International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Methodology to Alleviation of Security Attack in Software Defined Network

R Vijayan, V Mareeswari, S Prasanna, C Navaneethan, S Meenatchi, Amit Gupta

Abstract*: Computer Network is a collaboration platform for digital gadgets. Virtualization is abstracting layers from underlying Architecture. Virtualization platform provides flexibility, green resource usage and fast deployment of the carrier. Integration of Computer Network and Virtualization Platform Create Network Virtualization Platform. Software-Defined Network (SDN) Provide dynamic and scalable networking offerings to Business Environments Cloud Network and Data Centers. SDN is controlling network infrastructure with the control plane. Security is a challenging problem for the network. SDN comes with Network Programmability and automation. SDN has an advantage, but it contains a new safety issue. SDN is focused on network safety data plane and control. Security Challenges in SDN is Control Plane, Data Plane Attacks. In Controller Layer Attacker at controller Layer, an routing, visitors filtering denying, or allowing unnecessary site visitors. Control plane assault used to drop or lack of manage over traffic policy and Quality of carrier control. Data Plane Attack Attacker can create DOS Denial of Service.

***Keywords*: Denial of services, Internet Protocol, Medium Access Control, Local area network, Software-defined network**

I. INTRODUCTION

Data Center focuses have gotten critical consideration as a necessary foundation for its capacity to store an expansive measure of information and facilitating extensive scale benefit applications. Today substantial organizations utilize server farms for their expansive scale calculations and IT organizations. Server virtualization and distributed computing are changing the method for utilizing server farms. Virtualization permits the more productive use of IT Virtualization and Cloud figuring because most current system advances were not created to consider Virtualization and Cloud processing. Static typologies require manual mediation to convey and move virtual machines (VMs) that can make the systems to end up plainly a bottleneck later on IT advancement.

A Software Defined Network (SDN) is another systems administration worldview that brings a lot of new capacities and permits taking care of numerous difficult issues of legacy systems. This approach depends on isolating the system insight out of the bundle-exchanging gadget and placing it into a coherently unified controller. The controller is in charge of the sending choices that are set into the switches by means of standard conventions, as OpenFlow. The inspiration of SDN is to play out a system working framework, where arrange errands should be possible without including extra programming for each of the exchanging components and take into account creating applications that control the switches by working it on uppermost of a system working framework. SDN convention is acquainted with bind together the interface between the exchanging equipment and the remote controller in SDN worldview. This convention gives the controller a plausibility to find the OpenFlow- agreeable switches characterizes sending rules for the exchanging equipment and gathers insights from the exchanging gadgets. At present, there exist various controllers, where the most known controllers are OpenFlow.

Control planes cause rough routing or traffic filtering denying or permitting unnecessary traffic. Control plane, Application Layer, Data plan a traffic management and data transferring in the connected system. All connected system and switch controller in the data layer. SDN network provides service to business-critical High Availability Services. SDN layer manages QoS and Service Level Agreement, throughput, packet delivery and drop ratio in SDN API. Software Defined Networking (SDN) is another systems network administration approach that is acquainted with the objective of improving the system administration by isolating the information and control planes. in SDN the system control plane is a move of the controlling rationale from systems administration gadgets, for example, switches and switches, in customary systems to an incorporated unit known as the controller allows the physical system equipment to be withdrawn from the Control Plane. This partition disentangles the outline of new conventions and execution of new system administrations, for example, get to control, QoS, implementation of new arrangements, data transfer capacity administration, movement designing and so forth. No longer does each little change need to come at the cost of configuring and reconfiguring all the system gadgets.

Manuscript published on 30 September 2019
* Correspondence Author
R Vijayan*, Associate Professor, School of Information Technology and Engineering, VIT-Vellore Institute of Technology, Vellore, India.
V Mareeswari, Assistant Professor (Senior), School of Information Technology and Engineering (SITE), Vellore Institute of Technology (VIT), Vellore, India.
S Prasanna, Associate Professor, School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India.
C Navaneethan, Associate Professor, School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India.
S. Meenatchi, Assistant Professor (SG), School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India.
Amit Gupta, School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India.

Security is the most factor in networking. In-network data transmission to one to another system. It requires that network be protected and attack is not degreed network performance.

II. RELATED WORKS

OpenFlow is included into the network shape to govern the network flows and diverts the site visitors via a direction that it's far inspected by way of the preinstalled protection gadgets (Network intrusion detection device (NIDS), firewall, etc.). Employing the SDN infrastructure will simplify the community operator's task in a huge cloud infrastructure. The changes in the glide directions and community guidelines can without difficulty be performed by way of running easy scripts on the controller to be able to install new drift entries on the switches. [1].

Comparable technique Snort, an Intrusion Detection Systems (IDS), is used to screen community site visitors and measures to pick out mischievous sports in the community. Intrusion Prevention System (IPS) is an IDS that has the power to and OpenFlow modules. In this method, the cloud networking environment is dynamically reconfigured utilizing the electricity of OpenFlow switches in actual time to dynamically detect and prevent the assaults[2].]isplay the need of constructing protected and honest SDNs in the layout segment. Bringing replication, variety and dynamic switch affiliation to SDN manipulate platform design are the main arguments described as mitigation techniques for several danger vectors that enable them to make the most of SDN vulnerabilities. In the proposed instance by means of enforcing some of the replicated controller's competencies. Meanwhile, the switches need to have the potential to dynamically partner to the controllers. [3]

A DDoS detection technique built into the NOX controller-based totally on Self-Organizing Maps (SOM). SOM is an unsupervised synthetic neural community trained with the functions of the network go with the flow that is periodically accumulated from the switches. The traffic is assessed as either regular or ordinary based on the SOM sample. This detection method as shown in parent 10 runs in 3 modules jogging periodically inside a loop inside the NOX controller [4]. New era database that does the truly difficult work of OpenFlow information preparing for DDoS assault location. OpenFlow or "inspected stream", is an industry-standard for bundle trade at Layer 2 of the OSI show. To keep the authentic movement running and give source-and-goal based sifting OpenFlow. To do DDoS alleviation along these lines requires heaps of arrangement and a solid comprehension of the system streams. [5]

OpenFlow DDoS Shield that screens streams on an open stream switch. On the off chance, that the number of parcels got in 5 seconds surpasses 3000 then the number of bundles will be considered in every second length. On the off chance that the number parcels every second surpass 800 for 5 persistent circumstances then an assault is identified and the DDoS safeguard will begin dropping the approaching bundles until the stream passage times out [6]. The stream measurements sent from the open stream change to the controller to locate the extensive spikes in a movement that could be indications of an assault. The OpenFlow controller technique streams are introduced on the changes to drop the movement from the speculated sources. The proposed location strategies incorporate utilizing bundle symmetry and brief hindering of the movement. In routine activity express, asymmetrical conduct exists between the two sides of a correspondence. In the learning stage, the symmetry proportion is investigated in the system. [7]

The edge for a consistent number of times, an assault will be accounted for. There are various confinements to this strategy. At the point when the number of hosts under assault inside the system rise or when the whole system is under assault the entropy discovery will fall flat. , the backup controller will take over if one controller malfunctions. The controllers ought to be designed with interoperation Then the heap of the movement increments in the system with true blue activity in the pinnacle times utilizing the proposed entropy location instrument alone will bring about false-positive assault recognitions[8]. SDN Security and Research on SDN Architecture and Security Exterminating Network Prominence in Software-Defined Networks. Challenges and Effects Comparison of Software Defined Network SDN Security Attacks in SDN Implementation Strategies [9].RSSI Constructed Method Radio set signal power value is used to discover Sybil node in network Radio set Resource Testing Radio channel allocation Assign every node a specific radio channel to conversation with neighbor node Random Key pre-distribution Random key assigned to node for verbal exchange in every pair Cryptography options Public key infrastructure is used encryption or decryption of information with use of public and private keys [10].

Code Attestation an undisclosed hash rate is accompanying by means of the node and used as interchange rate among nodes for communiqué Secure AODV approach Uses Hop count and neighbor id base Detection. The influence of the Sybil Attack and Security issue in Software Defined Network security in mobile SDN is a major issue. Software Defined Network efficiency and protection are compromised to create instability, disrupt network performance lowering fault tolerance, functionality and assault on confidentiality, integrity and on hand of records in the network.[11].

[12]Authors discussed a Policy-based approach to control and defend the SDN domain behaviour. They have developed a Policy-based Security application for ONOS SDN controller by presenting a high-level overview of the application that helps to mitigate some of the real-time attacks towards the SDN domain.

[13]Authors propose a mitigation mechanism to limit the attack rate using the token bucket model. With the control of token add rate and bucket capacity, it avoids the table overflow on the victim switch.SDN intention revolutionizes networks with the aid of decoupling the Data or Control Planes then consequently providing a lot greater agility, flexibility, or end-to-end control; then it is such as is wanted lately by using Cloud Computing. SDN advantages intention enable each Enterprises then Cloud service carriers in accordance with enhance their functions and their user's experience. Security features the use of Software-Defined Networking (SDN) specifies necessities because of certain a framework for security purposes primarily based on network virtualization. Centralized firewall provision and DDoS-attack. Permanency. [14].

III. PROPOSED MITIGATION OF SECURITY ATTACK IN SOFTWARE DEFINED NETWORK

The SDN structure is extraordinarily bendy; it can perform with extraordinary kinds of switches and at unique protocol layers. SDN controlled switches may be applied for Ethernet switches Internet routers, transport switching, or application layer switching and routing. SDN is predicated on the commonplace features discovered on networking gadgets, which contain forwarding packets based on a few forms of float definition.

In Controller Layer Attack the attacker at the control plane cause rough routing, traffic filtering denying, or permitting unnecessary traffic. Control plane attack used to drop or loss of control over traffic policy and Quality of service management. In Data Plane Attack the attacker can create DOS Denial of Service attack from inside or outside devices and overflow the data plane capacity. an attacker can spoof new flow in a network resource exhaustion Attacker continuous attack packet in the target, Attacker will be single or many.

SDN network provides service to business-critical High Availability Services. Attacking on SDN layer attacker can reduce the QoS and Service Level Agreement breach which cause loss of reputation and money for an organization using a backdoor is SDN API. The attacker is middle of client and server connection this gathers information on both client and server-side and saves data packet for analysis. The attacker is middle of client and server connection this gathers information on both client and server-side and saves data packet for analysis.

In this proposed approach as in Fig. 1 prevention of attack in OpenFlow controller done by the development of SDN topology and analysis of security vulnerability in a network system, development of Secure Controller to prevent SDN system from the DDoS attacker and implement an efficient method to find a vulnerability in SDN Network.

In this proposed approach prevention of attack in OpenFlow controller done by the development of SDN topology and analysis of security vulnerability in a network system, development of Secure Controller to prevent SDN system from the DDoS attacker and implement an efficient method to find the vulnerability in SDN Network.

The single controller component subsumed through the controller switches practically control float tables whose sections can be populous best by means of the controller. Correspondence between the controller and the switches make utilization of an institutionalized convention and API. Most, as a rule, this interface is the OpenFlow particular, said in the long run new applications to arrange group site guests skim to meet particular association prerequisites for execution or security.

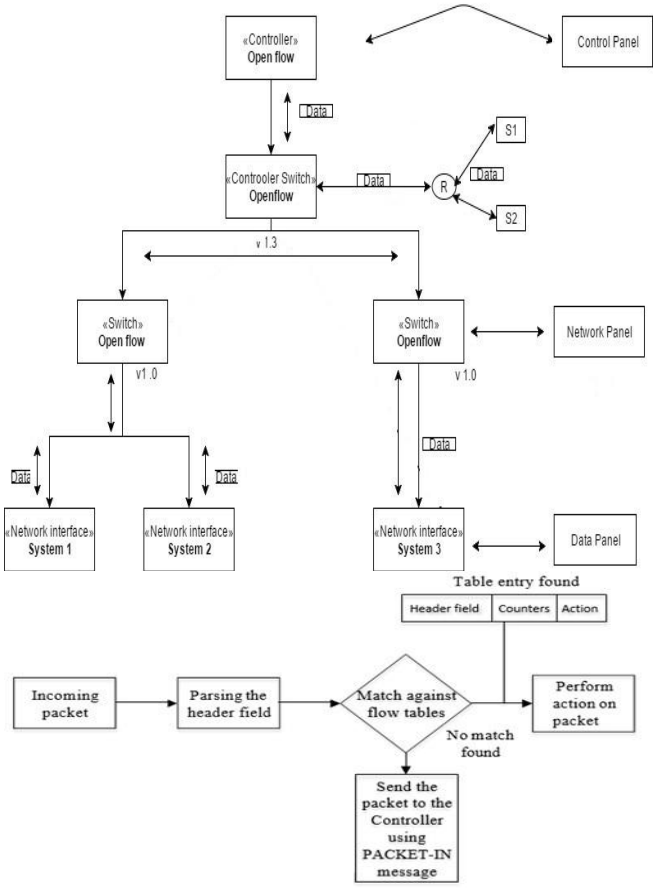

Fig. 1.Proposed Desing of SDN

A. Control Plane

SDN Applications are initiatives so expressly, specifically, or routinely carry their regulation stipulations or desired provision lead according to the SDN Controller thru NBIs. Moreover, those may deplete an anxious point of view over the system because of their internal primary leading purposes. An SDN Application involves some SDN Application Logic then at least some NBI Drivers. SDN Applications may additionally themselves find some other layer concerning anxious system control, within that pathway providing at least some large quantity NBI(s) thru odd NBI operator.

B. Network Plane

SDN Controller is a sensibly gray element responsible because of interpreting the necessities beyond the SDN Application layer beneath in accordance with the SDN Datapath providing the SDN Applications along with a conceptual point of view of the provision (which may also contain insights yet occasions). An SDN Controller consists of at least some NBI Agents, the SDN Control Logic, then the CDPI driver. Definition as like an intelligently unified article neither recommends nor blocks execution factors over interest, because of example, the agreement about a number of controllers, the revolutionary affiliation about controllers, conformation interfaces into controllers, nor virtualization or slicing on system assets.

C. Data Plane

The SDN Data plan is a coherent system gadget, which empowers deceivability and uncontended availability of the whole system and deals with all data transmission.

D. Entire Process flow chart for SDN communication

An SDN based system management server that connected to a database system. Plugin-container is connected to another system. A DHCP agent is connected to a message queue and provides IP allocation in the system. SDN services manage the entire network and transmission of data. In a huge undertaking system, the sending of a solitary controller to deal with all system gadgets would demonstrate cumbersome or undesirable. SDN space might be committed to an arrangement of clients who execute their own particular profoundly tweaked protection strategies, requiring that some systems administration data in this area (for instance, organize topology) not be unveiled to an outside element. A bearer's system may comprise parts of the conventional and more current foundation. Separating the system into different, separately sensible SDN spaces takes into consideration adaptable incremental organization. At the point when the parcel sent to a port utilizing the yield activity, Gathering Process parcel through indicated gathering. The new packet arrived in OpenFlow switch with IP and mac information. Switch send information to the controller and the controller is managing table for routing. Protocol agent UDP and TCP are supported in this process as shown in Fig 2.

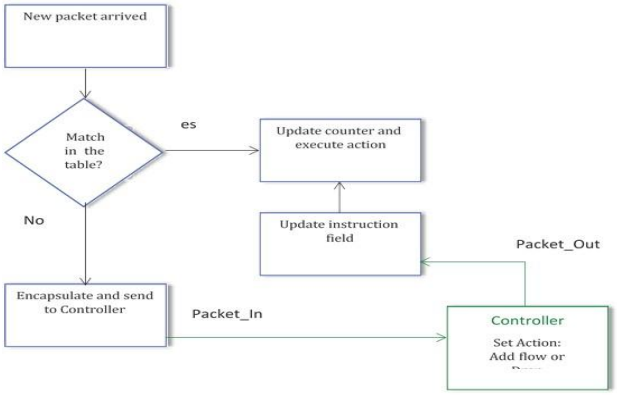

Fig. 2.Flow Chart for Entire Process

IV. DETECTION AND MITIGATION

A. Methodology for DDoS Attack

This detection algorithm is designed founded on three essential standards including Entropy version of vacation spot IP deal with, glide Initiation price and learn of flow Specification. The proposed detection algorithm may also be damaged in seven phases**.** Packet Delivery Ratio Calculation and Comparison. Packet Drop Ratio Calculation and Comparison. Discovering the attacker, if an attack is suspected identify this IP and MAC address. Add information to the OpenFlow controller switches in the attack route for flow records and finding out the blocking action. Updating routing path and table.

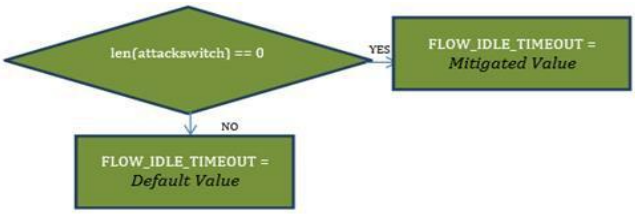

Fig. 3.Implementing attack mitigation in the controller

B. Methodology for OpenFlow Controller

The method of OpenFlow Controller, the subsequent parameters have been considered for the trying out of both latency and the throughput. The controller is programmed in python or routing programming language to prevent the attack. Controller Programming to prevent or mitigate SDN network to-dos and DDoS attack.

Table- I: Lists added to the controller

```
# Statistics Lists
count = 0     #Counting thenumberofincomingpackets entDic =
{}            #Hash table for the IP address and its occurrence
ipList = []   #List of IP addresses
dstEnt = []   #Listofentropies
```

C. Implementation setup

The simulation and checking out of the proposed technique for DDoS detection defined thru the subsequent sections. The algorithm is implemented at the python-based OpenFlow controller in the Estimate virtualized network environment. Bonesi scripts are used to generate do Dos traffics at the network hosts during the simulation. The test condition was done on OpenFlow controller programming. Using VMware workstation virtual machine Estinet tool NAT Ethernet interface speed confinements, both of the controllers and on a similar host (Intel Core i5-5200U 1.6 to 2.6 GHz CPU with 2 core and 4 logical, 16GB DDR3 ram)running (64-bit system and Installed VMware, Wireshark). Estinet is a tool used to simulate the software program defined Networks, allowing a simple and brief technique to create, engage and customize prototypes for software program described Networks. Estinet lets in community topologies to be distinctive parametrically. It also permits configuration of a number of overall performance parameters for every virtual hyperlink. This is important for simulating real-world systems and a requirement to put in force maximum assault eventualities simulated on this thesis. In Estinet IP, the address is started 10.10.10.10 so all attached component starting IP is 10.10.10.100 – 10.10.10.255.

In this method, a controller programmed to detect malicious node and record system IP and MAC that used to communicate to another system. Controller blocked IP and MAC address in the entire network. Attacker data packet is denied in the entire network. the component is finding a malicious node with id, the controller is blocked this malicious node.

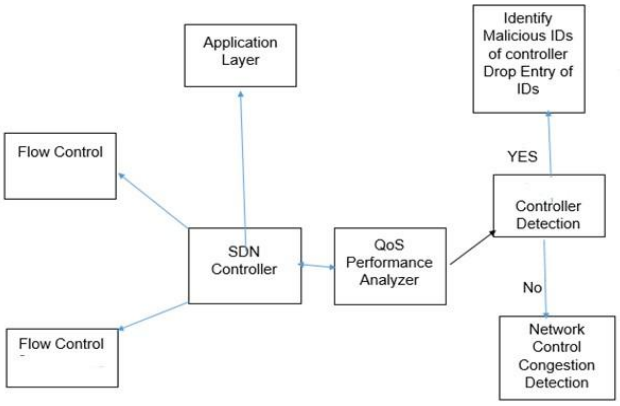

Fig. 4.Flow Diagram for Design and Implementing

Techniques for Identify and Prevent from Attacks are OpenFlow Controller to Detect Malicious Node, QoS Performance Analyzer to Check Performance, Data Packet Delivery Ratio and Data Packet Drop Ratio as shown in Fig 5 to 8.

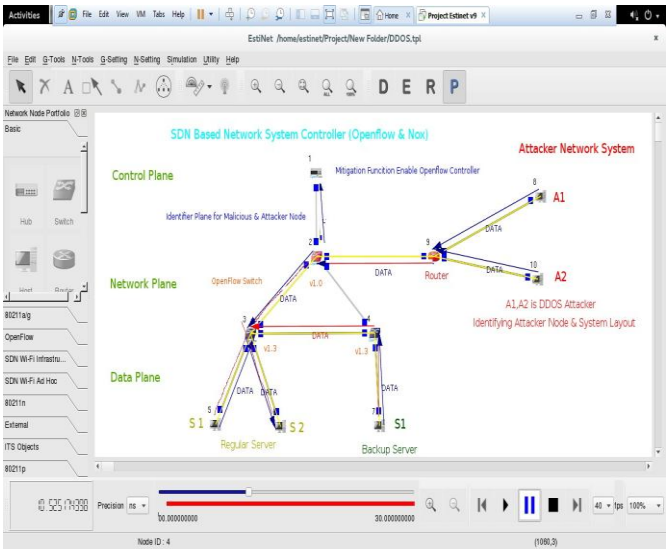

Fig. 5.SDN based topology when dos attack happen

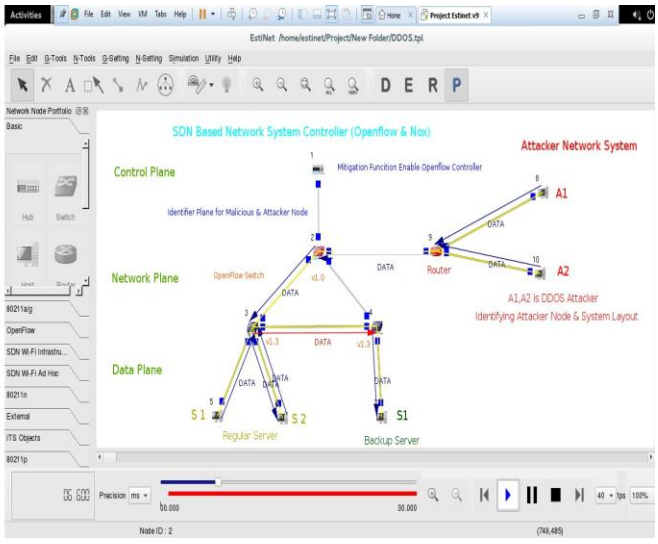

Fig. 6.SDN Topology with all component is working

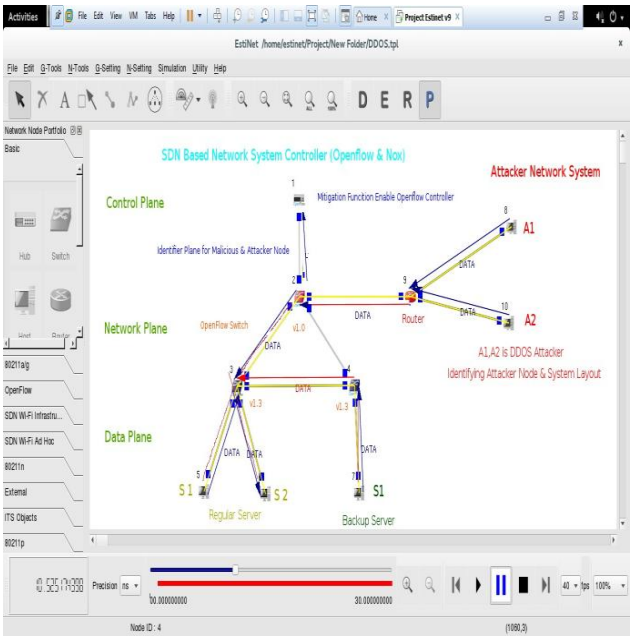

Fig. 7.SDN based topology when dos attack happen

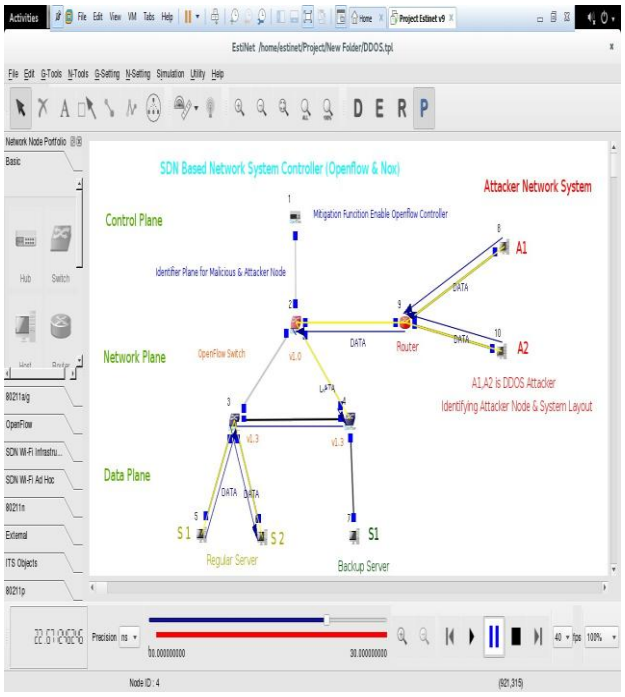

Fig. 8.SDN based topology mitigate dos attack

V. RESULT AND DISCUSSION

Examine attack, defense and monitoring mechanisms in the SDN environment and the opportunity of deployment of techniques current in current networks. Current studies on SDN protection is in its preliminary section. However, monitoring is in recent times mostly completed at the host or community stage in attacked networks that are nearly impartial on community structure.

There are many variants of DDoS assaults as properly as protection mechanisms against them for modern networks. Consider that the one's strategies. For the detection of DDoS, assaults are very frequently used waft-based traffic monitoring strategies. Due to the flow-based, totally nature of SDN, it is feasible tomake detections in each plane. However, detection mechanisms deployed in the controller without the right aggregation of community site visitors may want to overload the communication amongst manage and facts plane. In addition, the floating table in a network tool has boundaries. Proposed that some of those troubles will be resolved by means of including a few minimal intelligence to the records plane gadgets.

Parameters for Analysis are taken into consideration to generate results and analyze are Throughput is the system utilizes bandwidth in given time, Data Packet Delivery Ratio is Data packet delivery to the system without any loss, Data packet Drop Ratio is Data packet drop by the system in data transmission and quality of Service Delivery is Availability of system and system response. The result and analysis using Wireshark protocol analyzer and Estinet connected component generate a log file for analysis. This result is designed using both Combination of Wireshark and log file.

A. Before Attack

The system is working, no issue detected.

Table II: Throughput system vs. bandwidth. (Before Attack)

Sys ID	1	2	3	4	5	6	7
Bandwidth	1	2	4	6	8	10	12

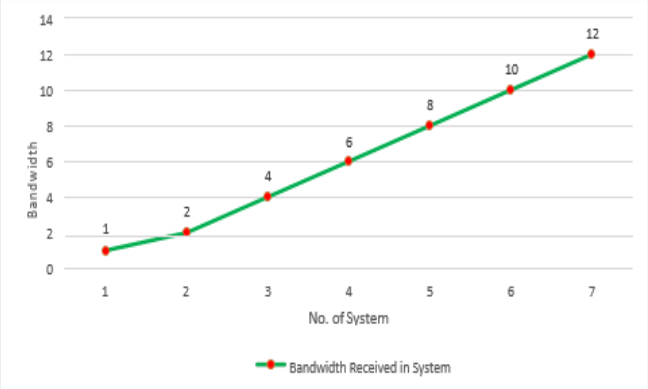

Fig. 9. Throughput system vs. bandwidth. (Before Attack)

The Total LAN bandwidth in Topology is 16 Mbps. Max bandwidth used by the backup server is 12 Mbps as shown in Fig 19.

Table III: Value of System ID and Data Packet Delivery. (Before Attack)

Sys ID	1	2	3	4	5	6	7
DPD	20	40	60	70	80	100	140

The Total Data packet Transmit in topology is 160. Different packet for Different Nodes Max Data Packet Received is 140 as shown above in Fig. 10.

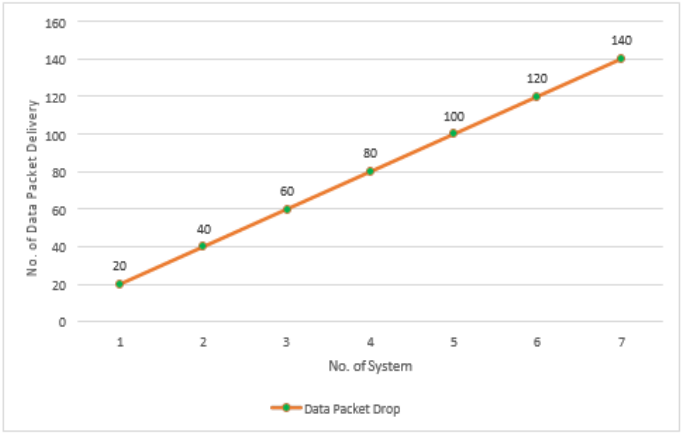

Fig.10: No. of Data packet received vs. System. (Before Attack)

B. After Attack

Table IV: Value of System ID and Bandwidth. (After Attack)

Sys ID	1	2	3	4	5	6	7
Bandwidth	1	2	2	3	3	4	4

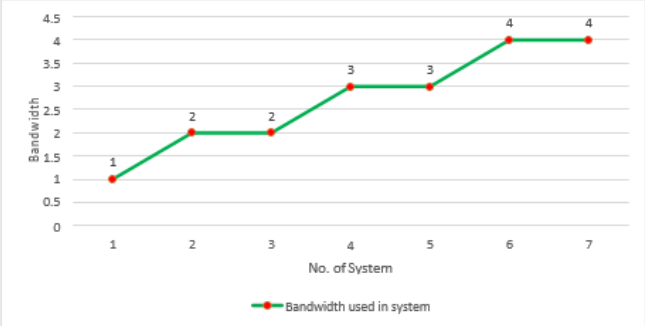

Fig.. 11. Throughput system vs. bandwidth. (After Attack)

The DoS and DDoS attack in the network the bandwidth utilized is less and remaining bandwidth is waste Utilize bandwidth max 4Mbps as in Fig.11

Table V: Value of System ID and Data Packet Delivery. (Before Attack)

Sys ID	1	2	3	4	5	6	7
DPD	10	10	10	20	20	20	20

Fig. 12. No. of Data packet received vs. System. (After Attack)

DoS and DDoS attack in the network Data packet delivery ratio is very less remaining Data packet is dropped and received data packet also not useful as shown in Fig.12.

C. After using Mitigation Method

Table-VI: Value of System ID and Bandwidth. (Before Attack)

Sys ID	1	2	3	4	5	6	7
PDR	0.5	1	2	3	4	5	6

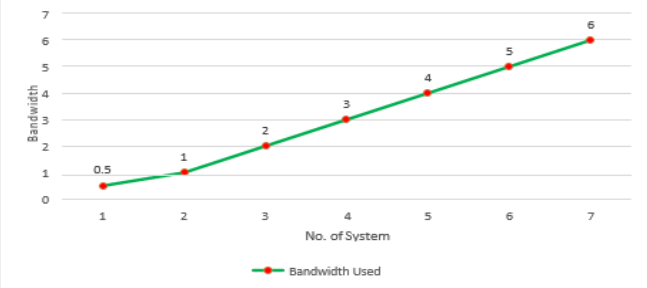

Fig. 13. Throughput system vs. bandwidth. (Before Attack)

After applying the mitigation method, half of the bandwidth is used and half of the bandwidth is waste as shown in Fig 13.

Table VII: Value of System ID and Data Packet Delivery. (Before Attack)

Sys ID	1	2	3	4	5	6	7
PDR	10	20	30	40	50	60	70

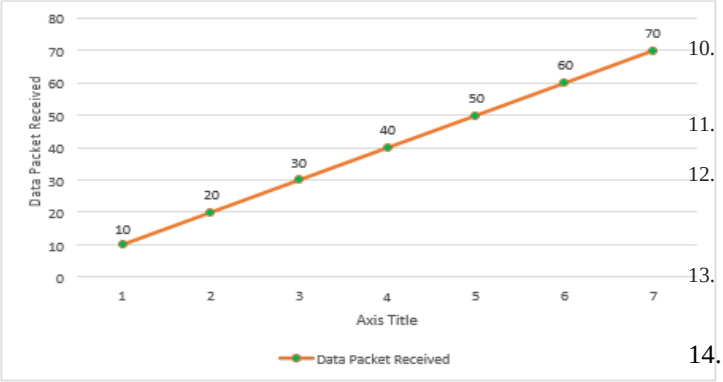

Fig. 14. No. of Data packet received vs. System. (After Mitigation)

After applying the mitigation method Data packet delivery ratio is half of the normal Data packet delivery ratio as shown in Fig.14.

VI. CONCLUSION

Networks can hit upon an attack whilst seventy-five % to 100% of traffic is DDos. It is agreed along up to the expectation it is an effective strategy of addressing the detection on DDoS into SDN including precision or efficiency. Protecting the system of SDN by using detecting DDoS, attacks became the middle of these studies. Dos attack is mitigate using OpenFlow Sdn controller, and the network is working in attack condition. The controller also identifies and blocked a unique attacker address in address table then it is not communicated to others.

REFERENCES

1. Gupta, A., Sukheja, D., & Tiwari, A. (2015). Impact of Sybil Attack and Security Threat in Mobile Adhoc Network. International Journal of Computer Applications, 124(9).
2. Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*, *51*(7), 36-43.
3. Lim, S., Ha, J., Kim, H., Kim, Y., & Yang, S. (2014, July). An SDN-oriented DDoS blocking scheme for botnet-based attacks. In *Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on* (pp. 63-68). IEEE.
4. Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, *16*(3), 1617-1634.
5. Tariq, U., Hong, M., & Lhee, K. S. (2006, August). A comprehensive categorization of DDoS attack and DDoS defense techniques. In International Conference on Advanced Data Mining and Applications (pp. 1025-1036). Springer, Berlin, Heidelberg.
6. Xing, T., Huang, D., Xu, L., Chung, C. J., & Khatkar, P. (2013, March). Snortflow: A openflow-based intrusion prevention system in cloud environment. In Research and Educational Experiment Workshop (GREE), 2013 Second GENI (pp. 89-92). IEEE.
7. Li, L., Zhou, J., & Xiao, N. (2007, December). DDoS attack detection algorithms based on entropy computing. In International Conference on Information and Communications Security (pp. 452-466). Springer, Berlin, Heidelberg.
8. Oshima, S., Nakashima, T., & Sueyoshi, T. (2010, February). Early DoS/DDoS detection method using short-term statistics. In Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on (pp. 168-173). IEEE.
9. YuHunag, C., MinChi, T., YaoTing, C., YuChieh, C., & YanRen, C. (2010, November). A novel design for future on-demand service and security. In Communication Technology (ICCT), 2010 12th IEEE International Conference on (pp. 385-388). IEEE.
10. Braga, R., Mota, E., & Passito, A. (2010, October). Lightweight DDoS flooding attack detection using NOX/OpenFlow. In Local Computer Networks (LCN), 2010 IEEE 35th Conference on (pp. 408-415). IEEE.
11. Hu, F. (Ed.). (2014). Network Innovation through OpenFlow and SDN: Principles and Design. CRC Press.
12. Karmakar, K. K., Varadharajan, V., & Tupakula, U. (2017, May). Mitigating attacks in Software Defined Network (SDN). In Software Defined Systems (SDS), 2017 Fourth International Conference on (pp. 112-117). IEEE.
13. Xu, T., Gao, D., Dong, P., Foh, C. H., & Zhang, H. (2017). Mitigating the Table-Overflow Attack in Software-Defined Networking. IEEE Transactions on Network and Service Management, 14(4), 1086-1097.
14. Hu, F. (Ed.). (2014). Network Innovation through OpenFlow and SDN: Principles and Design. *CRC Press*.
15. Mohan Kumar, M., and R. Vijayan.(2017). "Privacy authentication using key attribute-based encryption in mobile cloud computing." In *Materials Science and Engineering Conference Series*, 263(4), (pp 042069).
16. Singh, S., & Vijayan, R. (2011). Enhanced security for information flow in vanet using signcryption and trust level. *International Journal of Computer Applications*, *16*(5), (pp.13-18).

AUTHORS PROFILE

R Vijayan is working as Associate Professor at School of Information Technology and Engineering, VIT-Vellore Institute of Technology, Vellore, India. He received his Ph.D. in Information Technology and Engineering from VIT University, India in 2017. He graduated in Electronics and Communication Engineering from Madurai Kamaraj University, India and postgraduate in Computer Science and Engineering from VIT University, Vellore, India. He is a life member of the Computer Society of India (CSI). He has produced a number of national and international research articles in reputed journals and conferences. His research interest involves Web technology, Wireless networks, Adhoc networks, computer networks, cloud computing, and MANETs.

V Mareeswari is working as Assistant Professor (Senior) at School of Information Technology and Engineering (SITE), Vellore Institute of Technology (VIT), Vellore, India. She received her Ph.D. in Information Technology and Engineering from VIT University, India in 2019 in the area of Web Service and has produced a number of national and international articles in reputed journals and conferences. Her area of interest includes programming in web technologies, web services, cloud computing, networking, and data analytics in Bigdata.

C Navaneethan is currently working as Associate Professor in the School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu. He pursued his under graduation in Engineering with Computer Science and Engineering as Specialization in April 2004. He was awarded Honor in M.E CSE in July 2006 and Ph.D. in Wireless sensor Networks from Anna University, Chennai in the year 2017. He has published & presented many National and International Journals/Conferences. His current areas of research activities include Wireless Sensor Networks and Network Security. He is a research paper reviewer in conferences in National and International levels and also a Life Member in professional Bodies like IAENG, IACSIT, and CSTA

S Prasanna is working as Associate Professor at School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India. He received his Ph.D in Computer Science and Engineering from VIT. He graduated in Computer Science and Engineering from University of Madras, India and Postgraduate in Computer Science & Engineering from Anna University, India. He produced a number of national and international research articles in reputed journals and conferences. His research Interest involves Soft computing, Data mining, Blockchain Technology, and Machine Learning.

S. Meenatchi was awarded an honor in Bachelor of Engineering in Computer Science and Engineering specialization in 2004. She was also awarded the honor in Master of Engineering in Computer Science and Engineering specialization in 2006. She is working as an Assistant Professor (SG) in the Department of School of Information Technology and Engineering. She has published and presented many national and international journals and conferences. Her current areas of research activities include wireless sensor networks and network security. She is a life member of professional bodies like CSI..

Amit Gupta has completed the Master of Information Technology, School of Information Technology and Engineering (SITE), Vellore Institute of Technology (VIT), Vellore, India in 2018. His interest involves cloud computing, wireless networks, and computer networks