JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 01
2024

Research Article
https://doi.org/10.56979/701/2024

A Comprehensive Review on DDoS Attack in Software-Defined Network (SDN): Problems and Possible Solutions

Fateh Ahmed[1], and Irshad Ahmed Sumra[2], and Uzair Jamil[3]

[1]Department of Information Technology, Lahore Garrison University (LGU), Lahore, Pakistan.
[2]Department of Computer Science, Lahore Garrison University (LGU), Lahore, Pakistan.
[3]Department of Computer Science, University of Alabama at Birmingham, Birmingham, AL 35294, USA.
*Corresponding Author: Dr. Irshad Ahmed Sumra. Email: Irshadahmed@lgu.edu.pk

Received: December 11, 2023 **Accepted:** April 21, 2024 **Published:** June 01, 2024

Abstract: This paper provides key insights into the classification of distributed denial of service (DDoS) attacks and defensive techniques to protect software-defined net-works (SDN) in these attacks. The networking industry is evolving due to a revo-lutionary paradigm known as software-defined networking. It is the type of net-work where data and control planes have been decoupled to minimize errors and enable efficient use of network resources. DDoS attacks have proved to be a major threat to any business such as small- and large-scale enterprises. These attacks have the potential to destroy businesses in a few hours. Even giants like Amazon have reported that it has thwarted one of the biggest DDoS attacks. Attackers tar-get various SDN-based networks to cause huge losses to entrepreneurs and busi-nesses. The most worrisome part is that they are still taking place across the globe in no time. Unlike a simple denial of service attack, many nodes initiate an attack on the network or server in a distributed environment. Attacks are seriously damaging the CIA triad: confidentiality, integrity, and availability. Moreover, the performance and security metrics of infrastructure are also affected. As things stand, we need to realize that we can avoid DDoS to some extent but not com-pletely.

Keywords: Classification of Distributed Denial of Service (DDoS) Attacks; Software-Defined Networks (SDN); Defense against DDoS in SDN.

1. Introduction

The motivation for this research work arises from the need to develop robust and adap-tive defensive mechanisms specific to SDN environments, addressing the unique challenges posed by DDoS attacks. By conducting a thorough survey and analysis, the goal is to con-tribute valuable insights that advance the understanding of DDoS defense strategies in the context of Software-Defined Networks. For long, DDoS attacks have been a threat to everyone in any part of the world. According to statistics, these attacks are increasing by a whopping 67 percent yearly [1]. These attacks have the potential to partially or destroy businesses. SDN is also under attack from hackers across the globe. Compromised SDNs mean a lot to hackers as they can easily administer the entire network communication. It is difficult to completely secure the network because of the distributed nature of attacks. We can classify intruders into 2 types [2]. In the context of SDN, internal intruders have access to SDN and have substantial knowledge of networks and security in most cases. They are well equipped to harm the po-tential target. External intruders have no authorized access to SDN and operate externally with tools and tricks to intercept SDN communication. There can be many reasons for launch-ing an attack, including financial gain, revenge, and ideological belief [3]. Attackers over-whelm the victim's bandwidth and other resources to make legitimate services unavailable for legitimate users. Attackers use multiple compromised systems to flood the target net-work or server through botnets. SDN offers numerous benefits in terms of centralized control, enhanced security, and programmability. On the dark side, hackers strive to turn these bene-fits into a nightmare for legitimate

users. That is why, there is a dying need for safeguarding SDN to keep operations up and running without or with minimum disruptions in the long run. Two essential characteristics for identifying a DDoS attack are a high traffic rate and a departure from the usual traffic flooding in the flow. These two traits form the foundation of most SDN intrusion detection systems (IDS) [27]. Extensive research is being carried out to reach to the best possible solution to protect infrastructure in DDoS attacks. This paper high-lights types of DDoS attacks on SDN and makes a comparison between the various protective techniques.

Section 2 defines key security goals in terms of the confidentiality, integrity, and availability (CIA) triad. Section 3 specifically focuses on types of DDoS attacks as they pertain to soft-ware-defined networks. It classifies DDoS attacks based on sub-types and impact. Attention is drawn to the vulnerabilities inherent in traditional networks, juxtaposed with the defining attributes of SDN. Section 4 undertakes a comprehensive review of pertinent literature, cul-minating in a classification of diverse defense mechanisms against DDoS within the context of SDN. Finally, Section 5 serves as the conclusion, encapsulating the findings of this research endeavor.

1.1. Security objectives

Security objectives are established based on confidentiality, integrity, and availability factors, collectively known as the CIA triad, a foundational cybersecurity model guiding the creation of secure systems. The CIA triad advocates for a defense-in-depth approach, which uses sev-eral security tiers to fend off attackers. For example, integrity checks can identify and stop unwanted modifications by viruses, while confidentiality measures like encryption can stop unauthorized access to sensitive data. Availability controls, which include redundancy and disaster recovery plans, guarantee that systems continue to function even in the event of dis-turbances or virus assaults. Even in the case that a virus gets past one line of defense, the other lines can lessen the damage and stop it from getting worse. For instance, backup systems and recovery procedures can return data to its initial condition if a virus threatens data integrity, preserving the organization's capacity to function. Moreover, It offers a framework that is adaptable to changing problems and threats. Organizations can modify their security protocols to guarantee the preservation of confidentiality, integrity, and availability in the face of emerging infections and cyber threats. Maintaining an advantage over new threats and lowering the possibility of security breaches require this flexibility. The CIA triad consists of three key components:

1. Confidentiality: Ensuring data confidentiality involves preventing unauthorized access to sensitive information. Through a variety of techniques, including user education, access limits, encryption, and authentication methods, confidentiality measures seek to prevent unwanted access to sensitive data. By taking these precautions, data is kept private and shielded from theft, tampering, and unauthorized disclosure [26].
2. Integrity: Data integrity ensures that information and programs are altered only in author-ized ways, while system integrity guarantees that systems operate without impairment. Ensuring the dependability and credibility of data for decision-making, adhering to regu-lations, and upholding the general integrity of systems and procedures all depend on da-ta integrity. Without appropriate data integrity safeguards, businesses run the danger of data loss, fraud, corruption, and tainted decision-making, all of which can have serious negative effects on their finances, legal standing and reputation
3. Availability: This objective ensures that systems are readily accessible and that service is not withheld from authorized users. Ensuring availability is essential for customer satis-faction, productivity, and business continuity. Unavailability or downtime can lead to fi-nancial losses, lower output, harm to one's reputation, and legal ramifications. Therefore, to maintain high levels of availability for their systems and services, firms invest in strong infrastructure, monitoring tools, and proactive maintenance procedures.

1.2. DDoS Under the Scanner

Distributed denial-of-service attacks are tricky to cope with due to their distributed nature. Usually, computing devices have limitations in terms of processing speed and storage. In a distributed environment, attackers plan an attack to crash an application through flooding. In addition to launching an attack manually, there are software that are being used to intercept the communication between legitimate users and servers. So, one doesn't need to be a cyber security expert to initiate DDoS. They can do it with ease with software and online tools. Extensive research has been carried out and is still in progress to mitigate potential threats. Researchers are exploring intrusion detection systems, loss reduction mechanisms, and private and public networks to form formidable strategies against these attacks. Attackers send a large

number of packets through different sources to target the desired network. A botnet is several compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack. The compromised computers are called zombies. Botmasters can update the software to change the type of attack the bot can do. They launch an attack to consume the entire bandwidth so that they can take complete control over the communication of the targeted network. Attackers have access to unlimited compromised nodes to target the victim. Distributed nature makes DDoS attacks devastating and damaging. Every attack can differ from its counterpart in nature. Attacks portray normal behavior so it is difficult to differentiate between legit and spoofed packets [6].

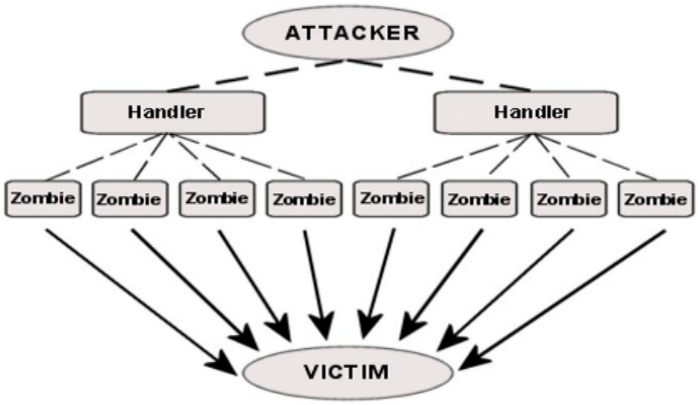

Figure 1. DDoS Architecture

1.3. Types of DDoS Attacks in SDN

1.3.1. Application or Layer 7 DDoS Attacks

Attacks are carried through compromised networks and administered by hackers or at-tackers. The motive behind these attacks is to deny legitimate users from using author-ized resources. [5] This type of attack can be in different forms: a large number of Hy-pertext Transfer Protocol (HTTP) requests and SYN packets can be sent to overwhelm the app's resources; On the other hand, attackers may also send HTTP requests very slowly to consume available resources. It is not an easy job at all to handle attacks on the layer because of its slow rate. Attacks on the application layer can further be catego-rized. Resource exhaustion attacks: In this scenario, the attack is orchestrated in such a way that the resources of servers get consumed randomly at a shallow rate. The rate is even lower than that of normal communication. Session rate limiting attacks: In this type of attack, breached systems send requests at a higher rate but with a lower session rate. Attacks targeting lower request rate: In this scenario, compromised hosts send re-quests at lower rates but with higher session rates.

1.3.2. Network-Level or Layer 3 or 4 DDoS attacks

Protocols are being used to initiate these layers 3 and layer 4 attacks. Botnets are used to generate large amounts of traffic to the server or network [7]. These attacks can also be in various forms such as user datagram protocol (UDP), transmission control protocol (TCP), internet control message protocol (ICMP), and synchronized (SYN) packets. These assaults typically result in severe operational damages and are used to deny access to servers. Massive overage costs and account suspension are a couple of them. Because the traffic is typically quite large, the scale of these attacks is typically measured in gigabits per second (Gbps) or packets per second (PPS). In actuality, most network infrastructures can be fully taken down with 20 to 40 Gbps, however, the most powerful attacks can exceed 200 Gbps[25].

Table 1. Classification and Impact of DDoS Attacks

Main Type	Sub Type	Impact
Application-Level DDoS Attacks	Resource Exhaustion Attacks	Resources of servers can be consumed randomly at a very slow rate. [5]
Application-Level DDoS Attacks	Session Rate Limiting Attacks	Botnets send requests at a higher rate but with a lower session rate to consume resources.

Application-Level DDoS Attacks	Request Rate Limiting Attacks	Compromised hosts send requests at lower rates but with higher sessions to consume resources.
Network-Level DDoS Attacks	Flooding attacks	An intensive attack on the resources through flooding of ICMP, TCP, and UDP to overwhelm resources. [7]
Network-Level DDoS Attacks	Protocol attacks	Flooding Attack on a protocol such as SYN Flood in an attempt to consume all critical resources.
Network-Level DDoS Attacks	Reflected attacks	The server can send packets back to the spoofed IP upon receiving a huge amount of UDP packets to DNS using forfeited IP.
Network-Level DDoS Attacks	Amplification attacks	The attacker controls the services of providers by making huge responses to each of the messages received.

1.4. Comparison between software-defined networks and conventional networks:

Main Characteristics of Conventional Networks:A conventional network is a static network that is comprised of 7 layers of Open Systems Interconnection(OSI) architecture. Data Link and Network layers are responsible for providing networking capability. In conventional networks, the management plane is used for monitoring and management tasks, the control plane handles coordination among the network devices, and the data plane is used for tasks related to data. Network administrators need to be actively engaged because any small upgrade in the network will be carried out manually regardless of the size of the network. Few elements in conventional networks can disrupt operations and be time-consuming[24]:

- New protocol for the resolution of every problem
- Manual configurations for error handling
- Limited testing environment
- Complex network control

Main Characteristics of SDN : SDN is the latest network architecture that separates the network plane from the data plane and has distinct features. Unlike traditional old networks, data and network planes have been separated in SDN. Devices are handled through a centralized controller. With SDN, control has been shifted from network devices to the centralized controller that assists network devices in forwarding packets. The network is programmable to interact with network devices efficiently and effectively. Administrators can easily handle network resources. Enhanced SDN provides the latest features to prevent the network from unauthorized access. The following are the main features of SDN[25]

- Programmability
- Centralized control
- Dynamic global control

SDN is pivotal in offering reliable defense against DDoS [7]. The decoupled nature of SDN offers great flexibility in doing research. The findings of research then can be easily implemented practically. All in all, the architecture of SDN offers ample room to convert your thoughts into practical implementation to get rid of DDoS. Centralization provides a strong platform for the controller to get all the required details about the related network. Controllers frequently monitor network traffic for any mishaps. In case of any compromised host, the centralized component has the potential to dynamically isolate them and validate legitimate users. The programmability feature offers a space to convert AI-based findings into programs for better prevention against intrusions in the future. Dynamic upgradation of rules enables prompt response in case of DDoS. The controller indicates new rules to the entire network to protect it from new attacks. Figure 2 indicates the key difference between traditional and SDN-based networks [28]. As a result of the comparison, it is evident that software-defined networks are far better than conventional networks. However, there are still several factors and threats that can have a significant impact on the performance of SDN.

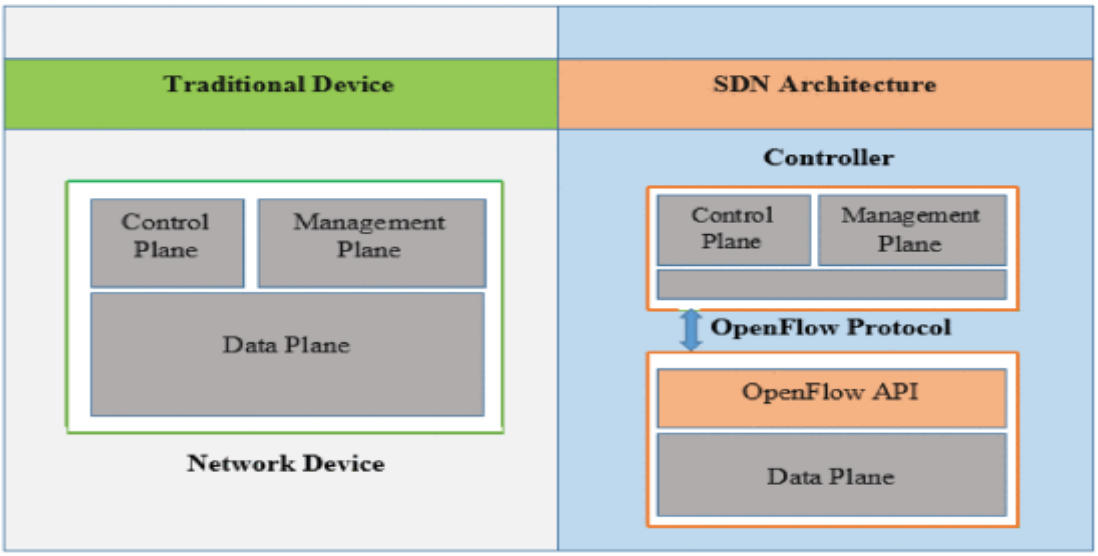

Figure 2. Conventional Networks vs Software-Defined Network

1.5. Threats to SDN

Optimized performance is desired in all the networks. There are a few key elements that one should not bypass while evaluating SDN. There are many factors such as bandwidth, internet speed, latency, and throughout that could impact the performance of SDN [9]. Availability is the other factor that needs to be taken care of. It can be expressed in percentage and defined as the uptime in a given period. Ideally, availability should be above 99.9 percent. Talking about SDN, if the controller fails due to any attack, there can be serious consequences of it. Security is another main component of any kind of network that cannot be neglected in any circumstances [30]. The network is vulnerable to many threats that include but are not limited to theft of data, alteration of data, and denial of service. The controller of SDN can be targeted by exploring vulnerabilities in it. Scalability is another important factor that plays a critical role in the performance of the network. It refers to the ability of the network to extend itself without impacting it.

2. Literature Review

The following techniques have been used to make a comparative analysis of existing defensive mechanisms against DDoS in SDN :

- K-Means
- K Nearest Neighbor (KNN)
- Generative Adversarial Network (GAN)
- Deep Reinforcement Learning
- Entropy-based method
- Z-Score-based technique

In this study, [10] summarize DDoS attacks, concerning defense. It analyzes prevention mechanisms in SDN. It discusses source, mid-level, target end, and layered strategy. There are many software-defined solutions but few of them contradict each other. It is a fact that viruses are increasingly transmitted over the internet to harm users. There is a need to collect a large amount of affected data for the analysis. It is challenging and time-consuming for anti-virus manufacturers to evaluate them manually. Numerous automatic codes are available on the internet to launch DDoS with ease. Security mechanisms of hardware, software, and level of awareness are different on the internet from traditional security. Unlike a simple denial of service attack, multiple targets can come under fire from multiple resources at the same time. DDoS is more damaging and devastating in comparison with a simple attack [29]. The Paper mentioned defensive mechanisms involving software-defined measures, online document scanning, and anti-virus technology. While elaborating on the source-level strategy, the paper suggests node deployment at the gateway router to allow consistent monitoring of traffic. In case, it detects any change in the behavior of regular traffic, it will start filtering the traffic. For defense, Mid-Level networks and nodes are usually inside the main router and trained to detect abnormal behavior of network packets. Defense strategy is based upon application design at the target end. Nodes are deployed on the closest router to the target end for

the detection of viruses. There is a need for a layered model because a single line of defense is not enough to combat DDoS.

Authors [11] present an adversarial example attack to trick Android devices equipped with in-cloud firewalls. They used a bi-objective Generative Adversarial Networks (GANs) variation of GANs to produce adversarial examples. There are two discriminators in the bi-objective GANs. In the first, examples are classified as malicious or benign, while in the second, examples are classified as adversarial or normal. According to the experiments, Tecncet Myapp and AndroZoo are the sources of benign apps. Tests were conducted in various scenarios and compared the suggested system's performance with a few other systems that have been documented in the literature. Python along with development libraries are employed for TensorFlow and Keras, two deep-learning applications. To avoid overfitting, the parameters for the training step were set as follows: the loss function when performing binary classification tasks, binary cross-entropy, a traditional loss function, is utilized as the default function.

Cui [12] mentioned that threshold detection and machine learning-based mechanisms are two of the most widely used ways to detect DDoS in SDN. There is a variation in network traffic patterns because of the emergence of edge, cloud, and mobile computing. This rapid change in the traffic makes the handling of hundreds of routers and switches tough for admins. Taking advantage of its decoupled nature, SDN can easily manage network devices through applications running on servers. This unified control, programmability, and global visibility make SDN software-defined. SDN is very famous in industry and academia. Even tech giants like Google have used it with great effect. Despite its enormous use, it has a few security challenges to be addressed. Hackers make frequent attempts to overwhelm normal service by forwarding huge traffic. Moreover, many DDoS attacking tools are easily accessible to people. Distributed Denial of Service attacks have distinct properties: easy to launch an attack, difficult to defend, and massive destruction. Despite the improvement in its defense capabilities, traditional networks are not much programmable making it tougher to launch reliable defense mechanisms.

Researchers [13] applied the improving genetic algorithm backpropagation (IGA-BP) network to address the security challenges in big data. The Internet of Things (IoT) has contributed significantly to sectors like medical sciences, logistics, and automobiles because of its ability to provide distributed servers, nodes, and software for smooth communication. However, threats and attacks had a great impact on it. The web model is trained on malicious activities and intrusion datasets to detect an attack. Sparse Convolute Networks (SCN) that form complex hypotheses using neurons are used to analyze IOT intrusion threats. Given output is further processed in hidden layers. This method reduces intrusions in IoT data. Training patterns rightly differentiate between a threat and normal patterns. Network Intrusion Detection Systems (NIDS) are much better than other traditional techniques to detect intrusions. IoT devices use Internet Protocol to transfer information from source to destination. Existing intrusion detection mechanisms may not be appropriate to offer protection against modern-day threats. So, IoT intrusions were put under scanner through SCN in the proposed solution []. Physical and virtual links, centralized architecture, and large data processing are the main characteristics of any IoT device. It is important to note that these characteristics can also disrupt IOT-enabled communication. These devices include printers, and refrigerators and operate with the assistance of artificial intelligence (AI) such as Amazon Alexa and Google Assistant. It is easy to hijack devices through malicious attempts. IoT devices are manufactured keeping security in mind. Billions of connections and huge data transmission make it difficult to keep security intact all the time. IoT devices are vulnerable to man-in-the-middle attacks, pose estimation, and code injection. Intruders can also control IoT devices remotely. Management of these devices is critical to minimize intermediate attacks. Intrusion detection systems utilize software and devices to monitor and detect malicious activities in the network. Host-based intrusion, network-based intrusion, wireless intrusion, and network behavior analysis are among the widely used methods. Literature mentions the DDoS evaluation dataset to process evolutionary sparse convolution network intrusion (ESCNN).

Galadima [14] and Ghourab et al [22] pinpoint knowledge gaps and highlight previously proven moving target defense (MTD) components in SDN against DDOS[20]. By decoupling the traditional control and data planes, Software Defined Networks (SDN) have developed to completely transform previous networking standards and make it possible for networks to be programmable, portable, and autonomous. Despite their effectiveness, there are some challenges as well. The controller gives the SDN a centralized perspective on network topology. Smart cities, smart grids, and other applications are expected to have a

major impact on society through the fast-growing Internet of Things (IoT) network. Edge computing provides services, data, or apps closer to the location of need. IoT is constrained in all respects—random access memory(RAM), and central processing unit (CPU). As more and more of them are integrated, effective security becomes progressively more challenging, particularly for low-power devices. The IoT platform is susceptible to availability attacks like denial-of-service (DDOS), surveillance, and exploit execution because of these constraints and its static nature. A few authors have not taken into account the assessment of quality of service (QoS) and system performance, and there are others whose suggested method affected QoS and system performance. This research gap will be filled by the suggested MTD mechanism, which also covers various performance metrics to support the context. The theory behind the suggested mechanism was primarily developed by an author who did not have any significant flaws and thought of it as an economical shuffling scheme that takes overhead into account. However, it did not take into account DDoS attacks that target IoT device exploitation or SDN IoT-Edge Architectures, which this study sheds light on [34]. To determine the MTD mechanism's resistance to DDoS attacks, the system is compared to a static system, and its Defense Performance is assessed using various metrics and factors. The attack was carried out using a customized Hping3 script, and static network topology. To combat reconnaissance assaults, which are the initial stage of cyberattacks and are aimed at servers running in an SDN environment. There is an architecture that makes use of the concept of shadow servers. Traffic is sent to round-robin-selected shadow servers as soon as probing is identified. After that, the chosen shadow server replies to the probing traffic sent by the attacker. In reaction to the probing traffic, the IP address of the shadow web server will be modified to match that of the actual web server [21].

Gupta [15] make a comparison between various studies carried out on SDN controllers such as OpenFlow, sampled flow (sFlow), real-time (RT) Flow, OpenDaylight (ODL), and Ryu. The OpenFlow and sFlow-RT flow analytics are the components of the SDN motor that the F1ow-TrApp framework aimed at establishing malicious components, from low level to high level. DDoS detection mechanism using some constraints on key for every traversal is recommended [32]. It has been developed and shown to outperform the current QoS strategy for the prevention of distributed denial of service attacks in a Mininet emulator. The FADM was proposed as a small and efficient framework for identifying and preventing SDN DDoS attacks. An entropy-based method is used to quantify the net properties, and the support vector machine (SVM) classifier is used to identify any anomalies in the network. By introducing the agent, traffic can be quickly dealt with while harmless traffic continues unhindered. This prevents controller resources from depleting while guaranteeing regular network access for authorized users. Detection and mitigation techniques of common types of DDoS attacks using a sFlow analyzer adapting threshold algorithm were mentioned. They illustrate how network traffic, which consists of both trusted and untrusted, is used to compute the dynamic threshold. It evaluates the accuracy, mitigation mechanism, and detector. By utilizing the Redis Simple Message Queue, various controllers can exchange policies for preventing attacks. Because of policy sharing, distributed attacks can be avoided. To scan DDoS traffic via controller, the sFlow-RT tool is recommended. The sFlow strategy illustrates how integration with the controller lessens control layer overhead and increases accuracy. Analysis shows the average reaction times of ODL and Ryu. ODL reacts more swiftly than Ryu [34].

Auhtors are proposed a deep reinforcement learning-based method that finds the best throttling policy for SDN. The component of router throttling enables us to safeguard against DDoS attacks by limiting the rate of abnormal traffic. Adapting to the varied server loads is a challenge. Extensive research is being carried out in this regard. To address the aforementioned issue, the DeepThrottle method based on deep reinforcement learning was established to give protection against DDoS. Results of the survey indicated improvement in forwarding of trusted traffic to the target server. The DDoS attack overloads the targeted server with excessive traffic from multiple nodes in an attempt to exhaust the resources of legitimate hosts [16]. The component of router throttling enables us to safeguard against DDoS attacks by limiting the rate of abnormal traffic. However, it is challenging to effectively adapt to diversified loads of servers due to the highly customized nature of router throttling approaches. To adapt to different scenarios, decouple the server load and function. The model is gradually adjusted by the reward function to pass more trusted traffic and throttle more malicious traffic [35].

In this study, authors was inspired by the nascent network function virtualization (NFV) technology. To protect the controller from overload, SDNShield uses attack mitigation units (AMUs) that carry out

authentication. Statistical differentiation (SD), is a fast method to find legitimate flows.TCP connection verification (TCV), the second step, verifies the remaining flow. Research on the security and dependability of the SDN control plane has been ongoing and has become more significant. After analyzing SDN vulnerabilities, one author determined that DDoS posed a serious threat. Numerous works have also addressed SDN's resilience to fluctuating workloads. For example, employed multi-threading on the controller side to increase flow processing capacity. By shifting the control functionality from center to edge devices [17]. An automated method for identifying the features and capacities of SDN switches would serve as the foundation for optimizing control decisions. Several works have been proposed to deal with DDoS attacks and SDN control plane overload. Instead of distinguishing between authentic and counterfeit flows, it seeks to scale up for overload. Multi-layer defense architecture like layered adaptive data (LADs) is another source of inspiration for defense design. Demirci et al [23] provide an overview of how SD and NFV technologies have been combined to produce outcomes.

Tan et al [18] introduce collaborative detection methods using K-Means and K-nearest neighbors(KNN) to improve the efficiency of detection. One popular technique for detecting DDoS attacks is the statistical information entropy algorithm. Although this method has some one-sidedness and its accuracy depends on threshold selection, it can process large amounts of traffic data quickly and at low computational cost. To identify and lessen DDoS attacks, a joint scoring system (JESS) that is based on entropy is beneficial. It detects DDoS attacks using joint entropy, which doesn't put more strain on the switches. A model was developed in the Mininet for verification and presented a technique for statistically analyzing traffic entropy to better defend the network against DDoS attacks. Machine learning-based network anomaly detection algorithm is very useful in detecting DDoS in SDN. Using training data as a basis, machine learning algorithms can create models and categorize traffic according to the flow of characteristics. DPTCM-KNN is suggested to detect abnormal behavior of traffic.

Highlight an entropy-based method for the detection and removal of attacks. The destination IP address is used in this method to calculate entropy. It offers early attack detection and effectively lessens the impact of attacks once they are discovered. "Safety," another entropy-based mechanism is used to mitigate flooding attacks [19]. A comprehensive analysis of the mitigation strategy using a range of performance metrics is provided by this work. According to the performance results, it outperforms an existing defense strategy [27]. The author presented a time-slicing-based controller scheduling method. Using this method, time slices are distributed based on the intensity. DDoS attacks primarily aim to slow down a system's processing and online services by focusing on its memory, CPU, and bandwidth. DDoS attacks are getting bigger and more intense every year. A 2.3 terabyte(Tbps) DDoS attack was launched against Amazon Web Services (AWS) in February 2020. As a result, DDoS attackers discovered that attacking online services was more beneficial. Nowadays, spoofing IPs are used to carry out flooding DDoS attacks, and figuring out which spoofs to use is the hardest part of trying to find the attack's origin. The controller, however, is the most crucial component of the SDN out of all of these entities. The spoof packets are sent to SDN switches in a DDoS attack to overwhelm its resources. The packets that users send are dropped as a result of this congestion.

Table 2. Comparative Analysis of Existing Techniques

Sr.	Authors	Approach	Dataset	Remarks
1	Wenliang et al [10]	Source Policy, Intermediate net work Policy, Victim End Strat egy, IP Filtering Strategy	Distributed Simulation	A distributed strategy was introduced.
2	Novaes et al [11]	Anomaly detection System based on GAN	Public dataset CICD-DoS 2019	Demonstrated that the system efficiently detected up-to-date common types of DDoS attacks

3	Cui et al [12]	ML-based and Threshold-based DDoS detection	Distributed Simulation	An inclusive and detailed classification of the DDoS detection mechanism is introduced.
4	Ali et al [13]	IGA-BP network using an autoencoder model	DDoS evaluation dataset	More than 99% accuracy.
5	Galadima et al [14]	Moving target defense (MTD)mechanism	The MTD system is evaluated against the static system	The MTD network did not accept any packets.
6	Gupta et al [15]	SDN Controllers: ODL and RYU	Examined ODL and RYU in terms of response time	ODL outperforms RYU on certain parameters
7	S.Chen et al [16]	Routing throttling mechanism based on deep reinforcement learning	Tested on scenarios of MARL, DP+Load and DP+SE	DP+SE method reduces the percentage of malicious traffic by 59%.
8	K.Y Chen et al [17]	NFV-based defense framework against DDoS attacks in SDN	WIDE-MAWI Working Groups DITL dataset	More than 90% of trusted flow falls in a white area
9	Tan et al [18]	Collaborative detection methods using K-means and KNN	NSL-KDD Dataset	99.03% average precision
10	Swami et al [19]	Z-score-based technique to detect DDoS attack	Tested on simulation environment of Mininet and RYU	Decreases CPU usage by 74% after detection

3. Conclusion

This study has carefully analyzed and classified several kinds of DDoS assaults in addition to defensive tactics meant to protect Software-Defined Networking (SDN) setups. But it's critical to understand that only putting one protective strategy into practice won't end the fight against DDoS attacks. Because cyber threats are dynamic in nature, adversaries must constantly adapt and evolve their strategies, calling for a proactive and comprehensive strategy for defense. Defensive strategies are only as good as their capacity to avert newly discovered avenues of assault. Consequently, it is crucial to commit to continuous research and development. Organizations can work to provide the strongest defense against DDoS assaults while reducing the time and computing complexity involved by consistently improving defensive tactics and technologies. Essentially, the defense against DDoS attacks is an unrelenting endeav-or that calls for alertness, creativity, and cooperation among members of the cyberse-curity community. Organizations can only hope to successfully combat the constantly changing threat landscape offered by DDoS attacks in SDN environments through persistent efforts in research, development, and implementation.

References

1. Sam Cook, "20+ DDoS attack statistics and facts for 2018-2024," Comparitech Blog.
2. Benzekki, K., El Fergougui, A., Elbelrhiti Elalaoui, A "Software-defined networking (SDN): a survey" Security and Communication Networks, 9(18), 5803–5833. 2016.
3. Zargar, S. T., Joshi, J., Tipper, D. "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks" IEEE Communications Surveys and Tutorials, 2013
4. Brooks, R. R., Yu, L., Ozcelik, I., Oakley, J., Tusing, N. "Distributed Denial of Service (DDoS): A History. ," IEEE Annals of the History of Computing, 44(2), 44–54. 2022.
5. Mahadev, Kumar, Vinod; Kumar, Krishan, "Classification of DDoS attack tools and its handling techniques and strategy at the application layer" 2nd International Conference on Advances in Computing, Communication, Automation (ICACCA). 2022.
6. Luo, Shibo; Wu, Jun; Li, Jianhua; Pei, Bei "A Defense Mechanism for Distributed Denial of Service Attack in Software-Defined Networks." IEEE, Ninth International Conference on Frontier of Computer Science and Technology (FCST) - 2015.
7. Tamanna, Tasnim; Fatema, Tasmiah; Saha, Reepa "SDN, A research on SDN assets and tools to defense DDoS attack in cloud computing environment". IEEE 2017 International Conference on Wireless Communications, Signal Processing and Networking(WiSPNET),2017.
8. Yan, Qiao; Yu, Richard; Gong, Qingxiang; Li, Jianqiang "SoftwareDefined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments A Survey, Some Research Issues, and Challenges" IEEE Communications Surveys,andTutorials,2015.
9. Ohri, P., Neogi, S. G., Muttoo, S. K "Security Analysis of Open Source SDN (ODL and ONOS) Controllers" IEEE International Students' Conference on Electrical, Electronics and,Computer-Science,SCEECS,2023.
10. Luo, W, Han, W "DDOS Defense Strategy in Software Definition Networks. " Proceedings 2nd International Conference on Computer Network, Electronic, and Automation,ICCNEA,2019,186–190.2019.
11. Novaes, M. P., Carvalho, L. F., Lloret, J., Proenc¸a, M. L. "Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments. " Future Generation,Computer,Systems,125,156–167.2021.
12. Cui, Y., Qian, Q., Guo, C., Shen, G., Tian, Y., Xing, H., Yan, L. "Towards DDoS detection mechanisms in Software-Defined Networking."Journal of Network and Computer,Applications,2021.
13. Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damasevi ˇ cius, R, Bahaj, S. A. "Threat Analysis and Distributed Denial ˇ of Service (DDoS) Attack Recognition in the Internet of Things (IoT). " Electronics 2022, Vol. 11, Page 494, 11(3), 494. 2022.
14. Galadima, H., Seeam, A., , Ramsurrun, V. "Cyber Deception against DDoS attack using Moving Target Defence Framework in SDN IOTEDGE Networks" 3rd International Conference on Next Generation Computing Applications, NextComp 2022.
15. Gupta, N., Tanwar, S., Behal, S., Badotra, S "DDoS attack defense mechanism using sFlow. ," International Conference on Data Analytics for Business and Industry, ICDABI 302–308.2022.
16. Chen, S., Shen, C., Wu, C, Shen, Y "DeepThrottle: Deep Reinforcement Learning for Router Throttling to Defend Against DDoS Attack in SDN" IEEE International Performance, Computing, and communications conference (IPCCC) 2022.
17. Chen, K. Y., Liu, S., Xu, Y., Siddhrau, I. K., Zhou, S., Guo, Z., Chao, H. J. "SDNShield: NFV-Based Defense Framework Against DDoS Attacks on SDN Control Plane" IEEE/ACM Transactions on Networking Volume: 30, Issue: 1, February 2022.
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, 8, 161908–161919, 2020.
19. Swami, R., Dave, M., Ranga, V. "Addressing Spoofed DDoS Attacks in Software-defined Networking. " 6th International Conference for Convergence in Technology, 2021.
20. International Journal of Information Security (2024) 23:141–185 https://doi.org/10.1007/s10207-023-00764-1
21. Hyder, M.F., Ismail, M.A.: INMTD: intent-based moving target defense framework using software-defined networks. Eng. Technol. Appl. Sci. Res. 10(1), 5142–5147 (2020).
22. Ghourab, E.M., Azab, M.: Software-defined moving-target defense for resilient trust-worthy VANETs. TechRxiv (2022)
23. Demirci, S., Demirci, M., Sagiroglu, S.: Virtual security functions and their placement in software-defined networks: a survey. Gazi Univ. J. Sci. 32(3), 833–851 (2019). [24] https://www.irjet.net/archives/V6/i12/IRJET-V6I1248.pdf

24. Martina Stoyanova Todorova and Stamelina Tomova Todorova, DDoS Attack Detection in SDN-based VANET Architecture, Innovation Communication Technologies and,Entrepreneurship(ICTE)
25. Y. Xu, Z. Sun and Z. Sun, "SDN-based Architecture for Big Data Network," 2017 In-ternational Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (Cy-berC), Nanjing, China, 2017, pp. 513-516,
26. S Samonas, D Coss, The CIA strikes back: Redifining confidentiality, integrity, and availability in security, Journal of Information System Security, 2014
27. M. I. Kareem and M. N. Jasim, "The Current Trends of DDoS Detection in SDN Envi-ronment," 2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA),Baghdad,Iraq,2021,pp.29-34,d
28. Saad Hikmat Haji, Subhi R. M Zeebaree, Rezgar Hassan Saeed and Siddeeq Yousif Ameen, Comparison of software-defined networking with traditional networking, Asian Journal,2021.
29. Hussain, S.K., Ramay, S.A., Shaheer, H., Abbas T., Mushtaq M.A., Paracha, S., & Saeed, N. (2024). Automated Classification of Ophthalmic Disorders Using Color Fundus Images, Volume: 12, No: 4, pp. 1344-1348 DOI:10.53555/ks.v12i4.3153
30. Zhong, X. J., Liu, S. R., Zhang, C. W., Zhao, Y. S., Sayed, A., Rajoka, M. S. R., ... & Song, X. (2024). Natural Alkaloid Coptisine, Isolated from Coptis chinensis, Inhibits Fungal Growth by Disrupting Membranes and Triggering Apoptosis. Pharmacological Research-Modern Chinese Medicine, 100383.
31. Abbas, M., Arslan, M., Bhatty, R. A., Yousaf, F., Khan, A. A., & Rafay, A. (2024). Enhanced Skin Disease Diagnosis through Convolutional Neural Networks and Data Augmentation Techniques. Journal of Computing & Biomedical Informatics, 7(01).
32. Sunny, S., Houg, J., Navaneeth, S., Aniqa, S., John Kofi, A., & Namakkal-Soorappan, R. N. (2023). Abstract P2073: Hyperbaric Oxygen Therapy Protects The Myocardium From Reductive Stress-induced Proteotoxic Remodeling. Circulation Research, 133(Suppl_1), AP2073-AP2073.
33. Shibu, N., Rajkumar, A., Sayed, A., Kalaiselvi, P., & Namakkal-Soorappan, R. (2022). N-Acetyl Cysteine Administration Impairs EKG Signals in the Humanized Reductive Stress Mouse. Free Radical Biology and Medicine, 192, 71-72.
34. Shah AM, Aljubayri M, Khan MF, Alqahtani J, Hassan MU, Sulaiman A, et al. ILSM: incorporated lightweight security model for improving QOS in WSN. Comput Syst Sci Eng. 2023;46(2):2471-2488 https://doi.org/10.32604/csse.2023.034951.