go program is regarded as a significant development in the field of artificial intelligence. Our findings support DRL's claims of some development in SDN concept networks. DRL for leveraging adaptive multimedia traffic control mechanism was researched by Huang et al. Without using a mathematical model, it can directly govern multimedia flow. Deep Q-Learning (DQL) is specifically employed for the majority of DRL-related activities [58]. And in various network circumstances, different DQL approaches can be employed to solve various challenges. He et al. [59] suggested an integrated DQL methodology with SDN that uses a deep Q network to approximate the Q value-action function. Overall, RL is a significant ML technique that is frequently applied to network-related problems. Keep in mind that it only describes the interaction processes as opposed to offering a different teaching strategy. Additionally, an RL can be created from any learning algorithm [60], and it will be frequently used for analysis and prediction. Figure 1 gives a brief description of machine learning methods [61].

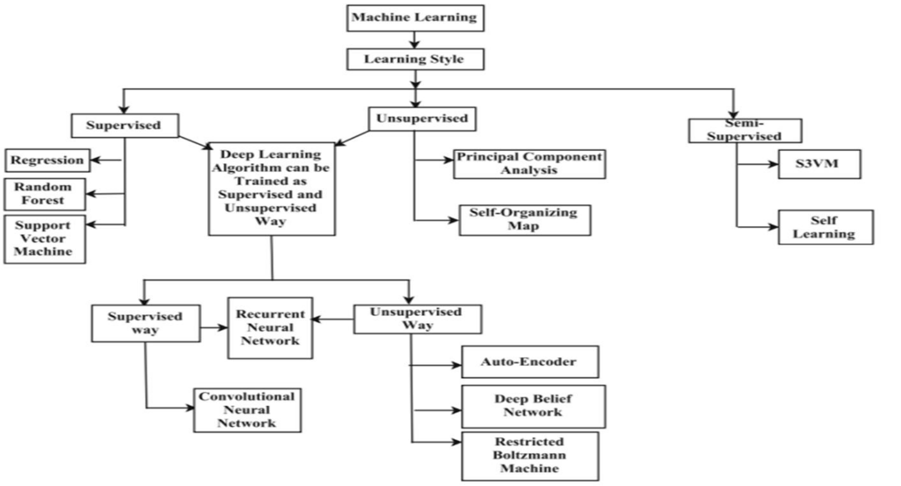

Fig 1. Overview of machine learning approaches

D. Quality of Service in SDN

The network will offer various levels of QoS depending on the offered traffic type, the volume of traffic at any given time, and the traffic's final destination[62]. Using Deep Air, a DRL-based adaptive intrusion detection Software-Defined Networks may successfully defend against cyber attacks (SDN). When compared to a Q-learning, Deep Air can significantly lower the ratio of QoS violating traffic flows [63]. To install SDN controller flow rules on the SDN-capable switches to decide the routing paths [64]. However, they are constrained in size due to their high cost and energy consumption. The installation in the SDN nodes’ flow tables is impacted by this restriction, and ineffective rule administration can result in a reduction in the network's QoS. In [65] a DRL-based solution to the SDN flow tables' rule insertion issue is provided. The fundamental concept is to get rid of the rules that are meant to be used less. In this method, the objective of increasing the quantity of flows that the network can handle and subsequently enhancing network QoS is accomplished.

Due to the expansion of IoT applications, cloud services, mobility and video streaming made available to internet users, networking systems are becoming more sophisticated. The problem is that different QoS demands made by internet users are not satisfied. Artificial intelligence can be integrated into the system to manage complex networks thanks to machine learning. To get a comprehensive network view and installing the best routes in the routing/switch devices, the SDN platform is employed. The difficult part is computing the choice reward value and dynamically gathering the parameters in network. Real-time network topologies are used to carry out the emulation. Comparing the results to the conventional link-state algorithm, they are encouraging. The learning agent can gradually learn the way thanks to the RL algorithm for path determination (training time). For a destination pair and single source, the testing step takes n-1 comparisons to find the path [66].

Network congestion and the end-to-end customer satisfaction exhibited by the QoE, the massive traffic utilization has adversely affected the network's QoS particularly during night time peak hours. A n intelligent multimedia framework in [67] is introduced to make use of the integration of SDN and RL, which allows for the exploration, learning, and exploitation of potential paths for video streaming flows, to optimize users' QoE and the network's QoS.

E. Impact of AI/ML on SDNs

The impact of AI/ML in SDNs is described in Table 2. AI facilitates intelligent resource optimization, promotes autonomous network management and controller, and increases security. Even though the majority of the techniques are proofs of ideas, they amply show how AI/ML may be used to manage QoS and QoE and automate networks. These results imply that SDNs can successfully implement AI/ML algorithms, potentially accommodating both present and future specifications

TABLE II. IMPACT OF AI/ML ON SDNS

References	AI/MI algorithms	Use Cases
[68]-[70]	Deep RL	Optimise network resource usage
[71]	Supervised ML	Guarantee traffic based on its QoS requirements
[72]	Matheuristic with ML based	Enhance autonomous network management and configuration
[73], [74]	Decision Table (DT), Bayesian Network (BayesNet), and Naive-Bayes;Neural Network	Improve network security
[75]	Unsupervised ML for Networking	Monitor load balancing
[76], [77]	semi-supervised ML; RF, DT, KNN	Guarantee Quality of Service
[78]	ML and Deep Packet Inspection	High accuracy and applicability of classifier

F. Limitations of applying AI/ML in SDNs

AI/ML techniques are useful in many sectors, but they have major drawbacks. The same premise holds true for SDNs, as seen in Table 3. There is potential for improvement, as many studies (76 %) report having trouble putting the AI/ML techniques into practice. The three main issues are learning distortion, difficulty in processing large amounts of data without sampling and locating quality training sets

TABLE 3. LIMITATIONS OF AI/ML ALGORITHMS OF QOS IN SDN ENVIRONMENTS

References	Method	Advantages	AI/MI Limitations
[79]	SDN-Cloud - DDoS attack	• Since a multi-controller SDN environment is emerging, attack mitigation at a single controller will result in increased computing overhead. • High scalability support	•Weaksecurity between controllers and switches •Reduces flow timeout duration ;•Time-consuming operation
[80]	AI-aided SD-IoT	•High scalability •Less complexity. •High QoS	Nil
[81]	FSM	•Less overhead •Does not require frequent flow migrations	•Impossible to forecast an absolute transition. •Not suited for a large-scale environment
[82]	Sway	•K-paths are determined •The route is constructed for multimedia traffic	•Low throughput •Low Load balance rate • Low scalability •Not suited for heterogeneous devices
[83]	DNN-SDR	•Achieved load balance rate •Network dimensionality is reduced	• Time-consuming • Single point of failure • Poor scalability
[84]	FRI	•Low packet loss rate •Predicts the best path for traffic	•Large delay in best path selection •Low throughput •Traffic overhead is high
[85]	Robust security (SDN-5G)	•Able to reduce security threats •Increases flow time out period	• Authentication is time consuming • Searching time for packet assignment is extensive • Conventional ECC is utilized to generate keys, reducing robustness and dependability;

IV. CONCLUSION

To investigate the application of AI/ML approaches in SDNs, we examined at 98 publications (out of a total of 1450). The findings imply that algorithms for supervised learning considerably outperform those for unsupervised learning and reinforcement learning. According to the majority of studies, NNs are the most effective way to improve intelligence and optimize SDNs. However, in environments where numerous diverse devices compete for network resources, RL has noticed a minor rise in adherence and may begin to see a higher rise in the number of SDN problems it is capable of resolving (e.g., 5G networks). Network management, automation, performance, and QoS are all enhanced through supervised and reinforcement learning.

One of the most effective AI technologies is ML for managing and operating autonomous networks because to its capacity to extract information from data, which is fuelled by the availability of data and the theoretical advancement of ML frameworks. Although there have been some analyses of the problems and difficulties for ML in different SDN-based networks there hasn't been much proof that the applications haven't succeeded in providing workable management solutions for autonomous networks. We concentrate on SDN network applications using ML techniques for the other part. We also talk about the future directions for this field of study. The primary problems with ML approaches are noted. Although ML areas have made considerable progress, effective ML is challenging due to challenging patterns and a lack of training data availability. Because of this, many ML programs frequently perform below expectations. We anticipate that our discussions will serve as a straightforward manual for the advancement of SDN and the creation of a more intelligent network. Researchers with various goals can use this study to better understand the fundamental problems in the subject.

Future network design and management will depend heavily on SDN-concept networks using ML techniques in all areas, including resource management, intelligent routing management, network security, flow control, etc. Future research will be done in-depth on the main issues mentioned in the study. The uses of AI/ML in SDN applications increases the potential and worth of these architectures in research and business. Future trends are expected to place an even greater emphasis on AI/ML techniques, as they offer substantial performance improvements.

REFERENCES

[1] Cisco: The Art of Application-Centric Networking. Tech. rep., https://www.cisco.com/c/dam/en/us/solutions/collateral/borderlessnetworks/officeextend-solution/cisco td 030513 fin.pdf

[2] M. R. Belgaum, S. Musa, M.M.Alam, M. M.Su'Ud, A Systematic Review of Load Balancing Techniques in Software-Defined Networking. IEEE Access 8 (2020)98612– 98636. https://doi.org/10.1109/ACCESS.2020.2995849

[3] P. P. Ray, N. Kumar, SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. Computer Communications 169 (2021) 129–153. https://doi.org/10.1016/J.COMCOM.2021.01.018

[4] N. Sultana, N. Chilamkurti, W. Peng, R.Alhadad,Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications 2018 12:2 12(2) (2018) 493–501. https://doi.org/10.1007/S12083-017-0630-0

[5] K. Benzekki, A. El Fergougui, and A. E. Elalaoui,Software-defined networking (SDN): A survey,Secur. Commun. Netw., 9(18) (2016) 5803-5833.

[6] S. Sezer, et al., "Are we ready for SDN? Implementation challenges for software-defined networks," IEEE Commun. Mag., 51(.7) (2013) 36-43.

[7] J. Xie, F. Richard Yu, T. Huang, R. Xie, J. Liu, C. Wang, Y. Liu, A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. COMST 2018 21(1)(2019)393–430. https://doi.org/10.1109/COMST.2018.2866942

[8] Y. Cao, R. Wang, M. Chen, A.Barnawi, AI Agent in Software-Defined Network: Agent-Based Network Service Prediction and Wireless Resource Scheduling Optimization. IEEE Internet of Things Journal 7(7) (2020) 5816–5826.https://doi.org/10.1109/JIOT.2019.2950730

[9] Y. Zhao, Y. Li, X. Zhang, G. Geng, W. Zhang, Y. Sun, "A survey of networking applications applying the software defined networking concept based on machine learning." *IEEE Access* 7 (2019) 95397-95417.

[10] M. Latah, L. Toker, Artificial Intelligence Enabled Software Defined Networking: A Comprehensive Overview. IET Networks 8(2) (2018) 79–99. https://doi.org/10.1049/iet-net.2018.5082

[11] S. Nanda, F. Zafari, C.Decusatis, E.Wedaa, B. Yang, Predicting network attack patterns in SDN using machine learning approach. NFV-SDN, (2017)67–172. https://doi.org/10.1109/NFV-SDN.2016.7919493

[12] J. C. Ferreira, D. Teixeira &J. Macedo, Systematic literature review of AI/ML in software-defined networks using the snowballing approach (2021).

[13] L. Zhu, X. Tang, M. Shen, X. Du, and M. Guizani, Privacypreserving DDoS attack detection using cross-domain traffic in Software Defined Networks, IEEE J. Sel. Area Comm., 36(3) (2018) 628-643.

[14] T.H. Lei, Y.T. Hsu, I. C. Wang, and C. H.P. Wen, Deploying QoSassured service function chains with stochastic prediction models on VNF latency,in Proc IEEE NFV-SDN, 2017, pp.1-6.

[15] W. Li, X. Li, H. Li, and G. Xie, "CutSplit: A decision-tree combining cutting and splitting for scalable packet classification," in Proc. IEEE INFOCOM, 2018, pp.2645-2653.

[16] Y. Sorrachai, D. James, A. X. Liu, and E. Torng, "A sortedpartitioning approach to fast and scalable dynamic packet classification," IEEE ACM T. Network, vol.26,no.4, pp. 1907-1920. 2018.

[17] Chen, X.F., Yu, S.Z.: 'CIPA: A collaborative intrusion prevention architecture for programmable network and SDN', Computers and Security, 2016,58, pp. 1-19.

[18] Sabbeh, A., Al-Dunainawi, Y., Al-Raweshidy, H.S., Abbod, M.F.: 'Performance prediction of software defined network using an artificial neural network'. In Proc. of SAI Computing Conference (SAI), London, UK, July 2016, pp. 80-84.

[19] Chen-Xiao, C., Ya-Bin, X.: 'Research on load balance method in SDN', International Journal of Grid and Distributed Computing, 2016,9,(1), pp. 25-36.

[20] L. S. R. Sampaio, et al., "Using NFV and reinforcement learning for anomalies detection and mitigation in SDN," in Proc IEEE ISCC, 2018, pp.432-437.

[21] F. Francois and E. Gelenbe, "Optimizing secure SDN-enabled interdata centre overlay networks through cognitive routing," in Proc IEEE MASCOTS, 2016, pp.283-288.

[22] X. Huang, T. Yuan, G. Qiao, and Y. Ren, "Deep reinforcement learning for multimedia traffic control in Software Defined Networking," IEEE Network, vol.32, no.6, pp. 35-41, 2018.

[23] N. C. Luong, et al., "Applications of deep reinforcement learning in communications and networking: A survey," arXiv preprint arXiv:1810.07862, 2018.

[24] Y. He, Z. Zhang, and Y. Zhang, "A big data deep reinforcement learning approach to next generation green wireless networks," in Proc IEEE GLOBECOM, 2017, pp. 1-6.

[25] K. Bao, J. D. Matyjas, F. Hu, and S. Kumar, "Intelligent Software-Defined Mesh Networks with link-failure adaptive traffic balancing," IEEE TCCN, vol.4, no.2, pp.266-276, 2018.

[26] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient SDNbased DDoS attack detection and rapid response platform in vehicular networks," IEEE Access, vol. 6, pp. 44570-44579, 2018.

[27] D. Hu, P. Hong, and Y. Chen, "FADM: DDOS flooding attack detection and mitigation system in software-defined networking," in Proc. IEEE GLOBECOM, 2017, pp.1-7

[28] P. Wang, S. C. Lin, and M. Luo, "A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs," in Proc IEEE SCC, 2016, pp.760-765.

[29] Testolin, A., Zanforlin, M., De Grazia, M.D.F., et al.: 'A machine learning approach to QoE-based video admission control and resource allocation in wireless systems. In: Proc. of 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOCNET), Piran, Slovenia, June 2014, pp. 31-38.

[30] S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa, and B. Yang, "Predicting network attack patterns in SDN using machine learning approach," in Proc. IEEE NFV-SDN, 2016, pp.167-172.

[31] C. Song, et al., "Machine-learning based threat-aware system in software defined networks," in Proc. IEEE ICCCN, 2017, pp.1-9.

[32] D. Comaneci, and C. Dobre, "Securing networks using sdn and machine learning," in Proc. IEEE CSE,2018, pp.194–200.

[33] H.Z. Jahromi, A.Hines, and D.T. Delanev, "Towards applicationaware networking: ML-based end-to-end application KPI/QoE metrics characterization in SDN," in Proc. ICUFN, 2018, pp.126–131.

[34] Alvizu, R., Troia, S., Maier, G., Pattavina, A.: 'Matheuristic with machinelearning-based prediction for software-defined mobile metro-core networks', IEEE/OSA Journal of Optical Communications and Networking, 2017,9,(9), pp. D19-D30

[35] Gamer, T.: 'Collaborative anomaly-based detection of large-scale internet attacks', Computer Networks, 2012,56,(1), pp. 169-185.

[36] He, M., Kalmbach, P., Blenk, A., Kellerer, W., Schmid, S.: 'Algorithm-Data Driven Optimization of Adaptive Communication Networks'. In Proc. of IEEE 25th International Conference on Network Protocols (ICNP), Toronto, Canada, Oct. 2017, pp. 1-6

[37] Abubakar, A., Pranggono, B.: 'Machine learning based intrusion detection system for software defined networks'. In Proc. of Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, Sept. 2017, pp. 138-143.

[38] P. Xiao, W. Qu, H. Qi, Y. Xu, and Z. Li, "An efficient elephant flow detection with cost-sensitive in SDN," in Proc IEEE INISCom, 2015, pp.24–28.

[39] M. Latah, and L. Toker, "Towards an efficient anomaly-based intrusion detection for software-defined networks," IET Networks, vol.7, no.6, pp.453-459, 2018.

[40] W. Li, X. Li, H. Li, and G. Xie, "CutSplit: A decision-tree combining cutting and splitting for scalable packet classification," in Proc. IEEE INFOCOM, 2018, pp.2645-2653.

[41] D. Côté, "Using machine learning in communication networks," J. Opt. Commun. Netw., vol.10, no.10, pp. D100-D109, 2018.

[42] Y. Sorrachai, D. James, A. X. Liu, and E. Torng, "A sortedpartitioning approach to fast and scalable dynamic packet classification," IEEE ACM T. Network, vol.26,no.4, pp. 1907-1920. 2018.

[43] D. Chemodanov, P.Calyam, S.Valluripally, H. Trinh, J. Patman & K. Palaniappan. (2018). On qoe-oriented cloud service orchestration for application providers. *IEEE Transactions on Services Computing*, *14*(4), 1194-1208.

[44] B. Leng, L. Huang, C. Qiao, and H. Xu, "A decision-tree-based online flow table compressing method in Software Defined Networks," in Proc IEEE/ACM IWQoS, 2016.pp.1-2.

[45] R. Gomes, M. Ahsan, and A. Denton, "Random forest classifier in SDN framework for user-based indoor localization," in Proc IEEE EIT, 2018, pp.537-542.

[46] Q. Cheng, et al., "Guarding the perimeter of cloud-based enterprise networks: An intelligent sdn firewall," in Proc IEEE HPCC,2018, pp.897-902.

[47] L. Barki, A. Shidling, N. Meti, D. G. Narayan, and M. M. Mulla, “Detection of distributed denial of service attacks in software defined networks,” in Proc IEEE ICACCI, 2016, pp.2576-2581.
[48] P. C. Lin, P. C. Li , and V. L. Nguyen, “Inferring OpenFlow rules by active probing in software-defined networks,” in Proc IEEE ICACT, 2017, pp.415-420.
[49] H. Kuang, Y. Qiu, R. Li, and X. Liu, “A hierarchical K-means algorithm for controller placement in SDN-Based WAN architecture,” in Proc ICMTMA, 2018, pp.263-267.
[50] Z. Fan, and R. Liu, “Investigation of machine learning based network traffic classification,” in Proc ISWCS,2017, pp.1-6.
[51] P. Wang, S. C. Lin, and M. Luo, “A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs,” in Proc IEEE SCC, 2016, pp.760-765.
[52] J. Chavula, M. Densmore, and H. Suleman, “Using SDN and reinforcement learning for traffic engineering in UbuntuNet Alliance,” in Proc ICACCE, 2016, pp.349-355.
[53] S. Sendra, A. Rego, J. Lloret, J. M. Jimenez, and O. Romero, “Including artificial intelligence in a routing protocol using Software Defined Networks,” in Proc IEEE ICC, 2017, pp.670-674.
[54] C. Yu, J. Lan, Z. Guo, Z. Guo, and Y. Hu, “DROM: Optimizing the routing in Software-Defined Networks with deep reinforcement learning,” IEEE Access, vol.6, pp.64533-64539, 2018.
[55] C. Wang, L. Zhang, Z. Li, and C. Jiang, “SDCoR: Software Defined cognitive routing for internet of vehicles,” IEEE Internet Things, vol.5, no.5, pp. 3513 – 3520, 2018.
[56] P. Tang, F. Li, W. Zhou, W. Hu, and L. Yang, “Efficient auto-scaling approach in the telco cloud using self-learning algorithm,” in Proc IEEE GLOBECOM, 2015, pp.1–6.
[57] T. Daher, S. B. Jemaa, and L. Decreusefond, “Softwarized and distributed learning for SON management systems,” in Proc IEEE/IFIP NOMS, 2018, pp.1-7.
[58] N. C. Luong, et al., “Applications of deep reinforcement learning in communications and networking: A survey,” arXiv preprint arXiv:1810.07862, 2018.
[59] Y. He, Z. Zhang, and Y. Zhang, “A big data deep reinforcement learning approach to next generation green wireless networks,” in Proc IEEE GLOBECOM, 2017, pp. 1-6.
[60] S. C. Lin, I. F. Akyildiz, P. Wang, and M. Luo, “QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach,” in Proc IEEE SCC, 2016, pp.25-33.
[61] Sultana, N., Chilamkurti, N., Peng, W., Alhadad, R.: Survey on SDN based network intrusion detection system using machine learning approaches. Peerto-Peer Networking and Applications 2018 12:2 12(2), 493–501 (jan 2018). https://doi.org/10.1007/S12083-017-0630-0
[62] Fathy, C., & Saleh, S. N. (2022). Integrating deep learning-based IoT and fog computing with software-defined networking for detecting weapons in video surveillance systems. *Sensors*, *22*(14), 5075.
[63] Phan, T. V., &Bauschert, T. (2022). Deepair: Deep reinforcement learning for adaptive intrusion response in software-defined networks. *IEEE Transactions on Network and Service Management*.
[64] Kim, G., Kim, Y., & Lim, H. (2022). Deep Reinforcement Learning-Based Routing on Software-Defined Networks. *IEEE Access*, *10*, 18121-18133.
[65] Jiménez-Lázaro, M., Berrocal, J., & Galán-Jiménez, J. (2022, April). Deep Reinforcement Learning Based Method for the Rule Placement Problem in Software-Defined Networks. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-4). IEEE.
[66] Raikar, M.M., Meena, S.M. (2022). Reinforcement Learning Based Routing in Software Defined Network. In: Rout, R.R., Ghosh, S.K., Jana, P.K., Tripathy, A.K., Sahoo, J.P., Li, KC. (eds) Advances in Distributed Computing and Machine Learning. Lecture Notes in Networks and Systems, vol 427. Springer, Singapore. https://doi.org/10.1007/978-981-19-1018-0_16
[67] Al Jameel, Mohammed, Triantafyllos Kanakis, Scott Turner, Ali Al-Sherbaz, and Wesam S. Bhaya. 2022. "A Reinforcement Learning-Based Routing for Real-Time Multimedia Traffic Transmission over Software-Defined Networking" *Electronics* 11, no. 15: 2441. https://doi.org/10.3390/electronics11152441
[68] Huang, X., Yuan, T., Qiao, G., Ren, Y.: Deep Reinforcement Learning for Multimedia Traffic Control in Software Defined Networking. IEEE Network 32(6), 35–41 (nov 2018). https://doi.org/10.1109/MNET.2018.1800097
[69] Liu, W.X., Zhang, J., Liang, Z.W., Peng, L.X., Cai, J.: Content Popularity Prediction and Caching for ICN: A Deep Learning Approach with SDN. IEEE Access 6, 5075–5089 (dec 2017). https://doi.org/10.1109/ACCESS.2017.2781716
[70] Yu, C., Lan, J., Guo, Z., Hu, Y.: DROM: Optimizing the Routing in SoftwareDefined Networks with Deep Reinforcement Learning. IEEE Access 6, 64533–64539 (2018). https://doi.org/10.1109/ACCESS.2018.2877686
[71] Ganesan, E., Hwang, I., Liem, A. T., & Ab-Rahman, M. S. (2021, June). SDN-enabled FiWi-IoT smart environment network traffic classification using supervised ML models. In *Photonics* (Vol. 8, No. 6, p. 201). Multidisciplinary Digital Publishing Institute.
[72] Alvizu, R., Troia, S., Maier, G., Pattavina, A.: Matheuristic with machinelearning-based prediction for software-defined mobile metro-core networks. Journal of Optical Communications and Networking 9(9), D19–D30 (sep 2017). https://doi.org/10.1364/JOCN.9.000D19
[73] Nanda, S., Zafari, F., Decusatis, C., Wedaa, E., Yang, B.: Predicting network attack patterns in SDN using machine learning approach. NFV-SDN 2016 pp. 167–172 (may 2017). https://doi.org/10.1109/NFV-SDN.2016.7919493

[74] Azzouni, A., Pujolle, G.: NeuTM: A neural network-based framework for traffic matrix prediction in SDN. NOMS 2018 pp. 1–5 (jul 2018). https://doi.org/10.1109/NOMS.2018.8406199
[75] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K.L.A., Elkhatib, Y., Hussain, A., Al-Fuqaha, A.: Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges. IEEE Access 7, 65579–65615 (2019). https://doi.org/10.1109/ACCESS.2019.2916648
[76] Wang, P., Lin, S.C., Luo, M.: A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs. SCC 2016 pp. 760–765 (aug 2016). https://doi.org/10.1109/SCC.2016.133
[77] Owusu, A.I., Nayak, A.: An Intelligent Traffic Classification in SDNIoT: A Machine Learning Approach. BlackSeaCom 2020 (may 2020). https://doi.org/10.1109/BLACKSEACOM48709.2020.9235019
[78] Yu, C., Lan, J., Xie, J., & Hu, Y., QoS-aware traffic classification architecture using machine learning and deep packet inspection in SDNs. *Procedia computer science*, *131*(2018)1209-1216.
[79] K. Bhushan, B. Gupta, Distributed denial of service (ddos) attack mitigation in software defined network (sdn)-based cloud computing environment, Journal of Ambient Intelligence and Humanized Computing (2018) 1–13.
[80] M. Begovic, S. Causevic, B. Memic &A. Haskovic AI-aided traffic differentiated QoS routing and dynamic offloading in distributed fragmentation optimized SDN-IoT. *Int. J. Eng. Res. Technol*, *13*(8)(2019) 1880-1895.
[81] F. AL-Tam and N. Correia, “Fractional switch migration in multi-controller software-defined networking,” Comput. Networks, 157(2019)1–10.
[82] N. Saha, S. Bera, and S. Misra, “Sway: Traffic-Aware QoS Routing in Software-Defined IoT,” IEEE Transactions on Emerging Topics in Computing, IEEE Computer Society, (2018)1–12.
[83] H. Yao, X. Yuan, P. Zhang, J. Wang, J. Chunxiao, and M. Guizani, Machine Learning Aided Load Balance Routing Scheme Considering Queue Utilization,IEEE Trans. Veh. Technol.,(2019) 1–1.
[84] I. I. Awan, N. Shah, M. Imran, M. Shoaib, and N. Saeed, An improved mechanism for flow rule installation inband SDN, J. Syst. Archit., 96(2019)1–19.
[85] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan& W. Dai, Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment. *IEEE Transactions on Emerging Topics in Computing*, *9*(2)(2018) 866-877.