Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-023-08075-2

RESEARCH ARTICLE-COMPUTER ENGINEERING AND COMPUTER SCIENCE

A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN

Naziya Aslam[1] · **Shashank Srivastava**[1] · **M. M. Gore**[1]

Received: 2 February 2023 / Accepted: 13 June 2023

Abstract
Software-defined networking (SDN) provides programmability, manageability, flexibility and efficiency compared to traditional networks. These are owing to the SDN's mutual independence or separation of the control and data planes. Decoupling two planes and the centralised nature of SDN enhance DDoS attack protection by facilitating easy implementation of network device policies. The controller's ability to filter network traffic and detect malicious flows is attributed to its global network view. Control and data plane separation brought numerous benefits, but it also introduced a new challenge in terms of its susceptibility to DDoS attack. DDoS attacks are one of the most severe threats to SDN, where the perpetrator disrupts the services of regular users. Machine learning (ML) and deep learning (DL) have emerged as good solutions compared to statistical or policy-based solutions to detect DDoS attack. We have created a detailed taxonomy of DDoS defense solutions. We have surveyed 260 research articles, of which 132 articles are selected based on ML- and/or DL-based solutions to detect DDoS attack in SDN. We discuss the existing works which have applied feature selection algorithms on the dataset to select the best and optimal features for detecting DDoS attack. We present the features of various DDoS datasets available publicly. We also argue for the need to create SDN-specific datasets and then apply feature selection algorithms that may help in better detection of DDoS attack. Finally, we present the research challenges in SDN security that can help the researchers to carry out further research and develop new methods to secure SDN.

Keywords SDN · DDoS attack · Machine learning · Deep learning

1 Introduction

Distributed denial of service (DDoS) attack overwhelms a server with Internet traffic, making it inaccessible to regular users. It restricts users' network access, possibly halting the entire network. This attack has evolved into a severe danger over the last decade due to its high intensity and severity of its effect on the network. First-ever large-scale DDoS attack emerged in 1999 [185], disrupting the network at the University of Minnesota. Since then, DDoS attacks have kept disturbing the Internet, mainly the service providers. The year 2013 governed the first ever 100 Gbps DDoS attack [109]. In 2016, within a time span of 3 years, the impact of highest DDoS attack evolved up to 1 Tbps [110], disrupting the communication of a large number of devices. In February 2023, an HTTP DDoS attack with 71 million requests per second was launched during USA-based NFL Super Bowl weekend [144]. Table 1 lists the DDoS attacks that have happened in the past. We can see from Table 1 the severity of DDoS attacks is progressively increasing each year, leading to a vast disruption of network services. A few factors boosting the scales of these attacks are the evolution of IoT devices in mass, high availability of upload bandwidth, and readily available attack source codes. The threatening action of DDoS attack has forced industries and academia to come up with innovative solutions to safeguard Internet infrastructure.

In traditional/conventional networks, the forwarding behaviour of network devices and packet control logic are linked strongly. This decreases flexibility, hinders innovation,

✉ Naziya Aslam
naziyaaslam29@gmail.com

Shashank Srivastava
shashank12@mnnit.ac.in

M. M. Gore
gore@mnnit.ac.in

[1] Department of Computer Science and Engineering, Motilal Nehru National Institute of Technology Allahabad, Prayagraj, Uttar Pradesh 211004, India

Published online: 11 July 2023

Table 1 DDoS attacks of the past

S. no.	Refs.	Year	Attack target	Attack rate	Description
1	[144]	Feb 2023	USA-based NFL Super Bowl weekend	71 million rps	Dozens of hyper-volumetric DDoS attack with 71 million requests per second was launched during USA-based NFL Super Bowl weekend
2	[17]	June 2022	Cloud Armor customer	46 million rps	A DDoS attack with 46 million requests per second was launched against a Cloud Armor client
3	[81]	June 2022	Customer website	26 million rps	A HTTP DDoS attack of 26 million targeting the customer websites was mitigated by Cloudflare
4	[250]	August 2021	Azure customer	2.4 Tbps	DDoS attack of 2.4 Tbps affected Azure cloud computing service's customer that lasted for 10 min
5	[1]	February 2020	Customer of AWS	2.3 Tbps	One of the customers of Amazon Web Services suffered a massive DDoS attack of 2.3 Tbps
6	[205]	April 2019	Client of Imperva	580 pps	One of the clients of Imperva faced DDoS attack peaked at 580 million packets per second
7	[233]	March 2018	USA-based wired telecommunication carrier	1.7 Tbps	USA-based company wired telecommunication carrier was affected by DDoS traffic of 1.7 Tbps
8	[189]	March 2018	Website of Russian Defense Ministry	10,000 rps	Russian Defense Ministry's website was hit by seven DDoS attacks sending tens of thousands of requests per second
9	[119]	February 2018	GitHub	1.35 Tbps	Using the Memcached-based technique, GitHub was subjected to an amplification attack of 1.35 Tbps through 126.9 million packets per second
10	[33]	November 2017	Boson Globe website	–	DDoS attack affected the company's website and servers bringing down the newspaper's telephone and editing systems
11	[225]	October 2017	Website of Czech parliamentary Election	–	During the vote counting in the Czech parliament's lower house election, a DDoS attack took down the Czech statistical office's website
12	[49]	September 2017	UK National Lottery	–	A DDoS attack on the UK National Lottery website prevented people from purchasing tickets
13	[26]	April 2017	Melbourne IT	–	Domain name registrar named Melbourne IT and its subsidiaries were hit by a DDoS attack, rendering cloud hosting and email services inaccessible
14	[252]	October 2016	Dyn server	1.2 Tbps	Servers of Dyn company was brought down by Mirai botnet. The attack involved around 1,00,000 malicious endpoints creating a DDoS attack of 1.2 Tbps
15	[172]	June 2016	Website of jewellery shop	35,000 HTTP rps	A jewellery shop website in the USA was attacked by a DDoS attack comprising 25,000 CCTV botnets. The site was hit by 25,000 HTTP requests per second

Table 1 (continued)

S. no.	Refs.	Year	Attack target	Attack rate	Description
16	[239]	May 2016	Bank of Greece website	–	Servers of Bank of Greece website was brought down for 6 h by launching DDoS attack
17	[171]	January 2016	HSBC Internet banking	–	HSBC's Internet banking facility was disrupted by DDoS attack for several hours
18	[94]	January 2016	Website of Irish government	–	A DDoS attack knocked off many Irish government websites
19	[24]	December 2015	BBC website	500 Gbps	DDoS attack of 500 Gbps bandwidth occurred
20	[228]	October 2015	Thai government websites	–	DDoS attack targeted several Thai government websites bringing them down for several hours
21	[156]	February 2014	Client of Cloudflare	400 Gbps	One of the clients of Cloudflare was hit by DDoS attack peaking at 400 Gbps
22	[251]	March 2013	Spamhaus website	300 Gbps	The Spamhaus website was targeted by DNS reflection attack with a bandwidth of more than 300 Gbps

and incurs increased operational costs. These drawbacks of traditional networks make it difficult to prevent DDoS attacks on the network. Consequently, the key network properties of integrity, information availability, non-repudiation, confidentiality, and authentication are becoming increasingly difficult to maintain. Many researchers and companies have focused on developing resilient, scalable, and secure networks. The innovation of software-defined networking (SDN) in 2008 [146] has boosted the research for identifying network DDoS attacks. It is a step towards establishing network's dynamic and centralised structure as opposed to the traditional networks.

Data, control, and application planes make up SDN. The data plane consists of switches and routers. They are in charge of carrying network user data, forwarding the data, and gathering statistics. The middle plane is the control plane, which plays a role in managing the data plane. The control plane is in charge of routing decisions and managing switches, routers, and hosts available on the data plane. The controller on the control plane has a broad centralised view of the network. The controller establishes the flow rules to ensure packets are forwarded to the desired location. The topmost plane is the application plane. It comprises network services, applications, and orchestration tools that communicate with the control plane. The application plane is primarily in charge of network traffic management. Unlike traditional networks, SDN separates a network device's forwarding and control logic. The control logic is logically centralised at the network controller, while the forwarding logic is kept at the network device. The applications connect with the controller via various Application Programming Interfaces (APIs), such as Java APIs for data transmission or REST APIs for distant communication [132]. The OpenFlow protocol exchanges information across the data and control planes. The controller is placed centrally and has a broad view of the network. It can optimise flow management, offer high bandwidth utilisation, flexibility and scalability using global information.

With the arrival of SDN, many research proposals for detecting and mitigating DDoS attacks were presented just in a short time. SDN protects against DDoS attack as policies might be easily enforced on network devices. Due to its broad network view, the controller can filter network traffic to detect malicious flows. Control and data plane separation brought numerous benefits, but it also introduced a new challenge in terms of its susceptibility to DDoS attacks. The controller being centrally placed, acts as a solitary point of failure. Any mishap to the SDN controller may result in network failure, making it an appealing target for attackers [97]. Defending SDN controllers from DDoS attacks is complex and resource-intensive. It restricts network management efficiency. The attacker can target any of the SDN planes. A thorough understanding of SDN features is necessary for any effort to defend SDN infrastructure from DDoS attacks. The fundamental characteristics of network traffic define DDoS attack behaviours in SDN. 2017 has been marked as the period of widespread SDN adoption and DDoS attack mitigation by Turner [234]. Jose and Kurian [98] stated in their research that the essential network traffic features can be utilised as indicators to identify DDoS attacks. Detecting

and mitigating DDoS attacks is a challenging issue that has emerged as a popular study topic.

The notion of DDoS attack is becoming more prevalent. The major concern is to detect the attack at early stages of its commencement so that the network administrator can take effective actions against the attack to protect regular network operations. An innovative solution that provides efficient safeguards for the network from DDoS attack is required. From the emergence of SDN to now, researchers have presented various solutions for detecting DDoS attacks. These methods are classified into statistical-based, policy-based, ML-based and DL-based methods. In statistical analysis-based detection method, DDoS attacks are identified using observation of threshold for specific statistical patterns. Policy-based methods detect DDoS attack on the exploitation of certain pre-defined policies. ML- and DL-based solutions detect DDoS attack by feeding network features to the detection model trained by machine/deep learning algorithms. A DDoS detection method is considered efficient if it accurately classifies the DDoS traffic from legitimate traffic. A high volume of legal network traffic may trigger false detection alarms for statistical analysis-based and policy-based detection methods. Therefore, our survey focuses on ML- and DL-based solutions for DDoS attack detection. Our work does not include statistical or policy-based solutions. Interested readers can go through the research works of [5, 30, 35, 44, 60, 59, 66, 70, 82, 85, 89, 102, 107, 114, 115, 121, 139, 142, 143, 153, 166, 192, 196, 204, 247, 246, 253, 268] that focus on statistical and policy-based methods for DDoS attack detection. Table 2 lists the acronyms used throughout the article.

SDN network management has benefited from ML- and DL-based solutions. ML methods are utilised in several domains to tackle challenging issues [178]. DDoS attacks are detected using these algorithms, and they have been shown to outperform signature-based detection methods [31]. ML and DL classifiers can be trained to detect abnormal traffic on the network more accurately. SVM, HMM, DT, ASVM, KNN, NB, RT, LR, and RF are extensively used ML classifiers, while LSTM, CNN, GRU and RNN are some of the DL-based algorithms. ML- and DL-based solutions provide effective and dynamic SDN security and management solutions.

We have reviewed 24 survey articles from the year 2014 to 2023. The surveys focused on various parameters such as DDoS attacks in SDN, different DDoS attacks that can affect the layers of SDN, and how SDN can act like a victim and threat to DDoS attacks. The surveys also depict different defense solutions in the SDN network for identifying and mitigating DDoS attacks. We discovered none of the surveys thoroughly analysed ML- and DL-based solutions for DDoS attack detection. Also, the surveys lacked detailed analysis of public DDoS datasets and analysis of various feature selection techniques for DDoS attack detection. These research gaps motivated us to write this survey. Apart from the survey articles, we have reviewed 260 research articles related to DDoS attacks in SDN. Out of the 260 research articles, we have considered 132 research articles related to DDoS defense solutions based on ML and/or DL algorithms in SDN. These 132 papers are divided into three categories based on the types of ML methods (supervised, unsupervised, and ensemble algorithms) and/or DL algorithms used to identify DDoS assaults in SDN.

In this paper, we have created a detailed taxonomy of DDoS defense solutions based on classification by the creation of detection and mitigation applications for different controllers, classification based on dataset used for identifying DDoS attacks, classification based on different ML/DL-based solutions, classification based on different feature selection techniques, based on attack target and based on the testing environment. We compared our survey to other surveys based on the number of research works referred over a range of years and whether a detailed analysis of ML- and DL-based solutions, public datasets, SDN-based applications and feature selection algorithms is presented. We have done a deep analysis of different datasets available publicly. Feature selection techniques have been elaborated, and the most efficient features researchers use for DDoS attack detection are listed. The merits and limitations of various ML- and DL-based solutions for DDoS attack detection are analysed, which opens the path for more study in this area. A list of applications created for DDoS attack detection and mitigation is presented. Finally, we talk about existing gaps and future research directions that will be useful to researchers to propose effective solutions for DDoS attack detection.

1.1 Scope and Contributions

Analysing all the studies presented by researchers following are the findings and contributions:

- *Past survey analysis:* We have examined previous surveys on the detection of DDoS assaults in SDN and compared our survey based on several research works, whether detailed analysis of ML-based and DL-based solutions is done, description of public DDoS datasets, creation of SDN-based application and analysis of feature selection algorithms.
- *Detailed analysis of DDoS datasets:* We analysed a number of datasets and presented a detailed explanation of various datasets available for DDoS attack detection, as none of the researchers surveyed public datasets in detail. We also specify the need to generate an SDN-based dataset.
- *Feature engineering:* Our survey presents the feature selection techniques researchers use to select the best and

Table 2 List of Abbreviations

Acronym	Full name	Acronym	Full name	Acronym	Full name	Acronym	Full name
SDN	Software-Defined Networking	NB	Naive Bayes	IDS	Intrusion Detection System	NSL-KDD	Network Security Laboratory—Knowledge Discovery in Databases
DDoS	Distributed denial of service	RT	Random Trees	DPI	Deep Packet Inspector	CAIDA	Cooperative Association for Internet Data Analysis
ML	Machine Learning	LR	Logistic Regression	QoS	Quality of Service	TCP	Transmission Control Protocol
DL	Deep Learning	RF	Random Forest	CAM	Content Addressable Memory	R2L	Remote-to-Local
API	Application Programming Interface	LSTM	Long Short-Term Memory	DrDoS	Distributed Reflection Denial of Service	U2R	User-to-Root
SVM	Support Vector Machine	AWS	Amazon Web Service	FTP	File Transfer Protocol	IMAP	Internet Messaging Access Protocol
HMM	Hidden Markov Model	HTTP	Hyper Text Transfer Protocol	DoS	Denial of Service	SMTP	Simple Mail Transfer Protocol
DT	Decision Tree	CNN	Convolutional Neural Network	SNMP	Simple Network Management Protocol	POP3	Post Office Protocol
ASVM	Advanced SVM	GRU	Gated Recurrent Unit	IRC	Internet Relay Chat	SiDDoS	SQL Injection DDoS
KNN	K-nearest neighbours	RNN	Recurrent Neural Network	DSN	Data Source Name	PCAP	Packet Capture
LDAP	Lightweight Directory Access Protocol	NTP	Network Time Protocol	ANN	Artificial Neural Network	SOM	Self-Organising Map
PCA	Principal Component Analysis	NCA	Neighbourhood Component Analysis	ANOVA	Analysis of Variance	SMCA	Semantic Multilinear Component Analysis
LASSO	Least Absolute Shrinkage and Selection Operator	RBF	Radial Basis Function	FPR	False Positive Rate	MLP	Multi-layer Perceptron
IG	Information Gain	GR	Gain Ratio	BPNN	Back Propagation Neural Network	SMO	Sequential Minimal Optimisation
NN	Neural Network	PSO	Particle Swarm Optimisation	TPR	True Positive Rate	FAR	False Alarm Rate
ELM	Extreme Learning Machine	LDA	Linear Discriminant Analysis	REP Tree	Reduced Error Pruning Tree	DNN	Deep Neural Network
GNB	Gaussian Naïve Bayes	QDA	Quadratic Discriminant Analysis	CART	Classification And Regression Tree	CAD	CUSUM Abnormal Detection
SAE	Sparse Autoencoder	ET	Extra Trees	GBDT	Gradient Boost Decision Tree	SSAE	Stacked Sparse Autoencoder
ACO	Ant Colony Optimisation	AUC	Area Under the ROC Curve	RL	Reinforcement Learning	RBM	Restricted Boltzmann Machine

optimal feature set from either their own generated or public datasets. We focus on the need to create SDN specific dataset and then apply feature selection algorithms that may help better detect DDoS attacks in the context of a real-world network.

- *Analysis of Machine learning-based solutions for DDoS attack detection:* We present a detailed analysis of different ML algorithms, such as supervised, unsupervised, and ensemble learning algorithms used by researchers as a solution to detect DDoS attacks. Our scope of work is limited to DDoS attack detection.
- *Analysis of Deep learning-based solutions for DDoS attack detection:* Deep learning algorithms have become popular and outperformed ML algorithms in identifying DDoS attacks in recent years. A detailed analysis of DL-based solutions to detect DDoS attack has not been done till now. As a result, our research presents a comprehensive review of DL-based solutions for DDoS detection.
- *Detection and Mitigation Application:* Timely identifying and reducing DDoS assaults is a challenge. An SDN application deployed at the application layer that communicates with the controller and performs DDoS attack detection and mitigation will be useful. We present the research works that have created applications to detect and mitigate DDoS attacks. We also emphasise the need to develop an SDN-based application for DDoS attack detection and mitigation to recognise and handle attacks efficiently, hence averting massive harm to legitimate users.
- *Highlights of future research directions:* Our study addresses research issues and pinpoints potential possibilities for DDoS attack detection in SDN systems, offering insightful information and assisting in creating effective detection tools.

1.2 Organisation of Paper

The survey article is organised into twelve sections. Section 2 gives a recap of the related surveys for DDoS attack detection in SDN environment. A comparison of our survey with related surveys based on certain parameters is presented in this section. Section 3 presents the primary purpose of conducting this survey. Section 4 gives an overview of SDN and its benefits. It explains the architecture of SDN and how SDN is better than conventional networks. Section 5 explains the DDoS attacks and how they can affect the different layers of SDN architecture. Section 6 presents a detailed description of different datasets available publicly that can be used for DDoS attack detection. Section 7 presents the different feature selection methods for creating the best and optimal feature dataset, which can aid in better detection of DDoS attacks. Section 8 presents the detailed literature survey of the ML algorithms used by researchers for detecting DDoS attacks in an SDN environment. This section is classified into supervised, unsupervised, and ensemble ML-based solutions. Section 9 overviews the various DL-based solutions for detecting DDoS attacks in SDN. Section 10 lists the applications created by researchers for the detection and mitigation of DDoS attack. Section 11 explains the different research challenges in SDN security that can help researchers conduct further research and develop new methods to secure SDN. The last Sect. 12 presents the conclusion followed by future work.

Figure 1 represents the structure of this paper section-wise.

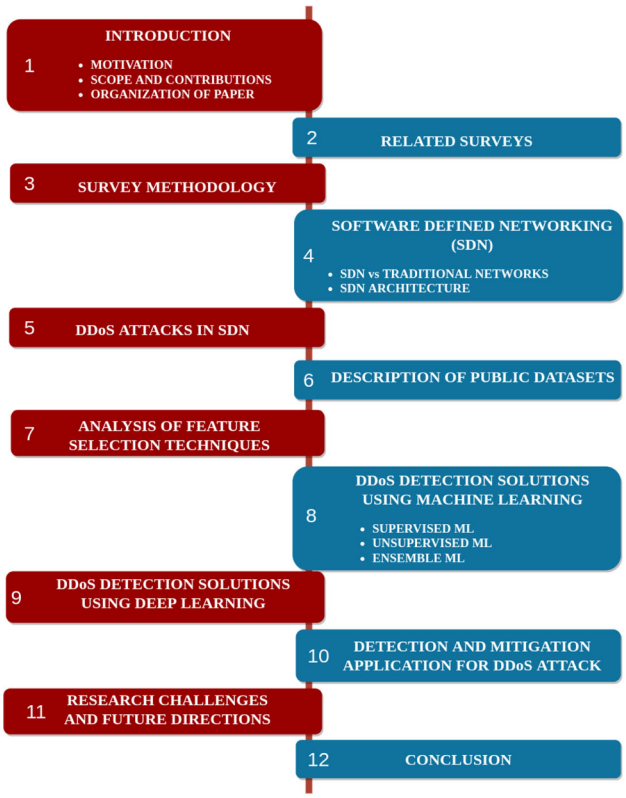

Fig. 1 Structure of the paper

2 Related Surveys

Jay Turner has declared 2017 the year of broad SDN implementation and DDoS attack mitigation [234]. SDN adoption and usage have increased rapidly since then. A similar analysis by MarketsandMarkets estimates that SDN demand will increase from $ 13.7 billion in 2020 to $ 32.7 billion in 2025 [190]. The demand for a sophisticated network administration system capable of handling the growing network traffic and complexity is a key driver in the market. However, the increased usage of networking devices has posed threats to SDN networks. The primary threat faced by SDN is DDoS attack. SDN is an obvious target for DDoS attackers due to

the centralised management and dumb forwarding characteristics of switches. DDoS attacks are devastating as they disrupt the services of servers and deny access to legitimate users. This could affect users primarily as their essential work might be interrupted, and they may be unable to access the service if the attack rate is high. Some of the major DDoS attacks of the past are summarised in Table 1. DDoS attacks have become common in disrupting servers by attacking at a rate as high as 2.4 Tbps. This shows a dire need to get rid of DDoS attacks.

Getting rid of DDoS attacks is a challenge that has led to increased research in finding solutions for detection and mitigation of DDoS attacks. After reviewing existing research, we found studies focusing on DDoS defense mechanisms in SDN. Ashraf and Latif [18], in their review work, analysed different ML techniques to cope with intrusion detection and DDoS attacks in SDN. Yan et al. [259] offered a complete assessment of DDoS defense methods employing SDN in cloud computing and explained how SDN could protect itself from DDoS attacks. The network's security is necessary so that SDN-based cloud can be formed smoothly and free from the fear of DDoS attacks. Bawany et al. [28] presented the SDN characteristics and how it can help detect DDoS attacks compared to traditional networks. They explained various DDoS detection techniques (entropy, machine learning, connection rate, traffic pattern analysis, SNORT, and OpenFlow integrated) for SDN. Some of the mitigation techniques used by researchers to prevent DDoS attack are also presented in their study. They also proposed their SDN-based DDoS detection and mitigation model for smart cities. Another survey by Dayal et al. [58] presented various security issues on various layers of SDN architecture. Xu et al. [255], Kalkan et al. [103], Fajar and Purboyo [72] and Joëlle and Park [100] also presented some of the defense solutions to protect SDN architecture from DDoS attacks. In their study, Imran et al. [93] presented the various mitigation techniques for DDoS attack prevention in SDN. Sahoo et al. [191] explained the SDN security issues, possible DDoS attacks on SDN layers and different detection techniques for securing SDN against DDoS attacks. They also proposed an information distance-based flow discriminator framework for distinguishing DDoS traffic during flash events in the SDN network environment. Their simulation experiment used CAIDA [37] and FIFA World Cup datasets to detect DDoS attacks. Swami et al. [218] studied the DDoS attacks in detail. They looked at the contradictory relationship between DDoS attacks and SDN. SDN is utilised to guard against DDoS attacks owing to its benefits of centralised traffic control, dynamic flow rule updation, and network programmability. The centralised controller can handle network traffic more efficiently than traditional networks because it can access all network data. Furthermore, when a controller detects any unusual congestion in the network, a control plane protection technique installs rules in SDN switches to delete or block harmful traffic. However, because of the centralised controller and dumb switches, SDN is prone to DDoS attacks. The centralised SDN controller becomes the primary target as the attackers can downgrade the entire network by overwhelming the control plane. Furthermore, because the forwarding devices lack intelligence, they must send every new packet to the controller for judgement. As a result, the controller's memory, processor, and network resources are depleted. Furthermore, forwarding devices are vulnerable to DDoS attacks because they have limited memory.

DDoS attacks in SDN and cloud environments were explained by Dong et al. [68]. Singh and Bhandari [211] provided a taxonomy of novel flow-based SDN-targeted DDoS attacks and several protection strategies to counteract them. Singh and Behal [210] categorised the DDoS protection solutions based on the type of detection mechanisms. They thoroughly evaluated 70 different DDoS detection and mitigation strategies. These 70 mechanisms are grouped into four sections: Artificial neural network-based approaches, ML-based methods, information theory-based methods, and others. They also discussed this topic's concerns, research gaps, and challenges encountered while designing a detection system. Ubale and Jain [236] explained the solutions for buffer saturation, flow table overflow, controller saturation, and control data channel congestion for tackling DDoS attacks in SDN. Another brief review by Al-Adaileh et al. [9] and Gupta and Grover [80] explained some detection techniques for detecting DDoS attacks on SDN controllers. A survey by Pajila and Julie [173], Kaur et al. [106], and Valdovinos et al. [240] also presented different DDoS defense solutions in SDN. In their work, Cui et al. [50] offered a detailed analysis of DDoS attack in SDN and classified it into attacks targeted at service providers and SDN layers. They also survey different DDoS detection techniques in SDN based on ML-based, statistical and threshold-based solutions.

Table 3 compares previous survey articles with our survey. The comparison is based on the number of research works referred over a range of years and whether a detailed analysis of ML- and DL-based solutions, public datasets, SDN-based applications and feature selection algorithms is presented.

3 Survey Methodology

This section describes how the survey was carried out. The fundamental causes that prompted this study and the technique used to conduct the review are explained.

The survey articles and research articles listed in our survey have been taken from various sources. Numerous research publications were read, research questions were created, and various databases were searched as part of

Table 3 Comparison of our work to related surveys

References	Research works	Range of year	Presented detailed analysis of				
			ML-based solutions	DL-based solutions	Public datasets	SDN-based application	Feature selection algorithms
Ashraf and Latif [18]	35	1991–2014	✓	×	×	×	×
Yan et al. [259]	131	2000–2015	Few	×	×	×	×
Xu et al. [255]	45	2003–2017	Few	×	×	×	×
Bawany et al. [28]	101	1999–2016	Few	×	×	×	×
Dayal et al. [58]	120	2002–2015	Few	×	×	×	×
Kalkan et al. [103]	15	2009–2016	Few	×	×	×	×
Fajar and Purboyo [72]	34	2000–2017	×	×	×	×	×
Joëlle and Park [100]	79	2003–2018	Few	×	×	×	×
Imran et al. [93]	54	2008–2018	×	×	×	×	×
Sahoo et al. [191]	162	2003–2018	Few	×	×	×	×
Swami et al. [218]	92	1994–2018	Few	Few	×	×	×
Dong et al. [68]	124	2001–2019	×	×	×	×	×
Pajila and Julie [173]	51	2003–2018	Few	×	×	×	×
Ubale and Jain [236]	54	2004–2018	×	×	×	×	×
Singh and Bhandari [211]	103	1990–2020	Few	Few	×	×	×
Singh and Behal [210]	161	1994–2020	✓	Few	×	×	×
Al-Adaileh et al. [9]	70	2004–2020	Few	×	×	×	×
Han et al. [86]	177	1995–2019	Few	×	×	×	×
Gupta and Grover [80]	20	2015–2021	✓	Few	×	×	×
Kaur et al. [106]	170	2007–2021	✓	Few	×	×	×
Valdovinos et al. [240]	173	2003–2020	✓	Few	×	×	×
Cui et al. [50]	216	2002–2021	✓	✓	×	×	×
Alhijawi et al. [11]	30	2013–2020	Few	Few	×	×	×
Alashhab et al. [10]	121	1990–2022	Few	Few	×	×	×
Our work	268	1994–2023	✓	✓	✓	✓	✓

this review approach. The approach used for this survey included searching several databases, i.e. Springer, Science Direct, IEEE Explore, Elsevier, ACM Digital Library, Google Scholar, and DBLP, for related works.

We have reviewed 24 survey articles from 2014 to 2023. The surveys focused on various parameters such as DDoS attacks in SDN, different DDoS attacks that can affect the layers of SDN, and how SDN can act like a victim

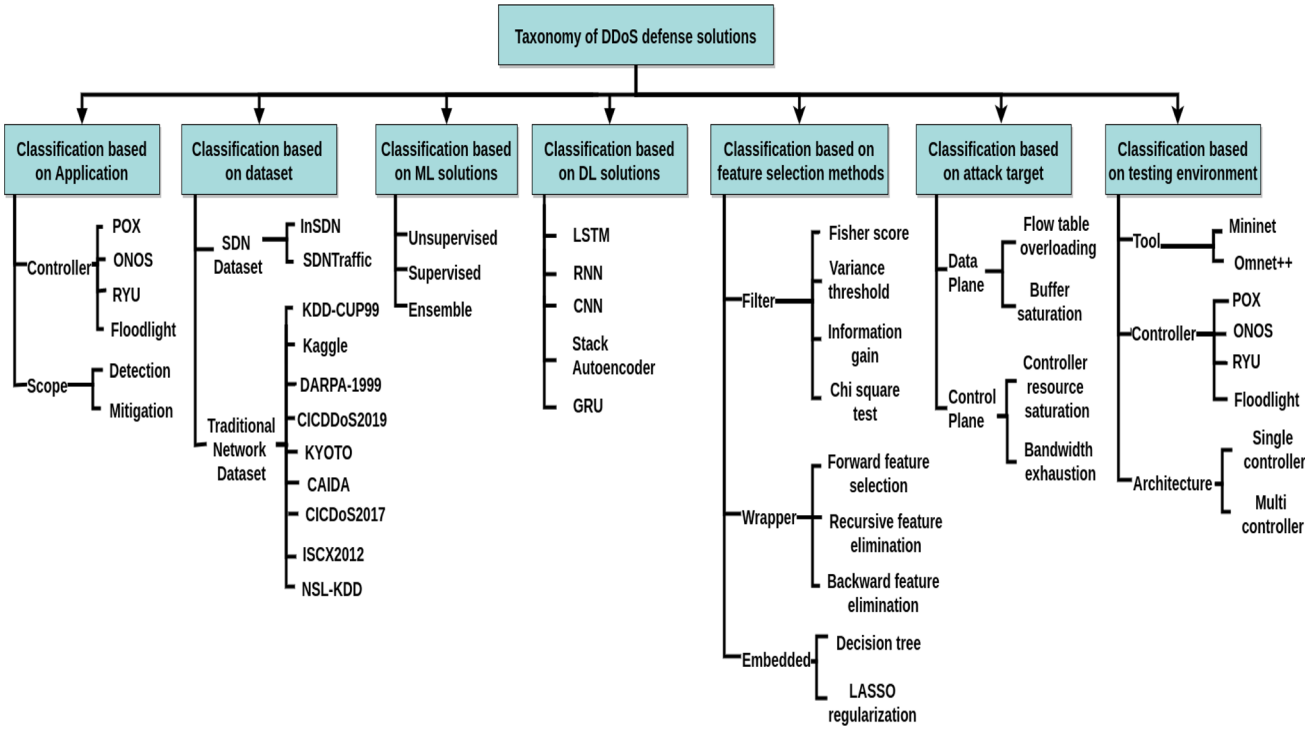

Fig. 2 Taxonomy of DDoS defense solutions

and threat to DDoS attacks. The surveys also depict other defense solutions for DDoS attack detection and mitigation in SDN environment. Apart from the survey articles, we have reviewed 260 research articles related to DDoS attack in SDN. Out of the 260 research articles, we have considered 132 research articles related to DDoS defense solutions based on ML and/or DL algorithms in SDN. These 132 articles are classified according to the different types of ML algorithms (supervised, unsupervised, and ensemble ML algorithms) and/or DL algorithms used to detect DDoS attacks in SDN. Figure 2 depicts a detailed taxonomy of DDoS defense solutions. Table 4 compares our work with State-of-the-Art taxonomy methods.

Also, Fig. 3 represents the percentage-wise distribution of articles that have used ML and/or DL algorithms as a solution to get rid of DDoS attacks in SDN.

4 Software-Defined Networking (SDN)

SDN is an improved network architecture that manages network traffic flows while allowing for better network administration. Researchers have been striving to develop strategies to protect networks against cyber attacks for years. However, their efforts have been hampered by efficiency, scalability, dependability, and security problems. The introduction of SDN technology fascinates the research and security sectors because it offers innovative and alternative approaches to addressing difficulties. The design of the SDN environment, which separates the control plane from the forwarding plane, provides unique security solutions to protect networks from attackers. It offers dynamic network management using a logical and centralised control system that instructs the data layer to channel network traffic. On the other hand, the centralised control function may be a drawback since it creates a risk of a single point of failure due to the network's reliance on it. As a result, the centralised SDN controller appears to be an appealing prospect for DDoS assaults, with a major attack possibly causing network damage or even catastrophic collapse. Attackers also take advantage of data plane switch constraints, such as memory capacity. The main purpose of a DDoS attack on an SDN controller is to overload and exhaust its resources, typically by flooding the network with fake IP packets, resulting in an overload that interrupts or fails the network. Simultaneously, a centralised SDN controller might act as a virtualised network, making the network flexible and easy to operate. The controller collects network information from incoming packets and identifies network devices that interact with it. By exploiting its programmability and flexibility, the SDN controller might also help to enhance network performance. Since the control plane is disintegrated from the data plane, all data packets that do not fit any of the flow table rules are routed to the controller. In other words, by dealing with two types of objects, the controller enhances network traffic flow monitoring. The first object is

Table 4 Comparison of our work with State-of-the-Art taxonomy methods

References	Year	Taxonomy method
[211]	2020	Based on classification by switch vulnerabilities, attack type, attack impact and attack strength
[240]	2021	Based on different DDoS detection and mitigation strategies: statistical, machine learning, SDN architecture, blockchain, network function virtualisation, honeynets, network slicing and moving target defense
[106]	2021	Based on attack targets, DDoS defense approaches, testing environment and traffic generation mechanism
[105]	2022	Based on different DDoS mitigation techniques on communication interfaces, application, control, and data plane of SDN
[158]	2023	Based on detection methods using deep learning techniques: discriminative learning, generative learning, hybrid learning
[12]	2023	Based on different detection techniques for DDoS attacks: statistical analysis, blockchain, machine learning, network function virtualisation
Our work	2023	Classification based on application, dataset, ML solutions, DL solutions, feature selection methods, attack target, and testing environment. Also created a taxonomy of different ML and DL algorithms

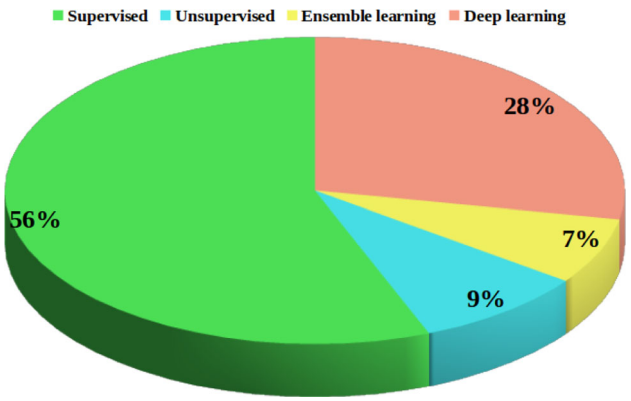

Fig. 3 Distribution of articles based on type of algorithms

network management, consisting of switch table packet forwarding policies. The second object is network observation which enables network traffic behaviour analysis. Figure 4 depicts SDN architecture consisting of application, control and data planes.

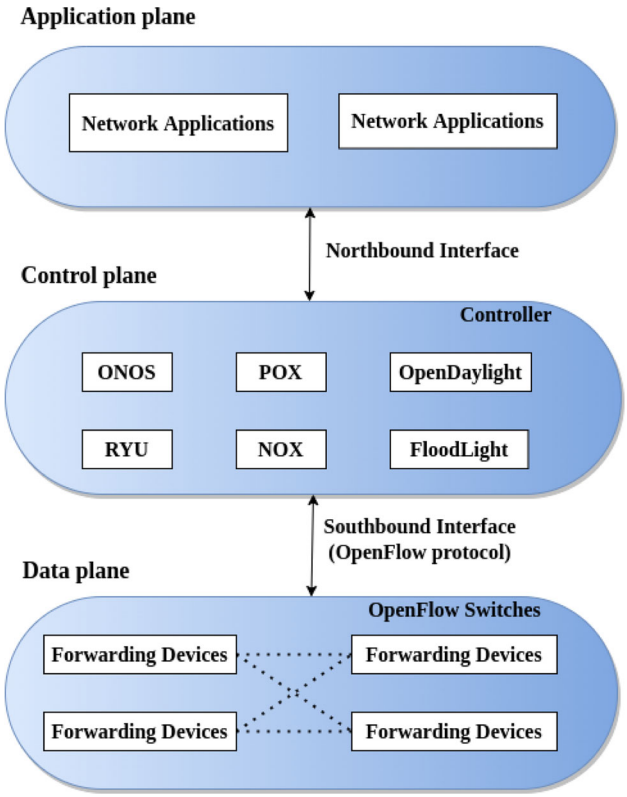

Fig. 4 SDN architecture

4.1 SDN Versus Traditional Networks

The essential notion of SDN architecture is decoupling the data plane from the control plane, which opens up immense potential for network design innovation. The mutual independence of the two planes promotes programmability in SDN networks. As a result, network traffic management and the configuration of SDN-enabled network devices have enhanced. Control logic is included in traditional network devices. If the policy needs to be modified, the logic on each device must be manually updated according to vendor-specific rules, which takes time. On the other hand, SDN isolates control logic and allows administrators to alter control logic via southbound APIs with centralised monitoring remotely. Adopting new creative rules in traditional switches is difficult since they are vendor-specific with restricted hardware capabilities. In addition to the centralised controller, policy changes are a relatively quick procedure in SDN. The conventional network offers only a restricted region for testing new policies, but SDN offers significantly more testing options than the traditional network.

4.2 SDN Architecture

Our society is becoming increasingly linked as information and communication technology progresses. However, our

traditional networks have limits, such as scalability, security, operating expenses, manageability, and personalisation. There has been much buzz in the academic and practitioner sectors to create a new SDN architecture to solve these restrictions while delivering new networking improvements. SDN may be an extension of prior notions, such as reconfigurable networks and interfaces. Decoupling the control and data planes in networking devices is a fundamental element in the SDN design. Plane separation lets each layer grow virtually independently, allowing for more creativity, faster deployment, acceptance of new features and services, and improved management and security. The second concept is transparency, which states that consumers should be unable to distinguish between traditional networks and SDN. The third concept is automation and real-time deployment, which centralises a control plane logically and adds customisable entities. This functionality allows for the development of advanced networking applications that improve network efficiency, administration, and management.

1. *Application plane:* The application or infrastructure plane consists of applications and services such as IDS, load balancer and DPI. These services help to perform decision-making in traffic engineering, routing, QoS differentiation and monitoring. The Northbound API allows applications to interact with the controller. This API may be implemented as either REST API or Java and Python APIs.
2. *Control plane:* The control plane manages core forwarding devices by making decisions based on global network information. The Northbound interface connects with the application plane to deliver critical information to apps. The controller converts the requirements of network applications that run on top of it into low-level flow rules communicated with SDN devices for deployment via the Southbound interface. The controller performs topology administration, which stores data about the connection of devices among end-users. It also performs flow management by managing the flows currently in the network to ensure effective synchronisation between SDN devices. Device management enabling is also done by the controller, which detects end-user and network elements that compose the network's infrastructure. A centralised controller is capable of handling massive quantities of network traffic. As the number of SDN devices and traffic flow rises, the controller may become a network bottleneck.
3. *Data plane:* This plane comprises network devices, commonly referred to as SDN devices, that are in charge of flow-rule-based packet forwarding. The control and data plane connection are accomplished using an open, vendor-independent Southbound interface. An SDN device's software and hardware elements can be used to define it further. The device employs OpenFlow as a Southbound interface and an abstraction for storing flow rule entries in flow tables. It also stores flow rules in either CAM or Ternary CAMs.

5 DDoS Attack in SDN

A distributed denial of service (DDoS) attack is a cyberattack where the attacker disrupts the services of the machine or the network. Attack traffic exhausts the system's resources, either temporarily or indefinitely. Consequently, systems are unable to provide service to the intended users. In DDoS attack, a malicious agent controls distributed systems to bring down the hosts. The increasing frequency of this attack is threatening the networks and needs to be addressed at the earliest. Identifying the source of DDoS attack and preventing the attackers from causing harm to the network is necessary. This has motivated the research industry to devise an efficient solution to eliminate DDoS attacks. Due to the disintegration of the SDN control plane and data plane, it has become easy for attackers to target any plane. Detecting the attack on these planes and mitigating them has become essential.

DDoS attack on data plane: The data plane of SDN consists of several forwarding devices (OpenFlow switches). Each switch consists of a flow table with a limited capacity for storing the rules. It lacks the processing ability to handle mismatched packets. The data plane has become vulnerable to intruders due to flow table overflow and buffer saturation.

DDoS attack on control plane: The control plane of SDN comprises a controller which controls the forwarding devices and makes routing decisions. As the controller manages the whole network, it is vulnerable to DDoS attacks. The attacker can affect the controller by overloading its network resources. The controller processes the unmatched packets and installs flow rules in the switches. This process involves all the controller resources, such as memory, buffer and CPU. If the controller remains busy for a significant period in processing the packets, then the network's performance is slowed down. This causes congestion in the network. As a result, legitimate users are denied services.

DDoS attack on application plane: The attackers can affect the application layer of SDN by launching application-layer DDoS attacks or exhausting northbound API. These attacks are caused by targeting the application by sending resource incentive requests. As a result of this attack, the web servers are affected. Examples of application-layer attacks are Slowloris and HTTP flooding attacks.

6 Description of Public Datasets

To detect DDoS attacks, a proper and standard SDN dataset is required. We have surveyed various public datasets for DDoS detection.

1. *KDD-CUP99 Dataset, 1999* [101, 215]: It is a well-known dataset commonly utilised in evaluating intrusion detection systems. This updated dataset version was created as part of an IDS initiative at MIT's Lincoln Laboratory in 1998 and 1999. The DARPA-funded programme resulted in the DARPA98 dataset. The KDD CUP 99 dataset was created by processing this dataset to be used in the International Knowledge Discovery and Data Mining Tools Competition. This dataset was generated using DARPA packet traces. The dataset in tcpdump format was collected over five weeks from a simulated military-like environment. It includes 41 traffic characteristics classified into three groups: content, fundamental, and traffic features. In addition to the standard statistics, the dataset provides four assault categories: DoS, User to Root (U2R), Remote to Local (R2L), and probe attacks. One challenge of the KDD'99 dataset is the presence of duplicate entries, which reached 78% in the training set and roughly 75 percent in the testing set. The significant degree of data redundancy makes it difficult for detection methods to provide high accuracy for low attacks: R2L and U2R. As a result, detection algorithms are skewed towards high-volume recordings, such as denial-of-service attacks.
2. *DARPA Dataset, 1999* [125]: Lincoln Laboratory developed the DARPA dataset on a simulation network for assessing the performance of intrusion detection systems in 1998 and 1999. It consisted of two parts: real-time evaluation and an offline examination. Offline testing of intrusion detection systems was performed using traffic on a network and audit records obtained on a simulated network. The systems analysed these data in batch mode, which tried to identify assault activities throughout routine operations. IRC, email, surfing, FTP, Telnet, and SNMP events are all included in this dataset. It includes Rootkit, remote FTP, DoS, Buffer overflow, Syn flood, and Nmap threats. This dataset somehow does not accurately depict genuine network traffic and has flaws, such as a lack of false positives. Furthermore, the dataset seems outdated for appropriate IDS assessment on current networks, including Internet infrastructure and attack types. Also, it lacks real assault datasets [34].
3. *Kyoto Dataset 2006+*: [214] The dataset was gathered via honeypot servers at Kyoto University. It comprises the actual network traffic from November 2006 to August 2009. Kyoto has 24 statistical characteristics, out of which 14 are shared with KDD dataset. Regular traffic was created alongside malicious traffic by establishing a second server in the same honeypot network to provide a more real dataset. As the traffic data was gathered via honeypot servers and the great majority of this data is malignant, the uneven class distribution of the dataset is regarded as the fundamental shortcoming of Kyoto 2006+. In addition, the attack types provided in the dataset are undocumented. When utilising this dataset, the inability to differentiate attack types leads to a biased image of intrusion detection performance. Furthermore, in Kyoto 2006+, regular traffic included only the email and DSN traces. The fraction of regular traffic in the sample, which ranges between 3 and 4% of the total, does not depict Internet activity. Furthermore, regular and malignant traffic was generated in two contexts, resulting in an artificial and uncorrelated dataset [83]. Despite the fact that Kyoto 2006+ dataset was created using real-world traffic information, it does not include any data on the attack types. Therefore, determining the effect of these attacks on SDN Internet infrastructure can be challenging.
4. *CAIDA DDoS2007* [36]: Cooperative Association of Internet Data Analysis developed three different datasets. Firstly, The CAIDA OC48 dataset [38] comprises various kinds of data witnessed over an OC48 link in San Jose over approximately 100 GB of unprocessed data traffic. Second, the CAIDA DDoS dataset consists of one hour of DDoS assault traffic split into five-minute pcap files. Finally, the 2016 CAIDA Internet traces dataset provides inert traffic evidence from CAIDA's Equinix-Chicago monitor via the fast Internet infrastructure. The vast bulk of CAIDA's datasets are tailored to specific attacks and are disguised with protocol data, payload, and destination. Due to various difficulties, they are inefficient benchmarking datasets [207].
5. *NSL-KDD Dataset, 2009* [226]: The NSL-KDD dataset is a revised form of the KDD'99 dataset built by Tavallaee et al. It was created to address certain inherent flaws with the KDD'99 dataset, like data redundancy. NSL-KDD is split into two sections: training and testing. Attack distribution in the test set is more significant than in the train set, with an estimated 17 assaults missing from the training dataset. Despite the fact that KDD'99 and NSL-KDD have been utilised in various intrusion detection studies, both datasets are unreal for representing present network traffic as they were developed 20 years ago and cannot reflect new attack patterns. In addition, the initial DARPA dataset was constructed using previous TCP protocol version. Using the outdated TCP version renders the header field IPv4 ToS obsolete, according to contemporary standards [145]. Aside from

the drawbacks of the KDD'99 and NSL KDD datasets for IDS evaluation, they also contain many irrelevant attributes to SDN networks. Some prior efforts [223, 224] used six of the 41 characteristics while implementing the NSL-KDD dataset in an SDN environment. Both studies concentrated on a subset of properties that may be obtained directly from the OpenFlow protocol. However, the classifier model's performance predicts a poor detection rate and a high FAR since the features cannot identify suspicious behaviour in hostile traffic. Furthermore, most previous attempts in SDN networks relied primarily on the KDD'99 and NSL-KDD datasets to detect DoS attacks. This is due to additional attack traffic, such as R2L and U2R, is contained in packet data, and content features are essential to detect these attacks. The content features, however, are not readily available via the OpenFlow protocol.

6. *ISCX2012 Dataset* [207]: Shiravi et al. generated data flow using two profiles based on simulated network. Alpha-profiles generate assault traffic, whereas Beta-profiles generate regular traffic. It covers network traffic for IMAP, SMTP, HTTP, SSH, FTP and POP3 protocols and their whole packet payload. The dataset includes 20 packet attributes of two network attacks: denial of service and brute force. However, the variety of DoS attack in data is somewhat restricted, and it does not address the vulnerability at multiple OSI layers. The dataset contains only HTTP traffic, which is not representative of actual traffic because the great majority of modern Internet traces are based on HTTPS traffic [206]. The number of features collected via the OpenFlow protocol, like the KDD'99 and NSL-KDD datasets, is inadequate for ML evaluation.
7. *Dataset by Alkasassbeh et al.* [15]: They developed a modern DDoS attack dataset having 21,60,668 records and 27 features. The dataset included HTTP, UDP, Smurf, and SiDDoS attacks. Several researchers have used their dataset to detect DDoS attacks in SDN environments using ML algorithms [194, 193].
8. *CICIDS 2017 Dataset* [206]: Sharafaldin et al. generated this dataset based on six attack profiles: Brute Force Attack, Web Attack, Botnet, Heartbleed Attack, DoS Attack, DDoS Attack, and Infiltration Attack. This dataset includes a variety of threat scenarios that earlier datasets did not. It also has the same quantity of recorded flow-based characteristics. Despite the fact that the CICIDS 2017 dataset is recognised as one of the most prominent datasets that enable many academics to design and test new models, it has various defects and challenges. The CICIDS 2017 dataset is based on ISCX2012, released in 2012. The total number of retrieved features represents the significant difference between the two datasets. The CICIDS 2017 dataset consists of 80 flow-based features, whereas ISCX2012 contains just 20 packet features. Furthermore, the HTTPS Beta profile was included in the CICIDS 2017 dataset to support the continued expansion of HTTPS use on the Internet. However, because of their inherent complexity, adopting the concept of profiling may be difficult [117]. Similarly, Panigrahi et al. identified several faults and defects in the CICIDS 2017 data [174]. The dataset has 288,602 empty class labels and 203 incomplete data pieces. Furthermore, the CICIDS 2017 dataset is massive and comprises several duplicate entries that appear redundant for any IDS training.
9. *CSE-CIC-IDS2018 Dataset* [43]: A cooperation between the Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity (CIC) resulted in the creation of the dataset. CICIDS 2018 was same as CICIDS 2017, with over 80 flow-based features retrieved from captured traffic via CICFlowMeter-V3. The profiles are used to produce the dataset methodically. This dataset comprises two broad classifications of profiles: B-profiles for regular traffic and M-profiles for irregular or assault traffic. The attack scenarios covered in this dataset are the same as those in the CICIDS 2017 dataset. However, the dataset faces same intrinsic flaws as CICIDS 2017.
10. *CIC DDoS 2019 Dataset* [39]: Canadian Institute for Cybersecurity developed DDoS attack dataset in 2019. CICDDoS2019 delivers regular and up-to-date common DDoS attacks close to real-world data (PCAPs). It also provides the findings of a network monitoring performed using CICFlowMeter-V3 that extracted 80 features apart from labelled flows. The features considered are the source and destination IPs, protocols, timestamp, source and destination ports, and type of attack. An abstract behaviour of 25 users was created for this dataset using the FTP, HTTP, SSH, HTTPS, and email protocols, including a variety of current DDoS assaults in this dataset, including LDAP, NTP, PortMap, MSSQL, NetBIOS, UDP-Lag UDP, SYN, SNMP, and DNS.
11. *SDNTrafficDS Dataset, 2019* [159]: Myint et al. proposed dataset for SDN traffic environment. UDP and SYN flood attacks have been collected along with normal traffic in their dataset from the OpenFlow switches over the OpenDaylight controller. Five features were extracted from the experimental SDN testbed.
12. *Kaggle DDoS 2019 Dataset* [67]: Several DDoS attack datasets generated by researchers are available on Kaggle publicly. One such DDoS dataset by Prasad et al. [67, 183] is generated by extracting flows from three publicly available open datasets of intrusion detection system by CIC Canada [96, 206]. The resultant DDoS

flows are combined with normal flows retrieved individually from the same dataset to construct a large dataset. The dataset contains 84 features of different DoS and DDoS attacks performed by various attack tools. Similarly, other DDoS attack datasets [123, 138, 241, 242] are also available for use by researchers in their work.

13. *InSDN Dataset, 2020* [71]: Elsayed et al. created an SDN-specific dataset to validate the intrusion detection system. It comprises the benign and diverse attack types which can arise in the SDN paradigm. Various attack tools were used to capture attack traffic for different threat classes like Exploitation, DDoS, Probe attacks, DoS, Password-Guessing, Web attacks, and Botnet. The dataset had over 80 characteristic features; 48 were extracted for the SDN environment. Usual traffic comprises DNS, Email, FTP, HTTP, SSH, and HTTPS, among other essential application services. Though this dataset addresses the concerns with existing freely accessible datasets, it is not intrinsic data and has not been tested on controllers other than the ONOS controller.

Discussion: From the publicly available datasets, it can be inferred that majority of the public datasets are traditional network datasets. SDNTrafficDS and InSDN are the only two SDN-based dataset available publicly. There is a lack of proper and standard SDN datasets. Applying ML algorithms to this dataset to detect DDoS attacks can prove fruitful to legitimate users in the real networking world. Traditional network datasets must be converted to flow-based for SDN networks. This may not always be helpful since the dataset may not precisely describe SDN behaviour during a DDoS attack. This is a significant disadvantage that has arisen as a challenge. Creating SDN-specific datasets is encouraged for better detection of DDoS attacks.

7 Analysis of Feature Selection Techniques

ML and DL methods have proved beneficial for DDoS attack detection. The literature presents numerous ML and DL solutions used by researchers for DDoS attack detection. According to continuing research to identify these assaults, there is no ideal technique for classification. The literature shows that SVM, ANN, SOM, LSTM, and NB models have performed better than other DDoS detection solution algorithms.

The datasets used for training the ML algorithms can contain many features. Not all the features contribute to DDoS attack detection. Some features may have no or just a little impact on the outcome. Having many features for detecting DDoS attacks can prove beneficial by providing higher accuracy, but it also increases the training time of ML algorithms.

Fig. 5 Filter-based feature selection method

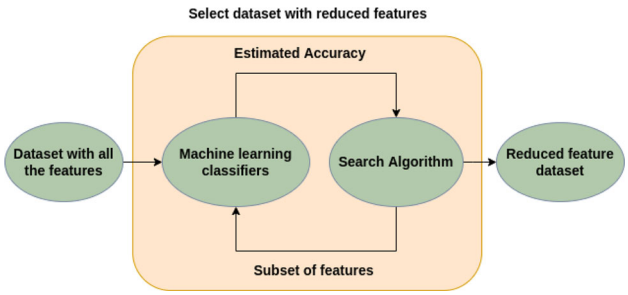

Fig. 6 Wrapper-based feature selection method

DDoS attacks can be detected with the best and optimal feature set. Increased time in detecting DDoS attacks is a disadvantage as it would cause much impact on legitimate users. Therefore, selecting the best features among a subset of features is highly necessary to detect attacks in less time without disrupting services to legitimate users. To select optimum features, Polat et al. [179] described three techniques: embedded, wrapper, and filter-based. Figures 5, 6, and 7 represent the three feature selection methods.

Filter-based method: The filter-based method focuses on the features' inherent properties. They serve as a preprocessing phase. Rather than ML algorithms, statistical techniques are used to choose the best features. Statistical experiments are used to select the best and fewest attributes. As model training is not required, filter-based techniques are quicker than other methods. The fisher score, information gain, variance threshold, correlation coefficient and chi-square test are all calculated using this method.

Wrapper-based method: The wrapper-based approach evaluates how the features will benefit the classifier's performance. The wrapper-based technique trains ML classifiers on a subset of features. The process is finished when an ideal subset of features is selected, and a dataset with fewer characteristics is created. In terms of time and speed, this model is computationally expensive. It has been proven to be more effective than statistical approaches. Backward and recursive feature removal and forward feature selection are two examples of wrapper-based feature selection algorithms.

Embedded based method: The embedded method enhances result prediction by combining the qualities of filter-based and wrapper-based methods. Each feature selection method is coupled with a different algorithm, which helps achieve the goals. Algorithms with built-in feature selection strategies implement it. The features are chosen by selecting those that improve the model's accuracy. It

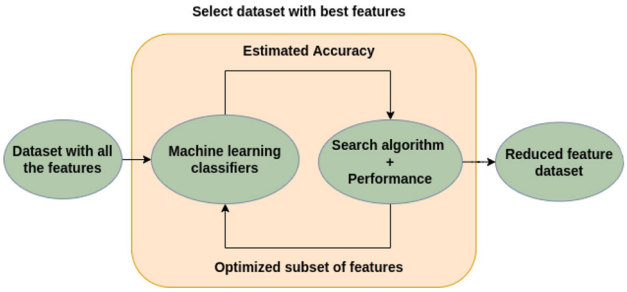

Fig. 7 Embedded-based feature selection method

performs feature selection and classification operations concurrently [155]. L1 (LASSO) regularisation and DT are two examples of this approach.

Discussion: Various researchers have used feature selection algorithms such as IG, PCA, genetic, greedy, and Chi-square test to obtain a reduced feature set. Table 5 presents the State-of-the-Art feature selection algorithms performed on a public dataset or self-generated dataset to select best features for DDoS attack detection. It can be inferred from the table that most of the researchers have used features from the public dataset for applying feature selection algorithms. In contrast, only two researchers have used self-generated SDN-based datasets. Applying feature selection algorithms on SDN-based datasets is essential in detecting DDoS attacks. As presented in Sect. 6, there is a dire need to generate SDN-based dataset due to its less availability. The challenge is to have the best feature set obtained from SDN-based dataset so that detection of DDoS attacks can be done in less time with higher accuracy. Therefore, generating an SDN-based dataset based on certain features and then applying feature selection algorithms to obtain the best and optimal feature set would prove beneficial to the researchers in detecting DDoS attacks. Detection features used by researchers for their work are presented in Table 6.

8 DDoS Detection Solutions Using Machine Learning

8.1 Supervised Machine Learning Solutions

ML algorithms for detecting DDoS attacks have been proven efficient by various researchers. This section analyses various supervised ML algorithms to detect DDoS attacks. Table 7 summarises the different supervised ML solutions for DDoS attack detection.

Kokila et al. [116] in their work used SVM classifier on DARPA [56] dataset for the detection of DDoS attacks. They compared their work with other NB, Bagging, RF, J48, and RBF classifiers and found that SVM gives high accuracy of 95.11% and a low FPR of 0.008. However, they have performed offline testing of their model. The performance of their work during online implementation cannot be predicted. Li et al. [130] also used SVM classifier in their work for detecting DDoS attacks. They improved their work by applying a genetic algorithm to SVM and obtained true negative of 0.35% and false negative of 0%. This was done to increase the performance, but the genetic algorithm learns quite slowly, prolonging the model's training period.

Meitei et al. [148] performed the detection of DNS amplification attacks using DT, MLP, NB, and SVM algorithms. DT performed best with high accuracy, true positive rate and FPR of 99.3%, all of the same value. Feature selection algorithms such as the Chi-Square test, IG, and GR are applied to obtain a reduced feature set of the dataset. It is observed that when ML algorithms are applied on a reduced set, then performance is slightly declined. Cui et al. [52] detected DDoS attack using neural network. They performed their experiment using a mininet emulator and RYU controller. Their model obtained CPU utilisation ratio of 5.5% and mean response time of 1 s, thereby decreasing the load on the controller. However, it was found that the TFN2K tool used to generate traffic is not in use nowadays. Similarly, Barki et al. [27] used NB, *K*-means, KNN, and K-medoids algorithms to identify DDoS attack traffic. NB performed best with high accuracy of 94%, but its training time is 11.8 s, which is higher than other algorithms.

A technique named FADM by Hu et al. [90] for protecting against DDoS attacks was presented. FADM exhibits high performance and lightweight qualities. Detection and mitigation by creating an application in the POX controller. The SDN controller analyses the network traffic data in FADM by the sFlow approach. The suggested method collects enough information to maintain the desired accuracy. For large traffic rates, it cannot acquire all of the information. The obtained data is used to extract network characteristics. The mitigation module is reliant on the migration of traffic and white-list. An entropy-based technique is used for assessing network characteristics, and SVM is used to detect DDoS assaults. Combining the suggested methodology with the other approaches can improve the responsiveness and efficiency of threat detection. The results of the experimental assessment show that their method can efficiently perform detection at a rate of 100%. Furthermore, FADM can restore the network in relatively less time. However, SYN flood attacks take longer to recover than other flooding attacks.

Meti et al. [149] used three ML methods, SVM, NB, and Neural network, to detect TCP SYN flood attacks. They calculated accuracy, precision, and recall for all three algorithms. SVM performed best with accuracy, precision and recall of 80%, all of the same value. However, their method demands high computation overhead at the controller. Chen et al. [45] developed an SDN-based detection method for

Table 5 Analysis of feature selection algorithms performed on dataset

Year and Refs.	Dataset used	No. of features	Feature selection algorithms	Reduced features for attack detection
2016, [148]	SimpleWeb [209], CAIDA [38]	8	IG, Gain Ratio, Chi-Square test	4
2017, [16]	NSL-KDD [226]	41	Genetic	16
			Ranker	17
			Greedy	11
			Proposed Algorithm	25
2018, [260]	KDD-Cup99 [101]	41	Based on OpenFlow characteristics	8
2018, [154]	NSL-KDD [226]	41	Genetic, Ranker, Greedy	25
2018, [126]	NSL-KDD [226]	41	PCA	9
2020, [137]	CIC-IDS2018 [43]	84	Chi-Square test	67
2021, [198]	Kaggle-DDoS attack network logs [241]	28	Chi-Square test	2
2021, [263]	CICDoS2017 [40], CICDDoS2019 [39]	20	PCA	15 of both datasets
2021, [229]	Dataset by [162]	22	NCA	14
2021, [99]	self-generated	7	ANOVA-F test	2
2021, [7]	self-generated	31	Genetic	11
2021, [180]	self-generated	42	Autoencoder	–
2021, [188]	KDD-Cup99 [101]	41	SMCA	9
2021, [120]	CICDDoS2019 [39]	84	Correlation coefficient	18
2022, [200]	InSDN [71], CIC-IDS2017 [41], CIC-IDS2018 [43]	48	IG, RF	10

DRDoS attack. The SDN controller is deployed with a detection module to detect the attack. This module includes a traffic surveillance tool as well as an ML classifier. Netmate tool collects network traffic, and SVM categorises traffic into malicious or benign. The classifier provides high accuracy of 99.99% in detecting the attacks. However, they did not discuss performance based on FPR and processing overhead. Similar work was done by Oo et al. [170] with the ASVM algorithm for detecting DDoS attacks. They tested their approach using hierarchical task analysis and obtained a quicker detection rate of 100% and low FAR of 0.65 compared to the SVM technique. They did not, however, test on SDN network.

Alshamrani et al. [16] proposed their best subset feature selection method for selecting a reduced feature subset of a dataset and compared the performance with other feature selection methods such as greedy, genetic, and Ranker's algorithm. Their method selected 25 features from NSL-KDD dataset, which had 41 features [226]. They detected DDoS attacks using three classification algorithms SMO, J48, and NB. SMO performed with high detection accuracy of 99.4% as compared to other algorithms. They also mitigated two new attacks: a newflow attack and a misbehaviour attack. However, the ease of use of the features is not considered in the SDN network.

Liu et al. [134] used a C-SVM classifier to detect IP spoofing by attackers and obtained an accuracy of 96.5%. The attack flows are dropped based on the IP address of the attacker or by observing their previous activity. However, in source spoofing, such IP-based source identification is ineffective. Similarly, Guozi et al. [79] used KNN for DDoS attacks and flash events detection. Their model performed with low FPR of 0.021 and high detection rate of 0.921 as compared to SVM algorithm. However, they considered only a few features for their detection, and their solution works with data that are not from the same network.

Yang and Zhao's [260] detected DDoS attacks using SVM classifier, and it was implemented as a DDoS detection module on the campus network's emulated SDN network. Their method produced an accuracy of 99.8%. However, the proposed system must be retrained when any new flow cannot be determined, which is time-consuming. Similarly, DDoS assaults (UDP, ICMP, HTTP, TCP and Smurf) were detected in SDN networks by Dayal and Srivastava [61] using the RBF-PSO approach. They detected attacks with reduced training time using a self-generated dataset. Claranet topology was used to generate the dataset comprising six features. They obtained 99.83% accuracy for their proposed approach.

Mohammed et al. [154] created a server application for the mitigation of SYN flood attacks. Their application consists

Table 6 Researchers' methods for spotting DDoS attacks include the following

Refs.	Features taken for detection
[90]	Source IP address, source port number, destination IP address, and destination port number entropy
[261]	The features include source IP addresses/unit time, source ports/unit time, flow packet standard deviation, flow byte standard deviation, flow entries/unit time, and interactive flow entry ratio to total flow entries
[147]	The features consist of entropy values for source IP address, source port number, destination IP address, packet type, and destination port number, along with the occurrence rate of packet types and the number of packets
[229]	The features encompass packets per flow, bytes per flow, packet rate, packet_in message count, total duration, bytes received on the switch port, bytes transferred from the switch port, packet count, total flow entries, data transfer rate, data receiving rate, port bandwidth, duration in seconds, byte count, switch ID, duration in nanoseconds, source IP, destination IP, port number, and monitoring interval
[187]	Total amount of packets received, total amount of bits, source port, destinations port, source IP address, destination IP address
[4]	datapath-id, source and destination IP addresses, packet and byte counts, duration in seconds, packetins, port number, and the number of bytes delivered on a particular switch port, Protocol, packet rate, A switch's overall number of flows duration—time during which the flow remains in the switch total duration—total sum of dur_sec and dur_nsec tx_kbps—kilobytes transferred per second rx_kbps—kilobytes received per second tot_kbps—bandwidth of a switch port Average Packet count per flow Average Byte count per flow Port bandwidth—sum of received bytes rx_bytes (r) and transmitted bytes tx_bytes (t)
[19]	The features include packet length, average bytes per flow, frames per second, flows per second, entropy of destination IP addresses per second, entropy of source IP addresses per second, entropy of IP protocol per second, packet variation in flow, packet count per source, and byte count per source

of three modules. The authorisation module verifies the controller's ability to submit requests to the server, the prediction module uses NB classifier to predict attacks, and the wrapper module implements wrappers in different programming languages. NSL-KDD dataset [226] was taken for training the NB classifier. They used three feature selection methods, genetic, greedy, and Ranker algorithms, to select optimal dataset features. They obtained 98% accuracy, precision and recall for their work. However, they did not mention the train and test split ratio taken for classification with the NB algorithm.

Sahoo et al. [194] applied seven ML classifiers, KNN, NB, LR, RF, DT, ANN, on the dataset created by Alkasassbeh et al. [15] for the prediction of UDP and ICMP flood attacks. Linear Regression performed well with high accuracy of 98.65% among the seven classifiers, while NB performed with 97.64% accuracy. However, better results could be obtained for UDP and Smurf attacks. Due to its high accuracy and detection rate, many researchers have widely used the SVM classifier over recent years to detect DDoS attacks on different datasets. The research works of [7, 14, 21, 45, 51, 90, 104, 118, 122, 124, 134, 147, 188, 193, 62, 249, 258, 260, 261] all have used SVM classifier in their work to detect DDoS attacks. Similarly, some researchers such as [69, 231, 230] have utilised the benefits of the KNN classifier for the detection of DDoS attacks and compared their performance with other classifiers.

Chen et al. [46] employed XGBoost classifier on KDD-CUP99 dataset [101] to detect flooding attacks. They compared the performance of the XGBoost classifier with other classifiers SVM, GBDT and RF. XGBoost outperforms all other classifiers with 98.53% accuracy, 11.07 s training time and false-positive rate of 0.008. Shafi et al. [203] used MLP, RNN and Alternate DT classifiers on the UNSW-NB15 [235] intrusion detection dataset for identification of attack. They performed their experiment on the RYU controller. For 1000 packets, collocated fog showed 0 packet delay compared to cloud network.

Myint Oo et al. [159], in their work, used the ASVM technique to detect malicious (UDP and SYN Flood) and normal flows in the network and obtained 97% accuracy. They created their testbed using Mininet and OpenDaylight controller and collected the traffic data, naming it SDNTrafficDS. Their work faired better with less training time of 50 s and testing time of 55 s, but they were threatened by bandwidth saturation.

The RYU controller was used to handle DDoS attack by Rahman et al. [186]. They employed the J48 classification method, directing the controller to block the specified port.

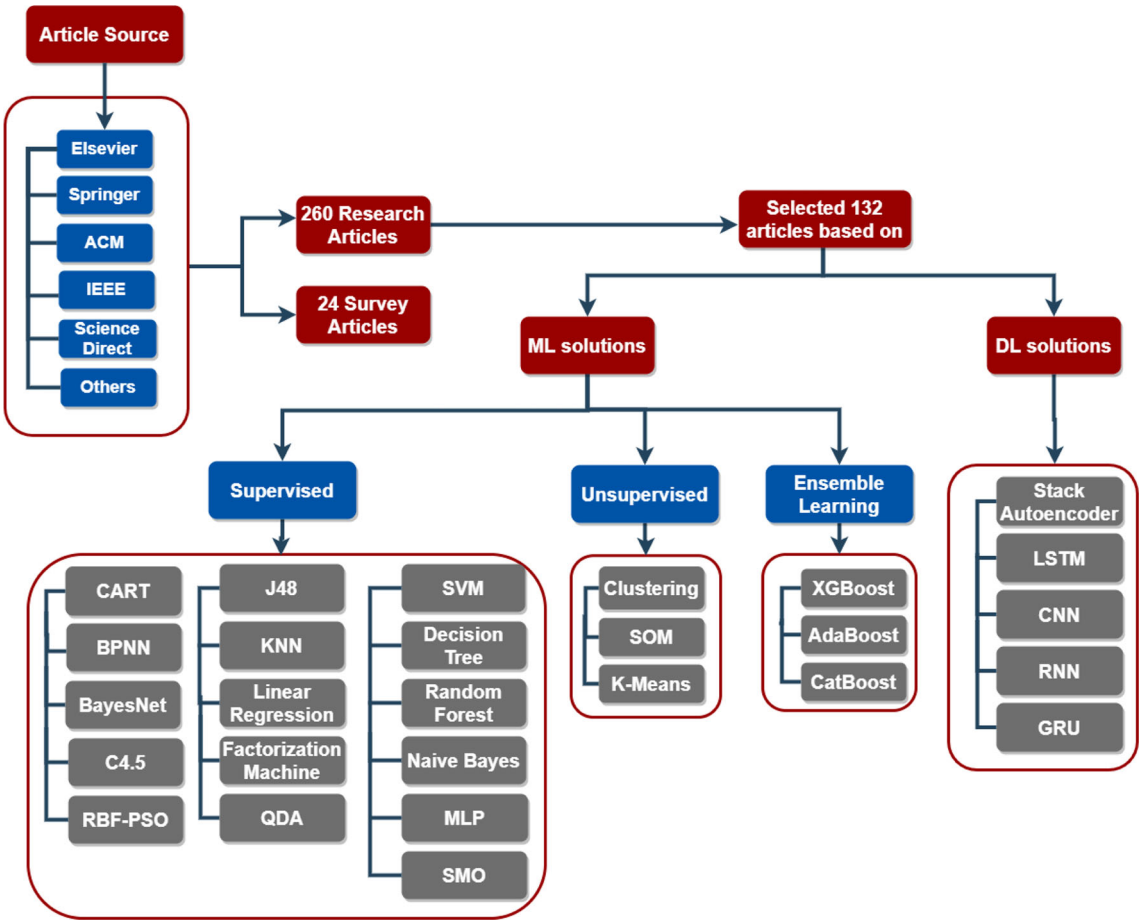

Fig. 8 Taxonomy of different ML and DL algorithms

J48 obtained an accuracy of 100% when compared to other classifiers. However, the port is disabled for only 30 s making the network vulnerable. Furthermore, the time necessary to identify attacks has increased, adding to the system's complexity.

Santos et al. [199] designed an SDN testbed for generating attack traffic for assessing the efficacy of multiple ML algorithms, including RF, SVM, DT, and MLP. To simulate the SDN network, Mininet and POX controller were utilised. Best results are obtained with RF achieving high accuracy of 100%, and less processing time of 10 s is obtained with DT in detecting bandwidth attack, controller attack, and flow-table attack. Similarly, Perez-Diaz et al. [175] tackled low rate DDoS attack in SDN environment. They trained IDS using ML algorithms J48, REP tree, MLP, RF, SVM and RT. They used the Mininet emulator and ONOS controller to perform their experiment on the CICDoS2017 dataset [40]. MLP algorithm performed best with an accuracy of 95%.

Polat et al. [179] performed DDoS attack detection using NB, KNN, SVM and ANN algorithms. They chose the best features from a set of 12 using three feature selection strategies: filter, wrapper and embedded-based techniques. They achieved the highest accuracy of 98.3% with the wrapper-based feature selection strategy and the KNN classifier. However, testing time evaluation of the algorithms in relation to obtained accuracy was not done by them.

Luong et al. [137] performed detection of DDoS attacks using SVM, NB, DT, RF classifiers and deep neural network. They used the Chi-Square test feature selection method for selecting 67 features out of 84 features of the CIC-IDS2018 dataset [43]. However, more feature selection methods could be performed to get the best feature dataset. DT gave an accuracy of 99.97% but during the simulation, DT was unable to detect abnormal traffic. The results obtained by SVM and DNN outperform other classifiers during simulation in detecting attack traffic. Similar work was performed by Cheng et al. [47] for DDoS attack detection using RF, NB, SVM and KNN classifiers. RF classifier performed best with accuracy of 91%, precision of 95%, recall of 94% and f1-score of 94%.

Work by Abou El Houda et al. [2] detects and mitigates DNS amplification attack using Bayes classifier effectively with high detection rate of 100%, less FPR of 21%, and low

Table 7 Supervised machine learning solutions for DDoS attack detection in SDN

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
1	Kokila et al. [116]	Control	DARPA [56]	SVM	Detection	Accuracy, FPR, Training time
2	Mihai-Gabriel and Victor-Valeriu [151]	Data	Self-generated	BPNN	Mitigation	Risk assessment
3	Li et al. [130]	–	DARPA-IDS [55]	SVM	Detection	True Negative, False Negative
4	Meitei et al. [148]	Data	SimpleWeb [209], CAIDA [38]	DT, MLP, NB, SVM	Detection	Accuracy, TPR, FPR
5	Cui et al. [52]	Data	Self-generated	BPNN	Detection, Mitigation	Response time, utilisation ratio, network load
6	Barki et al. [27]	Data	Self-generated	NB, *K*-means, KNN, K-medoids	Detection	Detection rate, Processing time
7	Wang et al. [249]	Data	KDD1999 [101]	SVM	Detection, Mitigation	Accuracy
8	da Silva et al. [62]	Data	Self-generated	SVM	Detection, Mitigation	Accuracy, Processing time, *F*-measure, Sensitivity, Specificity
9	Nanda et al. [161]	Data	LongTail [136]	C4.5, BayesNet, DT, NB	Detection	Accuracy
10	Hu et al. [90]	Data	Self-generated	SVM	Detection, Mitigation	Detection rate, FAR
11	Meti et al. [149]	Data	Public dataset	SVM, NB, Neural Network	Detection	Accuracy, Precision, Recall
12	Chen et al. [45]	Data	Self-generated	SVM	Detection	Accuracy, Detection time
13	Oo et al. [170]	–	Self-generated	ASVM	Detection	FAR, Detection rate, Training and Testing time
14	Alshamrani et al. [16]	Data	NSL-KDD [226]	SMO, J48, NB	Detection, Mitigation	Precision, Recall, *F*1 score
15	Liu et al. [134]	–	DARPA 1999 [125], CAIDA 2007 [36]	SVM	Detection	Accuracy
16	He et al. [88]	Data	KDDCUP99 [101]	SVM, DT, RF, Extra Trees, AdaBoost	Detection, Mitigation	Accuracy
17	Gharvirian and Bohlooli [78]	Data	Self-generated	NN	Detection	Accuracy, Detection rate, FAR
18	Guozi et al. [79]	Data	Self-generated	KNN	Detection	TPR, FPR, *F*1 Score
19	Yang and Zhao [260]	Data	KDDCUP99 [101]	SVM	Detection	Accuracy
20	Dayal and Srivastava, [61]	Data	Self-generated	RBF-PSO	Detection, Mitigation	Network load
21	Mohammed et al. [154]	Data	NSL-KDD [226]	NB	Detection, Mitigation	Precision, Recall, *F*1 Score, CPU usage
22	Sahoo et al. [194]	Data	Dataset by Alkasassbeh et al. [15]	KNN, NB, SVM, LR, RF, DT, ANN	Detection	Accuracy, Precision, Recall
23	Ye et al. [261]	Data	Self-generated	SVM	Detection	Detection rate, FAR

Table 7 (continued)

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
24	Chen et al. [46]	Data	KDDCUP99 [101]	XGBoost	Detection	Accuracy, FPR, Training time
25	Gao et al. [77]	Data	DARPA IDS [55]	Bayesian network	Detection, Mitigation	CPU usage, Accuracy
26	Cui et al. [53]	Data	–	BPNN	Detection	Accuracy, Recall
27	Prakash and Priyadarshini [182]	Data	Self-generated	NB, KNN, SVM	Detection	Accuracy, Precision, Recall, *F*-score
28	Singh et al. [212]	Data	Self-generated	SVM, DT, Gradient boosting, RF, KNN, LR, NB, NN	Detection	Accuracy, TPR, FPR
29	Latah and Toker [126]	Data	NSL-KDD [226]	DT, ELM, NB, LDA, NN, SVM, RF, KNN, AdaBoost, RUSBoost, LogitBoost, BaggingTrees	Detection	Accuracy, FAR, Precision, Recall, *F*-measure, Execution time, McNemar's test
30	Shafi et al. [203]	Data	UNSW-NB15 [235]	MLP, RNN, DT	Detection, Mitigation	Network delay, Throughput, Fairness
31	Myint Oo et al. [159]	Data	SDNTrafficDS [159]	ASVM	Detection	FAR, Detection rate, Accuracy
32	Rahman et al. [186]	Data	Self-generated	J48, RF, SVM, KNN	Detection, Mitigation	Accuracy, Specificity, Sensitivity, Kappa, Precision, Recall, *F*1 Score, Training and Testing time
33	Dong and Sarem [69]	Data	Self-generated	KNN	Detection	TPR, FPR, Precision, Recall, *F*1 Score
34	Cui et al. [51]	Data	CAIDA DDoS [36]	SVM	Detection	Detection rate, FPR
35	Tuan et al. [231]	Data	CAIDA DDoS [36]	KNN	Detection, Mitigation	Accuracy, Precision, Recall, *F*1 Score
36	Mehr and Ramamurthy [147]	–	Self-generated	SVM	Detection, Mitigation	Throughput
37	Wang et al. [244]	Control	Self-generated	BPNN	Detection, Mitigation	Controller response time, Flow setup time, CPU usage rate
38	Liu et al. [133]	Data	Self-generated	NN	Detection	FAR, Detection rate
39	Zhijun et al. [267]	Data	CAIDA DDoS [36]	Factorisation Machine	Detection	Accuracy, Precision, Recall, Training time
40	Santos et al. [199]	Data	Self-generated	SVM, MLP, DT, RF	Detection, Mitigation	Accuracy, Processing time
41	Perez-Diaz et al. [175]	Data	CICDoS2017 [40]	J48, MLP, SVM, RF, REP Tree, RT	Detection, Mitigation	Accuracy, Recall, Precision, *F*-measure, FAR

Table 7 (continued)

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
42	Polat et al. [179]	Data	Self-generated	SVM, KNN, NB, ANN	Detection	Accuracy, Sensitivity, Specificity, Precision, $F1$ Score
43	Tuan et al. [230]	Data	Self-generated	KNN	Detection, Mitigation	Accuracy, Precision, Recall, $F1$ Score
44	Kumar Singh [122]	Data	Self-generated	SVM	Detection, Mitigation	Accuracy, Detection rate
45	Luong et al. [137]	Data	CIC-IDS2018 [43]	SVM, NB, DT, RF, DNN	Detection, Mitigation	Accuracy, Precision, Recall, $F1$ Score
46	Kyaw et al. [124]	Data	KDD-CUP99 [101]	SVM	Detection	Accuracy, FAR, Detection rate, Precision
47	Cheng et al. [47]	Data	Self-generated	RF, SVM, KNN	Detection	Accuracy, Precision, Recall, $F1$ Score
48	Ali et al. [14]	–	DARPA [54, 56]	SVM	Detection	Accuracy, Training time, FPR
49	Aslam et al. [21]	–	Environment-specific dataset	SVM	Detection, Mitigation	Accuracy, $F1$ Score
50	Sahoo et al. [193]	Data	Dataset by Alkasassbeh et al. [15]	SVM	Detection, Mitigation	Accuracy, Precision, Recall
51	Abou El Houda et al. [2]	Data	Self-generated	Bayes Network	Detection, Mitigation	Detection rate, FPR
52	Le et al. [127]	Data	Self-generated	RF, DT, NB, SVM, MLP, KNN	Detection	Accuracy, Processing time
53	Musumeci et al. [157]	Data	Self-generated	RF, KNN, SVM	Detection	Accuracy, Testing time, Training time
54	Shohani and Mostafavi [208]	Data	Public dataset	LR	Detection	Entropy
55	Hannache and Batouche [87]	Data	Self-generated	NN	Detection, Mitigation	Accuracy, Recall, Precision, F-score
56	Dehkordi et al. [66]	Data	CIC-IDS2017 [41], CTU-13 [42], ISOT [92]	BayesNet, J48, RT, LR, REPTree	Detection	Accuracy, Precision, Recall, $F1$ Score, TPR, FPR
57	Yungaicela-Naula et al. [263]	Data	CIC-DoS2017 [40], CIC-DDoS2019 [39]	SVM, KNN, RF	Detection	Accuracy, Precision, Recall, $F1$ Score
58	Sanjeetha et al. [198]	Data	Kaggle-DDoS attack network logs [241]	Catboost, XGBoost, LR, GNB, DT	Detection, Mitigation	Accuracy, Precision, Recall, Training time
59	Jose et al. [99]	Data	Self-generated	LR, NB, LDA, KNN, RF, SVM	Detection	Accuracy, Recall, Precision, $F1$ score
60	Sangodoyin et al. [197]	Data	Self-generated	GNB, QDA, k-NN, CART	Detection	Accuracy, Recall, Training time
61	Khashab et al. [111]	Data	Self-generated	SVM, LR, KNN, DT, NB, RF	Detection, Mitigation	Accuracy, Recall, Specificity, Precision

Table 7 (continued)

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
62	Ahuja et al. [4]	Data	Self-generated	SVC-RF	Detection	Accuracy, Sensitivity, Specificity, Precision, $F1$-score
63	Banerjee and Chakraborty [25]	Data	Kaggle dataset [67]	NB, KNN, K-means, Linear Regression	Detection, Mitigation	Efficiency
64	Tan et al. [222]	Data	Self-generated	RF	Detection, Mitigation	Accuracy, Detection rate, FAR
65	Swami et al. [220]	Data	Self-generated	DT, RF, AdaBoost, MLP, LR	Detection	Accuracy, Precision, Recall, $F1$ Score, FPR
66	Pradeepa and Pushpalatha [181]	Data	Self-generated	CAD, SAE, SVM	Detection, Mitigation	Accuracy
67	Gadallah et al. [75]	–	Self-generated	SVM, NB, KNN, DT, RF	Detection, Mitigation	Accuracy, Recall, $F1$ Score, FPR, Precision
68	Tonkal et al. [229]	Data	Dataset by Nisha Ahuja [162]	KNN, DT, ANN, SVM	Detection	Accuracy, Sensitivity, Specificity, Precision, $F1$ Score
69	Yadav et al. [258]	Data, Control	Self-generated	SVM	Detection, Mitigation	Accuracy
70	Kotb et al. [118]	Data	Self-generated	SVM	Detection	Delay, Bandwidth, Accuracy
71	Tayfour and Marsono [227]	Data	InSDN2020 [71], CICIDS2017 [41], NSL-KDD [226], UNSW-NB15 [235]	Ensemble of NB, KNN, DT, ET	Detection, Mitigation	Accuracy, Precision, Recall, TPR, FPR, $F1$ Score
72	Nurwarsito and Nadhif [169]	Data	Self-generated	RF	Detection, Mitigation	CPU usage, Accuracy, FPR, Detection time, Mitigation time
73	Revathi et al. [188]	Data	KDDCUP99 [101]	SVM	Detection, Mitigation	Accuracy, Precision, Recall, F-measure
74	Aslam et al. [20]	Data	Environment specific dataset	SVM, NB, KNN, RF, LR, Ensemble voting	Detection, Mitigation	Accuracy, Precision, Recall, F-measure
75	Khedr et al. [112]	Data	Edge-IIoTset [73]	SVM, GNB, KNN, RF, DT, Binomial LR	Detection, Mitigation	Accuracy, Recall, F-measure

overhead. However, their method collects a significant quantity of recurring and normal traffic. The sampling strategy may overlook vital traffic data, leading to late detection and reaction to an assault. Dehkordi et al. [66] deployed ML algorithms such as BayesNet, REP tree and RT on ISOT [92], UNB-ISCX [235] and CTU-13 [42] datasets to detect DDoS attacks. Their proposed method gave highest accuracy of 99.12% on CTU-13 dataset.

Yungaicela-Naula et al. [263] in their work used supervised ML classification algorithms such as SVM, RF, and KNN and DL algorithms to detect application layer and transport layer DDoS attacks. Their experiment was carried out using an ONOS controller and a Mininet emulator. They worked on the CICDoS2017 [40] and CICDDoS2019 [39] datasets containing 76 features. The ML models gave an accuracy of more than 90%, and DL models gave an accuracy

of around 98% for both datasets. However, their work did not perform better when the network topology was modified.

Sanjeetha et al. [198] proposed a detection and mitigation application on the RYU controller to tackle UDP flood attacks. They considered two features, packet_rate and byte_rate after the feature extraction process from Kaggle-DDoS attack network logs [241] dataset containing 26 features. The detection was performed using several ML algorithms, out of which CatBoost algorithms performed better with 98% accuracy and training time of 119 s. However, the two features taken do not qualify for attack detection as more features can affect the performance. Their experiment performs for only RYU controller and UDP flood attack. The results might change when the controller and attack are changed.

Jose et al. [99] performed feature selection method by ANOVA-F test method on seven features to choose the two best features for DDoS detection using LR, NB, LDA, KNN, SVM, and RF classifiers on their own generated SDN dataset. The results obtained by SVM and LDA outperform other classifiers in detecting DDoS attacks with an accuracy of 99.98% and 99.87%, respectively. However, only two features selected alone do not qualify for detecting DDoS attacks. Similarly, Sangodoyin et al. [197] also detected DDoS attacks using GNB, CART, QDA and KNN classifiers. CART algorithm performs best in terms of 98% accuracy and 12.4 ms training time in detecting attacks. However, feature selection methods could have been used for better results. Prakash and Priyadarshini [182], Le et al. [127] and Khashab et al. [111] also used supervised ML algorithms such as KNN, LR, SVM, DT, RF and NB classifiers for the detection of DDoS attack. They performed their work on a self-generated dataset.

Ahuja et al. [4] detected DDoS attacks by proposing a hybrid ML model of SVM and RF classifiers (SVC-RF). They created their SDN traffic dataset containing 23 features to identify the traffic. The proposed method performs with high accuracy of above 98% and less FPR of 0.020. Banerjee and Chakraborty [25] also proposed IDS to identify attackers using NB, K-means clustering, KNN and Linear regression algorithms. KNN performs best with high detection rate of 96.65%.

Tayfour and Marsono [227] used a voting classifier to create an ensemble of NB, KNN, DT, and ET for DDoS attacks detection on four publicly available datasets [71, 206, 226, 235]. They also performed simulations on SDN traffic using mininet and RYU controller and evaluated the results. They used Redis Simple Message Queue (RSMQ) technique to minimise the load on a single controller and increase detection and mitigation performance on multi-controllers. ET classifier obtained high TPR of 0.985 and low FPR of 0.008 compared to other classifiers. However, they did not use feature selection methods to reduce the features of four datasets taken to increase detection accuracy.

Swami et al. [220] identified TCP-SYN flood attacks on their self-generated dataset. LR, DT, MLP, RF and AdaBoost algorithms were used in their work. At different traffic rates, the impact of the assault on the controller's CPU was investigated. The findings revealed that the packet arrival rate was closely related to the controller's CPU use. The proposed methodology achieved 0% FPR with 99.9% accuracy.

Gadallah et al. [75] proposed a detection and mitigation mechanism for detecting a DDoS attack. The model was trained using the kernel radial basis function of SVM classifier. The results were compared with other classifiers NB, KNN, DT, and RF and the results showed that SVM performed best among with 99.84% accuracy and false-positive rate of 0.21. The authors collect attack traffic using the Scapy tool but have not performed results on any particular DDoS attack apart from IP spoofing.

Tonkal et al. [229] used KNN, DT, SVM, and ANN classifiers to detect ICMP, UDP and TCP flooding attacks. SDN dataset generated by [162] was used in their work. The results demonstrate that DT outperforms the others with 99.82% accuracy. They utilised the NCA method to choose 14 features from a dataset of 22 features. The experiment, however, might be carried out with various attacks.

To identify flooding attacks, Kotb et al. [118] introduced SGuard (secure guard). They employed a five-tuple feature with an SVM classifier to categorise attack traffic and obtained average accuracy of around 99%. Another work by Pradeepa and Pushpalatha [181] used Intelligent Proactive Routing (IPR) model for the detection and mitigation of UDP flood and SYN flood attacks. They compared their model's performance to that of other detection models such as SVM, CUSUM abnormal Detection (CAD) and Stacked Autoencoder (SAE). The IPR model performed with less detection time and obtained an accuracy of 99% compared to SAE, SVM and CAD. Aslam et al. [20] utilised SVM, NB, RF, KNN, LR and ensemble voting classifiers in their proposed framework to detect DDoS attack on an environment specific dataset. Ensemble voting classifier fared best with accuracy of 98.5%, precision of 98%, f-score of 95% and recall of 96.5% for 30,000 test flows. Khedr et al. [112] detected DDoS attack on Edge-IIoTset [73] dataset using SVM, KNN, Binomial LR, GNB, DT and RF classifiers. RF performed best with 99.79% accuracy, 99.77% recall and 99.43% f-score. They performed their experiment on IoT network topology and POX controller.

Discussion: The research works of the past 8 years listed in this section employs supervised algorithms mainly SVM, KNN, MLP, NB, RF, DT, ANN, K-means, J48, RBF-PSO, AdaBoost, ET, XGBoost, LR, and Gradient Boosting to detect DDoS attack in SDN networks. It is observed that

SVM has been applied by most of the researchers while during result analysis MLP and RF outperformed other algorithms in detecting DDoS attacks. It is also observed that most of the researchers focused only on accuracy for result analysis. Very few research works have done testing time analysis of DDoS attacks. Some of the research works perform offline testing on publicly available datasets such as CAIDA, DARPA, KDD-CUP99, LongTail, SimpleWeb, UNSW-NB15, SDNTrafficDS, CICDoS2017, CICIDS2018, CTU-13, CICDDoS2019, Kaggle, InSDN, and CICIDS2017 to perform detection using ML algorithms. Due to the lack of standard datasets available for SDN networks, many researchers have generated their datasets and performed detection using ML algorithms. Figure 8 gives a comprehensive insight into the distribution of different ML and DL algorithms considered in this survey.

8.2 Unsupervised Machine Learning Solutions

Lee et al. [128] detected DDoS attacks using hierarchical cluster analysis. They used DARPA 2000 intrusion detection dataset [56] for their work and identified six clusters considering nine features. Their proposed clustering outcome is dependent on the initial working feature vector, which cannot be altered throughout the clustering process after it has been calculated. In reality, each feature's contribution to the clustering outcome may differ, and there may be a mutual effect among the characteristics. In response to a specific DDoS assault, if the functional feature vector is optimised by deleting repeated features, the potential disruption among features is avoided, and the performance of the clustering method is increased by lowering dimensionality and eliminating unnecessary data.

Braga et al. [32] used a popular method known as self-organising Maps for DDoS attacks detection in the NOX controller SDN environment. They have collected six traffic flow features using the flow collector module. A flow collector module collects the characteristics and then provides them to the classifier module to identify fraudulent flows. For flow analysis, a self-organising map is employed. The approach incurs negligible overhead compared to conventional alternatives since it takes advantage of SDN's potential for software-based traffic monitoring. Nonetheless, this study reveals that DDoS assaults may be detected with high detection rate of 98.61% and low FAR of 0.59. Furthermore, the flow collector module overlooked the controller overhead produced by accumulating the flow table entries for each switch. Similarly, Xu and Liu, 2016 [257] also used self-organising Maps to detect DDoS attack.

Ahmed et al. [3] proposed the Dirichlet process mixture model clustering method for distinguishing between normal and malicious DDoS traffic for mitigating DNS amplification attacks. They compared their work with the traditional mean shift-based method and proved that their method was effective in mitigating DNS-based DDoS attacks. However, they obtained an accuracy of 75%. Similarly, Nam et al. [160] used self-organising maps and KNN for DDoS attacks detection. They experimented on CAIDA DDoS 2007 [36] dataset and POX controller. SOM performed better in their work with low processing time of 0.004 ms.

KMeans++ and fast K-nearest neighbours were used to develop a detecting system named K-FKNN in the RYU controller by Xu et al. [254]. K-FKNN algorithm yields high precision of 97% compared to other algorithms. The results of their experiments reveal that their proposed approach is successful and that detection is quite stable. However, classifying and detecting the attack takes a long time, placing a heavy burden on the SDN resources. Similarly, AlMomin and Ibrahim [8] and Ramprasath and Seethalakshmi [187] used combination of two techniques to detect DDoS attacks. The former work uses entropy-PCA, while the latter uses the PSO-ACO technique and obtained 85% precision. They have compared their work with other ML algorithms and found that their work effectively detected and mitigated DDoS attacks compared to other works.

Polat et al. [180] applied ensemble model of softmax classifier and stacked sparse autoencoder (SSAE) to detect DDoS attack on SDN-based VANETs. Using the SUMO simulator, they performed their experiment on a POX controller and generated vehicular topology. They compared their results with SVM, KNN and DT classifiers and found that four-layer SSAE-Softmax classifiers yield better results with 96.9% accuracy than the remaining classifiers. Similarly Scaranti et al. [201] detected DDoS attacks using clustering approach by simulating 48 datasets. Their experiment yielded f-measure of 99.6%.

Table 8 summarises the unsupervised ML solutions for DDoS attack detection.

Discussion: It is observed that compared to supervised ML algorithms, unsupervised ML algorithms are emerging slowly in detecting DDoS attacks. From the year 2008 to 2023 we have listed 12 works of researchers that have applied SOM, graph-based clustering, entropy-PCA, SSAE, and PSO-ACO on either self-generated datasets or public datasets such as DARPA, ISCX2012, CTU-13, CAIDA, and NSL-KDD to detect DDoS attack in SDN environment.

8.3 Ensemble Machine Learning Solutions

Many researchers have used a combination of supervised and unsupervised ML techniques or two or more supervised ML techniques to detect DDoS attacks. Table 9 presents the ensemble ML solutions for DDoS attack detection in SDN.

Deepa et al. [64] designed a hybrid ML technique to safeguard the network against DDoS attacks. Their hybrid approach outperforms simple ML models in terms of high

Table 8 Unsupervised machine learning solutions for DDoS attack detection in SDN

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
1	Lee et al. [128]	Data	DARPA [56]	Cluster Analysis	Detection	Partitioning of cluster
2	Braga et al. [32]	Data	Self-generated	SOM	Detection	Detection rate, FAR
3	Xu and Liu [257]	Data	Self-generated	SOM	Detection	Accuracy
4	Ahmed et al. [3]	Data	ISCX2012 [207]	Clustering	Detection, Mitigation	Accuracy
5	Chowdhury et al. [48]	Data	CTU-13 [42]	Graph-based clustering	Detection	Bot detection
6	Nam et al. [160]	Data	CAIDA DDoS 2007 [36]	SOM, KNN	Detection, Mitigation	FPR, Detection rate, Processing time
7	Xu et al. [254]	Data	NSL-KDD [226]	*K*-Means++, K-FKNN	Detection, Mitigation	Precision, Recall, *F*-measure, Detection time
8	AlMomin and Ibrahim [8]	Data	Self-generated	Entropy-PCA	Detection	Accuracy
9	Ramprasath and Seethalakshmi [187]	Data	Self-generated	PSO-ACO	Detection, Mitigation	Precision, Recall, *F*-measure, FPR
10	Polat et al. [180]	Data	Self-generated	SSAE-Softmax	Detection	Accuracy, Sensitivity, Specificity, Precision, *F*-measure
11	Zhao et al. [265]	–	DDoS Attack 2007 [36]	SOM	Detection	Accuracy, Processing time
12	Scaranti et al. [201]	Data	Self-generated	Clustering	Detection	Accuracy, Recall, Precision, *F*-measure

accuracy of 96.77%, low FAR of 0.032%, and high detection rate of 90.45%. They used SVM and Self-Organising Maps. By routing traffic through the SOM module, their model identified the attacks. To identify new sorts of assaults, traffic from the SVM module is sent again via the SOM module. When an attack is detected, the individual connection is terminated, and the table's rules are modified.

Singh and Jayakumar [213] developed an ML-based "twin security model" that combines different information to achieve security in terms of DDoS attack detection in SDN. The detection is accomplished by combining SOM with an NB classifier, which forecasts attacks based on features. Kaur and Gupta [108] also employed Bayesian Network, Wavelets, SVM, and KNN. In comparison to the previous KNN technique, they suggested a unique hybrid strategy that employed artificial neural networks and SVM to mitigate these threats with better precision. The KDDCUP99 data [101] examined the clustered real-time data for the normal and abnormal flow. The average was determined to monitor the accuracy of the packet flow, and the growing complexity proved to be an ideal strategy that could be used even with noisy data. On the KDD dataset, it employs parameters such as accuracy, time duration, packet flow, and precision rate.

Deepa et al. [65] suggested an ensemble technique for detecting abnormal network traffic behaviour in the SDN controller. SOM, NB, KNN and SVM are used in the ensemble to improve efficiency. They used Mininet to validate their

Table 9 Ensemble Machine Learning solutions for DDoS attack detection in SDN

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
1	Deepa et al. [64]	Data	Self-generated	SVM, SOM	Detection	Accuracy, FAR, Detection rate
2	Singh and Jayakumar [213]	Data	Self-generated	SOM, NB	Detection	–
3	Kaur and Gupta [108]	Data	KDDCUP99 [101]	SVM, ANN	Detection	Accuracy, Precision
4	Deepa et al. [65]	Data	CAIDA [37]	KNN-SOM, NB-SOM, SVM-SOM	Detection	Accuracy, Detection rate, FAR
5	Phan and Park [176]	Data	CAIDA [37]	SVM-SOM	Detection, Mitigation	Accuracy, Detection rate, FAR
6	Firdaus et al. [74]	Data	InSDN [71]	*K*-Means++, RF	Detection	Accuracy, Precision, Recall, *F*-measure
7	Sen et al. [202]	Data	Self-generated	AdaBoost	Detection	Accuracy, Precision, Recall, *F*-measure
8	Tan et al. [221]	Data	NSL-KDD [226]	*K*-Means-KNN	Detection	Accuracy, Precision, Recall, FAR
9	Swami et al. [219]	Data	UNSW-NB15 [235], CICIDS2017 [41], NSL-KDD [226]	Voting-CMN, Voting-RKM, Voting-CKM	Detection	Accuracy, Precision, Recall, *F*-measure
10	Ahuja et al. [4]	Data	Self-generated	SVM-RFC	Detection	Accuracy, Precision, FAR, Specificity, *F*-measure
11	Tufa et al. [232]	Data	Self-generated	AdaBoost	Detection	Accuracy, Detection rate, FPR
12	Wang and Wang [245]	Data	CIC-IDS2017 [41], InSDN [71]	CNN-ELM	Detection, Mitigation	Accuracy

technique. The authors integrated SVM-SOM, KNN-SOM, and NB-SOM and discovered that SVM-SOM had a greater accuracy of 98.14% and detection rate of 97.14%.

Phan et al. [176] created a one-of-a-kind DDoS assault defender that uses a hybrid ML approach and an upgraded History-based IP Filtering (eHIPF) technique rather than HIPF to enhance detection accuracy and traffic categorisation speed. As eHIPF initiates a threat, the mitigation system sends a flow mod signal with a drop action, causing all packets at the cloud's edge to be dropped. They put up an experimental setting on the laboratory network to test their method.

Firdaus et al. [74] also developed ensemble ML approaches for DDoS attack detection. They suggested a KMeans++ and RF ensemble to identify DDoS attacks on the InSDN dataset [71]. Their results achieved 100% accuracy. Another work by Sen et al. [202] employed the Adaboost algorithm to identify DDoS attacks in an SDN context. When compared against J48, BayesNet, NB, MLP, SVM, and RF classifiers, the AdaBoost method fared best in good accuracy of 93% and low FPR.

By integrating KMeans with KNN Tan et al. [221] developed a DDoS detection system. It constituted a training data processing module based on KMeans and a traffic detection module based on KNN. The traffic is classified as malignant or benign based on the labels of the k points nearest to the measured instance. The simulation results suggest that their strategy outperformed the entropy approach and distributed SOM with precision of 99.03%, recall of 98.35% and FAR of 1.27%.

Ahuja et al. [4] developed the SDN dataset with the required characteristics for identifying attack traffic. The controller constructs the dataset by collecting port and flow information from OpenFlow switches and then applies a hybrid ML approach SVM-RF to discriminate between legitimate and malignant traffic. The suggested approach achieves excellent accuracy (98.8%) while having a low false-positive rate (0.020).

Wang and Wang [245] employed hybrid CNN-ELM model to detect and mitigate DDoS attacks. Their proposed model obtained 98.92% accuracy on CIC-IDS2017 [41] dataset and 99.91% on the InSDN dataset [71].

Discussion: Combining two or more algorithms yields better results than applying single algorithms. To detect DDoS attacks effectively, researchers created an ensemble of either two supervised ML algorithms or two unsupervised ML algorithms or a combination of both supervised and unsupervised ML algorithms. We have listed down some of the works of past years that used ensemble algorithms such as SVM-SOM, SOM-NB, KNN-SOM, *K*-Means-KNN, SVM-RF, and AdaBoost for detecting DDoS attacks using either public dataset or self-generated dataset created in SDN environment.

9 Deep Learning-Based Solutions for DDoS Attack Detection in SDN

Xu et al. [256] presented hidden Markov models (HMMs) to identify DDoS attacks. The HMM approach detects DDoS attacks by the origin IP invigilator in a single detection algorithm with a higher detection rate of 79.2%. In real-world applications, several identification operators address the challenges of information preparation bottleneck and single-point failure. As a result, the distributed location system is combined with the HMM-based discovery approach that uses source IP observation.

Niyaz et al. [163] proposed stack autoencoder-based DL technique for feature reduction. The authors took a large set of features and then applied a stack autoencoder scheme to reduce the feature set. In this work, an application for DDoS detection is built upon a POX controller to defend from TCP, UDP and ICMP flood attacks. The authors created a lab setup of 12 network devices for normal traffic collections. A private network of ten DDoS attackers and five victim hosts is established. Hping3 is used to perform different kinds of attacks to create attack traffic. The authors did not compare their approach with the state-of-the-art approach or other ML and DL techniques in this paper. In addition, the paper mainly focuses on detecting DDoS attacks. Although their proposed model achieved an accuracy of 95.65%, the attack's mitigation is not being considered.

Yuan et al. [262] modelled the DDoS detection problem as a sequence classification. The deep defense applies DL-based models like CNN, RNN, GRU, and LSTM. The error rate is reduced from 7.517% to 2.103%. The authors compared different RNN models on ISCX 2012 [207] dataset, but the authors did not utilise SDN here to support DDoS detection.

Zheng et al. [266] created a system Reinforcing Anti-DDoS Actions in real time known as RADAR to protect against DDoS attacks using adaptive correlation analysis. The system is based on commercial off-the-shelf switches known as COTS that serve as SDN switches. It is the first DDoS detection and recognition system built on commodity switches. The Floodlight controller is used to build the RADAR system. The RADAR system consists of a collector, detector and locator. In real time, the RADAR can detect threats such as DNS amplification attacks, crossfire assaults, SYN and UDP flood attacks with 90% detection rate. The findings demonstrate that the suggested system can detect DDoS more effectively, with low latencies and reasonable overhead.

Li et al. [129] build a DL-based DDoS defense module using RNN, CNN and LSTM. Their model has an accuracy of 99% in the training phase. In DDoS defense architecture, there are a feature extraction module, DL DDoS detection module, information statistics module, model updater and flow packets coming to open flow switches and constructing a feature matrix. The DL-based DDoS detection module uses the resulting feature matrix as input. Deep learning is used to train the DDoS detection module to retrieve the features from the features matrix. The information statistics module collects attack features and their frequency. The flow table generator produces flow rules for attack traffic based on feedback from the information statistics module. For training and creation of the attack dataset, the authors utilised the ISCX dataset [207]. Spirent C1 tool performs DDoS attacks like Ping of death, ARP flood, UDP flood, Smurf and SYN flood. However, their proposed DL-based model achieved a significant performance accuracy of 99%, but they did not discuss how training is performed on the ISCX dataset in the SDN environment.

Liu et al. [135] developed a DDoS mitigation architecture that includes an information collecting module and a DDoS mitigation module. The SDN controller receives network traffic data in the information collection module. The DDoS mitigation module used deep reinforcement learning techniques to learn the features of assault traffic. A deep reinforcement learning agent is placed at the application layer in this module, which aids in generating flow rules to prevent and mitigate DDoS attacks. The suggested architecture protects against multiple DDoS flooding attacks (TCP SYN, UDP and ICMP). The authors employed the RYU controller and Mininet to build an SDN system.

Phan et al. [177] proposed Q-Mind defense model for DDoS attack. This framework can mitigate slow-rate DDoS attacks using Q-learning-based reinforcement learning. They perform experiments on the Maxinet emulator and ONOS controller. After identifying the attack, the ONOS controller installs flow rules to block malevolent IPs and achieves 99.5% accuracy.

Haider et al. [84] proposed a CNN-based DDoS defense model in SDN. The proposed architecture is evaluated on CICDDoS 2017 dataset [40] and achieved an accuracy of 99.48%. However, the CICDDoS dataset is Flow-based, but the author did not validate their result in a real or emulated SDN environment. Authors selected features, i.e. average

packet size, flow duration, and packet length standard deviation for DDoS detection.

Priyadarshini and Barik [184] proposed a source-based DDoS detection approach. It uses SDN to build a DDoS defense module on an SDN controller trained with LSTM. For training the DL module, the CTU-13 [42] dataset is used for attack traffic and the ISCX-2012 dataset [207] is used for normal traffic. The authors obtained an accuracy of 98.88% for their proposed model.

Liang and Znati [131] proposed an LSTM-based DDoS detection approach, they did not do feature engineering, but only packet header information is used for analysis. To identify DDoS attacks, LSTM examines a brief sequence of network packets. Authors claimed their approach could capture the dynamic behaviour of attack traffic, which ML algorithms do not identify easily. In this scenario, analysing a limited number of network packets is adequate. The authors compared their approach with ANN, DT, and SVM and found LSTM slightly better on CICDDoS 2017 [40] dataset with around 99% of precision, recall and f-measure.

Nugraha and Murthy [167] proposed an ensemble model of LSTM and CNN for slow-rate DDoS attack detection. This hybrid model outperforms other approaches like MLP, and one-class SVM and achieves 99% accuracy. The authors concluded that DL models faired better than ML models for a large dataset. The Hping3 tool generates regular traffic, and Slowloris generates attack traffic. The authors took the ONOS controller and two switches for evaluation. The limitation of the work is its small network topology.

Ujjan et al. [237] detected DDoS attack using DL model in SDN with snort IDS. Anomalous traffic is identified using sFlow and measured traffic checking at the data plane. Their method reduced the controller load to handle the data plane layer. SAE and Snort IDS are used to achieve an accuracy of 95% and a low FPR of 4%.

Novaes et al. [164] proposed a modular DDoS detection and mitigation approach. The defense system comprises three modules. The first module characterises the network traffic using LSTM. DDoS attack is identified using a fuzzy inference system in the second module. The third module is responsible for DDoS mitigation. The authors experimented using a Mininet-based emulation environment and Floodlight controller. The authors also used CICDDoS 2019 [39] dataset to test their approach. They obtained 93.13% accuracy when compared to KNN, SVM, MLP, and LSTM-2. In their other work [165], the authors detected a DDoS attack using the Adversarial Deep Learning Anomaly Detection approach. Adversarial training is used in this technique using the GAN (generative adversarial network) architecture. The experimental setup was the same as in their previous work. The performance of GAN was compared with LSTM, CNN and MLP algorithms. Compared to other algorithms, the GAN framework did the best in identifying DDoS attacks, with an accuracy of 99.78%. Similarly, Nugraha et al. [168] applied DL models CNN-LSTM and MLP to detect flooding attacks on two adversarial datasets. One of the datasets is derived from SDN emulated dataset, and the other is generated synthetically using Tabular GAN. They perform experiments on the Maxinet emulator and ONOS SDN controller. The results show that adding more adversarial cases to the training dataset increases the resilience of the MLP model. Their suggested model achieves 99% result for all performance parameters, including accuracy, precision, recall, and f-measure.

Jia Min et al. [152] performed DDoS detection by combining SVM with an optimised LSTM DL model and obtained 99.77% accuracy. The SDN controller extracts the flow table statistics and creates a feature vector in this approach. SVM takes the feature vector for abnormal traffic detection. If the traffic is detected as abnormal, it is sent to the LSTM model along with traffic information of the previous time. Finally, LSTM decides the abnormality of traffic. The authors performed their experiment in a small topology. How normal traffic is generated is not discussed in detail. Information related to the dataset and controller used is not elaborated.

Gadze et al. [76] proposed a DDoS detection approach based on RNN LSTM and CNN model. In this paper, the authors claimed RNN LSTM outperformed other linear-based classification models like Linear regression, Naïve Bayes and SVM with an accuracy of 89.63%. Work was emulated using the Mininet emulator and Floodlight controller to evaluate their approach. The Hping3 tool is used for traffic generation. The proposed approach performs and detects UDP, TCP, and ICMP attacks. The major limitation of this approach is the small dataset. The authors collected only 10,031 data for traffic analysis which is very small for the DL approach.

Yungaicela-Naula et al. [263] tested various ML/DL models on two well-known datasets, namely CICDDoS2017 [40] and CICDDoS2019 [39]. The authors deployed the model on an SDN emulation environment using Mininet and ONOS SDN controller. This paper investigates attacks like SYN, UDP, and HTTP Get flood attacks. The proposed setup consists of a flow collector, preprocessing, detection, and flow manager module. The CICFlow meter is used for the network traffic flow generator in the flow collector module. The flow collector module collects flows with 76 features. Various ML models like KNN, SVM, RF, and different DL models like MLP, CNN, GRU, and LSTM are used in the detection module. The authors achieved 98% detection accuracy for transport layer DDoS assaults and 95% detection accuracy for application layer DDoS attacks, respectively.

Sudar et al. [216] also proposed a four-layer DNN model for DDoS detection. The authors used CIC-IDS2017 [41] dataset for evaluating their model. After feature selection,

the authors selected six features for DDoS detection and achieved an accuracy of 97.59%.

Ahuja et al. [6] detected DDoS attack from normal traffic using an ensemble of DL algorithms CNN-LSTM, SVC-SOM and SAE-MLP algorithms. They applied the algorithms on the dataset and compared them based on accuracy, recall, precision, and f-score. SAE-MLP algorithm performed best with an accuracy of 99.75%. Similarly, Makuvaza et al. [140] detected DDoS attacks using deep neural network on CICIDS2017 [41] dataset. They compared their results with other algorithms, RBM-SVM, GRU-RNN and GRU-LSTM, based on the accuracy. Their proposed DNN model performed best with 97.25% accuracy.

Yungaicela et al. [264] employed deep reinforcement learning for DDoS prevention in SDN networks. They worked on self-generated dataset using ONOS controller, mininet and Apache Web server. Their experiment yielded 98% and 30% detection and flow sampling rates, respectively, and effectively mitigated slow-rate DDoS attacks. Ali et al. [13] also detected low-rate DDoS attack using three ANN algorithms Levenberg–Marquardt, Scaled Conjugate Gradient, and Bayesian regularisation. They performed their experiment on CAIDA [37] dataset and obtained an accuracy of 98.85%, sensitivity of 98.13%, $F1$-Score of 94.21%, and misclassification rate of 1.15%.

Discussion: As per the State-of-the-Art, there are two schools of thought for intelligent DDoS attack detection using SDN. One thought is based on ML technique, and another is based on the DL-based solution. The foremost requirement for deep learning is a large dataset applied in vision processing, speech recognition and applications where feature dimension is very high, having unknown features. Deep learning is a technique for extracting features from data. DL algorithms perform better in detecting DDoS attacks than ML approaches. We have listed some of the research works of past years where the researchers have applied DL algorithms such as CNN, RNN, LSTM, GRU, and stack autoencoder on large datasets DARPA99, ISCX2012, CTU-13, CICIDS2017, CICDDoS2019, CICDoS2017 and CICIDS2018 to recognise DDoS attacks in SDN network environment. Table 10 summarises the DL solutions for DDoS detection in SDN.

10 Detection and Mitigation Application for DDoS attack

It is difficult to detect and mitigate DDoS attacks in real time. It will be advantageous to have an application deployed at the SDN application layer that communicates with the controller and detects and mitigates DDoS attack. DDoS detection applications for POX, ONOS, Floodlight, OpenDaylight, and RYU controllers have been developed by researchers. According to Table 11, very few applications have been developed to detect and mitigate DDoS attacks. Both Chen et al. [45] and Oo et al. [170] created an application for ONOS controller, although the former did not provide an application for detection and mitigation. We developed an OFD (ONOS Flood Defender) application [19] in SDN-based infrastructure due to a lack of apps for ONOS controllers. This application comprises main method, detection, mitigation and flow rule generation modules, all of which work together to handle DDoS attacks and remove them from the network.

Discussion: As we can see from the preceding sections, researchers have put forth a lot of effort in recent years to create various architectures for tackling DDoS attacks. However, an SDN-based application for tackling DDoS attacks is required to detect and mitigate attacks efficiently, preventing massive harm to genuine users.

11 Research Challenges and Future Directions

This section discusses the current issues for all research publications providing DDoS detection and mitigation techniques. As a result, researchers inspired by this field may raise the issues and suggest appropriate solutions for DDoS attack detection.

SDN has several benefits that can prove fruitful to the world. However, apart from the advantages, SDN also faces several issues. The data and control plane separation in SDN has posed security threats. SDN planes have become vulnerable to DDoS attacks. The attacker can now attack any plane of SDN. Protecting SDN from these attacks is a significant issue that must be handled so legitimate users can access the services without disruption or delay. This is also necessary so that the benefits of SDN can be utilised to a full extent. We outline some of the problems that researchers might use to do more study and build new approaches to secure SDN.

1. *Standard SDN dataset for DDoS research*
   One major challenge is having standard SDN dataset. Applying ML and DL algorithms to this dataset to detect DDoS attacks can prove fruitful to legitimate users in the real networking world. We have found that there are a lot of public datasets available such as NSL-KDD [101], CAIDA [37], DARPA [56], CICDDoS2017 [40] and CIC-DoS2019 [39] for detecting DDoS attacks. The researchers have used these datasets to detect attacks, but none are SDN-specific. They must be updated to be flow-based in SDN networks. This is not always possible since the dataset may not accurately describe SDN behaviour during DDoS assaults. This is a major disadvantage and has emerged as a challenge. Creating

Table 10 Deep learning solutions for DDoS attack detection in SDN

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
1	Xu et al. [256]	Data	DARPA99 [125]	HMM	Detection	Detection rate, communication frequency
2	Hurley et al. [91]	–	Self-generated	HMM	Detection	Accuracy
3	Niyaz et al. [163]	Data, Control	Self-generated	Stack autoencoder	Detection	Accuracy, Precision, Recall, *F*-measure
4	Yuan et al. [262]	Data	ISCX2012 [207]	CNN, RNN, LSTM, GRU	Detection	Error rate, Accuracy, Precision, Recall, *F*-measure, AUC
5	Aziz and Okamura [23]	Data	Dataset from Malware Capture Facility Project	DL, DT	Detection, Mitigation	Packet drop
6	Zheng et al. [266]	Data	Self-generated	RL	Detection, Mitigation	Accuracy, Delay, Overhead
7	Li et al. [129]	Data	ISCX2012 [207]	CNN, RNN, LSTM	Detection	Accuracy
8	Liu et al. [135]	Data	Self-generated	Deep RL	Mitigation	–
9	Sahoo et al. [195]	Data	–	Learning Automata	Detection	Connection delay, failure rate, packet drop
10	Phan et al. [177]	Data	Self-generated	Q-Learning	Detection, Mitigation	Precision, Recall, *F*-measure, Detection rate, FAR
11	Haider et al. [84]	Data	CICDDoS2017 [40]	CNN	Detection	Accuracy, Precision, Recall, *F*-measure
12	Priyadarshini and Barik [184]	Data	CTU-13 [42], ISCX-2012 [207]	LSTM	Detection	Accuracy
13	Liang and Znati [131]	Data	CICIDS2017 [41]	LSTM	Detection	Precision, Recall, *F*-measure
14	Sun et al. [217]	Data	Self-generated	BiLSTM-RNN	Detection	CPU utilisation, Accuracy
15	Haider et al. [84]	Data	ISCX 2017 [41]	CNN	Detection	Accuracy, Precision, Recall
16	Nugraha and Murthy [167]	Data	Self-generated	CNN, LSTM	Detection	Accuracy, Precision, Recall, *F*-measure, Specificity
17	Ujjan et al. [237]	Data	Self-generated	SAE	Detection	Accuracy, Precision, Recall, *F*-measure
18	Novaes et al. [164]	Data	Self-generated	LSTM	Detection, Mitigation	Accuracy, Precision, Recall, *F*-measure
19	Wang and Liu [248]	Data	CICIDS2017 [41]	CNN	Detection	Accuracy, Precision, Recall, *F*-measure, Training time

Table 10 (continued)

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
20	Benzaïd et al. [29]	Application	CICIDS2017 [41]	DL-MLP	Detection, Mitigation	Response time, Server load
21	Mhamdi et al. [150]	Data	CICIDS2017 [41]	SAE-1SVM	Detection	Accuracy, Precision, Recall, F-measure
22	Malik et al. [141]	Control	CICIDS2017 [41]	LSTM-CNN	Detection	Accuracy, Precision, Recall, F-measure, Testing time
23	de Assis et al. [63]	Data	CICDDoS2019 [39]	CNN	Detection, Mitigation	Accuracy, Precision, Recall, F-measure
24	Novaes et al. [165]	Data	CICDDoS2019 [39]	Adversarial Deep Learning	Detection, Mitigation	Accuracy, Precision, Recall, F-measure
25	Nugraha et al. [168]	Data	Self-generated	CNN-LSTM, MLP	Detection	Accuracy, Precision, Recall, F-measure
26	Min et al. [152]	Data	Self-generated	SVM-LSTM	Detection	Accuracy
27	Makuvaza et al. [140]	Data	CICIDS2017 [41]	DNN	Detection	Accuracy, Precision, Recall, F-measure
28	Sudar et al. [216]	Data	CICIDS2017 [41]	DNN	Detection	Accuracy, Precision, Recall, F-measure
29	Gadze et al. [76]	Data	Self-generated	RNN, LSTM, CNN	Detection, Mitigation	Accuracy, Recall, Detection time, Mitigation time
30	Yungaicela-Naula et al. [263]	Data	CICDDoS2017 [40], CICDDoS2019 [39]	MLP, CNN, LSTM, GRU	Detection, Mitigation	Accuracy, Precision, Recall, F-measure
31	Ahuja et al. [6]	Data	Dataset by Leading India Project	CNN, LSTM, CNN-LSTM, SVC-SOM, SAE-MLP	Detection	Accuracy, Precision, Recall, F-measure
32	Ujjan et al. [238]	Data	Self-generated	SAE, CNN	Detection, Mitigation	Accuracy, Precision, Recall, F-measure
33	Dake et al. [57]	Data	Self-generated	Deep RL	Detection, Mitigation	Packet loss, Network delay, Jitter, Bandwidth utilisation
34	Wan et al. [243]	–	UNSW-NB15 [235]	SSAE-BiLSTM	Detection	Accuracy, F-measure, FAR
35	Javeed et al. [95]	Control	CICDDoS2019 [39]	CuDNNLSTM, CuDNNGRU	Detection	Accuracy, F-measure, Precision, Recall
36	Assis et al. [22]	Control	CICDDoS2019 [39], CICIDS2018 [43]	GRU	Detection, Mitigation	Accuracy, F-measure, Precision, Recall
37	Yungaicela-Naula et al. [264]	Data	Self-generated	LSTM	Detection, Mitigation	Detection rate, Flow sampling rate

Table 10 (continued)

S. no.	Refs.	Attack plane	Dataset	Detection algorithms used	Scope	Performance metrics
38	Ali et al. [12]	Control	CAIDA [37]	ANN	Detection, Mitigation	Accuracy, Sensitivity, Specificity, *F*1-Score, FPR

Table 11 Comparative analysis of detection and mitigation applications

Refs.	Controller	Application created	Detection	Mitigation	Detection technique
Chen et al. [45]	ONOS	×	✓	✓	SVM
Oo et al. [170]	ONOS	✓	✓	×	ASVM
Hu et al. [90]	POX	✓	✓	✓	SVM
Chen et al. [46]	POX	×	✓	×	XGBoost
Yang et al. [260]	RYU	×	✓	×	SVM
Myint et al. [159]	OpenDaylight	✓	✓	×	ASVM
Polat et al. [179]	POX	×	✓	×	SVM, KNN, NB, ANN
Swami et al. [220]	OpenDaylight	×	✓	×	DT, RF, AdaBoost, MLP, LR
Akanji et al. [7]	RYU	×	✓	×	SVM
Yungaicela et al. [264]	ONOS	×	✓	✓	LSTM
Aslam et al. [19]	ONOS	✓	✓	✓	MLP, KNN, SVM, XGBoost, Adaboost, RF, Bagging, Gradient Boosting
Khedr et al. [112]	POX	✓	✓	✓	SVM, KNN, DT, RF

SDN-specific datasets is encouraged for better DDoS detection and network traffic management.

2. *Feature Engineering in SDN-based DDoS detection*
Despite the fact that feature selection has a significant influence on DDoS detection performance, only a few systems employ it as the primary method. When building DDoS detection techniques, most researchers overlook feature selection methodologies.
DDoS attacks can be identified using specific features. Analysing and using these features to create a dataset can help detect attacks better. Several essential features are studied by Braga et al. [32], Myint et al. [159], and Xu and Liu [257] for DDoS attack detection. According to our survey, some of the most common features extracted from SDN are the duration of flows, the entropy of source/destination IP address, the number of packets per flow, the number of bytes per flow and the entropy of source/destination ports. Having useful features is essential, but having the best and reduced feature set for detection is also essential. Feature selection methods do this. Methods for selecting features help us choose the best and fewest characteristics for the dataset. It speeds up the training of ML algorithm. The model's complexity is lowered, making it easier to comprehend. Using a reduced dataset improves model accuracy and reduces overfitting. As a result, selecting the best and most limited feature set is critical and has proven challenging for researchers. Table 5 presents the feature selection methods used by the researchers in their work for detecting DDoS attacks. However, to increase the efficiency of DDoS detection techniques, features must be dynamically selected and updated. We analysed that researchers have applied feature selection methods to their dataset. However, none of them has applied feature selection methods on SDN-specific datasets, which is a sign of concern. Our analysis might encourage the researchers to create an SDN-specific dataset based on essential features and then apply feature selection methods to detect attacks better. Moreover, finding a better subset of features for DDoS attack detection needs to be researched.
3. *Low-rate DDoS detection*
We discovered that most research is based on spotting high-rate DDoS attack. There are very few works that detect low-rate DDoS attacks. One recent attack on AWS [113] suggests that DDoS attacks are moving towards more stealthy low-rate attacks from high-volume DDoS attacks. Low-rate DDoS attacks can cause severe damage if not detected timely. The average traffic volume

of low-rate DDoS attacks is nearly the same as regular traffic flow, so they are challenging to detect. As these attacks send fewer packets than high-rate attacks, the characteristics that can detect high-rate attacks will not detect low-rate attacks. As a result, these attacks must not be overlooked because they can potentially disrupt benign traffic over time. Several research papers, including [177, 192], have provided detection strategies for low-rate DDoS assaults. Finding the characteristics of these attacks and devising a detection system with low FPR and high true positive rate is a challenge that needs to be addressed.

4. *Timely mitigation of DDoS attack with low impact on legitimate requests*
   It is vital to recognise the DDoS attack as soon as feasible and delete the malicious flows from the network. Even if the attacks are identified, administrators cannot counteract them within the time limit. Regular users will continue to get services without interruption if DDoS attacks are recognised early, and proper countermeasures are implemented. Real-time mitigation of these attacks might lessen the impact on genuine users. Creating an effective mitigation mechanism is a challenge to the researchers for increasing users' productivity in the SDN environment.
5. *Detection and Mitigation in multi-controller SDN WAN network*
   As the network capacity is expanding daily, lack of stable and secure SDN controller is a challenge. Therefore, implementing ML/DL-based detection methods for DDoS attacks on a single controller may overwhelm it, lowering its operational efficiency. A single controller might potentially be a vulnerability for the whole network. Implementing DDoS security solutions in a multi-controller environment might be beneficial since it can distribute traffic load amongst devices and perform load balancing as needed. Priority should be given to the stability and scalability of multi-controllers for SDN WAN networks. The root controller has a globalised network view in a multi-controller setup, whereas the other local controllers only have network information. The challenge of synchronising these controllers in a multi-controller system must be addressed. Designing an effective ML-based/DL-based DDoS attack detection method on large-scale networks in a multi-controller environment is a challenge for the researchers.
6. *Real Implementation instead of Simulation*
   According to our survey, most of the research works have implemented their detection/mitigation methods in a simulation environment only. Although the simulation results are satisfactory for research. The methods' performance can be evaluated more accurately and effectively if the same procedures are used and evaluated on a real SDN network. Most researchers employed a simple topology with a single controller and two hosts to test their methods. As a result, a significant amount of effort is necessary to build thorough and up-to-date test criteria that allow SDN to detect and mitigate DDoS attacks in real-world network environments.
7. *DDoS detection and mitigation in hybrid network environment*
   If SDN is integrated with other traditional networks, such as the Internet of Things or computing concepts, such as edge computing, then the efficiency of DDoS detection methods can be increased. In case of IoT, the detection system installed on the IoT gateway device reduces the response time of DDoS attack by collecting detection data. Similarly, the edge nodes detect DDoS attacks effectively in edge computing. The characteristics of both networks can be combined with SDN, which can increase the performance of DDoS detection methods. However, it may also happen that the computing power of IoT devices and edge nodes can make it difficult to deploy highly complex detection methods. As a result, researchers have faced significant challenges in researching and designing DDoS detection and mitigation systems by integrating SDN and other traditional networks.
8. *Controller and OpenFlow switch overhead analysis*
   Using a single controller to deploy DDoS detection and mitigation methods may overburden it, lowering its operating efficiency. It is also possible that the single controller will serve as the network's single point of failure. As a result, the use of DDoS detection methods in a multi-controller system is required, which can help to balance the load between different devices. Similarly, in case of OpenFlow switches, the switch may overload due to its restricted memory and stop working if the attacker loads the flow table with malign flows. This disrupts the network services. If the DDoS detection method is applied in OpenFlow switches, the computational load on the controller is reduced, but the complexity of the hardware is increased, incurring an additional expense. As a result, it is challenging to implement security modules in switches without causing an overhead on the controller and OpenFlow switches.
9. *Application for DDoS attack detection and mitigation*
   To detect and mitigate DDoS attacks simultaneously, creating an application for an SDN controller would prove beneficial. We have analysed that few researchers have created applications to identify and mitigate DDoS attacks. Most have created only detection applications for controllers such as OpenDaylight, Floodlight, POX, NOX, ONOS and RYU. It is necessary to mitigate the attack properly so legitimate users are unaffected. An application capable of detecting and mitigating the attack simultaneously is highly necessary.

11.1 Summary

This survey presents a detailed taxonomy of DDoS defense solutions. The taxonomy is classified based on application, DDoS dataset, ML/DL solutions, feature selection methods, attack target and testing environment. In this article, we have explained the works of researchers during the past years who have proposed a solution for DDoS attack detection and mitigation using different ML and DL techniques. The different DDoS datasets available publicly are also explained in detail.

We observed that although researchers have given many solutions for detecting and mitigating DDoS attack in SDN. There is still no universal solution for all the challenges faced during DDoS attack detection and mitigation. Owing to the enormous rise of DDoS attacks in the last few years, as mentioned in Table 1, we can expect a greater diversity of emerging technologies to mitigate the damage caused by DDoS attacks to legitimate users. There is still a huge scope of research for emerging researchers to come up with innovative solutions to safeguard SDN infrastructure.

12 Conclusion

SDN has a vast future in the networking world. The security of SDN is one of the significant concerns which needs to be addressed. DDoS attacks are increasing, which has generated concern among users. Attackers attack the services more frequently to bring the servers down each year. Timely handling of DDoS attacks is a significant challenge. Apart from detecting and mitigating, it is also vital to ensure that the server load is not raised and mitigation is done immediately without causing a massive loss to the users. We have surveyed 24 survey articles from the year 2014 to 2023. Apart from this, we have also reviewed 260 research articles related to DDoS attacks in SDN. Out of the 260 research articles, we have selected 132 research articles related to DDoS defense solutions based on ML and/or DL algorithms in SDN.

There are various potential future research directions. First, the unavailability of standard SDN-specific datasets may not prove fruitful in correctly identifying DDoS attacks. Creating SDN-specific datasets is encouraged for better detection of DDoS attacks and network traffic management. Second, although many researchers have given DDoS attack detection solutions, only some have applied feature selection algorithms on SDN datasets. Finding better feature subsets for DDoS detection needs to be further researched. Third, Finding the characteristics of low-rate DDoS attacks and devising a detection system with low FPR and high TPR is a potential area of research. Fourth, creating an effective mitigation mechanism to counteract DDoS attacks within the time limit is a future scope for researchers to increase users' productivity in the SDN environment. Fifth, designing an effective ML/DL-based DDoS attack detection method on large-scale SDN WAN networks in a multi-controller environment is a promising research direction for the researchers. Sixth, implementing detection/mitigation techniques on a real SDN network scenario is highly required to validate the performance of methods. Seventh, researchers can further design a DDoS detection and mitigation system using SDN and other conventional networks to boost detection/mitigation efficiency. Eighth, analysing controller and OpenFlow switch overhead while implementing security modules for attack detection is a further research scope. Lastly, researchers can build an efficient application deployed at the SDN application layer to identify and get rid of the attack simultaneously. These research directions can help the researchers conduct further research and develop new methods to secure SDN.

Funding This research is supported by the Department of Science and Technology (DST)-Interdisciplinary Cyber-Physical Systems (ICPS) initiative, with the research grant number DST/ICPS/CPS-Individual/2018-490 (G).

Availability of data and materials As this is a survey paper, no datasets were created throughout the research.

References

1. AWS Shield.: Aws shield threat landscape report - q1 2020 (2020). https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf. Accessed 11 Sept 2022
2. Abou El Houda, Z.; Khoukhi, L.; Hafid, A.S.: Bringing intelligence to software defined networks: mitigating DDoS attacks. IEEE Trans. Netw. Serv. Manag. **17**(4), 2523–2535 (2020)
3. Ahmed, M.E.; Kim, H.; Park, M.: Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking. In: MILCOM 2017–2017 IEEE Military Communications Conference (MILCOM), pp. 11–16. IEEE (2017)
4. Ahuja, N.; Singal, G.; Mukhopadhyay, D.; et al.: Automated DDoS attack detection in software defined networking. J. Netw. Comput. Appl. **187**(103), 108 (2021)
5. Ahuja, N.; Singal, G.: DDoS attack detection & prevention in SDN using OpenFlow statistics. In: 2019 IEEE 9th International Conference on Advanced Computing (IACC) , pp. 147–152. IEEE (2019)
6. Ahuja, N.; Singal, G.; Mukhopadhyay, D.: DLSDN: Deep learning for DDoS attack detection in software defined networking. In: 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 683–688. IEEE (2021)
7. Akanji, O.S.; Abisoye, O.A.; Iliyasu, M.A.: Mitigating slow hypertext transfer protocol distributed denial of service attacks in software defined networks. J. Inf. Commun. Technol. **20**(3), 277–304 (2021)
8. AlMomin, H.; Ibrahim, A.A.: Detection of distributed denial of service attacks through a combination of machine learning algorithms over software defined network environment. In: 2020 International Congress on Human–Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1–4. IEEE (2020)

9. Aladaileh, M.A.; Anbar, M.; Hasbullah, I.H.; et al.: Detection techniques of distributed denial of service attacks on software-defined networking controller—a review. IEEE Access **8**, 143,985-143,995 (2020)
10. Alashhab, A.A.; Zahid, M.S.M.; Azim, M.A.; et al.: A survey of low rate DDoS detection techniques based on machine learning in software-defined networks. Symmetry **14**(8), 1563 (2022)
11. Alhijawi, B.; Almajali, S.; Elgala, H.; et al.: A survey on DoS/DDoS mitigation techniques in SDNs: classification, comparison, solutions, testing tools and datasets. Comput. Electr. Eng. **99**(107), 706 (2022)
12. Ali, T.E.; Chong, Y.W.; Manickam, S.: Machine learning techniques to detect a DDoS attack in SDN: a systematic review. Appl. Sci. **13**(5), 3183 (2023)
13. Ali, M.N.; Imran, M.; din, M.S.; et al.: Low rate DDoS detection using weighted federated learning in SDN control plane in IoT network. Appl. Sci. **13**(3), 1431 (2023)
14. Ali, J.; Roh, B.h.; Lee, B.; et al.: A machine learning framework for prevention of software-defined networking controller from DDoS attacks and dimensionality reduction of big data. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 515–519. IEEE (2020)
15. Alkasassbeh, M.; Al-Naymat, G.; Hassanat, A.; et al.: Detecting distributed denial of service attacks using data mining techniques. Int. J. Adv. Comput. Sci. Appl. **7**(1), 436–445 (2016)
16. Alshamrani, A.; Chowdhary, A.; Pisharody, S.; et al.: A defense system for defeating DDoS attacks in SDN based networks. In: Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access, pp. 83–92. ACM (2017)
17. Anand, P.: Record for the largest ever https DDoS attack smashed once again (2022). https://t.ly/df6Z. Accessed 11 Sept 2022
18. Ashraf, J.; Latif, S.: Handling intrusion and DDoS attacks in software defined networks using machine learning techniques. In: 2014 National software engineering conference, pp 55–60. IEEE (2014)
19. Aslam, N.; Srivastava, S.; Gore, M.: Onos flood defender: an intelligent approach to mitigate DDoS attack in SDN. Trans. Emerg. Telecommun. Technol. **33**, e4534 (2022)
20. Aslam, M.; Ye, D.; Tariq, A.; et al.: Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. Sensors **22**(7), 2697 (2022)
21. Aslam, M.; Ye, D.; Hanif, M.; et al.: Machine learning based SDN-enabled distributed denial-of-services attacks detection and mitigation system for internet of things. In: International Conference on Machine Learning for Cyber Security, pp 180–194. Springer (2020)
22. Assis, M.V.; Carvalho, L.F.; Lloret, J.; et al.: A GRU deep learning system against attacks in software defined networks. J. Netw. Comput. Appl. **177**(102), 942 (2021)
23. Aziz, M.Z.A.; Okamura, K.: Leveraging SDN for detection and mitigation smtp flood attack through deep learning analysis techniques. Int. J. Comput. Sci. Netw. Secur. **17**(10), 166–172 (2017)
24. BBC website attack: web attack knocks BBC websites offline (2015). http://bbc.com/news/technology-35204915. Accessed 11 Sept 2022
25. Banerjee, S.; Chakraborty, P.S.: To detect the distributed denial-of-service attacks in SDN using machine learning algorithms. In: 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 966–971. IEEE (2021)
26. Barbaschow, A.: Melbourne it confirms DDoS attack behind DNS outage (2017). https://t.ly/R93y. Accessed 11 Sept 2022
27. Barki, L.; Shidling, A.; Meti, N.; et al.: Detection of distributed denial of service attacks in software defined networks. In: 2016 International Conference on Advances in Computing. Communications and Informatics (ICACCI), pp. 2576–2581. IEEE (2016)
28. Bawany, N.Z.; Shamsi, J.A.; Salah, K.: DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arab. J. Sci. Eng. **42**(2), 425–441 (2017)
29. Benzaïd, C.; Boukhalfa, M.; Taleb, T.: Robust self-protection against application-layer (D) DoS attacks in SDN environment. In: 2020 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE (2020)
30. Bhushan, K.; Gupta, B.B.: Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J. Ambient. Intell. Humaniz. Comput. **10**(5), 1985–1997 (2019)
31. Bindra, N.; Sood, M.: Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. Autom. Control. Comput. Sci. **53**(5), 419–428 (2019)
32. Braga, R.; Mota, E.; Passito, A.: Lightweight DDoS flooding attack detection using nox/openflow. In: IEEE Local Computer Network Conference, pp. 408–415. IEEE (2010)
33. Bray, H.: Boston globe hit by denial of service attacks (2017). https://rb.gy/7fyzzi. Accessed 25 Sept 2022
34. Brown, C.; Cowperthwaite, A.; Hijazi, A.; et al.: Analysis of the 1999 darpa/lincoln laboratory ids evaluation data with netadhict. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–7. IEEE (2009)
35. Buragohain, C.; Medhi, N.: Flowtrapp: An SDN based architecture for DDoS attack detection and mitigation in data centers. In: 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 519–524. IEEE (2016)
36. CAIDA DDoS Attack Dataset (2007). https://www.caida.org/catalog/datasets/DDoS-20070804_dataset/. Accessed 11 Sept 2022
37. CAIDA DDoS Dataset: Caida the cooperative association for internet data analysis (2021). https://www.caida.org/. Accessed 11 Sept 2022
38. CAIDA OC48: The caida oc48 peering point traces (2008). https://www.caida.org/catalog/datasets/passive_oc48_dataset/. Accessed 11 Sept 2022
39. CIC-DDoS2019: DDoS evaluation dataset (2019). https://www.unb.ca/cic/datasets/DDoS-2019.html. Accessed 11 Sept 2022
40. CIC-DoS2017 (2017) Cic dos dataset (2017). https://www.unb.ca/cic/datasets/dos-dataset.html. Accessed 11 Sept 2022
41. CIC-IDS2017: Intrusion detection evaluation dataset (CIC-IDS2017) (2017). https://www.unb.ca/cic/datasets/ids-2017.html. Accessed 11 Sept 2022
42. CTU-13 Dataset: A labeled dataset with botnet, normal and background traffic (2011). https://www.stratosphereips.org/datasets-ctu13. Accessed 11 Sept 2022
43. Canadian Institute for Cybersecurity: Cse-cic-ids2018 on aws (2018). https://www.unb.ca/cic/datasets/ids-2018.html. Accessed 11 Sept 2022
44. Chen, W.; Xiao, S.; Liu, L.; et al.: A DDoS attacks traceback scheme for SDN-based smart city. Comput. Electr. Eng. **81**(106), 503 (2020)
45. Chen, C.C.; Chen, Y.R.; Lu, W.C.; et al.: Detecting amplification attacks with software defined networking. In: 2017 IEEE Conference on Dependable and Secure Computing, pp. 195–201. IEEE (2017)
46. Chen, Z.; Jiang, F.; Cheng, Y.; et al.: Xgboost classifier for DDoS attack detection and analysis in SDN-based cloud. In: 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), pp. 251–256. IEEE (2018)
47. Cheng, H.; Liu, J.; Xu, T.; et al.: Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks. Int. J. Sensor Netw. **34**(1), 56–69 (2020)
48. Chowdhury, S.; Khanzadeh, M.; Akula, R.; et al.: Botnet detection using graph-based feature clustering. J. Big Data **4**(1), 1–23 (2017)

49. Cluley, G.: Uk national lottery knocked offline by DDoS attack (2017). https://www.welivesecurity.com/2017/10/02/uk-national-lottery-DDoS-attack/. Accessed 11 Sept 2022
50. Cui, Y.; Qian, Q.; Guo, C.; et al.: Towards DDoS detection mechanisms in software-defined networking. J. Netw. Comput. Appl. **190**(103), 156 (2021)
51. Cui, J.; Wang, M.; Luo, Y.; et al.: DDoS detection and defense mechanism based on cognitive-inspired computing in SDN. Futur. Gener. Comput. Syst. **97**, 275–283 (2019)
52. Cui, Y.; Yan, L.; Li, S.; et al.: SD-anti-DDoS: fast and efficient DDoS defense in software-defined networks. J. Netw. Comput. Appl. **68**, 65–79 (2016)
53. Cui, J.; He, J.; Xu, Y.; et al.: Tddad: time-based detection and defense scheme against DDoS attack on SDN controller. In: Australasian Conference on Information Security and Privacy, pp. 649–665. Springer (2018)
54. DARPA IDS: Darpa intrusion detection evaluation dataset (1998). https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset. Accessed 11 Sept 2022
55. DARPA IDS: Darpa intrusion detection evaluation (1999). https://archive.ll.mit.edu/ideval/docs/attackDB.html. Accessed 11 Sept 2022
56. DARPA IDS: Darpa intrusion detection scenario specific datasets (2000). https://t.ly/6vJf. Accessed 11 Sept 2022
57. Dake, D.K.; Gadze, J.D.; Klogo, G.S.: DDoS and flash event detection in higher bandwidth SDN-IoT using multiagent reinforcement learning. In: 2021 International Conference on Computing. Computational Modelling and Applications (ICCMA), pp. 16–20. IEEE (2021)
58. Dayal, N.; Maity, P.; Srivastava, S.; et al.: Research trends in security and DDoS in SDN. Secur. Commun. Netw. **9**(18), 6386–6411 (2016)
59. Dayal, N.; Srivastava, S.: SD-wan flood tracer: tracking the entry points of DDoS attack flows in wan. Comput. Netw. **186**(107), 813 (2021)
60. Dayal, N.; Srivastava, S.: Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. In: 2017 9th International Conference on Communication Systems and Networks (COMSNETS), pp. 274–281. IEEE (2017)
61. Dayal, N.; Srivastava, S.: Leveraging SDN for early detection and mitigation of DDoS attacks. In: International Conference on Communication Systems and Networks, pp. 52–75. Springer (2018)
62. da Silva, A.S.; Wickboldt, J.A.; Granville, L.Z.; et al.: Atlantic: A framework for anomaly traffic detection, classification, and mitigation in SDN. In: NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 27–35. IEEE (2016)
63. De Assis, M.V.; Carvalho, L.F.; Rodrigues, J.J.; et al.: Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. Comput. Electr. Eng. **86**(106), 738 (2020)
64. Deepa, V.; Sudar, K.M.; Deepalakshmi, P.: Detection of DDoS attack on SDN control plane using hybrid machine learning techniques. In: 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 299–303. IEEE (2018)
65. Deepa, V.; Sudar, K.M.; Deepalakshmi, P.: Design of ensemble learning methods for DDoS detection in SDN environment. In: 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), pp. 1–6. IEEE (2019)
66. Dehkordi, A.B.; Soltanaghaei, M.; Boroujeni, F.Z.: The DDoS attacks detection through machine learning and statistical methods in SDN. J. Supercomput. **77**(3), 2383–2415 (2021)
67. Devendra: DDoS dataset (2019). https://www.kaggle.com/devendra416/DDoS-datasets. Accessed 11 Sept 2022
68. Dong, S.; Abbas, K.; Jain, R.: A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access **7**, 80,813-80,828 (2019)
69. Dong, S.; Sarem, M.: DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. IEEE Access **8**, 5039–5048 (2019)
70. Dridi, L.; Zhani, M.F.: SDN-guard: DoS attacks mitigation in SDN networks. In: 2016 5th IEEE International Conference on Cloud Networking (Cloudnet), pp. 212–217. IEEE (2016)
71. Elsayed, M.S.; Le-Khac, N.A.; Jurcut, A.D.: InSDN: a novel SDN intrusion dataset. IEEE Access **8**, 165,263-165,284 (2020)
72. Fajar, A.P.; Purboyo, T.W.: A survey paper of distributed denial-of-service attack in software defined networking (SDN). Int. J. Appl. Eng. Res. **13**(1), 476–82 (2018)
73. Ferrag, M.A.; Friha, O.; Hamouda, D.; et al.: Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access **10**, 40,281-40,306 (2022). https://doi.org/10.1109/ACCESS.2022.3165809
74. Firdaus, D.; Munadi, R.; Purwanto, Y.: DDoS attack detection in software defined network using ensemble k-means++ and random forest. In: 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), pp. 164–169. IEEE (2020)
75. Gadallah, W.G.; Omar, N.M.; Ibrahim, H.M.: Machine learning-based distributed denial of service attacks detection technique using new features in software-defined networks. Int. J. Comput. Netw. Inf. Secur. (IJCNIS) **13**(3), 15–27 (2021)
76. Gadze, J.D.; Bamfo-Asante, A.A.; Agyemang, J.O.; et al.: An investigation into the application of deep learning in the detection and mitigation of DDoS attack on SDN controllers. Technologies **9**(1), 14 (2021)
77. Gao, D.; Liu, Z.; Liu, Y.; et al.: Defending against packet-in messages flooding attack under SDN context. Soft. Comput. **22**(20), 6797–6809 (2018)
78. Gharvirian, F.; Bohlooli, A.: Neural network based protection of software defined network controller against distributed denial of service attacks. Int. J. Eng. **30**(11), 1714–1722 (2017)
79. Guozi, S.; Jiang, W.; Yu, G.; et al.: DDoS attacks and flash event detection based on flow characteristics in SDN. In: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1–6. IEEE (2018)
80. Gupta, S.; Grover, D.: A comprehensive review on detection of DDoS attacks using ml in SDN environment. In: 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), pp. 1158–1163. IEEE (2021)
81. Guru: Largest https DDoS attack on record—26 million request per second (2022). https://cybersecuritynews.com/largest-https-DDoS-attack/. Accessed 11 Sept 2022
82. Gurusamy, U.; MSK, M.: Detection and mitigation of UDP flooding attack in a multicontroller software defined network using secure flow management model. Concurr. Comput. Pract. Exp. **31**(20), e5326 (2019)
83. Haider, W.; Hu, J.; Slay, J.; et al.: Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. J. Netw. Comput. Appl. **87**, 185–192 (2017)
84. Haider, S.; Akhunzada, A.; Ahmed, G.; et al.: Deep learning based ensemble convolutional neural network solution for distributed denial of service detection in SDNs. In: 2019 UK/China Emerging Technologies (UCET), pp. 1–4. IEEE (2019)
85. Hameed, S.; Ahmed Khan, H.: SDN based collaborative scheme for mitigation of DDoS attacks. Future Internet **10**(3), 23 (2018)
86. Han, T.; Jan, S.R.U.; Tan, Z.; et al.: A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers. Concurr. Comput. Pract. Exp. **32**(16), e5300 (2020)

87. Hannache, O.; Batouche, M.C.: Neural network-based approach for detection and mitigation of DDoS attacks in SDN environments. Int. J. Inf. Secur. Privacy (IJISP) **14**(3), 50–71 (2020)
88. He, D.; Chan, S.; Ni, X.; et al.: Software-defined-networking-enabled traffic anomaly detection and mitigation. IEEE Internet Things J. **4**(6), 1890–1898 (2017)
89. Hong, K.; Kim, Y.; Choi, H.; et al.: SDN-assisted slow http DDoS attack defense method. IEEE Commun. Lett. **22**(4), 688–691 (2017)
90. Hu, D.; Hong, P.; Chen, Y.: FADM: DDoS flooding attack detection and mitigation system in software-defined networking. In: GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1–7. IEEE (2017)
91. Hurley, T.; Perdomo, J.E.; Perez-Pons, A.: HMM-based intrusion detection system for software defined networking. In: 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 617–621. IEEE (2016)
92. ISOT: Datasets (2010). https://www.uvic.ca/ecs/ece/isot/datasets/index.php. Accessed 11 Sept 2022
93. Imran, M.; Durad, M.H.; Khan, F.A.; et al.: Toward an optimal solution against denial of service attacks in software defined networks. Future Gener. Comput. Syst. **92**, 444–453 (2019)
94. Irish government website attack: Irish government websites temporarily offline due to cyber-attack (2016). https://www.bbc.com/news/world-europe-35379817. Accessed 11 Sept 2022
95. Javeed, D.; Gao, T.; Khan, M.T.: SDN-enabled hybrid dl-driven framework for the detection of emerging cyber threats in IoT. Electronics **10**(8), 918 (2021)
96. Jazi, H.H.; Gonzalez, H.; Stakhanova, N.; et al.: Detecting http-based application layer dos attacks on web servers in the presence of sampling. Comput. Netw. **121**, 25–36 (2017)
97. Jiang, Y.; Zhang, X.; Zhou, Q.; et al.: An entropy-based DDoS defense mechanism in software defined networks. In: International Conference on Communications and Networking in China, pp. 169–178. Springer (2016)
98. Jose, T.; Kurian, J.: Survey on SDN security mechanisms. Int. J. Comput. Appl. **132**(14), 0975–8887 (2015)
99. Jose, A.S.; Nair, L.R.; Paul, V.: Towards detecting flooding DDoS attacks over software defined networks using machine learning techniques. Rev. Geintec Gestao Inov. E Tecnolog.. **11**(4), 3837–3865 (2021)
100. Joëlle, M.M.; Park, Y.H.: Strategies for detecting and mitigating DDoS attacks in SDN: a survey. J. Intell. Fuzzy Syst. **35**(6), 5913–5925 (2018)
101. KDD-Cup99 Dataset (1999). http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Accessed 11 Sept 2022
102. Kalkan, K.; Altay, L.; Gür, G.; et al.: Jess: joint entropy-based DDoS defense scheme in SDN. IEEE J. Sel. Areas Commun. **36**(10), 2358–2372 (2018)
103. Kalkan, K.; Gur, G.; Alagoz, F.: Defense mechanisms against DDoS attacks in SDN environment. IEEE Commun. Mag. **55**(9), 175–179 (2017)
104. Karan, B.; Narayan, D.; Hiremath, P.: Detection of DDoS attacks in software defined networks. In: 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), pp. 265–270. IEEE (2018)
105. Karnani, S.; Shakya, H.K.: Mitigation strategies for distributed denial of service (DDoS) in SDN: a survey and taxonomy. Inf. Secur. J. Glob. Perspect. **7**, 1–25 (2022)
106. Kaur, S.; Kumar, K.; Aggarwal, N.; et al.: A comprehensive survey of DDoS defense solutions in SDN: taxonomy, research challenges, and future directions. Comput. Secur. **110**(102), 423 (2021)
107. Kaur, A.; Bhandari, A.: Detection and mitigation of spoofing attacks by using SDN in LAN. In: Proceedings of Sixth International Conference on Soft Computing for Problem Solving, pp. 240–247. Springer (2017)
108. Kaur, G.; Gupta, P.: Hybrid approach for detecting DDoS attacks in software defined networks. In: 2019 Twelfth International Conference on Contemporary Computing (IC3), pp. 1–6. IEEE (2019)
109. Kerner, S.M.: The 100 Gbps DDoS attack that no one saw (2013). https://www.silicon.co.uk/workspace/the-100gbps-DDoS-attack-that-no-one-saw-128565. Accessed 10 May 2023
110. Khandelwal, S.: World's largest 1 Tbps DDoS attack launched from 152,000 hacked smart devices (2016). https://t.ly/CZPA. . Accessed 10 May 2023
111. Khashab, F.; Moubarak, J.; Feghali, A.; et al.: DDoS attack detection and mitigation in SDN using machine learning. In: 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), pp. 395–401. IEEE (2021)
112. Khedr, W.I.; Gouda, A.E.; Mohamed, E.R.: FMDADM: a multilayer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks. IEEE Access **11**, 28,934-28,954 (2023)
113. Khooi, X.Z.; Csikor, L.; Kang, M.S.; et al.: In-network defense against AR-DDoS attacks. In: Proceedings of the SIGCOMM'20 Poster and Demo Sessions, pp. 18–20. ACM (2020)
114. Kim, S.; Lee, S.; Cho, G.; et al.: Preventing DNS amplification attacks using the history of DNS queries with SDN. In: European Symposium on Research in Computer Security, pp. 135–152. Springer (2017)
115. Klymash, M.; Shpur, O.; Peleh, N.; et al.: Concept of intelligent detection of DDoS attacks in SDN networks using machine learning. In: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S &T), pp. 609–612. IEEE (2020)
116. Kokila, R.; Selvi, S.T.; Govindarajan, K.: DDoS detection and analysis in SDN-based environment using support vector machine classifier. In: 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 205–210. IEEE (2014)
117. KoronIoTis, N.; Moustafa, N.; Sitnikova, E.; et al.: Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Future Gener. Comput. Syst. **100**, 779–796 (2019)
118. Kotb, S.E.; El-Dien, H.A.T.; Eldien, A.S.T.: SGuard: Machine learning-based distrbuted denial-of-service detection scheme for software defined network. In: 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), pp. 251–257. IEEE (2021)
119. Kottler, S.: February 28th DDoS incident report (2018). https://github.blog/2018-03-01-DDoS-incident-report/. Accessed 11 Sept 2022
120. Kousar, H.; Mulla, M.M.; Shettar, P.; et al.: Detection of DDoS attacks in software defined network using decision tree. In: 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), pp. 783–788. IEEE (2021)
121. Kumar, P.; Tripathi, M.; Nehra, A.; et al.: SAFETY: early detection and mitigation of TCP SYN flood utilizing entropy in SDN. IEEE Trans. Netw. Serv. Manag. **15**(4), 1545–1559 (2018)
122. Kumar Singh, V.: DDoS attack detection and mitigation using statistical and machine learning methods in SDN. PhD thesis, Dublin, National College of Ireland, Ireland (2020)
123. Kumbam, Y.R.: Apa-DDoS dataset (2020). https://www.kaggle.com/yashwanthkumbam/apaDDoS-dataset. Accessed 11 Sept 2022
124. Kyaw, A.T.; Oo, M.Z.; Khin, C.S.: Machine-learning based DDoS attack classifier in software defined network. In: 2020 17th International Conference on Electrical Engineering/Electronics.

Computer, Telecommunications and Information Technology (ECTI-CON), pp. 431–434. IEEE (2020)
125. Laboratory, L.: 1999 darpa intrusion detection evaluation dataset (1999). https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset. Accessed 11 Sept 2022
126. Latah, M.; Toker, L.: Towards an efficient anomaly-based intrusion detection for software-defined networks. IET Netw **7**(6), 453–459 (2018)
127. Le, D.; Dao, M.; Nguyen, Q.: Comparison of machine learning algorithms for DDoS attack detection in SDN. Inf. Control Syst./Informazionno-Upravlyaushie Sistemy **106**(3), 59–70 (2020)
128. Lee, K.; Kim, J.; Kwon, K.H.; et al.: DDoS attack detection method using cluster analysis. Expert Syst. Appl. **34**(3), 1659–1665 (2008)
129. Li, C.; Wu, Y.; Yuan, X.; et al.: Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. Int. J. Commun Syst **31**(5), e3497 (2018)
130. Li, X.; Yuan, D.; Hu, H.; et al.: DDoS detection in SDN switches using support vector machine classifier. In: Proceedings of the 2015 Joint International Mechanical, Electronic and Information Technology Conference, pp. 1–5. Atlantis Press (2015)
131. Liang, X.; Znati, T.: A long short-term memory enabled framework for DDoS detection. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
132. Lin, C.H.; Li, C.Y.; Wang, K.: Setting malicious flow entries against SDN operations: attacks and countermeasures. In: 2018 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1–8. IEEE (2018)
133. Liu, Z.; He, Y.; Wang, W.; et al.: DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN. China Commun. **16**(7), 144–155 (2019)
134. Liu, J.; Lai, Y.; Zhang, S.: Fl-guard: A detection and defense system for DDoS attack in SDN. In: Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, pp. 107–111. ACM (2017)
135. Liu, Y.; Dong, M.; Ota, K.; et al.: Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks. In: 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6. IEEE (2018)
136. LongTail: Longtail log analysis (2021). http://longtail.it.marist.edu/honey/. Accessed 10 May 2023
137. Luong, T.K.; Tran, T.D.; Le, G.T.: DDoS attack detection and defense in SDN based on machine learning. In: 2020 7th NAFOSTED Conference on Information and Computer Science (NICS), pp. 31–35. IEEE (2020)
138. M.S.: DDoS botnet attack on IoT devices (2020) . https://www.kaggle.com/siddharthm1698/DDoS-botnet-attack-on-IoT-devices. Accessed 11 Sept 2022
139. Mahrach, S.; Haqiq, A.: DDoS flooding attack mitigation in software defined networks. Int. J. Adv. Comput. Sci. Appl. **11**(1), 693–700 (2020)
140. Makuvaza, A.; Jat, D.S.; Gamundani, A.M.: 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 (2021)
141. Malik, J.; Akhunzada, A.; Bibi, I.; et al.: Hybrid deep learning: an efficient reconnaissance and surveillance detection mechanism in SDN. IEEE Access **8**, 134,695-134,706 (2020)
142. Manso, P.; Moura, J.; Serrão, C.: SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. Information **10**(3), 106 (2019)
143. Mao, J.; Deng, W.; Shen, F.: DDoS flooding attack detection based on joint-entropy with multiple traffic features. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 237–243. IEEE (2018)
144. Masolo, C.: Cloudflare detects a record 71 million request-per-second DDoS attack (2023). https://www.infoq.com/news/2023/02/cloudflare-DDoS-attack/. Accessed 10 May 2023
145. McHugh, J.: Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Trans. Inf. Syst. Secur. (TISSEC) **3**(4), 262–294 (2000)
146. McKeown, N.; Anderson, T.; Balakrishnan, H.; et al.: Openflow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)
147. Mehr, S.Y.; Ramamurthy, B.: An SVM based DDoS attack detection method for Ryu SDN controller. In: Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies, pp. 72–73. ACM (2019)
148. Meitei, I.L.; Singh, K.J.; De, T.: Detection of DDoS DNS amplification attack using classification algorithm. In: Proceedings of the International Conference on Informatics and Analytics, pp. 1–6. ACM (2016)
149. Meti, N.; Narayan, D.; Baligar, V.: 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), pp. 1366–1371. IEEE (2017)
150. Mhamdi, L.; McLernon, D.; El-moussa, F.; et al.: A deep learning approach combining autoencoder with one-class SVM for DDoS attack detection in SDNs. In: 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), pp. 1–6. IEEE (2020)
151. Mihai-Gabriel, I.; Victor-Valeriu, P.: Achieving DDoS resiliency in a software defined network by intelligent risk assessment based on neural networks and danger theory. In: 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), pp. 319–324. IEEE (2014)
152. Min, J.; Yuejie, S.; Qing, G.; et al.: DDoS attack detection method for space-based network based on SDN architecture. ZTE Commun. **18**(4), 18–25 (2021)
153. Mishra, A.; Gupta, N.; Gupta, B.: Defense mechanisms against DDoS attack based on entropy in SDN-cloud using pox controller. Telecommun. Syst. **77**(1), 47–62 (2021)
154. Mohammed, S.S.; Hussain, R.; Senko, O.; et al.: A new machine learning-based collaborative DDoS mitigation mechanism in software-defined network. In: 2018 14th International Conference on Wireless and Mobile Computing. Networking and Communications (WiMob), pp. 1–8. IEEE (2018)
155. Mowla, N.I.; Doh, I.; Chae, K.: CSDSM: cognitive switch-based DDoS sensing and mitigation in SDN-driven CDNi word. Comput. Sci. Inf. Syst. **15**(1), 163–185 (2018)
156. Musil, S.: Record-breaking DDoS attack in Europe hits 400Gbps. (2014). https://t.ly/AdUK. Accessed 11 July 2022
157. Musumeci, F.; Ionata, V.; Paolucci, F.; et al.: Machine-learning-assisted DDoS attack detection with p4 language. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2020)
158. Mwanza, N.P.; Kalita, J.: Detecting DDoS attacks in software defined networks using deep learning techniques: a survey. Int. J. Netw. Secur. **25**(2), 360–376 (2023)
159. Myint Oo. M.; Kamolphiwong. S.; Kamolphiwong, T.; et al.: Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN). J. Comput. Netw. Commun. (2019)
160. Nam, T.M.; Phong, P.H.; Khoa, T.D.; et al.: Self-organizing map-based approaches in DDoS flooding detection using SDN.

In: 2018 International Conference on Information Networking (ICOIN), pp. 249–254. IEEE (2018)
161. Nanda, S.; Zafari, F.; DeCusatis, C.; et al.: Predicting network attack patterns in SDN using machine learning approach. In: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 167–172. IEEE (2016)
162. Nisha Ahuja DMGaurav Singal.: DDoS attack SDN dataset (2020). https://data.mendeley.com/datasets/jxpfjc64kr/1. Accessed 11 Sept 2022
163. Niyaz, Q.; Sun, W.; Javaid, A.Y.: A deep learning based DDoS detection system in software-defined networking (SDN) (2016). arXiv preprint arXiv:1611.07400
164. Novaes, M.P.; Carvalho, L.F.; Lloret, J.; et al.: Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. IEEE Access **8**, 83,765-83,781 (2020)
165. Novaes, M.P.; Carvalho, L.F.; Lloret, J.; et al.: Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments. Future Gener. Comput. Syst. **125**, 156–167 (2021)
166. Nugraha, M.; Paramita, I.; Musa, A.; et al.: Utilizing OpenFlow and sFlow to detect and mitigate SYN flooding attack. J. Korea Multimedia Soc. **17**(8), 988–994 (2014)
167. Nugraha, B.; Murthy, R.N.: Deep learning-based slow DDoS attack detection in SDN-based networks. In: 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 51–56. IEEE (2020)
168. Nugraha, B.; Kulkarni, N.; Gopikrishnan, A.: Detecting adversarial DDoS attacks in software-defined networking using deep learning techniques and adversarial training. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 448–454. IEEE (2021)
169. Nurwarsito, H.; Nadhif, M.F.: DDoS attack early detection and mitigation system on SDN using random forest algorithm and Ryu framework. In: 2021 8th International Conference on Computer and Communication Engineering (ICCCE), pp. 178–183. IEEE (2021)
170. Oo, M.M.; Kamolphiwong, S.; Kamolphiwong, T.: The design of SDN based detection for distributed denial of service (DDoS) attack. In: 2017 21st International Computer Science and Engineering Conference (ICSEC), pp. 1–5. IEEE (2017)
171. Osborne, H.: Hsbc suffers online banking cyber-attack (2016). https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack. Accessed 11 Aug 2022
172. Paganini, P.: Sucuri spotted a large botnet of CCTV devices involved in DDoS attacks (2016). https://securityaffairs.co/wordpress/48807/IoT/cctv-devices-DDoS.html. Accessed 16 Aug 2022
173. Pajila, P.B.; Julie, E.G.: Detection of DDoS attack using SDN in IoT: A survey. In: Intelligent Communication Technologies and Virtual Mobile Networks, pp. 438–452. Springer (2019)
174. Panigrahi, R.; Borah, S.: A detailed analysis of CICIDS2017 dataset for designing Intrusion detection systems. Int. J. Eng. Technol. **7**(3.24), 479–482 (2018)
175. Perez-Diaz, J.A.; Valdovinos, I.A.; Choo, K.K.R.; et al.: A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. IEEE Access **8**, 155,859-155,872 (2020)
176. Phan, T.V.; Park, M.: Efficient distributed denial-of-service attack defense in SDN-based cloud. IEEE Access **7**, 18,701-18,714 (2019)
177. Phan, T.V.; Gias, T.R.; Islam, S.T.; et al.: Q-MIND: defeating stealthy DoS attacks in SDN with a machine-learning based defense framework. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
178. Pitropakis, N.; Panaousis, E.; Giannetsos, T.; et al.: A taxonomy and survey of attacks against machine learning. Comput. Sci. Rev. **34**(100), 199 (2019)
179. Polat, H.; Polat, O.; Cetin, A.: Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. Sustainability **12**(3), 1035 (2020)
180. Polat, H.; Turkoglu, M.; Polat, O.: Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET. IET Commun. **14**(22), 4089–4100 (2021)
181. Pradeepa, R.; Pushpalatha, M.: IPR: Intelligent Proactive Routing model toward DDoS attack handling in SDN. J. Supercomput. **77**(11), 12,355-12,381 (2021)
182. Prakash, A.; Priyadarshini, R.: An intelligent software defined network controller for preventing distributed denial of service attack. In: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 585–589. IEEE (2018)
183. Prasad, M.D.; Babu, V.P.; Amarnath, C.: Machine learning DDoS detection using stochastic gradient boosting. Int. J. Comput. Sci. Eng. **7**(4), 157–16 (2019)
184. Priyadarshini, R.; Barik, R.K.: A deep learning based intelligent framework to mitigate DDoS attack in fog environment. J. King Saud Univ. Comput. Inf. Sci. **34**, 825–831 (2019)
185. Radware: DDoS attacks history (2017). https://www.radware.com/security/DDoS-knowledge-center/DDoS-chronicles/DDoS-attacks-history/. Accessed 10 May 2023
186. Rahman, O.; Quraishi, M.A.G.; Lung, C.H.: DDoS attacks detection and mitigation in SDN using machine learning. In: 2019 IEEE World Congress on Services (SERVICES), pp. 184–189. IEEE (2019)
187. Ramprasath, J.; Seethalakshmi, V.: Improved network monitoring using software-defined networking for DDoS detection and mitigation evaluation. Wirel. Pers. Commun. **116**(3), 2743–2757 (2021)
188. Revathi, M.; Ramalingam, V.; Amutha, B.: A machine learning based detection and mitigation of the DDoS attack by using SDN controller framework. Wirel. Pers. Commun. 1–25 (2021)
189. Russian Website attack: Russian Defense Ministry's website suffers DDoS attacks during poll for new weapons names (2018). https://tass.com/defense/995686. Accessed 11 Sept 2022
190. SDN Report: Software-defined networking market (2020). https://www.marketsandmarkets.com/Market-Reports/software-defined-networking-SDN-market-655.html. Accessed 11 Sept 2022
191. Sahoo, K.S.; Panda, S.K.; Sahoo, S.; et al.: Toward secure software-defined networks against distributed denial of service attack. J. Supercomput. **75**(8), 4829–4874 (2019)
192. Sahoo, K.S.; Puthal, D.; Tiwary, M.; et al.: An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Gener. Comput. Syst. **89**, 685–697 (2018)
193. Sahoo, K.S.; Tripathy, B.K.; Naik, K.; et al.: An evolutionary SVM model for DDoS attack detection in software defined networks. IEEE Access **8**, 132,502-132,513 (2020)
194. Sahoo, K.S.; Iqbal, A.; Maiti, P.; et al.: A machine learning approach for predicting DDoS traffic in software defined networks. In: 2018 International Conference on Information Technology (ICIT), pp. 199–203. IEEE (2018)
195. Sahoo, K.S.; Tiwary, M.; Sahoo, S.; et al.: A learning automata-based DDoS attack defense mechanism in software defined networks. In: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, pp. 795–797. ACM (2018)
196. Sahri, N.; Okamura, K.: Protecting DNS services from IP spoofing: SDN collaborative authentication approach. In: Proceedings

of the 11th International Conference on Future Internet Technologies, pp. 83–89. ACM (2016)
197. Sangodoyin, A.O.; Akinsolu, M.O.; Pillai, P.; et al.: Detection and classification of DDoS flooding attacks on software-defined networks: a case study for the application of machine learning. IEEE Access **9**, 122,495-122,508 (2021)
198. Sanjeetha, R.; Raj, A.; Saivenu, K.; et al.: Detection and mitigation of botnet based DDoS attacks using catboost machine learning algorithm in SDN environment. Int. J. Adv. Technol. Eng. Explor. **8**(76), 445 (2021)
199. Santos, R.; Souza, D.; Santo, W.; et al.: Machine learning algorithms to detect DDoS attacks in SDN. Concurr. Comput. Pract. Exp. **32**(16), e5402 (2020)
200. El Sayed, M.S.; Le-Khac, N.A.; Azer, M.A.; et al.: A flow-based anomaly detection approach with feature selection method against DDoS attacks in SDNs. IEEE Trans. Cogn. Commun. Netw. **8**(4), 1862–1880 (2022)
201. Scaranti, G.F.; Carvalho, L.F.; Junior, S.B.; et al.: Unsupervised online anomaly detection in software defined network environments. Expert Syst. Appl. **191**(116), 225 (2022)
202. Sen, S.; Gupta, K.D.; Ahsan, M.; et al.: Leveraging machine learning approach to setup software-defined network (SDN) controller rules during DDoS attack. In: Proceedings of International Joint Conference on Computational Intelligence, pp. 49–60. Springer (2020)
203. Shafi, Q.; Qaisar, S.; Basit, A.: Software defined machine learning based anomaly detection in fog based IoT network. In: International Conference on Computational Science and Its Applications, pp. 611–621. Springer (2019)
204. Shahzad, F.; Khan, M.A.; Khan, S.A.; et al.: AutoDrop: automatic DDoS detection and its mitigation with combination of Openflow and Sflow. In: International Conference on Future Intelligent Vehicular Technologies, pp. 112–122. Springer (2016)
205. Shani, T.: Updated: This DDoS attack unleashed the most packets persecond ever. here's why that's important (2019) https://rb.gy/t4cg9v. Accessed 11 Sept 2022
206. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp **1**, 108–116 (2018)
207. Shiravi, A.; Shiravi, H.; Tavallaee, M.; et al.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput. Secur. **31**(3), 357–374 (2012)
208. Shohani, R.B.; Mostafavi, S.A.: Introducing a new linear regression based method for early DDoS attack detection in SDN. In: 2020 6th International Conference on Web Research (ICWR), pp. 126–132. IEEE (2020)
209. SimpleWeb. Trace-simplewiki-the simpleweb (2010). https://www.simpleweb.org/wiki/index.php/Traces. Accessed 11 Sept 2022
210. Singh, J.; Behal, S.: Detection and mitigation of DDoS attacks in SDN: a comprehensive review, research challenges and future directions. Comput. Sci. Rev. **37**(100), 279 (2020)
211. Singh, M.P.; Bhandari, A.: New-flow based DDoS attacks in SDN: taxonomy, rationales, and research challenges. Comput. Commun. **154**, 509–527 (2020)
212. Singh, P.K.; Jha, S.K.; Nandi, S.K.; et al.: ML-based approach to detect DDoS attack in V2I communication under SDN architecture. In: TENCON 2018-2018 IEEE Region 10 Conference, pp. 0144–0149. IEEE (2018)
213. Singh, S.; Jayakumar, S.: Twin security model—a machine learning-based approach for DDoS attack detection in SDN. In: International Conference on Soft Computing and Signal Processing. Springer, pp. 53–62 (2019)
214. Song, J.; Takakura, H.; Okabe, Y.: Description of kyoto university benchmark data (2006). http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf. Accessed 15 Mar 2016
215. Stolfo, S.J.; Fan, W.; Lee, W.; et al.: Cost-based modeling for fraud and intrusion detection: Results from the jam project. In: Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, pp. 130–144. IEEE (2000)
216. Sudar, K.M.; Beulah, M.; Deepalakshmi, P.; et al.: Detection of distributed denial of service attacks in SDN using machine learning techniques. In: 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5. IEEE (2021)
217. Sun, W.; Li, Y.; Guan, S.: An improved method of DDoS attack detection for controller of SDN. In: 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), pp. 249–253. IEEE (2019)
218. Swami, R.; Dave, M.; Ranga, V.: Software-defined networking-based DDoS defense mechanisms. ACM Comput. Surv. (CSUR) **52**(2), 1–36 (2019)
219. Swami, R.; Dave, M.; Ranga, V.: Voting-based intrusion detection framework for securing software-defined networks. Concurr. Comput. Pract. Exp. **32**(24), e5927 (2020)
220. Swami, R.; Dave, M.; Ranga, V.: Detection and analysis of TCP-SYN DDoS attack in software-defined networking. Wirel. Pers. Commun. **118**(4), 2295–2317 (2021)
221. Tan, L.; Pan, Y.; Wu, J.; et al.: A new framework for DDoS attack detection and defense in SDN environment. IEEE Access **8**, 161,908-161,919 (2020)
222. Tan, J.; Jing, S.; Guo, L.; et al.: DDoS detection method based on gini impurity and random forest in SDN environment. In: 2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), pp. 601–606. IEEE (2021)
223. Tang, Mhamdi, L.; McLernon, D.; et al.: Deep recurrent neural network for intrusion detection in SDN-based networks. In: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), pp. 202–206. IEEE (2018)
224. Tang, T.A.; Mhamdi, L.; McLernon, D.; et al.: Deep learning approach for network intrusion detection in software defined networking. In: 2016 international conference on wireless networks and mobile communications (WINCOM), pp. 258–263. IEEE (2016)
225. Tannam, E.: DDoS attack takes down two election websites in czech republic (2017). https://www.siliconrepublic.com/enterprise/czech-election-DDoS. Accessed 11 Sept 2021
226. Tavallaee, M.; Bagheri, E.; Lu, W.; et al.: A detailed analysis of the kdd cup 99 data set. In: 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1–6. IEEE (2009)
227. Tayfour, O.E.; Marsono, M.N.: Collaborative detection and mitigation of DDoS in software-defined networks. J. Supercomput. 1–25 (2021)
228. Thai government websites attack: Thai government websites hit by denial-of-service attack (2015). https://www.bbc.com/news/world-asia-34409343. Accessed 11 Sept 2022
229. Tonkal, Ö.; Polat, H.; Başaran, E.; et al.: Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking. Electronics **10**(11), 1227 (2021)
230. Tuan, N.N.; Hung, P.H.; Nghia, N.D.; et al.: A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN. Electronics **9**(3), 413 (2020)
231. Tuan, N.N.; Hung, P.H.; Nghia, N.D.; et al.: A robust TCP-SYN flood mitigation scheme using machine learning based on SDN. In: 2019 International Conference on Information and Communication Technology Convergence (ICTC), pp. 363–368. IEEE (2019)
232. Tufa, S.W.; Mengstie, M.; Gebregziabher, H.; et al.: Detecting DDoS attack using adaptive boosting with software defined network in cloud computing environment. Rev. Geintec Gestao Inov. E Tecnolog.. **11**(4), 3485–3494 (2021)

233. Tung, L.: New world record DDoS attack hits 1.7 tbps days after landmark github outage (2018). https://t.ly/EJ1L. Accessed 11 Sept 2022
234. Turner, J.: 2017: The year of widespread SDN adoption and DDoS attack mitigation (2017). https://t.ly/tv0C. Accessed 11 Sept 2022
235. UNSW-NB15 Dataset (2017). https://research.unsw.edu.au/projects/unsw-nb15-dataset. Accessed 11 Sept 2022
236. Ubale, T.; Jain, A.K.: Survey on DDoS attack techniques and solutions in software-defined network. In: Gupta BB, Perez GM, Agrawal DP, Gupta D (eds.) Handbook of Computer Networks and Cyber Security, pp. 389–419. Springer (2020)
237. Ujjan, R.M.A.; Pervez, Z.; Dahal, K.; et al.: Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Gener. Comput. Syst. **111**, 763–779 (2020)
238. Ujjan, R.M.A.; Pervez, Z.; Dahal, K.; et al.: Entropy based features distribution for anti-DDoS model in SDN. Sustainability **13**(3), 1522 (2021)
239. Uzunovic, A.: Anonymous target bank of greece website with massive DDoS attack (2016). https://www.hackread.com/anonymous-DDoS-attack-bank-greece-website-down/. Accessed 01 Aug 2021
240. Valdovinos, I.A.; Pérez-Díaz, J.A.; Choo, K.K.R.; et al.: Emerging DDoS attack detection and mitigation strategies in software-defined networks: taxonomy, challenges and future directions. J. Netw. Comput. Appl. **187**, 103093 (2021)
241. van Steyn, J.: DDoS attack network logs (2019). https://www.kaggle.com/jacobvs/DDoS-attack-network-logs/version/1. Accessed 11 Sept 2022
242. Verma, A.: A comprehensive dataset for DDoS attack (2021). https://www.kaggle.com/amanverma1999/a-comprehensive-dataset-for-DDoS-attack. Accessed 11 Sept 2022
243. Wan, L.; Wang, Q.; Zheng, S.: Deep SSAE-BiLSTM model for DDoS detection In SDN. In: 2021 2nd International Conference on Computer Communication and Network Security (CCNS), pp. 1–4. IEEE (2021)
244. Wang, Y.; Hu, T.; Tang, G.; et al.: Sgs: safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking. IEEE Access **7**, 34,699-34,710 (2019)
245. Wang, J.; Wang, L.: SDN-Defend: a lightweight online attack detection and mitigation system for DDoS attacks in SDN. Sensors **22**(21), 8287 (2022)
246. Wang, J.; Wen, R.; Li, J.; et al.: Detecting and mitigating target link-flooding attacks using SDN. IEEE Trans. Dependable Secure Comput. **16**(6), 944–956 (2018)
247. Wang, H.; Xu, L.; Gu, G.: Floodguard: A dos attack prevention extension in software-defined networks. In: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 239–250. IEEE (2015)
248. Wang, L.; Liu, Y.: A DDoS attack detection method based on information entropy and deep learning in SDN. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 1084–1088. IEEE (2020)
249. Wang, P.; Chao, K.M.; Lin, H.C.; et al.: An efficient flow control approach for SDN-based network threat detection and migration using support vector machine. In: 2016 IEEE 13th International Conference on e-Business Engineering (ICEBE), pp. 56–63. IEEE (2016)
250. Warren, T.: Microsoft says it mitigated one of the largest DDoS attacks ever recorded (2021). https://www.theverge.com/2021/10/12/22722155/microsoft-azure-biggest-DDoS-attack-ever-2-4-tbps. Accessed 11 Sept 2022
251. Wong, F.; Tan, C.X.: A survey of trends in massive DDoS attacks and cloud-based mitigations. Int. J. Netw. Secur. Appl. **6**(3), 57 (2014)
252. Woolf, N.: DDoS attack that disrupted internet was largest of its kind in history, experts say (2016). https://www.theguardian.com/technology/2016/oct/26/DDoS-attack-dyn-mirai-botnet. Accessed 25 Oct 2021
253. Xing, X.; Luo, T.; Li, J.; et al.: A defense mechanism against the dns amplification attack in SDN. In: 2016 IEEE International Conference on Network Infrastructure and Digital Content (ICNIDC), pp. 28–33. IEEE (2016)
254. Xu, Y.; Sun, H.; Xiang, F.; et al.: Efficient DDoS detection based on k-fknn in software defined networks. IEEE Access **7**, 160,536-160,545 (2019)
255. Xu, X.; Yu, H.; Yang, K.: DDoS attack in software defined networks: a survey. ZTE Commun. **15**(3), 13–19 (2017)
256. Xu, X.; Sun, Y.; Huang, Z.: Defending DDoS attacks using hidden markov models and cooperative reinforcement learning. In: Pacific-Asia Workshop on Intelligence and Security Informatics, pp. 196–207. Springer (2007)
257. Xu, Y.; Liu, Y.: DDoS attack detection under SDN context. In: IEEE INFOCOM 2016-the 35th Annual IEEE International Conference on Computer Communications, pp. 1–9. IEEE (2016)
258. Yadav, A.; Kori, A.S.; Shettar, P.; et al.: A hybrid approach for detection of DDoS attacks using entropy and machine learning in software defined networks. In: 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–7. IEEE (2021)
259. Yan, Q.; Yu, F.R.; Gong, Q.; et al.: 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 (2015)
260. Yang, L.; Zhao, H.: DDoS attack identification and defense using SDN based on machine learning method. In: 2018 15th International Symposium on Pervasive Systems. Algorithms and Networks (I-SPAN), pp. 174–178. IEEE (2018)
261. Ye, J.; Cheng, X.; Zhu, J.; et al.: A DDoS attack detection method based on SVM in software defined network. Secur. Commun. Netw. (2018)
262. Yuan, X.; Li, C.; Li, X.: Deepdefense: identifying DDoS attack via deep learning. In: 2017 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1–8. IEEE (2017)
263. Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Perez-Diaz, J.A.: SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. IEEE Access **9**, 108495–108512 (2021). https://doi.org/10.1109/ACCESS.2021.3101650
264. Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Pérez-Díaz, J.A.; et al.: A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning. J. Netw. Comput. Appl. **205**(103), 444 (2022)
265. Zhao, K., Lu, B., Shi, H., et al.: A DDoS attack detection and defense mechanism based on the self-organizing mapping in SDN. Internet Technol Lett. e305 (2021)
266. Zheng, J.; Li, Q.; Gu, G.; et al.: Realtime DDoS defense using cots SDN switches via adaptive correlation analysis. IEEE Trans. Inf. Forensics Secur. **13**(7), 1838–1853 (2018)
267. Zhijun, W.; Qing, X.; Jingjie, W.; et al.: Low-rate DDoS attack detection based on factorization machine in software defined network. IEEE Access **8**, 17,404-17,418 (2020)
268. Zi, L., Yearwood, J., Wu, X.W.: Adaptive clustering with feature ranking for DDoS attacks detection. In: 2010 Fourth International Conference on Network and System Security, pp. 281–286. IEEE (2010)