Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July, 2021 :13883 - 13893

Research Article

# Approaches to Mitigate the DDoS Attack on Dataplane SDN

Prof.Pushpa J[a], Dr.Suma S[b], Dr. ArunaDevi M[c]

[a] Research Scholar VTU- RC Dayananda Sagar College of Engineering, Department of CS & IT, Jain Deemed-to-be-university, Bangalore, India
[b] Department of MCA, Dayananda Sagar College of Engineering, Bangalore, India
[c] Department of MCA, Cambridge Institute of Technology, Bangalore, India
Email: [a]pushpaj.mca07@gmail.com, [b]suma-mcavtu@dayanandasagar.edu,
[c]hod.mca@cambridge.edu.in

## Abstract

Overwhelming the traffic towards the network node to make them inoperable which may down the services. This will not only affect the servers but also impact on input and output channels where the request may exceed the limit of data flow. Attackers usually enter into the network by compromising the authenticated nodes or service provider via many methods such as IP Spoofing, malware penetrating or by morphing the identity.

This DDoS attack not only defunction the nodes but also affect the entire centralized networking such as on SDN which centrally control the network nodes. SDN is a new network architecture which brings the new evolution in IT networking, but the biggest threats on the control plane and data plane are DDoS attacks.

Our paper focuses on DDoS attack's detection on Software Defined Network components and proposing the hybrid model of SDN and adopting Improved Principal Component Analysis.

Resultant value of an experiment proved as an efficient algorithm compared to k-mean, DBScan and Entropy.

***Keywords:*** *Entropy, LDS,OFDP, ARP, LLDP, Datapath ID, Identity access management*

## Introduction

*Introduction to SDN Security:*

Software Defined Network(SDN) is built with three main blocks such as Network managing application(Northbound Application Interface), Central monitoring and managing controller and forwarding devices. Northbound Interfaces are composed of applications for load balancing,host tracking, forwarding mechanism and other networking monitoring applications that should be more secure and abide by the security standards to avoid the

vulnerability. Security Standard principle is described in openflow foundation to take the measurement on vulnerability.

Our main focus is on SDN Controller and forwarding device attacks because it will majorly be from external attackers.SDN is programmatically managing the network node with centralized security model by deploying the upgraded application . OpenNetworking proposed the security principle in [1] to be applied on all the components of SDN , in which the major aspect is to update the security controls regularly as declared in principle 8 [1].

Logically centralized control SDN is easy to manage but perhaps leads to exploitation by the attackers. Attack model [1] , attacks are classified into internal and external attacks. In an internal attack, the user inside the system explores the vulnerability to exploit the components of SDN by obtaining the privileges and gaining the access to sabotage the behavior of the SDN. This internal attack can be prevented with well designed securing mechanisms such as I AM security policy.

Second type of attack is an external attack that can induce invalid traffic to create the threshold level in the system. Few of the external attacks are such as MIMA,DDOS attack and Communication link attack. Beside the above attacks many other external attacks can also distract the service of Networking services.

In this paper will discuss the different types of external attacks in SDN, later will narrow down to the DDOS attack which is a major threat in SDN which detracts from its service. In section II will discuss the different types of DDoS attack on control plan and its impact and section III will discuss the attacks on dataplane and also discuss the methodology to handle the DDoS attack.

## Attack on Control Plane

SDN control plane is logically centralized which maintains the global view of the network and induces security to data plane calling services from the application plane. Controller will build the switch MAC address table by discovering the link of switches using LLDP.

As depicted in the figure[1] below, a link between controller and data plane is established for communication using Openflow protocol. This channel should be secure to avoid any kind of eavesdropping in the system. At the same time Controllers should also follow the security standard to ensure the integrity, authentication and authorization of connected nodes. As described in Open Network foundation, the function of the controller includes Host Tracking system, Routing discovery, topology view and many other managing services in the network.

*A) Function of Control Plane*

- *Host Tracking Service: Host connects to the switches by generating the ARP packet. Switches sends the ARP packets of the host to the controller,by which it learns the IP-MAC binding, its port, dpid and classification of host's.*
- *Topology Management: Controller sends packet-out from LLDP packet to build the topology, switches sends back the LLDP packet-in message to controller. Upon receiving the packet-in from switches it builds the datapath and assigns datapath ID(dpid).*
- *Link discovery Services: Openflow discovery protocol contains the sender DPID of the sender which helps to classify the data packets of the message originating from[7].*

Falsifying those functionality by manipulating LLDP and ARP results in a major threat for the control plane. Many approaches were proposed and have integrated the security guard model into the control plane to mitigate those threats such as TopoGuard[3],AvantGuard[4],FloodGuard[5],Flood Defender[6], SYN Defender[6].

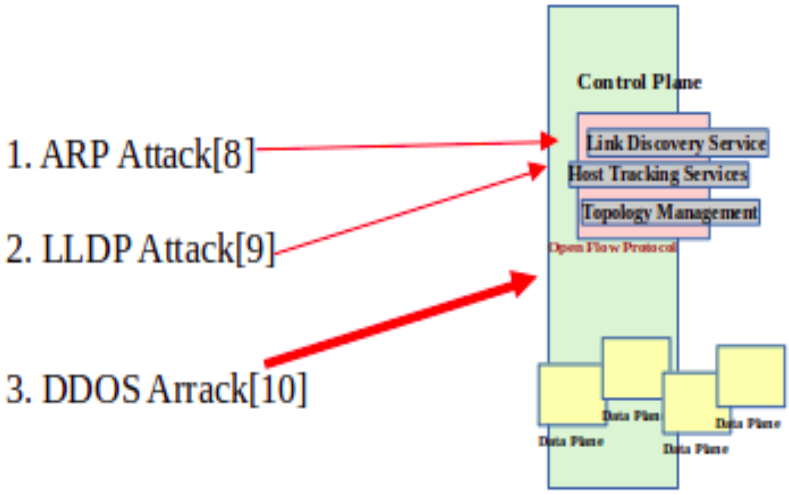



Figure [1]: Control Plane

- ☐ TopoGuard[3], keeps updating the Host tracker and Topology manager services to rule out the falsified LLDP packets. It uses a keyed-hash message authentication code as an optional TLV for LLDP packets to maintain the originality of LLDP packet.
- ☐ AvantGuard[4],a researcher has proposed an approach for the extension of security to the dataplane by two modules for migrating the fake TCP packet to proxy the TCP handshake and forward the legitimate TCP packet to the controller . Second module is actuating triggers which report the network status and payload information.
- ☐ FloodGuard[5],It contains two components to avoid flooding attack between data plane and controller.one is data plane cache which stores the table miss packet temporarily and apply packet analyzer for dropping the suspicious packet and apply the proactive flow rule analyzer.
- ☐ SYN Defender[6],TCP flood attack exploits the server by sending the syn packet repeatedly to all possible ports of the server. The server waits for the response after sending the SYN-ACK back to the attacker and opens the port for all the requests.

*B) Impact of attack on control plane*

Control plane is the core part in SDN which controls the entire network connectivity via services integrated in the controller. Many organizations have opted SDN with evolving NFV for betterment of managing and securing the network connectivity. As the controller is in high priority, it is more attractive and targeted by the attacker to sabotage the functionality of the control system which results in a single point of failure. In general, hosts will be the primary attackers or compromised by attackers to snoop the packets to fabricate the original header information. Attacks can be implemented by snooping, tampering and DoS using the tools such as scapy tools or macof to tamper dpid, egress port,IP spoofing.

As mentioned in the figure[1], ARP , LLDP and DDOS attacks are the most common attacks on controllers related to dataplane.

- ARP Attack: It is also called Host location hijacking, when a host send ARP Packets to the neighboring nodes it receives the reply which helps to build ARP tables. ARP table is used to map the MAC to IP address, if no map found then host will broadcast arp packet. Snooping the IP packet, ARP attacker will learn the MAC address and can compromise that host else can migrate its traffic. It can also capture the packet such as ICMP,TCP and UDP which helps to hijack the host location.
- LLDP Attack: Controller sends packet out message to gather the information of switches such as switch id, port number and update its routing table.

| Approaches | Handling ARP Attack | Handling LLDP Attack | Handling DoS/DDoS |
|---|---|---|---|
| TopoGuard[3] | ✔ | ✔ | ✔ |
| AvantGuard[4] | - | - | ✔ |
| FloodGuard[5] | ✔ | - | ✔ |
| Syn Defender[6] | - | - | ✔ |

**Table[1]: Approaches for control plan attack.**

With the above table[1], most of the approaches conclude that DoS/DDoS attack is more critical and needs sophisticated tools or modules to handle it. This Denial of Service is mainly caused from the data plane. Hence the root of attack should be handled efficiently.

## DoS/DDoS Attack on DataPlane

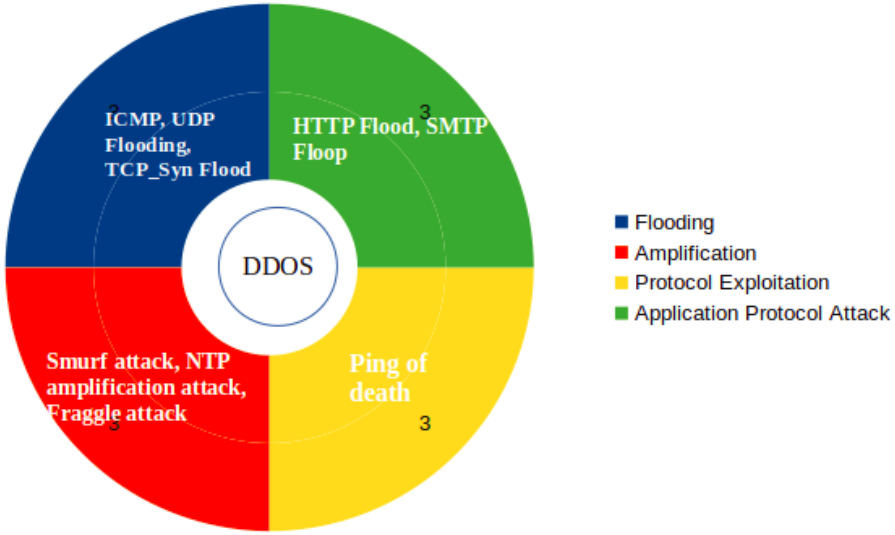
Network with high security services is an on demand requirement in emerging business and also expected to orchestrate with new technologies such as Artificial Intelligence, Machine Learning, Cloud,NFV.

Software Defined Networking(SDN) has been deployed in many organizations for providing managing network services. Though the SDN [9] is dynamic, secure, programable, orchestrated between the logical application to hardware devices it also suffers from single point of failure due to DDOS attack.

The main challenge in Security is the bottleneck situation between data plane and control plane when many new packets arrive at switches which result in table miss packet_in message is flooded towards controller. Control plane checks the packet information in its routing table if no match is found then it performs Link Discovery Service(LDS) to know about the node and its connectivity. Assume this type of queries is flooded by a southbound plane towards the control plane and will reach saturation level. Our survey towards threats on SDN Security is majorly due to the external attack on data plane components which is either by compromising the host/switches or snooping the routing table of switches, these kinds of attack is known as DDoS Attack. In this paper we discuss the different approaches to handle the DDoS Attack.

**a) DDoS Attack on DataPlane:** Rogue nodes are the prime elements in architecture to cause DDoS attack. Below figure[2], list the types of DDoS attacks which impact on increasing the latency in SDN as discussed in [10]. Primary focus of the attacker is saturation attack which can be achieved by flooding attack.

In *flooding attack* rogue nodes are flooding the request using protocol such as ICMP protocol with varying source(src), destination (dst)address, port Id and so on which result in threshold level in the control plane. This flooding attack is ranked first in a recent survey.
Attacking the networking server by snooping the IP address of src/dst to send queries to multiple servers such as DNS/NTP Server is another threat in networking which results in increasing down time in response such attacks are known as *amplification attacks.*
Snooping IP addresses also need intelligence and time consuming process for the attacker, some of the attackers will target network resources such as bandwidth by flooding http requests to the web server for huge amounts of data which consume the bandwidth and make the channel occupied for a long time could also bring the web server down.
We focus on threats that affect dataplane, especially flooding attacks such as ICMP flooding, TCP SYN_Flood, UDP Flooding and Flow Rule Flooding attacks which hamper the performance of SDN.




Figure[2]:Types of DDoS Attacks

**b) Mitigation of DDoS Attacks on Dataplane:**
Google, Cisco, Huawei, IBM and many technology based companies have integrated the SDN and embedded an proprietaty based model for handling the threats in SDN. Enabling Security for Software-Defined Networking with Zero Trust, Zero Touch from cisco[9] suggested to adopt the multilayer level of security with defense-in-depth approach and compliances.
Figure[3], shows the general paradigm to be implemented by the security models to prevent the DDoS attack.

Many such approaches are available/ proposed by researchers and Security Engineers in industries to mitigate the DDoS attack. As discussed above our objective is to study the approaches to handle the attack on dataplane.Two main components should be implemented to provide security to the dataplane. They are Detection model and a prevention model.
a) **Detection Model:** Identifying and classifying the malicious packet from the normal flow towards the dataplane is the major task of the detection method.

The below data flow diagram provides the notion for building the detection base model for implementation.

Primary input for the detection model is the network traffic which may contain network traffic from legitimate users and botnets. Identifying and classifying those traffic with minimal time with less error is the objective.

Below figure[3] gives an processing step of DDoS detection,

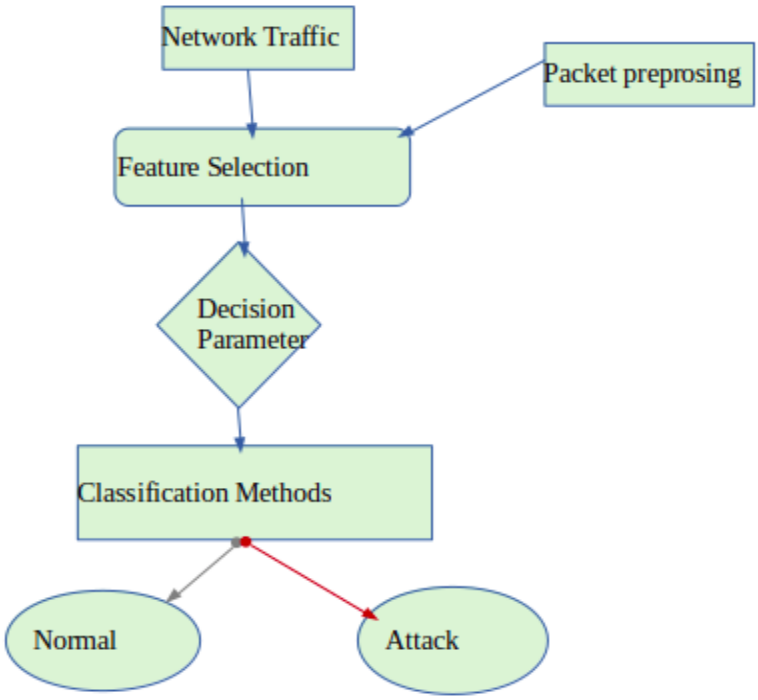


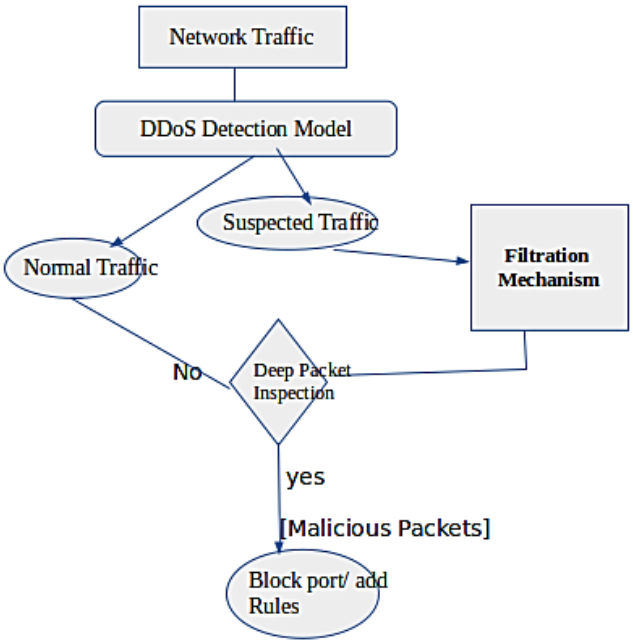

**Figure [3] : Detection Model**

b) **Prevention Model:** Redirecting or blocking the identified malicious packet and taking an appropriate action to countermeasure them is the task way to mitigate the attack. Certain measurement needs to follow to prevents the attack as specified by many experts such as,

-Content Delivery Network
-VXLAN
-TLS
-Authenticated Users
- Enabling Firewalls
- Adopting Detection methodology

Though the prevention methods are effective multi vector attack and botnet results Catastrophic impact on network, hence along with preventive measurement incorporating the mitigation model is necessary.

Below figure [4] provides the mechanism to lessen the attacks on the network, as shown below fraction of detected traffic May need training data or machine learning to identify the classified traffic and de-link the botnets.




**Figure[4]: Mitigation Model**

Many researchers have proposed the mechanism to detect the DDoS attack[13]-[18] by adopting the Entropy Techniques, PCA, artificial intelligence, mathematical model and novel based approaches.In the table[2], we try to consolidate the different approaches for specific types of attacks. Many of the approaches in the listed table are focusing on classifying packet traffic using entropy mechanism and also adopt the encryption methodologies for prevention.

| Methods/Models | ICMP Flooding Attacks | UDP Flooding Attacks | FLOW Rule Flooding Attacks | TCP_SYN Flooding attack |
|---|---|---|---|---|
| Detection Methods | Entropy[15],PCA[15] Ensemble learning[14],Support Vector Machine[19],OF-Guard,Kmean | Simple Entropy[15],PCA[15],Support Vector Machine[19],Flood Defender[22], Adaptive behavioral-based | Parallel flow installation[20], FloodGuard[5], Support Vector Machine (SVM), Naive Bayes (NB), Artificial Neural Network (ANN), and K-Nearest Neighbors (KNN) classification models | Entropy and Ensemble learning[14],Support Vector Machine[19],OF_Gaurd,Flood Defender[22],KNN, Probability-based Malicious Request Detection (PBMRD), Hidden Markov Model(HMM) |
| Prevention Methods | Detection Trigger[23],Multi-Layer Fair Queuing (MLFQ | Redirecting, Cache, proxy dataplane | Safeguard Architecture[24],Proactive Flow Rule, Adaptive suspicious prevention mechanism[26]. | VPN,SDN-Guard[25],Adopt Cloud-Based Service Providers. |

**Table[2]: Mitigation approaches.**

## IV. Conclusion

The paper is majorly focused on southbound interface attack which reduces the performance of SDN. With our survey, we conclude that DDOS attack is the major attack in dataplane in which flooding attacks are common attacks on switches. Mitigating those attacks is by detecting and classifying the traffic. Listed approaches give insight about the proposed approaches by researchers.

## References

[1] Diego Kreutz, Member, IEEE, Fernando M. V. Ramos, Member, IEEE, Paulo Verissimo, Fellow, IEEE, Christian Esteve Rothenberg, Member, IEEE, Siamak Azodolmolky, Senior Member, IEEE, and Steve Uhlig, Member, IEEE, "Software-Defined Networking: A Comprehensive Survey", arXiv:1406.0440, 2014.

[2] "A Survey on Security-Aware Measurement in SDN",Heng Zhang,1Zhiping Ca,Qiang Liu,Qingjun Xiao,Yangyang Li,and Chak Fone Cheang, Volume:2018 Article ID:2459154, Hindawi,2018.

[3] Hong, Sungmin et al.: Poisoning network visibility in software-defined networks: New attacks and countermeasures. In: NDSS. (2015

[4] S. Shin, V. Yegneswaran, P. Porras et al., "AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 413–424, Berlin, Germany, 2013.

[5] H. Wang, L. Xu, and G. Gu, "FloodGuard: a DoS attack prevention extension in software-defined networks," in *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 239–250, Rio de Janeiro, Brazil, 2015.

[6] WebSite: https://vlkan.com/blog/post/2013/08/06/sdn-discovery/
[7] Z. Hu, M. Wang, X. Yan, Y. Yin, and Z. Luo, "A comprehensive security architecture for SDN," in Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015, pp. 30–37, IEEE, Paris, France, February 2015.
[8] Dave Dukinfield, Cisco Customer Experience Product Manager; and Pam Richardson, Cisco Technical Writer, "Zero Trust, Zero Touch Enabling Security for Software-Defined Networking", Cisco, White Paper November, 2019.
[9] Neelam Dayal, Prasenjit Maity, Shashank Srivastava"Research Trends in Security and DDoS in SDN "SECURITY AND COMMUNICATION NETWORKSSecurity Comm. Networks 2016; 9:6386–6411Published online 9 February 2017 in Wiley Online Library (wileyonlinelibrary.com).
[10] Xiaotong Wu1,MengLiu, Wanchun Dou and Shui Yu, "DoS attacks on data plane of software-definednetwork: are they possible?", SECURITY AND COMMUNICATION NETWORKS, Published online 9 December 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1709.
[11] C. Li, H. J. Yang, F. Sun, J. M. Cioffi, L. Yang, Multiuser overhearing for cooperative two-way multiantenna relays. IEEE Trans. Vehi. Tech. 65(5), 3796–3802 (2016).
[12] W. Sun, Y. Li, S. Guan, An improved method of DDoS attack detection for controllers of SDN, in 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET) (2019), pp. 249–253.
[13] Shanshan Yu , Jicheng Zhang , Ju Liu 1 , Xiaoqing Zhang , Yafeng Li and Tianfeng Xu, "A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN", EURASIP Journal on Wireless Communication Networking,2021.
[14] Di Wu , Jie Li , Sajal K. Das Jinsong Wu , and Yusheng Ji, "A Novel DDoS Attacks Detection Scheme for SDN Environments",IEEE International Conference on Communications (ICC) DO - 10.1109/ICC.2018.8422448, 2018.
[15] M.P. Novaes, L.F. Carvalho, J. Lloret, M.L. Proença, Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. IEEE Access 8, 83765–83781 (2020)
[16] S. Haider, A. Akhunzada, I. Mustafa, T.B. Patel, A. Fernandez, K.R. Choo, J. Iqbal, A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access 8, 53972–53983 (2020)
[17] T.V. Phan, M. Park, Efficient distributed denial-of-service attack defense in SDN-based cloud. IEEE Access 7, 18701– 18714 (2019).
[18] YAO YU , (Member, IEEE), LEI GUO , (Member, IEEE), YE LIU, JIAN ZHENG, AND YUE ZONG, " An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks",SPECIAL SECTION ON SECURITY AND PRIVACY FOR VEHICULAR NETWORKS,IEEE ACCESS,2018.
[19] Imran, M., Durad, M.H., Khan, F.A.*et al.*Reducing the effects of DoS attacks in software defined networks using parallel flow installation.*Hum. Cent. Comput. Inf. Sci.***9,**16 (2019).
[20] Haopei Wang, Lei Xu and Guofei Gu (Texas A&M University),"OF-GUARD: A DoS Attack Prevention Extension in Software-Defined Networks",2014.

[21] Shang, Gao Zhe, Peng Bin, Xiao Hu, Aiqun,"FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks"DO - 10.1109/INFOCOM.2017.8057009,2017.

[22] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang and Y. Deng, "A New Framework for DDoS Attack Detection and Defense in SDN Environment," in IEEE Access, vol. 8, pp. 161908-161919, 2020, doi: 10.1109/ACCESS.2020.3021435.

[23] H. S. Abdulkarem and A. Dawod, "DDoS Attack Detection and Mitigation at SDN Data Plane Layer," 2020 2nd Global Power, Energy and Communication Conference (GPECOM), 2020, pp. 322-326, doi: 10.1109/GPECOM49333.2020.9247850.

[24] Dridi L, Zhani MF (2016) SDN-Guard: DoS attacks mitigation in SDN networks. In: 5th IEEE international conference on cloud networking (Cloudnet). IEEE, New York