DDoS Mitigation using Software Defined Network

Nayana Y, Mr.JustinGopinath M.Tech, Girish.L
PG Student, Asso. Professor, Assistant Professor
Dept of CSE, Cit, Gubbi, Tumkur

Abstract *—Software Defined Networking (SDN),is an archetype which decouples the control plane and data plane. Data plane is used to just forward the data and control plane is used to decide how data should be forwarded. Open networking Foundation (ONF) is a group that is used in the development of SDN. For interfacing of control plane and data plane in SDN requires some protocol. One such protocol is Open Flow. The first standard interface designed for SDN is Open Flow. It provides high-performance, controlling granular traffic across multiple vendor's network devices.*

As the network infrastructure of an organization grows, it's very difficult to manage and control such networks from a centralized system like laptop through programs. As an attempt in this paper we are adopting the SDN technology to manage and control the networks programmatically. In this paper we are addressing the two issues for providing security to the network from DDoS mitigation and balancing of the load using SDN.

In this paper for DDoS mitigation we are assigning a threshold value so that the SDN controller resists the DDoS attack programmatically. For Load balancing is to maximize throughput, minimizes response time, avoid overload by using round robin or random policy method using a new approach called SDN.

Keywords – *SDN, Flow, Open Flow, DDoS.*

I. INTRODUCTION

A group of two or more computers linked together is a network. So many types of computer networks are there including local area network, wide area network and metropolitan area network. Over past decades networking principles remained unchanged [1]. Networks are assembled using more or less refined switches and routers. Devices are developed by number of vendors commonly using proprietary operating system and interfaces. An institution has to apply a specialist on every router brand for building a heterogeneous network on devices from distinct vendors. Because of this probability of configuration mistakes also increases while configuring different systems. So a new technology has to be addressed to make networks more scalable, to allow easily managing of networks devices from distinct vendors. By programmable networks i.e., Software Defined Network (SDN), we can fulfil these needs.

SDN is an archetype which decouples the data plane and the control plane of network. This decoupling leads to a new architecture. Switches are used for basic packet forwarding devices consists of flow tables populated with the localized flow rules [2]. Rule tells how incoming packets are handled based on matching fields. These are managed by a remote "controller" entity. Control plane tells how packets should be moved. Controller communicates securely with switches using a standard and open interface like Open Flow protocol. It consists of internal flow table, and a standardized interface to add or remove flow entries [3]. This new architecture allows for a range of considerably more flexible and effective network management solutions. A logically centralized controller provides application developers with a unified programmable interface on which to deploy software and higher level application. It has the approach for providing flexible network programmability. It provides real time configuration, operation and monitoring of a network.

SDN encompass of three layers and their interactions are shown in figure 1. If there are large-scale or wide-area region network, then we may use more than one SDN controller[4]. Through network policies control layer always balances the network states in either a distributed or centralized manner. Due to dynamic flow of activities network policies should be updated timely, for the unrestricted access to global network elements and resources. All the SDN applications present in the application layer of the SDN architecture. The connection between the application layer and control layer are supported by a set of application programming interfaces such as north bound open APIs, for the enabling of common network services like routing, access control, TE, bandwidth management, QoS, DDoS mitigation usage of energy etc. forwarding of data layer can be employed by programmable Open Flow switches via Open Flow controller, and communication of switches with the controller through south-bound API (ex: Open Flow protocol).

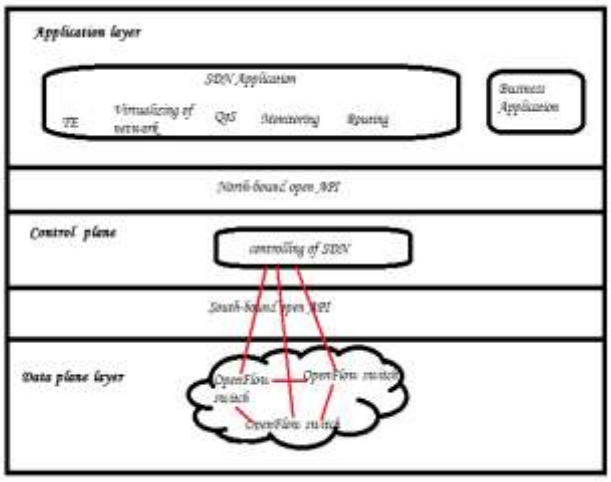

Fig 1: SDN architecture

The interactions among these layers, the SDN archetype allows a whole and global view of muddle network, and also gives a powerful control platform for the network management over traffic flows. Simplifying of the network management, reducing of operating costs, promote innovation and evolution in present and future network are all will be done in the SDN.

Distributed denial of service (DDoS) attack is one of the problems in network security. An attempt to make a machine or network resources unavailable to its intended users is a DDoS attack. It indefinitely interrupts or temporarily or suspends services of a host connected to the internet. This DDoS attack is the growing threat in the enterprises and need to be addressed. Next issue is that there would be a need for high performance and low latency for transmission of data, so this needs load balancer.

II. RELATED WORK

To begin with, it make sense for any network when it is connected efficiently, each of the end nodes should be able to communicate with each other end nodes [5]. In a switch fabric- switches are used in network topology. The main aim of switches is used to, connect a large number of end points, which have a limited number of ports. In 1985 Charles E. Leiserson proposed fat-tree network which is in tree like structure. And bottom layer is connected with a processor. For any switches the unique aspect of fat-tree is that, the number of links going up to its root in the upper level is same as the number of links going down to its sub-roots. So that the link get “bigger” towards the peak of the tree, more links are present at root switch of tree when compare to other switches. Calculations of packets were done in load balancing across the paths are based on hash. Problem in this approach is that every packet of a flow follows a single pre-defined path via a network. In case of any switch break down or link failure, packets tend to drop or other switches should be configured manually for choosing a different path. As the network grows this becomes a difficult task. In hashing one more disadvantages is that all the links gets same percentage of hash, means all paths have same capacity. So we cannot achieve efficient load balancing, because of equal capacity issue.

One of the most destructive attacks in the internet over decades areDDoS attack. So many strategies have been designed to avoid DDoS attack. From that only a few of them are considered for widespread deployment for the reasons of strong design assumptions on the internet infrastructure, prohibitive operational costs and complexity[6]. In existing networking system, they usually require huge network connection state tables to be maintained at routers or switches. This results in the extra storage and computational burdens. The techniques like packet marking require a large amount of packets to be monitored and collected, including additional processing overhead. So those techniques rely on the deployment of additional modules or devices, which lead to increasing deployment complexity.

Some of the reasons for DDoS attacks are [7]:

- The fundamental reason for DDoS attack is a design of the internet. These internets are designed to run end-to-end application. Routers provide best-effort packet forwarding. Senders and receivers are responsible for achieving service guarantees like QoS and security. Less bandwidth than routers are provided to the end hosts. By this attackers misuse the huge amount of resources in routers foe delivering of number of packets to a target.
- Controlling and managing of internet is distributed DDoS attack depends on the state of security in the rest of global internet. In distributed management it is impossible to investigate cross-network traffic behaviors. In a two-way communication if one party misbehaves, then arbitrary damage can be caused to its peer. So that no third party can stop it.
- Cyber warfare is also one of the reasons for DDoS attack.

DDoS exploit inherent weakness in the design and organization of the internet [8]. These are rapidly becoming the weapon for hackers throughout the globe. This paper tells about the types of DDoS attacks and some of the tools used in DDoS attack. Main tool in DDoS is bulk flooding, in this attackers flood the victim with so many packets as they can in order to overwhelm the victim. Example: if so many people came to buy something, but there is very less chance to get services, because they have are thousands of other people standing in line before them. DDoS requires a large number of hosts attacking at the same time together. DDoS attack are the most difficult to defend against and more new tools are developed. In traditional system security technologies like firewalls and intrusion

detection system do not provide sufficient DDoS protection. This simply filters solution such as router based access control list(ACLs), cannot separate good traffic from bad for most of the attacks, this results in legitimate transaction require next generation architecture.

In a distributed web server system one of the critical operating high performances is load balancing. It can be achieved by various approaches [9]. In this paper they have explained the approaches like client-based, dispatcher-based and server based systems.

- Client-based means routing of the document requests from the client side that can be applied to any replicated web server even when the nodes are loosely or not coordinated.
- Dispatcher-based: it is an alternative to DNs based architecture. It aims to achieve full control on client requests and it mask the request routing among multiple servers. This typically uses simple algorithms for selecting the web-server.
- Server-based: this uses two level dispatching mechanisms.

In this paper internet entities that may dispatch did not considered. Those are intelligent routers or intermediate name servers.

One of the recent popular techniques which protects ISP network from sudden congestion caused by spikes or link failure is the dynamic load balancing. This requires splitting traffic occurs multiple paths at a fine granularity [10]. Splitting traffic avoids packet reordering. This paper tells systematically split a single flow across multiple paths without causing packet reordering. And also this paper proposes a new traffic algorithm FLARE, which operates on busts of packets, carefully chosen to avoid reordering. It provides accuracy and responsiveness comparable to packet switching without reordering packets.

Now, the emerging is architecture is SDN. It has offered a solution to reduce network management and complexity. It is also used to provide the network security and balancing of load through programs. An SDN controller allows obtaining a global view of the network states and achieving centralized network. Human intervention will not be required to manage and maintain the DDoS mitigation schemes. Mitigation functions and load balancing are abstracted and integrated at the application layer of SDN. No need of installing specific devices.

III. PROPOSED SYSTEM

An alternative approach for the above two problems is SDN. SDN has the concept of controller makes decision for packet traversal and not the switches. Dynamically controller detects the topology by listening to the switches and also available path having fewer loads is calculated by the controller in load balancing. Then the controller directs the switches with forwarding entries needed for the paths thus helps in balancing the load efficiently with every flow.

A.DDoS mitigation:

In DDoS mitigation controller detects the DDoS attack by using threshold value and helps to remove DDoS attack in the network. In our project we are providing security challenges in DDoS attacks mitigation in SDN environment. For mitigation we are used the output of developed DDoS detection method. SDN network monitoring and security are created as a state of art.

Next, analyzing of attack, defence and monitoring structure in SDN and in current network analyzing the deployment of method. Now a day's monitoring is done at the host or network level in attacked network. That was independent on network architecture. Many variants of DDoS attack and defense mechanism are there against them proposed for current network. In SDN we believe those are fully adopted or re-implemented. Flow based monitoring technique are very often used for detecting DDoS attacks. In SDN due to flow based, it's possible to detect in both planes. Mechanisms of detection are deployed in controller without proper aggregation of network traffic, which may overload the communication among data and control plane. Flow table also poses some limitations. Some of them could be resolved by adding some minimal intelligence to the devices of data plane.

In our project we are going to mitigate the attack using SDN architecture. We considered two groups of DDoS attack for simplicity. Computing power are targeted by the first group i.e., semantic attack. Brute-force or flooding attacks are by the second group, which exceeds available bandwidth. Mitigation of first group can be done using SDN infrastructure of the attacked organization. All network devices can be used as mitigation mechanisms as one logical switch to balance the load in network traffic via network. Load balancing traffic provides mechanisms the possibility to configure many filtering rules for maximizing the amount of dropped malicious traffic. This is not effective for second group. For that we should stop the attack closer to the source of traffic example ISP of the source attack, country of origin. This technique for mitigation needs a cooperation of involved providers for the attack on the route. And needs a complex reconfiguration of ISP routing tables, SDN could make this reconfiguration easier.

We created a synthetic and real traffic based data sets and have experimented the network. In data plane this experiment uses OpenvSwitch. For the control plane we used Floodlight or Open daylight open source solutions. For mitigation structure has to be implemented by using output of new DDoS detection methods and on the top of infrastructure SDN controller is deployed. Combining all these areas should allow

network to react fast on DDoS attack and also to increase ability to filter malicious traffic. By this SDN provides a good platform for distributed detection and DDoS mitigation.

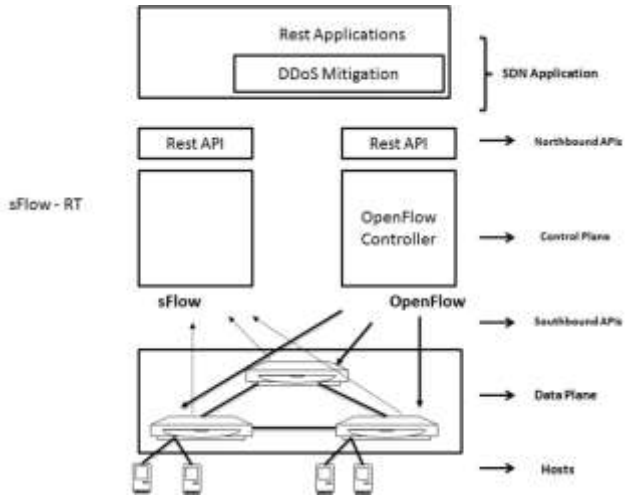

Fig 2: proposed system of DDoS mitigation

B. Load balancing:

Load balancing can also be applied using SDN. For data centres the most widely used topology is fat-tree network. But in traditional network this fat-tree cannot be fully satisfied. For that result we are using SDN. By a centralized controller Open Flow protocol enables monitoring of traffic statistics. In our project we proposed a load balancer for Open Flow, to achieve high performance and low latency. In dynamic traversal algorithm, the main task is to distribute traffic of upcoming and incoming network flows and making each second path receive same amount of traffic load. This can also applied to large network and dynamically schedule the data flow.

In our project we are using round robin or random policy for balancing the load. SDN guarantees dynamic network and are programmable. For any changes in packet forwarding SDN react faster and more effectively. SDN is still new and progressing area.

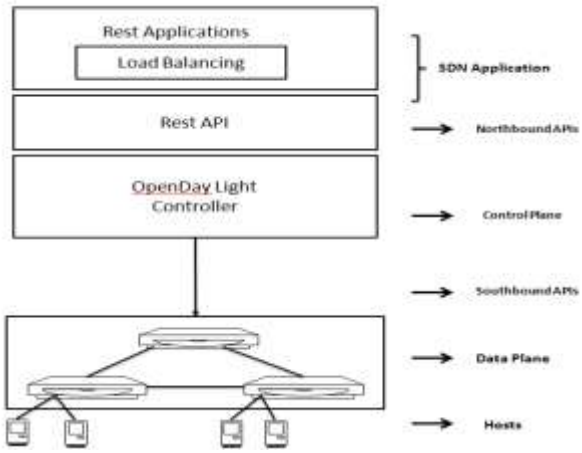

Fig 3: proposed system for load balancing using SDN

IV. IMPLEMENTATION

Implementation consists of two applications in this paper:

A. DDoS mitigation:

DDoS mitigation is a set of techniques for resisting DDoS attack on a network attacked to the internet by protecting target and rely network. This DDoS mitigation requires identifying correctly the incoming traffic to separate human traffic from human like bots and hijacked web browsers.

For rapidly detecting DDoS attack and drive automated controls to mitigate their effect will be done in sFlow. Continuous stream of datagrams are sent by the switches to the sFlow-RT controller, which is running the DDoS mitigation application. If the attack is detected, we need to block the traffic for that an Open Flow rule is pushed to the switch. The normal traffic will not be touched only the attack traffic is detected and removed from the network.

In this experiment sFlow-RT of InMon contains three basics

- Metrics

Metrics consists of name of the metric, value of the metric, maximum events. Metric name means it consists of flows, DDoS. If we select the DDoS metric name, is equal to the threshold id of an event then it will go to the top flows. There values will be shown.

- Flow definitions

Flow definitions tell how the flow of the packets is directed. In this we have policy, rules have to be written. Sequence of packets from source computer to the destination is a flow.

- Threshold

It is a value. It associated to be static. Selecting threshold value is necessary to help the DDoS detection to make a good decision in identifying the attacker at the fast attack especially. Selecting threshold value is very important. This value is helpful for differentiating normal activity and abnormal activity in network traffic. If we select a inaccurate threshold value will cause an excessive false alarm especially if the value is too high or too low. Detecting the intrusion as quickly as possible is very important to provide the security.
The above basics are the main thing has to be mentioned in the DDoS mitigation.

We are setting a threshold value, if the traffic i.e., number of packets crosses the threshold value the controller will take action and mitigate the attack immediately.

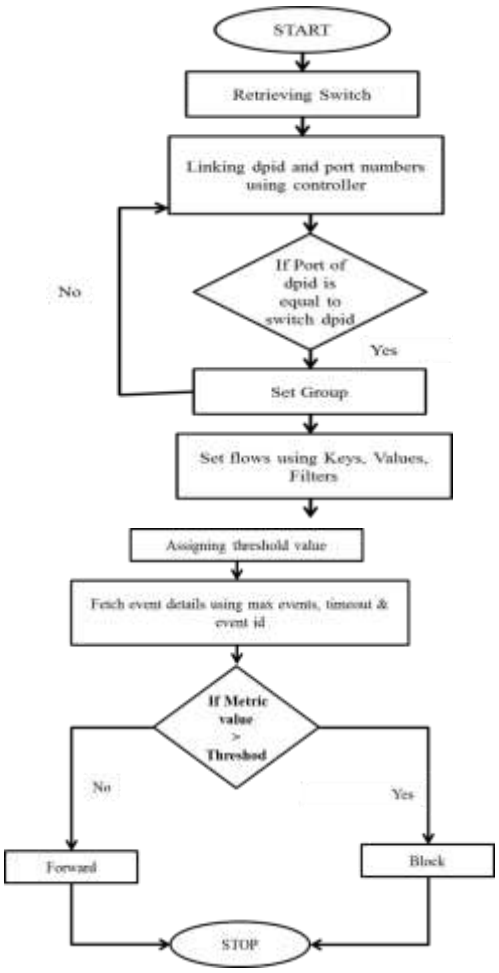

Fig 4:work flow of DDoS mitigation

B. Load balancing using SDN:

One of the applications in SDN is load balancer, that balances the traffic to backend servers depend on the source address and source port on every incoming packets. Open Flow rule will be reactively installed to direct all the packets with a specific source address and source port to one of the applicable backend server. Based on round robin policy or random policy server can choose services. Configuration of service can be done via REST APIs which are identical to Open stack Quantum LBaaS (Load-balance-as-a-service).

For this service to be used we need a virtual IP (VIP) that have to be exposed to the clients of this service and it is used as a destination address. VIP is as entity composed of a virtual IP, protocol(TCP or UDP) and port.

Assumptions:

We are created a pool which contains a one or more VIPs that mapped to the same server. Same pool should be shared by all VIPs and also share the same load balancing policy either round robin or random policy.

- There should be only one server pool that can be attached to a VIP.
- An idle timeout of 5 seconds is installed at all flow rules.
- Packets send to a VIP must go-ahead the cluster of Open Flow from the same switch from where it is enrolled.
- Once the flow rules are installed, then if we delete a VIP or a server pool or server from a pool it does not delete the flow rules.
- Automatically flow rules should take time out after idle timeout of 5 seconds.

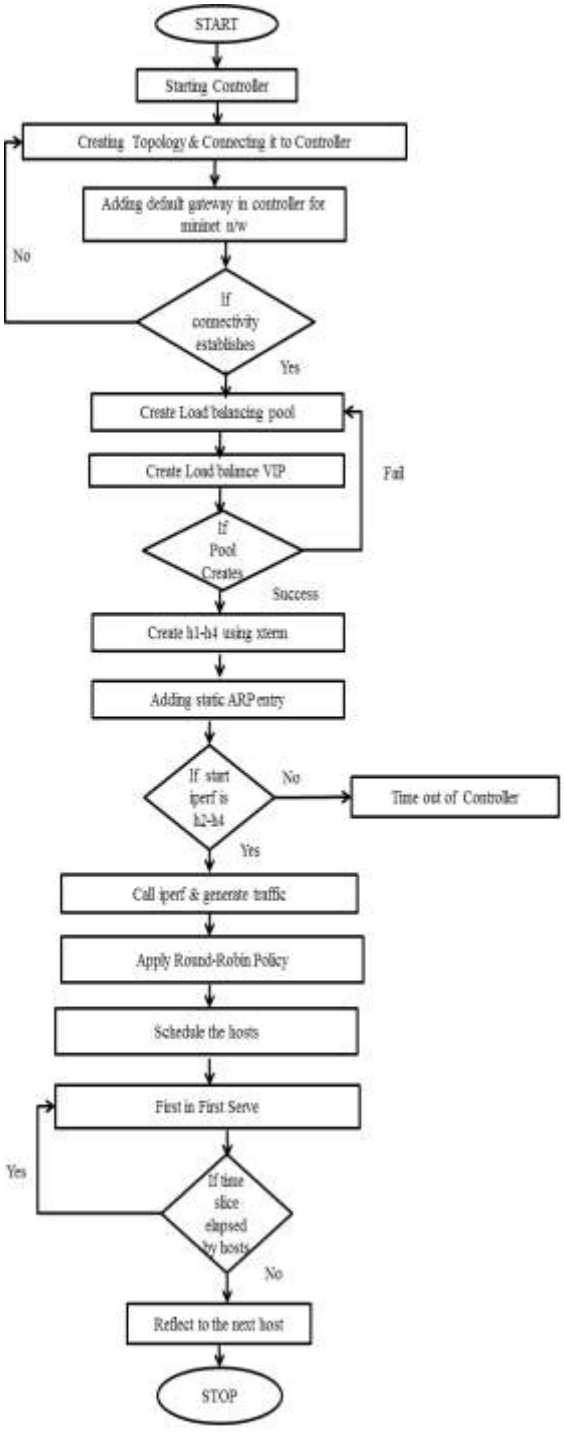

Fig 5: work flow of load balancing

V.RESULTANALYSIS

A. Experimental results:

Fig 6: DDoS attack without using mitigation

Figure 6 shows the graph without mitigation of DDoS. X-axis represents time of the traffic generated. Y-axis represents number of packets in second. The graph shows that without mitigation using ping flood generates a sustained traffic rate of around 2.5 M packets per second.

Fig 7: DDos attack using mitigation technique in SDN screen shot

Figure 7 shows the graph of DDoS with mitigation. X-axis represents time of the traffic generated. Y-axis represents number of packets in second. Graph shows that when the traffic flows is more than the threshold value then the controller is able to quickly respond to the generated traffic. Within a second mitigation is applied. Instead of reaching peak of 2.5M packets per second, the attack is limited to 23K packets per second.

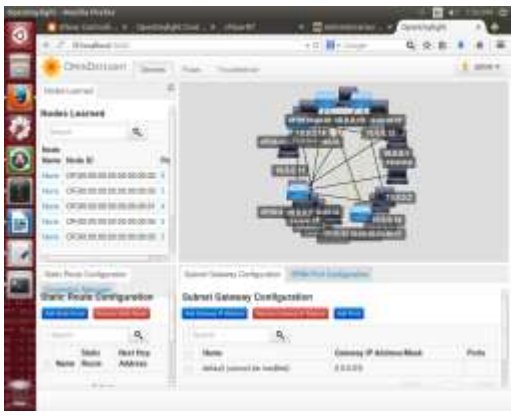

Fig 8: output of connectivity in OpenDaylight controller screen shot

Figure 8 represents the output of OpenDaylight controller for connectivity. This shows the tree topology created by using emulator Mininet.

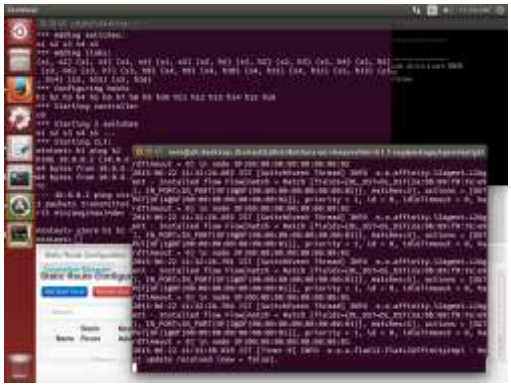

Fig 9: Output of controller running

Figure 9 represents the output of the controller Opendaylight running.

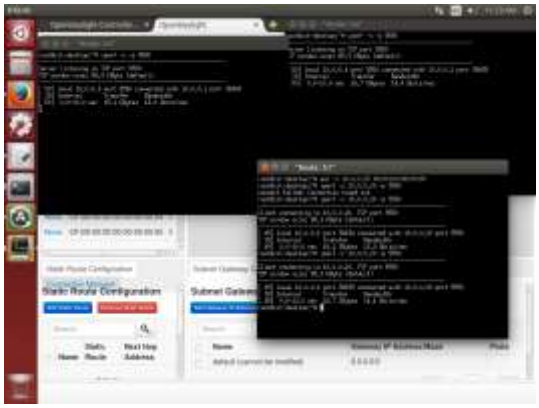

Fig 10: Output of load balancing screen shot

Figure 10 represents the load balancing output using SDN. Here we can see the round robin policy used in load balancing.

VI. CONCLUSION AND FUTURE WORK

In our paper successful implementation of sample network using Open Flow switches is done. Achieved network security issue DDoS attack, which controlling through programs using SDN in a controlled

system like laptop. Another problem we have achieved is load balancing using round robin in SDN. We are successful in achieving the round robin policy in SDN for scheduling of load. In the future we set for receiving the genuine SDN empowered switches for our demonstration. For element burden adjusting application, in future will utilize the cloud applications like open stack. Alert or error message will be sent to the network administrator automatically in DDoS application.

ACKNOWLEDGMENT

We are grateful to express sincere thanks to our faculties who gave support and special thanks to our department for providing facilities that were offered to us for carrying out this paper.

REFERENCES

[1] Martin Vizv´ary "Mitigation of DDoS Attacks inSoftware Defined Networks" Jan 2015

[2] Syed Taha Ali, Member, IEEE, Vijay Sivaraman, Member, IEEE,Adam Radford, Member, IEEE, and Sanjay Jha, Senior Member, IEEE "A Survey of Securing Networks using Software Defined Networking"

[3] Nick McKeown: Stanford University, Tom Anderson:University of Washington, HariBalakrishnan: MIT, Guru Parulkar: Stanford University, Larry Peterson: Princeton University, Jennifer Rexford: Princeton University, Scott Shenker: University of California Berkeley, Jonathan Turner: Washington University in St. Louis "OpenFlow: Enabling Innovation in Campus Networks" Mar, 2008

[4] ONF White Paper "Software-Defined Networking: The NewNorm for Networks" Apr, 2012

[5]Gunjan Patel Adithi S AthreyaSwethaErukulla "OpenFlowbased dynamic load balancedSwitching" 2013

[6] RishikeshSahay_z, Gregory Blanc_z, ZonghuaZhangyz and Herv´eDebar_z_Institut Mines-T´el´ecom, T´el´ecomSudParis"Towards Autonomic DDoS Mitigation using Software Defined Networking"

[7] QijunGu: Texas State University – San Marcos Peng Liu:Pennsylvania State University "Denial of Service Attacks"

[8] SílviaFarraposo, Laurent Gallon, Philippe Owezarski "Network Security and DoS Attacks"

[9] Valeria Cardellini: Universita di Roma \Tor Vergata, MicheleColajanni: Universita di Modena e Reggio Emilia, Philip S. Yu: IBM T.J. Watson Research Center "Dynamic Load Balancing onWeb-server Systems"

[10] SrikanthKandula: MIT Dina Katabi: MIT, Shantanu Sinha:Microsoft, Arthur Berger: MIT/Akamai "Dynamic LoadBalancing Without Packet Reordering"