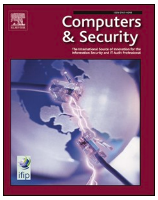
Computers & Security 139 (2024) 103652

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose



DDOS attack detection in SDN: Method of attacks, detection techniques, challenges and research gaps

Abdullahi Aishatu Wabi [*], Ismaila Idris, Olayemi Mikail Olaniyi, Joseph A. Ojeniyi

Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Niger State, Nigeria

ARTICLE INFO

Keywords:
SDN
DDOS attacks
Detection
Mitigation
Review
DDOS traffic features

ABSTRACT

The aim of a Software Defined Network is to provide flexibility and programmability towards ensuring network manageability and centralized control to deal with the growing users of future network. However, the advantages that SDN presents comes with security concerns arising from some vulnerabilities in its Architecture. Security concerns such as DDOS attack in SDN is growing in strength and sophistication trying to exploit the programmability and centralized control features of SDN Architecture. Although SDN is vulnerable to attack, SDN itself could be used to defeat attacks. This Article reviews DDOS Attack Detection and mitigation approaches and is further clustered into four as follows: Statistical based technique, techniques based on Machine Learning, Neural network and other detection approaches or Techniques. The capability and weakness of the detection techniques were pointed out. The metrics for the performance Evaluation of some of the various techniques as well as Data set repository were presented. Finally, some general research challenges and Gaps to guide future research in this area were discussed.

1. Introduction

A new network paradigm termed Software defined Networking (SDN) create an avenue for network intelligence and innovations (Xie et al., 2019). The network physically separates its control plane from the data plane there by giving room for network flexibility and the same time ensuring both Programmability and centralized control through a remote device called controller. The three planes of the SDN architecture are made up of the Control plane which defines how the network functions, the data plane which holds the networking switches or routers and the finally the Application plane which holds all Applications. This Applications encompasses all network services, business services as well as security services which interact with the infrastructure of the network (Cabaj et al., 2014).

The traditional network in comparison with the SDN requires high level skills, huge operational cost and expensive maintain (Benzekki et al., 2016).The network elements are expensive to maintain and less reliable in a situation where there are frequent network failures. The complexity in the traditional network architecture brought about some draw-backs such as non-scalability inconsistencies in policies and its dependence on vendors (Gong et al., 2015). The networking switch of the traditional network comprises both the Control and Data plane. Hence, when a new service is required, each device on the network (switch) needs to be configured or updated independently.

However, in SDN the control operations are catered for by the Controller while the Router and switches perform their functions based on instruction by the Controller. Even though SDN has gained tremendous acceptance and is a favorable solution for I.T, Cloud providers, and enterprises due to the attractive features it offers, it is faced with some challenges Shamugam et al. (2016) namely: Performance, Scalability, Interoperability, and Security.

SDN Security among other challenges has gained attention of Academia and industries (Dayal et al., 2016). IT infrastructure growth has brought about the challenges of ensuring the Integrity, confidentiality, Authentication, and Availability of information (Singh and Behal, 2020). Among the prevailing SDN security issues is the Distributed Denial of Service of Attacks (DDOS). These attacks attempt to make the resource of a system or network unusable or inaccessible and are carried out due to certain reasons such as financial gains, political gains and disruption of Service (Bawany et al., 2017). The architecture of SDN is vulnerable to DDOS attacks due to its attribute of programmability together with it logically centralized control features. This is because, the unavailability of SDN controller has the capability to break up the service of an entire network. (Benzekki et al., 2016).

[*] Corresponding author.
E-mail address: aishatuwabi@gmail.com (A.A. Wabi).

https://doi.org/10.1016/j.cose.2023.103652
Received 11 January 2023; Received in revised form 17 October 2023; Accepted 8 December 2023
Available online 14 December 2023

The usage of services and application of the internet is on the rise, whereas one the most common data centers such as Google, Microsoft, HP and others, have key into SDN. Thus, this has given rise to need to have effective and efficient means to counter against the DDOS attacks.

Hence, this research work presents a review on the various DDOS attacks together with their defense mechanisms as well as an analysis on the metric of performance Evaluation.

The purpose of the review is to have a clear-cut view how DDOS attack operates, the associated features and the distinct countermeasures that have been put in place by Researchers as well as other possible research gaps.

The major contribution of this research:

i. The DDOS attacks type and their impact on the SDN Plane is presented.
ii. A Summary of traffic features used to develop the existing detection Techniques
iii. A taxonomy showing the State-of-the-art DDOS Attacks and techniques of detection is depicted
iv. The evaluation metrics used to check the performance of DDOS attacks defense mechanism was analyzed.

This work has been organized as follows: Section 1: Introduction, Section 2: Previous related Surveys, Background of SDN, SDN security challenges Section 3: Research methodology, Section 4: DDOS attacks and SDN, Section 5 Taxonomy of DDOS attacks and detection techniques. Section 6 Analysis of metric for the performance evaluation.

2. Previous related surveys

Similar surveys carried out on DDOS attack detection and Mitigation in the domain of SDN have been presented in Table 1 and discussed in this section. In Yan et al. (2016), the characteristics and trends of DDOS attacks in cloud computing was discussed and how authors have leveraged on SDN to defend against DDOS attack. The study also looked at the various DDOS attack implementation methods in SDN layers and possible defense solutions. Some of the open research problems were highlighted; This includes issues such as how to leverage on SDN to combat application-level and mobile DDoS attacks, implement distributed layer defense, use cross-layer traffic analysis, and how to build a DDoS attacks resistant system. Dayal et al. (2016) conducted a critical review on the different security-based challenges of SDN, DDOS attacks and counter measure. The study did an analysis on the SDN layers to point out the vulnerabilities that resulted to the different security threats in SDN as well as the strategies of DDOS attack on the SDN layers. The study categorized the existing detection approaches into Statistical analysis-based detection, techniques based on Machine learning as well as Policy based Detection. The study opined that early detection of DDOS attack against the controller should be considered as important since it is comprising a single component of the SDN Architecture could easily disrupt network. The study suggested the use of Supervised learning for updating attack database such that, the DDOS attack detection schemes could identify them. Another study that surveyed the SDN-based DDOS detection and mitigation techniques is the work of Bawany et al. (2017). The study highlighted some of the requirements of an effective solution and went to further to propose a defense mechanism against DDOS attacks on a Large-scale network. A highlight of open research challenges and future directions were given. This includes: Adoption of SDN, Security of SDN Controller, and Identifying malicious traffic. Another similar survey is the work of Zubaydi et al. (2017) . The study categorized the existing work on DDoS attack detection techniques using the parameters used for the detection. This includes detection using Entropy, Time-based detection, low-traffic flow detection, Flow Ranger: Buffer Prioritizing and Algorithm, Scheduling-Based

Table 1
Previous related surveys in comparison with the proposed study.

S/N	References	Study focus	Latest reference						Taxonomy	Synthesis of performance evaluation metrics	Dataset REPOSITORY
			2016	2017	2018	2019	2020	2021			
1	(Yan et al., 2016)	Defense mechanism against DDOS in the cloud using SDN									
2	(Dayal et al., 2016)	SDN Security, DDOS attacks and countermeasure in SDN									
3	(Bawany et al., 2017)	Detection and mitigation Solutions together with research challenges									
4	(Zubaydi et al. *2017)*	DDOS Detection techniques									
5	(Kalkan et al., 2017)	Defense approaches for DDOS attacks in SDN									
6	(Xu et al., 2017)	Presented SDN-Self DDOS threat and existing DDOS detection and defense in SDN									
7	(Fajar and Purboyo, 2018)	Security challenges in SDN and approaches for mitigating DDOS attack									
8	(Joëlle and Park, 2018)	DDOS attack detection and mitigation-based method on SDN Environment									
9	(Dharmadhikari et al., 2019)	DDOS attack in SDN data and control plane, detection approaches									
10	(Dong et al., 2019)	Defense and mitigation mechanism of DDOS in SDN and cloud computing.									
11	(Singh and Behal, 2020)	DDOS Attacks in SDN context with detection and mitigation mechanism in SDN as well as the Research gaps									
12	(Ubale and Jain, 2020)	DDOS attack techniques and solutions in SDN									
13	(Silva et al., 2020)	Taxonomy of DDOS mitigation measures in IOT using SDN									
14	This study	DDOS attacks in SDN and the existing detection and mitigation techniques									

Architecture Flows. The pros and cons associated with some of the methods were pointed out. Kalkan et al., 2017 presented an analysis and categorization of the various solutions to defeat DDOS Attacks in the domain of SDN. The Authors classified the studied DDOS attack solutions into intrinsic and extrinsic solution. The Intrinsic solutions were directed towards network entities together with the functions they can perform whereas the extrinsic solution was focused on network flows together with their features. In the work of Kalkan et al. (2017), there are some studied models which suggested the integration of intelligence capabilities in Switches to maintain flows in the SDN data plane.

Xu et al. (2017) did a review on the DDOS in SDN, together with the detection and defense approaches suggested and implemented by various authors. The various detection techniques reviewed, were further classified into entropy, Machine learning and graphical based detection. The authors in (Xu et al. (2017)) opined that, detecting DDOS attack is just a first step in withstanding the DDOS attack. That, returning network to normalcy and cutting down network loss when an attack is detected, will require an effective and timely methods. The authors briefly summarized the studied defense measure based on the attack effect on the SDN architecture namely: controller resource saturation, Switch overload and communication Channel congestion. Similarly, Fajar and Purboyo (2018) presented a survey on the existing methods of DDOS attack detection in the domain of SDN. The study focused on the DDOS attacks and the attacks vectors of the SDN Architecture specifically the SDN control plane. In Joëlle and Park (2018), the authors reviewed the various DDOS detection approaches and grouped them as Machine learning Based, Statistical analysis base and Entropy based attack detection. It termed Entropy based detection method as one of the best and most used DDOS attack detection method because of it allows the estimation of randomness distribution of some features in the packet headers such as the flows in the network, Internet Protocol (IP) addresses and the number of packets. In Dong et al. (2019), the focus was not on SDN alone, the Authors also reviewed the DDOS attacks in the domain of cloud computing. Thus, the reviewed mitigation solutions for DDOS attacks were presented based on the Environment affected (that is SDN and Cloud Computing). Dharmadhikari et al. (2019), concentrated on DDOS attacks targeted towards the SDN Data and Control plane. The authors reviewed the existing approaches for countering against these attacks and further classified the detection approaches in terms of volumetric attacks, protocol exploitation attacks and machine learning Algorithm.

Singh and Behal (2020) and Ubale and Jain (2020) presented DDOS attacks in the context of SDN together with existing detection and mitigation mechanism in the domain of SDN as the well as the Research gaps/challenges. The two study Singh and Behal (2020) andUbale and Jain (2020), discussed the SDN security challenge as well as the vulnerabilities of SDN Architecture that could result in DDOS attacks. The vulnerability includes Buffer Saturation, controller saturation, congestion of control and data plane link and Flow table over flow. Ubale and Jain (2020) presented the existing defense mechanism interns of the vulnerability, however, Singh and Behal, (2020) classified the detection approaches in to Machine learning based, Artificial Neural network, Information theory metrics, and others. Silva et al. (2020) presented a Taxonomy of DDOS mitigation measures in IOT using SDN, that is the various mitigations put in place to protect the IOT by leveraging on SDN. The previous surveyed article revealed several recommendations for DDOS attack detection; However, the surveys did not consider giving details of the performance evaluation metrics used to validate their methods.

2.1. Software defined networking-SDN

Software-defined networking, or SDN, aims to make networks more adaptable and flexible. According to (Open Networking Foundation, 2012), SDN is the physical separation of the network control plane from the infrastructure plane. The control plane houses the controller that controls all network devices.

Martin Casado's Ph.D. thesis served as the basis for the concept of SDN in 2007. Martin Casado, Ph.D. candidate at Stanford University, worked with Professor Scott Schenker, a professor of computer science at the University of California, Berkeley, and Professor Nick McKeown, who served as Martin Casado's academic supervisor in the department of Electrical Engineering and Computer Science (Nisara et al., 2020). The title of the thesis was "Architectural Support for Security Management," and it was a piece of academic research. It introduced "Ethane," a flow-based Ethernet switch that could be controlled centrally from the outside (Nisara et al., 2020)

The OpenFlow protocol was developed from the Ethane model. This was followed by the development of software which was used to achieve some Control applications. These are some of the activities in the thesis, that enhanced the development of SDN (Nisara et al., 2020).

2.2. The software-defined network architecture

The Software-defined network Architecture is consisting of three Layers: The Application Layer, the Control Layer, and Infrastructure Layer. The SDN architecture is depicted in Fig. 2.

2.2.1. The application layer

The application plane is another name for this. All the Commercial applications and program software resides here. An abstract perspective on the whole network is displayed in this layer. The programmability feature that SDN presents allows the flexibility of using High-level programming language to design and install application services such as Load balancers, security monitoring, and traffic engineering (Singh and Kumar, 2016) and is possible through the Application layers . Some of the services provided at the Layer include: Adaptive routing, green network, network maintenance, network security, boundless roaming and Network Virtualization.

2.2.2. Control layer

The Control plane is another name for this. It lies in between the infrastructure layer and the Application layer. It is responsible for making decision on how packet should be forwarded by one or more devices (Prajapati et al., 2018). This layer holds the Controller, where all the implementation logic is done. SDN's central component is the Controller. It is centralized logically and may also be distributed physically. The west-bound and east-bound interfaces allow for communication between the distributed controllers. South-bound application programming interfaces (APIs), such as OpenFlow, connect this layer and the infrastructure layer (Singh and Behal 2020).

2.2.3. Infrastructure layer

The packet forwarding devices are domiciled on this layer, and act based on the instruction from the logically centralized controller. Hence this plane is referred to as the Data Plane (Singh and Behal, 2020). This plane ensures a decent network virtualization, security availability and at the same time preserve quality. This achieved by utilizing the resources that deal directly with customer traffic (Prajapati et al., 2018).

2.2.4. Northbound interface

The Application layer and the control plane can communicate with one another thanks to the REST API's Northbound interface. While safeguarding the network's internal details, this interface contributes to network programmability.

2.2.5. Southbound interface

The interfaces that make it possible to communicate with the data plane and control plane. Services like statistics reporting, event notification, programmatic control of all forwarding operations, and Capabilities advertisement are provided by the Southbound API. OpenFlow is the Southbound interface protocol that is used the most.

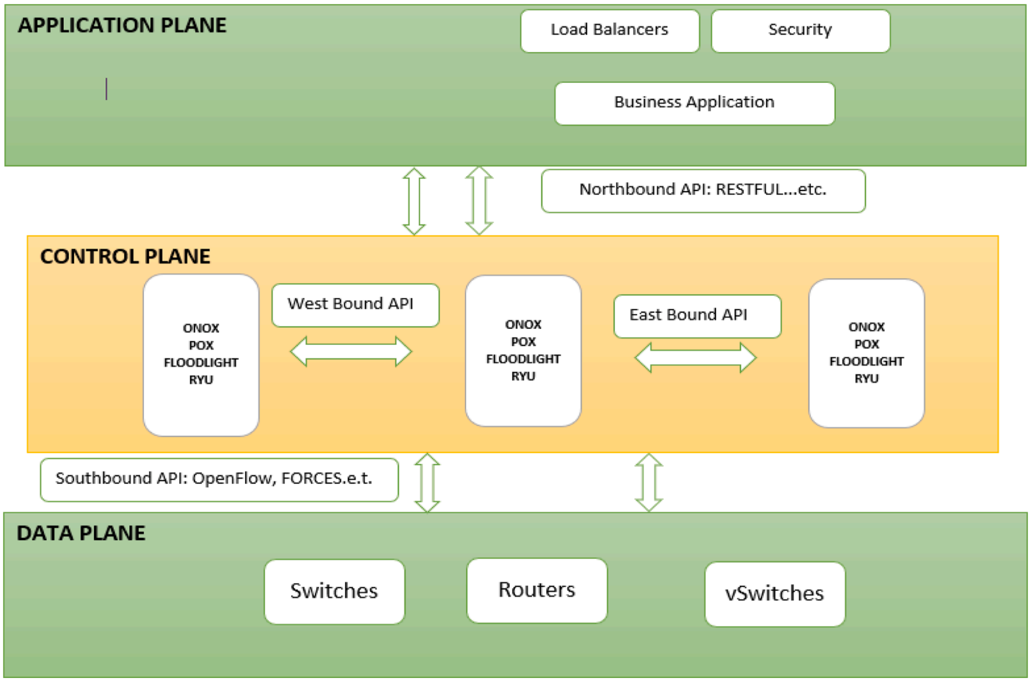


Fig. 2. The SDN Architecture.

2.2.6. *West and east bound interface*

The controller in the SDN is logically centralized. However, it can also be physically distributed. Eastbound and westbound interfaces enable these distributed controllers to communicate with one another. Because a controller failure could result in the collapse of the entire network, a single controller may not be able to manage a large network. To determine this, numerous regulators could be utilized. Thus, in the event of a controller failure, the other controllers may be instructed to assume network traffic handling (Singh and Behal, 2020).

2.3. *Security challenges of SDN*

Even though SDN has some benefit and has been accepted by many network giants, it is faced with some challenges. Among the challenges of the SDN, is the Security challenges. The SDN's centralized control makes it susceptible to DOS and DDOS attacks, which could have an impact on the entire network. SDN's other security issues include: Access control, accountability, and authentication and authorization This is particular to Application plane as expressed in Singh and Behal (2020). Threats from scalability and DOS and DDOS attacks are two security issues unique to the Control plane Whereas, that of the Data plane is faced with challenges of is confronted with difficulties of reliance on control plane, switch control connect, support for limited number of flow entries and so on.

2.4. *Distributed denial of service attacks*

2.4.1. *Distributed denial of service (DDOS) attack*

The malicious user attempts to compromise the normal operation of a network in a simple denial of service (DOS) attack; however, a DDOS attack occurs when the attack originates from a group of hosts rather than a single host (Hafizah et al., 2018). DDOS attack makes an internet-based asset inaccessible by sending overpowering number and size of phony bundles from numerous source (Fajar and Purboyo, 2018). There are a lot of people who use the internet. Because the majority of DDOS attacks originate from the external victim's network rather than the attacker's own system, a network can be attacked by DDOS regardless of its level of security Fajar and Purboyo, Due to their limited resources, bandwidth storage capacity, and processing power, the majority of network infrastructures are a natural target for DDOS attacks. Fig. 2.1 depicts the classifications of DDOS attacks.

2.4.1.1. Volumetric attack. The goal of this kind of attack is to exhaust the victim's network resources, such as bandwidth, by flooding them with a lot of traffic (Dayal et al., 2017). Bytes per second are the units used to measure the size of this kind of attack. An example of this kind of attack is: UDP and ICMP. According to Dayal et al. (2017) Volumetric DDOS attacks account for nearly 61 % of attacks. The amplification attack is another type of volumetric attack. By utilizing a different trigger machine, this kind of attack increases the volume of traffic while sending the least amount of traffic to the trigger machine. Some examples of this kind of attack are: Smurf attack, Fraggle attack, amplification of the Network Time Protocol (NTP), and amplification of the Domain Name System (DNS).

2.4.1.2. Resource depletion attack. An attacker can take advantage of the limited processing power and memory of the majority of network servers to launch distributed denial-of-service (DDoS) attacks and ultimately bring down the system server. Malformed packet attack and Protocol based exploit/TCP state exhaustion are example are example of such attack. In protocol exploit or TCP State exhaustion attack, the resource of the devices is exhausted by exploiting the network protocols for example TCP SYN Flood, Ping of death, PUSH+ACK.

2.4.1.3. Application layer attack. The goal of this kind of attack is to crash the application or the underlying server by taking advantage of the protocol at the application layer. Requests per second are used to measure the size of these attacks. HTTP and Slow Loris are two examples of these kinds of attacks.

2.5. *Current trends*

This study considered literature from 2014 to 2023 as the period of the study for the purpose of identifying studies geared towards addressing DDOS attacks that target the SDN architecture. From Fig. 2.2, it can be seen that research in this area reaches its peak in 2019 while in

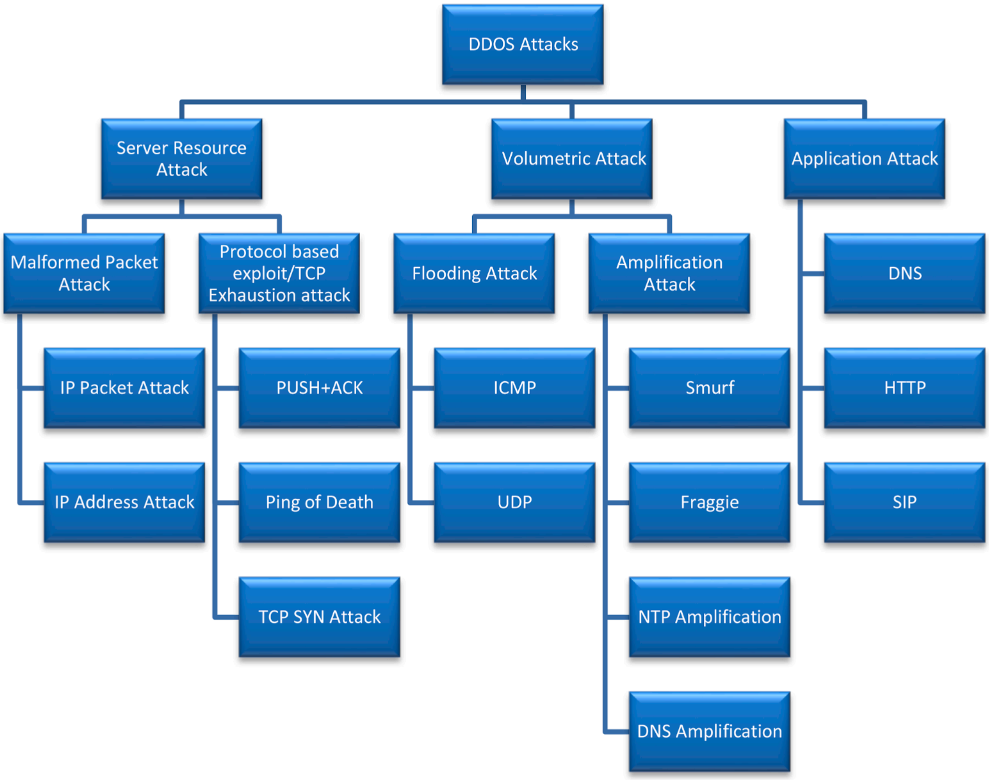


Fig. 2.1. Classes of DDOS Attacks.

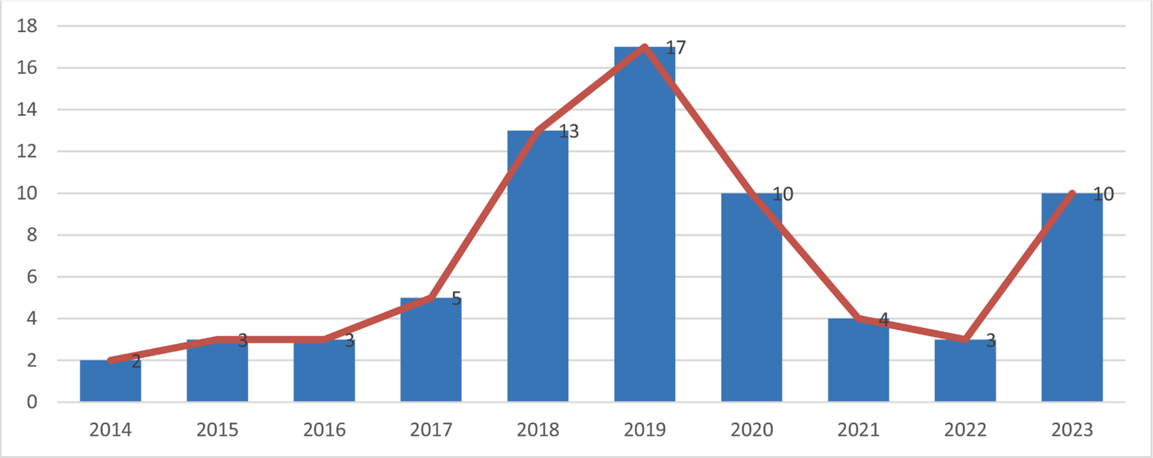


Fig. 2.2. Research trend of DDOS Attack Detection in SDN.

2022, fewer works appears to have been published. However, 2023 experienced a growth of research work probably because Authors are trying out different methods of tackling the SDN security issues since SDN has gain wide acceptance.

3. Research methodology

The research steps taken to examine the SDN literature are described in this section. Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) were used to select the existing studies and conduct the review. (Alfa et al., 2020) as shown in Fig. 3. Research question, research strategy and selection criteria were the processes used to carry out the review.

3.1. Research question

The research question used for the study is as follows:

1. In the context of SDN, identify and describe the tools used in DDOS attacks.
2. What are the existing DDOS attack detection techniques in SDN?
3. What metrics are used for performance evaluation?
4. What are the challenges of Existing DDOS Detection techniques in SDN?

The possibility of DDOS attacks in SDN is the focus of the first research question. The attack strategy and its effects on the SDN planes. The traffic features used to identify DDOS attacks, as well as the SDN DDOS attack threat model and exploited vulnerabilities. Lastly, DDOS

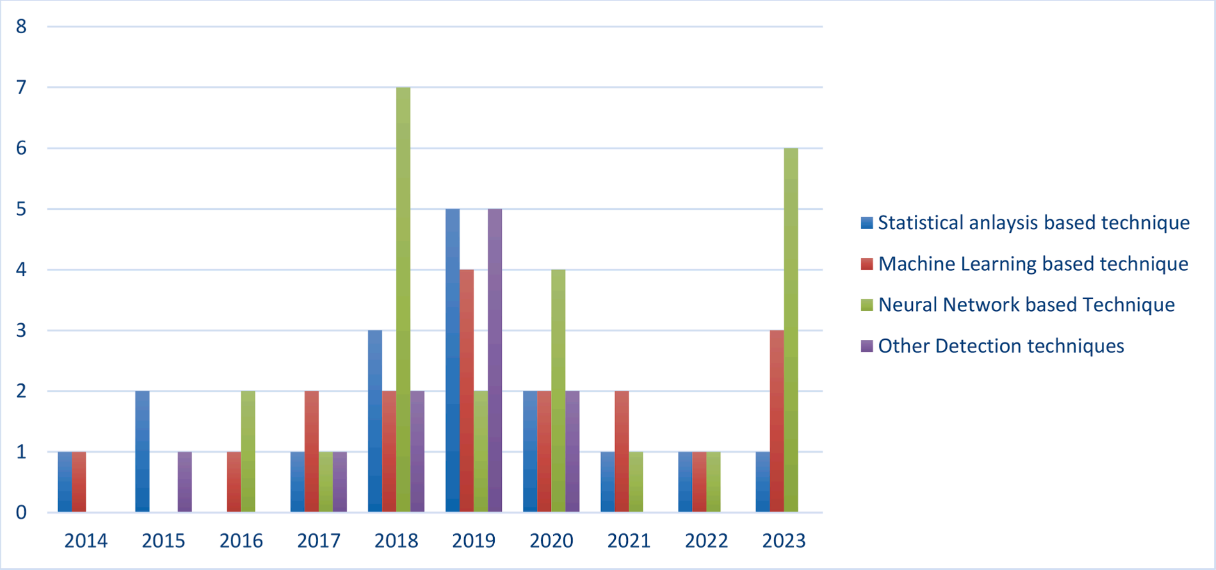


Fig. 3. The Study Work flow using PRISMA.

Table 3.1
Search database source.

Sn	Sources	URL
1	IEEE XPLORE	URL: https://ieeexplore.ieee.org/Xplore/home.jsp
2	SPRINGER	URL: http://www.springer.com.
3	SCIENCE DIRECT	URL: http://www.sciencedirect.com
4	ACM	URL: http://dl.acm.org.
5	WILEY	URL: http://onlinelibrary.com.

attacks were discussed in relation to SDN.

The second research question focused on the various methods for detecting DDOS attacks in SDN as well as methods for detecting DDOS attacks in SDN itself. The third question focuses on the metrics used to evaluate the detection technique's performance. While the fourth research question outlined some of the difficulties that DDOS detection techniques in SDN face as well as areas that require additional research in the future.

3.2. *Search and data sources*

A variety of databases as shown in Table 3.1 were searched in order to gather relevant literature on DDOS attacks in SDN. The examination articles were appropriately investigated utilizing distinguishing proof of essential investigations with other various strategies.

3.3. *Article identification*

Relevant papers were searched from various academic research libraries which include ACM Digital Library, IEEE, Science Direct, Springer, Wiley online Library, the academic database was queried using the combination of the following key terms to retrieve the relevant papers: DDOS attacks, SDN with a filtering criterion of papers from 2014 – 2023.

3.4. *Inclusion/exclusion criteria*

The exclusion criteria are defined as follows:

Sn	Inclusion	Exclusion
1	Study that focuses on DDOS attacks, Detection and mitigation mechanism in SDN	Study did not focus on DDOS attacks, Detection and mitigation mechanism in SDN
2	Study was published in English Language	Study was not published in English Language
3	Study published from 2014 to 2023	Study not published from 2014 – to 2023
4	Articles are either survey paper or Research Papers	Articles are neither survey paper or Research Papers

4. DDOS Attack and SDN

SDN's programmability and logically centralized control capabilities lead to DDOS attacks (Kreutz et al., 2013) According to Table 4.1, this study looked at 10 articles and found weaknesses in SDN that make it susceptible to DDOS attacks. These problems include inadequate memory storage for the controller, a single point of failure for the controller, inadequate storage for the switch, an idle timeout mechanism for the SDN switch, malicious or unauthorized applications, and communication channels (Control-Data Bandwidth, Control-Application Bandwidth). The three SDN Planes are affected by each of these issues. Fig. 4.1 depicts the SDN and attack point flow sequence. The figure demonstrates that SDN attack points cut across SDN planes, and the following is an explanation of the data flow sequence from 1 to 6:

1. Host A wishes to transmit some data to Host B; Switch receives the initial packet from it.
2. To determine whether the packet is a member of any flow table entry, the Switch checks its flow table. If so, the packet is processed by the switch; otherwise, the OpenFlow protocol sends it as a Packet_in to the Controller.

Table 4.1
Problems with sdn leading to ddos attack.

SN	Reference	Issues/vulnerabilities	Attack plane	Impact	Method of attack
1	(Raghunath et al., 2018), (Conti and Gangwal, 2019), (Polat and Polat, 2020), (Dayal et al., 2017), (Santos et al., 2019)	Controller limited capacity /single point of failure	Control	– Controller resource consumption /saturation – Bring down the controller making it unavailable for legitimate user	Packet in flooding attack Controller saturation attack
2	(Conti and Gangwal, 2019), (Ubale et al., 2019), (Wu 2016), (Polat and Polat, 2020)	Limited storage capacity of SDN switch	Data	Switch resource saturation, flow table overflow	Buffer saturation attack, flow table overflow attack, spoofing of switch
3	Wu 2016	Idle timeout mechanism		Keep flows in the flow table more than necessary	
4	Hafizah et al., 2018, (Santos et al., 2019), (Singh and Behal, 2020)	Unauthorized Application/ Malicious Application	Application	Trigger DDOS attacks to exhaust network resources	Application Exploit
5	(Raghunath et al., 2018), (Conti and Gangwal, 2019), (Dayal et al., 2017), (Polat and Polat, 2020) (Mladenov, 2019)	Control-data Bandwidth	Control-data plane (SBI)	Bandwidth exhaustion/ saturation controller resource	Bandwidth attack
6	Dayal et al., 2017,	Lack of standard protocol between the Northbound-Control Plane	Control-Application Plane (NBI)	Affects the controller	Bandwidth Attack

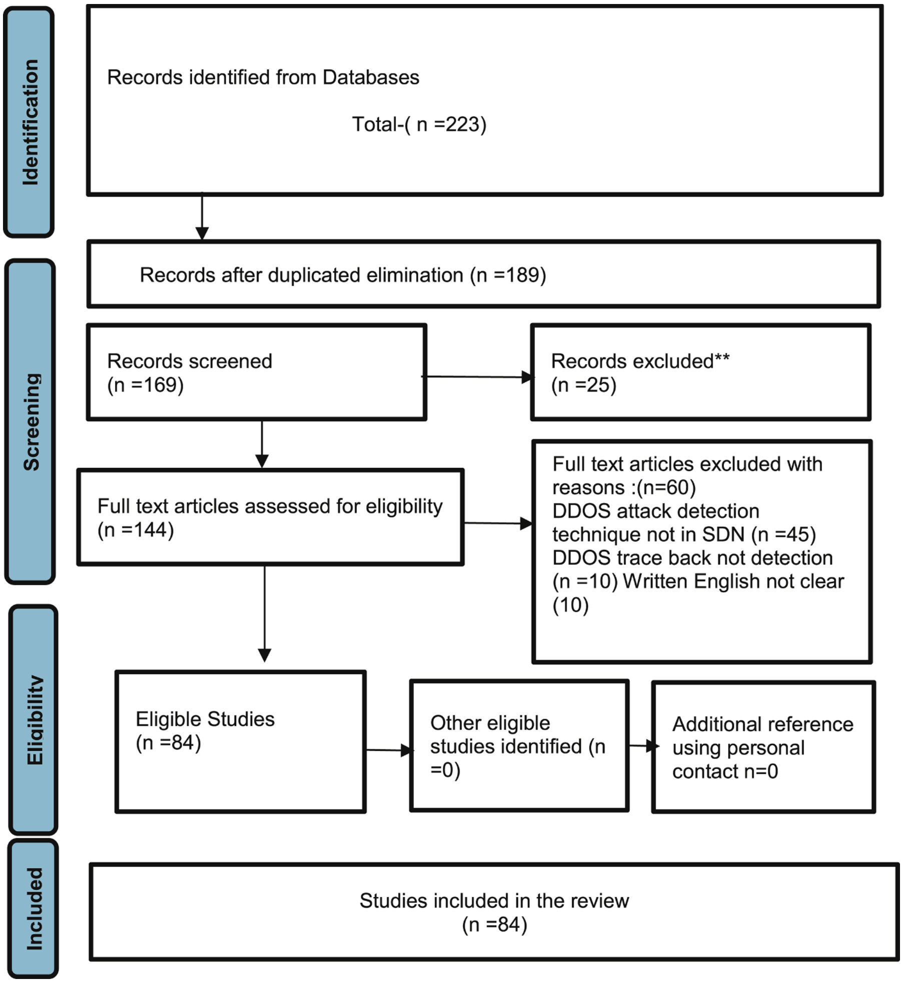

Identification
Records identified from Databases
Total-(n =223)
Screening
Records after duplicated elimination (n =189)
Records screened
(n =169)
Records excluded**
(n =25)
Full text articles assessed for eligibility
(n =144)
Full text articles excluded with reasons :(n=60)
DDOS attack detection technique not in SDN (n =45)
DDOS trace back not detection (n =10) Written English not clear (10)
Eligibility
Eligible Studies
(n =84)
Other eligible studies identified (n =0)
Additional reference using personal contact n=0
Included
Studies included in the review
(n =84)

Fig. 4.1. SDN Flow sequence and Attack point.

3. By sending a Packet_out message, the Controller tells the switch about the best path for flow to take after processing the Packet_in.
4. After that, the Switch sends the packet and updates its flow table.
5. Since the Switch already has an entry for the flow, it was not necessary to forward the packet to Controller once more when the next packet of the same flow is sent to the Switch. Instead, it will be sent directly to Host B.

4.1. *DDOS Attacks on the SDN Planes*

According to the studied literatures, SDN planes are susceptible to DDOS attacks. The vulnerabilities of SDN and DDOS attacks in the context of SDN are respectively depicted in Figs. 4.2 and 4.3

4.1.1. *DDOS attack on SDN data plane*

It has been clearly shown in Dayal et al. (2017) that DDOS attack

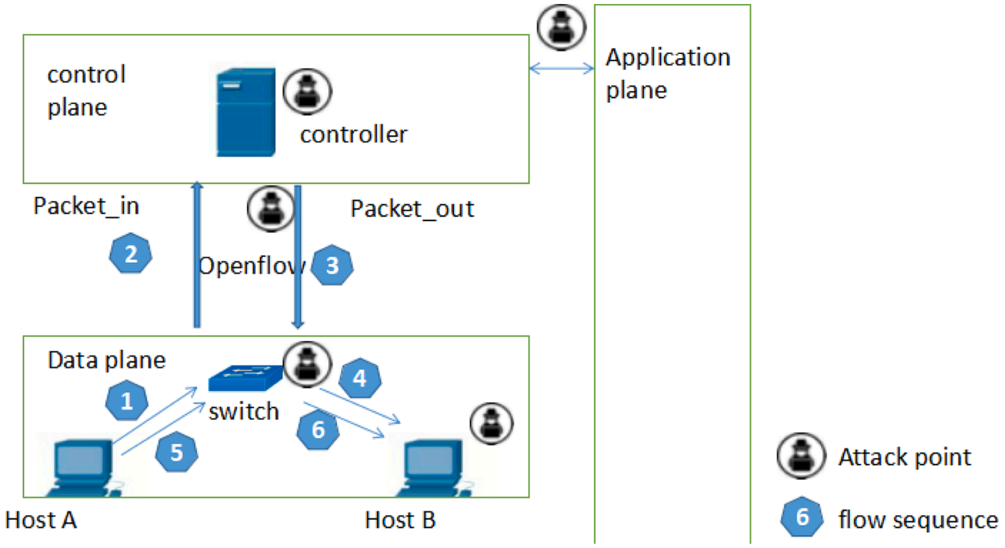


Fig. 4.2. Taxonomy of Vulnerabilities of SDN leading to DDOS Attacks.

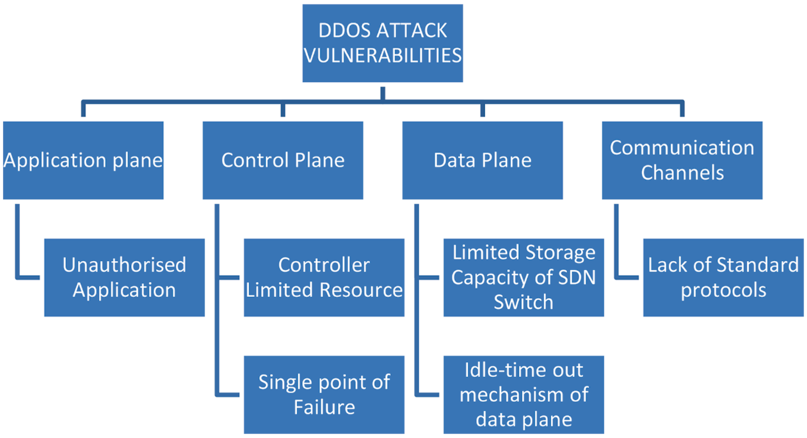

DDOS ATTACK VULNERABILITIES
Application plane
Control Plane
Data Plane
Communication Channels
Unauthorised Application
Controller Limited Resource
Single point of Failure
Limited Storage Capacity of SDN Switch
Idle-time out mechanism of data plane
Lack of Standard protocols

Fig. 4.3. Taxonomy of DDOS Attacks in the context of SDN.

affects the Data plane. Attackers leverage on Switch's limited memory storage as reported in Wu et al. (2016); Ubale et al. (2019); Polat and Polat (2020); Conti and Lal (2019) and Idle time-out in SDN Switch Wu et al. (2016). In the general operation of the SDN, when a matching flow does not exist in the flow table, the Switch sends part or all of the packet headers to the Controller. The packet is kept in the Switch's nodes while it awaits the controller's response (Hafizah et al., 2018). Hence, an attacker continues to send new unknown packets before the *idle timeout* bearing in mind the limited storage of the switch and consequently leading to Switch Buffer Saturation, Flow table overflow ultimately exhausting the data plane infrastructure resources (Wu et al., 2016; Ubale et al., 2019; Polat and Polat, 2020; Conti and Lal, 2019).

4.1.2. DDOS attack on control plane

The control plane is where SDN's centralized control features are located. The controller may be viewed by an adversary as a single point of failure (Santos et al., 2019) to launch distributed denial of service (DDoS) attacks by sending a variety of packet in messages to overload the controller, thereby saturating the controller's resources and rendering them unavailable to legitimate users or even shutting down the entire network Raghunath et al. (2018); Conti and Lal (2019); Polat and Polat (2020); Dayal et al. (2017); Santos et al. (2019).

4.1.3. DDOS attack in application plane

Different applications provide different services to the controller. Some applications could hide under another to access the network resources (Hafizah et al., 2018) hence, malicious application is able to gain access to the network resource at the instance of another application to exhaust network resource or bring down network (Singh and Behal, 2020; Santos et al., 2019; Hafizah et al., 2018). This exploit is also owing to lack of Standard authorization and authentication mechanism for checking the validity of the Applications (Hafizah et al., 2018).

4.1.4. DDOS attack on control-data plane

A channel or bandwidth known as the South Bound Interface (SBI) is the means by which the data plane and controller communicate with one another (Conti and Gangwal, 2019. Mladenov, 2019) demonstrated the possibility of a DDOS attack on the Data-Control-Communication channel. The Controller and the entire network can be brought down as a result of bandwidth saturation caused by an attacker sending increasing traffic between the two planes (Raghunath et al., 2018; Conti and Gangwal, 2019; Dayal et al., 2017; Polat and Polat, 2020).

4.1.5. DDOS attack on control – application plane

It was mentioned in Hafizah et al. (2018) that because there is no standard protocol for the North-bound API to enable communication between the two planes, the Northbound API, which is the

Table 4.2
DDOS traffic features.

SN	Reference	Collected features	How it was extracted /used	Target plane	Summary
1	Fouladi et al. (2020)	Unique source IP address, normalized unique destination IP address	Time series value of USIP and NUDIP is estimated	Control	Flow entries with unique source IP increases during DDOS whereas NUDIP is obtained by calculate UDIP with respect to number of packets in the flow table.
2	Gurusamy and Msk, (2019)	Transmitted packets – Received Packets – Transmitted bytes – Received bytes – Errored packets	Bandwidth usage was calculated using the collected features.	Control	The collected traffic flows were used to calculate the bandwidth usage of a host and compared to a threshold.
3	Cui et al., 2019	Source IP address Destination IP address	Entropy of source IP Entropy of destination IP	Control	The entropy of the source IP address and destination IP address was used for detection module
4	Lawal and At, 2018	Source IP Destination IP No. of packets/sec	Source IP Destination IP No. of packets/sec	Control Data	
5	Giotis et al., 2014	Source IP, Destination IP, Source port Destination port	Entropy of source IP, Destination IP, Source port, and destination port	Application Data	The entropy of the source IP address and Destination IP address source port and destination port were used for detection module
6	Sahoo et al., *2018*	– Payload – Packet type – Topology type – Destination port – Source port – Total Packet sent – Window size	-The entropy of the flow is ascertained	Control	Collected statistics and calculated the entropy of the flow.
7	Santos et al., 2019	Number of bytes in flow, opaque controller-issued identifier, ethernet destination port, Ethernet source address, ethernet frame type, ethernet VLAN ID, Ethernet VLAN priority, time flow has been alive in nanoseconds, Time flow has been alive in seconds, Max time before discarding, Idle time before discarding, Port ID, max length to send to controller, IP destination, address, IP protocol, IP source port, Type of service, number of packets in flows, priority level of flow entry, output port, ID of the	IP source port Time flow has been alive in nanoseconds Port ID Ethernet source address Time flow has been alive in seconds No of bytes in flow No. of packet in flow TCP destination port TCP source port IP protocol Ethernet destination port	Control, data, communication channels	Collected 23 features set IP Source port and duration time was considered as the most important features for detection. Attack on controller has lower detection accuracy because the classifier training database was equally distributed. Hence features that could aid detection of controller attack better accuracy was not adequate.
8	Ye et al., 2018	duration, table *NXSTFLOWreply* (*??id cookie, dl src n_bytes* idle timeout idle age, dl dst priority arp, in port, vlan tci =n_packets	– Speed of IP per unit time – Speed of source port per unit time – Standard deviation of low packets – Standard deviation of no. of flow bit – The speed of flow entries per unit time – The Ratio of Pair-Flow (RPF)	Control plane	Collected flow table information and transform them into 6tuple feature vector used for the DDOS detection in SDN
9	Oo et al., 2019	Flow packets Flow bytes duration	– Average number of flow packets – Average number of flow bytes – Variation of flow – Packets variation of flow bytes – Average duration	Control	Traffic data is collected and transformed into 5 tuples features used for classification
10	Hu et al., 2017	Source IP Destination IP Source port, Destination port Protocol	Entropy of source IP, Destination IP, Source port, Destination port and protocol	Control	Collected flow table information and transform them into 6tuple feature vector used for the DDOS detection in SDN
11	Assis et al 2020	– Bits/sec – Packet/sec – Source port – Destination port – Source IP – Destination IP	– Bits/sec – Packet/sec – Source port – Destination port – Source IP – Destination IP		

(*continued on next page*)

Table 4.2 (*continued*)

SN	Reference	Collected features	How it was extracted /used	Target plane	Summary
12	Cui et al., 2016	– number of packets matched by each flow entry, – number of bytes matched by each flow entry, – survival time of each flow entry, – packet rate of each flow entry and byte rate of each flow entry	– number of packets matched by each flow entry, – number of bytes matched by each flow entry, – survival time of each flow entry, – packet rate of each flow entry and byte rate of each flow entry		The collected traffic features are used for the classification
13	(Phan et al., 2016)	Packet number Duration	The Number of packets transmitted via the flow -How long the flow existed in the flow table	Control Data	The Number of packets transmitted via the flow and how long the flow existed in the flow table are the two features used for classification.
14	Kokila et al. (2019)	Source IP address, destination IP address, Source port, destination port, Protocol used for communication and the length of the packet.	Traffic data converted into binary (0 and 1)	Controller	Collected traffic attribute and converted into binary to be used as input for SVM classifier
15	Phan and Park (2019)		Flow number of source -Active of source -Average number of packets per flow		
16	Wang et al. (2015)	Destination IP	Entropy of Destination IP	Data plane	The IP destination was used as an attribute to aggregate the input flows and Entropy of the address was determined.
17	Mousavi and St-Hilaire, (2018)	Destination address	Destination address entropy value for each window	Control	The destination address was collected and was used to calculate the destination address entropy value for each window
18	Niyaz et al. (2017)	68 features	Number of bytes per flow Number of packets per flow Entropy of the features	Control	68 features collected from TCP, UDP Traffic and Number of bytes per flow was computed for few sets while number of packets per flow for another set and entropy of another remaining set was computed before usage.

communication channel between the Control and Application, could be used for DDOS attacks (Dayal et al., 2017).

4.2. Leveraging SDN to defeat DDOS

The conventional network is experiencing an increase in the size, frequency, and severity of DDOS attacks. This portrays that, the ongoing safeguard system can't handle this danger (Singh and Behal, 2020). However, DDOS attacks can be stopped with the help of the SDN's features such as traffic analysis, a global view of the network, programmability features, and dynamic policy update.

4.3. Traffic features used to identify DDOS attacks

The Open flow switch consisting flow table and other group table list information. A flow table entry is made up of some components such as priority, cookies, timeout (Hard or soft timeout) Packets headers field etc. Information about a packet, such as its source, destination, protocol, and port, can be found in the packet header field (Kokila et al., 2014). Hence, most detection techniques collect traffic statistics to form their features set. Table 4.2 depicts some of the traffic features adopted in the existing detection techniques and how it was used. This is because; some features are more important and critical to detection of DDOS attack. As the duration of an attack is short and the corresponding time is limited (Cui et al., 2019), features like time duration and threshold size are effective in attack detection (Banitalebi and Mohammadreza 2020).

5. Aproposed taxonomy of DDOS attack detection techniques

A proposed Taxonomy of DDOS attack detection based on the techniques proposed in literatures is presented in Fig. 5

Different studies on the SDN DDOS detection and mitigation techniques are presented from the taxonomy, which has been divided into five categories: Statistical model/entropy-based technique, machine learning-based technique, artificial neural network-based technique, and other detection techniques. Tables 5.1–5.4 present the summary, respectively.

5.1. Statistical analysis based detection techniques and entropy

Techniques of detection based on statistical analysis and entropy have been used to detect DDOS attacks, as shown in Table 5.1 and Fig. 5.1. Software-defined networks support programmability, making it possible to extract and analyze network flow statistics. In this light, the study of (Aladaileh et al., 2023) tries to ascertain the effectiveness of Entropy in detecting high and low rate DDOS attacks in SDN. The authors estimated entropy using the probability calculation of the source IP address, and the presence of randomness in the behavior of packet, the approach was implemented via simulation with a high DR and low FPR. Another similar study by Aladaileh et al. (2022) Proposed a Low-rate attack detection method based on entropy with adaptive dynamic thresholding to reduce FPR and DR. The approach was tested in a simulated environment and the results shows a higher DR compared to other works. Considering the effectiveness of entropy the (Yu et al., 2021) combined Entropy and Ensemble learning. Entropy for attack detection where a module was conveyed at the Switch to gather traffic data and attack discovery modules is deployed on the SDN Controller to classify abnormal from benign traffic using Ensemble learning algorithm. The classification was done with five tuple features, and the method was tested by simulating it on Mininet. Similarly, based on statistics and time series analysis, a DDOS attack detection and defense mechanism was proposed by Fouladi et al. (2020). The study used the open flow switch flow table's unique source IP address and normalized unique destination IP address to identify immediate changes in the behavior of the network. Four modules integrated into the SDN controller monitor individual switches to look for anomalies in the proposed scheme. The first module is the Feature extraction module, which uses the Open flow Switch flow table to extract traffic statistics like unique source IP (USIP) and normalized unique destination IP (NUDIP). The USIP anomaly detection module is the second module. This uses the USIP feature to give the sample an anomaly score, and the third module Anomaly Detection uses the NUDIP feature to give NUDIP another anomaly score. The actual Detection Module is the fourth module. It uses the anomaly score to determine whether or not traffic is anomalous. When any abnormal condition occurs in this module, a countermeasure mechanism is activated and an anomaly alarm is raised. Simulation and complexity analysis were used to evaluate the proposed scheme's performance. The scheme's detection performance was also evaluated using standard performance metrics like the True positive rate, False positive rate, F1 score, Accuracy, ROC, and AUC. Wu et al. (2020) suggested using DDOS detection scheme-based entropy to quickly distinguish attack traffic from normal traffic. In order to determine whether an attack is DDOS or legitimate, the detection strategy pulls IP addresses from the flow table and uses a time window to calculate entropy which is compared to an estimated threshold value. The experiment is conducted on Mininet using floodlight controller. Omar et al. (2019) and Cui, et al. (2019) also proposed DDOS detection techniques based on Entropy which used network traffic statistics for detection. Omar et al leveraged on the flexibility of OpenFlow to examine network packets. When a new packet arrives, the destination IP is examined to see if it exists in the window, if it doesn't, the count for the IP will be increased and then calculate the entropy when the windows size is full. The packet is classified as an attack when the entropy is greater that the set threshold for five consecutive counts. After that, the packet is sent to the mitigation module, which changes the flow table so that the traffic goes to a port that doesn't exist. The performance was evaluated via simulation using the POX controller. Cui et al. (2019) also used SDN's statistics collection capabilities to collect flow tables characteristic of the SDN Switch in order to detect DDOS attacks on the Control plane based on dual entropy cognitive inspired computing. The Statistic collection module of the DDOS attack defense mechanism periodically collects statistics about the Switch's current flow entries, calculates the degree of occurrence of the Source and Destination IP addresses, and then creates two hash lists to store the addresses separately. The detection module uses the characteristics of DDOS traffic to determine the appropriate DDOS attack mode, while the feature computing module calculates the entropy of the Source and destination addresses. The DDOS attack detection model is obtained when either the Source address's entropy is higher or the Destination IP address's entropy is lower than the threshold. Last but not least, the defense and recovery module took defensive measures to safeguard the victim's host by discarding packets sent to the victim's host address. Based on some recovery measures, normal communication was restored. Floodlight served as the controller for the simulation, which evaluated the effectiveness and performance of the defense model on Mininet.

Using Estimated weighted moving filters (EWMA), a new adaptive mechanism called SEAL (Secure and agile) was proposed by Bawany and Shamsi (2019)) to defend against DDOS attacks. The application-specific DDOS attack security solution was provided by the detection framework. The framework is made up of three modules, each of which uses SDN to protect network infrastructure and Smart City applications from DDOS attacks. The following three filters were used: Filtering is active, proactive, and passive. The first module, D-Defense, protects the Data Plane from DDOS attacks, while C-Defense and A-Defense protect the Control and Application Planes from DDOS attacks. EWMA filter, which monitors network traffic and generates attack alerts based on applications' security requirements, was used to achieve adaptability. The model was evaluated through simulation using Mininet and ONOX controller. The metrics used to evaluate performance were false

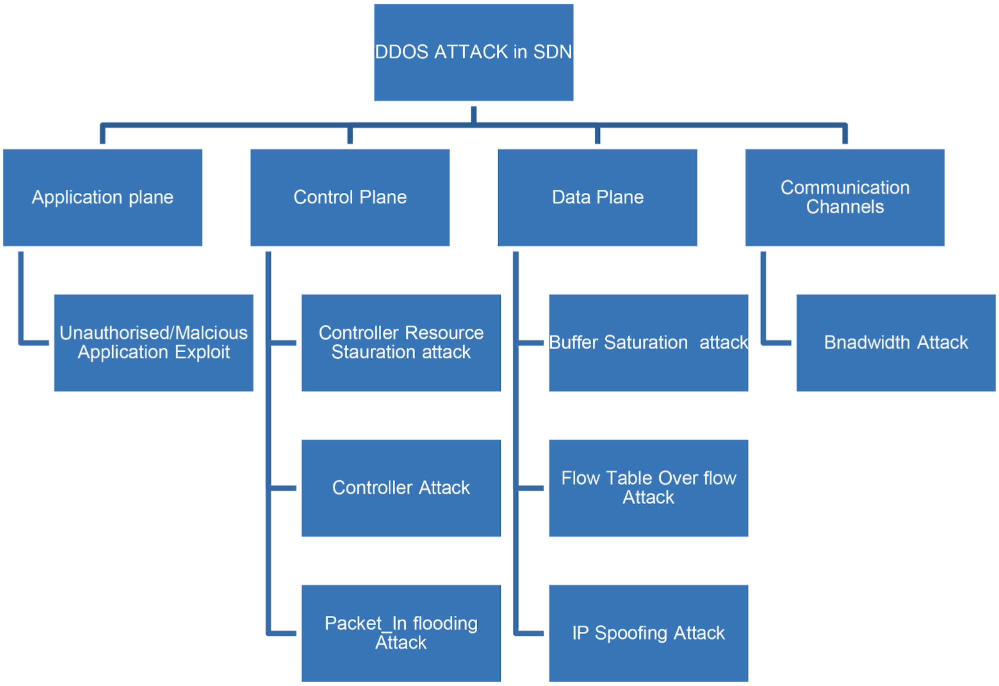


Fig. 5. Taxonomy of DDOS Attack Detection techniques.

Table 5.1
Statistical model based and entropy detection.

Sn	Reference	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
1	(Aladaileh et al., 2023)	examines the viability and effects of a DDoS attack detection method based on entropy for identifying high- and low-rate DDoS assaults on the controller	Detection	SDN	Entropy	Control	Src IP Number of packets	POX
2	(Aladaileh et al., 2022)	Proposed a Low-rate attack detection method based on entropy with adaptive dynamic thresholding to reduce FPR and DR	Detection	SDN	Entropy	Control	Timeslot, Attack traffic ratio	POX
3	(Yu et al., 2021)	- DDOS attack algorithm that combines entropy and ensemble learning. The controller is where the entropy-based detection module is located, and the ensemble learning algorithm is utilized for classification.	Detection	SDN	Entropy	Control Data	Average number of packets The average number of bits The growth rate of port The growth rate of flow The growth rate of source IP	RYU
4	Li and Wu (2020)	Detection scheme based on entropy to detect DDOS attack at an early stage	Detection	SDN	Entropy	Data	Destination IP	Floodlight controller
5	Fouladi et al. (2020)	– Seeks to address the problem of defining optimal thresholds to distinguish normal from attack traffic using statistical-based detection, – extract essential features from OpenFlow switches' flow tables to examine their timing series representation – Each switch is independently monitored by the controller, which employs the suggested method to find anomalies. Any aberrant circumstance results in the raising of an anomaly alarm and the activation of a countermeasure procedure.	Detection and Mitigation	SDN	Time series analysis using ARIMA, Chaotic theorem, and Exponential filter	Control Data plane	Unique Source IP address, Normalized Unique destination IP address	POX Controller
6	Omar et al. (2019)	– Analysis effect of DDOS on SDN – Leverage the flexibility of OpenFlow to examine packets and classify them based some threshold	Detection, Mitigation	SDN	Shannon entropy	Controller	Source IP, Destination IP, Source port, Destination port, protocol type	POX
7	Cui et al. (2019)	– After a DDoS detection, the defense and recovery strategies were put in place. – Statistic gathering, feature computation, detection, and defense/recovery modules make up the defense mechanism. – Incorporating the Support Vector Machine classification approach, a DDoS attack model is created by extracting the Switch's flow table features. – Defensive mechanisms are put in place to safeguard the victim's host and provide a mechanism for quick recovery.	Detection and Mitigation	SDN	Entropy	Control Data	Source IP DestinationIP address	Floodlight
8	Bawany and Shamsi, (2019)	– Provided an adaptive mechanism against DDOS attacks in Smart city – The three modules that make up the DDOS protection, D-Defense, C-Defense, and A-Defense, successively protect the Data plane, the Control plane, and the Application plane from volumetric attacks. EWMA filter, which monitors network traffic and generates attack alerts based on the security requirements of Applications, enables adaptation.- Installed mitigation strategy	Detection and Mitigation	Smart City	Entropy	Data and control Applicaation	Destination IP	ONOS
9	Bensalah et al. (2019)	Proposed an attack detection based on a statistical model process for detection of Bandwidth and flooding attack.	Detection	SDN	Hortelling statistics	Controller	- Rate of change of throughput - Packet loss	Open daylight

(continued on next page)

Table 5.1 (*continued*)

Sn	Reference	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
10	Gurusamy and Msk. (2019)	– Flow management model to identify and mitigate DDOS attacks – Control Saturation attacks and Volumetric attacks – Monitors all incoming ports of the controller – Mitigations are done separately for ingress and egress	Detection/ mitigation	SDN	Sflow management model	Control	– Transmitted Packets – Received Packets – Transmitted bytes – Received bytes – Errored packets	RYU Controller
11	Lawal and AT (2018)	– Sflow-based attack detection for Switch overflow and controller saturation attacks – Analysis Sflow agents for collecting packets transiting the network, Flow collector, a server for gathering and storing datagrams from the Sflow agent, and Sflow analyzer for identifying network irregularities make up the system that takes packet samples from network traffic and generates handling rules to be sent to the controller.	Detection and mitigation	SDN	Sflow	Control and data	– No of packets per second – Source host – Destination host	Floodlight
12	Kalkan et al. (2018)	When congestion is detected, the switch gives the controller simply the packet information, which he uses to determine the joint entropy of the pair profiles. DDoS attacks are recognized by the controller if the difference between the entropy values is greater than the threshold.	Detection Mitigation	SDN	Joint Entropy	Control	Destination IP Source IP	RYU
13	Sahoo et al. (2018)	DDOS attacks are targeted for early detection utilizing general entropy, Two modules are included in the plan, one of which collects statistics on incoming flows that are not matched. -The second is used to detect anomalies.	Detection	SDN	Entropy	Control Data	– Payload – Packet type – Topology type – Destination port – Source port – Total packet sent – Window size	POX controller
14	Sahoo (2017)	proposed an entropy-based detection technique to identify attack traffic in DDOS attacks against the SDN Controller using incoming packets to the controller	Detection	SDN	Entropy	Control	Destination IP	POX Controller
15	Wang et al., 2015	-Entropy was used to detect network anomalies in the proposed detection system, which is being implemented on OpenFlow switches to reduce flow collection overhead on the controller. For anomaly detection, the system examines the destination IP address's entropy variation.	Detection	SDN	Shannon Entropy	Data	Destination IP	Floodlight
16	Mousavi and St-Hilaire, 2015)	For anomaly detection, the system examines the destination IP address's entropy variation. – Entropy of the window will be determined after 50 packets. The method is adaptable since its settings can be changed to meet the Controller's needs.	Detection	SDN	Shannon Entropy	Control	Destination IP	POX
17	Giotis et al. (2014)	-A separate data gathering module is implemented. Entropy is used in data analysis to find anomalies in the data via the anomaly detection module, which analyzes collected data periodically. -Flow rules were implemented by the mitigation module to block any harmful flow.	Detection and mitigation	SDN	Shannon Entropy	Data Control	Source IP Destination IP Source port Destination port	NOX

positives, accuracy, and CPU utilization. Bensalah et al. (2019) proposed an attack detection system based on a statistical model called the Statistical Model process for detecting flooding attacks and bandwidth attacks in SDN. The hortelling Chart (T2) metric serves as the foundation for the detection strategy. First, a mathematical formula is used to determine the control limit; then, the control chart is used to supervise the growing chart. The network is under control when all of the points on the charts are within the upper and lower limits. However, a DDOS attack occurred when the Hortelling statistics exceeded the upper limit. Mininet and Open daylight controller simulations were used to evaluate the model.

Gurusamy et al., (2019) proposed a flow management model for

Table 5.2
Machine learning DDOS techniques.

Sn	Ref	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
1	(Alubaidan et al., 2023)	- Applied feature selection on different ML Algorithm to improve detection performance	Detection	SDN/ Cloud	LR, SVM, KNN, RF, LSTM	Control	dt, switch, src Pktcount, bytecount Flows, packetins Protocol, tx_kbps rx_kbps, tot_kbps	-
2	(Ali et al., 2023)	- Carried out a comparative study of ML and DL for DDOS Attack detection in SDN	Detection	SDN	SVM, KNN, DT, MLP, CNN	Control	50 Feature	-
3	(Bhayo et al., 2023)	- Proposed a ML based detection approach to protect the SDN control in the IOT	Detection	SDN/ IOT	NB, DT, SVM	Control	Number of IoT nodes, Simulation time, Packet frequency, Number of attack nodes	-
4	(S. Wang et al., 2022)	- Detect flooding-based attack via fluctuation of flows using various Supervised learning algorithm	Detection	SDN	SVM, GLM NB, DA, FNN, DT KNN, BT	Control	The fluctuation of number of *Packet_In* messages within a period	Ryu
5	(Sangodoyin et al., 2021)	- Applied different ML technique for DDOS attack detection	Detection	SDN	QDA, GNB, kNN, CART	Control	Throughput, Jitter, Response time	-
6	(Ahuja et al., 2021)	- Generated SDN Dataset using a set of features. - Proposed RF-SVC model	Detection	SDN	RF-SVC	Control Data	16 Features	Ryu
7	Sahoo et al (2020)	- employed an SVM model with a genetic algorithm to improve the SVM's parameters and KPCA to reduce the dimension of the feature vectors.	Detection Mitigation	SDN	SVM	Control	27 features and 41 features from two datasets	POX
8	Zhijun et al. (2020)	- Extract features from flow riles and used it to detect DDOS attack using factorization machine - Allows dynamic deletion of flow rules	Detection/ mitigation	SDN	Factorization machine	Data	Duration time Packets number Relative dispersion of match Bytes	RYU
9	Santos et al. (2019)	- Focus on bandwidth attack, controller-attack and Flow table attack - Compare 5 Machine learning techniques (MLP, SVM, DT RF) Decision tree performed better	Detection	SDN	MLP, SVM, DT RF	Control Data	11 flow table features	POX controller
10	Phan and Park (2019)	- To protect the network, the authors combine the SVM, eHIPF, and SOM classifiers. - The module that collects and extracts features from raw data sends the information to the classifier module. - The data is classified as anomalous or normal by an ensembled classifier. - The traffic is filtered using the eHIPF filtering approach for mitigation.	Detection Mitigation	SDN	HIPF, SVM, SOM	Control	– Flow Number of source – Active of source – Average number of packets per flow	NFV
11	Ye et al. (2018)	– Classification base on SVM – Collect switch flow table information to extract 6 tuple features – Establish detection mode	Detection	SDN	SVM	Control	-Speed of IP per unit time -Speed of Source port per unit time -Standard deviation of low packets -Standard deviation of no. of flow bit The speed of flow entries per unit time	Floodlight
12	Kaur and Gupta (2019)	– Hybrid machine learning based on SVM and KNN	Detection	SDN	SVM, KNN	Control	-Time Duration Packet flow	MATLAB
13	)Oo et al. (2019)	– Traffic data is gathered and sent to the classifier module by the traffic generation and extraction module. – The advanced SVM is employed by the classification module to differentiate the traffic as legitimate or attack traffic.	Detection	SDN	ASVM	Control	Average number of flow packets Average number of flow bytes Variation of flow Packets Variation of flow bytes Average duration	Open daylight
14	Meti et al. (2017)	– Early detection of DDOS at controller – Classify incoming request using ML – Goal is to secure SDN	Detection	SDN	SVM, NN	control	Host time No. of request	Ryu controller
15	Hu et al. (2017)	– Entropy and an SVM classifier are used in this method to identify flooding attacks and mitigate them. – Network changes can be identified using entropy. The DDoS Detection Module carries out three functions: information gathering, feature extraction, and attack detection: White-list and dynamic forwarding rule	Detection Mitigation	SDN	SVM Shannon Entropy (Feature Selection)	Control	Source IP Destination IP Source Port, Destination Port Protocol	POX Controller

(*continued on next page*)

Table 5.2 (*continued*)

Sn	Ref	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
		updating serve as the foundation for this attack mitigation mechanism.						
16	Liu et al. (2017)	- Resolved IP spoofing issue through Dynamic IP address - Used SVM to accurately detect DDOS attacks and prevent them by instructing flow tables to block attacks at the source port	Detection Mitigation	SDN	SVM	Control	Source IP address	Floodlight
17	Phan et al (2016)	- Protection scheme flood attacks based on the SVM classifier - Used Idle-timeout adjustment (IA) for mitigation measures	Detection and mitigation	SDN	SVM	Control	Packet number Duration	Pox Controller
18	Kokila et al (2014)	- Early detection of DDOS attack at the controller - Used support vector Machine classifier	Detection	SDN	SVM	Control	Source IP address, Destination IP address, source port, destination port, protocol used for communication and the length of the packet	

identifying a Multi-controller UDP flooding attack. The research aims to identify controller saturation attacks and, ultimately, safeguard the network from volumetric attacks in the SDN context. In order to detect and mitigate UDP flooding attacks, the proposed model is implemented on the control plane and monitors the traffic statistics of all incoming ports of the two controllers. The policies at the ingress port are used to block traffic if the incoming traffic exceeds a threshold that has been established.

Based on Sflow technology, Lawal and AT (2018) proposed a real-time detection and mitigation of DDOS attacks in SDN. This study took into account the Switch over flow and the controller saturation attack. A sample of packets from network traffic is analyzed by the study, and some handling rules are created and sent to the controller. There are three modules in the Sflow architecture. Flow collector is the server that collects and stores datagrams from the Sflow agent and Sflow analyzer used to detect network irregularities. Sflow agents collect packets transiting the network by sampling the interface counters within a particular period as well as sampling of switched packets statistically them to the flow collector. Mininet simulation was used to test the method. With a response detection time of less than 5 seconds and a control time of less than 10 s, the result demonstrates its real-time capability, making it a likely solution for mitigating SDN network resources DDoS attack threat. Kalkan et al.(2018) proposed a joint entropy-based security system. There are three stages to the proposed method: the nominal, preparatory, and active mitigation stages. The attack-free first phase creates nominal pair profiles for each attribute pair to generate baseline information. During this phase, the Controller receives all traffic. The Switch only sends information about the packets to the Controller during the preparatory stage. The Controller then calculates joint entropies of pair profiles, and if the difference between entropies is greater than that threshold, a DDoS attack is detected. The Controller notifies the switch whenever it detects an attack. The Attack Mitigation module then begins to drop attack packets while protecting legitimate ones.

Sahoo et al. (2018) proposed using general entropy (GE) for early detection of low rate DDOS attacks at the SDN's Control layer that took advantage of the flow-based feature of SDN. The two modules of the detection scheme are anomaly detection and statistics collection for generating a hash table from unmatched incoming flows. When another packet shows up, the Controller checks if the Destination IP exist on the Hash table, if it does, it updates the hash table entry else it adds the IP to the Hash Table and the GE classifies the network based on the set window size and threshold. A mitigation module was deployed at the controller to block specific flow rules and identify the source IP. Mininet with a POX controller was used in simulating the model to verify its accuracy.

Wang et al. (2015) suggested using OpenFlow switches to implement a method that reduces Controller flow collection overhead. Entropy is utilized to identify network anomalies, and their proposed method was based on flow statistics. The Mininet network emulator and floodlight controller were used to verify the method. Mousavi et al. (2015); Sahoo (2017) presented a real and lightweight technique for attack recognition in SDN. Anomalies are detected by their system by utilizing the destination IP address's entropy variation. In Mousavi et al. (2015), In order to detect an attack on the controller, the system tracks the number of packets coming from the same IP and the destination IP of the incoming packet. It will detect the anomaly in the network if packets arrive from the same destination and reduce entropy. For the experimental setup, a Mininet network emulator and the Scapy tool were utilized. Whereas, Generalized entropy was used in Sahoo (2017) to distinguish normal traffic from low-rate DDOS attack traffic. POX controller was used to simulate the method on Mininet. Giotis et al. (2014) proposed a three-module DDOS detection and mitigation strategy. The collector module is first implemented for collecting flow statistics and forwarded to the second module for anomaly detection which identify anomalies using entropy after analyzing the traffic data within a specific interval. The third module is the mitigation modules implement flow rules to hinder any pernicious flows in the network.

5.2. Machine learning-based technique

Machine learning techniques that have been utilized in SDN are shown in Fig. 5.2 and Table 5.2, respectively. Authors in (Alubaidan et al., 2023) utilized LR, SVM, KNN, RF, and LSTM models for DDOS attack detection using 11 feature set from an SDN dataset. The authors applied feature selection methods to improve Accuracy of the various Algorithm and compared their results which shows Random Forest with the highest Accuracy. Nonetheless, the approach was not tested online, hence may not be applicable for real time detection. Similar study was conducted in (Ali et al., 2023), the authors compared the performance of SVM, KNN, DT, MLP, CNN for DDOS Attack detection using two different traditional datasets. SVM was found to perform better than others. However, the approach may not provide a good generalization because the dataset was not created for SDN network and the detection was not done in real time. Protecting the SDN- based IOT Controller was the focus of Bhayo et al. (2023). The authors developed a module based on Machine learning detect DDOS Attacks on the Controller. Different traffic simulation scenarios were conducted and the result was promising. Wang et al. (2022) conducted a study using supervised learning algorithms to address DDOS attacks based on flow fluctuation. They collected Packet_in requests from an emulated SDN network and analyzed flow fluctuations. The performance of eight supervised learning models in detecting DDOS attacks was compared, and the results showed that each model's performance was influenced by the

Table 5.3
Neural network based detection.

Sn	Reference	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
1	(Gebremeskel et al., 2023)	Hybrid DDOS attack model based on entropy and Deep learning.	Detection	SDN	Deep Learning	Control	80 Feature dataset	POX
2	(Elubeyd and Yiltas-Kaplan, 2023)	DDOS detection based on hybrid CNN, GRU and DNN model for low rate DDOS attacks.	Detection	SDN	CNN, GRU, CNN	Data Control	Features from two dataset	-
3	(Mousa and Abdullah, 2023)	DDOS detection system based on deep learning against multiple attack vectors in SDN	Detection	SDN	LSTM, CNN, SAE	Data control	Features from two datasets	-
4	(Mansoor et al., 2023)	- Proposed a DDOS detection based on RNN - Utilized a cross feature selection approach to select the best features	Detection/ Mitigation	SDN	RNN	Control	bytecount, pktcount, dt, tot_dur, dur	Ryu
5	(Zhou, 2023)	– Utilized Information entropy for attack identification. – CNN-BiLSTM for detection of malicious attacks	Detection	SDN	CNN, BiLSTM	Control	19 Feature set	-
6	(J. Wang et al., 2023)	-Utilized CNN-GRU for fine grained detection of DDOS Attack flow	Detection	SDN	CNN, GRU	Control	avg_packets,avg_byte, survival_degree,avg_duration, ratio_packet	Ryu
7	(J. Wang and Wang, 2022)	- Defense system based on CNN-ELM model. - Mitigation module to locate attacker and stop abnormal traffic from the source	Detection/ Mitigation	SDN	CNN, ELM	Control	Features from two datasets	Ryu
8	(Makuvaza et al., 2021)	-IDS based on deep neural network for detecting DDOS attack in real time	Detection	SDN	DNN	control	– Backward packet length (B. packet Len) Standard deviation (Std) – Flow Duration – Average Packet Size – Flow Inter Arrival Time (IAT) Standard deviation (Std)	
9	Assis *et al,* 2020	Presented a security mechanism detection and prevention of DDOS from Source end and SDN controller -implemented two modules: detection and mitigation	Detection and Mitigation	IOT	CNN	Control	– Bits/sec – Packet/sec – Source port – Destination port – Source IP – Destination IP	Floodlight
10	Haider et al. (2020)	Proposed an efficient detection approach based on deep Ensemble CNN	Detection	SDN	Deep CNN	Control	Backward packet length (B. packet Len) Std, Flow Duration, Avg Packet Size, and Flow inter arrival time (IAT) Std,	-
11	Novaes et al . (2020)	– First, the entropy of the network flow features was calculated. – LSTM was applied to the entropy metric for each flow attribute, and LSTM predicts the signature of normal behavior for each attribute – Then, abnormalities in the network are identified using fuzzy logic. Later on, a dynamic policy for DDoS attack mitigation is created using an Event Condition-Action (ECA) model	Detection Mitigation	SDN	LSTM Fuzzy Logic Shannon Entropy	Application	Source IP Destination IP Source Port Destination Port Plane	Floodlight
12	Ujjan et al., 2020	– Adaptive polling and sflows based sampling approach to detect DDOS. – leverage on the programmability feature of SDN to allow placement of IDS. – The detection technique was deployed separately to reduce overhead and processing time of switch – 6 DDOS Attacks were launched	Detection	IOT	Stack autoencoder	Control Data	Source IP Destination IP Source port Destination port	Ryu
13	Priyadarshini and Barik. (2019)	– DDOS defense mechanism based on LSTM model of deep learning on controller – filtered and forward legitimate packets using network traffic analysis mechanism or block them.	Detection Mitigation	FOG/ CLOUD	LSTM (Deep learning)	Control	Source IP Destination IP	Floodlight
14	Sun (2019)	– Detection technique computes entropy and applied BiLSTM-RNN to classify traffic in real-time	Detection	SDN	BiLSTM-RNN is	Control	Average of Duration per Flow (ADF), Average of Packets per Flow (APF), Growth of Flow	

(*continued on next page*)

Table 5.3 (*continued*)

Sn	Reference	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
		– Anomaly Detection Module, Flow Table Collection Module, Feature Extraction Module and Attack Detection Module comprise the detection techniques					Entries (GFE), the Rate of Flow table Matching (RFM), Percentage of Pair-Flow (PPF), Entropy of Source IP Addresses (ESA), Entropy of Destination IP Addresses (EDA), Entropy of Protocol Type (EPT)	
15	Gong et al., 2018	-Proposed trust evaluation and management framework	Detection	SDN	ELM	Control Data Application	- Packet loss rate - Bandwidth - Time delay	Floodlight
16	Li et al. (2018)	The neural network models CNN, RNN, and LSTM are utilized for network attack detection. The Deep Learning DDoS Detector module determines whether packets entered into the current OpenFlow switch are attack packets by employing a trained deep learning model. – In the event that this is the case, the attack packet will be sent to the Information Statistics module for statistical analysis; If not, it won't be processed.	Detection/ Mitigation	SDN	CNN, RNN, LSTM	Data	Source port Destination port Source port Destination IP Source IP	
17	Varun and Sibi, (2018)	-lion optimization was utilized for feature selection while CNN for classification	Detection	SDN	LOA, CNN	Control	Time Connection based Content based	
18	Nam et al. (2018)	Proposed two approaches for DDOS detection in SDN based on SOM and KNN. The scheme consists four modules: Monitor, Algorithm, Alert and Mitigation	Detection Mitigation	SDN	SOM, KNN	Control	Entropy of Source IP Entropy of Source Port Entropy of destination port Entropy of packet protocol Total number of packets	POX
19	Pillutla and Arjunan, (2018)	-Fuzzy-SOM mitigation techniques that improves SDN capability against DDOS attacks in the cloud	Mitigation	Cloud	Fuzzy-SOM	Control	-mean number of packets per low (MNPPF), mean number of bytes per low (MNBPF), mean duration time per low (MDTPF), mean percentage of low pairs (MPFP) and rate of growth per lows (RGPF)	NOX
20	Karan, et al. (2018)	-DDOS attack detection using a two-level security -Snort is used to detect signature attack and later a classifier is built using SVM and Deep neural Network	Detection	SDN	SVM, DNN		41 features from Dataset	Ryu controller
21	Cui, *et al*, (2018)	-Identification of the attack was done by extracting temporal behavior of an attack and extracting the pattern of attack by training the back propagation neural network. – A flow entry is pushed by the attack defense module to the associated OF switch, and the switch then discards all packets arriving at the victim port. t	Detection Mitigation	SDN	BPNN	Control	Number of Packets per flow Number of flows per port Duration	Floodlight
22	Niyaz et al. (2017)	In order to extract a smaller collection of features from a larger set, a deep learning method was applied. With a very low FPR in comparison to other works, it accurately identifies the traffic with a rate of 99.82 %.	Detection	SDN	Stack Autoencoder	Control	Number of bytes per flow Number of packets per flow Entropy of the features set	POX Controller
23	Xu and Liu, (2016)	– The attacker detection mechanism finds the target first using a flow volume feature and a flow rate asymmetry characteristic, and then determines the attack using a SOM-based classifier.	Detection	SDN	SOM	Control	Packet count per source Byte count per source Packet count Asymmetry from source Byte count Asymmetry from source	-
24	Cui *et al*, 2016	-Four parts make up the protection mechanism against DDOS attacks. Trigger, detection module, traceback, and mitigation for DDOS attacks	Detection and Mitigation	SDN	Neural network	Control Data plane	– Number of packets matched by each flow entry, – Number of bytes matched by each flow entry, survival time of each flow entry, packet rate of each flow entry and byte rate of each flow entry	RYU Controller

Table 5.4
Other DDOS detection.

Sn	Reference	Highlights	Scope	Domain	Algorithm	Plane	Features	Controller type
1	(Wang and Wang, 2020)	Proposed efficient and low-cost defense mechanism against DDOS attack -it checks packets with high IP Variability determine the likely hood of DDOS attack -The controller instruct switch to block malicious connections by installing flows -Detect protocol-based attacks on time.	Detection/ Mitigation	SDN	-IP variability Algorithm	Control	– Flow size – Variability Source IP – Duration	Ryu
2	Al-duwairi et al. (2020)	-To discriminate between valid and malicious SYN packets, authors suggested a mitigation method based on deliberate packet dropping.	Mitigation	SDN	Intentional dropping technique	Control Data	IP source address, IP destination address, source port number, destination port number, packet arrival time	POX
3	Conti et al. (2019)	-Authors proposed selective blocking and periodic monitoring method	Detection	SDN	Selective blocking and periodic monitoring	Data plane	IP address MAC address	
4	Conti and Gangwal (2019)	Determine each queue's weight, and choose the one with the highest weight To find the anomaly, a cumulative sum (non-parametric) technique is applied. –Periodically, the server's Cu Sum value is calculated and compared to a predetermined threshold. If it does, the attack is recognized.	Detection	SDN	CUSUM (Cumulative Sum)	Control		POX
5	Manso et al. (2019)	– IDS based on SDN for early detection of DDOS attack – Automatically detects attack and then alert the SDN controller – Controller sends some forwarding rules to the network devices – Detect cyber-attacks, mitigate impacts on network – Performance and ensure data delivery	Detection and Mitigation	IOT	Rules based IDS Monitor	Data Control	Flow table information	Ryu
6	Bose et al. (2019)	-Utilized a Blockchain approach to provide security as a service in order to protect the SDN architecture against DDOS Attacks	Mitigation	SDN	Blockchain	Data	Flow table information	POX
7	Saifei et al. (2019)	– Schedule the processing of controller request – Calculate weight of each queue, the queue with biggest weight will be selected.	Mitigation	SDN	Scheduling/ Queuing	Data control	Waiting time Length of queue Extent of queue	Ryu
8	Bhushan and Gupta, (2018)	The list of IP addresses used as attack sources is kept up to date in the Black List database. – The strategy examines the flow table state of all other switches to find a suitable switch when the target switch is under attack. –calculating the vacant slots of other switches involves using a mathematical model based on queuing theory.	Mitigation	Cloud	Queuing theory	Data	Flow table space Plane	POX
9	Gao et al. (2018)	-To identify packets-in message attacks, authors employed fuzzy C-means.	Detection	SDN	Bayes network Fuzzy c-means	Control	Mean packet per flow Percentage of pair flows Growth of foreign flows Growth of different ports Deviation of packet counts Deviation of byes counts	POX
10	Yan et al. (2017)	Scheduling method was utilized by the authors to fight against the DDOS attack	Detection	SDN	Controller Scheduling method	Data Control	Flow request	POX
11	Wang 2015	– Employed graphical model – The DAMASK-D module generates an alert when an attack is detected; otherwise, it forwards to the destination. The DAMASK M module gets the alert and looks for a countermeasure that matches; if not, it drops, forwards, or modifies it.	Detection/ Mitigation	Cloud	Graph Inference Model (Chow–Liu Algorithm)	Data	Dynamic feature selection	Floodlight

training dataset in a real testbed, they achieved 90 % accuracy. However, the approach could only detect flood-based attacks, low-rate attacks that are detrimental to the network was not considered. In Sangodoyin et al. (2021) applied four machine learning algorithms to detect and classify DDOS flooding attacks using jitter, throughput, and response time. They first tested the vulnerability of SDN by launching attacks to affect the SDN server in an emulated SDN environment. The quadratic discriminant analysis (QDA), Gaussian Naïve Bayes (GNB), k-nearest neighbor (k-NN), and classification and regression tree (CART) algorithms were used for detection and classification, and the suitability of these algorithms was demonstrated using MATLAB.

The work of Ahuja et al. (2021) produced a novel dataset and a hybrid Random forest -Support vector classifier was applied for DDOS attack detection in SDN. However, the dataset used contains multiple features computed from both Switch flow and port statistics which may cause overhead on the controller if integrated in real SDN based network. Sahoo et al. (2020) suggested a detection and mitigation strategy that combine the Support Vector was used to reduce the

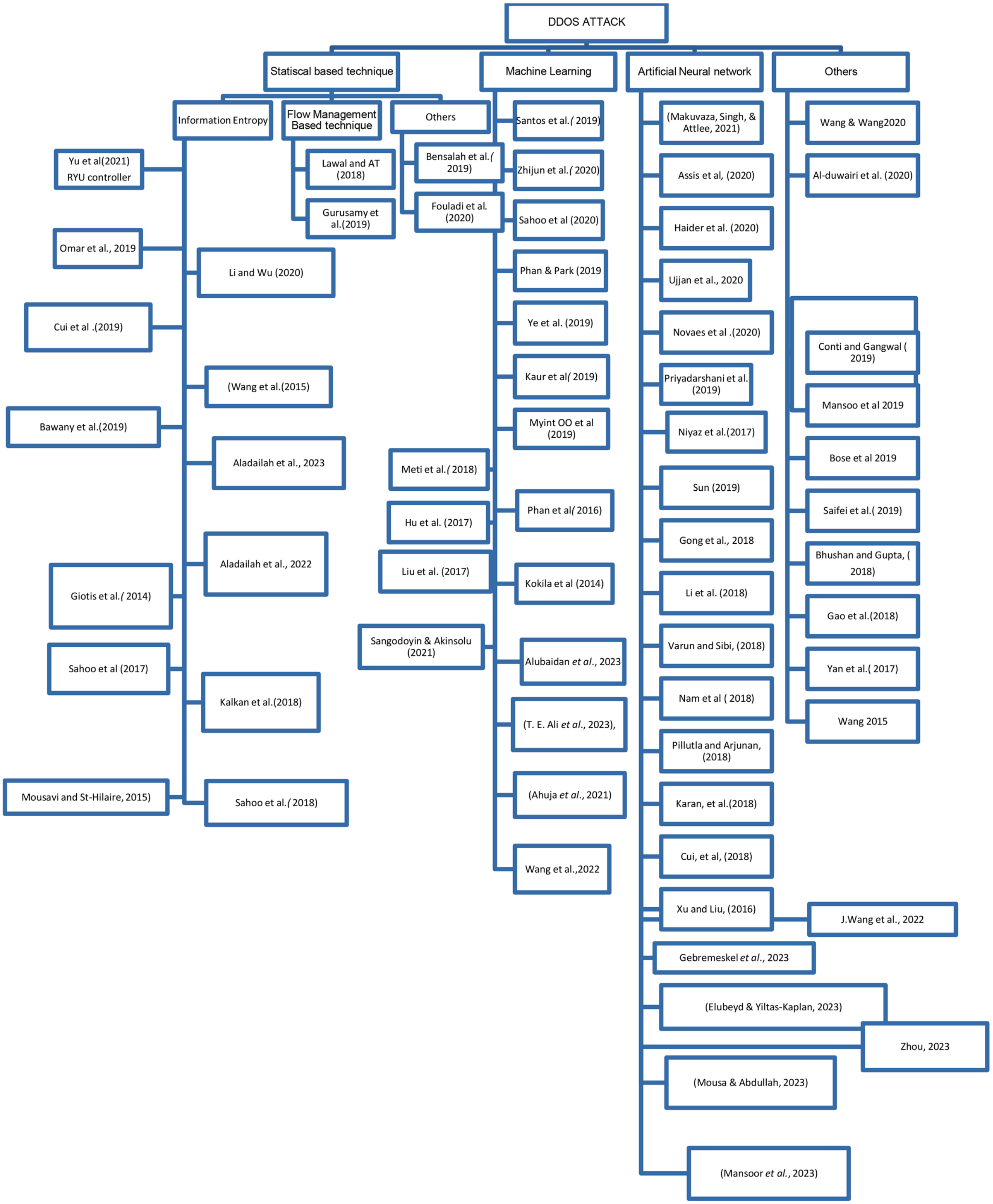


Fig. 5.1. A Taxonomy of Statistical based detection Techniques.

dimension of feature vectors, and the Genetic Algorithm was used to optimize SVM parameters. N-RBF was proposed and implemented to shorten the training duration. Zhijun et al. (2020) proposed a Factorization Machine-based DDOS detection method which was used to detect low-rate DDOS attacks after extracting approximately four features from flow rules: duration time, packet number, relative dispersion of match bytes, and relative dispersion of packet interval. After the attacks are identified, a mitigation system is triggered to erase flow rule to rule to free up the flow table space since the quantity of flow rules begins to ascend in a slope when an attack is launched. Mininet and

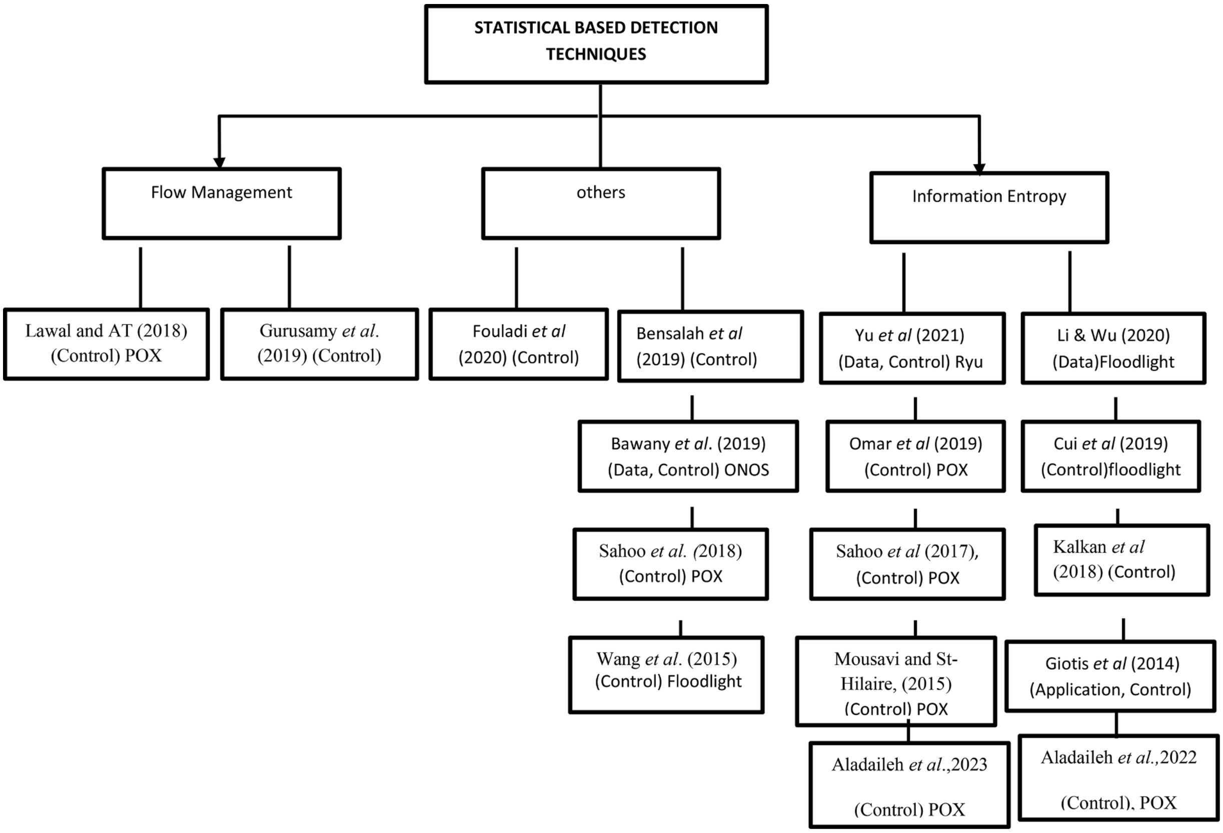

STATISTICAL BASED DETECTION TECHNIQUES
Flow Management
others
Information Entropy
Lawal and AT (2018) (Control) POX
Gurusamy et al. (2019) (Control)
Fouladi et al (2020) (Control)
Bensalah et al (2019) (Control)
Yu et al (2021) (Data, Control) Ryu
Li & Wu (2020) (Data)Floodlight
Bawany et al. (2019) (Data, Control) ONOS
Omar et al (2019) (Control) POX
Cui et al (2019) (Control)floodlight
Sahoo et al. (2018) (Control) POX
Sahoo et al (2017), (Control) POX
Kalkan et al (2018) (Control)
Wang et al. (2015) (Control) Floodlight
Mousavi and St-Hilaire, (2015) (Control) POX
Giotis et al (2014) (Application, Control)
Aladaileh et al.,2023 (Control) POX
Aladaileh et al.,2022 (Control), POX

Fig. 5.2. A Taxonomy of Machine learning based detection Techniques.

the RYU controller were used to simulate the performance and evaluate it.

In the work of Santos et al. (2019) SVM, Multiple layer Perceptron (MLP), Decision tree, and Random forest were used to distinguish DDOS attacks in the domain of SDN. Attacks targeting the Bandwidth, the SDN controller, and the Switch Flow table, were considered in the study. a. Mininet and POX Controller were used to simulate DDOS attacks in SDN Environment. The outcome demonstrates that, the Decision tree algorithm takes the least time to process while the Random Forest algorithm achieves the highest accuracy of 100 %.

An enhanced history-based IP filtering scheme (eHIPF) and a hybrid machine learning model based on SVM and SOM were proposed by Phan and Park (2019) to enhance attack detection rate, and speed and to improve traffic classification. The proposed mechanism was evaluated with a 99.27 percent detection rate and 99.30 percent accuracy. The control plane and the data plane are the attack points that this study looks at, and attack traffic for ICMP flooding and TCP SYN Flooding were made to test the proposed mechanism.

A Support Vector Machine-based classification of DDOS attacks was proposed by Ye et al. (2018). The Authors utilized a six tuple features for classifying normal traffic from DDOS traffic. The detection strategy first gets the statistics of flow from the flow table switch which is further processed to extract characteristic values related to the DDOS attack and then finally, it is sent to the classifier judgment for classification by SVM. Kaur et al. (2019) used a Hybrid Machine learning technique based on KNN and SVM to identify malicious flow at the controller using certain parameters. Packet flow and time durations were used as part of the parameters for detection. KDDCUP99 dataset were used to evaluate the model on MATLAB. Myint Oo et al. (2019) presented a DDOS attack detection strategy based on an Advanced Support Vector Machine (ASVM) which was used to identify two flooding-based DDoS attacks. The work considered Control plane Flooding attacks with detection rate of 97 %.

Meti et al. (2017) classified traffic as legitimate or DDOS attacks using machine learning methods like neural network classifier and SVM. This was accomplished by sending a client's request to the model on the server, which then predicted whether the traffic was legitimate or an attack. This study looked at attacks on the Controller. The SVM outperforms the Neural Network in terms of performance because it has the highest accuracy—80 percent—as well as reasonable precision and recall.

Hu et al. (2017) also proposed an SVM-based, lightweight framework for detecting and preventing DDOS attacks in SDN. The authors used SDN Controller and Sflow agent to collect traffic data to implement the framework. Entropy was used to extract network features. The SVM classifier was used to find the anomalies in the network. The Control plane and the Data plane are the attack vectors considered by the detection module, which is running as an application on the Controller. SYN Flood attack, UDP Flood, and ICMP Flood are the components of the Training sample that was applied to the SVM. Attacks of this kind use up server and network resources. When the attack rate was greater than 3000 packets per second, the detection rate reached 100 %. The lower detection rate is due to the low traffic. Liu et al. (2017) proposed a method for effectively detecting DDOS attacks using SVM and mitigating them by instructing the flow to block attacks from the Source Port as a means of resolving the IP spoofing issue. The security scheme was experimented on Mininet environment with a floodlight controller. Phan et al. (2016) proposed an SDN -optimized flood protection scheme based on the SVM classifier and a novel algorithm called Idle-timeout Adjustment (IA). The authors examined the proposed scheme and calculated metrics based on the number of streams, CPU usage of the SDN controller, and OpenvSwitch. Another SVM classifier-based DDOS attack detection was presented by Kokila et al. (2014). An existing data set was utilized by the Authors to test the detection approach. When compared to other methods for machine learning, the classifier produced a least positive result. This detection method was a used-on attacks targeting the SDN controller.

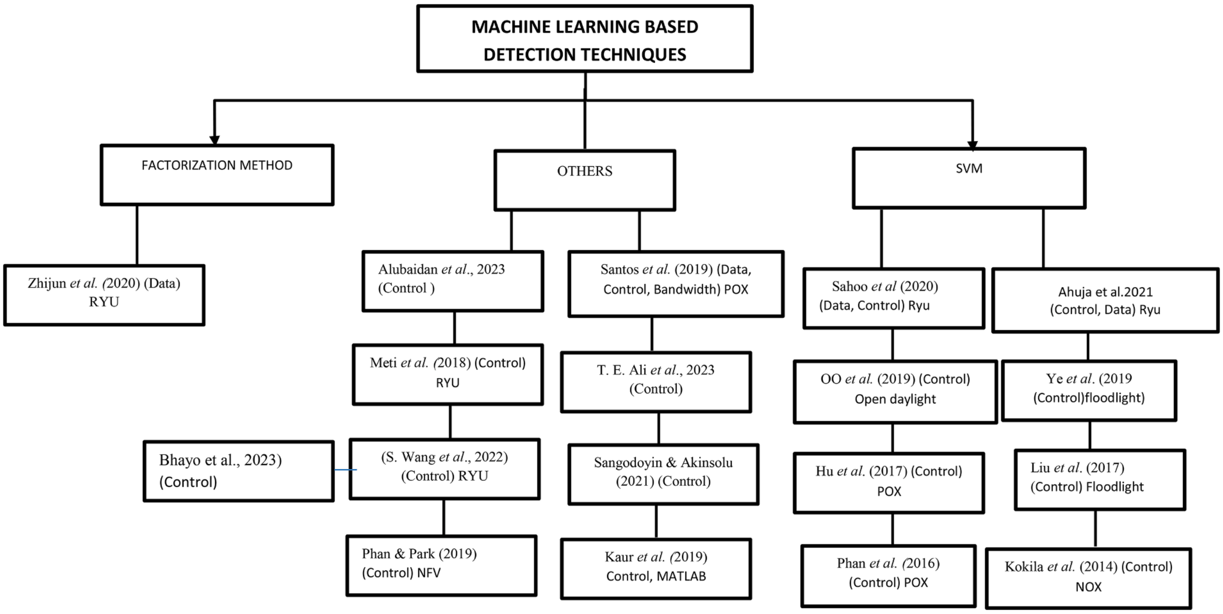

MACHINE LEARNING BASED DETECTION TECHNIQUES
FACTORIZATION METHOD
OTHERS
SVM
Zhijun et al. (2020) (Data) RYU
Alubaidan et al., 2023 (Control)
Santos et al. (2019) (Data, Control, Bandwidth) POX
Sahoo et al (2020) (Data, Control) Ryu
Ahuja et al.2021 (Control, Data) Ryu
Meti et al. (2018) (Control) RYU
T. E. Ali et al., 2023 (Control)
OO et al. (2019) (Control) Open daylight
Ye et al. (2019 (Control)floodlight)
Bhayo et al., 2023) (Control)
(S. Wang et al., 2022) (Control) RYU
Sangodoyin & Akinsolu (2021) (Control)
Hu et al. (2017) (Control) POX
Liu et al. (2017) (Control) Floodlight
Phan & Park (2019) (Control) NFV
Kaur et al. (2019) Control, MATLAB
Phan et al. (2016) (Control) POX
Kokila et al. (2014) (Control) NOX

Fig. 5.3. A Taxonomy of Neural Network based detection Techniques.

5.3. Neural network based detection

As can be seen in Table 5.3 and Fig. 5.3, a variety of researchers have utilized detection methods that are based on Neural networks. The work of Gebremeskel et al. (2023) used entropy variation of target host IP address to detect anomalies, and the deep learning model was applied for classification. The CICDDOS2019 dataset was used to implement the model in SDN environment using a distributed Controller. The result was promising. Hence, a hybrid deep learning model based on CNN, GRU and DNN model was proposed by Elubeyd and Yiltas-Kaplan (2023) for high and low - rate DDOS Attack detection with more emphasis on Low-rate attacks. The study generated its dataset and was tested for DDOS attack detection via Simulation in SDN Environment. Even though promising results was achieved, mitigation strategies were not put in place after detection. Additionally, small topology was used to test model which may not provide a good generalization ability. Another hybrid model based on CNN, LSTM and Stack Auto encoder was used by Mousa and Abdullah (2023) for DDOS attack detection in SDN. The model was tested by utilizing two datasets with promising results. However, it was not tested in real time. In the work of Mansoor et al. (2023) proposed an RNN based detection approach implemented using SDN dataset. The authors applied two feature selection method to improve detection which shows a high accuracy and low FPR. Other deep learning models could be implemented to test the effectiveness of the proposed approach. A CNN-GRU model was utilized in Wang et al. (2023) to detect DDOS attack flow. Entropy was first employed to identify anomalies using source and destination IP before applying the CNN-GRU model for classification. Author in Zhou (2023) proposed a detection approach which used information entropy to identify attacks while CNN-BiLSTM model was used for detection of maclious attacks using an SDN generated datasets. However, it was not tested in an SDN test Bed. Wang and Wang (2022) proposed a detection system based on CNN-ELM for DDOS attack detection. The study utilized IP trace back to locate the attacker and a blacklist of abnormal traffic is maintained to mitigate against future attacks. The model was implemented via simulation using Ryu Controller. The result shows a reasonable performance. However, the approach may need to be tested in a real SDN network. The work of Makuvaza et al. (2021) proposed a real-time IDS for DDOS-based Deep Neural Network detection. The CICIDOS 2017 dataset was used for the model's evaluation. The DNN model was trained using selected parameters such as the standard deviation (Std), the flow duration, the average packet size, and the flow inter arrival time (IAT) standard deviation (Std). The model processed quickly and produced high accuracy. However SDN an SDN-based dataset was not used, hence the generalization capability is in doubt. Assis et al. (2020) presented a security system that safeguards the SDN Controller and allows for the detection and prevention of DDOS attacks at the Source end. The mitigation module is responsible for selecting drop policies to secure the SDN controller. The detection module uses a multi-dimensional IP flow analysis called Convolutionary Neural network (CNN) to detect and identify the occurrence of an attack. In order to assess the effectiveness of the CNN method, two scenarios were presented as test sets. The first was a Mininet and Floodlight controller simulation of SDN data. Additionally, CNN is tested with the CicDDOS2019 dataset in the second scenario.

Haider et al. (2020) proposed a deep Convolutional Neural Network-based detection system for effectively detecting DDOS attacks in SDN. The Ensemble CNN was chosen for the proposed detection system because it performed better than the Ensemble RNN, LSTM, and Hybrid RL. The features utilized from the dataset to train the model include Backward Packet Length Std, Flow Duration, Avg Packet Size, as well as flow inter arrival time standard. Better accuracy and reduced computational complexity are evident in the experiments' output.

A hybrid scheme based on LSTM and Fuzzy logic for detecting both Port scan and DDOS attacks was presented in Novaes et al. (2020). In this study, the network features were first quantified based on the estimated entropy metrics. LSTM is then used to model the pattern of each attribute of the normal traffic and finally the anomalies in the network were detected using fuzzy logic. This approach was validated using Mininet simulations on a floodlight controller. Ujjan et al. (2020) suggested utilizing adaptive polling-based sample data and Sflow to detect DDOS attacks. To improve detection accuracy, the strategy used Stack Auto encoder and Snort IDS at the control plane. Through time- and packet-based sampling, it collects flows from the data plane and sends them to SNORT IDS and the Stack Auto encoder for detection. The model was tested with 22 feature vectors, and the results show that Sflows performed better than Adaptive sampling. Priyadarshini and Barik (2019) used SDN to implement a deep learning-based DDOS defense mechanism on an SDN controller. It used a technique called network traffic analysis to either block or forward legitimate traffic to the server. First, historical data are used to train the deep learning model. Floodlight was used as the SDN controller to simulate a cloud/fog environment. The characteristics of the network are gathered by the Controller and sent through a Deep learning detector module to distinguish between DDoS packets and normal packets.

A neural network-based detection method was proposed by Sun et al. (2019). After calculating the traffic features' entropy to determine a flow's abnormality and issuing a warning, the flow entry is acquired from the switch to take out essential features. The algorithm is trained with the BILSTM-RNN, and BiLSTM is used to classify real-time traffic in order to detect DDOS attacks. Experimentation in an SDN environment allowed for the validation of the model, and the detection method enables accurate classification with minimal controller overhead.

Gong et al. (2019) proposed a trust evaluation module in a trusted OpenFlow switch and a network monitoring module to build an intelligent trust model for hybrid DDOS detection in SDN. Mechanism for Monitoring Network parameters are included in the network monitoring module. Based on the monitored parameters, the network intelligent trust module evaluates trust, and the detection is done using Extreme learning machine.

Li et al. (2018) suggested using deep learning to detect DDOS attacks in Open flow-based SDN. The three classical neural network models used in deep learning served as the basis for the design of the model's four layers. Data traffic was used in a real-time DDOS attack test that included five different types of attacks: ARP Flood inundation, SYN Flood attack, Ping of Death, Smurf attack, and UDP Flood attack. In the model training phase, the detection method achieved high accuracy of 98 % and 99 %.

Varun and Sibi (2018)constructed an intrusion detection system by utilizing the Lion Optimization Algorithm and Convolutional Neural Network. Within a small amount of attack traffic, the method can identify DDOS attacks. For feature selection, the lion optimization algorithm was used, and CNN was used to classify attack traffic.

Nam et al. (2018) suggested employing two Self-Organizing Map--based detection methods. After training the attack traffic with SOM, the hybrid SOMM-KNN classification algorithm and the SOM distributed classification algorithm are used to speed up the process. Through an experiment on an SDN-based test bed, the algorithms were used to create the DDOS detection scheme and its implementer.

Pillutla and Arjunan, (2018) used a five (5) tuple features to design a Fuzzy - SOM DDOS mitigation approach that further develops SDN capacities in the cloud. An attack-response process is used to stop attack flows on the SDN controller, and the mitigation approach monitors input traffic. Adaptive threshold is used to find particular types of DDOS attacks. Experiments are used to test the model with high accuracy.

Karan et al. (2018) suggested using two levels of security to detect DDOS attacks. The signature attacks were detected using the Snort, and a classifier built with SVM and a deep neural network were used to find incoming data packet network anomalies. RYU controller was used to test the detection model on Mininet.

An approach that extracts an attack's temporal behavior and trains a back-propagation neural network to extract an attack pattern to identify the attack was proposed by Cui et al. (2018). The defense module is triggered to block both the attack source port and the legitimate source port when the attack is detected by the attack detection module. Last but not least, the port recovery module is used to dynamically recover the port belonging to the authorized user. Floodlight served as the controller for the DARPA 199 dataset that was used to validate the model on Mininet. Niyaz et al. (2017) proposed a profound learning based Multi vector DDOS attack location framework. Unsupervised use of a Deep learning technique was used to reduce the large number of features extracted from network packet headers. Traffic collector and flow installer (TCFI), feature extractor (FE), and traffic classifier (TC) are the three modules that made up the detection system. The model was then applied on Traffic informational index gathered in various climate. As a controller-based network application, the system tries to spot attacks on both the data plane and the control plane. With 99.82 percent accuracy and the lowest positive rate, the proposed system classifies traffic into either normal or attack classes and identifies each DDOS attack class individually. The proposed framework can restrict the Controller performance on a large network in light of the fact that, the Traffic collector, flow Installer and the Feature extractor are all implemented on the Controller.

Xu and Liu (2016) proposed DDOS identification scheme comprising of two stages, in particular; detection of attacks and victims. The system classified the network traffic as either normal or attack using neural network techniques known as SOM. The authors used the topology of an Internet network to validate their method. Cui et al. (2016) proposed a three-module DDOS defense mechanism. The detection trigger is presented to enable the detection module to respond quickly and also decides when the attack should begin. The detection module, which is based on a neural network, is the second module. The trace back module, which tries to figure out the path of attack traffic, is the third module. The mitigation module, on the other hand, blocks attack traffic and cleans the flow table.

5.4. *Other detection techniques*

Other methods for detecting and preventing DDOS, like the block chain, scheduling, and policy-based methods, among others, have been suggested by a number of authors and are depicted in Fig. 5.4 and Table 5.4. A block chain-based framework was implemented by Bose et al. (2019) termed *BlockSDsec*. The framework was designed to provide security as a Service on SDN in order to prevent DDOS attacks at the Switch. The approach was simulated using Mininet and POX Controller. Based on a few fundamentals and an algorithm, Wang and Wang 2020 proposed a DDOS defense system that is both effective and inexpensive. The flow size—the amount of traffic that moves through each Port—is tracked by the switches in the ELD model. Additionally, the Controller is notified by the switch whenever a port's flow size exceeds the average value across the network. The Controller, through the module for assessing IP variability, evaluate the inconstancy of Source IP addresses for that Port. The Controller considers an elephant flow safe if IP variability is low. Otherwise, the Controller uses the impulse flows modules to determine whether it is a safe impulse flow scenario. Given the modules check isn't passed, the Controller reasons that a DDoS attack is occurring. In this instance, the Controller uses the DDoS attack stop-ping module to inquire about the switch that is dropping malicious packets and then recovers the switch's settings once the attack has ended. Al-duwairi et al. (2020) developed a mitigation strategy known as ISDSDN that relies on deliberate dropping to differentiate legitimate from malicious SYN packets. The method makes use of the persistence of the client by sending SYN packets to try to establish a connection, but the packets are lost or dropped because of congestion. The TCP-time out mechanism was used to determine whether or not SYN packets are legitimate. Utilizing the POX Controller, simulation was used to verify the method. A two-lightweight strategy against two DDOS attacks—the resource exhaustion attack and routing spoofing—was proposed by Conti and Lal (2019). The selective blocking method, in which an adversary node is prevented from using any active communication routes in a malicious manner, is used to combat routing spoofing. The periodic monitoring method, on the other hand, is used to identify an adversary node based on traffic statistics gathered over a specific time period. Conti and Gangwal (2019) offered another lightweight strategy. The authors detected a DDoS attack in SDN using Cumulative sum. They validated the proposed method by employing two conventional data sets. Internet traces from the CAIDA dataset and the DARPA intrusion detection dataset are included in the dataset.

Manso et al. (2019) proposed an SDN-based intrusion detection system (IDS) for early DDOS attack detection; the framework is comprising of detection, communication and mitigation phases. The communication phase begins when a DDOS attack is detected by detection phase, the IDS notifies the controller, and the mitigation phase involves the Controller ensuring malicious traffic are blocked by sending

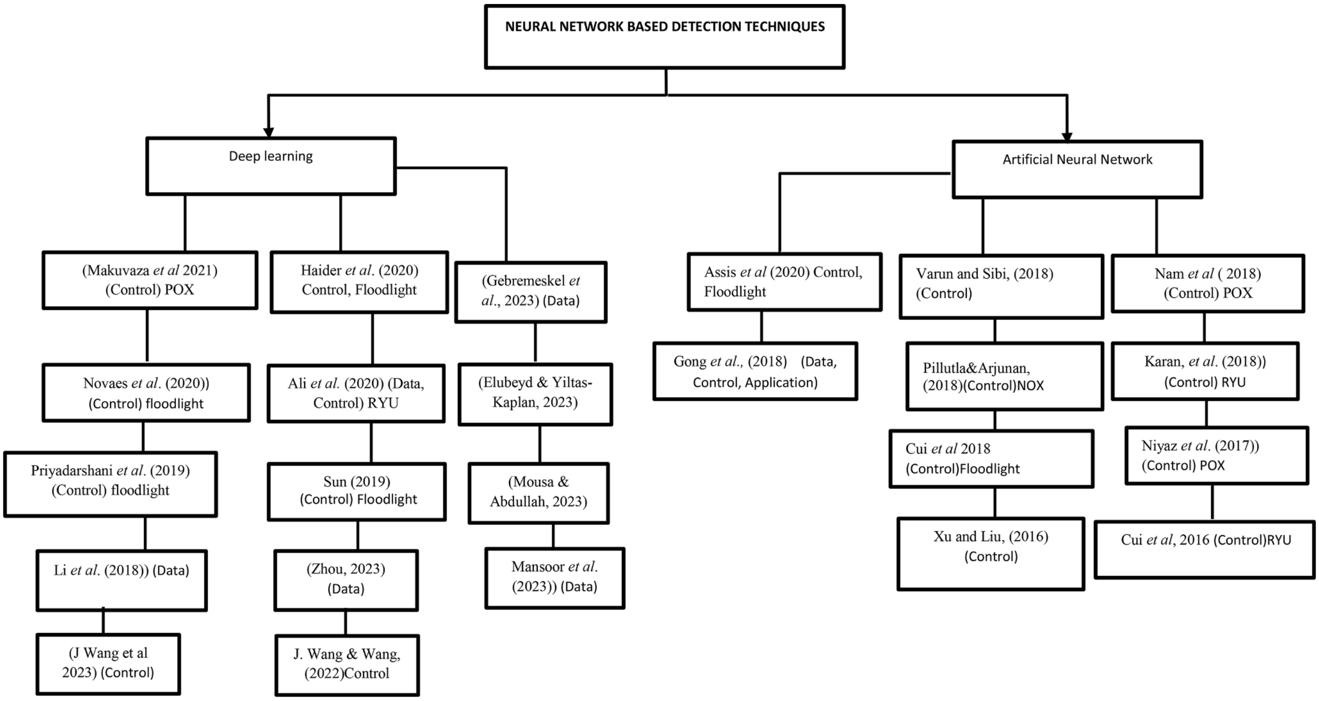

NEURAL NETWORK BASED DETECTION TECHNIQUES
Deep learning
Artificial Neural Network
(Makuvaza et al 2021) (Control) POX
Haider et al. (2020) Control, Floodlight
(Gebremeskel et al., 2023) (Data)
Novaes et al. (2020)) (Control) floodlight
Ali et al. (2020) (Data, Control) RYU
(Elubeyd & Yiltas-Kaplan, 2023)
Priyadarshani et al. (2019) (Control) floodlight
Sun (2019) (Control) Floodlight
(Mousa & Abdullah, 2023)
Li et al. (2018)) (Data)
(Zhou, 2023) (Data)
Mansoor et al. (2023)) (Data)
(J Wang et al 2023) (Control)
J. Wang & Wang, (2022)Control
Assis et al (2020) Control, Floodlight
Gong et al., (2018) (Data, Control, Application)
Varun and Sibi, (2018) (Control)
Pillutla&Arjunan, (2018)(Control)NOX
Cui et al 2018 (Control)Floodlight
Xu and Liu, (2016) (Control)
Nam et al (2018) (Control) POX
Karan, et al. (2018)) (Control) RYU
Niyaz et al. (2017)) (Control) POX
Cui et al, 2016 (Control)RYU

Fig. 5.4. A Taxonomy of Other DDOS detection Techniques.

a flow rule to the switch. A Controller scheduling strategy was proposed by Saifei et al. (2019) to prevent DDOS attacks. The Controller schedules the processing of requests by figuring out how much each queue weighs. The queue that needs to be handled is the one with the most weight. Through RYU controller simulation, the method was verified. Another Controller scheduling method for detecting DDOS attacks was proposed by Yan et al. (2017). Controller scheduling is utilized to process flow requests from various switches in order to safeguard the legitimate switch in the network. The method employs a variety of time slice allocation strategies based on the intensity of DDOS attacks. The efficiency of the model was tested by means of simulation with Mininet and POX Controller. The work of Bhushan and Gupta (2018) presented a strategy that examines the flow table state of all other switches to find a suitable switch when the target switch is under attack. Mathematical model based on queuing theory was used to calculate the vacant slots of switches. The model was implemented with a POX Controller. In Gao et al. (2018), Packet_in message attacks were identified using the Fuzz -c means. Traffic Features such as Mean packet per flow, Percentage of pair flows. growth of foreign flows, expansion of several ports, deviations of both packet counts and bye counts were utilized by the authors to implement the detection approach and was tested on SDN Environment with POX Controller. Wang et al. (2015) leveraging on SDN DDOS attack mitigation approach termed DaMask was introduced. The DaMask-D module is in charge of sending attack alerts to the DaMask-M module. Whereas, the DaMask M module is in charge of receiving alerts and locating countermeasures that are compatible. If not, it slows down, speeds up, or alters the flows. The Chow–Liu algorithm is the foundation of the model. Through simulation on Mininet with a floodlight Controller, the detection model was validated.

6. Parameters for performance evaluation

This section gives a synthesis of techniques used to evaluate performance by various authors in literature. In evaluating the performance of the various detection techniques as well as providing analysis of the experiment carried out, various authors have used some set of metrics such as: CPU utilization, Network load, True positive rate (TPR), False positive rate (FPR), False Negative Rate (FNR), Accuracy, Detection rate, Precision, ROC and Recall as tabulated in the Table 6.1 and categorized into Standard Metrics and Detection System Metrics in (Fig. 6.1).

6.1. Standard metrics

Various classically metrics of Performance evaluation have been used by various authors as shown in Fig. 6.2. From Fig. 6.2, Accuracy appears to be the highest used Evaluation metrics while the least metric used is Sensitivity. This study has categorized the metrics into three namely performance analysis metrics, Error/misclassification metrics and comprehensive assessment metrics.

6.1.1. Performance analysis metrics

The performance Analysis metrics are metrics that were used by various authors in the studied literatures to evaluate a model's performance. These metrics include: Sensitivity, Specificity, Accuracy, True Positive Rate (TPR), Recall. About 74 % (26) of the article reviewed highlighted the use of Accuracy to evaluate their methods. While 11 % (4) utilized TPR, 3 % (1) used Sensitivity, 6 % (2) used Specificity, and 31 % (11) used Recall.

a. *Relationship to attack Characteristics:* A majority of the literature examined has focused on identifying flooding-based attacks, a type of volumetric attack. (Ahuja et al., 2021) utilized volumetric attacks like UDP, ICMP, and SYN flood attacks to implement their detection strategy. On the other hand, Banitalebi and Mohammadreza (2020); Sahoo et al. (2020); Banitalebi and Mohammadreza (2020) incorporated datasets containing a combination of volumetric, application layer, and low-rate attacks. In contrast, studies by Alubaidan et al. (2023); Wang et al. (2022) among others, aimed to detect low-rate attacks. These variations underscore that, DDoS attacks manifest in different ways, each necessitating specific detection approaches outlined in the literature.

Given the diverse nature of DDoS attacks, achieving effective detection performance is paramount. Hence, metrics such as Sensitivity, Specificity, Accuracy, True Positive Rate (TPR), and Recall are

Table 6.1
Parameters of performance evaluation.

SN	Author		Performance metrics											System metric	
		ACC	DR	FAR	F1 SCORE	TPR	FPR	FNR	ROC	RECALL	PREC	SEN	SPEC.	CPU Util.	Network load
1.	Fouladi et al., 2020	✓			✓	✓	✓		✓						
2	Cui et al. (2019)		✓				✓		✓						
3	Bawany and Shamsi (2019)	✓					✓	✓				✓	✓		
4	Sun (2019)	✓												✓	
4	Giotis et al. (2014)	✓							✓					✓	
5	Priyadarshini and Barik, (2019)	✓													
6	Sahoo et al. (2018)							✓							
7	Cui et al. (2016)													✓	✓
8	Assis et al. (2020)	✓			✓					✓	✓				
9	Wang et al. (2022)	✓			✓					✓	✓				
10	Wang et al. (2015)		✓				✓		✓						
11	Oo et al. (2019)	✓	✓	✓											
12	Ye et al. (2018)	✓		✓											
13	Wang and Wang. (2020)					✓	✓								
14	Ahuja et al. (2021)	✓	✓	✓	✓						✓		✓		
15	(Ujjan et al., 2020)	✓			✓		✓			✓	✓			✓	✓
16	Altay, 2018	✓					✓								
17	(Banitalebi and Mohammadreza, 2020)	✓			✓	✓	✓				✓				
18	Santos et al.,2019	✓							✓						
19	Phan et al.,2016													✓	
20	Hu et al.,2017		✓	✓										✓	
21	Yu et al., 2021	✓												✓	
22	Li et al.,2018	✓													
23	Liu et al.,2017													✓	
24	Kalkan et al., 2018	✓			✓					✓	✓				
25	(Alubaidan et al., 2023)	✓			✓	✓	✓			✓	✓				
26	(Gebremeskel et al., 2023)	✓			✓					✓	✓				
27	(Aladaileh et al., 2023)		✓				✓								
28	(T. E. Ali et al., 2023)	✓			✓					✓	✓				
29	(Elubeyd and Yiltas-Kaplan, 2023)	✓			✓				✓	✓	✓				
30	(Mousa and Abdullah, 2023)	✓			✓					✓	✓				
31	(Wang and Wang, 2022)	✓			✓					✓	✓				
32	(Mansoor et al., 2023)	✓		✓	✓						✓				
33	(Zhou, 2023)	✓	✓	✓											
34	(Aladaileh et al., 2022)		✓				✓								
35	(Sayed et al., 2022)	✓			✓					✓	✓				

ACC: accuracy; DR: detection rate; FAR: false alarm rate; TPR: true positive rate; FPR: false positive rate; FNR: false negative rate; PREC.: precision; SEN: sensitivity; SPEC: specificity; CPU Util: CPU utilization

essential for evaluating DDoS attack detection, primarily due to the substantial impact of attack intensity on metric performance. Authors in Wang et al. (2022), utilized Recall to assess their model's performance under varying volumes of DDoS attack traffic. The results showed that, Recall was influenced by the intensity of attack traffic. For medium traffic, Recall achieved 99.7 %, while under high traffic, it reached 99.49 %. This suggests that, exceedingly high attack volumes can diminish Recall, indicating that detection systems might struggle to handle the attack intensity, potentially leading to reduced Recall, particularly in network architectures like SDN. Conversely, low traffic can also adversely affect Recall, as demonstrated in the study of Wang et al. (2022), where minimal traffic resulted in a 0 true positive rate for one of the models used, consequently lowering Recall. The study underscores the importance of achieving a high True Positive (sensitivity) to ensure a high Recall, thereby ensuring effective detection of DDoS attacks. Additionally, it was observed that, the True Positive rate is influenced by traffic intensity this is because when traffic behaves like normal traffic, the rate of positive detection will be low (Wang et al.,2022).

Sensitivity like TPR also measures the proportion of actual attack traffic that were correctly identified by the model (Bawany and Shamsi, 2019) and hence exhibit similar characteristics. Specificity on the hand is significant in identifying the actual negative prediction (Ahuja et al., 2021). When dealing with low-rate DDoS attacks, which often involve subtle and slow exploitation attempts, distinguishing these attacks from normal traffic becomes challenging. A detection system may incorrectly identify normal traffic patterns as an attack due to the subtle nature of low-rate attacks (Alubaidan et al., 2021; Wang et al., 2022), leading to false positives. These false positives can negatively impact specificity, as they increase the count of false positives (FP) in the specificity calculation.

The influence of high and low attacks on Specificity (TNR) and Sensitivity (TPR) is extended to the Accuracy as the two metrics influence Accuracy directly. Increasing TPR (higher sensitivity) improves the number of correctly identified positive instances, thus positively affecting Accuracy. Increasing TNR (higher specificity) improves the number of correctly identified negative instances, also positively affecting Accuracy. Accurate identification of both positive and negative instances is vital for achieving high Accuracy.

a. *Relationship to Detection Method*: Machine learning, Statistical based and Neural Network approaches have used: Sensitivity, Specificity, Accuracy, True Positive Rate (TPR), Recall a metrics of evaluation. Machine learning based approaches such as (Ahuja et al., 2021; Kalkan et al., 2017; Liu et al., 2017; Oo et al., 2019; Santos et al., 2019; Wang et al., 2022; Ye et al., 2018; Yu et al., 2021 highlighted the use of one or all of accuracy, Specificity, Sensitivity, TPR and Recall for evaluating their models, this is because these metrics helps to measure the ability of machine learning models to learn patterns and classify network traffic correctly, which is crucial for effective DDOS detection.

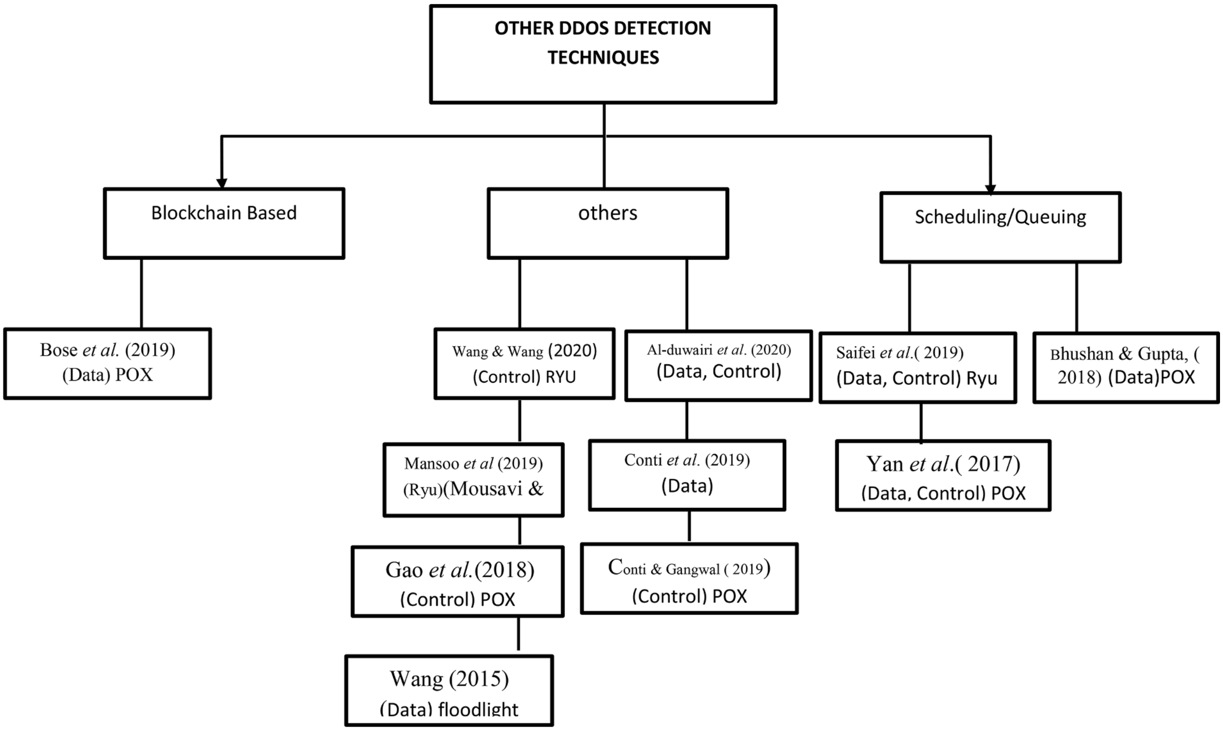

OTHER DDOS DETECTION TECHNIQUES
Blockchain Based
others
Scheduling/Queuing
Bose et al. (2019) (Data) POX
Wang & Wang (2020) (Control) RYU
Al-duwairi et al. (2020) (Data, Control)
Saifei et al.(2019) (Data, Control) Ryu
Bhushan & Gupta, (2018) (Data)POX
Mansoo et al (2019) (Ryu)(Mousavi &
Conti et al. (2019) (Data)
Yan et al.(2017) (Data, Control) POX
Gao et al.(2018) (Control) POX
Conti & Gangwal (2019) (Control) POX
Wang (2015) (Data) floodlight

Fig. 6.1. A Taxonomy of Performance Evaluation Metrics.

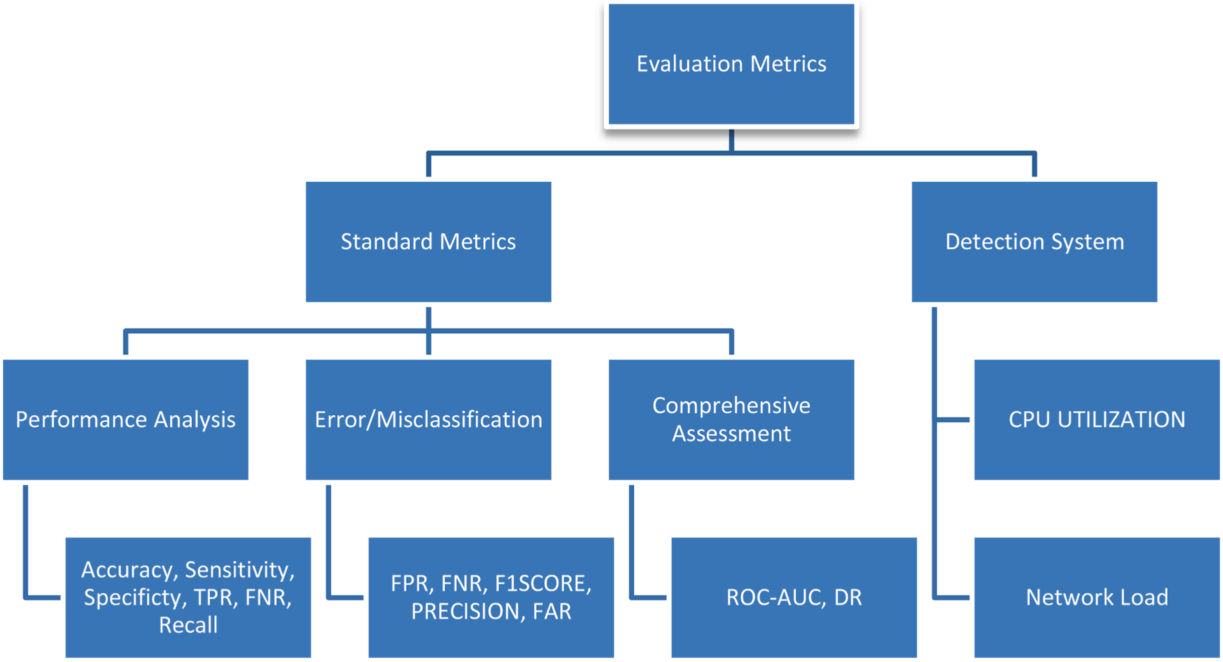


Fig. 6.2. Spread on the Usage of Standard metrics.

On the hand, the Neural networks are powerful for DDOS detection due to their ability to capture complex patterns. Hence, Accuracy is crucial to ensure that neural network models effectively learn these patterns and provide reliable detection. Consequently, the work of (Makuvaza et al., 2023; Priyadarshini and Barik, 2019; Ujjan et al., 2020; Sun, 2019) used Accuracy, Specificity, Sensitivity, TPR and Recall metrics for performance evaluation. Accuracy, Specificity, Sensitivity, TPR and Recall were also used as a metric for evaluating the detection performances of Statistical based detection approaches proposed by Bawany and Shamsi (2019); Cui et al. (2019); Fouladi et al. (2020); Wang and Wang (2020); Wang et al. (2015) to allow assessment of how well the models can distinguish between normal and malicious traffic based on predefined statistical features. Additionally, Hybrid models (Banitalebi and Mohammadreza, 2020) based Machine learning and Statistical method have also utilize Accuracy, Specificity, Sensitivity, TPR and Recall as metric of evaluation.

In light of the foregoing, Accuracy, Specificity, Sensitivity, TPR and Recall appears to be metrics that are applicable to different kind models for DDOS Attack detection in SDN.

Machine learning, Neural network and Statistical based model have different effect on these metrics. The study of Ahuja et al. (2021); Santos et al. (2020); Wang et al. (2022) had applied different models for detection of DDOS attacks. Each models have a varying performance in terms Accuracy, Specificity, Sensitivity, TPR and Recall. Additionally, these models could also be optimized to improve results of these metrics positively through the following:

i *Feature Engineering*: Selecting and transforming relevant features can enhance the model's ability to distinguish between classes, which can lead to improved Specificity, Sensitivity, TPR, Recall and ultimately, a higher Accuracy. This Can be related to the work of Ahuja et al. (2021); Mansoor et al. (2023), which generated their feature dataset, the work of Mansoor et al. (2023) with Sayed et al. (2022) who adopted feature selection methods. The result of these studies shows a superior performance for some of these metrics compared to other existing studies.

ii *Hyper parameter optimization*: Authors in Sahoo et al. (2020) optimized hyper parameters of SVM and consequently achieved a better Accuracy than the single SVM Model parameter. Hence, optimizing model parameters can improve the Specificity, Sensitivity, TPR, Recall and Accuracy.

iii *Architecture Design*: Designing deep learning architectures tailored for DDoS detection, considering the unique characteristics of attack traffic, can improve model performance as can be seen in the study of Mousa et al. (2023) which presented an in-depth hidden layers in their proposed deep learning-based architecture to improve Accuracy.

a. *Limitation/Challenges of using the performance analysis metrics*

iv ***Imbalanced Datasets and Misleading Results***: Metrics in this category are sensitive to imbalance dataset. For instance, the Accuracy can be misleading in the case of imbalance Dataset (Mansoor et al., 2023) probably due to the dominance of the majority class (normal traffic), leading to a false sense of high performance. In other words, a model may achieve high accuracy by predominantly predicting the majority class, overlooking the minority class (attacks) and yielding misleading results.

v ***Insensitive to False Positives and Negatives***: Mtericts like Accuracy treats false positives and false negatives equally, which might not reflect the real-world impact accurately. In DDoS detection, false positives (flagging normal traffic as an attack) and false negatives (missing real attacks) have different implications, but accuracy does not consider this distinction. Studies like (Sun 2019) used Accuracy as the primary metrics of evaluation. However, focusing on accuracy alone might overlook the significance of false negatives and false positives. Hence, the metric should be used alongside other metrics of evaluation.

6.1.2. Error/misclassification analysis

The Misclassification analysis metrics focus on understanding and assessing the errors made by a classification model. In the context of DDoS attack detection in SDN, these metrics help analyze how the model classifies network traffic and identify cases where the model may misclassify normal traffic as an attack (false positive) or miss actual attacks (false negative). The key misclassification analysis metric used in the reviewed literatures include: False positive rate. False alarm rate, False Negative Rate, Precision and F1 score. Among the reviewed literatures,15 authors used Fscore/Fmeasure, 14 Authors used Precision, 11 Authors used FPR, 6 Authors used FAR while 2 utilized FNR for error /misclassifications analysis corresponding to 43 %, 40 %, 31 %, 17 % 6 % of the authors respectively.

a) *Relationship with attack characteristics*: The intensity or combination of attacks in a dataset has significant influence on the values of the error/misclassification analysis metrics. For instances studies with low-rate attacks have high false positives rates (Kalkan et al., 2018) which have significant influence on the Precision. Low-rate attacks have tendencies to behave like normal traffic thereby increasing the rate of False Positive and consequently influencing the precision of detection. This is because there is an inverse relationship between False positive and precision; as False positive increases the precision decreases and vise versa. This characteristic is similar to False Alarm rate, therefore FAR and TPR can be used interchangeably. Reducing false positives is crucial to maintaining a high precision, especially in applications like DDoS attack detection where accurately identifying true positive cases (actual DDoS attacks) is of utmost importance to avoid unnecessary network disruptions or resource allocations.

F1score Provides a balance between precision and recall. If the increase in recall due to volumetric attacks is not matched by a corresponding increase in precision, the F1 score could decrease. Achieving a higher F1 score often requires optimizing both precision and recall simultaneously. Hence studies in (Ahuja et al., 2021) which had different proportion of attack and normal traffic used f1score for evaluation to allow a balance of effective detection of varying forms of attacks. FNR on the hand was found to have increased with increasing rate of low volume attack in the work of Sahoo (2018).

a) *Relationship with Detection model*: The error /misclassification metrics have been applied by various Machine learning, Statistical and Neural network model to assess the error made by the models. The type model has significant influence on the value of error/misclassification metrics. This can be seen in the work of (Ali et al., 2023) where different deep learning and Machine learning based models were applied for detection and each holds a varying results for precision, F1score. FNR, and FPR. However, the values for these metrics can be optimized through the following:

i *Improve the quantity and Quality of Dataset:* Applying large number of dataset instances which has a combination of normal and malicious traffic can improve the value of precision, FNR, FPR and F1 Score. This can be seen in studies of Elubeyd and Yiltas-Kaplan (2023; Ali et al. (2023) who used large datasets to test theirs models.

ii *Feature Selection*: Selecting the required features can lead to improved precision, reduce FNR, FPR and ultimately, improved the F1 score. This can be related to work of Alubaidan et al. (2023); Mansoor et al (2023) who adopted feature selection methods to improve the effectiveness of their model.

iii *Hyper parameter optimization*: hyper parameters can optimize the trade-off between precision and recall, thus improving the F1 score. Some algorithms might be biased towards precision or recall; tuning helps find the right balance. Authors in Sahoo et al. (2020) optimized hyper parameters of SVM and consequently achieved a better precision than the single SVM Model.

iv *Employ Hybridization*: Models were combined by authors in Ahuja et al. (2021); Sahoo et al. (2020); Elubeyd and Yiltas-Kaplan (2023) and the result shows a reduced false positive rate, improve precision and F1 score compared to other models in the various studies.

b) *Limitation of Error/Misclassification metrics*

Metrics that fall under this category also have challenges and limitation which impedes in their resultant values. This includes*:*

i *Sensitive to Class Imbalance:* One class is higher than the other, there is tendency that the majority class will get predicted more frequently there by missing the minority class thereby increasing FNR, FPR and reducing Fscore and precision for the minority class.

ii *Doesn't Capture True Positive Distribution*: Precision, and F1 score do not provide information about how well the model is capturing the distribution of true positives across different subsets of the data.

iii *Sensitivity to Outliers and Extreme Cases*: FPR, FNR, Precision, and the F1 score are sensitive to outliers or extreme cases, especially in small datasets or when dealing with rare events.

iv *Single point evaluation:* These metrics only provide evaluation of the error or misclassification of the detection model, however the DDOS attacks vary in intensity, hence a single evaluation may not capture this variation.

6.1.3. Comprehensive assessment metrics

The metrics under this category includes: ROC-AUC (Receiver Operating Characteristic - Area Under the Curve and Detection Rate (DR). Among the studied authors,6 utilized ROC while 8 used DR as metrics of evaluation corresponding to 17 % and 23 % of authors respectively.

a) *Relationship with Attack characteristics* High attack traffic has influence on the detection rate. The detection rate was found to be higher when the attack traffic was high in Aladaileh et al. (2023) .The ROC is the ratio of Sensitivity and Specificity. Hence, the impact of traffic on Sensitivity and Specificity will also affect the ROC curve.

b) *Relationship with Detection models*: Machine Learning and Statistical based approaches used ROC and DR as important metrics of evaluation. A entropy based approached was applied in in Aladaileh et al. (2023) to improve detection rate of high and low attacks in SDN. Machine learning based approach was applied in Santos and Moreno (2019) and ROC was found to be reasonable. Detection rate could be improved through combination of two or more models as done in Zhou (2023).

c) *Limitation/Challenges.* ROC -AUC and DR like other metrics are also sensitive to imbalance data with tendency to provide misleading results. The ROC curve assumes equal misclassification for FPR and FNR. For a detection system against DDOS attacks, ignoring false negative can have severe consequences than FPR.DR on the hand, is insensitive to True negative and a False Positive and therefor doesn't provide a complete picture of the model's performance

From 6.1.1 - 6.1.3, we can say that, considering performance analysis metrics alongside error/misclassification and Comprehensive assessment metrics is essential in order ensure a comprehensive evaluation of a model's performance.

6.2. Detection system metrics

The spread on the usage of the detection system metric is depicted in Fig. 6.3. CPU Utilization makes up 78 % of the metrics used in evaluating the performance of the Detection System while the remaining 22 % used Network load.

6.2.1. CPU utilization

Authors have used CPU utilization to measure the performance of the detection system by comparing the over the SDN Controller is causing on the system during attack. CPU Utilization could be that of the SDN Controller or of the SDN Switch.

Phan et al. (2016) utilized the CPU usage of SDN Controller to evaluate the average CPU Consumption of the proposed detection approach termed OpenFlowSIA. The CPU resources consumption was found to have reduced when the proposed OpenFlowSIA was implemented compared with the other detection approaches. The CPU Usage of the SDN Switch was also evaluated based on the number of flows which was found to have reduced when the proposed OpenFlowSIA was triggered. However, the CPU Consumption was still similar to other test cases used because the approach has an Idle-timeout adjustment module which kept the Switch Busy. In the work of Ujjan et al. (2020) the CPU Utilization and network load of two sampling techniques used in the deep learning detection approach were compared. The CPU utilization using the sflow sampling technique was observed to have reduced from 90 % to 51 % where as the CPU utilization using the Adaptive sampling, the CPU utilization increased to 78 %. Similarly. CPU usage of Native Openflow Switch and sflow based approach was compared in Giotis et al. (2014) and it was observed that, there was a significant decrease in the CPU usage of the OpenFlow Controller and switches through the sFlow-based approach.

Sun et al. (2019) monitored the CPU utilization to ascertain the overhead incurred on the CPU by the detection approach. While in a detection scheme termed FADM in Hu et al. (2017) evaluated overhead by estimating the average utilization of the Controller since the FADM system is running on the Controller. During an attack, it was discovered that, the CPU Utilization was high, however, when the mitigation module of FADM was activated, the CPU utilization was reduced and later return to normal.

The work of Cui et al. (2016) introduced a detection mechanism that

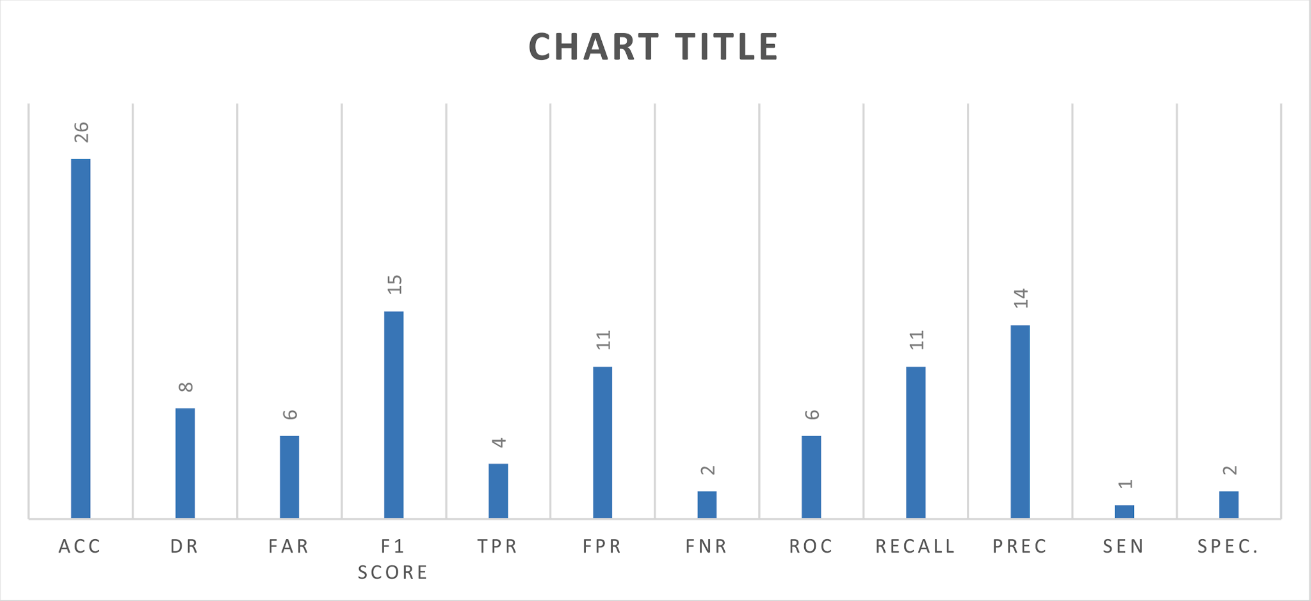


Fig. 6.3. Spread on the usage detection system metric.

Table 7
Research problems and strength of the existing DDOS detection techniques.

SN	Ref	Method	Security by SDN/for SDN	Strength	Shortfall/weakness
1	Fouladi et al. (2020)	Time Series Analysis/	By SDN	Detect instant change in network to protect the availability for cloud servers against security threats. -Solve the problem constant thresholding problem of statistical based detection techniques. High detection rate and low false alarm	Simulation was carried out with multiple switches. Considers only two features vector. hence, other feature to could aid detection of other forms of attacks was not used
2	Gurusamy et al. (2018)	-Secure Flow Management Model	For SDN	– Secure control plane bandwidth from DDOS attacks – Applied multi controllers in the test bed hence it with stand load Implemented both detection and mitigation to ensure controller recovery -Considers both interdomain and intra domain attack	Considers Volumetric attacks. such as UDP Flooding which attacks controller Bandwidth only
3	Santos et al., 2019	Random Forest, Decision tree, SVM, MLP	For SDN	Applied four Machine Learning techniques (Random Forests, Decision tree, Support Vector Machine, MLP) to classify DDOS to secure the controller as single point of failure from DDOS attacks. Decision tree performance better in times of efficiency while Random Forest has highest Accuracy and were better than the rest. -DT and RF can choose the best parameters for the classification process	Even though RF has high accuracy it has high processing time and time is crucial in the context of DDOS attacks. Cannot detect new type of attacks since implementation of the Algorithms was not done online. – Only three types of attack were considered: Bandwidth, Controller and Flow table attack. – Accuracy for detecting controller attack is low due to equal distribution of training database
4	Ye et al., 2018	Support vector machine	For SDN	– Combined a six-tuple feature vector with SVM to detect DDOS attacks. – SVM Used small amount flows	The legitimate traffic used for the simulation was not comprehensive enough. No mitigation measures put in place
5	Cui et al., 2019	Support vector Machine with cognitive inspired computing and dual address entropy	For SDN	-Achieved early detection of DDOS attack and timely recovery of network after detection	Two features were considered and may easily result in misjudgment The recovery algorithm is not efficient
6	Bawany and Shamsi (2019)	Adaptive filter based on estimated weighted moving average (EWMA) filter	By SDN	– protect Smart city application, control plane and data plane from DDOS attack – Achieved load balancing and could be implemented in real time	-Optimization of filters may be requires ensuring its effectiveness in another domain
7	Nam et al. (2018)	Distributed Self organizing Map	For SDN	– Used SOM to detect flooding attacks – Achieve other controller issues such as performance, load balancing	Experiment was conducted on a small topology
8	Kokila et al. (2014)	SVM	For SDN	SVM algorithm was used in the scheme for DDoS attack detection, The rate of detection was high with a low false positive rate	The measures adopted for defense and recovery after attack detection was not taken into consideration The training and creation of the detection model, which is used to predict traffic statistics, takes longer with SVM.
9	Wang et al. (2015)	Entropy	For SDN	Achieved a distributed anomaly detection in SDN and reduces the flow collection overload to the controller.	Used only one features which may lead to misjudgment easily -Detection function was embedded in the switch could lots of inconveniences
10	Mousavi et al. (2018)	Entropy	For SDN	Within the first 500 packets of the attack traffic, the detection methods were able to detect a DDoS attack	Measure that will ensure recovery from attack was not in place
11	Niyaz et al. (2017)	Deep learning/SAE	For SDN	Achieved real time DDOS attack detection	Deep learning requires large training sample and takes long time to training
12	Kalkan et al. (2017)	Hybrid mechanism (Flow based detection and Packet based detection	For SDN	The detection scheme could realize effective defense and filter out abnormal packets after checking attacks.	Most of the modules were embedded into the OpenFlow switch. Despite the fact that, the Switch and Controller's communication overhead could be minimized, measures against future attacks was not put in place. SDN testbed was not used to carry out experiments
13	(Sahoo, 2018)	Information distance and Entropy	By SDN	This method set a specific packet window size, combined generalized entropy with information distance, and periodically monitored the traffic. As a result, it was able to identify an attack at the start of a DDoS attack	Although it could detect attacks quickly, and the optimal threshold of generalized entropy was difficult to set
14	Phan et al. (2016)	SVM	SDN	It employed the IA algorithm and cogent policies to effectively safeguard networks from resource exhaustion brought on by flooding attacks. The protection method made use of SVM's classification advantages of high accuracy and quick processing.	Does not support multiple attacks detection

(continued on next page)

Table 7 (*continued*)

SN	Ref	Method	Security by SDN/for SDN	Strength	Shortfall/weakness
15	Giotis et al. (2014)	Entropy	SDN	In high traffic networks, the suggested mechanism may reliably identify network anomalies while decreasing false positive rates. The mechanism's implementation was designed to function effectively, managing real-time traffic 10 times greater than that encountered by the related work.	Cannot detect attack near the source
16	Oo et al. (2017)	Advanced SVM	For SDN	When compared to the SVM method, the proposed Advance SVM can dramatically cut both the testing and training times.	The Proposed system was not implemented on SDN Environment
17	Lawal and At, (2018)	Sflow management technology	SDN	- Present real time detection and mitigation of DDOS attacks - The technology is scalable, flexible and easy to deploy	Using Sflow might overload CPU and has limited device support which means each router or switch needs to support sflow. Only ICMP flooding attack was generated
18	(Kalkan et al., 2018)	Joint Entropy	For SDN	The detection scheme is effective against both known and unknown attacks efficiently. Can detect multiple attacks	Due to the necessity of sending packet headers through the switch to the controller, the switch has memory overhead and the control channel between the switch and controller experiences traffic overhead.
19	Conti and Gangwal (2019)	Cumulative Sum CUSUM	SDN	Detects DDOS attack within a short time and can detect different DDOS attacks	The controller utilized the commonly exchanged messages to obtain real time traffic statistic thereby leading to some amount of overhead on the CPU
20	Meti et al. (2017)	SVM, NB, Neural network	SDN	Detects DDOS attacks by classifying incoming requests. SVM Performed better than the other two	Only three algorithms were considered
21	Sahoo et al. (2020)	SVM with Kernel principal component analysis	SDN	Used SVM Model which used KPCA for reducing the dimension of feature vectors, and Genetic Algorithm to optimize the parameters of SVM. -The Model reduced training time and testing	Even while the model does well in a single controller environment for attack traffic detection, it might not be able to distinguish attack traffic in a multi-controller context.
22	Sun (2019)	BiLSTM-RNN	For SDN	The technique has the benefits of thoroughly extracting and evaluating the important aspects of the traffic under the SDN architecture and lowering network overhead by establishing a threshold.	Specifically designed to protect the controller alone
23	Cui et al. (2016)	Neural network/BPNN	For SDN	The detection approach can respond more quickly against DDoS attack and reduce the workload of controllers and switches The detection model can also trace back the attack source	The version OpenFlow used to test is old, thus using other higher or lower version might result in performance differences
24	Yu et al. (2021)	Entropy and Ensemble learning	For SDN	Effective DDoS attack detection is possible with this technique, which also lessens controller workload, southbound communication overhead, and attack detection time. Reduces CPU utilization of the Controller	Only two DDOS attack method was simulated and may not be a good generalization for other DDOS attacks
25	Alshamrani (2017)	Best selected subset features and Sequential Minimal Optimization (SMO)	For SDN	Developed a feature selection Algorithm, which aid selection of effective features and provided detection with high Accuracy. Considered Misbehavior and New flow Attacks.	Cannot detect unknown traffic. Small network topology was used for the simulation
26	Liu et al. (2017)	SVM	For SDN	Resolved IP Spoofing issue through Dynamic IP address Can detect and mitigate DDOS attack in SDN effectively	Only ICMP attack was generated fir the simulation hence, may not be applicable to other DDOS attacks
27	Zhijun et al. (2020)	Factorization method	For SDN	The FM algorithm was able to achieve fine-grained detection of Low rate DDOS attack targeting SDN layer	The FM Algorithm requires large number of training sample. The proposed algorithm was not implemented on SDN Environment.
28	Ali et al. (2020)	Time and space-based detection solution	For SDN	Because the stream of packet headers was processed on the fly without requiring a significant amount of capacity for data storage and processing, the Approach uses less computational resources, takes up less space, and does not require any specialized equipment.	Threshold values in relation with the number of hosts need to be investigated and improved. The implementation was on MATLAB not SDN Environment
29	Sumantra and Gandhi, (2020)	Shannon entropy	For SDN	With this method, attacks were quickly detected, genuine requests were delayed while an attacker was present, and total CPU usage was low.	Only a single victim was considered. It needs to scale to multiple victims
30	Omar et al. (2019)	Entropy	For SDN	Achieved detection within 3 to 10 seconds of attack	The threshold needs to be adjusted to avoid false positive detection in real scenario
31	Phan and Park (2019)	SVM and SOM	By SDN	Achieved good classification using the advantages of SVM and SOM. The overall scheme has high performance and low CPU Usage due to detection and mitigation	It is necessary to improve the packet in process in the proposed technique that identifies malicious packets in messages from the data plane and optimizes bandwidth usage in the secure communication channel.
33	Wang and Liu (2020)	Entropy and CNN	For SDN	Achieved packet-based detection through entropy and fine-grained detection using CNN. It distinguishes normal from abnormal traffic	The training time was a bit high

(*continued on next page*)

Table 7 (*continued*)

SN	Ref	Method	Security by SDN/for SDN	Strength	Shortfall/weakness
34	Ahuja et al., 2021	SVM-RF	For SDN	The scheme can distinguish flash crowd – Generate data set from SDN Emulated Environment. – Achieved good classification Accuracy	– Data set generated used only three DDOS traffic which may not provide a good generalization for DDOS attacks – Dataset was emulated and not generated in real time

Table 8
DDOS data set source.

SN	Reference	Dataset	URL	Size of traffic/no of instances	tools
1	Fouladi et al. (2020)	Mawi working group traffic Archive	http://mawi.wide.ad.jp/mawi	1.1GB	TCP Replay, Mininet, POX Controller
2	Cui et al. (2019)	CAIDA UCSD “DDoS Attack 2007" Dataset,	http://www.caida.org/data/passive/ddos20070804dataset.xml	7000	Distributed Internet Traffic Generator, Scapy tool, Mininet. Floodlight controller
3	Bawany and Shamsi, (2019)	ISCX Dataset	ISCX Datasets. http://www.unb.ca/research/iscx/dataset/iscx-IDS-dataset.html	1000packets	ONOX
4	Assis et al. (2020)	CicDDOS 2019	https://www.unb.ca/cic/datasets/ddos-2019.html	-	Mininet, Floodlight
5	Manso et al. (2019)	CAIDA Dataset 2019	(https://www.caida.org/home/	2,520,000packet/m	Mininet, RYU controller
6	Sahoo et al. (2020)	New Dataset NSL-KDD Dataset	https://www.researchgate.net/publication/292967044_ Dataset-_Detecting_Distributed_Denial_of_Service_ Attacks_Using_Data_Mining_Techniques https://www.unb.ca/cic/datasets/nsl.html	2160,668 records/27 features 108,400 records 41 features	POX Controller Sflow RT
7	Ahuja et al. (2021)	SDN Dataset	https://data.mendeley.com/datasets/jxpfjc64kr/1	1,04,345 23 features	Ryu controller

reduces overhead by the Controller and SDN Switch by detecting attack as quickly as possible as well as block the attack port. Hence, metrics like CPU Utilization were adopted to check performance. The result shows a minimal utilization. Other detection techniques such as Yu et al. (2021), and Liu et al. (2018) have used CPU utilization. In Liu et al. (2018), the authors proposed to detect amplification attacks and used CPU utilization to examine the performance of Controller since the it has to collect features from the Switch.

In Yu et al. (2021) a detection module based on Entropy and Ensemble learning was deigned on the Switch edge and Controller respectively. The study utilized the idle time computing capability of the switch to offload detection task from Controller to Switch. Consequently, CPU Utilization was utilized to monitor overhead of Controller on the CPU.

6.2.2. *Network load*

The Network load was used as metrics by the Ujjan et al., 2020 to estimate the amount kilobyte received by the Controller per second during the Sflow and adaptive polling-based sampling method. The result shows the network load was higher when the adaptive polling-based sampling method was used than the Sflow sampling method. Similarly in Cui et al. (2016), the network load metric was used to measure the performance of detection approach using the Packet_in trigger and periodic trigger. The network load during the Packet_in trigger appears to be lower than the periodic trigger.

Relationship with Attack Characteristics and Detection Models

From 6.2.1 to 6.2.2 above, it appears that the intensity of attacks has significant influence on the CPU utilization and network load (Phan et al.,2016) as well as the detection approaches However, this can be reduced by adopting measures such as selecting the relevant features (Mansoor et al., 2023) reducing the dimensionality of data (Sahoo et al, 2020) and nature of detection model proposed.

7. Issues/research challenges

In this section this study reviewed about 33 articles that focused on DDOS attack detection to ascertain their strength and some of their weaknesses as depicted in Table 7. While some are to protect the SDN architecture alone others evolve a technique to protect the Architecture to secure a domain such as IOT or Cloud. From the table, Entropy and Machine learning techniques are the most technique used for detection. Most of the detection techniques were implemented offline Santos et al. (2019) and hence may not be able to detect new attacks. While some techniques were not implemented on SDN environment some were implemented on a small network topology.

8. DDOS dataset

This section presents repository of datasets used by the literature to validate the detection approaches as shown in Table 8. Most of the research papers could not make available the sources of their dataset while some complained about lack of comprehensive dataset with Benign and Malicious traffic to test their proposed model. This resulted in some work adopting two different datasets for their experiments. Some of the Dataset seems to be obsolete, and were collected for traditional network. Hence, there is need to get new recent dataset for the SDN based network in order to evaluate the newly proposed intrusion detection systems. Taking into cognizance the advancement of technology and growth of DDOS attacks.

9. Summary of challenges /conclusion/future work

DDOS attack is growing in stealth and sophistication which poses a Security challenge to the Architecture of Software defined network. This review has presented a background on SDN and DDOS attacks, and some of the security vulnerabilities that leads to DDOS attacks in Software defined network. Various DDOS detection techniques have been presented which aimed to address DDOS security concerns in Software defined network. This work also studied the features used by various DDOS protection/detection scheme to ascertain the DDOS attack features that could aid its detection. Furthermore, a synthesis of Parameters for Performance Evaluation of the detection techniques was presented, as well as a repository of Dataset and tools used by the Authors to test their detection approaches.

From all articles reviewed, the following summarizes some of the challenges of detection and mitigation techniques and Possible future directions.

- **Controller Load Balancing**: Most studies have used single controller to validate the approaches in a simulated environment such as Bawany and Shamsi (2019); Cui et al. (2019); Phan and Park (2019), however this may leads to single point failure. Therefore, adopting a multiple controller to distribute the load could be a possible solution to achieve Controller load balancing during DDOS attacks.
- **Detecting Zero Day attack**: The detection approached where not implemented online such as Santos et al. (2019). Hence, the technique may not be able to detect new attacks.
- **Actual testbed for Simulation**: Several DDOS attack detection technique have used either Simulation or Emulation to validate their detection approaches Mousavi and St-Hilaire (2018), Cui et al. (2019), Bawany and Shams (2019) and may not depict the actual implementation in real life as some used Simulated SDN Environment under Virtual Host machine with minimal resources. In other words, small topology was used to validate and may not represent the internet resources with high bandwidth of which DDOS attacks are launched. hence, there is need have a research work with real test bed on large network topology to demonstrate and validate the detection approaches.
- **Standard Dataset**: Most of the articles reviewed namely: Sahoo et al. (2020); Manso et al. (2019), have used traditional and publicly available dataset such as KDDCUP99 Dataset, CAIDA 2007 dataset., DARPA Dataset. This dataset seems to be out of date to be used for detection of attacks in SDN Environment. This is because, the features used in the datasets are designed for traditional network and may not fit perfectly in SDN based network. Authors in Ye et al. (2018), Oo et al. (2019) have generated their Dataset to implement their detection approaches, however, the Dataset used is not publicly available for further validation. Ahuja et al. (2021) generated an SDN based dataset and made it publicly available. However, only three forms of attacks were launched during the dataset creation process. Considering the increase in sophistication and stealth of the DDOS attack techniques, there is need to generate a more comprehensive SDN based dataset using Different forms of attacks. Generally, availability of DDOS dataset for SDN is limited.
- **Collecting traffic Statistics**: Most of the DDOS attack detection approaches such as Cui et al. (2016); Hu et al. (2017) used the traditional Open flow to collect traffic features for implementation their detection approaches. However, using open flow to collect traffic statistic on large network may lead the data plane overhead. Meanwhile, in case of high rate DDOS the controller-data bandwidth will be exhausted, connection between switch could be broken and controller may not respond to request in in a timely manner (Phan et al., 2016). Flow management mechanism have been used as alternative; however, it cannot gather all the details about a packet. Consequently, there is need for method to collect traffic statistics without causing any overhead on the SDN Architecture.
- **Thresholding and feature selection:** The two most used techniques include Machine learning and Statistical analysis-based approaches. While the Statistical analysis technique such as Entropy have been used in detection of DDOS attacks Cui et al. (2016); Li and Wu (2020); Yu et al, (2021); Liu et al. (2017). However, computing the required threshold is still a challenge, as thresh-holding is critical and has effect on the attack detection (Banitalebi and Mohammadreza, 2020). Machine learning approaches have also proven to be one of the most effective as supervised learning Technique of Machine learning have the ability to detect unknown attacks and have be effectively used by authors in Santos et al . (2019); Sahoo et al. (2020); Ye et al. (2018); Meti et al. (2017) Hu et al. (2017), However, selecting the best features for DDOS detection is still a challenge.

In conclusion, Statistical based approach and Machine learning seems to be promising in the detection of DDOS attacks. However, this study recommends Machine learning technique for DDOS attack detection because, DDOS attack is growing in sophistication and Supervised Machine learning technique have the capability to detect unknown attacks, automation with little human intervention is possible and have been applied by researchers with high detection accuracy. Additionally, while choosing the Evaluation metrics, attention should be paid to the nature of the dataset and models in use. Also, using single evaluation metrics should be avoided in order to ensure the generalization capability of the detection strategy.

Hence, as part of future work, more work shall be done in DDOS detection and Mitigation techniques using Machine Learning Algorithms.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Ahuja, N., Singal, G., Mukhopadhyay, D., Kumar, N., 2021. Journal of network and computer applications automated DDOS attack detection in software defined networking. J. Netw. Comput. Appl. 187 (November 2020), 103108 https://doi.org/10.1016/j.jnca.2021.103108.

Al-duwairi, B., Al-quraan, E., Abdelqader, Y., 2020. ISDSDN: mitigating SYN flood attacks in software defined. J. Netw. Syst. Manag., 0123456789 https://doi.org/10.1007/s10922-020-09540-1.

Aladaileh, M.A., Anbar, M., Hintaw, A.J., Hasbullah, I.H., Bahashwan, A.A., Al-Sarawi, S, 2022. Renyi joint entropy-based dynamic threshold approach to detect DDoS attacks against SDN controller with various traffic rates. *Appl. Sci.* (*Switzerl.)* 12 (12). https://doi.org/10.3390/app12126127.

Aladaileh, M.A., Anbar, M., Hintaw, A.J., Hasbullah, I.H., Bahashwan, A.A., Al-Amiedy, T.A., Ibrahim, D.R., 2023. Effectiveness of an entropy-based approach for detecting low- and high-rate DDoS attacks against the SDN controller: experimental analysis. *Appl. Sci.* (*Switzerl.)* 13 (2). https://doi.org/10.3390/app13020775.

Alfa, A.A., Alhassan, J.K., Olaniyi, O.M., Olalere, M., 2020. Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions. J. Reliab. Intelli. Environ. https://doi.org/10.1007/s40860-020-00116-z.

Ali, S., Alvi, M.K., Faizullah, S., Khan, M.A., Alshanqiti, A., Khan, I., 2020. Detecting DDoS Attack on SDN Due to Vulnerabilities in OpenFlow.

Ali, T.E., Chong, Y.W., Manickam, S., 2023. Comparison of ML/DL approaches for detecting DDoS attacks in SDN. *Appl. Sci.* (*Switzerl.)* 13 (5). https://doi.org/10.3390/app13053033.

Alshamrani, A., 2017. A Defense System for Defeating DDoS Attacks in SDN based Networks, pp. 83–92.

Altay, L., 2018. *JESS: Joint Entropy Based DDoS Defense Scheme in SDN. 8716* (c), pp. 1–15. https://doi.org/10.1109/JSAC.2018.2869997.

Alubaidan, H., Alzaher, R., AlQhatani, M., Mohammed, R., 2023. DDoS detection in software-defined network (SDN) using machine learning. Int. J. Cybernet. Inform. 12 (04), 93–104. https://doi.org/10.5121/ijci.2023.120408.

Assis, M.V.O.De, Carvalho, L.F., Rodrigues, J.J.P.C., Lloret, J., Proença, M.L, 2020. Near real-time security system applied to SDN environments in IoT networks using convolutional neural network R. Comput. Electr. Eng. 86, 106738 https://doi.org/10.1016/j.compeleceng.2020.106738.

Banitalebi, A., Mohammadreza, D., 2020. The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing* (Issue 0123456789). Springer US. https://doi.org/10.1007/s11227-020-03323-w.

Bawany, N.Z., Shamsi, J.A., 2019. Journal of Network and Computer Applications SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. J. Netw. Comput. Appl. 145 (April), 102381 https://doi.org/10.1016/j.jnca.2019.06.001.

Bawany, N.Z., Shamsi, J.A., Salah, K., 2017. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arab. J. Sci. Eng. 42 (2), 425–441. https://doi.org/10.1007/s13369-017-2414-5.

Bensalah, F., EL, KAMOUN, El, M.-A., 2019. Inline detection of Denial of Service Attacks in Software Defined Networking using the Hotelling Chart. Procedia Computer Science 160, 785–790. https://doi.org/10.1016/j.procs.2019.11.010.

Benzekki, K., El Fergougui, A., Elbelrhiti Elalaoui, A., 2016. Software-defined networking (SDN): a survey. Secur. Commun. Netw. 9 (18), 5803–5833. https://doi.org/10.1002/sec.1737.

Bhayo, J., Shah, S.A., Hameed, S., Ahmed, A., Nasir, J., Draheim, D., 2023. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. Eng. Appl. Artif. Intell. 123 (April), 106432 https://doi.org/10.1016/j.engappai.2023.106432.

Bose, A., Aujla, G.S., Singh, M., Member, S., Kumar, N., Member, S., Cao, H., 2019. Blockchain as a Service for Software Defined Networks : A Denial of Service Attack Perspective. 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 901–906. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00166.

Cabaj, K., Wytrębowicz, J., Kukliński, S., Radziszewski, P., Dinh, K.T., 2014. SDN Architecture Impact on Network Security. In: Position Papers of the 2014 Federated Conference on Computer Science and Information Systems, 3, pp. 143–148. https://doi.org/10.15439/2014F473.

Conti, M., Gangwal, A., 2019. *A Comprehensive and Effective Mechanism for DDoS Detection in SDN. October 2017*. https://doi.org/10.1109/WiMOB.2017.8115796.

Conti, M., Lal, C.. Lightweight solutions to counter DDoS attacks in software defined networking. *Wireless Networks, 0123456789*. https://doi.org/10.1007/s11276-019-01991-y.

Conti, M., Lal, C., 2019. Lightweight solutions to counter DDoS attacks in software defined networking. Wirel. Netw., 0123456789 https://doi.org/10.1007/s11276-019-01991-y.

Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., Zheng, X., 2016. Author ' s accepted manuscript SD-Anti-DDoS: fast and efficient DDoS defense in software-defined networks reference. J. Netw. Comput. Appl. https://doi.org/10.1016/j.jnca.2016.04.005.

Cui, J., He, J., Xu, Y., Zhong, H., 2018. *TDDAD: Time-Based Detection and Defense Scheme Against DDoS Attack on SDN Controller* (Vol. 2). Springer International Publishing. https://doi.org/10.1007/978-3-319-93638-3.

Cui, J., Wang, M., Luo, Y., Zhong, H., 2019. DDoS detection and defense mechanism based on cognitive-inspired computing in SDN. Fut. Gener. Comput. Syst. https://doi.org/10.1016/j.future.2019.02.037.

Dayal, N., Maity, P., Srivastava, S., Khondoker, R., 2016. Research trends in security and DDoS in SDN. Secur. Commun. Netw. 9 (18), 6386–6411. https://doi.org/10.1002/sec.1759.

Dayal, N. (2017). *Analyzing Behavior of DDoS Attacks to Identify DDoS Detection Features in SDN*. 274–281.

Dharmadhikari, C., Kulkarni, S., Temkar, S., Bendale, S., 2019. A Study of DDoS Attacks in Software Defined Networks, pp. 448–453.

Dong, S., Abbas, K., Jain, R., 2019. A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access 7, 80813–80828. https://doi.org/10.1109/ACCESS.2019.2922196.

Elubeyd, H., Yiltas-Kaplan, D., 2023. Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. *Appl. Sci.* (*Switzerl.)* 13 (6). https://doi.org/10.3390/app13063828.

Fajar, A.P., Purboyo, T.W., 2018. *A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN)*, 13, pp. 476–482.

Fouladi, R.F., Ermiş, O., Anarim, E., 2020. Journal of Information Security and Applications A DDoS attack detection and defense scheme using time-series analysis for SDN. J. Inform. Secur. Applic. 54 (August), 102587 https://doi.org/10.1016/j.jisa.2020.102587.

Gao, D., Liu, Z., Liu, Y., Heng, C., Ting, F., Chao, Z.H., 2018. Defending against Packet-In messages flooding attack under SDN context. Soft Comput. https://doi.org/10.1007/s00500-018-3407-3.

Gebremeskel, T.G., Gemeda, K.A., Krishna, T.G., Ramulu, P.J., 2023. DDoS Attack detection and classification using hybrid model for multicontroller SDN. Wirel. Commun. Mob. Comput. 2023, 1–18. https://doi.org/10.1155/2023/9965945.

Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., Maglaris, V., 2014. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Computer Networks. https://doi.org/10.1016/j.bjp.2013.10.014.

Gong, Y., Huang, W., Wang, W., Lei, Y., 2015. A survey on software defined networking and its applications. Front. Comput. Sci. 9 (6), 827–845. https://doi.org/10.1007/s11704-015-3448-z.

Gong, C., Yu, D., Li, X., & Li, X. (2019). *An intelligent trust model for hybrid DDoS detection in software defined networks. March*, 1–16. https://doi.org/10.1002/cpe.5264.

Gupta, K.B.B.B., 2018. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN) -based cloud computing environment. J. Amb. Intell. Human. Comput. 0 (0), 0. https://doi.org/10.1007/s12652-018-0800-9.

Gurusamy, U., Msk, M., 2019. *Detection and Mitigation of UDP Flooding Attack in a Multicontroller Software Defined Network Using Secure Flow Management Model. April*, pp. 1–11. https://doi.org/10.1002/cpe.5326.

Hafizah, S., Ariffin, S., Muazzah, N., Latiff, A., Khairi, M.H.H., Ariffin, S.H.S., Latiff, N.M.A., Abdullah, A.S., Hassan, M.K., 2018. A review of anomaly detection techniques and distributed denial of service (DDoS) on software defined network (SDN). Technol. Appl. Sci. Res. 8 (2), 2724–2730. https://www.researchgate.net/publication/324830666.

Haider, S., Akhunzada, A., Mustafa, I., Patel, T.B., Fernandez, A., Choo, K.R., Member, S., Iqbal, J., 2020. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access 8, 53972–53983. https://doi.org/10.1109/ACCESS.2020.2976908.

Hu, D., Hong, P., Chen, Y., 2017. FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking.

Joëlle, M.M., Park, Y.H., 2018. Strategies for detecting and mitigating DDoS attacks in SDN: A survey. Journal of Intelligent & Fuzzy Systems 35 (6), 5913–5925.

Kalkan, K., Gur, G., Alagoz, F., 2017. Defense mechanisms against DDoS attacks in SDN environment. IEEE Communications Magazine 55 (9), 175–179.

Kalkan, K., Giir, G., Alagoz, F., 2017. SDNScore: A Statistical Defense Mechanism Against DDoS Attacks in SDN Environment.

Kalkan, K., Altay, L., Gür, G., Alagoz, F., 2018. JESS: Joint Entropy Based DDoS Defense Scheme in SDN. IEEE Journal on Selected Areas in Communications PP,, 1. https://doi.org/10.1109/JSAC.2018.2869997.

Karan, B.V., Narayan, D.G., Hiremath, P.S., 2018. Detection of DDoS attacks in software defined networks. In: Proceedings 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions, CSITSS 2018.

Kaur, G., Gupta, P., 2019. Hybrid approach for detecting ddos attacks in software defined networks. In: 2019 Twelfth International Conference on Contemporary Computing (IC3). IEEE, pp. 1–6.

Kokila, R.T., Selvi, S.T., Govindarajan, K., 2014. December). DDoS detection and analysis in SDN-based environment using support vector machine classifier. In: *2014 sixth international conference on advanced computing (ICoAC)*. IEEE, pp. 205–210.

Lawal, B.H., At, N., 2018. Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). In: *2018 26th Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4.

Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X., Gong, L., 2018. Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN. Int. J. Commun. Syst. 31 (5), e3497. https://doi.org/10.1002/dac.3497.

Liu, J., Lai, Y., Zhang, S., 2017. FL-GUARD: A Detection and Defense System for DDoS Attack in SDN. Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, pp. 107–111. https://doi.org/10.1145/3058060.3058074.

Liu, Z., Xu, M., Cao, J., & Li, Q. (2018). TSA: A two-phase scheme against amplification DDoS attack in SDN. In Mobile Ad-hoc and Sensor Networks: 13th International Conference, MSN 2017, Beijing, China, 2017, Revised Selected Papers 13; 483-496. Springer Singapore.

Makuvaza, A., Singh, D., Attlee, J., 2021. Deep neural network (DNN) solution for real - time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs). SN Comput. Sci. 2 (2), 1–10. https://doi.org/10.1007/s42979-021-00467-1.

Manso, P., Moura, J., 2019. SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks, pp. 1–17. https://doi.org/10.3390/info10030106.

Mansoor, A., Anbar, M., Bahashwan, A.A., Alabsi, B.A., Rihan, S.D.A., 2023. Deep learning-based approach for detecting ddos attack on software-defined networking controller. Systems 11 (6), 296. https://doi.org/10.3390/systems11060296.

Meti, N., Narayan, D.G., Baligar, V.P., 2017. Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In: *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, 2017-Janua*, pp. 1366–1371. https://doi.org/10.1109/ICACCI.2017.8126031.

Mladenov, B., 2019. Studying the DDoS attack effect over SDN controller southbound channel. In: *2019 X National Conference with International Participation (ELECTRONICA)*, pp. 1–4.

Mousa, A.K., Abdullah, M.N., 2023. An improved deep learning model for DDoS detection based on hybrid stacked autoencoder and checkpoint network. Future Internet 15 (8). https://doi.org/10.3390/fi15080278.

Mousavi, S.M., St-Hilaire, M., 2015. Early detection of DDoS attacks against SDN controllers. In: 2015 International Conference on Computing, Networking and Communications, ICNC 2015, pp. 77–81. https://doi.org/10.1109/ICCNC.2015.7069319.

Mousavi, S.M., St-Hilaire, M., 2018. Early detection of DDoS attacks against software defined network controllers. Journal of Network and Systems Management 26, 573–591.

Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T., Vasupongayya, S., 2019. Advanced support vector machine- (ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN). J. Comput. Netw. Commun. 2019 https://doi.org/10.1155/2019/8012568.

Nam, T.M., Phong, P.H., Khoa, T.D., Huong, T.T., Nam, P.N., Thanh, N.H., Thang, L.X., Tuan, P.A., Dung, L.Q., Loi, V.D., 2018. Self-organizing map-based approaches in DDoS flooding detection using SDN. 2018 International Conference on Information Networking (ICOIN), pp. 249–254. https://doi.org/10.1109/ICOIN.2018.8343119.

Open Networking Foundation. (2012). Software-defined networking: the new norm for networks. *ONF White Paper, 2*, 2-6.

Nisara, K., Welchb, I., Hassanc, R., Sodhrod, A.H., Pirbhulale, S., 2020. A survey on the architecture, application, and security of software defined networking. Internet of Thing., 100289 https://doi.org/10.1016/j.iot.2020.100289.

Niyaz, Q., Sun, W., Javaid, A.Y., 2017. A deep learning based DDoS detection system in software-defined networking (SDN). ICST Transact. Secur. Saf. 4 (12), 153515 https://doi.org/10.4108/eai.28-12-2017.153515.

Novaes, M.P., Carvalho, L.F., Lloret, J., 2020. Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment, 8, pp. 83765–83781. https://doi.org/10.1109/ACCESS.2020.2992044.

Omar, T.R., Ho, A., Urbina, B., 2019. Detection of DDoS in SDN Environment Using Entropy-based Detection. 2019 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–4. https://api.semanticscholar.org/CorpusID:212706103.

Oo, M.M., Kamolphiwong, S., Kamolphiwong, T., 2017. The design of SDN based detection for distributed denial of service (DDoS) attack. In: 2017 21st International Computer Science and Engineering Conference (ICSEC), 6, pp. 1–5.

Phan, T.V., Park, M., 2019. Efficient distributed denial-of-service attack defense in sdn-based cloud. IEEE Access 7, 18701–18714. https://doi.org/10.1109/ACCESS.2019.2896783.

Phan, T.V., Van Toan, T., Van Tuyen, D., Huong, T.T., Thanh, N.H., 2016. OpenFlowSIA: an optimized protection scheme for software-defined networks from flooding attacks. In: 2016 IEEE 6th International Conference on Communications and Electronics, IEEE ICCE 2016, pp. 13–18. https://doi.org/10.1109/CCE.2016.7562606.

Pillutla, H., Arjunan, A., 2018. Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing. J. Amb. Intell. Human. Comput. 0 (0), 0. https://doi.org/10.1007/s12652-018-0754-y.

Polat, H., Polat, O., 2020. Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models.

Prajapati, A., Sakadasariya, A., Patel, J., 2018. Software defined network: future of networking. In: *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018, Icisc*, pp. 1351–1354. https://doi.org/10.1109/ICISC.2018.8399028.

Priyadarshini, R., Barik, R.K., 2019. A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University - Computer and Information Sciences 34. https://doi.org/10.1016/j.jksuci.2019.04.010.

Raghunath, K., Krishnan, P., 2018. Towards A secure SDN architecture. In: 2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018, pp. 1–7. https://doi.org/10.1109/ICCCNT.2018.8494043.

Sahoo, K.S., Puthal, D., Tiwary, M., Rodrigues, J.J.P.C., Sahoo, B., Dash, R., 2018. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Futu. Gener. Comput. Syst. https://doi.org/10.1016/j.future.2018.07.017.

Sahoo, K.S., Tripathy, B.K., Naik, K., Member, S., Ramasubbareddy, S., 2020. An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks, 8. https://doi.org/10.1109/ACCESS.2020.3009733.

Sahoo, K.S., 2017. Detection of control layer DDoS attack using entropy metrics in SDN: an empirical investigation. In: *2017 Ninth International Conference on Advanced Computing (ICoAC)*, pp. 281–286.

Saifei, L.I., Yunhe, C.U.I., Yongfeng, N.I., Lianshan, Y.A.N., 2019. *An Effective SDN Controller Scheduling Method to Defence DDoS Attacks* *, 28, pp. 2017–2020. https://doi.org/10.1049/cje.2019.01.017.

Sangodoyin, A.O., Akinsolu, M.O., Pillai, P., Grout, V., 2021. Detection and classification of ddos flooding attacks on software-defined networks: A case study for the application of machine learning. IEEE Access 9, 122495–122508.

Santos, R., Moreno, E., 2019. *Machine Learning Algorithms to Detect DDoS Attacks in SDN. April*, pp. 1–14. https://doi.org/10.1002/cpe.5402.

Sayed, M.S.El, Le-Khac, N.A., Azer, M.A., Jurcut, A.D, 2022. A flow-based anomaly detection approach with feature selection method against DDoS attacks in SDNs. IEEE Transact. Cognit. Commun. Netw. 8 (4), 1862–1880. https://doi.org/10.1109/TCCN.2022.3186331.

Shamugam, V., Murray, I., Leong, J.A., Sidhu, A.S., 2016. Software defined networking challenges and future direction: A case study of implementing SDN features on OpenStack private cloud. In *IOP Conference Series*. In: *Materials Science and Engineering*, 121. Institute of Physics Publishing. https://doi.org/10.1088/1757-899X/121/1/012003.

Silva, F.S.D., Silva, E., Neto, E.P., Lemos, M., Neto, A.J.V., Esposito, F., 2020. A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT. Scenarios 1–28. https://doi.org/10.3390/s20113078.

Singh, J., Behal, S., 2020. Detection and mitigation of DDoS attacks in SDN: a comprehensive review, research challenges and future directions. Comput. Sci. Rev. 37, 100279 https://doi.org/10.1016/j.cosrev.2020.100279.

Singh, S., Kumar, R., 2016. A survey on software defined networking: architecture for next generation network. J. Netw. Syst. Manag. https://doi.org/10.1007/s10922-016-9393-9.

Sumantra, I., Gandhi, S.I., 2020. DDoS attack detection and mitigation in software defined networks. 2020 International Conference on System, Computation, Automation and Networking (ICSCAN). IEEE, pp. 1–5.

Sun, W., 2019. An Improved Method of DDoS Attack Detection for Controller of SDN, pp. 249–253.

Ubale, T., Jain, A.K., 2019. Taxonomy of DDoS Attacks in Software-Defined Networking Environment. Springer, Singapore. https://doi.org/10.1007/978-981-13-3804-5.

Ubale, T., Jain, A.K., 2020. Survey on DDoS attack techniques and solutions in software-defined network. Handbook of computer networks and cyber security: Principles and paradigms, pp. 389–419.

Ujjan, R.M.A., Pervez, Z., Dahal, K., Bashir, A.K., Mumtaz, R., González, J., 2020. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems 111, 763–779.

Varun, D.A., Sibi, K.K.A.S., 2018. LION IDS : A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks. Neural Computing and Applications 7. https://doi.org/10.1007/s00521-018-3383-7.

Varun, D.A., Sibi, K.K.A.S., 2018. LION IDS: A meta-heuristics approach to detect DDoS attacks against software-defined networks. Neural. Comput. Appl. 7 https://doi.org/10.1007/s00521-018-3383-7.

Wang, L., Liu, Y., 2020. A DDoS attack detection method based on information entropy and deep learning in SDN. Itnec 1084–1088.

Wang, Y., Wang, Y., 2020. *Efficient and Low-Cost Defense Against Distributed Denial-Of-Service Attacks in SDN-Based Networks. March*, pp. 1–24. https://doi.org/10.1002/dac.4461.

Wang, J., Wang, L., 2022. SDN-defend: a lightweight online attack detection and mitigation system for DDoS attacks in SDN. Sensors 22 (21). https://doi.org/10.3390/s22218287.

Wang, R., Jia, Z., Ju, L., 2015. An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking. https://doi.org/10.1109/Trustcom.2015.389.

Wang, S., Fernando, J., Gomez, K., Al-hourani, A., Kandeepan, S., Rizwan, M., Russello, G., 2022. Engineering Science and Technology, an International Journal Detecting flooding DDoS attacks in software defined networks using supervised learning techniques. Eng. Sci. Technol. Int. J. 35, 101176 https://doi.org/10.1016/j.jestch.2022.101176.

Wang, J., Wang, L., Wang, R., 2023. A method of DDoS attack detection and mitigation for the comprehensive coordinated protection of SDN controllers. Entropy 25 (8). https://doi.org/10.3390/e25081210.

Wu, X., Liu, M., Dou, W., Yu, S., 2016. DDoS Attacks on Data Plane of Software-Defined Network: Are They Possible? https://doi.org/10.1002/sec.

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

Xu, Y., Liu, Y., 2016. DDoS Attack Detection under SDN Context.

Xu, X., Yu, H., Yang, K., 2017. DDoS attack in software defined networks: a survey. ZTE Commun 15 (3), 13–19.

Yan, Q., Yu, F.R., Gong, Q., Li, J., 2016. Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Commun. Surv. Tutor. 18 (1), 602–622. https://doi.org/10.1109/COMST.2015.2487361.

Yan, Q., Gong, Q., Yu, F.R., 2017. Effective Software-Defined Networking Controller Scheduling Method to Mitigate DDoS Attacks, 53, pp. 5–6. https://doi.org/10.1049/el.2016.2234.

Ye, J., Cheng, X., Zhu, J., Feng, L., Song, L., 2018. A DDoS Attack Detection Method Based on SVM in Software Defined Network. Security and Communication Networks. https://doi.org/10.1155/2018/9804061.

Yu, S., Zhang, J., Liu, J., Zhang, X., Li, Y., Xu, T., 2021. A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN. EURASIP J. Wirel. Commun. Network. https://doi.org/10.1186/s13638-021-01957-9.

Zhijun, W., Qing, X., Jingjie, W., Meng, Y., Liang, L., 2020. *Low-rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network. XX.* https://doi.org/10.1109/ACCESS.2020.2967478.

Zhou, H., 2023. A Cooperative Detection of DDoS Attacks Based on CNN-BiLSTM in SDN. Int. J. Fut. Comput. Commun. 27–36. https://doi.org/10.18178/ijfcc.2023.12.2.600.

Zubaydi, H.D., Anbar, M., Wey, C.Y., 2017. Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller. In: Proceedings - 2017 Palestinian International Conference on Information and Communication Technology, PICICT 2017, pp. 10–16. https://doi.org/10.1109/PICICT.2017.26.

Aishatu Abdullahi Wabi is a Ph.D Student at the Federal University of Technology Minna, Nigeria. She received her Bachelors degrees in Computer Science from Ibrahim Badamasi Babangida University, Lapai and a Masters of Technology (M.Tech) degree in Cyber Security Science from Federal University of Technology, Minna. She is currently a Civil Servant with the Niger State Government, Nigeria and is interested in research in the area of Network security and Machine learning.