A Method for DDOS Attacks Prevention Using SDN and NFV

Mohammad Javad Shayegan (showcaran@gmail.com)
University of Science and Culture
Amirreza Damghanian
University of Science and Culture

Research Article

Keywords: Network Functions Virtualization (NFV), Virtualization of Network Functions (VNF), Network Security Functions (NSF), virtualization, denial of service attack, Moving Target Defense (MTD), DDOS attacks

Posted Date: June 21st, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3054252/v1

Abstract

One of the most widespread forms of security attacks in enterprise networks is Distributed Denial-of-Service (DDOS) attacks. The purpose of DDOS attacks is to intentionally disrupt a network by sending a large amount of false requests. A new path for network design and management has been created with the introduction of Network Functions Virtualization (NFV). NFV architectures allow network functions to be defined quite dynamically. Dynamic definitions of network functions provide the best support for organizational environments. The aim of this research is to prevent DDOS attacks using NFV and SDN platforms. The research method uses the Moving Target Defense (MTD) idea to change the network routes and services location for specific detection packets. The MTD prevents attackers from performing DDOS attacks on real network topologies. A major innovation presented in this research is the selection of moving target defense types based on the processing resources of the overlay networks. The results indicates that the proposed method will save these resources and reduce the time required to check packets in networks.

Introduction

In today's world, there are companies all over the world with a small number of people to multi-national companies, where their main priority is secure communication. Security should be considered a critical prerequisite that has a direct relationship with the service type, infrastructure (hardware and software), extent, and scale. DDoS attacks are network denial of service attacks and are created to disturbance the service. This attack occurs when the desired service is unavailable and disrupted. Network functions virtualization provides a new way for infrastructure form and network setup. NFV is different from traditional virtualization techniques. A NFV may contain one or more virtual machines (VM) that run different software and processes. NFV can be implemented in a variety of conditions, and its application to network security presents a new and economical opportunity [1]. Additionally, by separating the control and management aspects of the network architecture, SDN technology provides automation and programmability. The combination of SDN and NFV creates a network that is built, operated, and managed by software. An NFV network is implemented using the software network features, thereby creating beneficial conditions and optimizing the resources of the network. [2]. Therefore, moving target defense mechanisms change the configuration and structure of networks both during and before an attack, making it very difficult for network connections to be identified.

The idea of moving target defense changes the routes for specific detection packets so that attackers cannot identify the actual network topology for a potential DDOS attack. An attempt has been made in this research to prevent DDOS attacks by changing strategies and procedures in software network platforms, virtualizing network functions, and utilizing moving target defense techniques. In previous research, moving target defense performance has been measured by prevention against attacks, but no attention has been given to details regarding overlay networks and processing resources. The main focus of this defense model is a selective approach to moving target defense, which is determined based on the free bandwidth of virtual machines, as well as the type of strategy used. The criterion considered is the

free bandwidth of the virtual machines of the overlay networks. The more the bandwidth of a processing system is free, the required processing resources are minimized and as a result, the delay for the clients is reduced.

Related Works

Network defense and security in the discussion of DDOS attacks have traditionally been discussed in past articles. In these studies, virtualization criteria and software networks have been considered. Different research has been done on how to maintain security and evolve defense with NFV and SDN.

In the research conducted by Abdulqadder et al.[3], a powerful security scheme for threats in 5G is introduced, in which the algorithm presented with the help of entropy, suspicious packets are classified into normal packets and malicious packets based on their characteristics. In the research conducted by Chowdhary [4], a framework for evaluating cloud network vulnerabilities is presented, which is called MASON, and a method based on the PageRank algorithm is used to identify network services with a high-security risk. In [5], Liu et al, have proposed a DDOS defense algorithm based on the network functions virtualization using a fuzzy system and virtual proxy network to detect and reduce DDOS. In the presented method, suspicious traffic is rerouted and finally disconnected from the network. Aydeger et al. have introduced moving target defense mechanisms in [2], which changes the structure and configuration of networks not only during an attack but also before an attack. In addition, various network forensic mechanisms have been introduced to help determine the attacks location and type as a reactive defense mechanism. In the research done by Rawski [1], the concept of moving target defense with topology mutation is presented. This method identifies the hosts and obtains their topology to identify known vulnerabilities to improve defenses. Singh et al [6] presented a new model to mitigate the effects of DDOS attacks by virtualizing network functions. After making certain changes, this model has used the ARDefense algorithm to defend online services such as websites. Bringhenti et al. [7] have proposed a new method to automatically calculate the optimal layout, location and configuration of virtual firewalls according to a set of security requirements. In the research conducted by Alhebaishi [8], a concept based on the creation of a virtual network architecture was presented, which dynamized the virtual parts and rearranged the logical structure of the network. The purpose of this method is to create complexity in identifying links for each attacker in the system and reducing opportunities to prevent the identification of targets. A comprehensive survey of moving target defense techniques, their key classifications, design dimensions, and attack behaviors with existing moving target defense approaches has been conducted in [9] by Cho et al. In [10] Bulbul and Fischer have proposed a DDOS attack mitigation plan that uses a machine learning algorithm to discover DDOS attack patterns. Chen in [11] discussed the architecture and detailed design of SDNShield, a defense system against DDOS attacks in the data control layer. SDNShield is a linear defense system coordinated by the SDN controller. Agrawal et al [12] presented an algorithm that assigns the network control layer to route decisions and controls the entire network using a centralized network controller. Rangisetti et al in [13], mainly discussed the Address Resolution Protocol (ARP) of forgery in cloud, fog, or hybrid platforms using software networks. The main contribution of Torquato in [14], is a moving target defense that involves a dynamic change to existing attack or

neutralization and defense against attacks. Their research method has been based on alternative reduction based on Throttling. In [15], Valdovinos et al presented a relatively new network paradigm by presenting software networks that can potentially overcome the limitations of current switching networks by separating the control and data layers. The main idea in [16] is to increase resource utilization and support scalability in such a way that the control layer is physically or logically distributed hierarchically in the control layer. Dimolianis et al in [17] proposed an IP-based DDOS protection mechanism in addition to the traditional filter mechanisms that are based on IP rules and increase in proportion to the number of malicious sources.

In [18], a stochastic reward network model is presented to evaluate the success probability of an attack in a cloud infrastructure as a service IaaS (infrastructure as a service) with the help of dynamic defense based on virtual machine migration scheduling. Nguyen et al. [19] adapted three existing models for traditional networks with software networks, which include traditional, semi-software, and virtual networks. The classification of this attack model can deeply explain, analyze, and simulate DDOS. According to Alavizadeh et al.[20], heterogeneous dynamic defense is designed to increase a system's overall security by changing its attack level. Shakil et al [21] provide a method with the help of the blockchain technique, which is a new key idea and integrated security with a cryptographic algorithm in a trustless way and without any intermediary for DDOS defense. In [22] Balarezo and Wang have discussed non-moving target defense-based DOS defense strategies for cloud and non-cloud infrastructures. In [23], Roshani presented a hybrid solution called HyBRIDDAD to detect volumetric DDOS attacks using a pre-trained machine learning model. Jiang et al [24] proposed BSD-Guard, a scalable blockchain-based intrusion detection and defense system to protect software networks from DDOS attacks.

Research Method

After checking the existing controllers and their facilities, it was found that the Floodlight controller should be used for simulating the laboratory platform. This controller is developed in Java programming language and is responsible for maintaining all network rules and providing necessary instructions to the underlying infrastructure on how to manage traffic. Also, the controller supports functional interfaces such as (REST API) for easier programming of people with the product. Mininet has been used to simulate the desired topology of switches, bots, and the main server. MiniNet hosts are based on Linux and the switches used also support OpenFlow for high flexibility in SDN. The Mininet network system is used for creating hosts, and it is a lightweight and efficient method of creating these nodes; however, this method does not provide the opportunity to create virtual machines that operate independently from each other, and the configurations of the hosts are not saved when they are turned off. Also, in mininet, it is possible to connect directly to the controller via its special connection. Next, a script has been developed to execute a DDOS attack with the help of Python version 3 that targets websites and sends fake traffic to the servers. As soon as the script receives the desired port number and packet rate for the website, it begins attacking it. In this method, the links for the attack packets have a route mutation so that the attackers cannot identify the real topology of the network for a possible denial of service attack. At the same time, it allows the defender to save the information of the attacker through forensics. In the end, the

strategy presented in the moving target defense sector needs to be implemented. By implementing the presented method and checking the results, it is observed that the delay in normal packets is reduced and the resources used are reduced compared to the past methods.

3.1 Moving Target Defense Strategy

The second part of the research method is the selection and change in moving target defense strategies. In this research, the idea of the moving target defense approach is taken from the classic "Shell Game" which dates back at least to ancient Greece. By expanding this idea, it is possible to reach a new type of defense in networks, which can defend the networks without looking at the vulnerabilities and hardware and software facilities. By carefully examining the model presented in [2], it can be seen that no attention has been paid to the bandwidth or overhead of the systems. By changing the type of strategies used in overlay networks and replacing random algorithms with measurement methods, it is possible to enhance network defenses.Considering the overhead of the virtual machines involved, it is possible to mutate the packet on the freest virtual machine. In this way, even a larger amount of traffic can be checked in less time, which reduces the delay and increases the efficiency of the system. After the packet passes through the firewall and enters the database (watch list), the desired information of the packet is stored, and according to the number of times the packet passes through the controller, the decision about the packet begins. If the number of packet views is more than the specified limit, the packet will be disconnected, otherwise, if it is less than the specified limit, it will be transferred to the moving target defense section. In this part, decisions are made according to the overhead of virtual shadows host (VSH). In other words, if the specified bandwidth of VSH is less than the allowed limit, the packet will be mutated and re-entered by the tricked networks. If the specified bandwidth is within the normal range, the packet is first entered into the tricked networks and is examined by forensic mechanisms [25].

Additionally, if the packet does not contain any suspicious items, it will continue its route normally and enter the main website or server, and if there are any suspicious items, the packet will be discarded.

3.2 Final implementation

Making changes to the moving target defense in the strategy section is explained in the two pseudo-codes in this section. With the help of pseudo-code, the outline of these two defense algorithms is determined before execution.

The first algorithm is the most important part of the moving target defense strategy. This algorithm is used to select the moving target defense strategy for packets that reach the strategy selection section after passing through the firewall. In the next step, a decision is made according to the network resources. In this pseudo-code, based on the bandwidth, the strategy is selected and the closed route is determined. If the bandwidth exceeds the limit set by the user, it enters the virtual functions of the network. Otherwise, the route mutation strategy will occur and the packet will undergo a route mutation and the route database will be updated.

In Fig. 3, the packet entry section is shown with pseudocode and this algorithm continues until the moment of packet delivery to the strategy selection section. This algorithm specifies the items that need to be stored in the watch list, such as srcIP and dstIP, and indicates the reaction based on the number of packets passed. In this pseudo-code, variables such as SwitchiD, srcIP, dstIP, protocol, and maxUsage are received from the packet and according to the maxUsage number (maximum watching), a decision is made to enter the package or delete it.

If the route mutation occurs, the values of srcIP, dstIP, protocol, and MTDStrategy are sent to the router to perform the mutation. Also, the triggeredUpdate value is updated and the new value is recorded in the database.

Findings

In this research, a virtual machine with specifications (20 processor cores, 32 GB RAM, ubuntu operating system) was used to run the tests. Floodlight is used to implement the main network controller. Java prerequisites must be implemented to run Floodlight. In this study, the practical method of manual implementation has been used. This controller is compatible with many virtual switches such as Open vSwitch and physical switches such as Dell Z9000, Arista 7050, and HP 3500, which shows that it can be implemented in the real environment. In [26], to deal with overload and establish security, VOIP virtualization is introduced and two new frameworks are

presented. sFlow-RT has been used for indexing and outputting system status, monitoring, bandwidth, and some connections.

The sFlow-RT analysis engine is a continuous measurement system that receives information from agents on network devices, hosts, and applications. sFlow-RT transforms raw data into usable variables that are accessible through an API. The variable used in the sFlow-RT engine graphs to display the maximum number of passing flow values (maximum number) is mn_flow. The use of the maximum number is because the attacks will stop after the service is disrupted, and after that, the graph will be downward. Figure 4 shows the number of flows of a normal request (without attack).

In the next step, after executing the attack, the firewall in the controller can be used to prevent and limit the attacks. Figure 5 shows that after applying the firewall control, attacks have been significantly reduced. In this diagram, the attacks peaked at 15,000 packets, and at the end, the attack was completely neutralized.

4.1 Smart Defense by Moving Target Defense Strategy

In the next step, when the controller and indexing engine, and attacks are executed, moving target defense can be implemented. The firewall is programmed by API React, which will create intelligent defense capabilities by sending API commands to the controller and analysis engine. By setting the threshold

value of the allowed traffic, the controller detects attacks. After that, the IP address of the attackers will be detected by the algorithm and sent to the firewall of the controller for defense. In this way, after executing the React software, the parameters of the attack are received from the controller and after cleaning the data, it succeeds in preventing the attack. As a result, the possibility of accessing the desired web service is denied to the attacker. In the next step, according to the moving target defense approach, the maximum flow algorithm is used to implement route mutation and create priority on different routes and change them. IP address and Time to Live (TTL) are two parameters that must be added to the switches to play the role of layer three for the algorithm to work. Using Openflow controllers, layer 1 to 4 functions can be implemented [27]. In this way, by adding routers and NFV network functions, it is possible to check the bandwidth in the controller, if the bandwidth is less than the level of response to the users, the route mutation will occur and otherwise, it will enter the overlay networks to reach the final server.

Evaluation

The proposed defense technique works successfully against DDOS attacks. One of the advantages of this strategy is to reduce the complexity of the system execution compared to the state mentioned in [2]. The choice of moving target defense strategy is determined by factors such as mutation probability, time limit, and alternative probability in [2]. But in the presented method, by reducing the overhead of the overlay network system, the freed resources can be used to respond to normal traffic as much as possible. This method also reduces the required storage and processing space. In this condition, healthy packets can reach the final destination faster than the previous time mutation. An innovation of the proposed method is the replacement of the Russian roulette algorithm by the suggested resource usage method. By classifying the sent packets, the attacker is detected by the controller, then the attack is prevented. In the proposed approach, the processor usage of the device on which the controller is implemented was significantly reduced. Based on the research findings, 10 to 20 percent of the processor is used by the controller in the proposed framework. If all incoming traffic is checked, this number reaches more than 90% of the processor's capacity. Due to the use of the controller software and forensic properties, the system overhead will reach its maximum level when the system is fully loaded. When the system updates the route, the topology information may be stored in the RAM memory, while in other cases, LLDP packets may be required to update the network information. In [2] time of route mutation is shown in the moving target defense. From this time, it can be concluded that the increase in the number of route nodes has a slight delay in the packet arrival time. The complexity of the route mutation execution time is $O(n * \log n)$. The route mutation only causes a few milliseconds of delay. According to the record created in the database, the values are input ID (2 bytes), source IP (4 bytes) and destination IP (4 bytes), protocol type (1 byte), and time (7 bytes). Also, the size of the packet route can be different according to the specified length in the route mutation. The value of 1 byte is the direction of the mutation probability field or the mutation probability of the moving target defense strategy.

Discussion

In the proposed method, attackers are confronted with a continuously changing and random view of the underlying system. In this research, two moving target defense strategies are presented for implementation, one of which operates on layer 7 and the other on layer 3. Thus, a stronger defense can be provided. As this process prevents the attack at the detection phase, it is very time-consuming for the attackers, yet it imposes very little overhead on the system. As a result of route mutation, a different route is created in the packet's inbound route, making it impossible for the attacker to locate it. In [2], the moving target defense decision is made based on Russian roulette, which is determined with a 33% chance; however, the advantage of this method is that it reduces the overhead of the overlay network system, a consequence of taking into consideration the resources available to the system. By using this method, the possibility of the controller being unavailable is lower than 1%, which is an important advantage when researching DDOS attacks.

A further advantage of the proposed approach is the reduction of about 50% in storage space as a result of removing the Tracking database. The entry in the Tracking database is 39 bytes. Due to the possibility of memory overhead as the number of hops increases, the space of this variable has been completely replaced. Table 1 illustrates that a comparison between the proposed method and [2] reveals that it is both advanced and reliable in some criteria. However, the previous method has certain advantages.

Table 1
Comparison between current study and previous work [2]

	Current Study	**Previous work [2]**
MTD Type	Based On sources	Randomly
Required processing resources	Only Ovlerlay networks	Use Shadow and ovlerlay networks
MTD Strategies	Ovlerlay networks	VSH and ovlerlay networks
Ovlerlay networks	Optimal use of resources	Only Change the route
Databases Used	Use a shared database	At least 2

Conclusion

In spite of decades of research, DDOS attacks are extremely difficult to defend against [28][29]. These attacks are planned according to the attacker's creativity [30]. SDN and NFV provide a bed for handling attacks that disrupt services or service resources [31]. In this research, moving target defense techniques have been used to prevent DDOS in ISP networks using software network architecture and virtualization of network functions. This approach makes decisions based on resources and includes two dynamic defense strategies: the first strategy is route mutation, which is provided to obfuscate the network topology information during the DDOS detection stage and move the attacker away from the final target. The next presented strategy makes it possible to mutate the route of malicious packets away from their final destination, which is an important principle of moving target defense. Another strategy is to use covert networks for mutation so that by constantly migration the server, attackers cannot identify the real

server. In [2], no mention was made of how overlay networks are implemented in terms of resources. This study attempts to implement this defense method by examining the bandwidth and minimum resources necessary for defense, using virtualization of network functions. In this study, we attempted to create a detailed simulation of various aspects of attack and defense, which can serve as a basis for future research in the field of moving target defense.

Using the fault tolerance system in the controller introduced in [32] can be used to avoid the failure point in the control layer in future work. By adding fault tolerance, attackers cannot disable the control layer, and the desired defense services are fully accessible. Additionally, service function chaining [33] enables operators to design VNF functions on demand to meet the needs of their customers.

Declarations

Conflicts of interest: The authors declare that they have no conflict of interest.

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

Ethical Approval: Not applicable.

Authors' contributions : M.J.S. and A.D. wrote the main manuscript text. M.J.S. supervised the research. Both authors contribute to research design and implementation. Both authors reviewed the manuscript.

Funding: The authors did not receive support from any organization for the submitted work.

Availability of data and material: Data will be available by request.

References

1. Rawski M (2019) “Network Topology Mutation as Moving Target Defense for Corporate Networks,” *Int. J. Electron. Telecommun.*, vol. 65, no. 4, pp. 571–577, Oct.
2. Aydeger A, Saputro N, Akkaya K (May 2019) A moving target defense and network forensics framework for ISP networks using SDN and NFV. Futur Gener Comput Syst 94:496–509. 10.1016/J.FUTURE.2018.11.045
3. Abdulqadder IH, Zou D, Aziz IT, Yuan B, Dai W (2021) “Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment,” *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 2, pp. 866–877, Apr. doi: 10.1109/TETC.2018.2879714
4. Chowdhary A, Huang D, Alshamrani A, Liang H (2018) “MTD analysis and evaluation framework in software defined network (MASON),” *SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018*, vol. 2018-Janua, pp. 43–48, Mar. doi: 10.1145/3180465.3180473

5. Liu CC, Huang BS, Tseng CW, Yang YT, Chou LD (2019) SDN/NFV-based moving target DDOS defense mechanism. Adv Intell Syst Comput 843:548–556. 10.1007/978-3-319-99007-1_51/COVER
6. Singh AK, Jaiswal RK, Abdukodir K, Muthanna A (2020) "ARDefense: DDOS detection and prevention using NFV and SDN," *Int. Congr. Ultra Mod. Telecommun. Control Syst. Work.*, vol. 2020-Octob, pp. 236–241, Oct. doi: 10.1109/ICUMT51630.2020.9222443
7. Bringhenti D, Marchetto G, Sisto R, Valenza F, Yusupov J (2020) "Automated optimal firewall orchestration and configuration in virtualized networks," *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. 2020 Manag. Age Softwarization Artif. Intell. NOMS 2020*, Apr. doi: 10.1109/NOMS47738.2020.9110402
8. Alhebaishi N, Wang L, Jajodia S (2020) Modeling and mitigating security threats in network functions virtualization (NFV). Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 12122 LNCS:3–23. 10.1007/978-3-030-49669-2_1/FIGURES/8
9. Cho JH et al (Jan. 2020) Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Commun Surv Tutorials 22(1):709–745. 10.1109/COMST.2019.2963791
10. Bulbul NS, Fischer M (2020) SDN/NFV-based DDOS Mitigation via Pushback. IEEE Int Conf Commun vol 2020-June Jun. 10.1109/ICC40277.2020.9148717
11. Chen KY et al (2022) "SDNShield: NFV-Based Defense Framework Against DDOS Attacks on SDN Control Plane," *IEEE/ACM Trans. Netw.*, vol. 30, no. 1, pp. 1–17, doi: 10.1109/TNET.2021.3105187
12. Agrawal N, Tapaswi S (2021) "An SDN-Assisted Defense Mechanism for the Shrew DDOS Attack in a Cloud Computing Environment," *J. Netw. Syst. Manag.* vol. 29, no. 2, pp. 1–28, Jan. 2021, doi: 10.1007/S10922-020-09580-7
13. Rangisetti AK, Dwivedi R, Singh P (2021) "Denial of ARP spoofing in SDN and NFV enabled cloud-fog-edge platforms," *Clust. Comput.* vol. 24, no. 4, pp. 3147–3172, Jun. 2021, doi: 10.1007/S10586-021-03328-X
14. Torquato M, Vieira M (2021) "VM Migration Scheduling as Moving Target Defense against Memory DoS Attacks: An Empirical Study," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2021-Septe, doi: 10.1109/ISCC53001.2021.9631397
15. Valdovinos IA, Pérez-Díaz JA, Choo KKR, Botero JF (2021) "Emerging DDOS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 187, p. 103093, Aug. doi: 10.1016/J.JNCA.2021.103093
16. Abdulqadder IH, Zhou S, Aziz IT, Zou D, Deng X, Abrar Akber SM (2021) "An Effective Lightweight Intrusion Detection System with Blockchain to Mitigate Attacks in SDN/NFV Enabled Cloud," *6th Int. Conf. Converg. Technol. I2CT 2021*, Apr. 2021, doi: 10.1109/I2CT51068.2021.9417961
17. Dimolianis M, Pavlidis A, Maglaris V (2021) Signature-based traffic classification and mitigation for DDOS attacks using programmable network data planes. IEEE Access 9:113061–113076. 10.1109/ACCESS.2021.3104115
18. Torquato M, Maclel P, Vieira M (2021) "Analysis of VM migration scheduling as moving target defense against insider attacks," *Proc. ACM Symp. Appl. Comput.*, pp. 194–202, Mar. doi:

10.1145/3412841.3441899

19. Nguyen M, Debroy S (2022) “Moving Target Defense-Based Denial-of-Service Mitigation in Cloud Environments,” *Secur. Commun. Networks*, vol. 2022, doi: 10.1155/2022/2223050
20. Alavizadeh H, Aref S, Kim DS, Jang-Jaccard J (2022) Evaluating the Security and Economic Effects of Moving Target Defense Techniques on the Cloud. IEEE Trans Emerg Top Comput. 10.1109/TETC.2022.3155272
21. Shakil M, Fuad Yousif Mohammed A, Arul R, Bashir AK, Choi JK (Mar. 2022) A novel dynamic framework to detect DDOS in SDN using metaheuristic clustering. Trans Emerg Telecommun Technol 33(3):e3622. 10.1002/ETT.3622
22. Balarezo JF, Wang S, Chavez KG, Al-Hourani A, Kandeepan S (Jul. 2022) A survey on DoS/DDOS attacks mathematical modelling for traditional, SDN and virtual networks. Eng Sci Technol an Int J 31:101065. 10.1016/J.JESTCH.2021.09.011
23. Roshani M, Nobakht M (Aug. 2022) HybridDAD: Detecting DDOS Flooding Attack using Machine Learning with Programmable Switches. 1–11. 10.1145/3538969.3538991
24. Jiang S et al (2022) “BSD-Guard,” Secur. Commun. Networks, vol. 2022, doi: 10.1155/2022/1608689
25. Agarwal A, Singh R, Khari M (2022) “Detection of DDOS Attack Using IDS Mechanism: A Review,” Proc. 1st Int. Conf. Informatics, ICI 2022, pp. 36–46, 2022, doi: 10.1109/ICI53355.2022.9786899
26. Montazerolghaem A (2022) 7812 “Softwarization and virtualization of VoIP networks,” J. Supercomput. vol. 78, no. 12, pp. 14471–14503, Apr. 2022, doi: 10.1007/S11227-022-04448-W
27. Darekar SH, Shaikh MZ, Kondke HB (2022) Performance Evaluation of Various Open Flow SDN Controllers by Addressing Scalability Metric Based on Multifarious Topology Design on Software-defined Networks: A Comprehensive Survey. 327–338. 10.1007/978-981-16-7330-6_25
28. Rizvi ASM, Mirkovic J, Heidemann J, Hardaker W, Story R (2023) “Defending Root DNS Servers Against DDoS Using Layered Defenses,” 2023 15th Int. Conf. Commun. Syst. NETworkS, COMSNETS pp. 513–521, 2023, doi: 10.1109/COMSNETS56262.2023.10041415
29. “Akamai Blog | 2021 (2023) : Volumetric DDoS Attacks Rising Fast.” https://www.akamai.com/blog/security/2021-volumetric-ddos-attacks-rising-fast (accessed Apr 20,
30. “Azure DDoS Protection—2021 Q1 (2023) and Q2 DDoS attack trends | Azure Blog and Updates | Microsoft Azure.” https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q1-and-q2-ddos-attack-trends/ (accessed Apr 20,
31. Al Sadi A, Savi M, Berardi D, Melis A, Prandini M, Callegati F, “Real-time Pipeline Reconfiguration of P4 Programmable Switches to Efficiently Detect and Mitigate DDoS Attacks,” Proc. 26th Conf. Innov. Clouds, Networks I (2023) ICIN pp. 21–23, 2023, doi: 10.1109/ICIN56760.2023.10073501
32. Valizadeh P, Taghinezhad-Niar A "DDoS Attacks Detection in Multi-Controller Based Software Defined Network," 2022 8th International Conference on Web Research (ICWR), Tehran, Iran, Islamic Republic of, 2022, pp. 34–39, doi: 10.1109/ICWR54782.2022.9786246

33. Pattaranantakul M, Vorakulpipat C, Takahashi T (Feb. 2023) Service Function Chaining security survey: Addressing security challenges and threats. Comput Networks 221:109484. 10.1016/J.COMNET.2022.109484

Figures

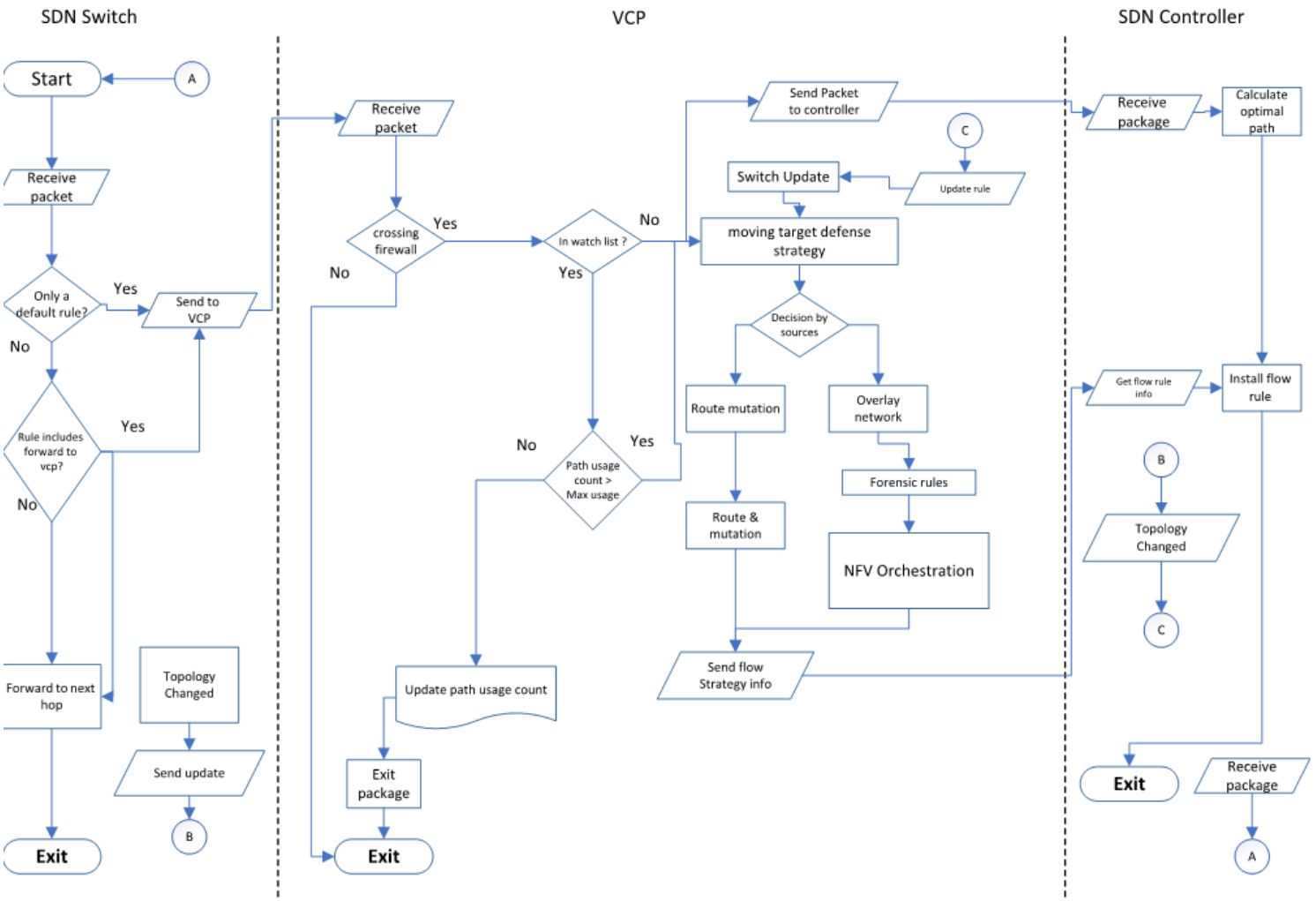

Figure 1

Flowchart for moving target defense management

```
1:  function select MTD StraTegy
2:  if this is not the first-time packet then
3:  getVSNbandwidth(vsn-vm bandwidth)
4:  if bandwidth ≥ max_bandwidth then
5:  selected StraTegy ←  (Overlay StraTegy )
6:  NFV managment()
7:  else
8:  selected StraTegy ←  DirectMutationStrategy
        a.  end if
        b.  Update Path DB
9:  end if
10: return  selected StraTegy
11: end function
```

Figure 2

Choosing moving target defense strategy

```
1:  function ReceivePacket(SwitchiD, srcIP, dstIP, protocol, maxUsage,
    triggeredUpdate)
2:  RoutingEntry ← GetFRoMPATHDB(srCIP, dstIP, protocol)
3:  isExpired ← false
4:  if RoutingEntry! = null then
5:  usageCounter ← GETENTRYINFO(RoutingEntry)
6:  if (usageCounter > maxUsage) OR (triggeredUpdate
7:  isExpired ← true
8:  end if
9:  usageCounter ← usageCounter+1
10: Update usageCounter of RoutingEntry in PathDB
11: endif
12: if (RoutingEntry == null)OR( isExpired == true) then
13: MTDStrategy ← SelectMTDStrategy( getEntryID(RoutingEntry))
14: route ← FINDRoutes(srclP, dstIP, protocol, MTDStrategy)
15: RoutingEntry ← currentTime, srciP, dstIP. protocol, route
16: Add RoutingEntry to PathDB
17: end if
18: end function
```

Figure 3

Packet Received on the defense system

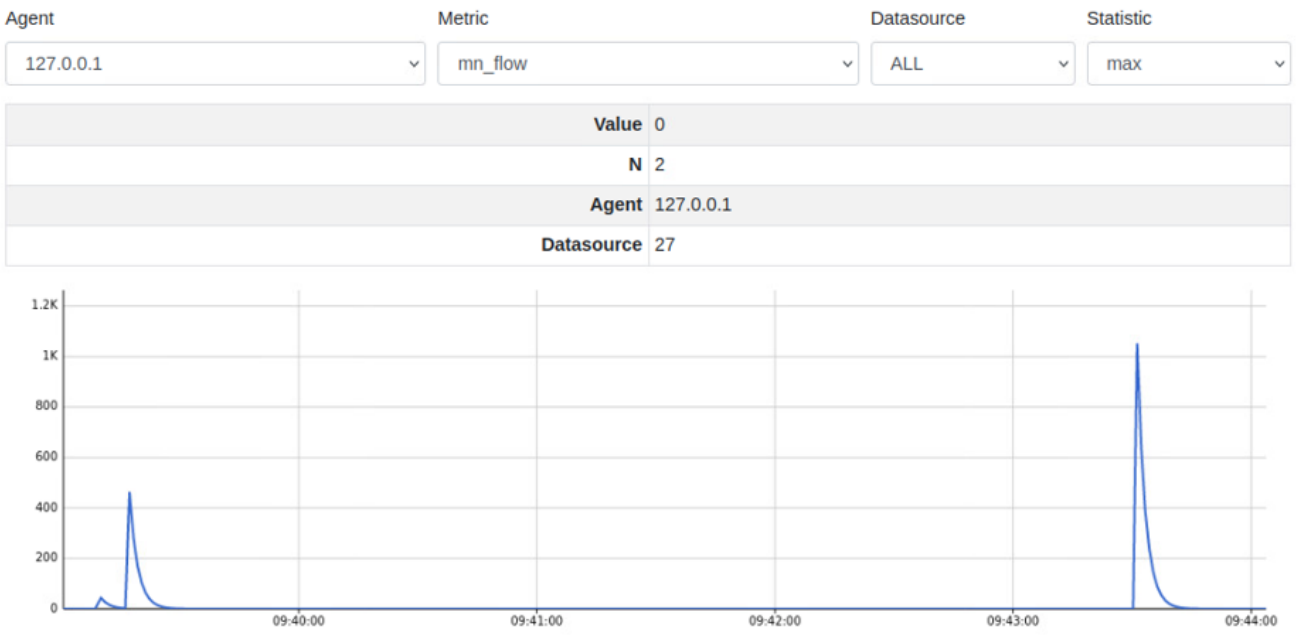

Figure 4

Web server view request

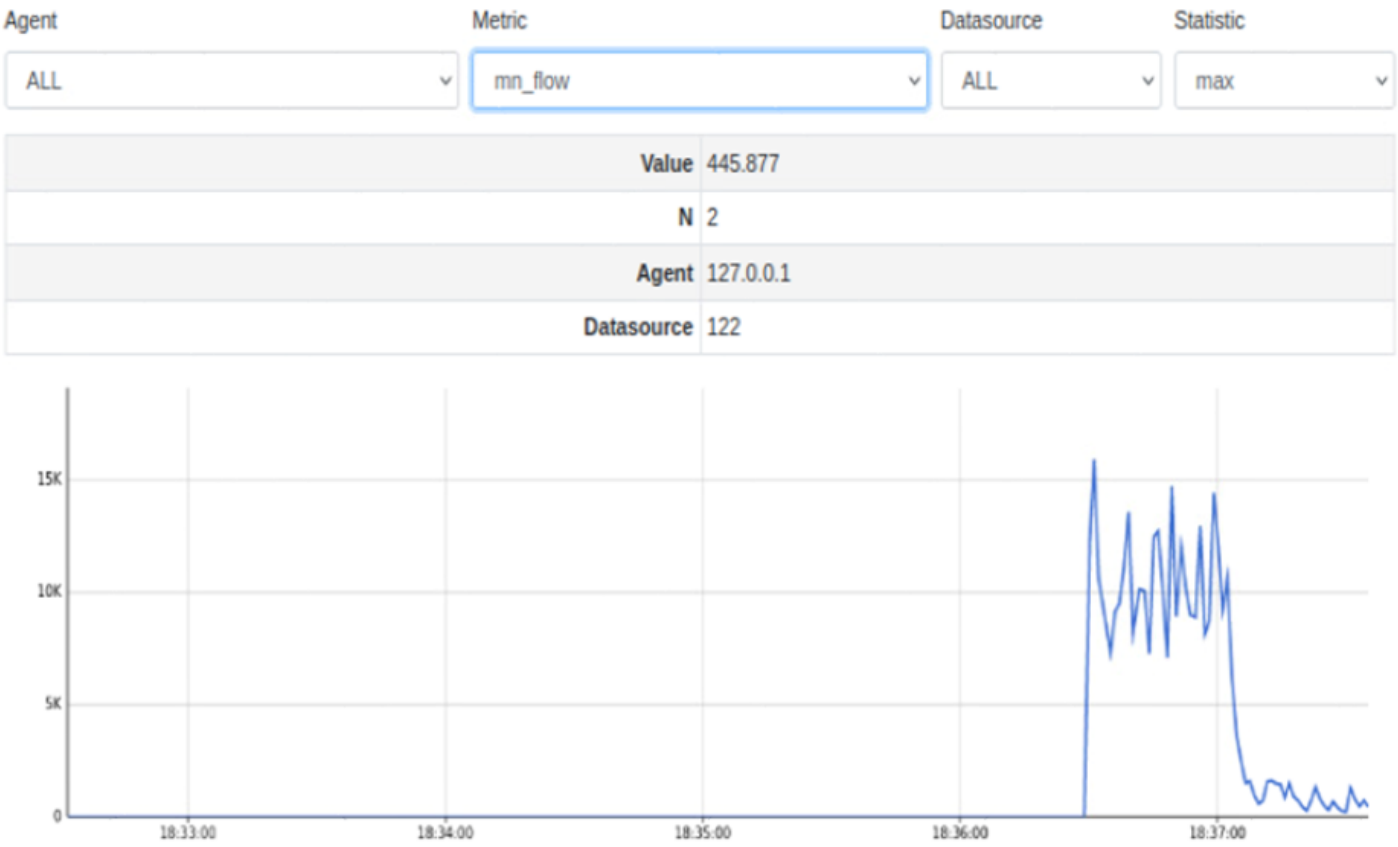

Figure 5

number of blocked packets by firewall