Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3,Issue 6,June -2016

Detection and Prevention Of DDoS Attack In software Defined Network

Prof Y. S. Hande[#1] Tejas Kadu[#2] Aishwarya Kshirsagar[#3] Saurabh Hublikar[#4] Sameer Kulkarni[#5]

[1-5] *Computer Engineering, Sinhgad Institute of Technology And Science*

Abstract -*Software Defined Network (SDN) is new upcoming field in networking domain which has potential to change the current networking concepts. It has changed the current network architecture in terms of operation and network deployment. In SDN, the data and control planes are made separate giving network administrator to design and implement their own concept for network control. The controller is core part of SDN network as it manages the whole network centrally. It basically controls the incoming packets and their forwarding route. However the controller are vulnerable to flooding attacks. Because of natural feature of centralised control these become the potential target. The attackers attack by sending continues spoofed packets leading to bandwidth occupation and overloading the flow tables in the switch.*
To overcome such attack we are using IP based filtering in particular time frame in order to Detect and Prevent DDoS attack.

Keywords *– DDoS, SDN, Distributed system, IDS.*

I. INTRODUCTION

The ability to partition networks based on software defined networking (SDN) has risen in popularity. Presently OpenFLow is a new network technology and an open standard for SDN in which the control plane and data plane of network equipment's are separated. OpenFLow provides an open protocol to program the flow table in different switches and routers. Network administrator can partition traffic into production research flow. Researchers can control their own flow. Production traffic is isolated and processed in same way as today.

SDN architectures decouple network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services. Purpose of the proposed mechanism is to detect and reduce the effect of DDoS attack. We propose a method in order to combat against DDoS attack.

II. LITERATURE SURVEY

SDN is expected to replace the existing traditional network with a lot of advanced features. However, it is facing with many security challenges. In this paper, we propose a probable method to battle against DDoS flooding attack. Although the method can decrease the impact of DDoS attack, but not enough when the amount of attack traffic is very huge.[1]

In Software defined networking, characterized by a clear separation of the control and data planes is being adopted as a novel paradigm for wired networking. With SDN, network operators can run their infrastructure more efficiently, supporting faster deployment of new services while enabling key features such as virtualization. In this article, they adopt an SDN-like approach applied to wireless mobile networks that will not only benefit from the same features as in the wired case, but will also leverage on the distinct features of mobile deployments to push improvements even further.[2]

III. PROPOSED METHODOLOGY

@IJAERD-2016, All rights Reserved

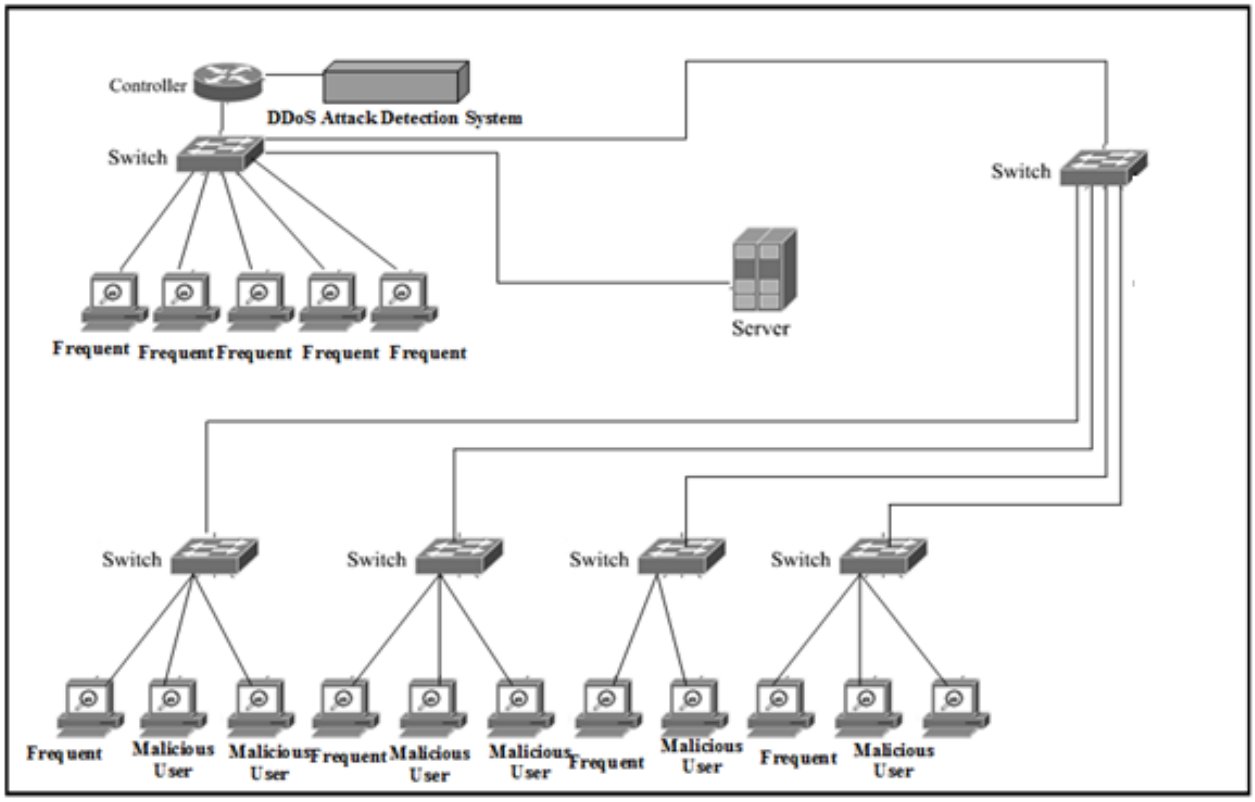

fig. ARCHITECTURAL DESIGN

A description of the program architecture is presented with description of the general architecture of the underlying system.

The above system describes the architecture of a SDN system in the distributed environment. The system shows the connectivity of SDN system with the outer system. Also it suggests the various types of users and their behaviour.

In our paper we proposed method to detect the occurrence of DDoS attack on Software Defined Network(SDN). In our proposed method we consider number of packets coming into the network as well as time factor as a base parameters for detection of attack. As we know in SDN when packet enters into the network it comes to the switch and switch transfer the packet to the controller for further operations. Controller of SDN is software controlled entity because of which we can program the controller in order to function according to our proposed methodology.

In our methodology when a packet enters into SDN, controller starts counting number of packets. Time frame is also very important while considering the packet count. In a particular time frame if the number of packets are greater than a predefined threshold value then the network is consider under attack. The threshold value of packets in particular time frame is dependent on various factors such as

- Scale of Network
- Time of day
- Regular analysis of network(which contains data about average regular traffic on SDN)

@IJAERD-2016, All rights Reserved

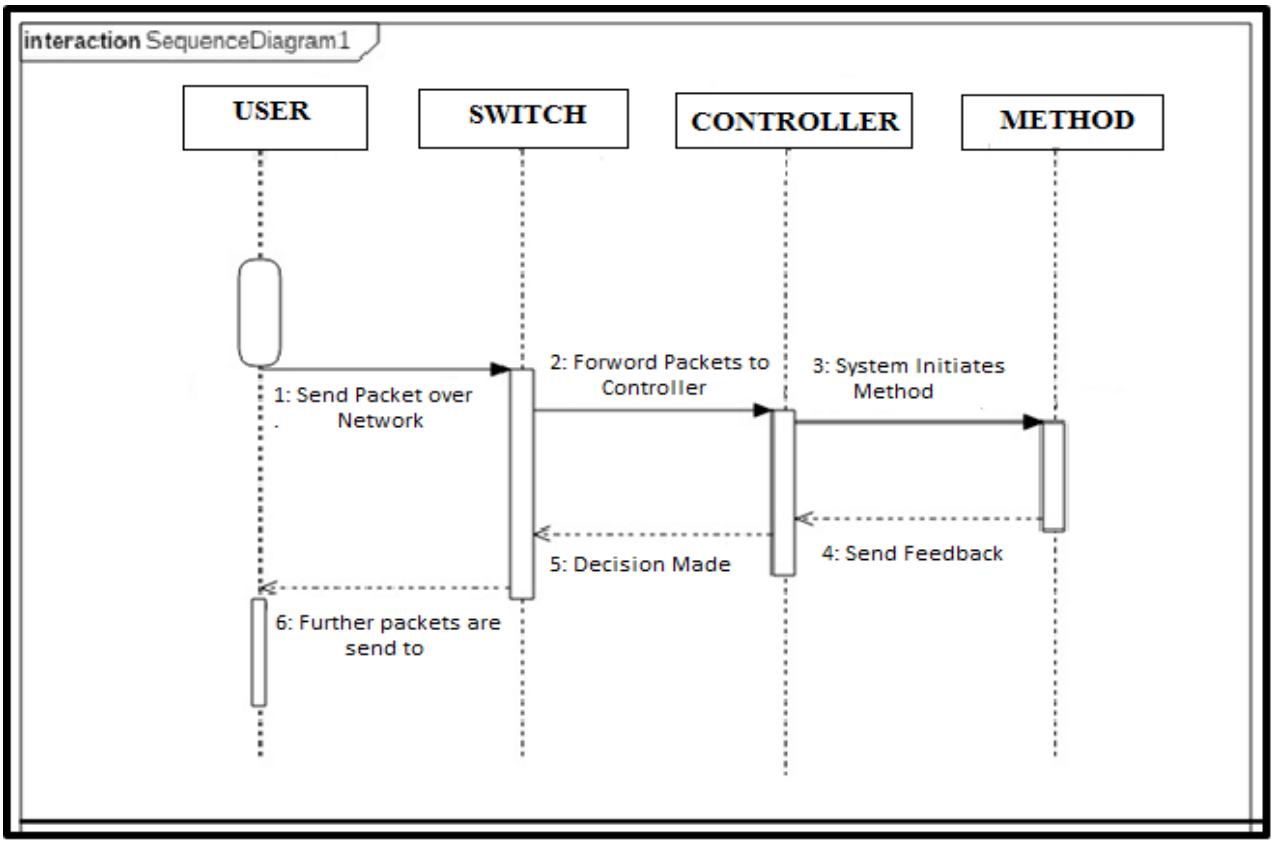

Fig1.Sequence Diagram

So the threshold value will be different for different network. For precise detection we count number of packets per ip address. If the number of packets on a IP address in a particular time frame is greater than threshold then the ip address is consider as attacker ip address and the method running on controller will block that ip address from the network. In such way we are going to detect and prevent DDoS attack on network.

IV. ALGORITHM

1) Start Controller
2) Start Timer
3) Start Receiving Packets
4) If Packet's IP is present in the list
   4.1 Yes: Increment Count
   4.2 Add am entry and increment the count
5) After every 3 seconds check the count
   5.1 If count>200/sec: [DDoS Attack]
   Move IP address block list and drop packets from that IP
6) Else continue

V. CONCLUSION

Thus**,** in software defined networking with DDoS attack detection system, we decouple the data plane and control plane. Here the data planes only acts according to the control plane. The control plane acts as the brain of the network and is centralized. The data plane acts as the muscles of network that is it just does the work of forwarding packet. All the routing or forwarding decisions are taken by the open Flow controller. In this project we are showing the flow of traffic by using SDN concept. We are detecting the attacks and display its IP address.
So, we studied the basic architecture of SDN, threats to SDN as DDoS. We studied in detail about DDoS attack, its type and various approaches to perform DDoS attack.

@IJAERD-2016, All rights Reserved

VI. REFERENCES

[1] Nhu-Ngoc Dao1, Junho Park1, Minho Park, and Sungrae Cho, School of Computer Science and Engineering, Chung-Ang University, Seoul, South Korea School of Electronic Engineering, Soongsil University, Seoul, South Korea, "A Feasible Method to combat against DDoS Attack in SDN Network" 2015

[2] Seyed Mohammad Mousavi and Marc St-Hilaire Department of Systems and Computer Engineering Carleton University, Ottawa, Canada, "Early Detection of DDoS Attacks against SDN Controllers" 2015

[3] Manar Jammal, Taranpreet Singh, Abdallah Shami, Rasool Asal, and Yiming Li, "Software-Defined Networking: State of the Art and Research Challenges" 2014

[4] Siamak Azodolmolky, Junho Park1, Minho Park, "Software defined Networking with OpenFLow controller" 2014

[5] Yogita Hande, Aishwarya Jadhav, Rutuja Zagade, Achaleshwari Patil, "Software Defined Networking with Intrusion Detection System" 2015

[6] Suresh Kumar, Tarun Kumar, Ganesh Singh, Maninder Singh Nehra,"OpenFlow Switch with Intrusion Detection System", International Journal of Scientific Research and Technology, Volume 1, Issue 7, October 2012.

[7] M Canini, D. Vanzane, P. Peresini D. Kostic and J. Rexford, A NICE way to Test OpenFlow Applications. In Proceedings of the 9th USENIX Conference on Networked Systems Design and Implemntations (NSDI) 2012.

@IJAERD-2016, All rights Reserved