IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 11, November 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011050|

Implementation of DDOS Detection System using Mininet and Pox Controller in Software Defined Network

Jagadish. S[1], M. N. Sreerangaraju[2]

P.G. Student, Dept of Electronics & Communication Engineering, Bangalore Institute of Technology, Bangalore, India[1]

Professor, Dept of Electronics & Communication Engineering, Bangalore Institute of Technology, Bangalore, India[2]

ABSTRACT: SDNs are different from typical networks in that they separate the data and control planes. In SDN architecture, the controller is a critical component. It's also vulnerable to a variety of security threats. The impact of a DDoS assault is one of these key challenges. The goal of this research is to use the POX to create an entropy-based detection method to DDoS assaults in Software network to improve security, and to evaluate the algorithm's performance with the POX in various topologies and controllers, the Entropy-based detection method was put to the test in a variety of scenarios, including connecting controller Different numbers of POX controllers were linked to a single topology with 64 hosts, and then to a linear topology with 64 hosts. The Entropy detection technique was discovered to perform better in lightly loaded networks, and the results show that increasing the number of controllers improves the outcomes can enhance the network's security. makes a novel addition to the implementation of a statistical detection to increase the security Software defined network, use several controller and topology.

KEYWORDS: SDN, OpenFlow, POX, Entropy, DDOS

I. INTRODUCTION

Software defined networking (SDN) is a network management strategy that enables dynamic, programmatically efficient network design to improve network performance and monitoring, making it more similar to cloud computing than traditional network management. The software defined network (SDN) was created to address the issue of previous networks de-centralised and complicated static architecture, today's networks, on the other hand, demand greater flexibility and troubleshooting simplicity. The primary difficulty with SDN is the disadvantages of intelligent centralization are numerous. in terms of security, scalability, and elasticity. OpenFlow is a technology that allows a server to direct packets to network switches. It regulates packet flow over the network by controlling the network switches and allowing an external entity, such as the controller, to manage it. Open flow was developed as a network analysis tool. OpenFlow is the protocol used to manage the switch. The user program that uses OpenFlow to communicate with the OpenFlow switch is called the controller.

DoS(Denial of Service), a malicious attempt to prevent genuine end users from accessing a targeted system is known as an attack, a website, application and mobile apps. When a huge amount of internet packets are sent to a victim's network, this is perpetuated from multiple infected systems (usually referred to as salves/zombies), consuming network bandwidth, performance of system, unavailable of service, in worst-case scenario, destroying the system. Legitimate users will find it difficult to use the targeted system as a result of these activities. DDoS assaults are one of the threats to the Internet's reliability, affecting services such as System and network performance, emails, and other system resources are all factors that must be considered while using online applications and procedures.

Mininet is a network emulator that gives us a virtual network comprising hosts, switches, controllers, and links. Hosts runs a standard network with Linux Ubuntu software, OpenFlow and Software-Defined Networking are supported by its switches, allowing for highly flexible custom routing.It can construct on any sort of technology, a realistic virtual network with a single command. As a result, it offers a low-cost solution as well as expedited development that is in sync with production networks.

A Python based Open Flow Controller. It is also called as Software defined Networking controller. It is used to build and prototype new network applications more quickly. The mininet virtual machine has a pre-installed POX controller. Openflow devices can be turned into hubs, switches, load balancers, and firewalls using this controller. This controller

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011050|

can run Open Flow experiments in a simple way. Different parameters are provided on experimental or actual topology, by allowing you, to perform with emulators.

II. RELATED WORK

This article discussed novel use cases with a large number of heterogeneous devices that are all linked to the same infrastructure. This growth also presents new security concerns, with a DDoS assault being for network service availability. This study proposes a unique method for circumventing the limitations of standard detection methods. Even if an attacker moves between various sites, a new sensor gives the necessary information to track them down. Almost every aspect of a 5G network, including the Edge, can benefit from the suggested strategy. It also mentioned DDoS attack detection and when the attacker is a UE travelling between locations, fine-grained mitigation is necessary.[1]

According to this study, the Fifth Generation (5G) wireless A wide range of cyber-threats, including sophisticated and complex attacks, will put the network at risk. To protect wireless networks from sophisticated and hazardous network assaults, such as DDoS and jamming. To detect network assaults, this study proposes and develops a Based on a hierarchical Reinforcement Learning (RL) method, a new cooperative attack detection system has been developed. Cooperative detection is carried out via distributed detection systems that are installed at several important access points, base stations, and servers are all 5G network organs.[2]

In this, a unified approach to early detection of DDoS is presented and assaults organised a botnet that is in charge of malicious devices, based on deep Convolutional Neural Networks (CNNs) and actual network. With the introduction of 5G, vertical industry and critical infrastructure cyber-physical systems (CPSs) will be more reliant on network than before. As a result, protecting network from cyber-attacks is important not just for the network's core customers, but also to avoid it being used as a proxy to target CPSs. Individually, these puppet devices execute quiet call, signalling, SMS, Internet to produce a cell-wide DDoS attack that could stymie CPS operations. The results, the framework recognizes a normal and under-attack cells with an accuracy of more than 91 percent.[3]

Due to the possibility of assaults from internal and external source, an intrusion detection system is an essential tool of any internet connected system. These types of security systems are used to detect network-based attacks like floods, malware, twin evil invaders and DoS. They used a dense neural network with deep auto-encoding technique in this article to identify intrusion or assaults in networks. They tested the method using the Aegean Wi-Fi Intrusion dataset as a benchmark. For Flooding, Impersonation, and Injection assaults, the findings demonstrated exceptional with an overall detection accuracy of 99.9%, the performance is outstanding. This included a comparison with current techniques in the literature, which revealed that the suggested algorithm provided a significant increase in terms of detection accuracy and speed.[4]

Using deep learning techniques, this article offers a 5G architecture for doing network flow analysis to identify cyber threats in mobile networks cheaply and fast. Experiments on the proposed system with inspection capabilities are also provided, in order to examine and identify how many network flows are gathered from the User Equipments of 5G subscribers. These findings may provide insight into when and why 5G protection systems will stop detecting cyber-attacks due to overload. In recent years, cyber security defence systems have advanced with novel methodologies and new Intrusion Detection capable of detecting cyber-threats that had previously gone undiscovered. The impending fifth generation (5G) mobile technology, with its new and enhanced features, poses significant security challenges. If current detection procedures are not updated to accommodate 5G, they will become obsolete.[5]

The paper starts with some of the more recent emerging technologies, such as SDN and NFV, and then digs into artificial neural networks in depth. As a result, the algorithms are safe to use, and system maintenance and updates provide a genuine career opportunity. We look at how smart networks can be leveraged to enable a built-in common sense AI, with a particular focus on scalability, performance, reliability, security, and resiliency. [6]

III. METHODOLOGY

During a normal traffic between clients in a SDN network, the first packet transmitted from one client to another. Initially, the switch will not have any entry in its flow table as to where it should forward the incoming packet. The default route will be forwarding the packet to the controller. The controller will dictate the switch to forward the packet to respective destination port. The controller will also provide an entry rule in the flow table in the switch for that particular source and destination. In the future, the packet with the same source and destination will be automatically forwarded without the intervention of the controller

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011050|

1)Creation of Network: Mininet is a software emulator for prototyping a large network on a single machine. Mininet can be used to quickly create a realistic virtual network running actual kernel, switch and software application code on a personal computer.

2) Monitoring Network:POX SDN controller is used to monitor the network traffic and it's entropy.It is present as part of Mininet. POX provides a framework for communicating with SDN (Software defined networks) switches using either the OpenFlow or OVSDB protocol. The detection program will run on POX as stand-alone modules. Multiple modules will be used to allow the controller to perform different functionalities such as installing flows, forwarding packets, and validating the DDoS attacks.

3) L3 Learning Module: This module, L3 learning, is the most important module in the POX controller. It is a simple layer 3 learning module that provides connectivity between the nodes in the network. L3 learning module handles the incoming packet and maintains a list of bindings between the OVS ports and the MAC addresses of the connected clients. It utilizes this information to install the rule that replaces a destination MAC while forwarding a packet to the destination port. If no binding is found, the module instantiates ARP requests. Along with the connectivity, it is integrated with the detection algorithm to detect a malicious traffic flow.

In DDoS, if the source addresses of incoming are spoofed, then the switch would not find a match and the packet needs to be forwarded to the controller. The collection of DDoS spoofed packets and legitimate packets can bind the controller into continuous processing, which exhausts them. Due to this, the controller is unreachable for the new incoming legitimate packets. This will bring the controller down causing loss to the SDN architecture. For a backup controller, the same challenge is to be faced.

Such kind of attacks can be detected in the early stage by monitoring few hundred of packets considering changes in entropy. The early detection of DDoS attacks stops the controller from going down. The term 'early' is related to tolerance level and traffic being handled by the controller. Due to this, the impact of malicious packets flooding can be controlled. Such a mechanism needs to be lightweight and high response time. The high response time saves the controller during the attack period for regaining the control by terminating the DDoS attack.

DDoS Detection Algorithm using Entropy

1. Function ENTROPY
2. Collect flow from switch and store in a file.
3.Calculate total number of packets for every destination IP in current interval.
4. Declare global variables
5. End Function
6. Function COLLECT_STATISTICS
7. Calculate the probability using, Pi = Xi/$\sum_{i=0}^{N}$ Xi where, Pi =Probability of i th destination ip, Xi =Packet count on ith destination ip, N =Total number of destination IP
8. Calculate entropy of network using, H(Sj) = $\sum_{i=1}^{n}$−Pi logPi where, H(Sj) is the Entropy of jth switch
9. Calculate the difference between above calculated & normal entropy value
10. End Function
11. Function ENTROPY_DETECTION
12. Compare the above calculated diff with predefined threshold value.
13. if diff > threshold then
14. Increment DDoS detected count
15. if DDoS detected count > min DDoS detected in particular window then
16. Generate alert of DDoS attack
17. else
18. Increment program counter.
19. end if
20. end function

IV. EXPERIMENTAL RESULTS

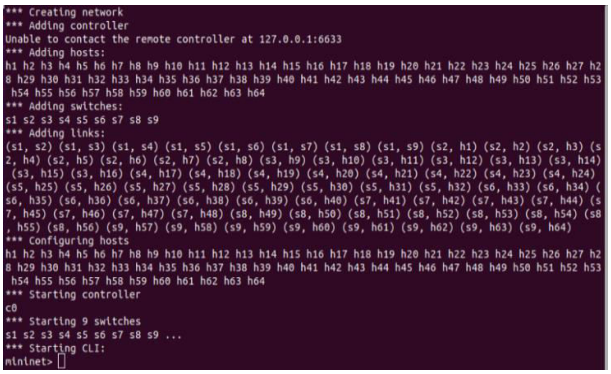
Mininet is used to emulate the network with POX as the controller platform. The detection program will be a standalone module integrated within the L3 Learning module. This will allow the controller to perform additional

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

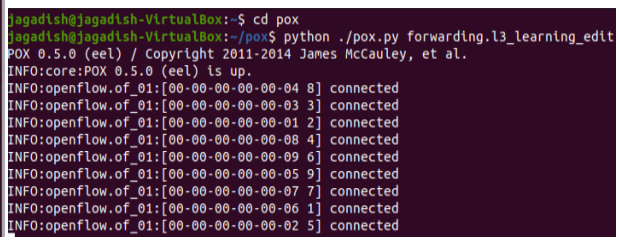
|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011050|

functionalities such as installing flows and validating DDoS attacks. In this testbed, OF-switch is used to simulate the behavior of an edge switch in a SDN network. The Mininet network comprises a victim node that is the destination for both normal traffic and attack traffic generated from a client within the SDN network. By using Mininet, we can attack a virtual host and analyze the results of our detection algorithm. The client's IP addresses are assigned incrementally from 10.0.0.1.

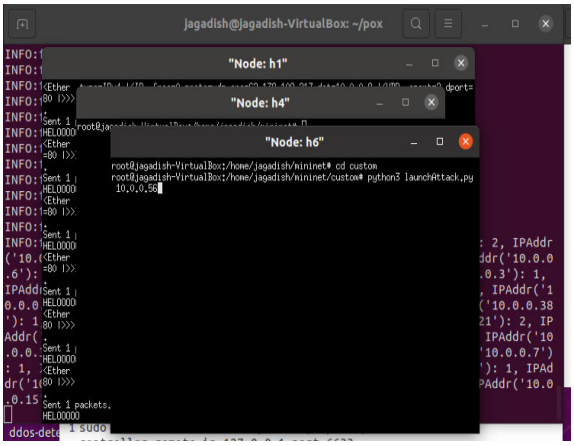


(a)

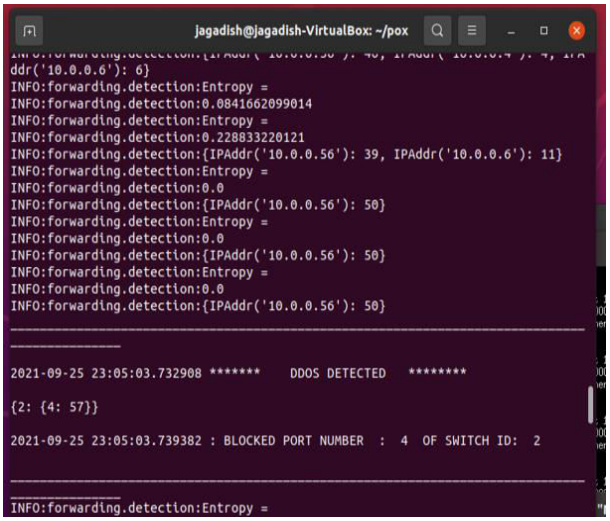


(b)

(c)



(d)



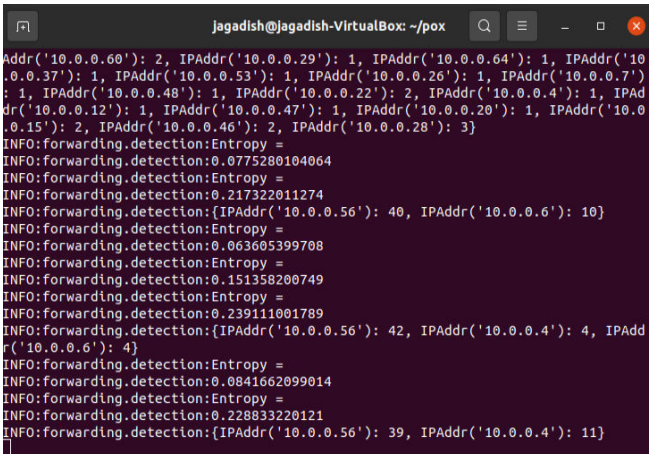
(e)

(f)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011050|



(g)

Fig. 4. (a)Hosts and Switches connected with links (b) All switches will be connected to Pox controller (c) Entropy values before attack (d) Host H6 launch attack (e) An example of DDoS dectected in 10.0.0.56 from Host H4 (f) Entropy value after attack (g) Entropy value and DDoS attack on H56 from Host H6 and H4.

Mininet is the network Emulator which is used and by starting the controller the network creates with 64 number of Hosts and 9 number of Switches (a). The POX controller which is used is shown, to monitor traffic and entropy. This is a framework for using the OpenFlow protocol to communicate with SDN switches. It can be programmed using Python language (b). This fig shows the entropy value before the DDoS attack, its nothing but Traffic (c) Launching the attack in Host H6 window, open the H6 window from mininet with xterm H6 command, go to mininet path and launch attack file. As the destination IP is specified, it will send 50 packets to Host 56 from source IP Host H6 (d) As, launch Attack is executed in Host H4, then it calculates the entropy by counting for 5 times and if threshold is less than the specified value, it shows DDOS DETECTED, also it blocks the host H4, and switch ID 2 (e).

The Entropy values are observed in POX Controller. The Entropy value decreases below the threshold value which is equal to 0.5 for normal traffic and hence we can detect the attack within the 250 packets of malicious type of traffic attacking a host in the SDN network.If the hosts stop sending attack packets, the switches are started again by the POX controller after shutting it down during the attack.

V. CONCLUSION

The purpose is to identify DDoS assaults and safeguard the SDN operating system (i.e. the controller). The key to recognizing detecting an assault might be construed flexibly, we set a minimum of 250 packets and a maximum of 500 packets for early detection. This method not only detects threats well, but it also adds little code to the controller program and both in attack or in normal circumstances, the CPU burden is not increased. There are various attack detection systems, each of which is used in a different way. We concentrated this research performs. The fact that the SDN specification needs new packets to be delivered to the controller was used to our advantage. While introducing entropy statistics collection, Finally, we designed a means to immediately identify any threat. Although In non-SDN networks, entropy is utilized in DDOS detection, we are aware of no such solution in SDN, and this is the first of its kind in SDN.Detection approach was able to accurately detect entropy reductions even though attack packets made up only controller receives 25% of all incoming traffic. When the number of packets are 50% of the traffic arriving at controller, our method correctly recognised the subnet attack. This method has a 96 percent success probability when using a 25% rate attack packets per total traffic threshold. When 75 percent to 100 percent of traffic is DDoS, in non-SDN networks, the nearest method can identify an attack. We believe that this is a viable solution for detecting DDoS in SDN with precision and efficiency.The issue of Software defined network is new, and this is due to the fact that this structure has yet to be deployed as a real network.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011050|

REFERENCES

[1] Ana Serrano Mamolar, Zeeshan Pervez, Univ. of the West of Scotland, "Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks", 2019 IEEE.
[2] HichemSedjelmaci, " Attacks Detection Approach Based on a Reinforcement Learning Process to Secure 5G Wireless Network" 2020 IEEE
[3] Bilal Hussain, Qinghe Du," Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System over 5G network", 2020 IEEE.
[4] ShahadateRezvy, Yuan Luo, Miltos Petridis, AboubakerLasebae," An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks", 7281-1151, 2019 IEEE.
[5] Lorenzo Fernandez Maim, Felix J. Garcıa Clemente, "On the Performance of a Deep Learning-Based Anomaly Detection System for 5G Networks", 2017 IEEE.
[6] Mr.Siddhant Shah," An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era", 2019 IEEE.
[7] Rabia Khan, Pardeep Kumar," A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions", 1553-877X, 2019 IEEE.
[8] YounessArjoune," Smart Jamming Attacks in 5G New Radio: A Review",2020 IEEE.
[9] Reeta Devi, Rakesh Kumar Jha," Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network", 1434-8411, 2017 IJEC
[10] R. Vedhapriyavadhana, E.FrancyIrudaya Rani, Francis Xavier Engineering College, "Simulation and performance analysis of Security issue Using Floodlight controller in Software Defined Network, 2018 IEEE.
[11] Mousavi, S. M., & St-Hilaire, M. (2015, February). Early detection of DDoS attacks against SDN controllers. In 2015 International Conference on Computing, Networking and Communications (ICNC) (pp. 77-81). IEEE.
[12] Miladinovic, I., &Schefer-Wenzl, S. (2018, February). NFV enabled IoT architecture for an operating room environment. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 98-102). IEEE.
[13] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463.
[14] Skowyra, R., Bahargam, S., &Bestavros, A. (2013, September). Software-defined ids for securing embedded mobile devices. In 2013 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1-7). IEEE.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details