Distributed Denial of Service Attack Alleviated and Detected by Using Mininet and Software Defined Network

Abdulrahman Khalid Abdullah Al-Mashadani
Engineer, Department of Electrical and Electronics, Altinbas University, Istanbul, Turkey.
E-mail: abdulrahman.almshhadani@ogr.altinbas.edu.tr

Muhammad Ilyas
Assistant Professor, Department of Electrical and Electronics, Altinbas University, Istanbul, Turkey.
E-mail: Muhammad.ilyas@altinbas.edu.tr

Received September 23, 2021; Accepted December 18, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19272

Abstract

The network security and how to keep it safe from malicious attacks now days is attract huge interest of the developers and cyber security experts (SDN) Software- Defined Network is simple framework for network that allow programmability and monitoring that enable the operators to manage the entire network in a consistent and comprehensive manner also used to detect and alleviate the DDoS attacks the SDN now is the trending of network security evolution there many threats that faces the networks one of them is the distributed Denial of Service (DDoS) because of the architecture weakness in traditional network SDN use new architecture and the point of power in it is the separation of control and data plane the DDoS attack prevent the users from access into resource of the network or make huge delays in the network this paper shows the impact of DDoS attacks on SDN, and how to use SDN applications written in Python and by using OpenFlow protocol to automatically detect and resist attacks with average time to response to the attack between 95-145 second.

Keywords

DDos, Mininet, Opendaylight, OpenFlow, SDN.

Introduction

DDoS attacks use traffic from multiple attackers to flood the victim making online services unavailable (Aamir & Ali Zaidi, 2021). Example of SDN features is it can separate of the user plane and (CP) control plane (Martinez, Ferro, & Ruiz, 2015), as shown in Figure 1. The data packet and data plane implement these decisions and actually forward the data packet (Hu, Hao, & Bao, 2014). In addition, the best network operation can be achieved through centralization make decisions from a single central point and fully understand the overall network conditions. The application layer is at the top of the control plane and provides services through REST APIs (Ali et al., 2020). The control plane deal with the data plane offset defined by the standard SDN referred to as OpenFlow (Dargahi, Caponi, Ambrosin, Bianchi, & Conti, 2017). Therefore, OpenFlow is the communication protocol between the SDN controller and the physical switch (Siamak Azodolmolky, 2013). The (OVS) OpenVSwitch is open source switching software utilize OpenFlow application (Kumar, Kumar, Singh, & Nehra, 2012). It is also compatible with cloud platforms such as OpenStack and Mininet as virtual network simulation software. The paper proposes a possible SDN-based general solution to defend against DDoS attacks without excessively increasing network load. The current proposal points to detect and alleviate DDoS attacks when online servers are under attack In short period, the suggested solution has the following characteristics:- first It compares at runtime the expected way of normal traffic against the path of monitored traffic. Second If a major variation on the traffic direction is detected, then an event will created. Third As an event associated with a DDoS attack is produced, then an SDN application programmed used to start capturing and analyzing the traffic to creates flow rules for blocking the malign traffic with OpenDayLight controller.

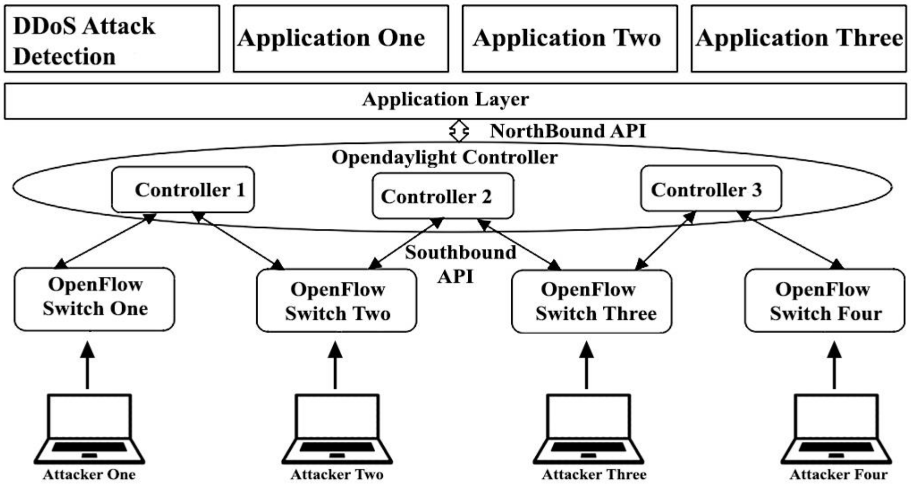


Fig. 1 DDoS attack on SDN environment

There are many types of ddos attack can classified into two categories the attack on resource and on bandwidth (Singh & Bhandari, 2020) as shown in figure 2. ref and the statics shows increase of ddos attack by using SYN flood (Alzahrani & Hong, 2018) in our present time show attack on industry by DDoS ("Kaspersky Q3 2021 DDoS attack report | Securelist," n.d.) in fig 3

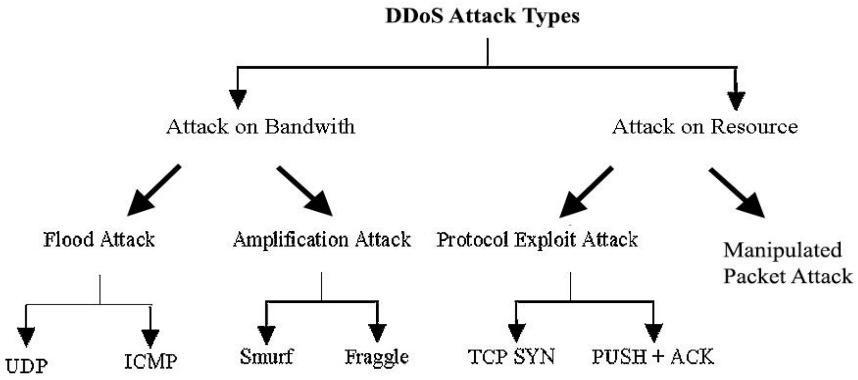


Fig. 2 DDos attack types

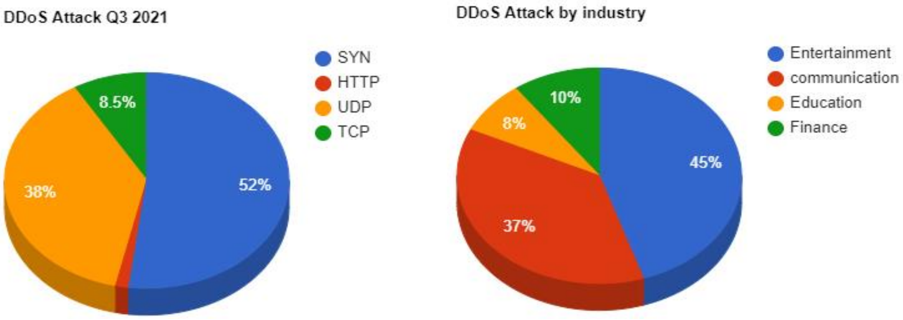


Fig. 3 DDoS attack in different type

Literature Review

In this paper (Sangodoyin et al., 2018), show how the dos attack impact on the network with SDN by using mininet and it is emulator the (ODL) open light controller .the network (UDP,TCP) servers that linked to openflow switches and flood attacking executed on it (ICMP) internet control message protocol to show how it will effect on this network the results show that a drop occurred on the throughput of network from higher measure above 200 Mbps to lower measure down of 90 Mbps also huge jitter happened between 0.008 ms to 0.678 ms in the time of dos attack but in this scenario there is no mitigation. In paper (Dridi & Zhani, 2016), other case like SDN-GUARD is very recommended option it has all the features and suitable method to reduce the impact of dos attacks like automatic updating for rule flow also redirect any malicious traffic that may effect on the network dynamically and modify the flow timeouts. The only disadvantage of this option it takes about few minutes to reduce the effect of attack. But these solutions are just for Dos attacks not for the DDoS attacks.in(Oo, Kamolphiwong, & Kamolphiwong, 2017) this case (AVSM) is suggested to for reveal DDoS attacks it stand for Advanced Support Vector Machine.in this scenario show how to employ SDN for discover and detect DDoS harmful attacks two feature is the most important for detection one is measure the flow volume and the other one to see asymmetry of flow rate with these feature you can monitor and if there is any suspicious flow traffic it will reveal quickly the possible victims and attackers. Those previous papers show how to detect DDoS with (POX) is a Python-based network software platform. And Open Network Operating System (ONOS).in(Salman, Elhajj, Kayssi, & Chehab, 2016) this paper show how firewall will prevent the packet that forwarded from server and stop them first capture traffic then analyze it and detect DDoS attack then rerouting it to firewall for blocking it use a firewall third-party to block the attack with using of POX controller this paper has traditional solution as normal network that forward traffic to firewall centralized.in (Sanjeetha, Prasanna, Kumar, & Kanavalli, 2018) this paper we have topology of one primary server and one switch connected to it the DDoS attack will applied on the switch by send large amount of packet on specific ip addresses and the flow table rule will update constantly by POX controller to the switch this attack leads the flow table space to be full and overwrought. this scenario is unreliable because the entries inserted from the controller labeled as malicious traffic and flow the switches asked for labeled as real traffic by changing timeout values with no need of SDN application.in (Sirijaroensombat, Nangsue, & Aswakul, 2019) this paper the topology of network contain virtual hosts and GNS3 and virtual machine it point to use modified SDN to detect and block the attack of DDoS traffic it also show information about throughput of UDP and TCP it has normal mesh topology and the disadvantage in this paper the ip address of the attacker is known and the code run manually so no time available to counter the attack but our goal is to use script written in python to dynamically and automatic response for any traffic DDoS attack also using openflow protocol in mininet it gives us a flexibility to custom routes with SDN . This figure 4 shows details of sdn for cyber security solutions and fig 5 shows where attacks aim in sdn layers and type of it.

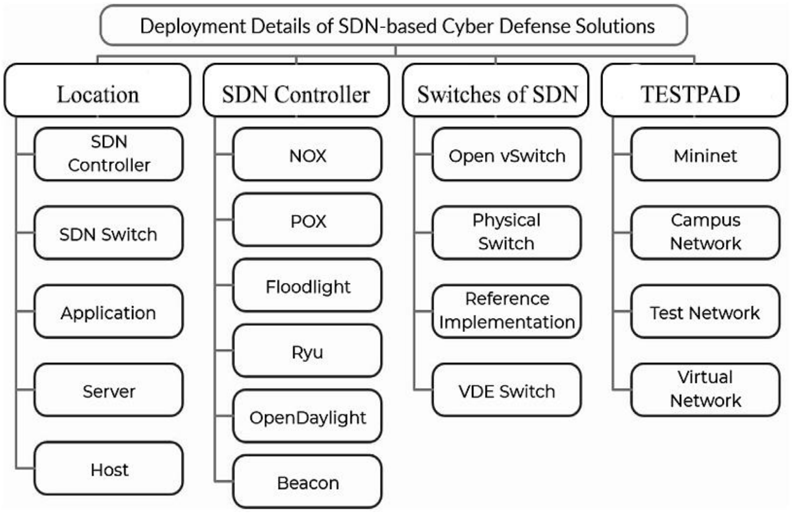


Fig. 4 SDN Details

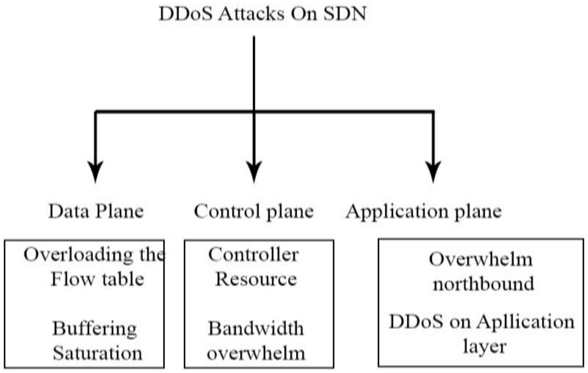


Fig. 5 Aim of DDoS Attack on SDN

The DDoS attack on SDN Layers the openflow switches (OVS) in data plane have contain limited size flow tables so the aim of attack is to overwhelm it also aims the control plane because it manage the whole network and aim to drop the network by attack on northbound in application layer (S. Kaur, Kumar, Aggarwal, & Singh, 2021)

Open flow protocol

An OpenFlow is a protocol used in communication especially in SDN (Lara, Kolasani, & Ramamurthy, 2014). With the ability to govern and forward SDN layers OpenFlow is usual used in southbound interference (Isolani, Wickboldt, Both, Rochol, & Granville, 2015). OpenFlow allows access and edit on network components such as routers and switches (Isyaku, Mohd Zahid, Bte Kamat, Abu Bakar, & Ghaleb, 2020). The OF protocol send information to the controller and it will perform tasks on switches like drop, forward. And other actions the OF switch consist of many flow table Inside the flow table there is many flow entries it can perform packet checking and rerouting it (Gopakumar, Unni, & Dhipin, 2015). Stanford University first suggested OpenFlow, which is currently standardized by the (ONF) Open Networking Foundation. It has versions it get updated to make the protocol more useful.it can used in network security for MITM man in the middle attack and against malicious traffic of DDoS attack (Benton, Camp, & Small, 2013) showed in figure 6 in table 1 show compression between SDN and Traditional Network.

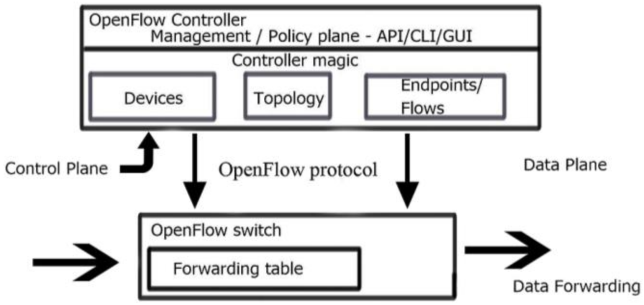


Fig. 6 The Protocol of OpenFlow

Table 1 Different between sdn and normal network

No	Standard	SDN	Traditional network
1	Cost of maintenance	Low cost	High cost
2	Time of error handling	Short time	May take months
3	Network management	Easy with aid of controller	Hard, because change must done for each device
4	Controller employ	important	Not relevant
5	Resource utilization	High	Less
6	Packet traffic	Can block or prioritize specific packets	Leads all packet to one way
7	Programmable	Yes	No
8	Interface	Open interface	Closed
9	Response to attacks	Faster and easier	Difficult
10	Forwarding and control	Separation	Coupling

Implementation and Compression

In this section will describe the architecture of the network and how SDN works with the network.

The tools used for make the environment start with Scapy is powerful new tool written in python language used to interpret packet it has many features that helps to test and exploit modules it can send invalid packets and can replace many tool as Nmap, hping (Moharir, Adyathimar, Shobha, & Soni, 2020) linux system Ubuntu developer used to make lab about cyber and network security (Lougheed, 2021) is mininet is network emulator used for make the suitable network environment (Hasan & Hisham Dahshan, 2020) wireshark is robust tool for analyze and capture traffic from network all these tools used to make our environment with other protocols(Sasi, 2020) in table 2 show the tools used in simulation.

Table 2 Tools and describe

Tools	Describe and use for
Scapy	Traffic generator
Ubuntu & Kali Linux	(OS) Operating system
Mininet	Network simulation
Openflow	Protocol
Opendaylight	Controller of Sdn
Wireshark	Analyze traffic
Openvswtich	Sdn switch

Part A

The system consist of three sections each one have basic components the first one named A it contain the (ODL) controller. And the second section named B contains the hosts and server with mininet. Where the third section contain the SDN programmed by python for block DDoS attack.in the system virtual machine used with Ubuntu operating system on network A and mininet emulator image installed on B network to create virtual switchs, hosts, links. A network with ip address192.168.153.131 the main goal of this section is to drop DDoS attack traffic when detected and Send the API out of northbound.in section B Mininet image installed to create switches that support OpenFlow protocol for rerouting flexibility ip address of Mininet is 192.168.153.133. The network topologies have 24 hosts with ip address start 10.0.1.0/24 end 10.0.4.0/24 every network connected to switch. The attack will lunch from hosts used DDoS inside the network .fig 7 describe overview of system element fig8 system concept model.

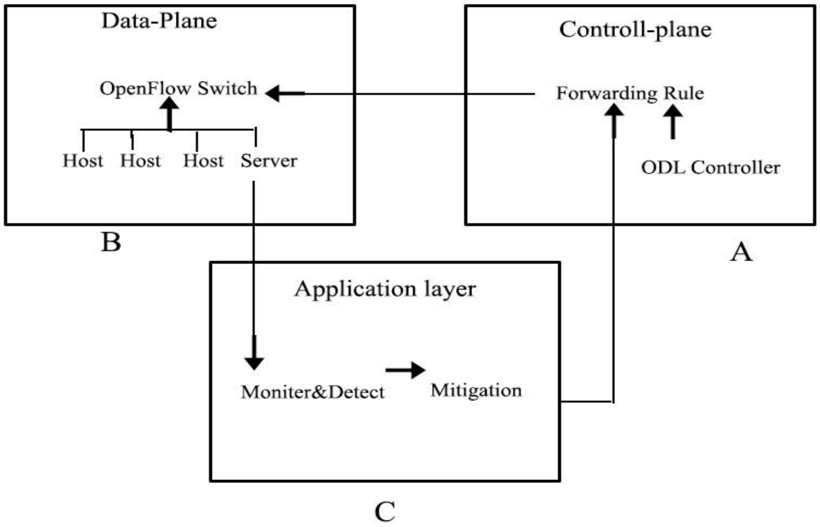


Fig. 7 Component of system

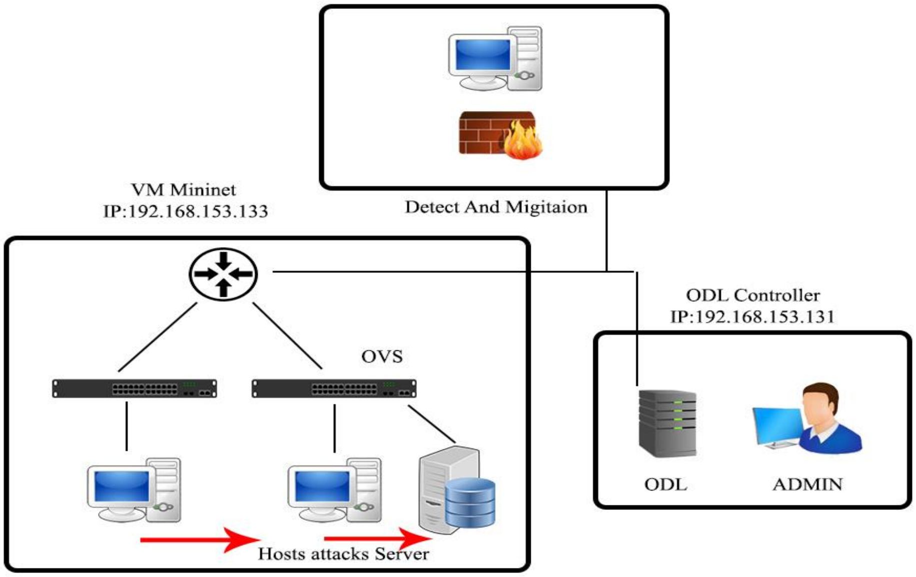


Fig. 8 System concept model

Part B

Build up the network using mininet with hosts and OV Switches and ODL using python code to generate the network as shown fig 9.

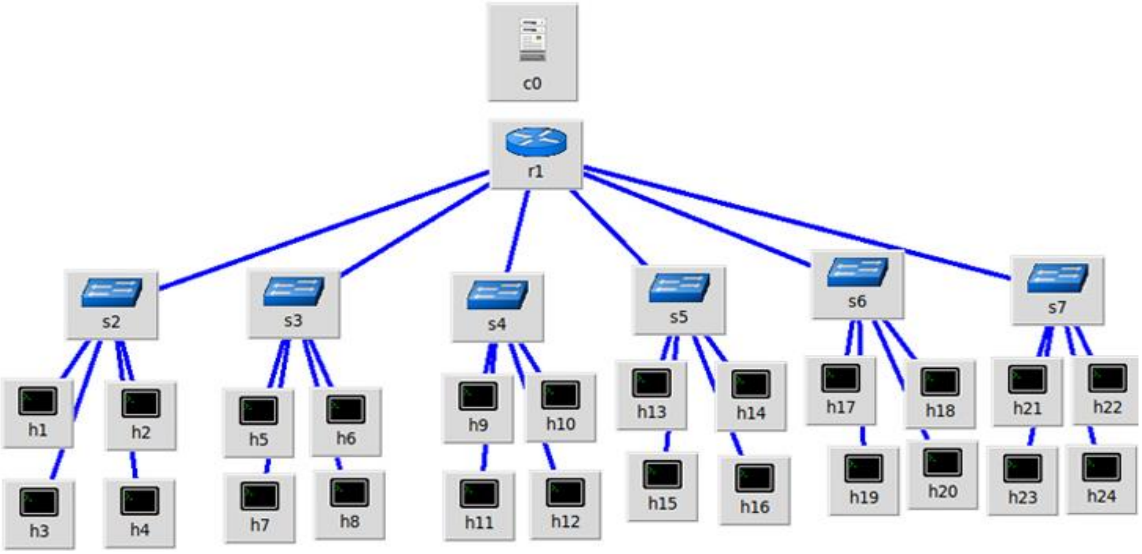
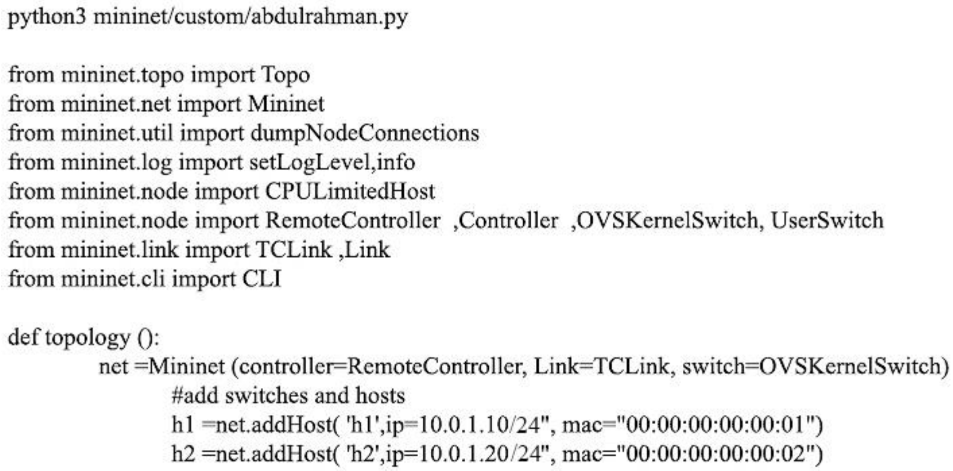


Fig. 9 Network by Python Code



```
python3 mininet/custom/abdulrahman.py

from mininet.topo import Topo
from mininet.net import Mininet
from mininet.util import dumpNodeConnections
from mininet.log import setLogLevel,info
from mininet.node import CPULimitedHost
from mininet.node import RemoteController  ,Controller  ,OVSKernelSwitch, UserSwitch
from mininet.link import TCLink ,Link
from mininet.cli import CLI

def topology ():
         net =Mininet (controller=RemoteController, Link=TCLink, switch=OVSKernelSwitch)
                 #add switches and hosts
                 h1 =net.addHost( 'h1',ip=10.0.1.10/24", mac="00:00:00:00:00:01")
                 h2 =net.addHost( 'h2',ip=10.0.1.20/24", mac="00:00:00:00:00:02")
```

Fig. 10 Python Code for Custom Topology

Part C

Attack scenario the DDoS attack will start from unknown random selected hosts inside the network and one of the hosts will used to ping with server to see if it reachable or not also see the network statues before the attack and after also show the performance to compare between the results in fig 11 there is no attack the used tool is Scapy use for manipulation packet and has a lot of feature like trace routing, botnet attacks and network scan it also provide GUI with wireshark this tool is written in python example of command line attack in Scapy is: send (IP (src="10.0.2.20", dst="10.0.2.10") /ICMP()/" ABDULRAHMAN"), COUNT=())

ICMP flood attack will make the or bandwidth attack will overwhelm the network with high harmful traffic this fig 11 show the traffic without attack.

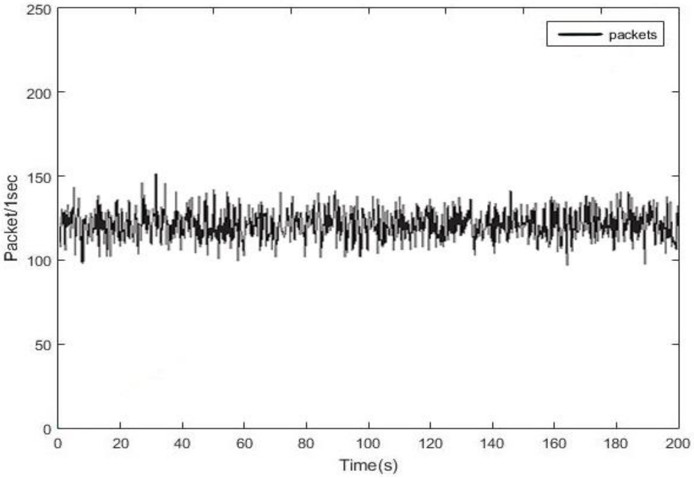


Fig. 11 Network with no attack

In the normal network firewall used to drop malicious traffic but in own network SDN used with open source virtual switches (OVS) programmed to detect and drop the attack by checking the traffic of the network if there is unusually high traffic goes toward server will located by ip address and make a new rule forwarded from (ODL) into the (OVS) to drop the packet fig 12 show after detect and Alleviate the attack by enter the administer mode of (OVS) it will show the state of the switches with many features like show table entries and configurations.

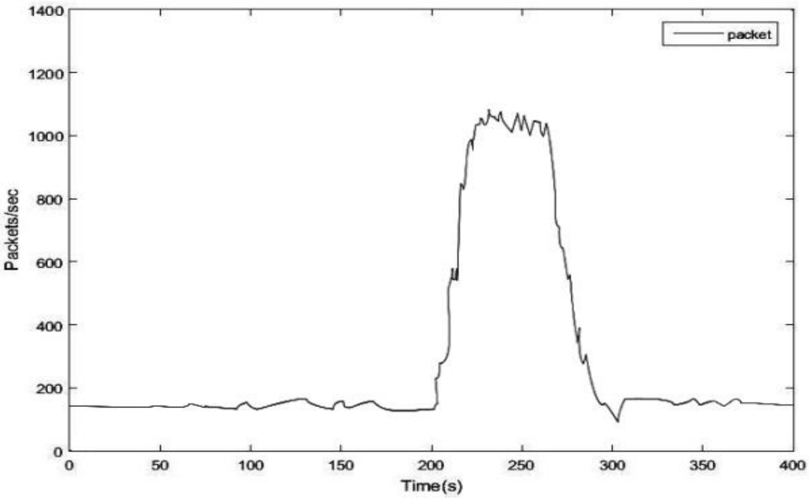
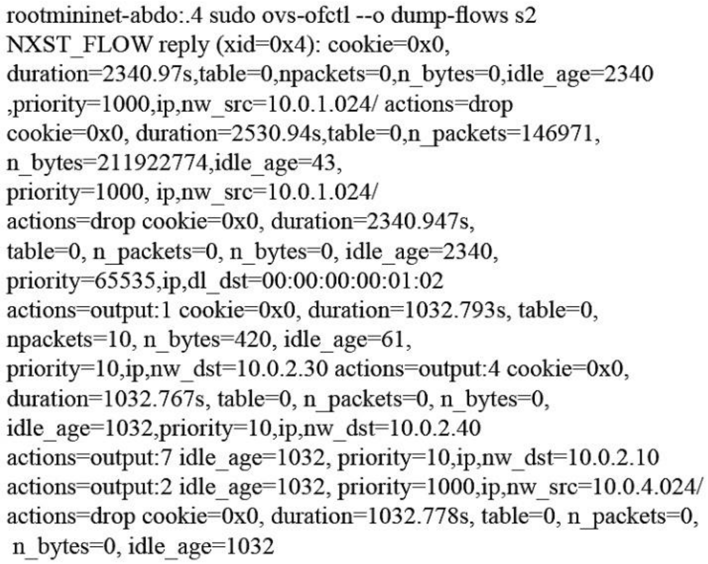


Fig.12 Before and after Mitigation f DDoS

In fig 13 this log show how rules are applied to network.



```
rootmininet-abdo:.4 sudo ovs-ofctl --o dump-flows s2
NXST_FLOW reply (xid=0x4): cookie=0x0,
duration=2340.97s,table=0,npackets=0,n_bytes=0,idle_age=2340
,priority=1000,ip,nw_src=10.0.1.024/ actions=drop
cookie=0x0, duration=2530.94s,table=0,n_packets=146971,
n_bytes=211922774,idle_age=43,
priority=1000, ip,nw_src=10.0.1.024/
actions=drop cookie=0x0, duration=2340.947s,
table=0, n_packets=0, n_bytes=0, idle_age=2340,
priority=65535,ip,dl_dst=00:00:00:00:01:02
actions=output:1 cookie=0x0, duration=1032.793s, table=0,
npackets=10, n_bytes=420, idle_age=61,
priority=10,ip,nw_dst=10.0.2.30 actions=output:4 cookie=0x0,
duration=1032.767s, table=0, n_packets=0, n_bytes=0,
idle_age=1032,priority=10,ip,nw_dst=10.0.2.40
actions=output:7 idle_age=1032, priority=10,ip,nw_dst=10.0.2.10
actions=output:2 idle_age=1032, priority=1000,ip,nw_src=10.0.4.024/
actions=drop cookie=0x0, duration=1032.778s, table=0, n_packets=0,
 n_bytes=0, idle_age=1032
```

Fig.13 Logs of openvswitch

In fig 14 shows another attempt of attack and the result of it in table 3 shows full time from detect to mitigate.

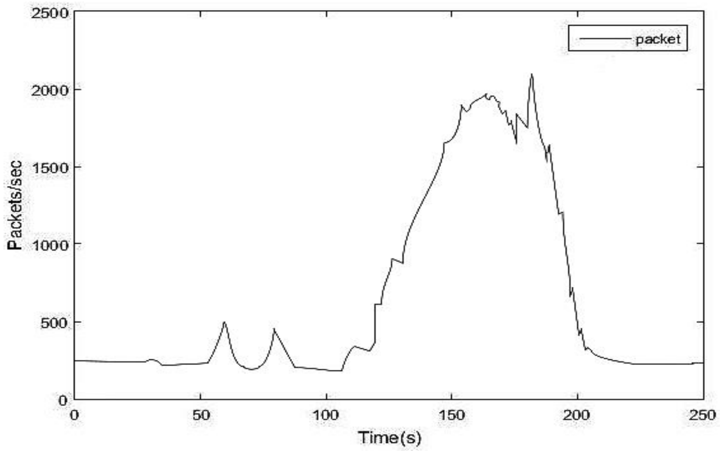


Fig. 14 Another example of attack traffic x axis (t) y axis packet

Table 3 Output from fig 14 traffic during attack

No	Time(s)	Packet/1 sec
1	30	220
2	60	210
3	90	200
4	120	230
5	150	2024
6	180	1800
7	210	220

Compression between different type of mechanism used to detect and reduce the effect of ddos attack with different of controller and strategies

Table 4 Sdn counter to DDoS

Author and publish year	Defense type	Location	Controller	Aim
1-Li et al/ year 2020 (Li & Wu, 2020)	Only detect	Control plane	Floodlight	1-Create hash table of destination ip by collect info from switch periodically.
2-MATHEUS P. NOVAES/year 2020 (Novaes, Carvalho, Lloret, & Proenca, 2020)	Detect and Mitigation	Application	Floodlight	2-(ECA) Event Condition-Action model is applied to make dynamic policies to mitigation of DDoS attacks.
3-Hong et al/year 2019 (Hong, Lee, & Lee, 2019)	Detect and Mitigation	Control plane	Openday-light	3-collect data from switch decide if there is attack or not and generate new rule.
4-Xuanyuan et al/year 2019 (Xuanyuan, Ramsurrun, & Seeam, 2019)	Detect and Mitigation	Control plane	Pox	4-entropy used for detect wildcard policy applied to drop the attack packet.
5- Myint et al./year 2019 (Myint Oo, Kamolphiwong, Kamolphiwong, & Vasupongayya, 2019)	Only detect	Application	Openday-light	5-Module used to collect information and send it to SVM to decide if there is attack.
6- Bhushan et al./year 2019 (Bhushan & Gupta, 2019)	Detect and Mitigation	Data	Pox	6-there is black list data base keep the attacker's ip address math model used when there is attack to calculate free space of other switch and mitigate the attack.
7-Anupama Mishra /year 2021 (Mishra, Gupta, & Gupta, 2021)	Detect and Mitigation	Application	Pox	7-use entropy variations to detect and flow drop to mitigate.
8-Nagarathna Ravi /year 2020 (Ravi & Shalinie, 2020)	Detect and Mitigation	IoT-Data	Ryu	8-used SDELM (Semi supervised deep extreme learning Machine) to detect for mitigation module used to drop rules in flow table.
9-R.M.A. Ujjan, Z. al/year 2019 (Ujjan et al., 2021)	Only Detect	IoT-Data	Ryu	9-collect data from IoT nodes snort IDS used to detect any malicious traffic.
10- JESÚS ARTURO PÉREZ-DÍAZ1/year 2020 (Perez-Diaz, Valdovinos, Choo, & Zhu, 2020)	Detect and Mitigation	Application	ONOS	10-IDS module used to detect the attack and for mitigation (EWMA) filter and kalman filters to put new flow rule and don't block legitimate users.

The sdn can merge with other different technology to achieve more secure system the IOT internet over things (Al-Saadi & Ilyas, 2020) and machine learning and AI artificial intelligence also SDN used in routing method for Wi-Fi in mininet emulator sdn-wifi technology is developed with high efficacy (Ahmed, Alkahrsan, & Ilyas, 2020) SDN is the new trend of technology same as IoT both of these two techs depend on other. And sdn is very reliable for network management like for hospital or company network can handle the traffic and make new policy to avoid traffic stress on the network. There are SDN-enabled adapter for secure end-to-end data these adaptors make the med devices more secure and can inject dynamic police in real-time and in this table compression between similar work and our proposal

Table 5 compression work

Parameter	Our proposal	Similar work
1-emulator	Mininet	Gns3
2-controller	Sdn-opendaylight	ODL
3-topology	Custom	Mesh topology
4- traffic generator	Scapy	Ping attack
5-response time	Much faster	Require more time
6-Dynamic	Yes	No manually

In table 5 Mininet is newer than gns3 and have many new features and it is easy to use and the booting time is faster and have large scale can add a lot of hosts and switches with higher bandwith (K. Kaur, Singh, & Ghumman, 2014). Openday-light performs better than other controller lower delay time and (Smida, Tounsi, Frikha, & Song, 2020) and our custom toplogy allow is to do test on it with high performance without lags or delays.scapy is the ultimate tool for testing network all these tools give us high response time to counter the ddos attack.

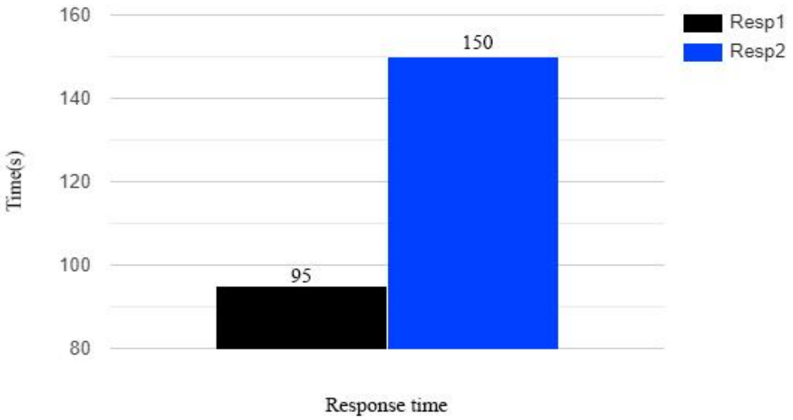


Fig. 15 Compression in Response Time

In fig 15 where response 1 with black color represents our work and the time of response to attack and mitigate it and response 2 with blue color represent the similar work

Conclusions

This paper present DDoS attack and the damage can caused by it to the network and overwhelm the space of flow table that leads to not get access into the resource of the network and how to reduce and redirect the traffic to drop it by using SDN with mininet installed on virtual machine and by using (ODL) openday light also on virtual machine. There is a lot of option of how to reduce effect of DDoS but in this paper proposed the SDN as Controller to alleviate the impact. (ICMP) internet control message protocol flood used to launch the attack on the custom topology that created before. The system was able to detect and mitigation the attack of DDoS in average time. The openvswitch can be modified and programed however you need that make it strength tool so in the future can do multiply tasks up to the situation or the problem that face the developer .in the future suggest to search about rate and how to limit it and merge SDN technology with IOT internet of things so can avoid DDoS attack remotely.

References

Aamir, M., & Ali Zaidi, S.M. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University - Computer and Information Sciences*, *33*(4), 436–446. https://doi.org/10.1016/j.jksuci.2019.02.003

Ahmed, M., Alkahrsan, A., & Ilyas, M. (2020). Load Balancing in Hybrid WIFI/LIFI Networks Based on the RSSI of the Load Using Optimized KNN Clustering. *HORA 2020 - 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, 1–4. https://doi.org/10.1109/HORA49412.2020.9152887

Al-Saadi, M.J.M., & Ilyas, M. (2020). Identity Management Approach in Internet of Things (IoT). *4th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2020 - Proceedings*, (May). https://doi.org/10.1109/ISMSIT50672.2020.9254470

Ali, S., Alvi, M.K., Faizullah, S., Khan, M.A., Alshanqiti, A., & Khan, I. (2020). Detecting DDoS attack on SDN Due to vulnerabilities in OpenFlow. *2019 International Conference on Advances in the Emerging Computing Technologies, AECT 2019*. https://doi.org/10.1109/AECT47998.2020.9194211

Alzahrani, S., & Hong, L. (2018). Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation. *Journal of Information Security*, *09*(04), 225–241. https://doi.org/10.4236/jis.2018.94016

Benton, K., Camp, L.J., & Small, C. (2013). OpenFlow vulnerability assessment. *HotSDN 2013 - Proceedings of the 2013 ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, 151–152. https://doi.org/10.1145/2491185.2491222

Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 1985–1997. https://doi.org/10.1007/s12652-018-0800-9

Dargahi, T., Caponi, A., Ambrosin, M., Bianchi, G., & Conti, M. (2017). A Survey on the Security of Stateful SDN Data Planes. *IEEE Communications Surveys & Tutorials*, *19*(3), 1701–1725. https://doi.org/10.1109/COMST.2017.2689819

Dridi, L., & Zhani, M. F. (2016). SDN-Guard: DoS Attacks Mitigation in SDN Networks. *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)*, 212–217. https://doi.org/10.1109/CloudNet.2016.9

Gopakumar, R., Unni, A. M., & Dhipin, V. P. (2015). An adaptive algorithm for searching in flow tables of openflow switches. *2015 39th National Systems Conference (NSC)*, 1–5. https://doi.org/10.1109/NATSYS.2015.7489115

Hasan, M., & Hisham Dahshan. (2020). *SDN Mininet Emulator Benchmarking and Result Analysis*. (February), 1–32.

Hong, G.C., Lee, C.N., & Lee, M.F. (2019). Dynamic threshold for DDoS mitigation in SDN environment. *2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2019*, (November), 1–7. https://doi.org/10.1109/APSIPAASC47483.2019.9023229

Hu, F., Hao, Q., & Bao, K. (2014). A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation. *IEEE Communications Surveys & Tutorials*, *16*(4), 2181–2206. https://doi.org/10.1109/COMST.2014.2326417

Isolani, P.H., Wickboldt, J.A., Both, C.B., Rochol, J., & Granville, L.Z. (2015). Interactive monitoring, visualization, and configuration of OpenFlow-based SDN. *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 207–215. https://doi.org/10.1109/INM.2015.7140294

Isyaku, B., Mohd Zahid, M.S., Bte Kamat, M., Abu Bakar, K., & Ghaleb, F.A. (2020). Software Defined Networking Flow Table Management of OpenFlow Switches Performance and Security Challenges: A Survey. *Future Internet*, *12*(9). https://doi.org/10.3390/fi12090147

Kaspersky Q3 2021 DDoS attack report | Securelist. (n.d.). Retrieved November 15, 2021, from https://securelist.com/ddos-attacks-in-q3-2021/104796/

Kaur, K., Singh, J., & Ghumman, N.S. (2014). Mininet as Software Defined Networking Testing Platform. *International Conference on Communication, Computing & Systems (ICCCS–2014)*, (August), 3–6.

Kaur, S., Kumar, K., Aggarwal, N., & Singh, G. (2021). A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions. *Computers and Security*, *110*, 102423. https://doi.org/10.1016/j.cose.2021.102423

Kumar, S., Kumar, T., Singh, G., & Nehra, M.S. (2012). Open Flow Switch with Intrusion Detection System. *International Journal of Scientific Research Engineering & Technology (IJSRET)*, *1*(October), 1–4. http://www.ijsret.org/pdf/suresh_kumar.pdf

Lara, A., Kolasani, A., & Ramamurthy, B. (2014). Network Innovation using OpenFlow: A Survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 493–512. https://doi.org/10.1109/SURV.2013.081313.00105

Li, R., & Wu, B. (2020). Early detection of DDoS based on \varphi-entropy in SDN networks. *Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020*, (Itnec), 731–735. https://doi.org/10.1109/ITNEC48623.2020.9084885

Lougheed, K. (2021). *What Is Ubuntu?* https://doi.org/10.4324/9781003141747-2

Martinez, C., Ferro, R., & Ruiz, W. (2015). Next generation networks under the SDN and OpenFlow protocol architecture. *2015 Workshop on Engineering Applications - International Congress on Engineering (WEA)*, 1–7. https://doi.org/10.1109/WEA.2015.7370147

Mishra, A., Gupta, N., & Gupta, B.B. (2021). Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. *Telecommunication Systems*, *77*(1), 47–62. https://doi.org/10.1007/s11235-020-00747-w

Moharir, M., Adyathimar, K. B., Shobha, G., & Soni, V. (2020). Scapy scripting to automate testing of networking middleboxes. *Advances in Science, Technology and Engineering Systems*, *5*(2), 293–298. https://doi.org/10.25046/aj050238

Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T., & Vasupongayya, S. (2019). Advanced Support Vector Machine-(ASVM-) based detection for Distributed Denial of Service (DDoS) attack on Software Defined Networking (SDN). *Journal of Computer Networks and Communications*, *2019*. https://doi.org/10.1155/2019/8012568

Novaes, M.P., Carvalho, L.F., Lloret, J., & Proenca, M.L. (2020). Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access*, *8*, 83765–83781. https://doi.org/10.1109/ACCESS.2020.2992044

Oo, M.M., Kamolphiwong, S., & Kamolphiwong, T. (2017). The Design of SDN Based Detection for Distributed Denial of Service (DDoS) Attack. *21st International Computer Science and Engineering Conference (ICSEC)*, 1–5. https://doi.org/10.1109/ICSEC.2017.8443939

Perez-Diaz, J.A., Valdovinos, I.A., Choo, K.K.R., & Zhu, D. (2020). A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. *IEEE Access*, *8*, 155859–155872. https://doi.org/10.1109/ACCESS.2020.3019330

Ravi, N., & Shalinie, S.M. (2020). Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture. *IEEE Internet of Things Journal*, *7*(4), 3559–3570. https://doi.org/10.1109/JIOT.2020.2973176

Salman, O., Elhajj, I.H., Kayssi, A., & Chehab, A. (2016). SDN controllers: A comparative study. *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, 1–6. https://doi.org/10.1109/MELCON.2016.7495430

Sangodoyin, A., Sigwele, T., Pillai, P., Hu, Y.F., Awan, I., & Disso, J. (2018). DoS Attack Impact Assessment on Software Defined Networks. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *231*, 11–22. https://doi.org/10.1007/978-3-319-76571-6_2

Sanjeetha, R., Prasanna, A., Kumar, D.P., & Kanavalli, A. (2018). Mitigation of Controller induced DDoS Attack on Primary Server in High Traffic Scenarios of Software Defined Networks. *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 1–6. https://doi.org/10.1109/ANTS.2018.8710066

Sasi, G. (2020). *Computer Networks using Wireshark*. (Icisc), 456–461.

Siamak Azodolmolky. (2013). *Software Defined Networking with OpenFlow*.

Singh, M.P., & Bhandari, A. (2020). New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. *Computer Communications*, *154*(October 2019), 509–527. https://doi.org/10.1016/j.comcom.2020.02.085

Sirijaroensombat, S., Nangsue, C.P., & Aswakul, C. (2019). Development of Software-Defined Mesh Network Emulator Testbed for DDoS Defence Study. *IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 468–472. https://doi.org/10.1109/CCOMS.2019.8821667

Smida, K., Tounsi, H., Frikha, M., & Song, Y.Q. (2020). Efficient SDN Controller for Safety Applications in SDN-Based Vehicular Networks: POX, Floodlight, ONOS or OpenDaylight? *2020 8th International Conference on Communications and Networking, ComNet2020 - Proceedings*, 1–6. https://doi.org/10.1109/ComNet47917.2020.9306095

Ujjan, R.M.A., Pervez, Z., Dahal, K., Khan, W.A., Khattak, A.M., & Hayat, B. (2021). Entropy based features distribution for anti-ddos model in SDN. *Sustainability (Switzerland)*, *13*(3), 1–27. https://doi.org/10.3390/su13031522

Xuanyuan, M., Ramsurrun, V., & Seeam, A. (2019). Detection and mitigation of DDoS attacks using conditional entropy in software-defined networking. *Proceedings of the 11th International Conference on Advanced Computing, ICoAC 2019*, (March 2020), 66–71. https://doi.org/10.1109/ICoAC48765.2019.246818