JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Multi Dimensional Analysis on SDN Data Plane Attacks

Prof.Pushpa J[1] , Dr.Suma S [2]

[1]Research Scholar VTU- RC Dayananda Sagar College of Engineering, Bangalore, India.

[2] Department of MCA, Dayananda Sagar College of Engineering, Bangalore, India

Abstract : In this paper we would like to highlights the vulnerabilities in Data plane , Perform attacking on data plane components and Measure the impact on performance of system. The attacks on data plane creates the major impact on system performance and consumes more bandwidth of the system. It jeopardize the controller and result in defunction of SDN architecture. 3D analysis on data plane attack highlights the impact of flooding and arp spoofing attack and its affect in the performance of SDN.

IndexTerms - sFlow, LLDP,DPID, ID, Flow Rule.

1. Literature Survey

Threat detection and protection is major task in network which evolve many of the model in networking. Cisco[1], proposed Zero Trust, Zero Touch concept about enabling the security with its survey. It has highlighted the impact of attack which cause the data breaching and also survey the duration of those attack takes number of days which result the jeopardize in IT industries. Multi layer protection needed to mitigate the potential threats. An SOC is proposed by Cisco which composes the component of Anomaly detection, automation model and Machine Learning techniques to support security. DDoS is one of the major concern in network security as discussed in [2], impact on SDN due to DDoS is high and have proposed the mitigation algorithm by blocking the source whose rate of data transfer is greater than 10000 bit per second. sFlow is one of the effective tool for detection and mitigation DDoS attack which has helped many researcher to explore on those field as presented by[3]. An experiment is conducted on the network traffic collected from university give variety of input data collection on which entropy based mechanism is deployed with sFlow to mitigate the attacks detected by sFlow. In [3]-[9] detecting the attacks and finding the vulnerabilities are been considered, as the result many researcher have adopted the machine learning to detect the malicious traffic and the rogue nodes in the network. Most of the DDoS attack consider flooding attack which target the resources.

Attack on Northbound application can also impact the misconfiguration which should also consider about its authenticity. Towards building the secure network many Threat model is proposed, as we see in [16] Safe Guard proposed two modules to protect against DDoS detection such as Anomaly traffic detection and controller dynamic defense which detect the botnet in data plane and controller remapping to avoid the overloading effect on controller. Opennetworking recommended the principle of security is also important to follow which can subside the major impact at initial stages, as suggested [21] ,retrofitting the security model and avoiding vulnerable protocol or algorithm, carefully vet the overall architecture.

Deep vulnerability assessment is very essential before deploying SDN, as discussed from[10]-[16], many measurement are taken the prove the effectiveness of detection algorithm and also highlighted the time taken to detect the attack should less to block the further impact on network system. Also recommended to use the open source such as snort IDS to detect the attacks.

As stated in[21], Security measurement against the different attack should adopt efficient algorithms for network classification, feature selection and accuracy of identify the attack vector and verification with tested data are the few step should be considered.

2. Security of Data Plane in SDN:

SDN is an process of controlling the network operation in software. It conceptually divided into three layer Control Plane, Data Plane and Application Plane. Control Plane is an centralized unit which control, communicate and monitor other two Plane. Data Plane is a firmware implemented on router or switches for forwarding the network traffic to the connected devices. The Data plane components functionalities are discussed below,

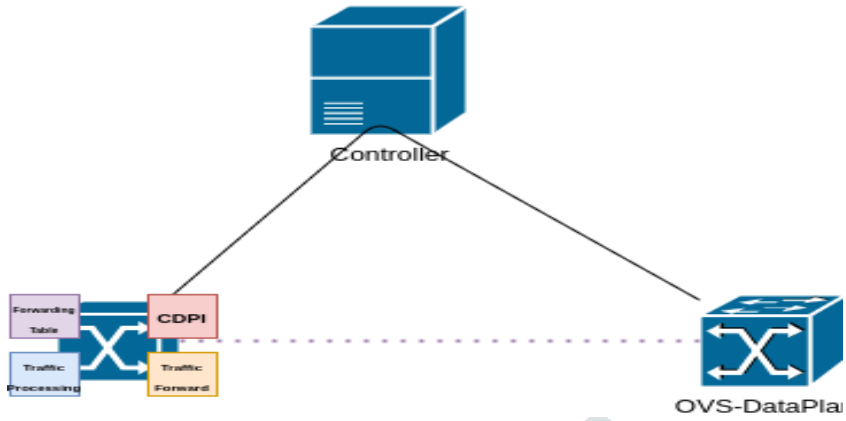


Figure [1]: OVS_Connectivity

2.1 Component of Data Plane

a. Flow Table: In SDN all forwarding decision are flow based than destination based, controller will be having the flow statistic and send the flow rule to switches which is updated in flow table of OVS. The major functions of flow table is to store the flow rules in tables and matches the with incoming traffic. Figure [2] shows the snap of flow table.

```
mininet> dpctl dump-flows --protocols=OpenFlow13
*** s1 ------------------------------------------------------------------------
 cookie=0x0, duration=3.659s, table=0, n_packets=0, n_bytes=0, idle_timeout=60, reset_count
s priority=65535,icmp,in_port="s1-eth2",vlan_tci=0x0000/0x1fff,dl_src=b2:fb:c3:8c:38:ce,dl_
dst=c6:59:cc:a7:47:28,nw_src=10.0.0.2,nw_dst=10.0.0.1,nw_tos=0,icmp_type=0,icmp_code=0 acti
ons=output:"s1-eth1"
```

Figure [2]: Flow Table of S1

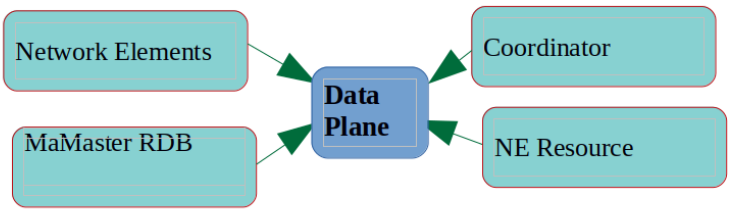
b. Controller Data plane Interface(CDPI): It is also known as south bound interface which consist of programming control of forwarding operations[21].

c. Packet Forwarding Engine: OpenFLow is a standard way of forwarding the packets or flow from controller to switches. This engine matches the packet header against the match field

d. Packet Processing: It is a process to extract the information needed to identify information for further processing by integrating hardware component with proprietary software , this can be achieved by using DPDK, Vector packet processing and other library functions.

2.2 Security in Data Plane, Currently Openflow protocol is used to communicate between data plane and control plane which use TLS for secure data transfer. Data plane can be implemented on hardware switches which are compatible for OVS Software. Open Flow Switches is a pro grammatically controls the switches which uses openflow protocols to communicate with controller of SDN.

Security of Data Plane encomposes of the mechanism used to implement the OVS as described below,



Figure[1]: Components of Data Plane

Network *Resources* are the resources components in data plane for traffic processing, It may br the composion of network bandwidth, throughput and relative elements.

Networking Elements are the virtualize switches which forward the packets and also process it using OAM(Operation Administration Management) Engine which also configure the routing information.

Master RDB It provide the conceptual information to the network elements about the resources.

Security Integrated in data planes are,

1. Single Management controller
2. Ability to inject the test
3. Local Fault recovery
4. Event notification & publication
5. Policy Enforcement.
6. Interconnect the Virtual Network Element to enforce the rules

The above mentioned properties makes the forwarding more robust and secure for data transmission , but still few challenges in data plane need to be addressed. TLS is not considered asdefault option which open the attacker to probe the data planes. It is difficult to attack from external element to data plane as it authenticate with identity certificate all the forwarding devices but it is not feasible in wireless communication either with TLS nor enforcing for certification due to high speed requirement with asymmetric communication.

2.3 Vulnerability in SDN Data Plane

If the data plane is compromised, as discussed in [21] than it generates the attack vector. This Attack vectors are classified into Passively eavesdrop on messages, DDoS attack and side channel attacks.
a. Passively eavesdrop: Phishing or social engineering attack can be handed by principles by encrypted techniques and tunneling mechanism.
b. Side Channel attacks: This can be combat by resolving policy conflict and using secure protocol for communication communication.
c. *DDoS Attack*: SDN imbibes security rules and more secure compare to than traditional network, but internally initiated attacks by comprised hosts is more difficult to detects. Those hosts will consumes privileged resources and disrupt the flow of traffics.
Open Network Foundation recommended the consideration of principles to adopt for security.

The basic **security principles** integrated in SDN architectures are Robust Identity, Recommend the proven protocols and methodologies such as TLS, MD5. Data plane is one of the major component in SDN, securing this also an important task. As recommended by Open Networking in [21], security the data plane should consists of following principles

I. Encourage Message Validation
II. Protect the switch storage
III. Aware about tunnel ID by the controller
IV. Secure channel between Switches and Controllers:
V. Resolve the policy conflicts.

Vulnerability in SDN Data Plane

If the data plane is compromised, as discussed in [21] than it generates the attack vector. This Attack vectors are classified into Passively eavesdrop on messages, DDoS attack and side channel attacks.
Passively eavesdrop: Phishing or social engineering attack can be handed by principles by encrypted techniques and tunneling mechanism.
Side Channel attacks: This can be combat by resolving policy conflict and using secure protocol for communication communication.
DDoS Attack: SDN imbibes security rules and more secure compare to than traditional network, but internally initiated attacks by comprised hosts is more difficult to detects. Those hosts will consumes privileged resources and disrupt the flow of traffics.

We are focusing on DDoS Attack, as this attack create threshold level for resources and services. It affect the market with huge disruption. DDoS attack will jeopardize the business by slow downing the services and lose of user data which impact around 40% which also cost high amount.

Identifying the vulnerabilities in the data plane is essential to focus on the area of research for further development by the researcher. We highlight the vulnerabilities in below tables [1] and the impact will be analyzed after implementing the attack model.
In table[1] vulnerabilities with respect to data plane is discussed and tabulated the collective inputs from different research[21]-[23] . OpenFlow protocol and channel of communication between the switches and controller is secure but the optional TLS services in many controller such as NOX, POX and FloodLight creates the space for attack.

Vulnerabilities in Network Element : No automatic bandwidth rate limiting to the high volume packets, man-in middle may generate the malicious flow and lack of authentication of third party switches results to attack.

Vulnerabilities in Connected nodes: Dynamic Nodes/Host addition or relocating is common in wifi network for mobilized devices which require fast authentication model and also lack of idea about the configuration setting are prone to DDoS attack such as botnet which may result in flooding attacks, topology poisoning and IP Spoofing.

Vulnerabilities in Flow Tables: Wild card matching of packets and limitation of memory leads to modify the table entry frequently with new request to controller generate queue of message in the channel.

Vulnerabilities in Communication Channel: Tunneling is the secured way of transfer the data which may also leads to time consuming in different subnet, for which many constumers will go for plain
text TCP connection leads to vulnerabilities in channel for spoofing mac address and network information for attacks.

Table[1]: Vulnerabilities

Component of Data Plane	Vulnerability 1	Vulnerability 2	Vulnerability 3	Vulnerability 4
Network Element	Rate Limiting	MAC Spoofing	Flow generation	Authentication
Connected Nodes	Authentication	Configuring Firewall	Unsecured Website	-
Flow Table	Flowrule Enforcement	Flase-Flow Rule from adversary nodes	-	-
Connectivity between NE	Optional TLS	Forwarding Loop	Limiting bandwidth	Shared Networking interface

2.4 Attacking Ideology

Intrusion Detection system are major component in networking system evolve with new approach to defend against fraudulent activities. Network attack activities are used to consume lot of networking resources and attack the networking system. Based on the studies of vulnerabilities We would create an attack vector to measure the performance of SDN. As discussed in our paper [20], DDoS attack can be broadly classified into 3 types Volume Based attack, Protocol attack and Application layer attack. Each attacks goal is to invade the network system, as represented in the figure[1], we listed the attack vector which impact of attacks on network resources are analyzed from the experiments on data plane.

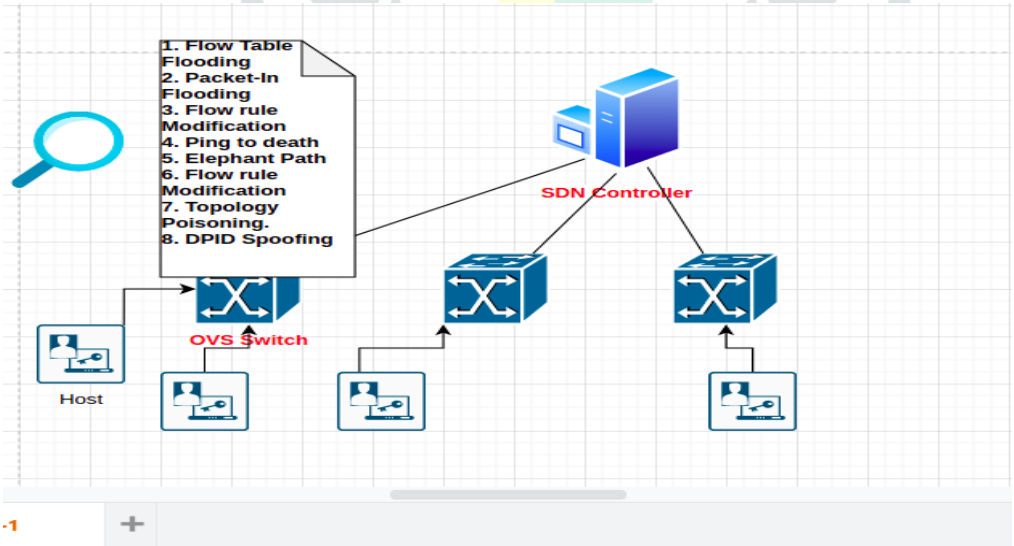


Figure [2]: Attack Vector

Ideology 1: Arp Spoofing, which entails spoofing the MAC addresses of hosts and performing a man-in-the-middle attack so that traffic passes via the attacker's system. This can be done with the arp spoof utility or the scpay package [requires a gateway and the victim's IP address].

Ideology 2: DDoS attack, which can build a botnet to affect multiple hosts at the same time and bring many services to a halt by flooding the targeted server with packets. We utilise hping3 to get through the firewall and flood UDP and SYN packets of various sizes.

Ideology 3: LLDP assassination Topology management services will collect host tracking information and switch information via LLDP packets. Host location hijacking and link fabrication attacks will jeopardize topology information. This strike has the potential to be devastating.

Ideology 4: *Side channel attack,* It is also know as information disclosure or Eavesdropping in which the configuration information of flow table statistics or capabilities of switches will be captured.

Ideology 5: *Host Location Hijacking,* In this attack network traffic for the original host will be diverted to attack host.

Ideology 6: *Flow table overflow,* Random packet generated by the botnet generate the new request to controller which also fills the capacity of TCAM of switches result to overflow or drop in packets. It also consume the throughput and impact on TCP performance[25]. Flow table overflow due to random flooding request perhaps create controller stroke which will be not listen to legitimate request during the flooding attack. As depicted in figure[2], any flooding attack such as ping to death attack will result in traffic congestion and connected switch will be not reachable.

Figure [3]: Flow table Overflow.

Ideology 7: *Flow Rule Modification,* side channel attack can also result into flow rule modification by the attacker and which misleads the routing stratergy.

Ideology 8: *DPID Spoofing,* Modifying the datapath id of switch disconnect the legitimate switch and establish connection with malicious switch. Controller receive the dpid while getting reply from switches in OFPT_FEATURE_REPLY.

Ideology 9: *Elephant flow,* It may be the legitimate traffic or malicious traffic classifying this include not only the byte count but also need to scan the authenticity of the port. This attack generate the packet with high payload.
We have conducted the attacks on all vectors to analyze the impact on data plane and take the primitive measure against it. We have consider the network resources for measuring the affects to network traffics.

3. Result Analysis:

We are using mininet to create the test bed for measuring the attacks impact on the performance of network. Tools using for the experiments are iperf, hping3, scapy scripts and configuring the bridge information to conduct the attacks and measure the performance. Weka tool for filtration process and classification process. sFlow tool is used to asses the performance of network, consumption of bandwidth and impact on memory is captured. Among Nine ideology each attack are directly or indirectly affecting the performance of SDN. With experiment the resource consumption such as cpu utilization, memory and bandwidth is consumed high in flooding attack and Elephant flow attack.

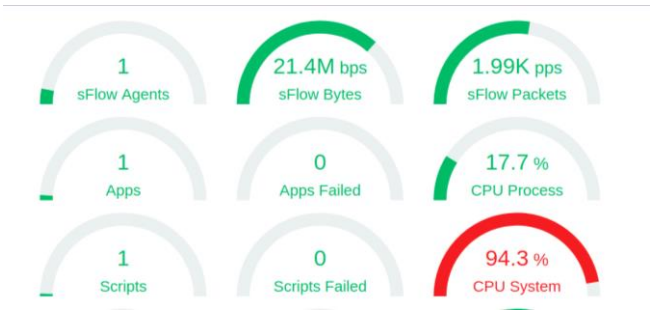


Figure (4a): Flooding attack

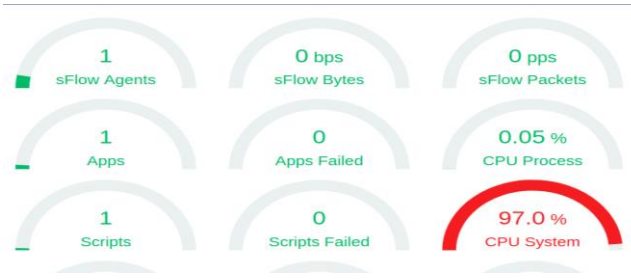


Figure (4b): Elephant Flow

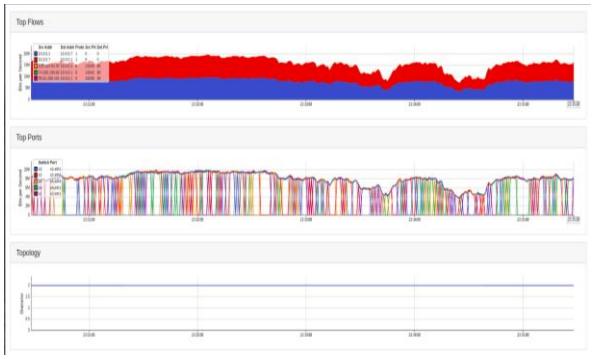


Figure (4c): Flow table over flow

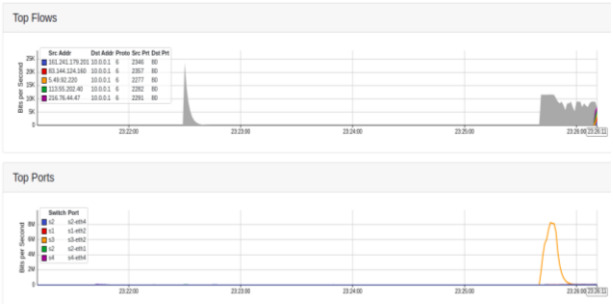


Figure (4d): arp spoofing attack

Conclusion: In this paper we have highlighted different possible attack on data plane and its impact on system performance. Hence this helps to prioritizing the attacks detection for maintaining the stable and efficient network connectivity.

Reference:

[1]. Cisco Zero Trust, Zero Touch Enabling Security for Software-Defined Networking November, 2019.
[2]. Krishnan, Saravanan; Oliver, John Joel E (2019).*[IEEE 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) - Tirunelveli, India (2019.4.23-2019.4.25)] 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) - Mitigating DDoS Attacks in Software Defined Networks. , (), 960–963*.doi:10.1109/ICOEI.2019.8862589.
[4]. Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., Maglaris, V., 2014. Combining openflow and sflow for an effective and scalable anomaly detection and mitigation mechanism on sdn environments. Comput. Netw. 62, 122–136. URL: http://dx.doi.org/ 10.1016/j.bjp.2013.10.014, doi:10.1016/j.bjp.2013.10.014.
[5]. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN Raja Majid Ali Ujjana , Zeeshan Perveza , Keshav Dahala , Ali Kashif Bashirb , Rao Mumtazc and J. Gonzálezc aSchool of Computing, Engineering and Physical Sciences, University of the West of Scotland, Paisley, PA1 2BE, UK bDepartment of Computing, Mathematics, and Digital Technology, Manchester Metropolitan University, Manchester M1 5GE, UK cGS LDA, Aveiro, Portugal
[6]. A. Ahalawat, S. S. Dash, A. Panda and K. S. Babu, "Entropy Based DDoS Detection and Mitigation in OpenFlow Enabled SDN," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019, pp. 1-5, doi: 10.1109/ViTECoN.2019.8899721.
[7]. Hassan Mahmood, Danish Mahmood, Qaisar Shaheen ,Rizwan Akhtar, and Wang Changda, S-DPS: An SDN-Based DDoS Protection System for Smart Grids, Article ID 6629098, Security, Trust and Privacy for Cloud, Fog and Internet of Things, Volume 2021.
[8]. K. Kalkan, G. Gür, F. Alagöz, Sdnscore: A statistical defense mechanism
against DDoS attacks in sdn environment, in: 2017 IEEE Symposium on
Computers and Communications, ISCC, IEEE, 2017, pp. 669–675.
[9]. Singh, Jagdeep; Behal, Sunny (2020).*Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review, 37(), 100279*–.doi:10.1016/j.cosrev.2020.100279
[10]. S.-C. Tsai, I.-H. Liu, C.-T. Lu, C.-H. Chang, J.-S. Li, Defending cloud computing environment against the challenge of DDoS attacks based on software defined network, in: Advances in Intelligent Information Hiding and Multimedia Signal Processing, Springer, 2017, pp. 285–292. [11] K. Kalkan, L. Altay, G. Gür, F. Alagöz, JESS: Joint entropy-based DDoS defense scheme in SDN, IEEE J. Sel. Areas Commun. 36 (10) (2018) 2358–2372.
[12].] R. Sahay, G. Blanc, Z. Zhang, H. Debar, ArOMA: An SDN based autonomic DDoS mitigation framework, Comput. Secur. 70 (2017) 482–499.
[13] S. Hameed, H. Ahmed Khan, SDN based collaborative scheme for mitigation of DDoS attacks, Future Internet 10 (3) (2018)
[14] M. Conti, C. Lal, R. Mohammadi, U. Rawat, Lightweight solutions to counter DDoS attacks in software defined networking, Wirel. Netw. 25 (5) (2019) 2751–2768.
[15] K.K. Karmakar, V. Varadharajan, U. Tupakula, Mitigating attacks in software defined networks, Cluster Comput. 22 (4) (2019) 1143–1157.
[16] Y. Wang, T. Hu, G. Tang, J. Xie, J. Lu, SGS: Safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking, IEEE Access 7 (2019) 34699–34710.
[17] A.S. Da Silva, C.C. Machado, R.V. Bisol, L.Z. Granville, A. SchaefferFilho, Identification and selection of flow features for accurate traffic classification in SDN, in: 2015 IEEE 14th International Symposium on Network Computing and Applications, IEEE, 2015, pp. 134–141.
[18]. Khundrakpam Johnson Singh and Tanmay De, “Efficient Classification of DDoS Attacks Using an Ensemble Feature Selection Algorithm”, Journal of Intelligent Systems, 2017.
[19]. https://www.unb.ca/cic/datasets/nsl.html
[20]. “Approaches to Mitigate the DDoS Attack on Dataplane SDN”, Turkish Online Journal of Qualitative Inquiry (TOJQI)Volume 12, Issue 7, July, 2021 :13883-13893.
[21]. Open Networking Foundation, Principles and Practices for Securing Software-Defined Networks January 2015.

[22]. AayushPradhan, RejoMathew, "Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)", Elessevier, Volume 171, 2020, Pages 2581-2589.
[23]. Benton, Kevin & Camp, L. & Small, Chris. (2013). OpenFlow vulnerability assessment. HotSDN 2013 - Proceedings of the 2013 ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. 151-152. 10.1145/2491185.2491222.
[24]. https://sdnpwn.net/2017/08/22/what-is-sdnpwn/
[25]. Guo, Z., Liu, R., Xu, Y., Gushchin, A., Walid, A., & Chao, H. J. (2017). *STAR: Preventing flow-table overflow in software-defined networks. Computer Networks, 125, 15–25.*doi:10.1016/j.comnet.2017.04.0