International Journal of Multidisciplinary Research and Growth Evaluation.

Analytical study of effects of DDoS mitigation methods

Hema Dhadhal [1*], Dr. Paresh Kotak [2]
[1] Research Scholar GTU (Gujarat Technological University), Ahmedabad, Gujarat, India
[2] AVPTI (AV Parekh Technical Institute) Rajkot, Gujarat, India

* Corresponding Author: **Hema Dhadhal**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 05
September-October 2023
Received: 04-09-2023;
Accepted: 24-09-2023
Page No: 728-731

Abstract
Distributed Denial of Service (DDoS) attacks continue to pose a significant threat to network infrastructure and services. Software Defined Networks (SDNs) have emerged as a promising technology to enhance network flexibility and adaptability. This paper explores various DDoS attack mitigation approaches within the context of SDNs, with a focus on their effectiveness, limitations, and key considerations.
The study begins by providing an overview of DDoS attacks and their evolving complexities. It then delves into the fundamental principles of SDNs and their potential advantages in combating DDoS attacks. Various mitigation techniques are analyzed, including rate limiting, flow diversion, and traffic anomaly detection, and their applicability in an SDN environment is discussed
Our research takes a multi-dimensional approach, evaluating the performance of mitigation methods in terms of attack detection, response time, false positives, and the impact on legitimate traffic. Additionally, the study considers the adaptability of these methods to emerging threats, such as IoT-based attacks and zero-day vulnerabilities.
Furthermore, we discuss the trade-offs and challenges associated with the implementation of these methods, including their impact on user experience, resource utilization, and operational overhead.
The results of this comparative analysis aim to provide valuable insights for organizations and network security professionals in selecting appropriate DDoS mitigation strategies. This paper provides insights into the evolving landscape of DDoS attack mitigation in Software Defined Networks, emphasizing the need for a proactive and dynamic defence strategy to protect network infrastructure and ensure uninterrupted service availability. This study serves as a valuable resource for mitigating the risks and consequences of DDoS attacks in today's interconnected and digitally-dependent world.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.5.728-731

Keywords: SDN, DDoS Mitigation, defence methods

Introduction
DDOS Attack Overview
DDoS (Distributed Denial of Service) attacks in the context of Software-Defined Networking (SDN) can have significant impacts on various planes of the SDN architecture. SDN's separation of the control plane, data plane, and application plane allows for a more flexible and dynamic network, but it also introduces new attack vectors and vulnerabilities. Here's an overview of DDoS attacks in SDN, considering their effects on each plane:

Control Plane
- **Impact:** DDoS attacks on the control plane can disrupt the centralized controller's ability to manage the network. Attack traffic can overwhelm the controller's resources and lead to misconfigurations or network-wide failures.

- **Effects:** Loss of control can lead to unauthorized access, misrouting of traffic, and service degradation. The attacker might also gain insights into network policies and topologies.

Data Plane

- **Impact:** DDoS attacks targeting the data plane can flood network links and devices with malicious traffic, causing congestion and packet drops. This can render the network unusable for legitimate traffic.
- **Effects:** Network outages and service disruptions are common outcomes. The attacks can lead to reduced Quality of Service (QoS), increased latency, and packet loss, affecting the performance of applications and services.

Application Plane

- **Impact:** DDoS attacks at the application plane target specific services, applications, or virtualized functions orchestrated by SDN. These attacks can overwhelm these services and degrade their availability.
- **Effects:** Services, including critical ones, may become inaccessible, impacting business continuity. Attackers can also exploit application vulnerabilities, leading to data breaches and further network compromise.
- To mitigate the impact of DDoS attacks in SDN, several strategies can be employed:
- **Traffic Engineering:** SDN controllers can reroute traffic in real-time to mitigate the effects of DDoS attacks. This involves optimizing the use of network resources and reconfiguring flows to bypass congested or compromised paths.
- **Rate Limiting:** Implementing rate limiting policies within SDN controllers can help to control the volume of traffic reaching vulnerable network elements, reducing the impact of DDoS attacks.
- **Anomaly Detection:** Employing anomaly detection algorithms in the control plane can identify unusual traffic patterns indicative of DDoS attacks. The controller can then take proactive measures to mitigate these attacks.
- **Isolation and Quarantine:** SDN can be used to isolate or quarantine affected parts of the network, preventing DDoS attacks from spreading and causing further damage.
- **Scalability and Load Balancing:** SDN's flexibility allows for the dynamic allocation of resources and the load balancing of traffic, which can help distribute the impact of DDoS attacks more effectively.
- **Security Policies:** Implement robust security policies in the SDN controller to filter and block malicious traffic at the network's edge before it reaches vulnerable network elements.

In conclusion, DDoS attacks in SDN can disrupt all three planes of the architecture, and mitigating these attacks requires a combination of traffic management, security measures, and adaptive network policies to maintain network performance, availability, and security.
To mitigate the impact of DDoS attacks in SDN, several strategies can be employed:

- **Traffic Engineering:** SDN controllers can reroute traffic in real-time to mitigate the effects of DDoS attacks. This involves optimizing the use of network resources and reconfiguring flows to bypass congested or compromised paths.
- **Rate Limiting:** Implementing rate limiting policies within SDN controllers can help to control the volume of traffic reaching vulnerable network elements, reducing the impact of DDoS attacks.
- **Anomaly Detection:** Employing anomaly detection algorithms in the control plane can identify unusual traffic patterns indicative of DDoS attacks. The controller can then take proactive measures to mitigate these attacks.
- **Isolation and Quarantine:** SDN can be used to isolate or quarantine affected parts of the network, preventing DDoS attacks from spreading and causing further damage.
- **Scalability and Load Balancing:** SDN's flexibility allows for the dynamic allocation of resources and the load balancing of traffic, which can help distribute the impact of DDoS attacks more effectively.
- **Security Policies:** Implement robust security policies in the SDN controller to filter and block malicious traffic at the network's edge before it reaches vulnerable network elements.

Below given in Table 1. We show the comparative analysis of different mitigation approaches used in SDN and their effects in networks as well as pros and cons of using each method for mitigation. This provides an insight to the researcher that which method is most suited for their studies along with their effects.

Table 1: Comparision of various mitigation approaches and its effects in SDN

Mitigation Approach	Description	Effects in SDN	Pros	Cons
Rate Limiting	Throttling traffic based on predefined thresholds	Effective at controlling bandwidth consumption	Effective at controlling bandwidth consumption Simplicity and resource efficiency	May disrupt legitimate traffic if not tuned correctly Inadequate against sophisticated DDoS attacks
Flow Diversion	Redirecting suspicious traffic away from the target	- Reduces impact on the target	- Reduces impact on the target - Works well for known attack patterns	- Requires flow path modifications within SDN - Ineffective against unknown attack patterns
Anomaly Detection	Analyzing network behavior for deviations	- Detects unknown or evolving attack patterns	- Detects unknown or evolving attack patterns - Provides advanced threat detection	- May produce false positives - Requires historical data and machine learning models
Traffic Scrubbing	Cleaning malicious traffic before reaching the target	- Protects the target from attack traffic	- Effective for application-layer DDoS attacks	- Requires specialized scrubbing centers or cloud-

			- Protects the target from attack traffic	based services - May introduce latency
ACL-based Filtering	Implementing Access Control Lists (ACLs) to block malicious traffic	- Immediate and granular control	- Efficient for known attack sources - Immediate and granular control	- Manual rule creation may be time-consuming - Limited in handling sophisticated attacks
SDN-Based Adaptive Policies	Dynamically altering network policies based on attack detection	- Provides adaptability to various attack types	- Real-time response to changing attack patterns - Provides adaptability to various attack types	- Requires a well-defined policy management system - Complex policy creation and management
AI/ML-Based Approaches	Leveraging machine learning for advanced threat detection	- Automation and continuous learning	- Effective in identifying evolving DDoS attacks - Automation and continuous learning	- May require significant computational resources - Continuous training and fine-tuning needed
Blockchain-Based Approaches	Utilizing blockchain for secure routing and traffic verification	- Tamper-proof and resilient	- Enhances network trust and authentication - Tamper-proof and resilient	- Requires blockchain integration within SDN infrastructure - Potential scalability concerns
Hybrid Approaches	Combining multiple mitigation techniques for comprehensive defense	- Maximizes DDoS attack resilience	- Maximizes DDoS attack resilience -Adaptive and versatile	- Complex to manage and may require considerable resources - Coordination between methods can be challenging

This combined table provides a holistic view of each mitigation approach, including its effects on SDN, advantages (pros), and disadvantages (cons). The choice of approach should consider the specific security needs and constraints of the SDN environment.

Table 2: Comparative analysis of various mitigation methods using performance metrics

Metric	Rate Limiting	Flow Diversion	Anomaly Detection	Traffic Scrubbing	SDN-Based Adaptive Policies	AI/ML-Based Approaches	Hybrid Approaches
Effectiveness	Moderate	Moderate	High	High	High	High	High
Resource Utilization	Low	Moderate	High	Moderate	Moderate	High	High
Latency Impact	Low	Moderate	Moderate	High	Moderate	High	Moderate
Scalability	High	High	Moderate	High	High	Moderate	High
Detection Time	Fast	Fast	Moderate	Fast	Fast	Fast	Fast
False Positives	Low	Low	Moderate	Low	Low	Low	Low
Complexity	Low	Moderate	High	Moderate	Moderate	High	High
Adaptability to New Attacks	Limited	Limited	High	Limited	High	High	High
Management Overhead	Low	Low	Moderate	High	Moderate	High	High
Cost-Effectiveness	High	Moderate	Low	Moderate	Moderate	Low	Moderate

Table 2 provides a comparative analysis of DDoS attack mitigation methods using various performance metrics. Each method's effectiveness, resource utilization, latency impact, scalability, detection time, false positives, complexity, adaptability to new attacks, management overhead, and cost-effectiveness are evaluated. The choice of mitigation method should consider the specific requirements and constraints of the network.

Conclusion

The field of Distributed Denial of Service (DDoS) attack mitigation in Software-Defined Networking (SDN) has seen significant advancements and is crucial in ensuring network resilience and security. Various DDoS mitigation approaches have been explored, each with its own strengths and limitations.

Network-based mitigation strategies are effective in mitigating volumetric attacks but may falter against sophisticated application-layer attacks. SDN-based solutions offer dynamic traffic engineering and centralized control, adapting to emerging threats, but they require a robust SDN infrastructure. Cloud-based services provide scalable 24/7 protection but may introduce latency. Application-layer mitigation is granular but may not be suitable for all attack types. Anomaly-based detection can adapt to new threats but may generate false positives. Hybrid approaches combine strengths but can be complex to implement

As DDoS attacks continue to evolve and grow in scale, DDoS mitigation in SDN will remain a critical research and development area. The future holds the promise of more robust, adaptive, and efficient solutions that can protect networks and services from even the most sophisticated attacks. Collaboration between researchers, network engineers, and security experts will be essential in advancing the field and ensuring the resilience of network infrastructures.

References

1. T Mahjabin, Y Xiao, G Sun, W Jiang. A survey of distributed denial-of-service attack, prevention, and mitigation techniques, Int. J Distrib. Sens. Networks, 2017, 13(12). doi: 10.1177/1550147717741463.
2. SR Talpur, T Kechadi. A survey on DDoS attacks: Router-based threats and defense mechanism in real-world data centers, FTC 2016 - Proc. Futur. Technol. Conf., no. December, 2017, 978-984. doi: 10.1109/FTC.2016.7821722.
3. J Singh, S Behal. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions, Comput. Sci. Rev.

2020; 37:100279. Doi: 10.1016/j.cosrev.2020.100279.

4. B Pande, G Bhagat, S Priya, H Agrawal. Detection and Mitigation of DDoS in SDN, 2018 11th Int. Conf. Contemp. Comput. IC3. 2018, 1-3. doi: 10.1109/IC3.2018.8530551.
5. M Imran, MH Durad, FA Khan, A Derhab. Reducing the effects of DoS attacks in software defined networks using parallel flow installation, Human-centric Comput. Inf. Sci. 2019-2020; 9(1):1-19. doi: 10.1186/s13673-019-0176-7.
6. T Xing, D Huang, L Xu, CJ Chung, P Khatkar. Snort Flow: A Open Flow-based intrusion prevention system in cloud environment, Proc. - 2013 2nd GENI Res. Educ. Exp. Work. GREE, 2013, 89-92. doi: 10.1109/GREE.2013.25.
7. A Imran. SDN Controllers Security Issues, [Online], 2017. Available: ayesha.a.imran@student.jyu.fi.
8. K Kalkan, L Altay, G Gür, F Alagöz. JESS: Joint Entropy-Based DDoS Defense Scheme in SDN, IEEE J. Sel. Areas Commun. 2017-2018; 36(10). Doi: 10.1109/JSAC.2018.2869997.
9. S Zavrak, M Iskefiyeli. A feature-based comparison of SDN emulation and simulation tools, Proc. Int. Conf. Eng. Technol.(ICENTE), 2017-2018, 214-217.
10. MHH Khairi, SHS Ariffin, NM Abdul Latiff, AS Abdullah, MK Hassan. A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN), Eng. Technol. Appl. Sci. Res. 2017-2018; 8(2):2724-2730. doi: 10.48084/etasr.1840.
11. J Wang, R Wen, J Li. Detecting and Mitigating Target Link-Flooding Attacks Using SDN. 2018; 5971:1-13. doi: 10.1109/TDSC.2018.2822275.
12. S Saharan, V Gupta. Prevention and Mitigation of DNS based DDoS attacks in SDN Environment, 2019 11th Int. Conf. Commun. Syst. Networks, COMSNETS. 2019; 2061:571-573. doi: 10.1109/COMSNETS.2019.8711258.
13. T Wang, H Chen, G Cheng, Y Lu. SDNManager: A Safeguard Architecture for SDN DoS Attacks Based on Bandwidth Prediction, 2018.
14. KK Karmakar, V Varadharajan, U Tupakula. Mitigating Attacks in Software Defined Network (SDN), 2017 Fourth Int. Conf. Softw. Defin. Syst, 2017, 112-117. doi: 10.1109/SDS.2017.7939150.
15. NN Tuan, PH Hung, ND Nghia, N Van Tho, T Van Phan, NH Thanh. A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN, Electron. 2020; 9(3):1-19. doi: 10.3390/electronics9030413.