Exploring the Synergy: A Review of Machine Learning Techniques in Software Defined Networking (SDN)

Karwan M. Muheden[1*], *Rawshan* N. Othman[2], *Roojwan* Sc. Hawezi[1], *Shadan* M.J. Abdalwahid[1], *Omer* S. Mustafa[1], *Shahab* W. Kareem[1]

[1]Information Systems Engineering Department, Erbil Technical Engineering College, Erbil Polytechnic University, Iraq.
[2]Department of Information Technology College of Engineering and Computer Science Lebanese French University-Erbil, Iraq.

Abstract. Recent years have seen a drastic increase in the varieties and intricacies of network systems which are made up by rapid improvements that follow mobile connections as well as the internet. These systems are becoming increasingly complicated and more sophisticated solutions must be developed to ensure close cooperation, control, activation, and optimization of network structures. But conventional networks, due to their programmatically distributed functionality are a challenge when incorporating machine learning methods for network management. With the emergence of Software Defined Network (SDN), there is a new dimension for introducing intelligence in networks. Particularly, three core characteristics of SDN – unity management, global network visibility, and dynamic rule update - support seamless integration of machine learning technologies. This review provides a comprehensive overview of the literature on machine learning algorithms in SDN frameworks, presenting an extensive survey of this area. The paper systematically describes different machine learning algorithms that have been employed in SDN domains, thereby revealing their implementation opportunities as well as advantages and peculiarities. Furthermore, the review provides an overview of related works and background on SDN-based machine learning approaches for readers to gain a broad understanding of ongoing research in this field. While the topics covered extend beyond algorithmic research, it also challenges integration issues of machine learning into SDN and provides a wider scope. This review aims to be a reliable source of information for researchers, practitioners, and industry experts interested in Software Defined Networks and machine learning applications on network optimization and management.

*Corresponding author: karwan.muheden@epu.edu.iq

1 Introduction

Recently, the volume of data traffic in society has been increasing exponentially with the fast growth of smart appliances and network infrastructure. A couple of years ago the Knowledge Planes approach [1], by using Machine Learning and cognitive methods, suggested taking automation, suggestion, and intelligence to the internet. However, the Knowledge Planes were not prototyped or implemented at the time this article was written. One key explanation is the conventional network systems' fundamentally clustered function that allows every node, for instance, switch or router, to access besides run only in a minor section of the network. It is very difficult to learn of the nodes, only having a little partial sight of the entire system to monitor the system outside the indigenous field [2]. Fortunately, the complexity of schooling can be facilitated by new innovations in software (SDN).

SDN distinguishes the control from the data planes. The logical controller serving as the networking operating system operates SDN network services. The control system can track and collect network in real time status and configurations data, along with granularity information on packet and flow, from a general network view [3]. For the following purposes, it is reasonable and effective to implement machine learning techniques in SDN. The first thing that provides consumers with a strong chance for promising network learning strategies (e.g. deeper neural networking) to make new progress in computational technology for example Graphic Processing Unit or Tensor Processing Unit [4]. Secondly, the knowledge on the algorithms is the gateway in learning of data driven. With a global perspective on the network, the centralized SDN controller will capture different network data that allow the use of machine-learning algorithms [5]. The third solution is to advise the controller of SDN by doing the processing of data, the optimizations of the network, and automating the rendering of the resources of the network based on historical and the data of real time from the network. Finally, the programmability of SDN makes it possible for machine learning algorithms to implement an efficient network solution (e.g. setup and resource allocation) network in real time [6].

The rest of the review paper is prepared as follows: Section 1, introduction. Section 2, introduction to SDN. Section 3, explains machine learning methods in SDN with previous studies. Section 4, challenges. Section 5, some wider viewpoints. Section 6 discussion and the last section 7 conclusion.

2 Introduction to SDN

The SDN paradigm presents centralized design functions and programs that are designed to meet traditional network shortcomings such as the manual setup and maintenance of every network device, high path-recovery latency due to distributed approaches, etc. Figure1 describes the fundamental three layers of SDN (applications, control, and infrastructure).

The Layer of Infrastructure: The devices of the network including the router, switch and access point are part of the Infrastructure Layer in SDN; in this layer, there are many virtual switches like Open v Switches. Packets are primarily forwarded in accordance with the rules delegated to the infrastructure layer [7].

The Layer of Control: The layer control requires a controller that manages the SDN functions in their entirety. This layer serves as a mediator for the layer and operation of the infrastructure. The dispatcher shall handle the whole flow of traffic and shall only decide on programming, transmission of flow and package drops. Controllers interact with each other within the distributed environment via north and south interfaces. The control layer and infrastructure layer interact with one another through southbound APIs like OpenFlow [8].

The Layer of Application: The layer of application is the primary layer of the SDN. It handles enterprise and security systems related to the applications. Examples of technologies operated across the layer include network virtualization, intrusion prevention systems, firewall deployment and the management of mobility [8,9]. The Application Control Plane interface, also referred to as the northbound application interface, communicates with the control layer as shown in Fig1.

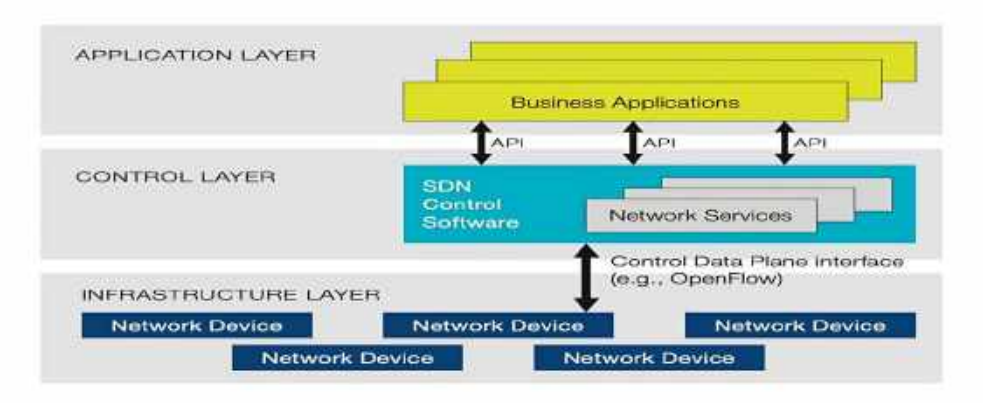

Fig. 1. Architecture of Software defined network

3 Machine learning in SDN

An intelligent computer learns from experience and uses it to boost overall performance (for example, learns from the data generated by its environment).
Learning methods fell into four categories in this context [10].

3.1 Supervised learning

A pre-defined understanding is provided for supervised learning methods. For example, a dataset of training consisting of input/output pairs, where a function mapping as input to a suitable output is learned by the system. This approach allows a dataset representing the system under consideration to be available and can be used to approximation the output of the technique chosen.

3.1.1 Artificiel neural networks in Software Defined Network

Neural neuronal networks are primarily inspired by biological mechanisms of learning such as human brain neurons of biological. Networks with artificial neural have multiple benefits. Firstly, they should compensate for the data without defining direct distribution or function for the model. Secondly, neural networks form an approximate widespread function, which can approximate any function. Thirdly. Nonlinear models are neural networks that allow for versatile representation and modelling of complex relationships [11]. The perceptron of multilayers is the greatest commonly used in the classification of neural networks. The multilayer perceptron is programmed primarily with supervised algorithms in training. Some previous work in SDN using the neural network:
The new model of RouteNet which is based on the Graph Neural Network (GNN), which is capable of understanding the complicated relation among topology, the input of traffic and routing, has been proposed by Rusek et al. [10] to provide reliable approximations of the

delay per source of distribution of destination. Appropriate to resolve the problem of intruding detection of SDN, Kurochkin et al. [12] carried out a machine learning experiment (Neural network). The new neural service chaining (SFC) the architecture of a network based on (GNN) has been proposed by Heo et al. [13], which takes account of Network Topology's graphical organized properties. Mohd et al. [14] proposed a simple class-based diagnosis to detect valves with stiction through multi-computer neural feed forward networks (NN). The collective intrusion prevention architecture Chen et al. [15] suggested the CIPA, which offers a distributed method of intrusion prevention based on the NN approach. A multi-label classification approach was suggested by Kalmbach et al. [16] to predict global network allocations. Alvizu et al. have used an off-line traffic forecasting approach on a mobile network operator for a neural network approach [17]. A method for SDN intrusion detection was proposed by Abubakar et al. [18] based on the NN approach that strong accuracy was obtained by the use of NSLKDD data, reaching 97.3 percent. Sabbeh et al. [19] proposed a Levenberg Marquardt (LM) algorithm-based NN method to predict SDN's efficiency by (RTT) and the amount of the two parameters of training. A risk management technique for the mention of the attacks of DDoS on SDN based on neural networks, threat theory was suggested by Mihai et al. [20].

3.1.2 SVM (Support Vector Machines) in Software Defined Network

To make the classification more generalized, this algorithm recognizes the separators of linear maximizing the margin among two classes. Input data can be converted into a wide size field by kernel methods in order to differentiate between linear separable instances. Complex functions can be defined by SVMs and display robustness against overfitting [21]. There have been works for SVM in SDN that are shown as follows:
The proposed SVM model by Sahoo et al. [21] was used to minimise the vectors of feature measurements, and GA is used to refine various parameters of SVM. The new SDN-enabled DDOS attacks which were proposed by Aslam et al. [22], used an SDN enabled security protocol for the devices of IoT with the assistance of ML algorithms to build a DDoS method of detection and mitigation. Zhao et al. [23] are suggested a single class SVM DDoS attack detection system in SDN, offering a greater detection precision. Kyaw et al. [24] proposed the SVM algorithm of system learning to detect DDOS attacks and to identify usual or threat traffic into an SDN network. In a study by Aung et al. [25], the approach proposed for detecting anomalies involving SVM entropy through the implementation of three processes (the classification of features, extraction of features and the management of flow) as an SDN control stage in POX controllers. In order to achieve better precision, an increased identification rate for SDN DDoS attacks, and lower false alarm rates, Phan et al. [26] suggested a novel method that integrates SVM with the self-organising map. Zhe et al. [27] suggested an SVM solution for the implementation of a filtering scheme for traffic-based classification, which forms the second stage of the proposed process for DoS attack mitigation. Hong et al. [28] proposed FADM to detect and mitigate the attacks of DDoS inside the SDN in real-time. The intelligence framework for the identification of problems and errors in SDN-based surveillance IoT environments was proposed by Canovas et al. [29].

3.1.3 Decision trees in Software Defined Network

In classification problems, decision trees (DT) are highly efficient. A tree-liking structure can be defined by DT. Data may be confidential or continuous input and output. Both Boolean functions can be represented by decision trees [30]. The conducts of a decision tree are a test sequence where every tree node of internal matches one of the input attributes. The desire to consider why the learning algorithm was created is one of DT's core benefits, as it is a normal

approach to humans. This approach is not unusual for people. DT, on the other hand, suffers from overfitting in which the pattern is not contained in the input data and could lead to a wide tree. Such earlier work in SDN using DT:
Mertens et al. [31] have been implemented a simple, successful decision tree algorithm that predicts the route of the data mule by using the sensor measured values as inputs. The traffic classifications of ML Models for in IoT network of traffic engineering of SDN, which is categorized by a random wood algorithm, judgment algorithm and K-nearest neighbors' algorithm, the suggestion was made by Owusu et al [32]. Reticcioli et al. [33] have proposed a novel method of learning a precise model of the dynamic I/O portion of an interconnected system which can be used competently to monitor the queue bandwidth within an SDN paradise, taking historical data as a starting point and adequately merging ARX ID with regression tree and random forests. The improved KD-tree algorithm presented by Mahdi et al. [34], which was used to show different fields using geometric space and also implements the leaf pushing method, which improves the KD tree performance search during the classification into a software-defined vehicle network. In the study of Balta et al. [35], for traffic signalling, which is the most critical urban traffic problem, the 3-stage fuzzy decision tree model was suggested. In the other hand, Dinh et al. [36] suggested a method of C4-5-based detection of intrusion. Nagarathna et al. [37] suggested SLAMHHA to reduce host location hijacking attacks on SDN controllers, which was a supervised learning methodology based on the (ID3) decision tree. For the identification of SDN-based botnets, Tariq et al. [38] used C4.5. The new extensions for decision-trees, i.e., adaptive grouping factor as well as an individual sub-rule structure, to achieve improved parcel classifications with broader regulations have been implemented by Stimpfling et al. [39], and have been decreased by a factor of 3 for memory access.

3.1.4 Ensemble methods in Software Defined Network

Ensemble methods incorporate forecasts for multiple techniques and are generally used to boost the efficiency of learning algorithms. Bagging constitutes the first useful technique used to maximise precision by establishing an enhanced composite classifier that incorporates multiple outputs into a single output of the studied classifiers. Each of them is qualified in instances created by sampling at random and replacing the data set. As opposed to bagging, in boosting, the success of the prior classification influences each classification and seeks to give greater thought to the mistakes of the previous classification. Such earlier works in SDN with ensemble approaches are as follows:
Tsogbaatar et al. [40] suggested a new set of IoT anomaly detection learning models, using SDNs, which are also deep self-encoders, to retrieve functional features in order to pile them in a collaborative learning model. Miao et al. [41] have suggested a modern, SDN approach to detective phishing activities via web-based communications which, using the ensemble learning system, distinguishes the identification mechanisms from end users, with a high degree of precision. The SDN paradigm method based on the ML of QoE has been suggested by Abar et al. [42]. Amaral et al. [43] employed several ML strategies for the classification of traffic, including RF, and extreme gradient boost. Zago et al. [44] suggested a cyber hazard monitoring RF strategy. The intelligent solution to P2P Botnets was put forward by Su et al. [45]. Chen et al. [46] used the SND based DDoS attack detection XGBoost classifier in the cloud. Two ML methods for the control of IP and optical networks were proposed by Choudhury et al. [47].

3.1.5 Supervised deep learning in Software Defined Network

The multifunctional representational-learning approach offers deep learning for general purposes. A computer can discover the representations that are required for classification or identification based on raw knowledge automatically while learning by representation, while traditional machine teachings cannot deal with natural facts. Multi-level representation helps the representation to be converted from low to higher abstract. A large number of these transformations make it possible to learn more complex functions. In contrast with standard algorithms used for several tasks of ML, such as recognition of speech, detection of intrusion, detection of objects, and natural language, the techniques of deep training have achieved better efficiency [48]. Recurrent NN and coevolutionary NN are two more relevant models used in deep learning. Such prior work using the following supervised methods of deep learning in SDN:

The hyper-based method Said et al. [49] proposed to detect anomaly unbalanced dataset attacks based on training models using standard classes, and this test was conducted using the most recent SDN detection of intrusion data set. In order to identify the traffic of data on the basis of applications in a software-based network platform, Raikar et al. [50] propose the incorporation of the SDN architecture and computer training equipment. In order to build a collaborative, intricate detection system with VANETs, Shu et al. [51] used a deep learning approach with generative adverse networks, and explored distributed SDNs that allow multiple controllers of SDN to cooperatively train intrusion sensing models for the entire system, without sharing their sub-network fluxes. A new deep learning model was proposed for SDN by Malik et al. [52], which, in a short time, can reliably classify a broad range of traffic applications, known as Deep-SDN. In comparison with other supervision of supervised ML algorithms, for example, SVM, and DT, Tanget et al. [53] suggested a detection of intrusion method based on the network of deep neural networks. The smart traffic measuring system for SDN, used by available TCAM memory for the setup of measuring rules for big flows, is proposed by Lazaris et al. [54].

3.2 Unsupervised learning in Software Defined Network

Unsupervised methods of learning are presented without predefined information which means that data is unlabelled. The key goal of the framework is therefore to find unique input patterns. Clustering for the identification of beneficial clusters in the input data based on related characteristics identified by the distance of proper metric is an instance of the unsupervised learning strategy.

3.2.1 K-means clustering in Software Defined Network

One of the most common methods of clustering is K-means. This algorithm includes a previous familiarity with the parameter k, showing the clusters number of resulting. The next core of each cluster is assigned to each data point. The objective function representing the detachment between the points of data and their centroids of corresponding is minimalized by K-means. Based on their allocated data points, the method of updating the centers will repeat until the center updates the same points or no point. Most K-means focus on the original clusters set. In other words, all clusters with separate memberships will have a data point. Some previous work with K-means in SDN are described as follows:

In SDN-based cloud settings, Ivannikova et al. [55] suggested a method for detect the usage layer DDoS attack based on a k-media transformation. The k-means approach to achieve Wi-Fi clustering in campus networks was implemented by Nguyen et al [56]. For profiling of

traffic of user on SDN, Bakhshi et al. [57] used k-means on the basis of their application trend.

3.2.2 Self-organizing maps (SOM) in Software Defined Network

The SOM, which depicts high-dimensional distributions in low-dimensional representations called a SOM diagram, is a well-known non-monitored method in neural artificial networks. In several recognition tasks, like quite noisy signals, which are very noisy, SOMs have proved successful. In SOM, instruction takes the map across input data to be created and reorganized. The new input vector is further graded on the basis that its acquiring neuron or node is located in the map.
There are previous SOM works in SDN like:
In order to have a higher identification rate in the cloud prevention of DDoS attacks, Harikrishna et al. [58] suggest a recursive improved SOM and SDN based on the scheme of mitigation. Intrusion detection based on a SOM method was proposed by Jankowski et al. [59]. Wang et al.[60] suggest that Sguard, a light weight DoS threat, can use a mix of access control and SOM classification to identify and minimise the frameworks. DSOM, a distributed SOM technique to fix bottlenecks and overload problems for large-scale SDNs under flood attacks, was suggested by Phan et al. [61]. The lightweight DDoS flood-attack system based on the SOM strategy has been implemented by Braga et al. [62].

3.2.3 Hidden Markov model (HMM) in Software Defined Network

This model of Hidden Markov (HMM), a mathematical model, is believed to be a Markov mechanism with hidden states not observed. The Markov method refers to the Markov supposition that the likelihood of one state being contingent solely on the preceding state. One of the most commonly-used unattended algorithms in HMM is the Baum-Welch algorithm. The following discusses previous studies in SDN that utilized hidden Markov model (HMM):
Huang et al. [63] suggest a constructive method based on the estimation of the matching probability data, and the likelihood is determined using the Markov hidden model (HMM). The system to boost cluster protection and the efficiency of the SDN controller is suggested by Prasanth et al. [64] The Markov secret model (HMM) scheme. With a view to overcoming the load imbalance of the SDN architecture, Yang et al. [65] propose a scheme of optimization of traffic based on the Maximum Entropy HMM within the SDN network. Fan et al. [66] investigated the assessment of the security situation in SDNs based on an HMM. On the other hand, Shan et al. [67] introduced a concept for the identification in HMM-based SDNs of advanced persistent threat.

3.2.4 Unsupervised deep learning approaches in Software Defined Network

The generational models use unsupervised methods of learning to define the order of high association features of input data. Generative models involve the pre-training of unsupervised models to derive structures from the input information. In order to execute the discriminatory job, they will require another top layer. We discuss previous studies in SDN using unsupervised deep learning approaches as follows:
Das et al. [68] have introduced a new SDN-supported wireless network architecture that increases network capacity through unsupervised machine learning (ML) to build ON cells with sufficient RAT. Mao et al. [69] suggested a routing table-oriented approach based on deep faith networks. Zhang et al. [70] have implemented the SDN-based hybrid deep neural network, consisting of the autoencoder stacked with the SoftMax regression layer. The DDoS

detection method based on the SAE was suggested by Niyaz et al. [71] as SDN extractor feature. Liu et al. [72] SAE was used to derive spatio-temporal content popularity characteristics.
Ahmed et al. [73] suggested DNS-based query DDoS attacks mixture for clustering of traffic flows based on Dirichlet phase mixture.

3.3 Reinforcement learning in Software Defined Network

When the machine learns from its environment, based on a series of reinforcements, this method is called reinforcement-learning (RL). For example, whether the mechanism works well or not depends on the reward or penalty. Any environmental activity provides input that the machine uses to understand and update its expertise to the highest extent possible. When only the current state influences the next state (Markovian property), which means a fundamental principle for enhancement education. Prior studies using SDN models and RL approaches will describe the following:
Zolotukhin et al. [74] suggested an intelligent protection mechanism that would be used as the reinforcement machine learning agent to process the existing network status and take a sequence of steps needed to divert such traffic on the network to virtual machines in the form of SDN flows. QoS-aware adaptive routing proposed by Sendra et al. [75] for the distributed hierarchical control aircraft for which the system modelling feature of the processes of Markov decision with QoS compensation function is used. The video streaming adaptive method, based on the Q-learning technique, has been proposed by uzakgider et al. [76] and used for device modelling by the Markov decision process (MDP). The deeper RL approach for the routing of SDN-based optimization was explored by Stampa et al. [77] using the deep deterministic policy gradients approach.

3.4 Semi-supervised learning in Software Defined Network

Labelling and unlabelled data, the system learns from both during semi-supervised learning, that may include random noise due to the absence of labels, and the labelling portion, which is a state among supervised and unsupervised learning. In certain systems in real time, it's more practical, because the data is manually tagged by the professionals, it is always challenging to collect many classified data points, whereas gathering many unlabelled data points is easier. Since it contains some smaller labelled results, semi supervised learning approaches are better than unsupervised learning approaches. Some previous studies using the unsupervised deep learning approaches model in SDN explain as follows:
The new mechanism, called LEDEM, that detects DDoS using a semi supervised algorithm of ML and mitigates the DDoS is proposed by Ravi et al. [78], it also includes the LEDEM mechanism. The effective pre-design routing solution based on the semi-supervised method was developed by Chen et al. [79]. For probability-based classifiers, Loog et al. [80] conduct a semi-supervised parameter calculation.

4 Challenges

Given the efforts conducted in SDN and the demands of robustness and sophistication in the field, many important challenges for research still have to be tackled before a truly smart SDN is broadly deployed in the near future. One of the major challenges is the need to increase the efficacy of the estimate or classification of models trained with appropriate training datasets through ML techniques. A variety of researchers are investigating the relationship among the size of the dataset, the network features, and machine learning

models. Particularly fast-growing fields like machine learning rely on high-quality and well-annotated training datasets. Therefore, it's very challenging to achieve good and sophisticated samples of annotated network traffic over a wide spectrum of applications. This problem can be addressed by uploading freely accessible datasets, which is a popular approach for many machine learning applications. In this way, analogous practices should be realized for the publishing of data linked to networking AI.
Another significant challenge is strengthening network stability. The isolation of data and control planes eliminates the difficulty of network equipment and delivers scalable management of the network. Subsequently, the data plane switches don't have any knowledge, and only send raw data packets towards the controller. Regrettably, this action presents a significant flaw that attackers use to overwhelm the controller with a huge number of flow requests. ML based anomaly detection is also used by the SDN controller to track and attack the network. Nevertheless, the detection of anomalies is an adversarial challenge where malicious attackers are constantly attempting to build original attacks to prevent the discovery of the controller. In this scenario, using historical data to train the models of ML could not be an efficient way to detect attacks because of the creation of new attacks. A Generative Adversarial Network (GAN) is a conceivable solution to overcome the problem by anticipating new attacks.

5 Some Wider Viewpoints

Although, using ML in SDN, gained extensive popularity and has been widely studied, a lot of techniques can affect its growth. In the meantime, the SDN architecture affects not only wired networks, such as IP networks, but also wireless networks, for instance the networks of vehicle, the networks of cellular (such as LTE, 4G and 5G), and the networks of sensor.

6 Discussion

The tables presented in this text provide a comprehensive overview of various machine learning techniques used in Software Defined Networks (SDN) for various objectives. Neural Networks (NN) are utilized to predict network delays and failures, while deep neural networks are used for intrusion detection. Support Vector Machines (SVM) are employed for DDoS attack identification, with deep learning algorithms being suggested for improved classification. Decision Trees are used for packet classification, tracking and blocking DoS attacks, and mitigating server attacks.
Tables 4 through 8 contain information about Ensemble Methods, Supervised Deep Learning K-means Clustering Hidden Markov Models (HMM), and Reinforcement learning. These tables offer a clear picture of the aims, methods, datasets and outcomes of studies in each category. Tsogbaatar et al. particularly focus on the identification of critical attacks by using an IoT anomaly detection model based on ensemble learning technique. Alternatively, Zago et al have appraised the performance of Random Forests K-NN and Naïve Bayes in cyber threat detection such as botnets. Raikara et al. recommend using a supervised learning technique for data traffic analysis. They demonstrate the need for resource and service delivery systematic models incorporating intricate learning theories. Ivannikova et al. try to detect application layer DDoS attacks of SDN cloud systems by using a probabilistic transition that does not require K-means clustering. They suggest corrections to increase the precision of detection. Lastly, Tables 9 and 10 address studies that use reinforcement learning in particular. In this regard, Zolotukhin et al. suggest employing software-defined networking agents and VXLAN bridges to protect devices from attacks; further scalability testing should be done. Sendra et al. combine a routing protocol into SDN design through the leveraging of

reinforcement learning, highlighting the importance to do performance verification in different use cases.

Table 1. Comparison of some existing studies of using NN in SDN

Authors	**Objective**	**Method/Model Used/ Dataset**	**Output and Accuracy**	**Weakness or improvement**
Rusek et al. [10]	To predict the distributionof delays and failure in topologies correctly,	Graph neural networks/ Software-Defined Networks. 14node NSF [76], 24node Geant2 [77] and 50-node Germany50 [78] networks.	Results illustrate that the framework is able to Generalize architectures and traffic matrixes not used in the training of other topologies of network	Deep Learning is a compelling approach to this dynamic difficulty that can harness the complete capacity of SDN.
Kurochkin et al. [12]	to investigate the possibilities of using ML approaches for detection of intrusion in a software control network.	deep neural networks (Keras, TensorFlow) / data set :CSE-CIC-IDS2018	The overall F-measure for two classes declined when a few class instances accomplished their key mission successfully (Out 140 attacks 131 have been identified and only five of the remaining ten have been recognized as benign traffic).	Machine learning algorithms for intrusion detection systems (IDS) research and development that are used in the detection of inappropriate behavior in software-defined networks
Mohd et al. [14]	detecting valves suffering from stiction	multi-layer feedforward neural networks (NN)	Precision of 78% in the predict of loop conditions (75% in sticking and 81% in the non-sticking)	Improvement is required by further training data and pre-processing the signal. in order to better understand the stiction properties within the signals.
Abubakar et al. [18]	To detect intrusion in SDN	Neural Network / NSL-KDD dataset	97.4 percent good detection precision in the detection of training set attacks and 97 percent on the test set, while	Using different dataset.

			97.4 percent total accuracy.	
Mihai et al. [20]	mitigating DDoS attacks in (SDN)	Floodlight controller, Forward Backward-Two input layers-based neural network propagation	The findings presented tend to be the correct approach to minimize DDoS attacks by networks following the SDN definition.	The mitigation time needs to be accelerated by using TLS on the contact channel switch-controller.

Table 2. Comparison of some existing studies of using SVM in SDN

Authors	**Objective**	**Method/Model Used/ Dataset**	**Output and Accuracy**	**Weakness or improvement**
Sahoo et al. [21]	To identify the DDoS attack traffic (SDN) by processing all the packets in a central location.	SVM is assisted by KPCA with genetic algorithm. NSLKDD of dataset.	The accuracy of results 98.907%	Build more interesting algorithms integrating kernel functions with some other typing processes
Kyaw et al. [24]	To comparison current SVM with a scapy, which is the RYU SDN controller and packet generation tool.	polynomial SVM	The evaluation results show that the proposed system would classify DDOS attacks by using the SVM classification with an average precision of about 95 and a false alarm rate of 5 percent.	applying the deep learning
Aung et al. [25]	Method of detection that integrates entropy with SVM	SVM method with three features (classification, extraction and flow management) in SDN. Dataset: ASNM-NPBO	The results demonstrate that the proposed system's total precision range is capable of detecting anomaly attacks with reasonable results and a low false alarm rate.	Anomaly identification can be enhanced by using deep learning algorithms that can use more fixed parameters and more datasets.

Phan et al. [26]	To improve classification efficiency of network traffic.	SVM and SOM	SVM 98.13% and SOM 97.6%, respectively	Different attacks types can added.
Zhe et al. [27]	To mitigate DoS attacks in SDN/OpenFlow networks	Flood Defender is a flexible and protocol independent system with three innovative techniques: table mismanagement, SDN, and flow table track-record.	Experimental findings demonstrate that Flood Defender can effectively mitigate a targeted. DoS attack, causing less than 0.5 percent of total CPU consumption and a maximum 18ms packet delay.	Weakness is will fail with multi controller

Table 3. Comparison of some existing studies of using Decision trees in SDN

Authors	**Objective**	**Method/Model Used/ Dataset**	**Output and Accuracy**	**Weakness or improvement**
Balta et al. [35],	Enhanced the KDtree that uses the geometric space.	KD-tree algorithm/ software defined vehicular networks	An experimental comparison revealed the proposed leaf pushed KD-tree increased packet classification speed up to 24 times.	Parallel platforms such as GPUs can be used to reduce the classification time.
Dinh et al. [36]	To track and block Denial of Service and Probe attacks using unified intrusion Detection and prevention with SDN.	Darpa 99 dataset / C4.5 Decision tree model	IPS will only produce a 60% warning if the network output is above 80 Mbps	Any functional problems could occur with the proposed IDPS because fixed data set
Nagaratn et al. [37]	Hijacking attack to minimize the host location.	(ID3) , MININET, POX controller.	As compared to the Authentication process, less overhead falls in terms of CPU and memory usage. This top-level algorithm senses the attack in three seconds because it can only hit 100 hosts.	To examine better ways to mitigate server attacks from site customers.

Tariq et al. [38]	SDN botnet detection	C4.5 decision tree	The training process was made up of 66.06% regular traffic, and the remaining percentage was from the botnet. 61.63 per cent of the traffic is normal for the testing stage and the remaining traffic is botnet	using bi direction flow counters in SDNs environment to achieve a richer feature set and then assess the accuracy of the detection model.

Table 4. Comparison of some existing studies of using Ensemble methods in SDN

Authors	**Objective**	**Method/Model Used/ Dataset**	**Output and Accuracy**	**Weakness or improvement**
Tsogbaatar et al. [40]	Detect intense attacks and improve the uptime of devices	IOT anomaly detection model for ensemble learning using (SDN). Real-time datasets for test beds and benchmarks	For real-time data, 0.1–0.3 and for benchmark data, 0.1–0.3.	Build and deploy an IoT Multi-Class Identification of Deep Ensemble Learning Model
Abar et al. [42]	Performance Prediction Based on Complete Reference Parametrics (SSIM, VQM) and Device Metrics, SDN Network Knowledge	DCR, RMSE, Weka and using MSU tool.	k=9, Random Forest is the most powerful algorithm for predicting consumer perception.	Improve the QoS parameter data collection such as reaction time and time delay.
Amaral et al. [43]	Traffic data processing in the SDN	SVM, NN and decision trees. unlabelled data-set and smaller dataset.	The results were identical across algorithms, suggesting that SDN-based data is ideal for ML supervised traffic classification.	The review of various types of useful data, such as user accounts, profiles for network use, or circulation forecasts
Zago et al. [44]	To evaluate, identify and respond to current and new cyber threats like botnets	SDN and NFV a Random Forest, K-NN, a Naïve Bayes	Random Forest= 0.985, K-nearest neighbours = 0.984, Naive Bayes= 0.831	Need obtaining as many datasets as possible to test the model with the broadest possible scope

Table 5. Comparison of some existing studies of using Supervised deep learning in SDN

Authors	Objective	Method/Model Used/ Dataset	Output and Accuracy	Weakness or improvement
Raikara et al.[50]	SDN environment proposes characterization of data traffic using a supervised learning approach	SDN platform applications. Tracks of network traffic are collected and features of flows produced that are forwarded to the prediction classifier.	The results of SVM, NB and nearest centroid are 92.3 %, 96.79% and 91.02%, respectively.	The proposed resource/service allocation structure should provide profound learning models.
Shu et al.[51]	To search for unnatural activities in local areas inside the VANET rather than the entire VANET.	deep learning, SDN, (CIDS) for VANETs. NSL-KDD dataset	Experimental findings validate that CIDS is effective and powerful for VANETs in intrusion detection.	Different dataset
Malik et al. [52]	To recognise, in a short time, a broad variety of traffic applications	deep learning model for SDN	96% as an overall accuracy	to use the valuable knowledge gained from the learning process in various network areas for instance resource allocation and routing.
Tanget et al. [53]	In an SDN setting, flow-based anomaly detection	DNN. NSL-KDD Dataset	Their results indicate an accuracy of 99.11 percent and a false alarm rate of 0.46 percent.	Improve the accuracy with other types of feature

Table 6. Comparison of some existing studies of using K-means clustering in SDN

Authors	Objective	Method/Model Used/ Dataset	Output and Accuracy	Weakness or improvement
Ivannikova et al. [55]	Detection of DDoS application layer attacks in SDNN cloud environments	probabilistic transition approach based	The findings show that DDoS attacks on the intermediate application layer can be correctly identified, although	In terms of detection precision, enhance the algorithm and evaluate it with a larger dataset.

			the number of false alarms remains low.	
Nguyen et al [56].	detect and monitor with SDN DDoS attacks in the cloud.	K-means algorithm	provide a better quality of service via cell phone network by reducing the interruption in a wireless environment.	examine caching of data and multicast transmission with Android tablets and create a prototype to be used in a university.
Bakhshi et al. [57]	Proposes the visualization of the network of real-time workload and the accurate providing of services by campus user traffic	OpenFlow traffic exposed to k-means clustering	The maximum Bidirectional packet overhead (4.02 percent) and control traffic rate (4.96 percent) for an edge switch catering, Due to the compilation of flow statistics alone, approximately 600 users do not have a major effect on current OpenFlow channel traffic.	Apply with many controllers

Table 7. Comparison of some existing studies of using K-means clustering in SDN

Authors	**Objective**	**Method/Model Used/ Dataset**	**Output and Accuracy**	**Weakness or improvement**
Harikrishna et al. [58]	By maintaining a smooth detection mechanism during DDoS attacks in the clouds.	SOM and SDN based Mitigation Scheme	Precision of around 21% compared with existing False Minimized systems The False Positive rate of about 19% compared to DDoS benchmarking schemes for literature mitigation.	A SOM based distributed Denial of Service (DDoS) attack mitigation solution is an approximate optimized SDN and neighborhood feature.
Wang et al.[60]	To reduce attacks on the DoS in OpenFlow networks	Implement SGuard a NOX controller security application	Implement SGuard on top of the NOX controller, a security application	To produce more persuasive results, introduce SGuard with larger experimental topologies.

Table 8. Comparison of some existing studies of using K-means clustering in SDN

Authors	**Objective**	**Method/Model Used/ Dataset**	**Output and Accuracy**	**Weakness or improvement**
Huang et al.[63]	Prediction of the likelihood of the entries matching	hidden Markov model (HMM)	As a result, the chance of flow entry matching can be maximized.	Improved by analysing the factors affecting prediction efficiency, counting idle break and the influence of the controller
Prasanth et al.[64]	Enhances cluster security and SDN controller output	Hidden Markov Model (HMM) for analyzing the Big Data for optimized bandwidth utilization	the proposed algorithm will dramatically increase energy efficiency and network life time by using mobile sinks in home automation networks.	a function that recognizes the app on board will be created. Then the authors would suggest a distributed SDN protection controller cluster.
Yang et al.[65]	To overcome the SDN architecture load imbalances	HMM in (SDN) networks	With feedback, SDN network traffic could be optimized and load balancing promoted.	Apply many controllers
Fan et al.[66]	To detect these four attacks (ARP, switch compromise, switch-flooding and network scan) in both data plane and control plane.	hidden Markov model (HMM)	Attacks with the maximum average value of 60,607 and attacks with the second value of59,526, the third value of59,212, the fourth value of32,835, and values of steady time are around 29.	Most attacks are very hard to diagnose. More complicated attacks are also common.

Table 9. Comparison of some existing studies of using Reinforcement learning in SDN

Authors	Objective	Method/Model Used/ Dataset	Output and Accuracy	Weakness or improvement
Zolotukhin et al.[74]	Protection device that senses an attack on time and makes the real-time crisis maximum.	A software-defined networking agent that receives the network state, then uses it to define a network flow which redirects some traffic to a VXLAN bridge.	results show that this particular approach can be used to defend a private network from large-scale attacks.	Further expand the framework's scalability, and evaluate how the system performs for larger and/or more complex networks.
Sendra et al. [75]	To incorporate a routing protocol in the SDN architecture.	the reinforcement learning process that allows searching the most cost-effective path, based on the network status.	The results showed that packet delivery ratio is significantly different.	verify the algorithm's performance in various scenarios and in a virtual lab.

Table 10. Comparison of some existing studies of using Reinforcement learning in SDN

Authors	Objective	Method/Model Used/ Dataset	Output and Accuracy	Weakness or improvement
Ravi et al. [78],	a malicious wireless IoT attack on IoT servers. Attacking DDoS attacks	extreme learning machine (ELM)	Enhanced DDoS attack detection accuracy by 96.28 percent	Additional ML models to improve attack detection accuracy
Chen et al. [79].	Pre-design approach in three areas: extraction of flow characteristics, prediction of requirements and selection of routes.	Semi-supervised clustering algorithm increases the classification and feature extraction performance.	Single restriction factor fails to achieve optimum outcomes of the application itself in the realistic application of bandwidth, costs, energy usage and other factors like protection.	other ML models

7 Conclusion

In general, this review paper offers a comprehensive synopsis of the research initiatives aimed at integrating SDN with machine learning strategies. The survey shows that the deployment of SDN practices instead of different networking problems using machine learning approaches bears great success. The integration of SDN with machine learning has yielded significant improvements in handling complicated issues related to network management, security and optimization. The comparative tables showcase the effectiveness of machine learning techniques in enhancing SDN functionality. However, the paper also highlights that machine learning model resilience in unfavourable circumstances should be considered. While machine learning has shown promise for improving network design, it is important to continue research to deal with challenges including intrusion detection, attack prevention and anomaly identification. Such rigor is necessary to ensure the resilience of these models in different–and sometimes hostile-environments.

In conclusion, the comparative analysis provides a comprehensive understanding of the benefits and drawbacks that are present in various ML methods employed by SDN. This statement acknowledges the dynamic nature of the challenges and opportunities in this emerging field. It is also apparent that the need for continuous research to transform existing models, explore new methods and target peculiar limitations resonates with a high level of intensity. Ultimately, further questions become necessary to better the general efficacy and effectiveness of machine learning use in SDN thus allowing for more adaptable structures that can deal with increasing threats as well as complexities.

References

1. Clark, D. D., Partridge, C., Christopher Ramming, J., & Wroclawski, J. T., A Knowledge Plane for the Internet. Computer Communication Review. 33(4), 3–10, 2003.
2. Mestres, A., Rodriguez-Natal, A., Carner, J., Barlet-Ros, P., Alarcn, E., Sol, M., Munts-Mulero, V., Meyer, D., Barkai, S., Hibbett, M. J., Estrada, G., Ma'ruf, K., Coras, F., Ermagan, V., Latapie, H., Cassar, C., Evans, J., Maino, F., Walrand, J., Muntés-Mulero, V. (2017). Knowledge-Defined Networking Artifacts Review for Knowledge-Defined Networking Knowledge-Defined Networking. ACM SIGCOMM Computer Communication Review, 47(3), 2–10, 2017.
3. Ali, O. M. A., Kareem, S. W., & Mohammed, A. S., Evaluation of electrocardiogram signals classification using CNN, SVM, and LSTM algorithm : A review. In 2022 8th International Engineering Conference on Sustainable Technology and Development (IEC) (pp. 185-191). IEEE, 2022.
4. Wang, M., Cui, Y., Wang, X., Xiao, S., & Jiang, J., Machine learning for networking: Workflow, advances and opportunities. IEEE Network, 32(2), 92–99, 2017.
5. Ma, R., Kareem, S. W., Kalra, A., Doewes, R. I., Kumar, P., & Miah, S., Optimization of electric automation control model based on artificial intelligence algorithm. Wireless Communications and Mobile Computing, 2022.
6. Ciuibao, X., Yubo, M., & Jialiang, L., The impact of Artificial Intelligence on communication networks and services. ITUJournal, 1(1), 33–38, 2018.
7. CEKIC, J., & DUJANOVIC, P., Osnovi Metodologije Planiranja Zdravstvene Za Stite. Higijena; Časopis Za Higijenu, Mikrobiologiju, Epidemiologiju i Sanitarnu Tehniku, 15(1), 3–15, 1963.

8. Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R., Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2), 493–501, 2019.
9. Latah, M., & Toker, L., Artificial intelligence enabled software-defined networking: A comprehensive overview. IET Networks, 8(2), 79–99, 2019
10. Rusek, K., Suarez-Varela, J., Almasan, P., Barlet-Ros, P., & Cabellos-Aparicio, A., RouteNet: Leveraging Graph Neural Networks for Network Modeling and Optimization in SDN. IEEE Journal on Selected Areas in Communications, 38(10), 2260–2270, 2020.
11. Mikhail, Dina Yousif, Roojwan Sc Hawezi, and Shahab Wahhab Kareem., "An Ensemble Transfer Learning Model for Detecting Stego Images." ,Applied Sciences 13.12 : 7021, 2023.
12. Kurochkin, I. I., & Volkov, S. S., Using GRU based deep neural network for intrusion detection in software-defined networks. IOP Conference Series: Materials Science and Engineering, 927(1), 2020.
13. Heo, D., Lange, S., Kim, H.-G., & Choi, H., Graph Neural Network based Service Function Chaining for Automatic Network Control. 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS), 7–12, 2020.
14. Mohd Amiruddin, A. A. A., Zabiri, H., Jeremiah, S. S., Teh, W. K., & Kamaruddin, R., Valve stiction detection through improved pattern recognition using neural networks. Control Engineering Practice, 90(May), 63–84, 2019.
15. Chen, X. F., & Yu, S. Z., CIPA: A collaborative intrusion prevention architecture for programmable network and SDN. Computers and Security, 58, 1–19, 2016.
16. He, M., Kalmbach, P., Blenk, A., Kellerer, W., & Schmid, S., Algorithm-data driven optimization of adaptive communication networks. Proceedings - International Conference on Network Protocols, ICNP, 2017.
17. Alvizu, R., Troia, S., Maier, G., & Pattavina, A., Matheuristic with machine-learning-based prediction for software-defined mobile metro-core networks. Journal of Optical Communications and Networking, 9(9), D19–D30, 2017
18. Abubakar, A., & Pranggono, B.,Feminismo masculino. 2015.
19. Sabbeh, A., Al-Dunainawi, Y., Al-Raweshidy, H. S., & Abbod, M. F., Performance prediction of software defined network using an artificial neural network. Proceedings of 2016 SAI Computing Conference, SAI 2016, 80–84, 2016
20. Mihai-Gabriel, I., & Victor-Valeriu, P., Achieving DDoS resiliency in a software defined network by intelligent risk assessment based on neural networks and danger theory. CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings, 319–324, 2014
21. Sahoo, K. S., Tripathy, B. K., Naik, K., Member, S., & Ramasubbareddy, S., An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks. 2020.
22. Aslam, M., Ye, D., Hanif, M., & Asad, M., Machine Learning Based SDN-enabled Distributed Denial-of-Services Attacks Detection and Mitigation System for Internet of Things. International Conference on Machine Learning for Cyber Security, 180–194, 2020.
23. Zhao, J., Zeng, P., Shang, W., & Tong, G., DDoS Attack Detection Based on One-Class SVM in SDN. International Conference on Artificial Intelligence and Security, 189–200, 2020.
24. Kyaw, A. T., Zin Oo, M., & Khin, C. S., Machine-Learning Based DDOS Attack Classifier in Software Defined Network. 17th International Conference on Electrical

Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2020, 431–434, 2020.

25. Aung, K. M., & Htaik, N. M., Anomaly Detection in SDN's Control Plane using Combining Entropy with SVM. 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2020, 122–126, 2020.
26. Phan, T. V., Bao, N. K., & Park, M., A Novel Hybrid Flow-Based Handler with DDoS Attacks in Software-Defined Networking. Proceedings - 13th IEEE International Conference on Ubiquitous Intelligence and Computing, 13th IEEE International Conference on Advanced and Trusted Computing, 16th IEEE International Conference on Scalable Computing and Communications, IEEE International Conference on Cloud and Big Data Computing, IEEE International Conference on Internet of People and IEEE Smart World Congress and Workshops, UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld 2016, 350–357, 2017.
27. Shang, G., Zhe, P., Bin, X., Aiqun, H., & Kui, R., Flood Defender: Protecting data and control plane resources under SDN-aimed DoS attacks. Proceedings - IEEE INFOCOM, 2017.
28. Hu, D., Hong, P., & Chen, Y., FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking. 2017 IEEE 30 Global Communications Conference, GLOBECOM 2017 - Proceedings, 1–7. 2018-January
29. Rego, A., Canovas, A., Jimenez, J. M., & Lloret, J., An Intelligent System for Video Surveillance in IoT Environments. IEEE Access, 6(c), 31580–31598, 2018.
30. Ali, O. M. A., Kareem, S. W., & Mohammed, A. S., Comparative evaluation for two and five classes ECG signal classification: applied deep learning. Journal of Algebraic Statistics, 13(3), 580-596, 2022.
31. Mertens, J. S., Milotta, G. M., Nagaradjane, P., & Morabito, G., SDN-(UAV)ISE: Applying Software Defined Networking to Wireless Sensor Networks with Data Mules. 323–328, 2020.
32. Owusu, A. L., & Nayak, A., An Intelligent Traffic Classification in SDN-IoT: A Machine Learning Approach. 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 1–6. 2020.
33. Reticcioli, E., Di Girolamo, G. D., Smarra, F., Carmenini, A., D'Innocenzo, A., & Graziosi, F., Learning SDN traffic flow accurate models to enable queue bandwidth dynamic optimization. 2020 European Conference on Networks and Communications, EuCNC 2020, 231–235.2020.
34. Abbasi, M., Rezaei, H., Menon, V. G., Qi, L., & Khosravi, M. R., Enhancing the Performance of Flow Classification in SDN-Based Intelligent Vehicular Networks. IEEE Transactions on Intelligent Transportation Systems, 1–10, 2020.
35. Balta, M., & Özçelik, İ., A 3-stage fuzzy-decision tree model for traffic signal optimization in urban city via a SDN based VANET architecture. Future Generation Computer Systems, 104, 142–158, 2020.
36. Le, A., Dinh, P., Le, H., & Tran, N. C., Flexible Network-Based Intrusion Detection and Prevention System on Software-Defined Networks. 31 Proceedings - 2015 International Conference on Advanced Computing and Applications, ACOMP 2015, 106–111, 2016.
37. Nagarathna, R., & Shalinie, S. M., SLAMHHA: A supervised learning approach to mitigate host location hijacking attack on SDN controllers. 2017 4th International Conference on Signal Processing, Communication and Networking, ICSCN 2017.

38. Tariq, F., & Baig, S., Botnet classification using centralized collection of network flow counters in software defined networks. International Journal of Computer Science and Information Security,14(8),1075–1080, 2016.

39. Stimpfling, T., Bélanger, N., Cherkaoui, O., Béliveau, A., Béliveau, L., & Savaria, Y., Extensions to decision-tree based packet classification algorithms to address new classification paradigms. Computer Networks, 122, 83–95, 2017.

40. Tsogbaatar, E., Bhuyan, M. H., Taenaka, Y., Fall, D., Gonchigsumlaa, K., Elmroth, E., & Kadobayashi, Y., SDN-Enabled IoT Anomaly Detection Using Ensemble Learning. In IFIP Advances in Information and Communication Technology: Vol. 584 IFIP. Springer International Publishing, 2020.

41. Miao, M., & Wu, B., A Flexible Phishing Detection Approach Based on Software-Defined Networking Using Ensemble Learning Method. Proceedings of the 2020 4th International Conference on High Performance, Compilation, Computing and Communications, 70–73, 2020.

42. Abar, T., Ben Letaifa, A., & El Asmi, S., Machine learning based QoE prediction in SDN networks. 2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017, 1395–1400, 2017.

43. Amaral, P., Dinis, J., Pinto, P., Bernardo, L., Tavares, J., & Mamede, H. S., Machine learning in software defined networks: Data collection and traffic classification. Proceedings - International Conference on Network Protocols, ICNP, 2016-December(NetworkML), 91–95, 2016.

44. Zago, M., Ruiz Sánchez, V. M., Gil Pérez, M., & Martínez Pérez, G., Tackling Cyber Threats with Automatic Decisions and Reactions Based on Machine-Learning Techniques. Presented at EuCNC'17: 2nd Conference on Network Management, Quality of Service and Security for 5G Networks, Held at European Conference on Networks and Communications, At Oulu (Finland), September 2017.

45. Su, S. C., Chen, Y. R., Tsai, S. C., & Lin, Y. B., Detecting P2P Botnet in Software Defined Networks. Security and Communication Networks, 2018.

46. Chen, Z., Jiang, F., Cheng, Y., Gu, X., Liu, W., & Peng, J., XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-Based Cloud. Proceedings - 2018 IEEE International Conference on Big Data and Smart Computing, BigComp 2018, 251–256, 2018.

47. Choudhury, G., Lynch, D., Thakur, G., & Tse, S., Two use cases of machine learning for SDN-Enabled IP/Optical networks: Traffic matrix prediction and optical path performance prediction. ArXiv, 10(10), 52–62, 2018.

48. Karwan, M., Abdullah, O. S., Amin, A. M., Mohamed, Z. A., Bestoon, B., Shekha, M., & Salihi, A., . Cancer incidence in the Kurdistan region of Iraq: Results of a seven-year cancer registration in Erbil and Duhok Governorates. Asian Pacific Journal of Cancer Prevention: APJCP, 23(2), 601. 2022.

49. Said Elsayed, M., Le-Khac, N.-A., Dev, S., & Jurcut, A. D., Network Anomaly Detection Using LSTM Based Autoencoder. Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 37–45, 2020.

50. Raikar, M. M., Meena, S. M., Mulla, M. M., Shetti, N. S., & Karanandi, M., Data Traffic Classification in Software Defined Networks (SDN) using supervised-learning. Procedia Computer Science, 171(2019), 2750–2759, 2020.

51. Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M., Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach. IEEE Transactions on Intelligent Transportation Systems, 1–12, 2020.

52. Malik, A., De Frein, R., Al-Zeyadi, M., & Andreu-Perez, J., Intelligent SDN Traffic Classification Using Deep Learning: Deep-SDN. 2020 2nd International Conference on Computer Communication and the Internet, ICCCI 2020, 184–189, 2020.
53. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M., Deep learning approach for Network Intrusion Detection in Software Defined Networking. Proceedings - 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking, 258–263, 2016.
54. Lazaris, A., & Prasanna, V. K., Deep Flow: A deep learning framework for software-defined measurement. CAN 2017 - Proceedings of the 2017 Cloud-Assisted Networking Workshop, Part of CoNext 2017, 43–48, 2017.
55. Ivannikova, E., Zolotukhin, M., & Hämäläinen, T., Probabilistic transition-based approach for detecting application-layer DDoS Attacks in encrypted software-defined networks. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10394 LNCS, 531–543, 2017.
56. Nguyen, T. M. T., Hamidouche, L., Mathieu, F., Monnet, S., & Iskounen, S., SDN-based Wi-Fi Direct clustering for cloud access in campus networks. Annales Des Telecommunications/Annals of Telecommunications, 73(3–4), 239–249, 2018.
57. Bakhshi, T., & Ghita, B., OpenFlow-enabled user traffic profiling in campus software defined networks. International Conference on Wireless and Mobile Computing, Networking and Communications, 2016.
58. Harikrishna, P., & Amuthan, A., SDN-based DDoS Attack Mitigation Scheme using Convolution Recursively Enhanced Self Organizing Maps. Sadhana - Academy Proceedings in Engineering Sciences, 45(1), 2020.
59. Jankowski, D., & Amanowicz, M., Intrusion detection in software defined networks with self-organized maps. Journal of Telecommunications and Information Technology, 2015(4), 3–9. 2015.
60. Wang, T., & Chen, H., SGuard: A lightweight SDN safe-guard architecture for DoS attacks. China Communications, 14(6), 113–125, 2017.
61. Phan, T. V., Bao, N. K., & Park, M., Distributed-SOM: A novel performance bottleneck handler for large-sized software-defined networks under flooding attacks. Journal of Network and Computer Applications, 91, 14–25, 2017.
62. Braga, R., Mota, E., & Passito, A., Lightweight DDoS flooding attack detection using NOX/OpenFlow. Proceedings - Conference on Local Computer Networks, LCN, 408–415. 2010.
63. Huang, G., & Youn, H. Y. (2020). Proactive eviction of flow entry for SDN based on hidden Markov model. Frontiers of Computer Science. 14(4), 1–10, 2020.
64. Prasanth, L. L., & Uma, E., Hidden Markov Model Based Secure Cluster Management in Software Defined Networking. 5, 123–126, 2020.
65. Yang, Y., & Sun, H., Research on Traffic Optimization Scheme of SDN Network Based on ME-HMM. Journal of Physics: Conference Series, 1624, 042052, 2020.
66. Fan, Z., Xiao, Y., Nayak, A., & Tan, C., An improved network security situation assessment approach in software defined networks. Peer-to-Peer Networking and Applications, 12(2), 295–309, 2019.
67. Shan-Shan, J., & Ya-Bin, X., The APT detection method in SDN. 2017 3rd IEEE International Conference on Computer and Communications, ICCC 36, 2018-January,
68. Das, D., Bapat, J., & Das, D., Unsupervised Learning Based Capacity Augmentation in SDN Assisted Wireless Networks. SN Computer Science, 1(4), 2020.

69. Mao, B., Fadlullah, Z. M., Tang, F., Kato, N., Akashi, O., Inoue, T., & Mizutani, K., Routing or Computing? the Paradigm Shift Towards Intelligent Computer Network Packet Transmission Based on Deep Learning. IEEE Transactions on Computers, 66(11), 1946–1960, 2017.

70. Zhang, C., Wang, X., Li, F., He, Q., & Huang, M., Deep learning–based network application classification for SDN. Transactions on Emerging Telecommunications Technologies, 29(5), 2018.

71. Niyaz, Q., Sun, W., & Javaid, A. Y., A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN). ICST Transactions on Security and Safety, 4(12), 2017.

72. Liu, W. X., Zhang, J., Liang, Z. W., Peng, L. X., & Cai, J. (2017). Content Popularity Prediction and Caching for ICN: A Deep Learning Approach with SDN. IEEE Access, 6(c), 5075–5089. https://doi.org/10.1109/ACCESS.2017.2781716

73. Ahmed, M. E., Kim, H., & Park, M., Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking. Proceedings - IEEE Military Communications Conference MILCOM, 2017-October, 11–16, 2017.

74. Zolotukhin, M., Kumar, S., & Hamalainen, T., Reinforcement learning for attack mitigation in SDN-enabled networks. Proceedings of the 2020 IEEE 37. Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization, NetSoft 2020, 282–286, 2020.

75. Sendra, S., Rego, A., Lloret, J., Jimenez, J. M., & Romero, O., Including artificial intelligence in a routing protocol using Software Defined Networks. 2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017, Sepa, 670–674, 2017.

76. Uzakgider, T., Cetinkaya, C., & Sayit, M., Learning-based approach for layered adaptive video streaming over SDN. Computer Networks, 92, 357–368, 2015.

77. Stampa, G., Arias, M., Sánchez-Charles, D., Muntés-Mulero, V., & Cabellos, A., A deep-reinforcement learning approach for software-defined networking routing optimization. ArXiv, 14–16, 2017.

78. Ravi, N., & Shalinie, S. M., Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture. IEEE Internet of Things Journal, 7(4), 3559–3570, 2020.

79. Chen, F., & Zheng, X., Machine-learning based routing pre-plan for SDN. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9426, 149–159, 2015.

80. Loog, M., Contrastive Pessimistic Likelihood Estimation for Semi-Supervised Classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(3), 462–475, 2016.