EasyChair Preprint

№ 15323

Mitigating DDoS Attacks in SDN Using Machine Learning and Deep Learning: Challenges and Opportunities

G.B Veeresh, Vanita Jaitly and V Lokeswara Reddy

October 28, 2024

Mitigating DDoS Attacks in SDN Using Machine Learning and Deep Learning: Challenges and Opportunities.

Sri.G.B.Veeresh,MCA.
Research Scholar,
CA Department ,
HITS, PADUR,CHENNAI
veereshksrm@gmail.com

Dr.Vanita Jaitly,MCA.,Ph.D
Asst. Professor III ,
CA Department,
HITS, PADUR, CHENNAI.
vanitaj@hindustanunv.ac.in

Dr.V.Lokeswara Reddy,M.Tech.,Ph.D.
Professor,
CSE Department,
KSRMCE, KADAPA, AP.
vlreddy74@gmail.com

Abstract

Distributed Denial of Service (DDoS) attacks represent a significant and evolving threat within the realm of cybersecurity. In Software-Defined Networking (SDN), leveraging Machine Learning (ML) and Deep Learning (DL) techniques has proven to be a promising strategy for detecting and mitigating these attacks. This systematic literature review (SLR) provides a comprehensive analysis of current research in this field. The findings illustrate the versatility of ML and DL models in adapting to various attack vectors, their capacity for real-time decision-making, and their resilience against adversarial threats. However, challenges remain, including optimizing performance, ensuring scalability, enhancing resource efficiency, improving model interpretability, and addressing ethical considerations. The SLR highlights the critical importance of having labeled datasets, fostering ethical and legal awareness, and preparing network administrators for collaborative engagement with ML and DL-based DDoS mitigation systems. As the cybersecurity landscape continues to evolve, this review underscores the ongoing effort required to fully exploit the potential of ML and DL in protecting SDN networks against DDoS threats

1. Introduction:

Software-defined networking (SDN) has been recommended as the future of internet architecture in light of the rising need for high-quality multimedia content. Decoupling the control plane (the network's "brains") from the data plane (its "muscles") is a fundamental tenet of this networking model [1]. SDN models include both southbound and northbound APIs, in addition to SDN controllers. With this design, a centralized and programmable network is made available, allowing for the dynamic provisioning of services [2]. OpenFlow (OF) is an industry-standard, publicly-available protocol used in software-defined networking that defines how a centralized controller sets up and manages a network's control layer. Mac tables and routing tables store data in SDN, and a number of complex switching and routing protocols manage it. In conventional networks, these tables are used to form the forwarding plane [3].

The internet is crucial for modern society's commercial transactions, educational opportunities, and interpersonal connections. Criminal behavior like hacking, disseminating false information, and denial-of-service (DoS) assaults have all increased along with the internet's many positive effects. When an authorized service, system, or network is intentionally rendered unavailable to its intended users, this is known as a denial of service attack. The goal of a Distributed Denial of Service (DDoS) attack, a subset of Denial of Service (DoS) assaults, is to interrupt normal traffic to a single target by infiltrating numerous systems .

When compared to conventional networks, SDN makes it harder to prevent denial-of-service and distributed denial-of-service attacks. The performance of computer networks has suffered as a result of these assaults, which pose a

serious danger due to their ability to drain resources and disable services. An efficient denial of service or distributed denial of service attack drains resources and blocks host access to the targeted service on purpose. With SDNs, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack may cripple the network by hogging bandwidth on the control plane, the data plane, or both. Because of the OpenFlow switch's limited flow table RAM, packets may be discarded and new flow rules may not be installed if the switch is under assault on the data plane. It is possible that a significant number of erroneous flows will be generated as part of a data plane DoS/DDoS attack. The switch buffers these packets, and when it is full, it sends the complete packet to the controller via packet-in messages rather than simply the packet's headers. This may lead to longer wait times when implementing new flow rules and increased demands on available communication bandwidth [5]. DDoS attacks involve a network of devices under the attacker's control, whereas DoS attacks use several internet connections to knock the victim's computer network down. Due to the dispersed nature of DDoS attacks and the massive attack volumes often used, they are more difficult to identify and track. While a DoS attack may be launched by a script or a dedicated instrument like the Low-Orbit Ion Cannon, a Distributed Denial of Service (DDoS) attack is executed in a different way. Buffer overflows, Internet Control Message Protocol floods, tears, and flooding are all examples of DOS attacks, whereas volumetric attacks, fragmentation attacks, application layer attacks, and protocol attacks are all examples of DDOS attacks. Because they include several systems, DDoS attacks are more devastating than DoS attacks. However, it is more difficult for security teams and products to identify the origin of the attack. Traditional computer networks are distinct in many perspectives when compared with software defined networks.

1.1 Comparison of Traditional Computer Networks (CN) and Software-Defined Networks (SDN):

Perspective	Traditional Computer Networks	Software-Defined Networks
Architecture	• These networks have a fixed and hardware-based architecture, with separate network devices (such as routers and switches) responsible for data forwarding and control functions. • The network configuration is often static.	• SDN separates the control plane from the data plane. It centralizes network control in a software-based controller, making the network more flexible and programmable. • This allows for dynamic reconfiguration of the network
Control	Control in CNs is distributed across individual network devices. Configuration changes are typically manual and device-specific.	SDN provides centralized network control, allowing administrators to define network behavior through software. This centralization offers more granular control and easier management.
Flexibility	CNs are often less flexible and require substantial manual configuration. Changes may require device-specific commands and are less adaptable to dynamic needs.	SDNs are highly flexible and adaptable. Network behavior can be adjusted in real-time through software, making it easier to respond to changing network conditions and requirements.
Scalability	Scaling a traditional network often involves adding more physical hardware, which can be expensive and time-consuming.	SDNs can be more easily scaled because changes can be implemented through software, and virtual network resources can be dynamically provisioned as needed.
Security	Security measures in CNs are typically device-centric, with firewalls, intrusion detection systems, and access controls implemented on individual devices.	SDNs offer the potential for more centralized and programmatic security policies. Security policies can be easily applied across the network, and threat detection can be integrated with network control.

Management	Network management in CNs is often complex and may involve multiple management systems for different network elements.	SDNs provide a more unified and centralized management approach, simplifying network administration
Cost	Initial setup and ongoing operational costs can be high due to the need for physical hardware and manual configuration.	SDNs may reduce operational costs over time due to automation and centralized control, but initial deployment costs for SDN infrastructure can be a consideration.

1.2 DDoS in Traditional networks and Software defined Networks

DDoS (Distributed Denial of Service) attacks can occur in both traditional computer networks (CN) and Software-Defined Networks (SDN), but the way these attacks are executed and mitigated may differ due to the fundamental differences in the architecture of these two types of networks.

DDoS in CN (Traditional Computer Network):

- Centralized Infrastructure: In traditional computer networks, the infrastructure is often more centralized. This means that network traffic flows through routers and switches that are not easily reconfigurable during an attack.
- Mitigation Challenges: DDoS attacks in CNs can overwhelm network devices, saturate bandwidth, and lead to unavailability of network services. Mitigation often involves configuring network hardware to drop or rate-limit malicious traffic, which can be slow and less flexible.
- Scalability Issues: CNs may struggle to scale their infrastructure to handle sudden increases in traffic during a DDoS attack, making them more vulnerable to attacks that use a large number of botnet devices.

DDoS in SDN (Software-Defined Network):

- Programmable Infrastructure: SDN decouples the control plane from the data plane and provides a more programmable network infrastructure. This means that network behavior can be dynamically adjusted.
- Mitigation Advantages: In SDNs, DDoS mitigation can be more dynamic and automated. Network controllers can detect traffic anomalies and reconfigure network devices in real-time to redirect or drop malicious traffic.
- Isolation and Segmentation: SDNs can create isolated network segments and apply fine-grained policies to limit the impact of DDoS attacks. This can help prevent the attack from affecting the entire network.
- Granular Control: SDNs provide granular control over network traffic, which allows for more efficient traffic filtering and redirection during an attack.

The key contribution of a literature review paper on Software-Defined Networking (SDN) is to provide a comprehensive synthesis of the existing body of knowledge on SDN, offering a valuable resource that summarizes essential concepts, identifies research gaps, and highlights trends, ultimately serving as an informative guide and reference for researchers, students, and practitioners in the field.

2. SDN Architecture

The phrase "software-defined networks" (SDN) is used to refer to a network design where the forwarding status of the data plane is managed by a third-party control plane. By separating the forwarding and control activities of a network, this architecture allows network control to be directly programmable and gives applications and network

services access to an abstraction layer over the underlying infrastructure. The three layers and three interfaces listed below make up the backbone of the SDN design.

2.1 The Data Plane

The data plane is made up of the network's packet-forwarding devices. Various protocols are supported for sending and receiving data between the end hosts and the remote peers that manage the communication. Instead of physically separating the control plane from the data plane, SDN does it in software [1]. SDN/OpenFlow-enabled switch solutions include Switch Light, Open vSwitch, Pica8, Pantou, XorPlus, etc..

2.2 The Control Plane

The SDN controller, which is part of the control plane, decides where data should be delivered. This "network brain" is represented by the SDN control plane. The controller's principal function is to act as a mediator between the network's data layer and the applications that are using that layer. By moving the control plane into software, it will be easier to implement changes and streamline operations. A network administrator may make rule and configuration changes to several switches without leaving the control room. There are now around twenty SDN controllers out there. In this part, we provide a list of all relevant open-source SDN controllers that are both free to use and functional. One popular SDN controller that is compatible with the OpenFlow protocol is Java's Project Floodlight controller. Floodlight can be used with module apps as well as RESTful apps. Module applications are those developed using the controller and are written in Java. These systems are simultaneously running and are included into the programming for the floodlights. To communicate with the controller, REST applications must use the RESTful API that is made available by Floodlight. You may query the controller for data and provide it the latest information about your trip arrangements using this interface. Disengaging the controller from TCP/IP traffic is one way to stop malicious network application injection [16], although the RESTful API is less versatile than the module application API when it comes to interfacing with the controller.

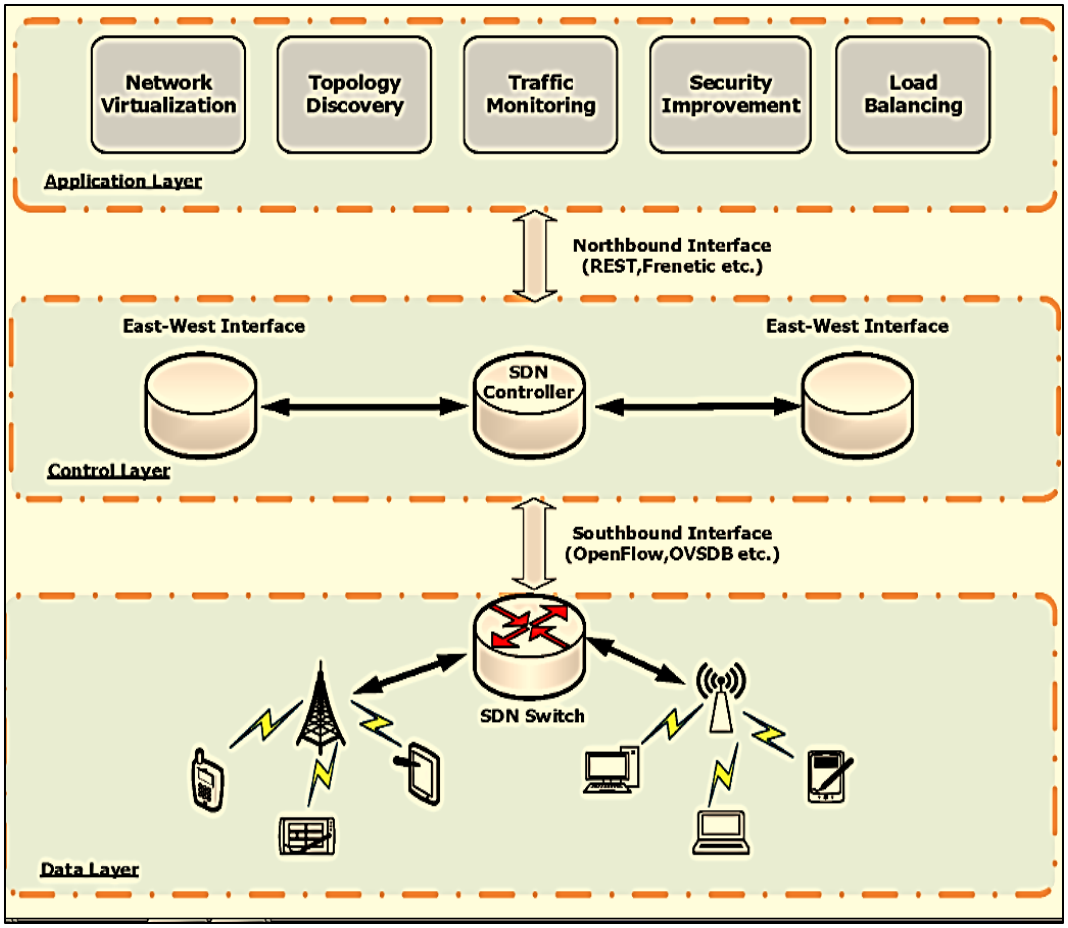

Figure 1 SDN architecture

2.3 The Application Plane

The term "application plane" is used to describe all the programs that utilize the northbound interface's capabilities to provide the logic necessary to run a network. Included are programs like routers, firewalls, ACLs, load balancers, monitors, IDS, scan detectors, DDoS attack mitigation methods, and so on (see Figure 1.2 for details). [19] . To put it simply, a network application defines the rules, and those rules are subsequently translated into southbound-specific instructions that regulate the activities of the forwarding devices. IDS network software, for instance, may monitor traffic, user activity, packet payload, and other system-wide metrics. If contaminated data packets could be automatically filtered away after being identified as malicious, it might greatly reduce the spread of infection. However, many issues with security in the deployment of network applications still need to be addressed.

3. Role of ML/DL Techniques for Detecting DDoS Attacks

Machine Learning (ML) and Deep Learning (DL) techniques play a significant role in the detection of Distributed Denial of Service (DDoS) attacks in network security. Their roles include:

- ***Pattern Recognition:*** ML and DL models can learn and recognize patterns in network traffic. By analyzing historical data and identifying normal traffic patterns, these techniques can detect deviations from the norm, which may indicate a DDoS attack.

- ***Anomaly Detection:*** ML models, such as Support Vector Machines (SVMs) or neural networks, can be trained to identify anomalies in network traffic. DDoS attacks often exhibit unusual behavior, such as a sudden surge in traffic, and anomaly detection can flag these events.
- ***Real-time Monitoring:*** ML/DL models can continuously monitor network traffic in real time. They can process large volumes of data quickly, making them suitable for identifying sudden and rapid changes in traffic associated with DDoS attacks.
- ***Adaptive Detection:*** ML/DL models can adapt to evolving attack techniques. As attackers develop new methods, ML models can be retrained to detect these emerging threats, offering more robust defense mechanisms.
- ***Feature Engineering:*** ML and DL practitioners can engineer features from network traffic data to enhance detection. These features may include packet size, packet rate, protocol distribution, entropy, and other relevant characteristics that help distinguish normal traffic from DDoS attacks.
- ***Behavioral Analysis:*** Deep Learning techniques like Recurrent Neural Networks (RNNs) can analyze temporal dependencies in network traffic data. This allows them to capture deviations from expected network behavior, which is valuable in DDoS detection.
- ***Packet Analysis:*** ML/DL models can examine packet-level data to identify malicious patterns, including characteristics like packet size, source/destination IP addresses, and payload content.

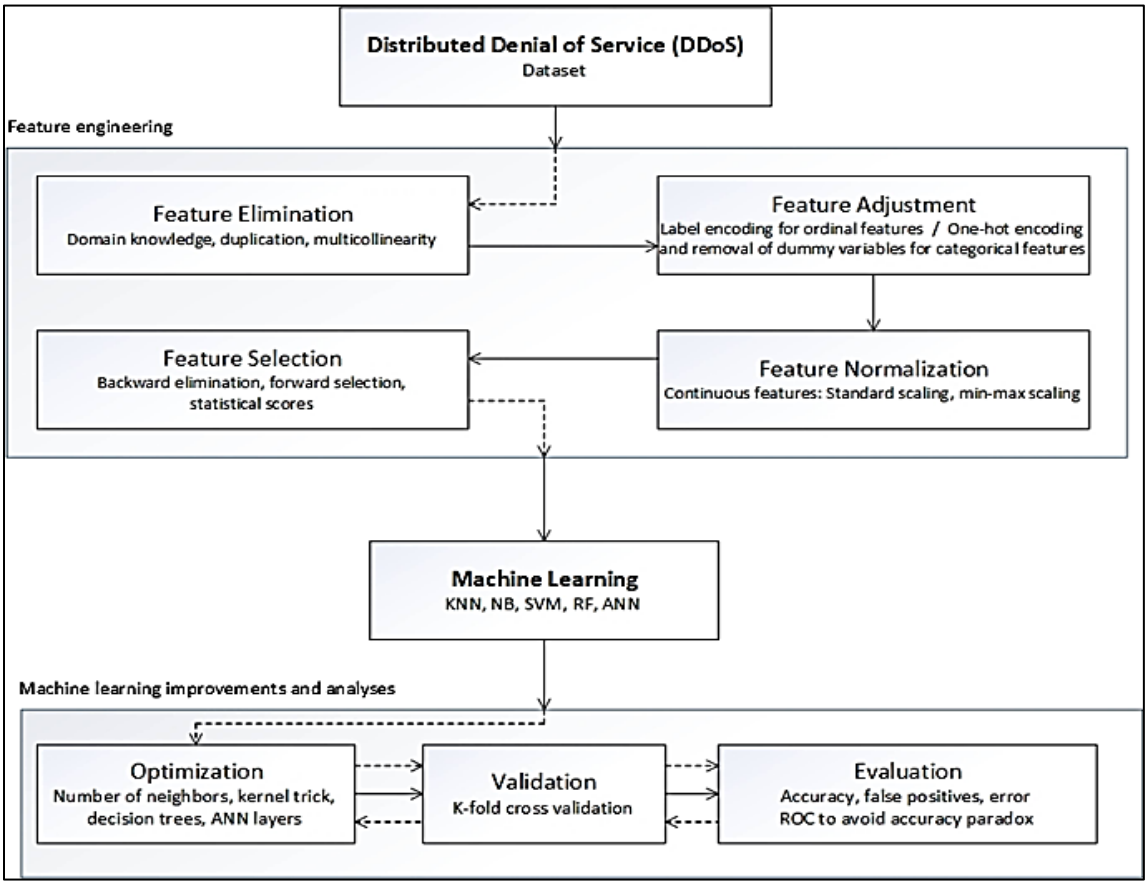

Figure 2: Methodology for generalized machine learning/deep learning-based DDoS detection systems

- ***Flow-Based Analysis:*** Convolutional Neural Networks (CNNs) can be applied to flow data, describing network connections between hosts. CNNs can extract features and identify patterns that are indicative of DDoS attacks.
- ***Hybrid Approaches:*** Combining ML/DL techniques with traditional network-based approaches, such as rate limiting and blacklisting, can provide a multi-layered defense against DDoS attacks. ML models can identify attacks, while traditional mechanisms can be used for mitigation.
- ***Transfer Learning:*** Pre-trained models, often used for different tasks or in a general domain, can be fine-tuned for DDoS detection. Transfer learning makes models more effective in identifying new and evolving attack patterns.
- ***Multi-Modal Detection:*** Combining multiple types of data sources, such as flow data, packet data, and network logs, provides a more comprehensive view of network activity. This enhances the accuracy of DDoS detection.
- ***Scalability:*** ML/DL techniques can handle large volumes of data and scale efficiently to analyze network traffic across complex infrastructures, making them suitable for both small and large-scale networks.
- ***Automated Response:*** ML/DL models can be integrated into automated response systems, allowing for immediate actions when DDoS attacks are detected, such as traffic rerouting or rate limiting.

4. Review of Machine learning Approaches to Mitigate DDoS attacks in SDN

This section provides an in-depth review of the various ML-based methods available for identifying and protecting SDN networks against DoS and DDoS assaults. Based on their methodology, ML approaches can be broken down into the first group, which focuses on improving existing ML methods by using multiple ML algorithms in concert to boost overall performance (especially detection accuracy), the second group, which focuses on developing new ML-based approaches by hybridizing or relying on multiple ML algorithms, and the third group, which focuses on investigating a single ML classification algorithm. The most important results from each research are highlighted here, and a summary table comparing the strengths and weaknesses of different ML methods is provided. The following provides a comprehensive analysis of various methods.

4.1 Ensemble ML Methods

Multiple classifiers may be used in an ensemble technique, and the ensemble itself may be made up of various machine learning classifiers. Multiple separate classifiers may be combined to complete the training process. An optimal weighted voting ensemble (OWVE) model is proposed to identify and mitigate distributed denial of service (DDoS) assaults. Different hyperparameter settings are used for the SVN, RF, and GBMC in the ensemble model. For the CIC-DDoS-2019 and CAIDA-2007 datasets, respectively, the ensemble model demonstrates a high classification accuracy of 99.41% and 99.35%. To defend SDN against DDoS assaults, the voting-based intrusion detection framework, an ensemble ML model, was suggested in ref. [1]. Using the UNSW-NB15, CICIDS2017, and NSL-KDD datasets for training and testing, the suggested voting model outperformed the competition in terms of detection accuracy.

To better categorize and detect DDoS assaults, the researchers at ref. [2] created an ensemble ML approach using K-mean and RF. After extensive training and testing on the InSDN dataset, the suggested system showed a flawless detection accuracy of 100%. K-NN, naive Bayes (NB), support vector machine (SVM), and self-organizing map (SOM) algorithms were presented as part of an ensemble ML for anomaly detection in [3]. Models are tested and prioritized using data from CAIDA's 2016 dataset. The detection accuracy and false-positive rates of the ensemble technique were, however, poor for both the ensemble and the single ML algorithms.

4.2 Hybrid Machine Learning Methods

Multiple hybrid ML-based strategies, including [4], used a combination of SVM and random forest (RF) classification algorithms to distinguish between benign and malicious traffic. A genuine SDN dataset was used to test and assess the method, with positive results: high accuracy (98.8 percent) and low numbers of false alarms. In order to improve the classification performance of identifying DDoS flooding assaults against OpenFlow switches and SDN controllers, the authors of ref. [6] presented a hybrid technique based on SVM and SOM. The method was evaluated using the CAIDA dataset, where it showed a detection rate of 98.13 percent and an accuracy of 97.2 percent.

For real-time detection systems, Ref. [7] looked at P4 programmability and K-NN, RF, SVM, and ANN algorithms. They suggested using a DDoS attack detection (DAD) system that operates automatically. Overall, the DAD method has a detection rate of 98% for SYN flood assaults on local SDN switches. The decision tree (DT), naive Bayes (NV), support vector machine (SVM), and RF techniques were used to defend the SDN controller against DDoS assaults in Ref. [8]. The method was tested on the NSL-KDD dataset, where it performed well for DT (99.97%) but poorly for SVM (60.19%).

In order to study and identify TCP-SYN flood DDoS assaults against the SDN controller, researchers in ref. [9] looked into a number of ML classification models, including DT, random forest (RF), AdaBoost (AB), multiayer perceptron (MLP), and logistic regression (LR). All categorization models tested showed significant improvement over the baseline. K-NN, DT, ANN, and SVM are only some of the ML techniques used by ref. [10] to determine whether or not packets traversing an SDN network were part of a DDoS assault. They demonstrated that among classification algorithms, DT has the highest accuracy (99.75%) while SVM has the lowest (81.48%).

The model for detection and classification based on ML was presented in ref. [11]. To identify TCP, UDP, and HTTP flood DDoS assaults, they used four common classifiers: K-NN, quadratic discriminant analysis (QDA), Gaussian naive Bayes (GNB), and classification and regression tree (CART). When compared to other methods, CART excels in terms of both prediction accuracy (98%) and speed of prediction (12.4 ms on average during training). An method to DDoS attack detection and mitigation was presented in ref. [12]. They started using a support vector machine (SVM) for classification, then used kernel principal component analysis (KPCA) as an approach for selecting features, and then improved the SVM's settings with a genetic algorithm (GA). The detection accuracy of the suggested model was 98.907%.

More than one ML algorithm is used by various methods, as seen in [13]. To defend an SDN network from DDoS assaults, they used six different machine-learning algorithms: NB, SVM, K-NN, extreme gradient boosting (XGBoost), DT, and RF. The XGBooSt method achieves 99.7% accuracy, whereas the other algorithms only get about 80%. The authors of ref. [14] developed a strategy to identifying DDoS assaults using DT and SVM algorithms. The KDD CUP dataset was used to test and evaluate the suggested method. However, they performed poorly. The accuracy rates of DT and SVM, for instance, are just 78% and 85%.

In order to identify DDoS assaults in an SDN setting, the authors of ref. [15] use four ML classification algorithms (i.e. KNN, SVM, ANN, and NB). KNN was shown to have the highest detection accuracy (98.3%) of the recommended methods when it came to identifying DDoS assaults when tested on a synthetic dataset. The detection accuracy of the remaining ML classifiers, in comparison, was only moderate. In [16], the authors presented a malleable IDS to detect and stop SDN DDoS assaults at low rates. They use the CIC-DoS-2017 dataset for their evaluations after training the IDS with six different ML algorithms (including RT, REP tree, RF, SVM, MLP, and J48). The suggested IDS was successful in detecting 95% of threats.

An attack detection framework using K-Means and K-NN algorithms was developed in ref. [17]. To lessen the burden on the controller, they implemented a detection trigger method using the data plane switches. Both simulated and NSL-KDD datasets were used to test the framework, and both showed excellent detection accuracy. For the purpose of accurate attack detection and optimum network resource usage, the authors of reference [18] suggested a

DDoS attack mitigation strategy for the SDN network that relies on a bandwidth-control mechanism and the extreme gradient boosting (XGBooST) algorithm. The method was tested in an SDN environment, where it was shown to be 99.9% accurate with a low false-positive rate. The controller is also used in the suggested system.

The "Artificial Immune System-IDS" (AIS-IDS) was suggested in ref. [19], and it was modeled after the human immune system. The suggested method takes biologically-inspired fuzzy logic into account to fully automate the process of detecting and fixing network anomalies. It was shown to outperform other classifiers on both simulated and CICDDoS 2019 datasets in terms of detection accuracy and other performance parameters. Furthermore, the SDN controller was updated to make use of the suggested method. An SVM-based, DT-based, NB-based, and LR-based method for detecting DoS and DDoS assaults in an SDN network was presented in ref. [20]. SVM obtained 97.5% accuracy, NB and DT at 96%, and LR at 89.98% when tested on a simulated dataset.

A method for identifying Distributed Denial of Service attacks was presented in ref. [21] using SVM, DT, K-NN, and BN classifiers. Training and testing on the NSL-KDD dataset revealed that the DT classifier had the highest detection rate (95.16 percent). To identify TCP SYN and UDP flood DDoS assaults against the SDN controller and flow-table switch and bandwidth saturation attacks, the authors of ref. [22] used MLP, RF, SVM, and DT algorithms. The suggested model was evaluated and trained using a synthetic dataset, which revealed that classification results for the controller DDoS assault were worse (less than 90% accuracy for SVM and MLP) compared to those for the flow-table switch and bandwidth attacks. The algorithms SVM, J48, and NB were presented as a protection mechanism against DDoS assaults in ref. [23]. The suggested defensive system achieved a 99.40% detection accuracy for classification after being trained and tested on the NSL dataset.

In order to protect against DDoS and port scan assaults, the researchers at reference [24] designed a fast SDN defensive system that would analyze IP flow traffic every five seconds. Particle swarm optimization (PSO), multi-layer perceptron (MLP), and discrete wavelet transform (DWT) are used in the suggested system, which is implemented on the SDN controller and used to identify anomalies. It also employs a game-theoretic strategy to reduce the impact of distributed denial-of-service assaults. All assaults, including DDoS and port scans, are being detected by the suggested security system, and the SDN has been successfully restored thanks to the mitigation approaches. Finally, Ref. [25] developed a method for classifying and detecting DDoS (i.e., HTTP, UDP flooding assaults, and Smurf) based on seven ML algorithms (i.e., K-NN, RF, NB, SVM, linear regression (LR) DT, and ANN). All classification methods benefit from the proposed method's high average detection accuracy, which is applied at the SDN controller.

Table 1: ML Approaches for Mitigating DDOS in SDN

Reference	Approach	ML/Ensemble Models	Datasets Used	Detection Accuracy	Drawbacks
[1]	Voting-Based Intrusion Detection Framework	Not specified	UNSW-NB15, CICIDS2017, NSL-KDD	Better than other approaches	Not specified
[2]	K-Mean and RF Ensemble	K-Mean, RF	InSDN	100%	Not specified
[3]	Ensemble Model	K-NN, Naïve Bayes, SVM, Self-Organizing Map	CAIDA 2016	Low detection accuracy and high false-positive rates	Low detection accuracy and high false-positive rates

[13]	Multiple ML Algorithms	NB, SVM, K-NN, XGBoost, DT, RF	Not specified	XGBoost with the highest accuracy (99.7%)	Not specified
[14]	DT and SVM Ensemble	DT, SVM	KDD CUP dataset	Low performance (DT: 78%, SVM: 85%)	Low performance
[15]	Multiple ML Classifiers	KNN, SVM, ANN, NB	Synthetic dataset	KNN with high detection accuracy (98.3%)	Not specified
[16]	Flexible IDS	RT, REP tree, RF, SVM, MLP, J48	CIC-DoS-2017	Moderate detection rate performance (95%)	Moderate detection rate performance
[17]	K-Means and K-NN	K-Means, K-NN	Synthetic, NSL-KDD	High detection accuracy	Not specified
[18]	XGBoost and Bandwidth Control	XGBoost	Not specified	99.9% accuracy	Not specified
[19]	Artificial Immune System-IDS	Not specified	Synthetic, CIC-DDoS 2019	High detection accuracy	Not specified
[20]	SVM, DT, NB, LR	SVM, DT, K-NN, BN	NSL-KDD	SVM with the highest accuracy (97.5%)	Not specified
[21]	SVM, DT, K-NN, BN	SVM, DT	NSL-KDD	DT with the highest detection rate (95.16%)	Not specified
[22]	MLP, RF, SVM, DT	MLP, RF, SVM, DT	Synthetic dataset	Variable performance	Variable performance
[23]	SVM, J48, NB	SVM, J48, NB	NSL dataset	99.40% detection accuracy	Not specified
[24]	Particle Swarm Optimization (PSO), MLP, DWT	PSO, MLP, DWT	Not specified	Functional performance for detection and mitigation	Not specified
[25]	Multiple ML Algorithms	K-NN, RF, NB, SVM, LR, DT, ANN	Not specified	High average detection accuracy	Not specified

5. Review of Deep learning Approaches to Mitigate DDoS attacks in SDN

This section covers the use of single DL, hybrid DL, and ensemble DL to identify SDN DDoS assaults. Again, this part emphasizes the most important takeaways from each study, followed by a table summarizing the most important factors and their constraints. The sections that follow further on DL methods.

5.1. Ensemble DL Approaches

The authors of ref. [26] classified DDoS assaults using convolutional neural networks (CNN), gated recurrent unity (GRU), and long short term memory (LSTM). In the case of a low number of features, the suggested model trained using the CICIDS 2017 dataset obtained a detection accuracy of 99.77 percent. An IDS employing DL ensemble methods, including CNN, RNN, and DNN, was presented for DDoS attack detection in ref. [27]. The detection accuracy of the CICIDS2017 dataset-trained ensemble model was 99.05%, which is very high. In [28], the authors suggest yet another CNN-based ensemble solution to detecting DDoS assaults on SDNs. When tested on the ISCX 2012 dataset, the ensemble model showed a 98.48% accuracy rate in its detection capabilities.

5.2. Hybrid DL Approaches

In order to identify traffic irregularities brought on by DDoS assaults, CNN and LSTM are utilized in ref. [29]. When tested on the InSDN dataset, the suggested method was shown to have a detection accuracy of 96.32 percent. A hybrid DL model implemented on the SDN controller was presented in ref. [30]. In order to spot DDoS assaults as soon as they begin, they use DL algorithms like CNN and LSTM. When tested on the CICIDS2017 dataset, the hybrid method showed excellent detection accuracy (99.45%). Reference [31] described a method for detecting low-rate SDN DDoS assaults using CNN and LSTM, which would be implemented on the SDN controller. The suggested method was tested on a simulated data set, where it performed over 99% of the time. To prevent Distributed Denial of Service (DDoS) assaults, [32] suggested using an RNN, GRU, and LSTM on the SDN controller. Using the InSDN dataset, they found that their suggested method had a high rate of correct detections.

After looking at several classifiers, such as LSTM and CNN, the authors of ref. [33] presented a way to safeguard the SDN controller against DDoS assaults. When tested on the synthetic dataset, the suggested method only managed a detection accuracy of 89.63%. A method for identifying SDN DDoS assaults using an RNN equipped with an autoencoder is proposed in ref. [34]. The suggested approach was tested on the CICDDoS-2019 dataset, where it outperformed previous ML methods in terms of detection accuracy, achieving a rate of 99%. To identify previously unknown DDoS assaults, reference [35] presented a DL-based IDS (DeepIDS). DNN and GRU-RNN (gated recurrent neural network) techniques are used. The suggested system was tested on the NSL-KDD dataset, where it performed poorly (80.7% for DNN and 90% for GRU-RNN).

RNN and GRU were used by the authors of Reference [36] to enhance the performance of their anomaly-based IDS for SDN networks. The suggested method was trained, tested, and evaluated using the NSL-KDD and CICIDS2017 datasets; on the former, it achieved an accuracy of 89% in detecting DDoS assaults, while on the latter, it achieved an accuracy of 99%. CNN, RNN, and LSTM algorithms were presented as a detection method for DoS assaults in ref. [37]. The ISCX 2012 dataset was used to test the effectiveness of the suggested method. For DDoS assaults, the suggested model has a 98% verification accuracy on test data and a 99% accuracy on training data.

It was suggested in ref. [38] that SDN network traffic be classified as either normal or abnormal (attack) using an IDS based on GRU and RNN (GRU-RNN). Regrettably, the suggested method only managed an 89% and 90% detection rate for regular and attack traffic, respectively. Using entropy to identify faked switch ports and a convolutional neural network (CNN) as a classifier to improve accuracy and efficiency while decreasing training costs, the authors of reference [39] suggest a two-tiered approach to DDoS attack detection in SDN networks. This resulted in a high level of accuracy for the DL model (98.98%) but low levels of accuracy for information entropy

(92.37%) and the two-level technique (96.97%) using the suggested strategy. CNN and a transformer (made up of an encoder and a decoder) were presented as part of a hybrid solution to detecting DDoS assaults in ref. [40]. The suggested method was evaluated on the CICDDoS2019 dataset and outperformed all other methods.

5.3. Single DL Approaches

Several methods use a single DL algorithm to identify assaults as early as feasible, such as [41], which presented a controller-based security solution. Using the InSDN dataset for training and evaluation, the suggested method was able to achieve both high accuracy in traffic categorization and low latency and high throughput. Concurrently, a GRU-based SDN defensive system for DDoS attack detection was presented in Ref. [42]. In order to mitigate the impact of attacks on SDN, the suggested system examines each traffic record for IP flows. The method was put to the test on two different situations and two different datasets (CICDDoS 2019 and CICIDS 2018), with successful results in both cases.

An SDN controller-based detection and protection system was presented in ref. [43]. In order to identify DDoS assaults, the system employs a GAN. In the first scenario, when the suggested defensive system was tested, 99.78% of DDoS attacks were detected; in the second scenario, where the CICDDoS 2019 dataset was used, the detection rate dropped to 95.54%. To identify DDoS assaults, the authors of ref. [44] use the stacked autoencoder multi-layer perceptron (SAE-MLP) method. The suggested method was trained and evaluated using a genuine SDN dataset, and it was able to reach a 99.75% accuracy in its identification.

To better identify intrusions, the authors of ref. [45] presented an IDS built on the CNN algorithm. The suggested method was put through its paces on the InSDN dataset, where it scored a 94.01% detection accuracy. DNN was investigated by Makuvaza et al. [46] for detecting SDN DDoS assaults. The suggested method was tested on the CICIDS 2017 dataset and found to have a detection accuracy of 97.25 percent. Similarly, the bi-directional recurrent neural network (BRNN) technique was studied by Ref. [47] to categorize SDN DDoS assaults. The suggested method was trained and evaluated on a synthetic dataset, where it showed a detection accuracy of 99.21%.

TCP, UDP, ICMP, and SYN flood DDoS assaults may be mitigated in an SDN network environment with the help of a real-time mitigation agent based on deep reinforcement learning, as presented in ref. [48]. Therefore, while the mitigation agent is active, around 85% of typical traffic is able to reach the server. An IDS was suggested by Arivudainambi et al. [49] that uses the lion optimization algorithm (LOA) to pick features and a convolutional neural network (CNN) to classify DDoS attacks. When tested on the NSL-KDD dataset, the suggested method has a classification accuracy of 98.2 percent. An SDN controller network application was presented in [50] to monitor for control and data plane DDoS assaults. The suggested method uses the stacked autoencoder (SAE) to identify TCP, UDP, and ICMP DDoS assaults in SDN network settings. Therefore, the suggested system can identify the kinds of DDoS attacks with a success rate of 95.65%.

To keep tabs on network activity, the authors of ref. [51] integrated a network intrusion detection system (NIDS) into the SDN controller. The proposed NIDS makes use of DNN to identify aberrant flows in SDN networks and label them as normal or not. When tested on the NSL-KDD dataset, however, their suggested NIDS obtained only a 75.75% level of accuracy. Ref. [52] proposes a solution that employs an unsupervised restricted Boltzmann machine algorithm to identify SDN DDoS assaults. After being tested on a fabricated dataset, the suggested system showed a 92% detection rate with an 8% false-positive rate. Table 7 provides a concise summary of the DL-based methods and their shortcomings.

Table 1: DL Approaches for Mitigating DDOS in SDN

Reference	Approach	DL Models	Datasets Used	Detection Accuracy	Limitations
[26]	CNN, GRU, LSTM Ensemble	CNN, GRU, LSTM	CICIDS 2017	99.77%	Not specified
[27]	DL Ensemble	CNN, RNN, DNN	CICIDS2017	99.05%	Not specified
[28]	CNN-Based Ensemble	CNN	ISCX 2012	98.48%	Not specified
[29]	CNN and LSTM	CNN, LSTM	InSDN	96.32%	Not specified
[30]	Hybrid DL Model	CNN, LSTM	CICIDS2017	99.45%	Not specified
[31]	CNN and LSTM	CNN, LSTM	Synthetic dataset	More than 99%	Not specified
[32]	RNN, GRU, LSTM	RNN, GRU, LSTM	InSDN	High detection accuracy	Not specified
[33]	Investigative Classifiers	LSTM, CNN	Synthetic dataset	89.63%	Low detection accuracy
[34]	RNN with Autoencoder	RNN	CICDDoS-2019	99%	Not specified
[35]	DeepIDS	DNN, GRU-RNN	NSL-KDD	80.7% (DNN), 90% (GRU-RNN)	Lower detection accuracy
[36]	RNN and GRU	RNN, GRU	NSL-KDD, CICIDS2017	89% (NSL-KDD), 99% (CICIDS2017)	Variable detection rates
[37]	CNN, RNN, LSTM Ensemble	CNN, RNN, LSTM	ISCX 2012	98% (test data), 99% (training data)	Not specified
[38]	GRU and RNN	GRU, RNN	Not specified	89% (normal traffic), 90% (attack traffic)	Relatively low detection accuracy
[39]	Two-Level DDoS Detection	CNN	Not specified	98.98% (DL model), 92.37% (two-level method)	Lower accuracy for information entropy
[40]	CNN and Transformer	CNN, Transformer	CICDDoS2019	High performance	Not specified
[41]	Controller-Based Security System	Not specified	InSDN	High traffic classification accuracy	Not specified
[42]	GRU-Based SDN Defensive System	GRU	CICDDoS 2019, CICIDS 2018	High detection accuracy	Not specified
[43]	GAN-Based Detection	GAN	Real SDN network dataset, CICDDoS	99.78% (real SDN network), 95.54% (CICDDoS 2019)	Not specified

			2019		
[44]	SAE-MLP Algorithm	Stacked Autoencoder, MLP	Realistic SDN dataset	99.75%	Not specified
[45]	CNN-Based IDS	CNN	InSDN	93.01%	Not specified
[46]	DNN for SDN DDoS Detection	DNN	CICIDS 2017	97.25%	Not specified
[47]	BRNN Classification	Bi-Directional RNN	Synthetic dataset	99.21%	Not specified
[48]	Deep Reinforcement Learning	Deep RL	Not specified	Not specified	Operational challenges and efficiency concerns
[49]	LOA and CNN	Lion Optimization Algorithm, CNN	NSL-KDD	98.20%	Not specified
[50]	SAE for Multi-Vector DDoS	Stacked Autoencoder (SAE)	Not specified	95.65%	Not specified
[51]	DNN-Based NIDS	DNN	InSDN	75.75%	Lower detection accuracy
[52]	Unsupervised RBM Algorithm	Restricted Boltzmann Machine	Synthetic dataset	92%	False-positive rate

6. Research Gaps and Open Research Issues

Mitigating DDoS (Distributed Denial of Service) attacks in Software-Defined Networking (SDN) using Machine Learning (ML) and Deep Learning (DL) presents a unique set of challenges and opportunities. Here are some research gaps and open research issues in this specific domain:

- ***Evolving Attack Vectors:*** DDoS attack vectors are continually evolving. Research needs to focus on developing adaptive ML and DL models that can detect and mitigate not only known attack types but also new, previously unseen attack vectors.
- ***Adaptive Mitigation Strategies***: Building ML and DL models that can adapt their mitigation strategies in real-time based on the characteristics of the attack is a critical research challenge. The ability to adjust mitigation actions to minimize collateral damage is essential.
- ***Transfer Learning***: Research should explore the potential of transfer learning to leverage knowledge gained from one type of DDoS attack to enhance the detection and mitigation of other types. This could improve the efficiency of response mechanisms.
- ***Detection vs. Mitigation Balance***: Striking the right balance between detection and mitigation is challenging. Research should address when and how to initiate mitigation actions without impacting legitimate traffic.

- ***Zero-Day Attacks:*** Zero-day DDoS attacks that exploit previously unknown vulnerabilities are a significant threat. Research needs to focus on methods for early detection and mitigation of these attacks.
- ***Performance Optimization***: The resource-intensive nature of ML and DL models can impact the performance and responsiveness of SDN networks. Research should concentrate on optimizing the computational efficiency of these models for real-time operation.
- ***Multi-Layered Defenses:*** Combining ML and DL with traditional security mechanisms like firewalls and intrusion prevention systems is a potential approach. Research should explore how to integrate these layers effectively.
- ***Resource Allocation:*** Determining how to allocate computational resources for ML and DL models in SDN environments is an open issue. Adaptive resource allocation strategies are required.
- ***Data Labeling Challenges:*** Annotated datasets for training ML and DL models are essential. However, labeling network traffic data accurately, especially in the context of SDN-specific attacks, can be difficult. Research should address this challenge.
- ***Robustness to Adversarial Attacks***: DDoS mitigation models are vulnerable to adversarial attacks aimed at deceiving the system. Research should investigate methods for making ML and DL models more robust against adversarial attacks.
- ***Privacy-Preserving Solutions:*** Developing mechanisms to protect sensitive data while still allowing ML and DL models to operate effectively is a critical research gap, especially in the context of SDN.
- ***Interpretability and Explainability***: Understanding how ML and DL models make decisions is essential for network administrators and security analysts. Developing interpretable and explainable models is an ongoing research challenge.
- ***Network Anomaly Detection:*** Beyond DDoS attacks, research should address the detection of various network anomalies that can disrupt SDN environments. These anomalies may not always be the result of malicious activity but can still affect network performance.
- ***Ethical and Legal Considerations***: As automated DDoS mitigation systems become more prevalent, researchers should investigate the ethical and legal implications of actions taken in response to detected attacks.

7. Conclusion

In this literature review (LR) paper, we have examined a wide range of research efforts aimed at mitigating Distributed Denial of Service (DDoS) attacks within Software-Defined Networking (SDN) environments, primarily leveraging Machine Learning (ML) and Deep Learning (DL) approaches. The comprehensive analysis of the selected studies reveals several significant findings. First, ML and DL techniques have demonstrated substantial potential in enhancing DDoS attack detection and mitigation in SDN, showing adaptability to evolving attack vectors and real-time response capabilities. Furthermore, these models exhibit robustness and efficiency, offering a promising route to counter the dynamic threat landscape. However, challenges remain in achieving optimal performance, scalability, and resource efficiency while preserving the interpretability of these models and addressing ethical and legal considerations. Curating labeled datasets and preparing network administrators for the collaborative use of ML and DL-based DDoS mitigation systems are essential steps in realizing the full potential of these technologies. This LR underscores the evolving nature of DDoS threats and the critical need for innovative and adaptive approaches in SDN to ensure the security and stability of modern networks.

8. References:

[1] Maheshwari, A.; Mehraj, B.; Khan, M.S.; Idrisi, M.S. An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment. Microprocess. Microsyst. 2022, 89, 104412. [Google Scholar] [CrossRef]

[2] Swami, R.; Dave, M.; Ranga, V. Voting-based intrusion detection framework for securing software-defined networks. Concurr. Comput. Pract. Exp. 2020, 32, e5927. [Google Scholar] [CrossRef]
[3] Firdaus, D.; Munadi, R.; Purwanto, Y. DDoS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest. In Proceedings of the 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 10–11 December 2020; pp. 164–169. [Google Scholar] [CrossRef]
[4] Deepa, V.; Sudar, K.M.; Deepalakshmi, P. Design of Ensemble Learning Methods for DDoS Detection in SDN Environment. In Proceedings of the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019; pp. 1–6. [Google Scholar] [CrossRef]
[5] Eliyan, L.F.; Di Pietro, R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Gener. Comput. Syst. 2021, 122, 149–171. [CrossRef]
[6] Ahuja, N.; Singal, G.; Mukhopadhyay, D.; Kumar, N. Automated DDOS attack detection in software defined networking. J. Netw. Comput. Appl. 2021, 187, 103108. [Google Scholar] [CrossRef]
[7] Phan, T.V.; Bao, N.K.; Park, M. A Novel Hybrid Flow-Based Handler with DDoS Attacks in Software-Defined Networking. In Proceedings of the 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 18–21 July 2016; pp. 350–357. [Google Scholar] [CrossRef]
[8] Musumeci, F.; Fidanci, A.C.; Paolucci, F.; Cugini, F.; Tornatore, M. Machine-Learning-enabled DDoS Attacks Detection in P4 Programmable Networks. J. Netw. Syst. Manag. 2022, 30, 1–27. [Google Scholar] [CrossRef]
[9] Nadeem, M.W.; Goh, H.G.; Ponnusamy, V.; Aun, Y. DDoS Detection in SDN using Machine Learning Techniques. Comput. Mater. Contin. 2022, 71, 771–789. [Google Scholar] [CrossRef]
[10] Swami, R.; Dave, M.; Ranga, V. Detection and Analysis of TCP-SYN DDoS Attack in Software-Defined Networking. Wirel. Pers. Commun. 2021, 118, 2295–2317. [Google Scholar] [CrossRef]
[11] Tonkal, O.; Polat, H.; Başaran, E.; Cömert, Z.; Kocaoğlu, R. Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. Electronics 2021, 10, 1227. [Google Scholar] [CrossRef]
[12] Sangodoyin, A.O.; Akinsolu, M.O.; Pillai, P.; Grout, V. Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning. IEEE Access 2021, 9, 122495–122508. [Google Scholar] [CrossRef]
[13] Sahoo, K.S.; Tripathy, B.K.; Naik, K.; Ramasubbareddy, S.; Balusamy, B.; Khari, M.; Burgos, D. An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks. IEEE Access 2020, 8, 132502–132513. [Google Scholar] [CrossRef]
[14] Alamri, H.A.; Thayananthan, V. Analysis of Machine Learning for Securing Software-Defined Networking. Procedia Comput. Sci. 2021, 194, 229–236. [Google Scholar] [CrossRef]
[15] Sudar, K.; Beulah, M.; Deepalakshmi, P.; Nagaraj, P.; Chinnasamy, P. Detection of Distributed Denial of Service Attacks in SDN using Machine Learning Techniques. In Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 27–29 January 2021; pp. 1–5. [Google Scholar] [CrossRef]
[16] Polat, H.; Polat, O.; Cetin, A. Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. Sustainability 2020, 12, 1035. [Google Scholar] [CrossRef]
[17] Pérez-Díaz, J.A.; Valdovinos, I.A.; Choo, K.K.R.; Zhu, D. A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. IEEE Access 2020, 8, 155859–155872. [Google Scholar] [CrossRef]

[18] Tan, L.; Pan, Y.; Wu, J.; Zhou, J.; Jiang, H.; Deng, Y. A New Framework for DDoS Attack Detection and Defense in SDN Environment. IEEE Access 2020, 8, 161908–161919. [Google Scholar] [CrossRef]
[19] Alamri, H.A.; Thayananthan, V. Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks. IEEE Access 2020, 8, 194269–194288. [Google Scholar] [CrossRef]
[20] Scaranti, G.F.; Carvalho, L.F.; Barbon, S.; Proença, M.L. Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks. IEEE Access 2020, 8, 100172–100184. [Google Scholar] [CrossRef]
[21] Ahmad, A.; Harjula, E.; Ylianttila, M.; Ahmad, I. Evaluation of Machine Learning Techniques for Security in SDN. In Proceedings of the 2020 IEEE Globecom Workshops, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [Google Scholar] [CrossRef]
[22] Satheesh, N.; Rathnamma, M.; Rajeshkumar, G.; Sagar, P.V.; Dadheech, P.; Dogiwal, S.; Velayutham, P.; Sengan, S. Flow-based anomaly intrusion detection using machine learning model with software defined networking for OpenFlow network. Microprocess. Microsyst. 2020, 79, 103285. [Google Scholar] [CrossRef]
[23] Santos, R.; Souza, D.; Santo, W.; Ribeiro, A.; Moreno, E. Machine Learning Algorithms to Detect DDoS Attacks in SDN. Concurr. Comput. Pract. Exp. 2020, 32, e5402. [Google Scholar] [CrossRef]
[24] Alshamrani, A.; Chowdhary, A.; Pisharody, S.; Lu, D.; Huang, D. 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, Miami, FL, USA, 21–25 November 2017; pp. 83–92. [Google Scholar] [CrossRef]
[25] De Assis, M.V.; Novaes, M.P.; Zerbini, C.B.; Carvalho, L.F.; Abrãao, T.; Proença, M.L. Fast Defense System Against Attacks in Software Defined Networks. IEEE Access 2018, 6, 69620–69639. [Google Scholar] [CrossRef]
[26] Fatmah, A.; Kamal, J.; Fathy, E.; Maher, K.; Abdullah, B.; Khalid, A. Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network. Intell. Autom. Soft Comput. 2022, 33, 923–938. [Google Scholar] [CrossRef]
[27] Mbasuva, U.; Zodi, G.A.L. Designing Ensemble Deep Learning Intrusion Detection System for DDoS attacks in Software Defined Networks. In Proceedings of the 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea, 3–5 January 2022; pp. 1–8. [Google Scholar] [CrossRef]
[28] Haider, S.; Akhunzada, A.; Ahmed, G.; Raza, M. Deep Learning based Ensemble Convolutional Neural Network Solution for Distributed Denial of Service Detection in SDNs. In Proceedings of the 2019 UK/China Emerging Technologies (UCET), Glasgow, UK, 21–22 August 2019; pp. 1–4. [Google Scholar] [CrossRef]
[29] Abdallah, M.; An Le Khac, N.; Jahromi, H.; Delia Jurcut, A. A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–7. [Google Scholar] [CrossRef]
[30] Haider, S.; Akhunzada, A.; Mustafa, I.; Patel, T.B.; Fernandez, A.; Choo, K.K.R.; Iqbal, J. A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. IEEE Access 2020, 8, 53972–53983. [Google Scholar] [CrossRef]
[31] Nugraha, B.; Murthy, R.N. Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks. In Proceedings of the 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Leganes, Spain, 10–12 November 2020; pp. 51–56. [Google Scholar] [CrossRef]
[32] Alshra'a, A.S.; Farhat, A.; Seitz, J. Deep learning algorithms for detecting denial of service attacks in software-defined networks. Procedia Comput. Sci. 2021, 191, 254–263. [Google Scholar] [CrossRef]
[33] Gadze, J.D.; Bamfo-Asante, A.A.; Agyemang, J.O.; Nunoo-Mensah, H.; Opare, K.A.B. An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. Technologies 2021, 9, 14. [Google Scholar] [CrossRef]

[34] Elsayed, M.S.; Le-Khac, N.A.; Dev, S.; Jurcut, A.D. DDoSNet: A Deep-Learning Model for Detecting Network Attacks. In Proceedings of the 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Cork, Ireland, 31 August–3 September 2020; pp. 391–396. [Google Scholar] [CrossRef]

[35] Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M.; El Moussa, F. DeepIDS: Deep Learning Approach for Intrusion Detection in Software Defined Networking. Electronics 2020, 9, 1533. [Google Scholar] [CrossRef]

[36] Tang, T.A.; McLernon, D.; Mhamdi, L.; Zaidi, S.A.R.; Ghogho, M. Intrusion detection in sdn-based networks: Deep recurrent neural network approach. In Deep Learning Applications for Cyber Security; Springer: Berlin, Germany, 2019; pp. 175–195. [Google Scholar] [CrossRef]

[37] Li, C.; Wu, Y.; Yuan, X.; Sun, Z.; Wang, W.; Li, X.; Gong, L. Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. Int. J. Commun. Syst. 2018, 31, e3497. [Google Scholar] [CrossRef]

[38] Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M. Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 202–206. [Google Scholar] [CrossRef]

[39] Liu, Y.; Zhi, T.; Shen, M.; Wang, L.; Li, Y.; Wan, M. Software-defined DDoS detection with information entropy analysis and optimized deep learning. Future Gener. Comput. Syst. 2022, 129, 99–114. [Google Scholar] [CrossRef]

[40] Wang, H.; Li, W. DDosTC: A Transformer-Based Network Attack Detection Hybrid Mechanism in SDN. Sensors 2021, 21, 5047. [Google Scholar] [CrossRef] [PubMed]

[41] Janabi, A.H.; Kanakis, T.; Johnson, M. Convolutional Neural Network Based Algorithm for Early Warning Proactive System Security in Software Defined Networks. IEEE Access 2022, 10, 14301–14310. [Google Scholar] [CrossRef]

[42] Assis, M.V.; Carvalho, L.F.; Lloret, J.; Proença, M.L. A GRU deep learning system against attacks in software defined networks. J. Netw. Comput. Appl. 2021, 177, 102942. [Google Scholar] [CrossRef]

[43] Novaes, M.P.; Carvalho, L.F.; Lloret, J.; Proença, M.L. Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments. Future Gener. Comput. Syst. 2021, 125, 156–167. [Google Scholar] [CrossRef]

[44] Ahuja, N.; Singal, G.; Mukhopadhyay, D. DLSDN: Deep Learning for DDOS attack detection in Software Defined Networking. In Proceedings of the 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 28–29 January 2021; pp. 683–688. [Google Scholar] [CrossRef]

[45] Elsayed, M.S.; Jahromi, H.Z.; Nazir, M.M.; Jurcut, A.D. The role of CNN for intrusion detection systems: An improved CNN learning approach for SDNs. In Proceedings of the International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, Virtual Event, 6–7 May 2021; pp. 91–104. [Google Scholar] [CrossRef]

[46] 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. 2021, 2, 1–10. [Google Scholar] [CrossRef]

[47] Itagi, V.; Javali, M.; Madhukeshwar, H.; Shettar, P.; Somashekar, P.; Narayan, D. DDoS Attack Detection in SDN Environment using Bi-directional Recurrent Neural Network. In Proceedings of the 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Nitte, India, 19–20 November 2021; pp. 123–128. [Google Scholar] [CrossRef]

[48] Liu, Y.; Dong, M.; Ota, K.; Li, J.; Wu, J. Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software-Defined Networks. In Proceedings of the 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 17–19 September 2018; pp. 1–6. [Google Scholar] [CrossRef]

[49] Arivudainambi, D.; KA, V.K.; Sibi Chakkaravarthy, S. LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks. Neural Comput. Appl. 2019, 31, 1491–1501. [Google Scholar] [CrossRef]
[50] Niyaz, Q.; Sun, W.; Javaid, A.Y. A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN). ICST Trans. Secur. Saf. 2016, 4, 1–18. [Google Scholar] [CrossRef]
[51] Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M. Deep learning approach for Network Intrusion Detection in Software Defined Networking. In Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 26–29 October 2016; pp. 258–263. [Google Scholar] [CrossRef]
[52] MohanaPriya, P.; Shalinie, S.M. Restricted Boltzmann Machine based detection system for DDoS attack in Software Defined Networks. In Proceedings of the 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 16–18 March 2017; pp. 1–6. [Google Scholar] [CrossRef]
[53] Novaes, M.P.; Carvalho, L.F.; Lloret, J.; Proença, M.L. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access* 2020, *8*, 83765–83781. [Google Scholar] [CrossRef]
[54] Said Elsayed, M.; Le-Khac, N.A.; Dev, S.; Jurcut, A.D. *Network Anomaly Detection Using LSTM Based Autoencoder*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 37–45. [Google Scholar] [CrossRef]
[55] Karan, B.; Narayan, D.; Hiremath, P. Detection of DDoS Attacks in Software Defined Networks. In Proceedings of the 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 20–22 December 2018; pp. 265–270. [Google Scholar] [CrossRef]
[56] Al-Amiedy, T.A.; Anbar, M.; Belaton, B.; Kabla, A.H.H.; Hasbullah, I.H.; Alashhab, Z.R. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. *Sensors* 2022, *22*, 3400. [Google Scholar] [CrossRef] [PubMed]