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](http://www.webology.org)

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
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.

![Deployment Details of SDN-based Cyber Defense Solutions](image)

**Fig. 4 SDN Details**
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 usefui.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.
Table 1 Different between SDN and normal network

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

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

<table>
<thead>
<tr>
<th>Tools</th>
<th>Describe and use for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scapy</td>
<td>Traffic generator</td>
</tr>
<tr>
<td>Ubuntu &amp; Kali Linux</td>
<td>(OS) Operating system</td>
</tr>
<tr>
<td>Mininet</td>
<td>Network simulation</td>
</tr>
<tr>
<td>Openflow</td>
<td>Protocol</td>
</tr>
<tr>
<td>OpenDaylight</td>
<td>Controller of Sdn</td>
</tr>
<tr>
<td>Wireshark</td>
<td>Analyze traffic</td>
</tr>
<tr>
<td>OpenvSwitch</td>
<td>Sdn switch</td>
</tr>
</tbody>
</table>

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 switches, 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.
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.

```python
python3 mininet/custom/abdurrahman.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')
    r1 = net.addHost( 'r1', ip='10.0.1.1/24', mac='00:00:00:00:01:01')
    c0 = net.addHost( 'c0', ip='10.0.1.2/24', mac='00:00:00:00:00:02')

    s2 = net.addSwitch('s2'
```

Fig. 9 Network by Python Code

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](image1)

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](image2)
In fig 13 this log shows how rules are applied to network.

```
rootmininet-abdo:~$ sudo ovs-ofctl --o dump-flows s2
NXST_FLOW reply (xid=0x4): cookie=0x0,
duration=2340.97s,table=0,n_packets=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,dll_dst=00:00:00:00:00:01:02
.actions=output:1 cookie=0x0,duration=1032.793s,table=0,
n_packets=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.

![Graph showing another example of attack traffic](image)

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

**Table 3 Output from fig 14 traffic during attack**

<table>
<thead>
<tr>
<th>No</th>
<th>Time(s)</th>
<th>Packet/1 sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30</td>
<td>220</td>
</tr>
<tr>
<td>2</td>
<td>60</td>
<td>210</td>
</tr>
<tr>
<td>3</td>
<td>90</td>
<td>200</td>
</tr>
<tr>
<td>4</td>
<td>120</td>
<td>230</td>
</tr>
<tr>
<td>5</td>
<td>150</td>
<td>2024</td>
</tr>
<tr>
<td>6</td>
<td>180</td>
<td>1800</td>
</tr>
<tr>
<td>7</td>
<td>210</td>
<td>220</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Author and publish year</th>
<th>Defense type</th>
<th>Location</th>
<th>Controller</th>
<th>Aim</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Li et al/year 2020 (Li &amp; Wu, 2020)</td>
<td>Only detect</td>
<td>Control plane</td>
<td>Floodlight</td>
<td>1-Create hash table of destination ip by collect info from switch periodically.</td>
</tr>
<tr>
<td>2-MATHEUS P. NOVAES/year 2020 (Novaes, Carvalho, Lloret, &amp; Proenca, 2020)</td>
<td>Detect and Mitigation</td>
<td>Application</td>
<td>Floodlight</td>
<td>2-(ECA) Event Condition-Action model is applied to make dynamic policies to mitigation of DDoS attacks.</td>
</tr>
<tr>
<td>3-Hong et al/year 2019 (Hong, Lee, &amp; Lee, 2019)</td>
<td>Detect and Mitigation</td>
<td>Control plane</td>
<td>Opendaylight</td>
<td>3-collect data from switch decide if there is attack or not and generate new rule.</td>
</tr>
<tr>
<td>4-Xuanyuan et al/year 2019 (Xuanyuan, Ramsurrun, &amp; Seeam, 2019)</td>
<td>Detect and Mitigation</td>
<td>Control plane</td>
<td>Pox</td>
<td>4-entropy used for detect wildcard policy applied to drop the attack packet.</td>
</tr>
<tr>
<td>5- Myint et al./year 2019 (Myint Oo, Kamolphiwong, Kamolphiwong, &amp; Vasupongayya, 2019)</td>
<td>Only detect</td>
<td>Application</td>
<td>Opendaylight</td>
<td>5-Module used to collect information and send it to SVM to decide if there is attack.</td>
</tr>
<tr>
<td>6- Bhushan et al./year 2019 (Bhushan &amp; Gupta, 2019)</td>
<td>Detect and Mitigation</td>
<td>Data</td>
<td>Pox</td>
<td>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.</td>
</tr>
<tr>
<td>7-Anupama Mishra /year 2021 (Mishra, Gupta, &amp; Gupta, 2021)</td>
<td>Detect and Mitigation</td>
<td>Application</td>
<td>Pox</td>
<td>7-use entropy variations to detect and flow drop to mitigate.</td>
</tr>
<tr>
<td>8-Nagarathna Ravi /year 2020 (Ravi &amp; Shalinie, 2020)</td>
<td>Detect and Mitigation</td>
<td>IoT-Data</td>
<td>Ryu</td>
<td>8-used SDELM (Semi supervised deep extreme learning Machine) to detect for mitigation module used to drop rules in flow table.</td>
</tr>
<tr>
<td>9-R.M.A. Ujjan, Z. al/year 2019 (Ujjan et al., 2021)</td>
<td>Only Detect</td>
<td>IoT-Data</td>
<td>Ryu</td>
<td>9-collect data from IoT nodes snort IDS used to detect any malicious traffic.</td>
</tr>
<tr>
<td>10- JESÚS ARTURO PÉREZ-DÍAZI/year 2020 (Perez-Diaz, Valdovino, Choo, &amp; Zhu, 2020)</td>
<td>Detect and Mitigation</td>
<td>Application</td>
<td>ONOS</td>
<td>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.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Parameter</th>
<th>Our proposal</th>
<th>Similar work</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-emulator</td>
<td>Mininet</td>
<td>Gns3</td>
</tr>
<tr>
<td>2-controller</td>
<td>Sdn-opendaylight</td>
<td>ODL</td>
</tr>
<tr>
<td>3-topology</td>
<td>Custom</td>
<td>Mesh topology</td>
</tr>
<tr>
<td>4-traffic generator</td>
<td>Scapy</td>
<td>Ping attack</td>
</tr>
<tr>
<td>5-response time</td>
<td>Much faster</td>
<td>Require more time</td>
</tr>
<tr>
<td>6-Dynamic</td>
<td>Yes</td>
<td>No manually</td>
</tr>
</tbody>
</table>

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 topology 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](http://www.webology.org)
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 programmed 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


