



Distributed Denial-of-Service (DDoS) Attack Detection and Mitigation for Internet of Things (IoT)

OPEYEMI PETER OJAJUNI
SMED
Southern University and A&M College

SOUTHERN®
UNIVERSITY

AND AGRICULTURAL & MECHANICAL COLLEGE

PRESENTATION OUTLINE



Introduction



Proposed Solution



Implementation and Results



Limitation, Conclusion and Future work

Internet of Things (IoT)

- The Internet of Things (IoT) allows different device with Internet Protocol (IP) address, to be connected together via internet to collect, provide, store, and exchange data among themselves.
- The IoT generates large amounts of data that IoT software use for data analysis.
- Cisco projected that by 2022 the global amount of data that will be generated will reach 4.8
 Zettabytes, and by year 2030 over 500 billion devices will be connected to the internet.
- These devices are vulnerable to malicious attacks because they have limited computer system resources to support firewall and defense mechanism protocols.

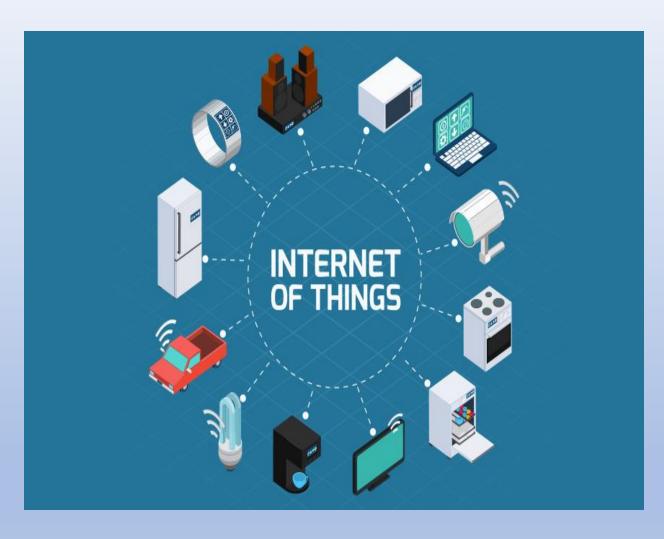


Figure 1 . Internet of things overview

Security and Privacy Issues in IoT

- Machine to machine trust,
- Authorization Authentication and Accounting,
- End- user privacy,
- Data privacy and Data confidentiality.
- Malicious attacks such as, man-in-the-middle attack, denial-of-service attack, Sybil attack, and node capture attack, distributed denial of service (DDoS)

Distributed denial of service (DDoS) Attack

The distributed denial of service is an extensive type denial of service (DoS) attack where the attacker uses more than one Internet Protocol (IP) address to send malicious traffic to its target victim in order to exhaust its computer system resources such as sockets, CPU, memory, disk or database bandwidth therefore, making the victim's service unavailable.

DDoS attack can lead to problems such as

- Loss of confidential data,
- Website service outage,
- Financial loss,
- Brand reputation damage

Major DDoS attacks in the past decade.

- Github attack : peak at 1.35 terabytes per second
- Dyn Domain name Server (DNS) attack : peak at 1.2 terabytes per seconds
- BBC attack: peak at 600 Gigabytes per second
- Spamhaus attack: peak at 400 Gigabytes per second

Types of DDoS attacks are TCP SYN flood (Transmission Control Protocol synchronize flood), ICMP (Internet Control Message Protocol) flood, Ping of death, HTTP(Hyper Text transfer Protocol) flood

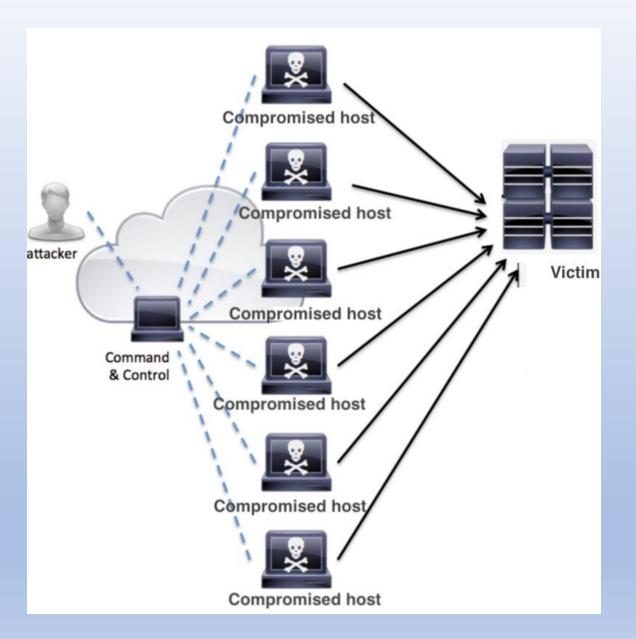


Figure 2. DDoS attack

PROPOSED SOLUTION

Software Defined Networks (SDN)

• SDN is a new architecture that offers a new chance in defeating DDoS attacks.

Why SDN over Traditional firewall?

- Software-based real-time traffic analysis,
- Centralized control management,
- Global view of the network,
- Dynamic updating of forwarding rules,
- Separation of the control plane from the data plane,
- Programmability of the network by external application

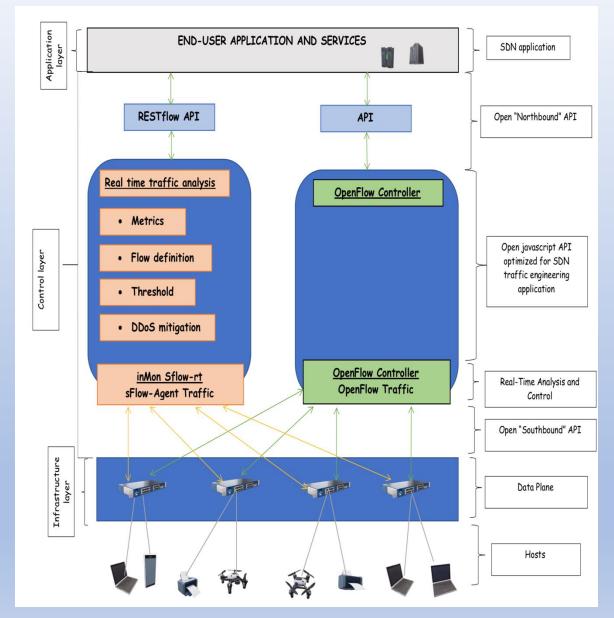


Figure 3. SDN Architecture

SDN-based DDoS attack Detection techniques

- Entropy, : network feature distribution to detect anomalous network activities.
- Machine learning: use algorithms like Bayesian networks, SOM, and fuzzy logic to identify the presence of anomalies.
- Traffic pattern analysis,: work on the assumptions that the infected IoT hosts exhibit similar behavioral patterns which are different from normal IoT hosts
- Connection rate: number of connections instantiated within a certain window of time
- SNORT :use combination of the intrusion detection system (such as SNORT)
- Open-flow integrated: OpenFlow to detect attacks and reconfigure the network dynamically.

Mitigation techniques

- Drop packet,
- Block port,
- Redirection of legitimate traffic to a new IP address,
- Control bandwidth,
- Deep packet inspection,
- network reconfiguration and topology change,
- Quarantine or Traffic isolation,
- MAC address change and/or IP address change.
 to mitigate DDoS attack.

PROPOSED SYSTEM SETUP

- The host PC CPU is 2.3Ghz Intel Core i5 and 8 GB 2133 MHz LPDDR3 memory.
- The virtual machine has one processor core CPU and 2GB memory.
- The Mininet is a network simulator that runs on a virtual machine with Ubuntu 14.0 operating system.
- The Mininet is used to create the SDN network topology with OpenFlow switch and host PCs and it is connected to SDN controller.
- The floodlight is the Java-based OpenFlow controller and it runs on the virtual machine with Ubuntu 14.0 operating system.
- The inMon sFlow-RT is used for real-time traffic analysis and it runs on the virtual machine with Ubuntu 14.0 operating system.
- The Nodejs is an open-source, cross-platform JavaScript run-time environment that executes JavaScript code outside of a browser and it runs on the virtual machine with Ubuntu 14.0 operating system.
- The browser is used to access graphical user interface (GUI) of the floodlight and inMon sFlow-RT.

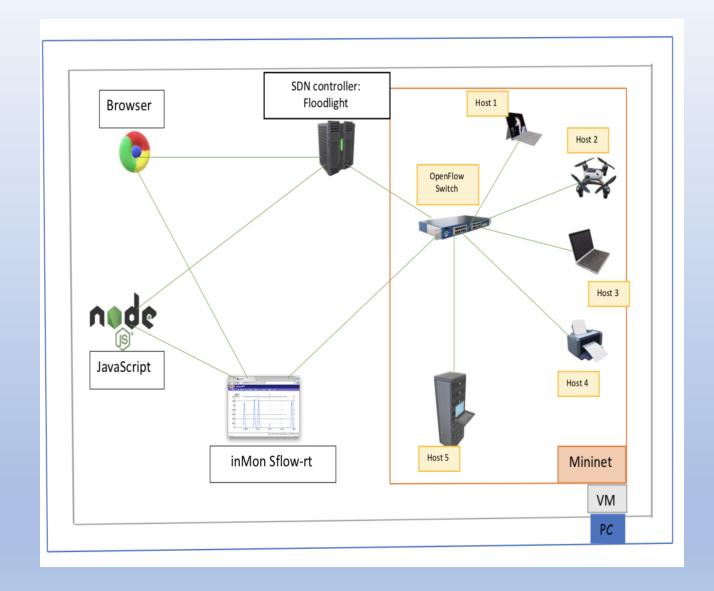


Figure 4. Proposed system setup.

IMPLEMENTATION AND RESULTS

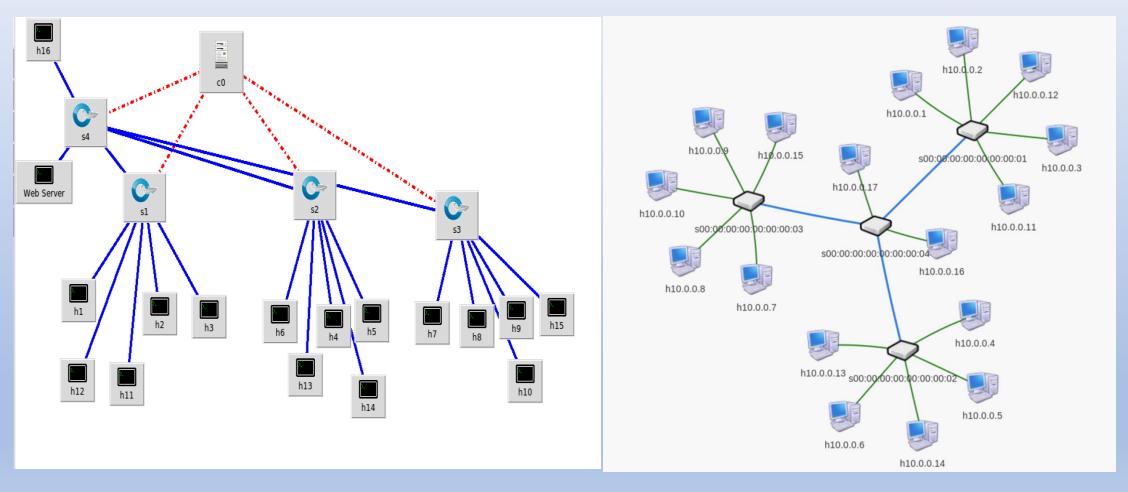


Figure 5. Topology of proposed system

Figure 6. Topology of proposed system in SDN controller

Results before DDoS Attack

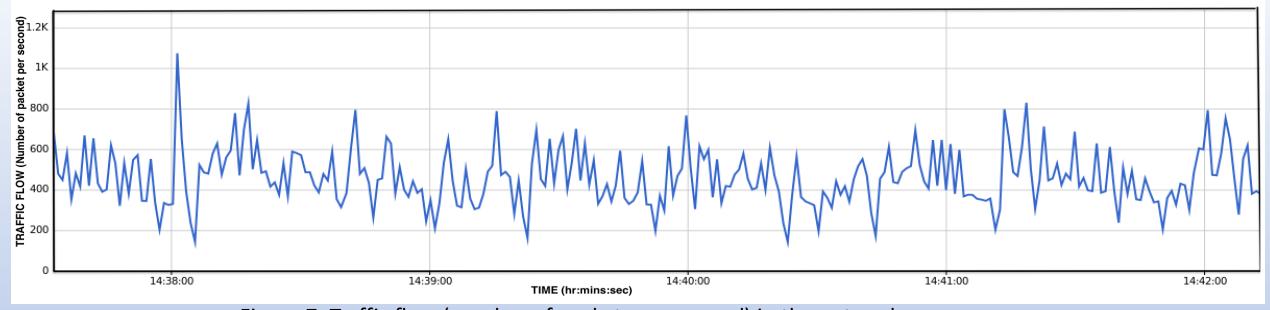


Figure 7. Traffic flow (number of packets per second) in the network

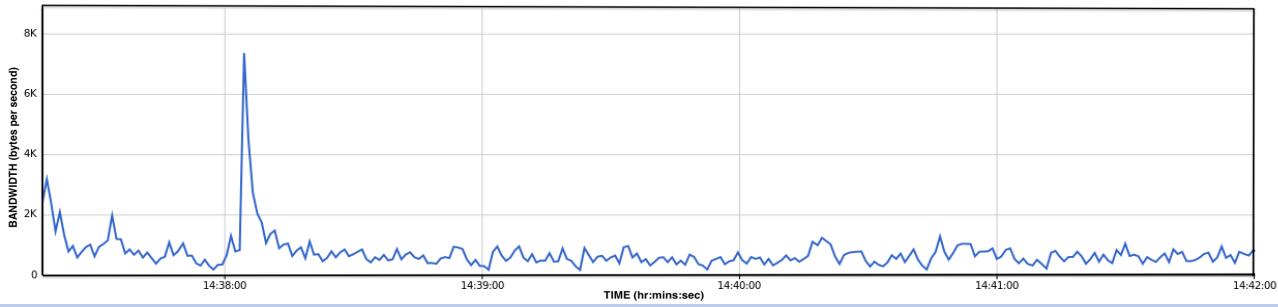


Figure 8. Network bandwidth (bytes per second)

□ □ "Host: h10" icmp seq=520 tt1=64 time=0.035 ms| <64 bytes from 10.0.0.17: icmp_seq=327 ttl=64 time=0.046 ms $icmp_seq=521 ttl=64 time=0.030 ms$ 64 bytes from 10.0.0.17: icmp_seq=328 ttl=64 time=0.032 ms icmp_seq=522 ttl=64 time=0.042 ms 64 bytes from 10.0.0.17: icmp_seq=329 ttl=64 time=0.043 ms icmp_seq=523 ttl=64 time=0.045 ms. is64 bytes from 10.0.0.17: icmp_seq=330 ttl=64 time=0.036 ms icmp_seq=524 ttl=64 time=0.037 ms 64 bytes from 10.0.0.17: icmp_seq=331 ttl=64 time=0.040 ms icmp_seq=525 ttl=64 time=0.031 ms 64 bytes from 10.0.0.17: icmp_seq=332 ttl=64 time=0.038 ms icmp_seq=526 ttl=64 time=0.041 ms **\5**64 bytes from 10.0.0.17: icmp_seq=333 ttl=64 time=0.036 ms icmp_seq=527 ttl=64 time=0.033 ms 64 bytes from 10.0.0.17: icmp_seq=334 ttl=64 time=0.036 ms icmp_seq=528 ttl=64 time=0.049 ms 64 bytes from 10.0.0.17: icmp_seq=335 ttl=64 time=0.041 ms icmp_seq=529 ttl=64 time=0.103 ms **LS**64 bytes from 10.0.0.17: icmp_seq=336 ttl=64 time=0.067 ms icmp_seq=530 ttl=64 time=0.035 ms. 64 bytes from 10.0.0.17: icmp_seq=337 ttl=64 time=0.040 ms icmp_seq=531 ttl=64 time=0.030 ms 64 bytes from 10.0.0.17: icmp_seq=338 ttl=64 time=0.035 ms icmp_seq=532 ttl=64 time=0.046 ms 64 bytes from 10.0.0.17: icmp_seq=339 ttl=64 time=0.037 ms icmp_seq=533 ttl=64 time=0.057 ms 64 bytes from 10.0.0.17: icmp_seq=340 ttl=64 time=0.033 ms icmp_seq=534 ttl=64 time=0.041 ms 64 bytes from 10.0.0.17: icmp_seq=341 ttl=64 time=0.050 ms icmp_seq=535 ttl=64 time=0.041 ms $-\sqrt{64}$ bytes from 10.0.0.17: icmp_seq=342 ttl=64 time=0.032 ms icmp_seq=536 ttl=64 time=0.037 ms 1664 bytes from 10.0.0.17: icmp_seq=343 ttl=64 time=0.051 ms icmp_seq=537 ttl=64 time=0.049 ms 64 bytes from 10.0.0.17: icmp_seq=344 ttl=64 time=0.041 ms icmp_seq=538 ttl=64 time=0.059 ms 64 bytes from 10.0.0.17: icmp_seq=345 ttl=64 time=0.040 ms icmp_seq=539 ttl=64 time=0.146 ms 64 bytes from 10.0.0.17: icmp_seq=346 ttl=64 time=0.041 ms icmp_seq=540 ttl=64 time=0.026 ms 64 bytes from 10.0.0.17: icmp_seq=347 ttl=64 time=0.027 ms icmp_seq=541 ttl=64 time=0.040 ms 64 bytes from 10.0.0.17: icmp_seq=348 ttl=64 time=0.031 ms icmp_seq=542 ttl=64 time=0.041 ms 5C64 bytes from 10.0.0.17: icmp_seq=349 ttl=64 time=0.035 ms □ □ "Host: h14" **5C** 64 bytes from 10.0.0.17: icmp_seq=298 ttl=64 time=0.047 ms icmp_seq=503 ttl=64 time=0.030 ms 10 64 bytes from 10.0.0.17: icmp_seq=299 ttl=64 time=0.038 ms icmp_seq=504 ttl=64 time=0.032 ms icmp_seq=505 ttl=64 time=0.040 ms 64 bytes from 10.0.0.17: icmp_seq=301 ttl=64 time=0.032 ms icmp_seq=506 ttl=64 time=0.038 ms 64 bytes from 10.0.0.17: icmp_seq=302 ttl=64 time=0.062 ms icmp_seq=507 ttl=64 time=0.056 ms 64 bytes from 10.0.0.17: icmp_seq=303 ttl=64 time=0.052 ms icmp_seq=508 ttl=64 time=0.046 ms 5C 64 bytes from 10.0.0.17: icmp_seq=304 ttl=64 time=0.042 ms icmp_seq=509 ttl=64 time=<u>0.027 ms</u> icmp_seq=510 ttl=64 time=0.031 ms **10** 64 bytes from 10.0.0.17: icmp_seq=305 ttl=64 time=0.041 ms 64 bytes from 10.0.0.17: icmp_seq=306 ttl=64 time=0.047 ms icmp_seq=511 ttl=64 time=0.042 ms 64 bytes from 10.0.0.17: icmp_seq=307 ttl=64 time=0.037 ms icmp_seq=512 ttl=64 time=0.088 ms icmp_seq=513 ttl=64 time=0.058 ms 64 bytes from 10.0.0.17: icmp_seq=308 ttl=64 time=0.126 ms 64 bytes from 10.0.0.17: icmp_seq=309 ttl=64 time=0.032 ms icmp_seq=514 ttl=64 time=0.034 ms 64 bytes from 10.0.0.17: icmp_seq=310 ttl=64 time=0.044 ms icmp_seq=515 ttl=64 time=0.068 ms icmp_seq=516 ttl=64 time=0.053 ms 64 bytes from 10.0.0.17: icmp_seq=312 ttl=64 time=0.049 ms icmp_seq=517 ttl=64 time=0.038 ms 0.64 bytes from 10.0.0.17: icmp_seq=313 ttl=64 time=0.051 ms icmp_seq=518 ttl=64 time=0.050 ms 64 bytes from 10.0.0.17: icmp_seq=314 ttl=64 time=0.043 ms icmp_seq=519 ttl=64 time=0.039 ms icmp_seq=520 ttl=64 time=0.052 ms 64 bytes from 10.0.0.17: icmp_seq=315 ttl=64 time=0.029 ms icmp_seq=521 ttl=64 time=0.052 ms **as** 64 bytes from 10.0.0.17: icmp_seq=316 ttl=64 time=0.027 ms icmp_seq=522 ttl=64 time=0.032 ms 64 bytes from 10.0.0.17: icmp_seq=317 ttl=64 time=0.032 ms 64 bytes from 10.0.0.17: icmp_seq=318 ttl=64 time=0.048 ms icmp_seq=523 ttl=64 time=0.025 ms 64 bytes from 10.0.0.17: icmp_seq=319 ttl=64 time=0.040 ms 64 bytes from 10.0.0.17: icmp_seq=320 ttl=64 time=0.040 ms icmp_seq=525 ttl=64 time=0.041 ms

🚳 🖨 📵 "Host: h13" **1**64 bytes from 10.0.0.17: icmp_seq=292 ttl=64 64 bytes from 10.0.0.17: icmp_seq=293 ttl=64 64 bytes from 10.0.0.17; icmp_seq=294 ttl=64 nc64 bytes from 10.0.0.17: icmp_seq=295 ttl=64 64 bytes from 10.0.0.17: icmp_seq=296 ttl=64 64 bytes from 10.0.0.17: icmp_seq=297 ttl=64 **1**64 bytes from 10.0.0.17: icmp_seq<u>=298 ttl=64</u> 64 bytes from 10.0.0.17: icmp_seq=299 ttl=64 64 bytes from 10.0.0.17; icmp_seq=300 ttl=64 **6**64 bytes from 10.0.0.17: icmp_seq=301 ttl=64 64 bytes from 10.0.0.17: icmp_seq=302 ttl=64 64 bytes from 10.0.0.17: icmp_seq=303 ttl=64 €64 bytes from 10.0.0.17: icmp_seq=304 ttl=64 **e**†64 bytes from 10.0.0.17: icmp_seq=305 ttl=64 64 butes from 10.0.0.17: icmp_seq=306 ttl=64 64 bytes from 10.0.0.17: icmp_seq=307 ttl=64 64 bytes from 10.0.0.17; icmp_seq=308 ttl=64 **F**64 bytes from 10.0.0.17: icmp_seq=309 ttl=64 _64 bytes from 10.0.0.17: icmp_seq=310 ttl=64 64 bytes from 10.0.0.17: icmp_seq=311 ttl=64 64 bytes from 10.0.0.17: icmp_seq=312 ttl=64 64 bytes from 10.0.0.17; icmp_seq=313 ttl=64 64 bytes from 10.0.0.17: icmp_seq=314 ttl=64

root@ubuntu:~# ifconfig h17-eth0 Link encap:Etl inet addr:10. inet6 addr: f UP BROADCAST | RX packets:23 TX packets:8 | collisions:0 | RX bytes:3231: lo Link encap:Lo inet6 addr: : UP LOOPBACK R

RX packets:0

TX packets:0 collisions:0 <u>RX b</u>ytes:0 (0

root

root@ubuntu:~# python -

Figure 9. Time delay for ping command from normal host users.

Results after DDoS attack



Figure 10. Traffic Flow (number of packets per second) in the network under attack

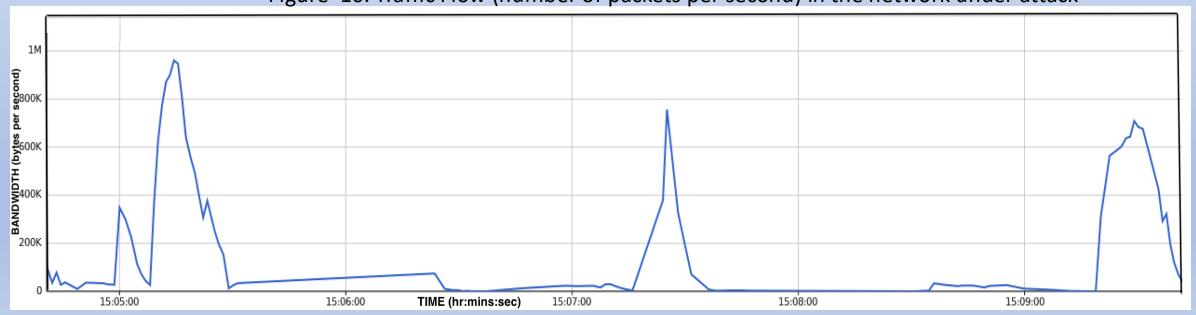


Figure 11. Network Bandwidth under attack

□ □ "Host: h11" 64 bytes from 10.0.0.17: icmp_seq=435 ttl=64 time=8860 ms 64 bytes from 10.0.0.17: icmp_seq=436 ttl=6<u>4 time=7852 ms</u> 64 bytes from 10.0.0.17: icmp_seq=437 ttl=64 time=6844 ms 64 bytes from 10.0.0.17: icmp_seq=438 ttl=64 time=5836 ms 64 bytes from 10.0.0.17: icmp_seq=439 ttl=64 time=4828 ms 64 bytes from 10.0.0.17: icmp_seq=440 ttl=64 time=3820 ms 64 bytes from 10.0.0.17: icmp_seg=441 ttl=64 time=2811 ms 64 bytes from 10.0.0.17: icmp_seq=442 ttl=64 time=1811 ms 64 bytes from 10.0.0.17: icmp_seq=443 ttl=64 time=945 ms 64 bytes from 10.0.0.17: icmp_seq=444 ttl=64 time=0.407 ms 64 bytes from 10.0.0.17: icmp_seq=445 ttl=64 time=687 ms From 10.0.0.17 icmp_seq=497 Destination Host Unreachable From 10.0.0.17 icmp_seq=498 Destination Host Unreachable From 10.0.0.17 icmp_seq=499 Destination Host Unreachable From 10.0.0.17 icmp_seq=500 Destination Host Unreachable From 10.0.0.17 icmp_seq=501 Destination Host Unreachable From 10.0.0.17 icmp_seq=502 Destination Host Unreachable From 10.0.0.17 icmp_seq=503 Destination Host Unreachable From 10.0.0.17 icmp_seq=504 Destination Host Unreachable From 10.0.0.17 icmp_seq=505 Destination Host Unreachable From 10.0.0.17 icmp_seq=506 Destination Host Unreachable From 10.0.0.17 icmp_seq=507 Destination Host Unreachable From 10.0.0.17 icmp_seq=508 Destination Host Unreachable Change Controllers 🗎 🔲 "Host: h12" bytes from 10.0.0.17: icmp_seq=440 ttl=64 time=0.027 ms bytes from 10.0.0.17; icmp_seq=441 ttl=64 time=0.020 ms bytes from 10.0.0.17: icmp_seq=442 ttl=64 time=0.045 ms bytes from 10.0.0.17: icmp_seq=443 ttl=64 time=0.032 ms bytes from 10.0.0.17: icmp_seq=444 ttl=64 time=0.034 ms bytes from 10.0.0.17: icmp_seq=445 ttl=64 time=0.021 ms bytes from 10.0.0.17: icmp_seq=446 ttl=64 time=0.018 ms bytes from 10.0.0.17: icmp_seq=447 ttl=64 time=0.017 ms bytes from 10.0.0.17; icmp_seq=448 ttl=64 time=0.016 ms bytes from 10.0.0.17: icmp_seq=449 ttl=64 time=0.025 ms bytes from 10.0.0.17; icmp_seq=450 ttl=64 time=0.016 ms om 10.0.0.17 icmp_seq=492 Destination Host Unreachable om 10.0.0.17 icmp_seq=493 Destination Host Unreachable om 10.0.0.17 icmp_seq=494 Destination Host Unreachable om 10.0.0.17 icmp_seq=495 Destination Host Unreachable om 10.0.0.17 icmp_seq=496 Destination Host Unreachable om 10.0.0.17 icmp_seq=497 Destination Host Unreachable om 10.0.0.17 icmp_seq=498 Destination Host Unreachable om 10.0.0.17 icmp_seq=499 Destination Host Unreachable om 10.0.0.17 icmp_seq=500 Destination Host Unreachable om 10.0.0.17 icmp_seq=501 Destination Host Unreachable om 10.0.0.17 icmp_seq=502 Destination Host Unreachable om 10.0.0.17 icmp_seg=503 Destination Host Unreachable

```
"Host: h10"
64 bytes from 10.0.0.17: icmp_seq=1678 ttl=64 time=0.027 ms
64 bytes from 10.0.0.17: icmp_seq=1679 ttl=64<u> time=0.038 ms</u>
64 bytes from 10.0.0.17: icmp_seq=1680 ttl=64 time=79.8 ms
64 bytes from 10.0.0.17: icmp_seq=1681 ttl=64 time=10.5 ms
64 bytes from 10.0.0.17: icmp_seq=1682 ttl=64 time=149 ms
54 bytes from 10.0.0.17: icmp_seq=1683 ttl=64 time=5.46 ms rd for opevemiojajuni:
64 bytes from 10.0.0.17: icmp_seq=1684 ttl=64 time=21.0 ms
64 bytes from 10.0.0.17: icmp_seq=1685 ttl=64 time=5.18 ms
64 bytes from 10.0.0.17: icmp_seq=1686 ttl=64 time=8.15 ms
64 bytes from 10.0.0.17: icmp_seq=1688 ttl=64 time=6.48 ms
64 bytes from 10.0.0.17: icmp_seq=1689 ttl=64 time=5.20 ms
 4 bytes from 10.0.0.17: icmp_seq=1690 ttl=64 time=5.77 ms
64 bytes from 10.0.0.17: icmp_seq=1691 ttl=64 time=10.9 ms
64 bytes from 10.0.0.17: icmp_seq=1692 ttl=64 time=4.44 ms
 4 bytes from 10.0.0.17: icmp_seq=1693 ttl=64 time=4.44 ms
64 bytes from 10.0.0.17: icmp_seq=1694 ttl=64 time=2.49 ms
64 bytes from 10.0.0.17: icmp_seq=1695 ttl=64 time=5.24 ms
64 bytes from 10.0.0.17: icmp_seq=1696 ttl=64 time=6.52 ms
4 bytes from 10.0.0.17: icmp_seq=1699 ttl=64 time=1625 ms
04 bytes from 10.0.0.17: icmp_seq=1700 ttl=64 time=622 ms
64 bytes from 10.0.0.17: icmp_seq=1703 ttl=64 time=12.3 ms
64 bytes from 10.0.0.17: icmp_seq=1706 ttl=64 time=186 ms
```

🕽 🖨 📵 "Host: h14" From 10.0.0.17 icmp_seq=1977 Destination Host Unreachable From 10.0.0.17 icmp_seq=1978 Destination Host Unreachable From 10.0.0.17 icmp_seg=1979 Destination Host Unreachable From 10.0.0.17 icmp_seq=1980 Destination Host Unreachable From 10.0.0.17 icmp_seq=1981 Destination Host Unreachable 0 From 10.0.0.17 icmp_seq=1982 Destination Host Unreachable From 10.0.0.17 icmp_seq=1983 Destination Host Unreachable From 10.0.0.17 icmp_seq=1984 Destination Host Unreachable From 10.0.0.17 icmp_seq=1985 Destination Host Unreachable From 10.0.0.17 icmp_seq=1986 Destination Host Unreachable From 10.0.0.17 icmp_seq=1987 Destination Host Unreachable From 10.0.0.17 icmp_seq=1988 Destination Host Unreachable From 10.0.0.17 icmp_seq=1989 Destination Host Unreachable From 10.0.0.17 icmp_seq=1990 Destination Host Unreachable From 10.0.0.17 icmp_seq=1991 Destination Host Unreachable From 10.0.0.17 icmp_seq=1992 Destination Host Unreachable From 10.0.0.17 icmp_seq=1993 Destination Host Unreachable From 10.0.0.17 icmp_seq=1994 Destination Host Unreachable From 10.0.0.17 icmp_seq=1995 Destination Host Unreachable From 10.0.0.17 icmp_seq=1996 Destination Host Unreachable From 10.0.0.17 icmp_seq=1997 Destination Host Unreachable From 10.0.0.17 icmp_seq=1998 Destination Host Unreachable

From 10.0.0.17 icmp_seq=1999 Destination Host Unreachable

miojajuni@ubuntu: ~

h15 h3 h14 h1 h7 h2 h13 h12 h4 h8 h16 h10 h5

i@ubuntu:~\$ sudo ~/mininet/examples/miniedit.py

```
4 bytes from 10.0.0.17: icmp_seq=1687 ttl=64 time=3.86 ms olFrom 10.0.0.17 icmp_seq=1986 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=1987 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=1988 Destination Host Unreachable
                                                         ncFrom 10.0.0.17 icmp_seg=1989 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=1990 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=1991 Destination Host Unreachable
                                                           1From 10.0.0.17 icmp_seq=1992 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=1993 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2004 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2005 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2006 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2007 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2008 Destination Host Unreachable
                                                          etFrom 10.0.0.17 icmp_seq=2009 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2010 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2011 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2012 Destination Host Unreachable
                                                           FFrom 10.0.0.17 icmp_seq=2013 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2014 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2015 Destination Host Unreachable
                                                           From 10.0.0.17 icmp_seq=2016 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2017 Destination Host Unreachable
                                                            From 10.0.0.17 icmp_seq=2018 Destination Host Unreachable
```

Figure 12. Time delay for ping command from normal host users under attack.

After Nodejs execute detection and mitigation Javascript

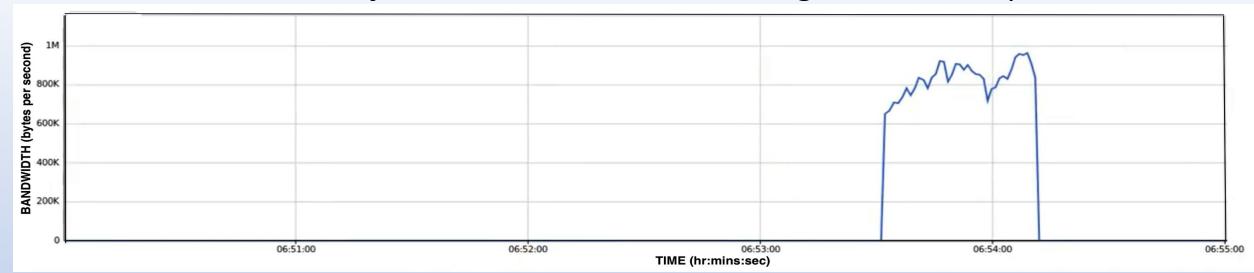


Figure 13. Network Bandwidth after Nodejs in SDN executes the detection and mitigation JavaScript.

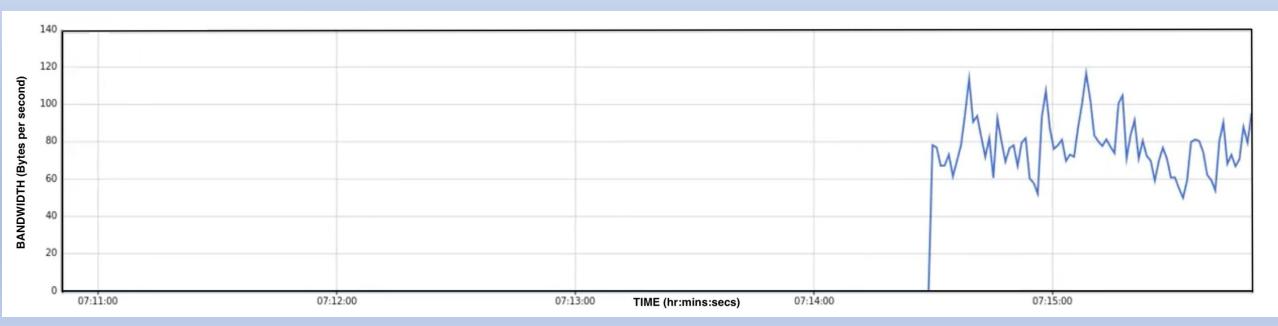


Figure 14. Network bandwidth Threshold

Limitation, Conclusion and Future work

Results show the efficacy of SDN in detecting and mitigating DDoS attack.

The limitation of the proposed framework are

- Detection of malicious traffic below the control bandwidth limit and the detection of the attacker.
- System considered only static threshold for bandwidth limit.

Future work will consider dynamic threshold for bandwidth limit.

Reference

- [1] Y. Lu and L. Da Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," IEEE Internet of Things Journal, pp. 1–1, 2018.
- [2] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
- [3] "Cisco Visual Networking Index: Forecast and Trends, 2017–2022," Cisco. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. [Accessed: 09-Feb-2019].
- [4] "Internet of Things at a glance Cisco," Cisco. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf. [Accessed: 08-Feb-2019].
- [5] M. Mukherjee et al., "Security and Privacy in Fog Computing: Challenges," IEEE Access, vol. 5, pp. 19293—19304, 2017.
- [6] R. K. L. Ko et al., "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in 2011 IEEE World Congress on Services, Washington, DC, USA, 2011, pp. 584–588.
- [7] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.
- [8] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things," IEEE Communications Magazine, vol. 56, no. 2, pp. 30–36, Feb. 2018.
- [9] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "IoDDoS The Internet of Distributed Denial of Sevice Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets:," in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 2017, pp. 47–58.

- [10] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602–622, 2016.
- [11] M. E. Ahmed and H. Kim, "DDoS Attack Mitigation in Internet of Things Using Software Defined Networking," in 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), Redwood City, CA, USA, 2017, pp. 271–276.
- [12] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425–441.
- [13] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 2015, pp. 77–81.
- [14] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," IEEE Access, vol. 6, pp. 24694–24705, 2018.
- [15] N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, "Research Trends in Security and DDoS in SDN," Security and Communication Networks, vol. 9, no. 18, pp. 6386–6411, 2016.
- [16] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425–441.
- [17] "sFlow-RT." sFlow-RT 2019, [Online]. Available: https://sflow-rt.com /. [Accessed: 14-Feb-2019].

QUESTIONS?

THANK YOU