Analysis of Different Attacks on Software Defined Network and Approaches to Mitigate using Intelligent Techniques

P. Karthika, Dr. A. Karmel
School of Computer Science and Engineering
Vellore Institute of Technology, Chennai Campus, Chennai, India

***Abstract*—The detection of DDoS (Distributed Denial of Service) attacks is essential topic under network security. DDoS attacks cause network services to become unavailable by repeatedly flooding servers with unwanted traffic. The volume, magnitude, and complexity of these attacks increased dramatically as a result of low-cost Internet connections and easily available attack tools. Both Software Defined Networking (SDN) and Deep Learning (DL) have recently found a number of practical and fascinating applications in industry and academia. SDN enables centralized management, a global view of the overall network, and configurable control planes, allowing network devices to adapt to diverse applications. When applied to diverse categorization problems, DL-based approaches outperformed classic machine learning techniques, while SDN characteristics offer better network monitoring and security of the managed network when compared to traditional networks. By inheriting the non-linearity of neural networks, they increase feature extraction and reduction from a high-dimensional dataset in an unsupervised way. An overview of deep learning algorithms for sensing distributed denial of service attacks in software-defined networks with Deep learning is presented within this article. Furthermore, SDN environment is simulated in Mininet using RYU controller. In addition, each paper's mitigation method is examined in the survey.**

***Keywords*—Distributed Denial of Service (DDoS); Software Defined Networking (SDN); attack detection; Mininet; OpenFlow; mitigation; machine learning; deep learning**

I. Introduction

As a result of consecutive evolution of network infrastructure, unending extension of network professional requirements, the massive development of Internet economy in the Internet environment, network facilities containing critical business and industry information have permeated modern society's production and life. The introduction of DDoS assaults can result in irregularities in associated network services, resulting in significant economic losses and even disastrous effects. DDoS assaults are a severe danger to the Internet's network security. The accurate and rapid detection of DDoS assaults is a critical study area in the security industry. The network and control planes are separated in SDN, which is a novel network design. [1-2] enabling network programmability, centralized administration control and interface opening.

Controllers operate solely as packet forwarders in a new networking paradigm, isolating control logic from forwarding and switching aspects. The data plane is made up of network components such as switches that are controlled by the controller in the control plane (also known as Open Flow or simply referred to as OF switches). In large-scale and high-performance computer systems, decoupling the routing plane and forwarding plane is crucial for gaining higher performance. Additionally, it simplifies network management by centralizing configuration and management within the controller. This technique enables for more frequent modifications because the administrator does not have to configure and reconfigure all of the network devices to execute network updates and adjustments. They can utilize the controller to quickly and effectively implement policy and network configuration needs.

To manage data plane, the controller requires numerous core services. It enables the exchange of data with application layer services that perform network functions such as routing, load balancing and intrusion detection. The application layer's services the applications are mapped to entire network by an operating system of network installed on the controller and provides a high level of optimization, automation and network control. Java APIs for local communication and representational state transfer (REST) APIs for remote communication are used by the applications to interface with the controller.

However, a very factor that propels SDN networks to prominence and popularity too exposes them to slew of novel security threats. The distributed denial-of-service (DDoS) attack is a unique of these consumes the utmost devastating outcome on an SDN network. If the network is not adequately protected, DDoS attacks can overwhelm the controller. To defend the SDN network against DDoS attacks, there is a variety of documentation available. In networks, Intrusion Detection Systems (IDSs) sniff packets and alert the administrator if a Distributed Denial of Service (DDoS) assault is identified. One strategy that is attracting the attention of researchers is the use of machine learning to detect distributed denial of service assaults. Defending SDN against threats is continuing research area.

A. Motivation

In past 5 years, the DDoS attacks have strained more attention towards the cyberspace. In large networks, Intrusion Detection Systems (IDS) are widely used to safeguard the network from threats. However, IDS are not a practical option for real-time monitoring, leaving systems open to various

attacks. Attackers continue to develop new processes and strategies for deceiving protection systems, allowing them to illegally use accessible software and harm service providers. Several ways of dealing with DDoS attacks have been proposed in previous research. Various ML/DL techniques have been proposed in earlier studies to fight against DDoS attacks. The goal of this research is to aid the research field in developing and inventing new DDoS attack remedies.

The following are the main contributions of this survey work:

- In the context of SDN, an overview of several types of DDoS attacks are provided.
- Mininet was used to emulate the SDN environment.
- Based on machine learning and deep learning approaches, an in-depth assessment of the most important DDoS detection and mitigation solutions are provided.
- The research issues in SDN deployment and security that need to be investigated are highlighted.

The rest of this paper is structured as follows. Section II details a related work that includes an overview of DDoS attack types, mitigation approaches, and the creation of SDN in Mininet. Section III discusses the need for artificial intelligence in SDN and the various methodologies arrived at using Deep Learning discusses in section IV. The research issues in the deployment and security of SDN are outlined in section V, and the discussion is presented in section VI.

II. Related Work

A. Overview of DDoS Attack

This kind of attack results in the inability of legitimate users to access services and is thus denoted as DoS (Denial of Service) attacks [3]. Consider the following attack situation: A hacker can send several service inquiries to the enterprise to register with organization or obtain connection to some enterprises legitimate service instances. The organizational server will get overwhelmed with service requirements and cannot deliver services to other right customers/users. Another possible assault scenario is one in which numerous machines are used to perform a denial-of-service attack:

Organization's or enterprise's network connects a significant number of machines. Suppose an attacker obtains access to individual or more extra computers belonging to an organization or enterprise. This can abuse the opportunity plus perform DoS attacks against further systems in similar network subnet. This attack surface is extensive in this case; an attacker can take over many machines (Zombies) as well utilize them to execute DoS. Aforementioned type of DoS assaults sometimes referred to as a Distributed Denial of Service attack (DDoS). Fig.1, classifies DDoS attacks.

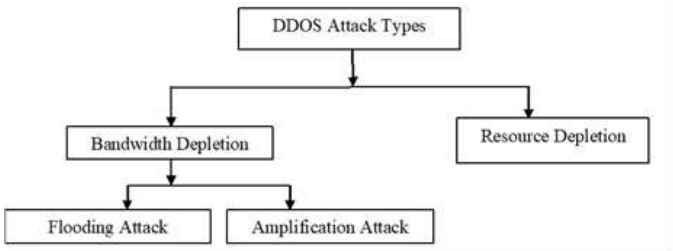

Fig. 1. DDoS Attack Classification.

In addition to Bandwidth deficiency and resource deficiency attacks, around two more classes of DoS attacks are available: Bandwidth Depletion plus Resource Depletion. Bandwidth Depletion is an attack that attempts into overwhelm network with network packets. Bandwidth Depletion attacks are classified as follows: Attackers who use flooding or amplification.

- Flooding attacks seek to overwhelm the network's resources by sending an excess quantity of ICMP or UDP packets.
- Amplification attacks attempt towards the advantage of the IP address broadcast features found on majority of routers. Aforementioned aspect enables a directing system to provide a broadcast internet protocol address instead of a specific address as the destination address. Smurf and Fragile assaults are examples of such attacks [4]. In Resource Depletion assaults, the attacker suffocates the target system's resources. This attack perhaps conducted by attacking a network protocol (for example, Neptune, mail bomb) or generating malformed packets (for example ping of death, Apche2, teardrop Back, land, etc.) and sending them over the network to the victim machine. A concise description of several of these attacks [5] is provided in Table. I.

1) DDoS attack detection: The primary approaches for detecting DDoS attacks are classified as detection of attack established on traffic features as well detection of attack created on traffic abnormality. The first collects numerous attack characteristics and produces a database of DDoS assault characteristics. We can determine whether DDoS, attacks a network by relating and examining the data statistics included in current network data packet as well nature of database. Expert systems, model reasoning, features matching and state transition are primary implementation methods. The latter is generally used to construct a traffic model including analyse aberrant flow variations to assess whether or not the traffic is abnormal and determine whether or not the server has been attacked. Fig. 2, depicts a flowchart of identifying DDoS assault in different stages.

TABLE I. DDOS – ATTACKS, DESCRIPTIONS AND FEATURES

DDoS Attack	Description	Attack features
Land attack	The attacker transmits a manipulated SYN packets with the similar source and destination address. It is helpful in several TCP/IP implementation	Consider the feature 'Land' to detect the attack. If 'Land' is 1, the source address and destination address are alike. Thus, trait is critical in detecting assault.
Smurf attack	Smurf attack is denial-of-service amplification attack whereby an attacker transmits many ICMP echo packets through fake address of the victim's computer to broadcasting internet protocol address. Each host on the broadcast network answers when the packet is received that the victim's system uselessly uses their resources.	This attack might be identified on the victim system by looking at an enormous amount of victim machine ICMP echo responses without transmitting packets from the victim machine to an ICMP echo request.
Teardrop attack	The attacker attempts to transmit the fragmented packets to the intended recipient. Attackers adjust the fragment offset such that the following packets overlap. If the receiving target operating system's IP fragmentation reassembly code contains a fault, the computer will crash owing to inappropriate processing of the overlapping packets.	The feature 'Wrong Fragment', is sum of the connection's faulty checksum packets, provides some insight into the erroneous IP packets. As a result, this attribute is critical in identifying the attack.
Ping of Death attack	An attacker sends an IP packet more significant than the 65,536-byte limit to elicit a "ping of death" denial of service (DOS). The maximum permissible IP packet size is 65.535-bytes, comprising 20-bytes long packet header. This crashes or freezes the machine.	By recording the scope of every ICMP packet and identifying which are larger than 65,535-bytes, and tried Ping of Death can be found.
Mail bomb attack	Mail bomb attacks occur when unauthorized users send a massive sum of e-mail messages through considerable additions to specific mail server, clogging up disc-space and denying other users email capabilities.	This type of attack can be spotted by the presence of thousands of e-mail information from a single person in a short-period.
SYN flood attack	TCP/IP implementation is used in SYN flood. The SYN request is sent to the victim system by an attacker. The victim responds with an ACK and waits for a response. Each half-open connection's information is added to the pending connection queue by the server. The victim server system's half-open links will soon plug the queue, and the system will turn out to be inadequate towards acquire further connections.	A flood assault via SYN may be separated from regular network traffic while searching for many simultaneous SYN packs intended for a specific machine that comes from unattainable host.

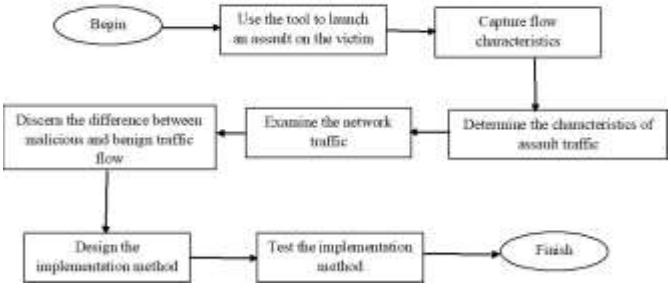

Fig. 2. Stages of Identifying DDoS Assault.

B. Software Defined Network

Deep packet analysis is possible via a complete network view in the revolutionary architecture environment of SDN [6]. It allows for quick response and changes to traffic policies and procedures. The SDN allows perceptual regulators of global visualization illustration to be flexible and timed. Quick deployment that is schedule-aware and intelligent scheduling that is service-aware.

Though assuring network facilities plus lowering implementation value, the software defined network improves user experience and enables more comprehensive network rollout promotion. Fig. 3, shows software defined network architecture. It is visibly clear that the architecture is divided into Applications, Controller and Data plane, which enables us to identify and mitigate attacks in SDN.

Lin and Wang [7] offered DDoS assault detection and defence technique based on SDN. Still, system required three Open flow management tools to accomplish anomaly detection using Flow standard, making implementation and operation complicated.

Yang et al. [8] described a strategy for combining flow statistics and IP entropy-specific information. Using a single flow as well as internet protocol entropy characteristic information, the flow and IP entropy distinctive information are detected, resulting in a more effective and precise detection impact. While information entropy is adaptable and appropriate, it must be used with other technologies to determine the threshold and multi-element weight distribution.

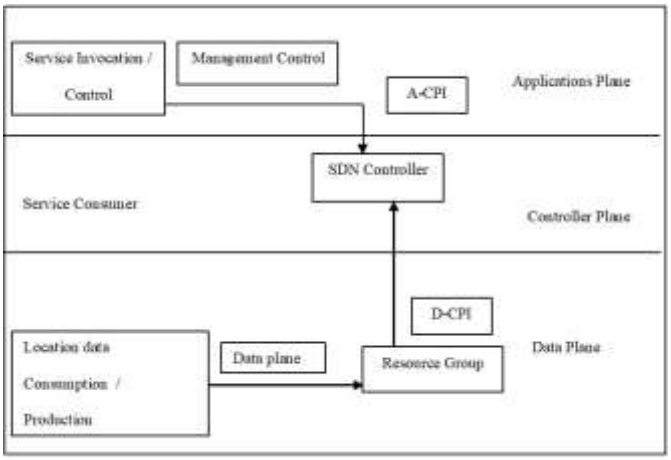

Fig. 3. Software Defined Network Architecture.

Author [9] suggested that to detect DDoS attacks, the approach must analyse the features of each ICMP/TCP/UDP protocol using the training ANN algorithm, which is difficult and ineffective.

In [10], the author presented a strategy for identifying and preventing DDoS assaults in a large network, however it is not suitable for simple implementation. [11] offers a logical source and destination IP address database-based DDoS attack detection system. When a DDoS attack occurs, it investigates the unusual properties of the source and destination IP addresses. It successfully verifies the DDoS attack using the non-parametric cumulative algorithm CUSUM, but the approach needs to change and set the threshold.

Data entropy and the usage of the data-mining method, in which the SOM methodology is most prominent, have been found to be the most important factors in DDoS detection in SDN networks. The SOM algorithm requires determining the number of neurons in advance because of the high false-positive information entropy rate.

1) Mininet and openflo: Mininet is a virtual network device emulator that simulates virtual network devices such as hosts, switches, controllers, and links. Mininet switches offer OpenFlow for highly flexible custom routing and Software-Defined Networking, and its hosts run conventional Linux network software. Mininet makes it easier to conduct research, development, learning, prototyping, testing, and debugging on a laptop or other PC.

Mininet :

- Low-cost and easy-to-use testbed for developing OpenFlow applications.
- Rapid software-defined network prototyping.
- Without the requirement to set up a physical network, complex topology testing may be performed.
- The same topology can be worked on by multiple developers at the same time.

OpenFlow :

- The interface between the OpenFlow controller and the OpenFlow switches is defined by the OpenFlow protocol.
- The OpenFlow protocol assists the OpenFlow controller in instructing the OpenFlow switches how to handle incoming packets.
- Using multiple packet header data, identify and classify packets from an ingress port.
- The packets are dropped or pushed to a specific egress port or to the OpenFlow Controller.

2) Creating SDN in mininet: First, use the following command to construct a topology with a single switch and five separate hosts.

sudo mn --topo single,5 --mac --controller remote --switch ovsk

We need to execute as a sudo instance since we need to access the kernel protocol stack as root. Fig.4 depicts the creation of SDN in Mininet.

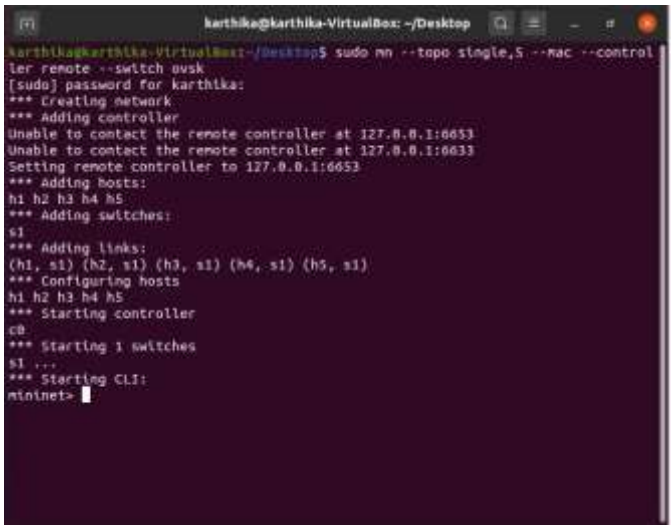

Fig. 4. SDN in Mininet.

It has added switches to three separate hosts, h1, h2, and h3, and that the links are h1 to s1, h2 to s1, and h3 to s1, forming a star topology. It was unable to reach the remote controller on the local PC every time it attempted to add the controller. The controller is generally connected to two ports: 6653 and 6633. It is looking for the controller, but no controller has been executed yet.

The next step is to run the controller in the RYU controller's mininet directory. The following command is used to start the controller,

PYTHONPATH=. ./bin/ryu-manager
ryu/app/simple_switch_13.py

The ryu-manager application is set to run in verbose mode, and it will configure the switch as well as install the forwarding rules. The default python script used inside the RYU controller as shown in Fig.5 and it performs similar to a forwarding manager. It assists in packet forwarding from one machine to another.

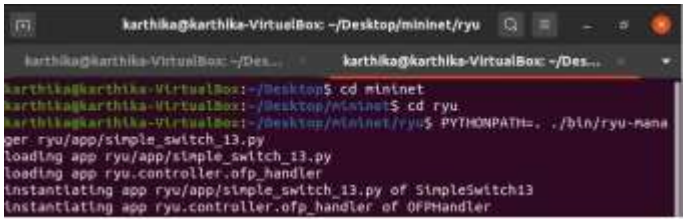

Fig. 5. Connection of RYU Controller to the Switch.

Now, the following command is used to ping the hosts, h1 ping h2

Fig.6 depicts how specific packets are delivered to the controller, which then configures the associated switch based on that packet.

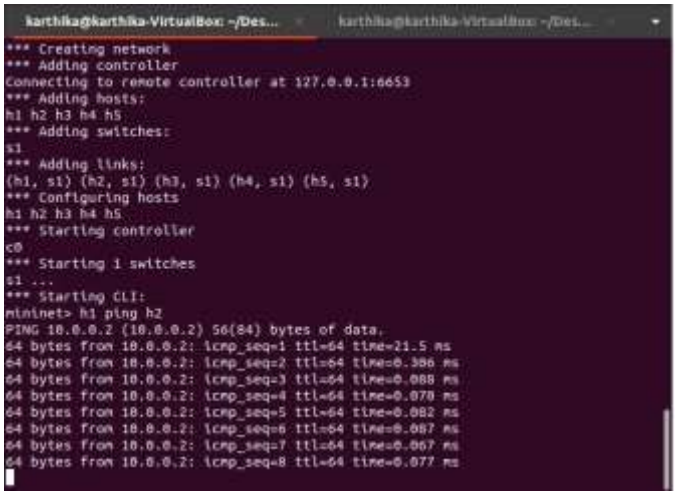

Fig. 6. Successful Packet Transfer.

When we examine the switch's response time, the initial packet sent took 21.5ms, while the remaining ping packets took 0.306ms and 0.088ms. Because the switch has no knowledge of how to forward the first packet when it arrives. As a result, the switch generates an OpenFlow event, which is forwarded to the controller. Fig.7 depicts the OpenFlow event that have been generated.

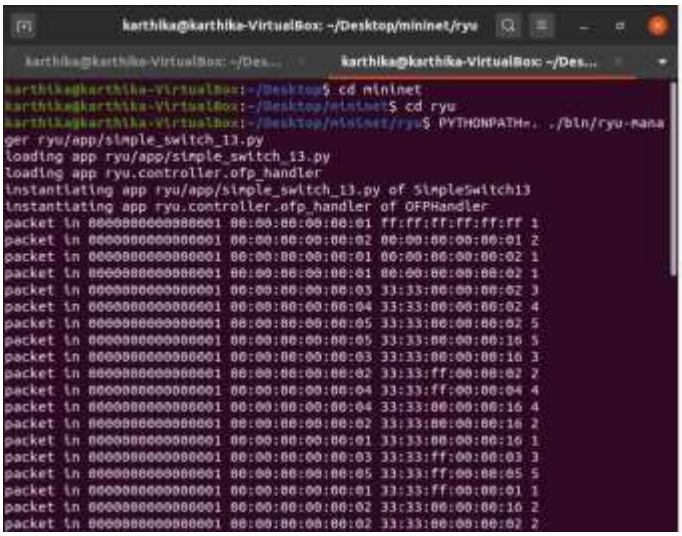

Fig. 7. OpenFlow Event.

The OpenFlow event will be generated and transmitted to the appropriate switch, which will then forward it to the appropriate RYU controller application. That specific switching application will build the rules, configure the switch with the rules, and then forward the packet. The packet will remain in the switch's buffer throughout this period. As a result, the initial packet has a higher delay, whereas the remaining packets have a shorter delay.

III. Artificial Intelligence

Artificial Intelligence (AI) is the process of teaching machines to require human intelligence, particularly the human brain and its reasoning abilities. AI systems develop the ability to reason and conduct actions that have the best likelihood of reaching a certain goal, similar to the human brain.

A. Need for Artificial Intelligence in SDN

The diverse network infrastructure adds complexity to networks and creates a slew of issues for organizing, controlling, and maximizing network resources effectively. Traditional network systems are designed to be dispersed, with every node, such as a remote device like switches and routers, seeing and reacting to just a minor portion of the system. Learning to offer control outside the local domain from nodes with only a partial perspective of the entire system is a challenging process. The training process has been made easier because to recent improvements in Software Defined Networking (SDN).

In SDN, both the control and data planes are decoupled. In an SDN architecture, the data plane contains real and virtual switches that serve as forwarding devices. Remote switches are software-based switches that work with a number of different operating systems. Using the Control Plane's structure, these data plane switches are responsible for forwarding, discarding, and manipulating packets (CP). The CP can use the Southbound Interfaces (SBIs) interface to regulate the data plane's converting and forwarding capabilities.

Control plane stands "brain" regarding SDN system, capable of programming network sources, dynamically updating forwarding guidelines as well enabling formative and agile network administration. The central controller, which is responsible for managing communication between forwarding devices and applications, is the most important part of CP. On the one hand, the controller takes network status data from the data plane and passes it along to the application plane. In other circumstances, the controller develops custom rules based on application requirements and assigns them to promotional items. Important network application capabilities including network topologies storage, state data notification, device structure, and shortest path routing are all provided by the controller.

The Networking Operating System (NOS) handles network resources with a logically centralized controller (NOS). The SDN controller has the ability to programme the network in real time. The centralised controller has a complete perspective of the network by observing and accumulating real-time network state and configuration data, as well as packet and flow graininess statistics. The following factors justify the usage of machine learning performances in SDN.

1) Recent advances in computing technology, such as the Graphics processing unit (GPU) and Tensor Processing Unit (TPU), give a perfect chance to apply credible machine learning approaches to the network area (e.g., Deep Neural Networks) [12], [13].

2) Accounting Data is vital factor to the algorithms for data-driven basic cognitive process. The central Controller has a comprehensive network interpretation and the ability to collect a large amount of network data, allowing machine learning approaches to be used.

3) By accessing data, upgrading networks, and automating network service delivery with legitimate and previous network data, machine learning algorithms can provide data to the SDN controller. Furthermore, SDN's programmability allows the network to implement the optimal network solutions (Example: Resource allocation & configuration) identified by machine learning algorithms in real-time.

ML is an area of particular study focuses on design methods that can acquire automatically from information and encounter hidden design not including explicitly programmed to do so [14]. Classification of ML algorithms depend on their learning approach and functional similarities [14]. Fig .8, summarizes ML methodologies according to their learning approach.

Machine learning approaches are considered efficient strategies in order to increase detection rates, decreasing false alarm rates, and decreasing the costs of computing and transmitting [15]. Machine learning approaches are classed as either supervised, unsupervised, or semi-supervised [16].

Because of their high classification power and computational efficiency, support vector machine (SVM) approaches are extensively used in NIDS research. They can be used with information that has a lot of dimensions. It is, nevertheless, critical to utilize the correct kernel function. A resource-intensive program places a high premium on computational processing units and memory [14]. While random forest method [17] is collective supervised learning approach for dealing along unequal data and vulnerable to over fitting.

Unsupervised learning methods derive the configuration and illustrations of data from enabled inputs. Unsupervised learning algorithms anticipate unidentified data by modelling entire system or delivery of the data [15]. Techniques for feature contraction, such as PCA, and clustering, such as self-organizing maps, are included in unsupervised learning methods (SOM).

PCA is an approach that significantly accelerates unsupervised feature learning [24]. Numerous scholars utilize PCA to pick features before performing classification. Clustering techniques like the K-means algorithm and other distance-based learning algorithms are used to find anomalies. The problem with using clustering algorithms to discover anomalies is that they are vulnerable to early conditions like the centroid, which can lead to a large number of false positives [18].

Semi-supervised learning is a type of supervised learning that uses unlabelled data for training and labelled data for testing. The training data set is made up of a small amount of tagged data and a big number of unlabelled data. It's beneficial in situations where significant amounts of tagged data aren't available, such as image archives with only a subset of the images labelled (for example, a person's image within a group photo). Simultaneously, the vast majority are not labelled [19]. MPCK-means, a semi-supervised clustering algorithm, was employed to improve the detection system's performance [20].

B. Distributed Denial-of-Service Attack Mitigation in Software Defined Network

Mitigation of distributed denial of service (DDoS) attacks is also crucial for protecting network resources under assault. Researchers used packet migration, intake bandwidth restriction, connection migration, modifying time outs, and a controller to manage protocols to resist DDoS attacks in networks based on Software-Defined networking architecture.

Shin et al. [21] developed a technique for mitigating saturation attacks by extending the Open Flow data plane's capabilities. They improved Avant-Guard by including two new modules: a network migration section and a trigger activation module. Before alerting the control plane, the connection migration module might move failed TCP sessions to it. The actuating trigger element collects network and packet payload data and uses it to trigger various flow rules depending on the situation. To demonstrate their solution, they employed the Net FPGA architecture.

Wang et al. [22] promoted protection for SDN networks using a lightweight, active and protocol-autonomous structure called Flood Guard. The proactive segment dynamically generates aggressive flow procedures based on SDN controller's run-time logic, preserving network strategy requirement. To avoid getting overwhelmed, the packet migration segment caches packets and transfers them to the controller via rate-limiting and round-robin forecast.

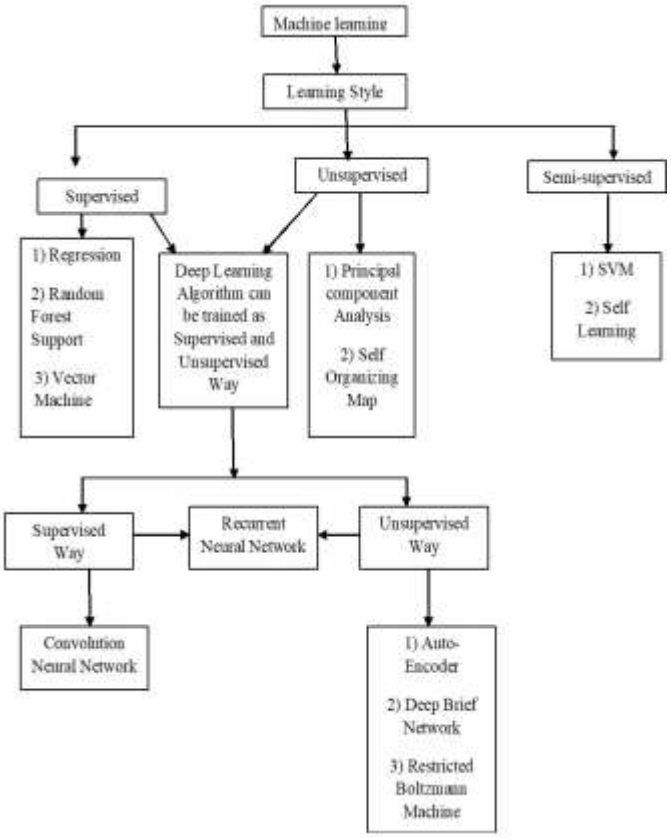

Fig. 8. ML Methodologies.

Piedrahita et al. [23] developed FlowFence, quick and lightweight DDoS attack mitigation method. The degree of use of router and SDN controller interfaces is monitored in this approach to determine the state of congestion. When a router identifies congestion on one or more interfaces, it alerts the controller, who orders the router to limit bandwidth on those interfaces.

Wang et al. [24] proposed an assured method for access control that requires entities to be authenticated. One such approach comprises three modules:

- Policy management, authentication and registration.
- Access mechanism and communication strategy.
- Trace back with audit strategy.

To communicate with another entity, it must first schedule with validation and registration segment which offers a passcode for subsequent message. They realized all components at the SDN architecture's application layer. By creating a POX controller, they validated their technique.

Yuan et al. [25] employed a peer support technique to minimize DDoS attacks on flow table overflows by pooling the available unused RAM throughout the entire SDN system. Their approach takes into account all switches on a peer-to-peer basis. When a switch is attacked, other switches will assist the targeted switch by donating their unused flow table space, thereby minimizing the DDoS attack. They approximated the vacant areas of switches that are not under attack using queuing theory.

Dridiet al. [26] proposed a unique SDN guard system for defending SDN networks versus DDoS outbreaks by dynamically rerouting malicious traffic as well managing flow-time outs. They built the solution by means of Mininet as well validated that it can reduce controller performance by up to 32%.

To avoid flooding attacks, Phan et al. [27] presented an effective approach based on support vector machines dubbed Idle-time Adjustment (IA). Before begin, the flow collector accumulates data from switches, which is subsequently extracted by the extractor. Following that, SVM-I processes the related features. Following that, whichever the flow is passed to the strategy implementation module or also the IA algorithm, depending on the outcome of SVM-I. The IA algorithm will handle the flow if the result is standard; if it isn't, it will be sent to strategy implementation, which will run a novel framework.

Sahay et al. [28] suggested a solution called ArOMA towards mitigating DDoS attacks by leveraging the SDN's centralized manageability and programmability highlights. At the ISP end, a controller receives the alarm and generates a switch policy to manage the DDoS attack. They utilized a RYU controller to validate the strategy.

Hameed et al [29] developed a combined way for defending SDN against DDoS attacks. They set the Controller-to-Controller protocol (C-to-C), enabling SDN controllers to impart and securely exchange threat information. They used Mininet to create the POX controller for authentication purposes.

Conti et al. [30] suggested a DDoS mitigation strategy in SDN that combined route spoofing and resource fatigue. Selective Blocking gathers internet protocol and MAC address data and sends it to the controller for further processing. Regular observation measures the entropy of destination address (Internet protocol) and port to establish the dataspace between them to detect probable aberrant behavior. On Mininet, they implemented a target scenario.

The northbound program was utilized by Karmakar et al. [31] to mitigate DDoS assaults in SDN. To combat DDoS attacks, this system took advantage of the specification and storing of security policies. They used the ONOS controller to validate their technique.

To secure the control plane from DDOS attacks, Wang et al. [32] proposed the Safe-Guard-Scheme (SGS). The BPNN approach is used by the anomaly detection module to find any irregularities in the given network flow. Using flow-blocking rules to remap a controller's flows stops the hosts from transmitting bogus traffic.

To counteract the Domain Name System amplification threat, Houda et al. [33] developed the wisdom SDN. To map DNS requests and responses one to one, the suggested method employs a proactive and stateful technique. The DDoS detection module collects flow characteristics to assess network traffic unpredictability before using a Bayes network-based filtering algorithm to categorise bogus DNS requests based on entropy. If the classified illegal traffic features' speed exceeds the band, the DNS mitigation (DM) mechanism systematically drops the illegitimate DNS request.

Adaptable modular frameworks, according to Daz et al. [34], can identify and mitigate LR-DDoS assaults utilizing SDN settings. The proposed work employed the CIC Dos dataset to analyze the performance of six machine learning methods for training the intrusion detection system: Random Tree, J48, RF, REP Tree, SVM, and MLP.

In order to improve the accuracy of detection with low-rate DDoS attacks, Zhijun et al. [35] developed a multi-feature DDoS attack detection approach based on FM principles and investigated the mechanism of attacks outside of the SDN data layer. This paper proposes a defense strategy based on the fundamentals of dynamic deletion in flow rules, and the results are studied to demonstrate the defense strategy's effectiveness. Some of the existing approaches challenges are listed in Table. II.

TABLE II. CHALLENGES OF EXISITNG APPROACHES

Author	Approaches	Challenges
Shin et al. [21]	Avant-Guard	Network scanning attacks and TCP SYN flood resilience may be increased by the connection migration components of Advent - Guard. As a result, network developers protecting against DoS attacks or using TCP and UDP may not find it useful. Normal network connections experience a slight but noticeable delay when connection migration is used.
Wang et al. [22]	Flood Guard	The proposed method faces two difficulties. The first is the deployment of a single data plane cache to serve all switches. Another difficulty is the usage of TCAM, which does not have the memory to carry out all proactive requirements.
Piedrahita et al. [23]	FlowFence	The proposed effort focuses on simple bandwidth to reduce DoS impact rather than wider topologies.
Wang et al. [24]	Software defined security networking mechanism (SDSNM)	It has limited influence on finding the attacker with the host in the botnet when access control is lax, and it has no impact in finding the genuine attacker.
Yuan et al. [25]	QoS-aware mitigation strategy	The proposed effort focuses on preventing switches from becoming overloaded, rather than preventing the attacker node from gaining access to the network
Dridiet al. [26]	SDN-Guard	Instead of discarding the flow, the proposed solution predicted it as harmful if it crossed the threshold value and routed it to its destination via least-used links with high time-out. As a result, the amount of bandwidth consumed by switches grows.
Phan et al. [27]	Idle-time Adjustment (IA)	The proposed study focuses on specific sorts of assaults, such as ICMP and TCP SYN flooding, rather than broader forms of attacks.
Sahay et al. [28]	ArOMA	The proposed method was tested using a simple network environment with only one controller and no real-time mitigation mechanism is provided.
Conti et al. [30]	Route Spoofing and Resource Exhaustion	The number of attacks detected using the proposed approach is higher, but the precision is a little weak.
Houda et al. [33]	wisdom SDN	Large values cause flow rules to stay in the OF table for a long period, exhausting the TCAM of OF switches, while tiny values cause legitimate DNS responses to be dropped.
Daz et al. [34]	6 ML algorithm (J48, Random Tree, REP Tree, Random Forest, MLP, SVM)	The administrator must manually intervene in order to reset the host's flow, drop probability.

IV. DEEP LEARNING

DDoS attacks are still the most common and lethal danger to current and next-generation network systems. DDoS attacks have evolved besides in frequency and severity but also in sophistication overtime. Transport layer DDoS attacks like TCP-SYN and UDP flooding, as well as network layer DDoS operations like ICMP flooding, were the most common threats to networks. As ML and DL's capacity to detect threats improves, more challenging and precise DDoS operations, known as application-layer attacks, emerge. DDoS application-layer assaults are more advanced and focused threats that exploit a server's resources. As a result, traditional attack detection techniques that rely on packet-level data are rendered ineffective.

To identify DDoS attacks, data from network traffic flow must be used to build a network-based Intrusion Detection System (IDS) that employs cutting-edge networking techniques like Software-Defined Networking (SDN). The control plane (CP) is detached from the network in SDN, which is a revolutionary networking prototype. The aforementioned technique differs from traditional network design in how it works. Users can use this technology to dynamically recreate routing operations in network systems like switches and routers. These capabilities enable in-line and network-based threat detection and mitigation measures to be implemented.

Deep Learning algorithms are new evolution of Artificial Neural Networks (ANN)which use plentiful, inexpensive computers. Deep learning enables an algorithm to discover representations for data that exhibit varying degrees of generalization. These algorithms have been used in various fields, including network intrusion, object detection, detection and visual object recognition [36]. A deep learning structure perhaps trained in either supervised or unsupervised fashion [15]. Supervised training of a deep learning algorithm, Convolution Neural Networks (CNNs) [37] remain usually taught in a supervised manner. CNN is presently de facto typical model for the applications of computer-vision.

A. Unsupervised Deep Learning Algorithm

The auto encoder [38] utilized to discover a description (encoding) for a collection of data to reduce its dimension. When trained unsupervised on collection of examples, a Deep Belief Network (DBN) [39] might train to rebuild its data. After that, the layers operate as feature detectors for the data. Following aforementioned learning stage, a DBN is trained further to do categorization in supervised manner. DBNs, also known as restricted Boltzmann machines RBM's or an auto-encoders, are helpful for feature learning, dimension reduction, topic modelling, regression and collaborative filtering.

B. Supervised or Unsupervised Algorithm

Recurrent Neural Network (RNN) algorithm [38] is a method for supervised or unsupervised learning. This network might process inputs in random order by utilizing internal memory. RNNs are frequently used in speech recognition [38]. These networks are effective at predicting characters in the text and recognizing patterns that have existed for a long time. Recent advances in deep learning algorithms for identifying and mitigating DDoS assaults in SDN are summarized in the Table. III.

TABLE III. TECHNIQUES ON RECENT DEEP LEARNING- DETECTING AND MITIGATING DDOS ATTACKS IN SDN

Publication	Deep Learning Techniques	Traffic collection	Tool used	Inference / Challenges	Accuracy
Nisha Ahuja et al, 2021 [40]	SAE-MLP	Mendeley Data	Ryu controller	On the basis of the dataset's features, network traffic is classified as normal or malicious.	99.75%
Auther Makuvaza et al, 2021 [41]	DNN	CICIDS 2017	CICFlowMeter	Improved F1 score, precision and recall	97.59%
Noe M Yungaceila-Naula et al, 2021 [42]	RF, SVM, KNN, MLP, CNN, GRU, LSTM	SDN Controller and CICDoS2017, CICDDoS2019	ONOS Controller and CICFlowMeter	The architecture's deployment simplifies its migration to production environments.	Above 99% using two public datasets
Arul and Punidha, 2021 [43]	Supervised Deep Learning Vector Quantization	MemCached server	Learning vector quantization (LVQ)	By analyzing the efficiency of cloud-mounted systems, the limitations of a static and interactive grouping of various DDoS-encrypted cross-site assault detection methodologies are overcome.	97.23%
Lu Wang, Ying Liu, 2020 [44]	CNN	POX SDN Controller and CICIDS2017	POX Controller	With a high recall and F-score, accurate and precise results are obtained. The time required to train a neural network can be reduced.	98.98%
Shahzeb Haider et al, 2020 [45]	CNN	CICIDS-2017	CICFlowMeter	Attack detection is precise, despite the computational complexity.	99.45%
Lotfi Mhamdi et al, 2020 [46]	SAE- 1SVM	CICIDS2017	CICFlowMeter	Works well with unbalanced and unlabeled datasets, resulting in more accurate and improved attack detection.	99.35%
Mahmoud Said Elsayed et al, 2020 [47]	RNN	CICDDoS2019	CICFlowMeter	Results that are significantly improved in respect of precision, F-score, and recall	99%
Beny Nugraha and Rathan Narasimha Murthy, 2020 [48]	CNN-LSTM	SDN Controller	ONOS Controller	When confronted with a huge dataset, deep learning prototype performs conventional prototype.	99.99%
Trung V. Phan et al, 2020 [49]	RL Technique	SDN Controller	ONOS Controller	Improved precision, recall, F-score and accuracy. But the proposed scheme was validated for selected network scenarios	Above 90%

V. REASERCH CHALLENGES

Though SDN enhances network speed and network monitoring management, intelligence centralization comes with its own set of security, scalability, and elasticity issues. SDN presents a number of security challenges, which are listed in this section.

A. OpenFlow Switches / Flow Table Pace

DDoS attacks against OpenFlow switches can be launched through a number of network devices to slow down or stop legal flow. The size of the OpenFlow table of the switches is one of the main vulnerabilities of SDN. Due to the growing demand for a fast and reliable data plane, flow tables are typically implemented using TCAM, which is highly expensive and limited in size [25]. By forwarding attack flow for route discovery, these compromised switches will overwhelm the controller. As a result, these compromised switches will become a major constraint for the entire network.

B. Traffic Flow

The majority of DDoS attacks are intended to generate traffic that appears to be legitimate (Low-rate DDoS attack) and is difficult to detect [23, 34,35]. The mitigation module will block the flow if the present flow exceeds the rate limit because it is unable to discriminate between regular and malicious flows. This degrades the network performance. As a result, a legitimate and robust security solution is required that can effectively differentiate between benign and anomalous network data flows.

C. Communication Links

Network performance could be harmed if communication links between switches and controllers fail. The attacker can utilize resources in both the data plane and the control plane by delivering a large number of table-miss messages. When a switch receives a new flow for which there are no matching flow rules in the flow table [22], the data plane will request actions from the control plane. As a result, scalability and security problems arise.

D. Single Point of Failure

The control plane and the data plane are decoupled in Software Defined Networking (SDN), which makes it easier to deploy new services. In the meantime, a controller faces a security threat. Because of SDN's centralized nature, the

controller can become a bottleneck, and attackers can use this flaw to perform distributed denial-of-service (DDoS) attacks against it through switches [30, 32, 44]. The attackers may be able to bring down the entire network if the centralized controller is compromised. The research community faces an open problem in developing a robust and reliable controller.

VI. Discussion

In this study, various proposal for detection and mitigation of DDoS attacks in SDN are discussed. However, the main goal of this study is to derive certain conclusions about ML/DL detection methods.

Many of the studies included in this paper employ a simulated dataset rather than a real one, which reduces the accuracy level. The learning phase of ML/DL techniques is used to learn from a specified dataset and build a training model to detect patterns. Although several studies have shown promising results in detecting assaults, it is usually recommended that the methodologies be tested in a large-scale network.

As attackers might devise new techniques to launch new attacks, various studies sought to mitigate specific types of attacks, leaving the approaches open to other types of DDoS attacks. Another note is that few studies used simulation tools to initiate an attack flow and normal flow, but real-world DDoS attackers employ a compromised host to launch a DDoS attack. This method should be used to validate the effectiveness and resilience of a defense system in a real-world setting.

VII. Conclusion

Software-defined networks are the way of the future. It enables abstraction with its programmable features. The rise of SDNs also poses security concerns due to the architecture's centralized intelligence. With the continued growth of extensive data and computing capacity, deep learning methods have exploded in popularity and are now widely used in various fields. Deep learning has the potential to extract more accurate representations from data to generate significantly more accurate models. This paper examines the use of ML/DL approaches in SDN systems to mitigate DDoS attacks. The Convolutional Neural Network-Long-Short Term Memory (CNN-LSTM) model is determined to be an effective and efficient way for identifying slow DDoS attacks in the software-defined network environment, according to the accuracy gained in the review paper. With the survey mentioned above on Deep learning techniques, we intend to continue working and touching on other areas in the future to fully exploit the significant potential of deep learning techniques for DDoS.

References

[1] H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li, and C. F. Cheang, “A survey on security-aware network measurement in SDN,” Security and Communication Networks, Article ID 2459154,2018.

[2] J. Cao, M. Xu, Q. Li, K. Sun, Y. Yang, and J. Zheng, “Disrupting SDN via the data plane: a low-rate flow table overflow attack, “in Proceedings of the 13th EAI International Conference on Security and Privacy in Communication Networks, Niagara Falls, Canada, October 2017.

[3] G. Mantas, N. Stakhanova, H. Gonzalez, H. H. Jazi, and A. A.Ghorbani, “Application-layer denial of service attacks: taxonomy and survey,” International Journal of Information and Computer Security, vol. 7, no. 2-4, pp. 216–239, 2015.

[4] D. Kumar, “DDoS attacks and their types,” Network Security Attacks and Countermeasures, p. 197, 2016.

[5] MIT. (1999) Darpa intrusion detection attacks database. [Online]. Available: http://www.ll.mit.edu/ideval/docs/attackDB.html

[6] Y. Li, Z. Cai, and H. Xu, “LLMP: exploiting LLDP for latency measurement in software-defined data center networks,” Journal of Computer Science and Technology, vol. 33, no. 2, pp. 277–285, 2018.

[7] H. Lin and P.Wang, “Implementation of an SDN-based mechanism against DDOS attacks,” in Proceedings of the 2016 Joint International Conference on Economics and Management Engineering (ICEME 2016) and International Conference on Economics and Business Management (EBM 2016),Pennsylvania, Penn, USA, 2016.

[8] J. G. Yang, X. T. Wang, and L. Q. Liu, “Based on traffic and IP entropy characteristics of DDOS attack detection method,” Application Research of Computers, vol. 33, no. 4, pp. 1145–1149,2016.

[9] A. Saied, R. E. Overill, and T. Radzik, “Detection of known and unknown DDOS attacks using artificial neural networks,” Neurocomputing, vol. 172, pp. 385–393, 2016.

[10] N. Z. Bawany, J.A. Shamsi, and K. Salah, “DDOS attack detection and mitigation using SDN: methods, practices, and solutions,” Arabian Journal for Science and Engineering, vol. 42, no. 2, pp.425–441, 2017.

[11] X. Wang, M. Chen, C. Xing, and T. Zhang, “Defending DDOSattacks in software-defined networking based on and destination IP address database,” IEICE Transaction on Information and Systems, vol. E99D, no. 4, pp. 850–859, 2016.

[12] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, “Machine learning for networking: Workflow, advances and opportunities,” IEEE Network, vol. 32, no. 2, pp. 92–99, March 2018.

[13] M. Usama, J. Qadir, A. Raza, H. Arif, K.-L. A. Yau, Y. Elkhatib,A. Hussain, and A. Al-Fuqaha, “Unsupervised machine learning for networking: Techniques, applications and research challenges,” arXivpreprint arXiv:1709.06599, 2017.

[14] Atkinson RC, Bellekens XJ, Hodo E, Hamilton A, Tachtatzis C(2017) Shallow and deep networks intrusion detection system: ataxonomy and survey. CoRR, arXiv preprint arXiv:1701.02145.2017 Jan 9.

[15] Zamani M, Movahedi M (2015) Machine learning techniques for intrusion detection. CoRR, arXiv preprint arXiv:1312.2177. 2017Jan 9

[16] Aburomman AA, Reza MBI (2016) Survey of learning methods in intrusion detection systems. International conference on advances in electrical, electronic and system Engineering (ICAEES), Putrajaya, pp 362–365.

[17] Niyaz Q, Sun W, Javaid AY, Alam M (2016) A deep learning approach for network intrusion detection system. International conference wireless networks and mobile communications (WINCOM).

[18] Bennett KP, Demiriz A (2017) Semi-supervised support vector machines. NeuralComput &Applications 28(5):969–978.

[19] Haweliya J, Nigam B (2014) Network intrusion detection using semi supervised support vector machine. Int J ComputAppl 85, 9.

[20] LeCun Y, Bengio Y, Hinton G (2015) Deep learning review. Weekly journal of science in nature international. Nature 521.

[21] S. Shin, V. Yegneswaran, P. Porras, G. Gu, Avant-guard: Scalable and vigilant switch flow management in software-defined networks, in:Proceedings of the 2013 ACM SIGSAC Conference on Computer &Communications Security, 2013, pp. 413–424.

[22] H. Wang, L. Xu, G. Gu, Floodguard: A dos attack prevention extension in software-defined networks, in: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, IEEE, 2015, pp.239–250.

[23] A.F.M. Piedrahita, S. Rueda, D.M. Mattos, O.C.M. Duarte, Flowfence: adenial of service defense system for software defined networking, in:2015 Global Information Infrastructure and Networking Symposium, GIIS,IEEE, 2015, pp. 1–6.

[24] X. Wang, M. Chen, C. Xing, SDSNM: a software-defined security networking mechanism to defend against DDOS attacks, in: 2015 Ninth International Conference on Frontier of Computer Science and Technology, IEEE,2015, pp. 115–121.

[25] B. Yuan, D. Zou, S. Yu, H. Jin, W. Qiang, J. Shen, Defending against flow table overloading attack in software-defined networks, IEEE Trans. Serv.Comput. 12 (2) (2016) 231–246.

[26] L. Dridi, M.F. Zhani, SDN-guard: DOS attacks mitigation in SDN networks, in: 2016 5th IEEE International Conference on Cloud Networking, Cloudnet, IEEE, 2016, pp. 212–217.

[27] T.V. Phan, T. Van Toan, D. Van Tuyen, T.T. Huong, N.H. Thanh, Open-FlowSIA: An optimized protection scheme for software-defined networks from flooding attacks, in: 2016 IEEE Sixth International Conference on Communications and Electronics, ICCE, IEEE, 2016, pp. 13–18.

[28] R. Sahay, G. Blanc, Z. Zhang, H. Debar, ArOMA: An SDN based autonomic DDOS mitigation framework, Computer. Security. 70 (2017) 482–499.

[29] S. Hameed, H. Ahmed Khan, SDN based collaborative scheme for mitigation of DDOS attacks, Future Internet 10 (3) (2018) 23.

[30] M. Conti, C. Lal, R. Mohammadi, U. Rawat, Lightweight solutions DDOS attacks in software defined networking, Wireless. Networks. 25(5) (2019) 2751–2768.

[31] K.K. Karmakar, V. Varadharajan, U. Tupakula, Mitigating attacks in software defined networks, Cluster Computing. 22 (4) (2019) 1143–1157.

[32] Y. Wang, T. Hu, G. Tang, J. Xie, J. Lu, SGS: Safe-guard scheme for protecting control plane against DDOS attacks in software-defined networking, IEEEAccess 7 (2019) 3469934710.

[33] Z. A. El Houda, L. Khoukhi and A. S. Hafid, "Bringing Intelligence to Software Defined Networks: Mitigating DDoS Attacks," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2020.3014870.

[34] J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," IEEE Access, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[35] W. Zhijun, X. Qing, W. Jingjie, Y. Meng and L. Liang, "Low-Rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network," in IEEE Access, vol. 8, pp. 17404-17418, 2020, doi: 10.1109/ACCESS.2020.2967478.

[36] Deng L, Yu D (2014) Deep learning methods and applications. Microsoft Research. Available https://www.microsoft.com/en-us/research/publication/deep-learning-methods-and-applications/.

[37] Alom MZ, Bontupalli VR, Taha TM (2015) Intrusion detection using deep belief networks. Aerospace and electronics conference, IEEE.

[38] Hughes T, Mierle K (2013) Recurrent neural networks for voice activity detection IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, pp 7378–7382.

[39] Eid HFA, Darwish A, Hassanien AE, Abraham A (2010) Principal components analysis and support vector machine based intrusion detection system. International conference intelligent systems designand applications.

[40] Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay, 2021, DLSDN: Deep Learning for DDOS attack detection in Software Defined Networking, International Conference on Cloud Computing, Data Science & Engineering, 683 – 688.

[41] Auther Makuvaza, Dharm Singh Jat, Attlee M. Gamundani, 2021, Deep Neural Network (DNN) Solution for Realtime Detection of Distributed Denial of Service (DDOS) Attacks in Software Defined Networks (SDNs), SpringerNature Computer Science, Vol 2, Issue 1, pp 1 -10.

[42] Noe M. Yungaicela-Naula, Cesar Vargas-Rosakes, Jesus Arturo Perez-Diaz, 2021,SDN-Based Architecture for Transport and Application Layer DDOS Attack Detection by Using Machine and Deep Learning, IEEE Access, Vol 10, pp 1 – 18.

[43] E. Arul, A. Punidha, 2021, Supervised Deep Learning Vector Quantization to Detect MemCached DDOS Malware Attack on Cloud, Springer Nature Computer Science, Vol 2, Issue 1, pp 1 -12.

[44] Lu Wang, Ying Liu, 2020, A DDoS Attack Detection Method Based on Information Entropy and Deep Learning in SDN, IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, pp 1084-1088.

[45] Shahzeb Haider, Adnan Akhunzada, Iqra Mustafa , Tanil Bharat Patel, Amanda Fernandez, Kim-Kwang Raymond Choo , Javed Iqba , 2020, A Deep CNN Ensemble Framework for DDOS Attack Detection inSoftware Defined Networks, IEEE Access, Vol. 20, pp 53972-53983.

[46] Loftfi Mhamdi, Desmond McLernon, Fadi El-moussa, Syed Ali Raza Zaidi, Mounir Ghogho, Tuan Tang, 2020, A Deep Learning Approach Combining Autoencoder with One-class SVM for DDOS Attack Detection in SDNs.

[47] Mahmoud Said Elsayed, Nhien-An Le-Khac, Soumyabrata Dev, Anca Delia Jurcut, 2020, DDOSNet: A Deep-Learning Model for Detecting Network Attacks, IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks", pp 391 – 396.

[48] Beny Nugraha, Rathan Narasimha Murthy, 2020, Deep Learning-based Slow DDOS Attack Detection in SDN-based Networks, IEEE Conference on Network Function Virtualization and Software Defined Networks, pp 51 – 56.

[49] T. V. Phan, T. G. Nguyen, N. Dao, T. T. Huong, N. H. Thanh and T. Bauschert, "DeepGuard: Efficient Anomaly Detection in SDN With Fine-Grained Traffic Flow Monitoring," in IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1349-1362, Sept. 2020, doi: 10.1109/TNSM.2020.3004415.