International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Implementation of Software Defined Networking using Openflow Protocol.

Anshath Nisha P, Jessica Priya dharshini P, K.J.Prasanna Venkatesan.

Abstract: ***Software Defined Networking is a new rising technique that allows to separate the planes. This emerging technology provides agility and flexibility to a network. Agile means the administrator can automatically adjust the network traffic to meet the changing needs. Its main aim is to make the network devices by using software and controlling the networking devices using software. It is attained by using in Mininet software.The SDN is implemented using the OF Protocol in the ONF Software. It is done by using Open flow switch and mainly for accurate communication done by the open flow switch. Here it gives accurate connection and the information is transmitted in the form of packets and delivered correctly to the server or other user, etc., Open flow switch has two types where centralized switch is used here.***

Keywords: Agile, SDN.

I. INTRODUCTION

Software Defined Networking is a growing technology which allows breaking of integration of planes. This concept was first officially introduced in June 2009 at Stanford University, US. Each routing device has a control plane which is placed in a centralized controller to have a single point of control. On the contrary, data plane which comprises of routers, which are attached together in a topological fashion. The data transfer is controlled by the data plane and it is done by the resolution taken by the central controller[a].Both the planes communicate through the protocol .With the introduction of the Open Flow, the major advantages comes in the fact of simpler modification. SDN permits simple high-level policies to modify the network as the device level dependency is eliminated to some extent. Globally by its design, the whole network is viewed by the controller. This design of the controller helps to introduce a program which has to be embedded in the centralized controller. Many industrialists worked around and they came with some solutions like Open Daylight, Open Stack.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 20, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Anshath Nisha P,pursuing final year in the stream of ECE in the institution of National Engineering College,Kovilpatti Email:anshath7503@gmail.com
Jessica Priyadharshini P, pursuing final year in the stream of ECE in the institution of National Engineering College, Kovilpatti Email: jessicaimmanuel111@gmail.com
Dr.Prasanna Venkatesan,Asst.Professor in National Engineering College,Kovilpatti. Email: prasana.nec@gmail.com

II. ARCHITECTURE OF SDN:

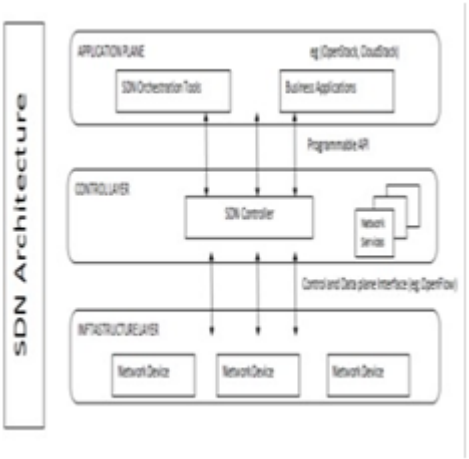

FIG 2.1 ARCHITECTURE OF SDN.

The Architecture of SDN from the figure 2.1, clearly explains about the SDN control and data plane elements of architecture were packed in retention, distributed by one or more dominion vendors.

Planes Of Sdn:

SDN consists of two types of planes. They are

a. Control plane

b. Data plane

The basic components of the architecture are data plane, control plane and the management plane. Data plane is served by control and management plane. It takes care of the traffic that the network needs to carry[b]. It also allows the transfer of the data to and fro from clients. It handles multiple conversations by using multiple protocols. The conversations of the remote peers are well managed by the data plane. The congestion of the data plane is travelled through the routers, instead of to or from them. The subset of the control plane is the management plane. It carries administrative traffic. All the three planes are implemented in the firmware of routers and switches.

III. OPENFLOW PROTOCOL:

SDN has grown to circumscribe numerous protocols. Open Flow protocol is a leading protocol and the only protocol defined by SDN standard. In past years numerous questions have risen about the Open Flow in the current SDN technology. Here, the SDN Central research team encounters all matters with a comprehensive investigation on the state of Open Flow. Firstly, some background[c]. The SDN revolution was initiated with the development of Open Flow.

Open Flow version 1.0 was released in 2009 and was significantly updated which led to the release of the version 1.3 in 2012. Open Flow standard is managed by the 'The Open Networking Foundation' (ONF).

4.1 Openflow Switch:

SDN uses Centralized openflow switch because using one controller all the network devices can be connected and it is cost efficient. In the same way the distributed switch is defined as that it has many controllers and each controller is connected to any two of the network devices. This is more costly and so centralized openflow switch is preferred always[d].Controller/switch messages are initiated by the

Features: The capabilities of a switch are requested by the controller by sending a features request; features reply is responded by the switch.This is commonly performed when Open flow channel is being established. Configuration: The controller sets and queries configuration parameters in the switch[e]. The switch responds to a query only from the controller. Modify-State: The controller sends the Modify-State messages to manage state on the switches. Its primary purposes are delete, modify and add flow/group entries in the Open Flow tables. It also sets switch port properties. Read-State: the controller sends read-state messages to collect various information from the switch, like current configuration, capabilities and statistics. Packet-out: the packets are sent through a distinct port by the controller, and Packet-in messages are used to receive the forwarded packets.

IV. MININET:

Mininet is a software in which a network is created of switches, links, end-hosts and controllers. A collection of links, routers, switches, and end-hosts are run on a single kernel by mininet. The host of the mininet replicates just like an actual machine; the arbitrary programs are run when you ssh into it. The packets are sent by the programs which we run, with a given link speed and delay by Ethernet interface, which looks like a real one. This switch, middlebox, or router processes the packets. The performance should match that of the machines that are native, when two programs, like an iperf client and server, communicate through Mininet. In a nutshell, the real thing are the Mininet's virtual switches, switches, controllers, and links–hardware is not used to create them, instead software is used –and primarily it is same as the conduct of discrete hardware elements[f]. A mininet network is generally created exactly like the hardware network, vice versa, and the similar binary codes can be executed in either one of the platforms. Mininet doesn't have a strong conviction of virtual time; that implies that the measurements of the time must be based on the real time, and anything faster than that cannot be produced (e.g. 100 Gbps networks). The controller and the switch may communicate via a TLS connection. This connection is commenced by the
switch to the controller, which has a default location on TCP port 6633. The controller and the switch correlatively validate
by interchanging certificates which are signed by a private key. For validating the controller (controller certificate) and the other for validating to the controller (switch certificate), each switch must be user-defined with one certificate. Using plain TCP the communication between the switch and the controller is made.

V. PROPOSED METHOD:

The suggested method is with the usage of SDN with the help of Openflow protocol and its table we can find the destination and source easily[g]. The network devices are connected to the SDN controller to find the source and destination simply by using openflow table. The openflow switch is connected between the computers and all the openflow switches are interconnected among themselves. By using the mininet software and with the help of wireshark the output is found. By connecting the devices in the mininet software the packet transmission starts when the openflow protocol is chosed. After that the at the back end the wireshark software starts to capture the packets easily and the information column in the wireshark software gives through which protocol the packetis transmitted and the encryption used in the protocol is TLS algorithm, which is the best algorithm for encrytption and difficult to decrypt it using the keys. Openflow protocol is the best protocol that uses the three way handshaking as that of TCP which is the best way to transmit the packets.

VI. OUTPUT:

Output Of Normal Network:

From the figure 7.1, It is said that the network is normally connected using packet tracer for the comparison it with the SDN networks. In the traditional network, it is seen that to connect the network devices and uses certain protocols to find the shortest path and find the next hop using the destination address of the next router through which the cost is low chosen using RIP and OSPF protocols. There is many chance for the attackers to easily attack the network. So that the confidential information is difficult to transmit, for this purpose the technology have developed the SDN network.

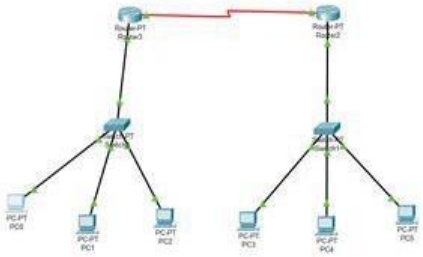

Fig 7.1 Output Of Normal Network.

Output Of Terminal Network:

From the figure 7.2, the comments are given in the terminal window and from terminal , the connection is given between the network devices such asuser 1(host)
, switches,routers and then it is straightly connected to the controller from the controller it is connected to the switches. The switches and routers were configured and then connected to the SDN controller. By establishing this connection through mininet the controller starts to control the devices and says the way through which it should reach the destination it follows the openflow table.

Fig 7.2 Output Of Terminal Network.

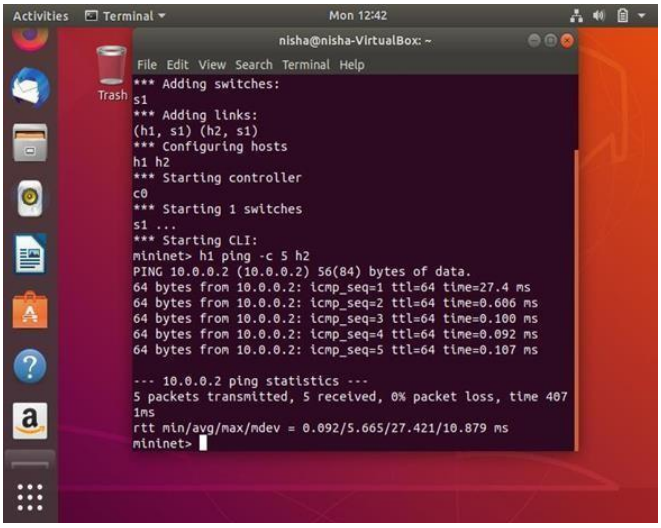

fig 7.4 output of wireshark window.

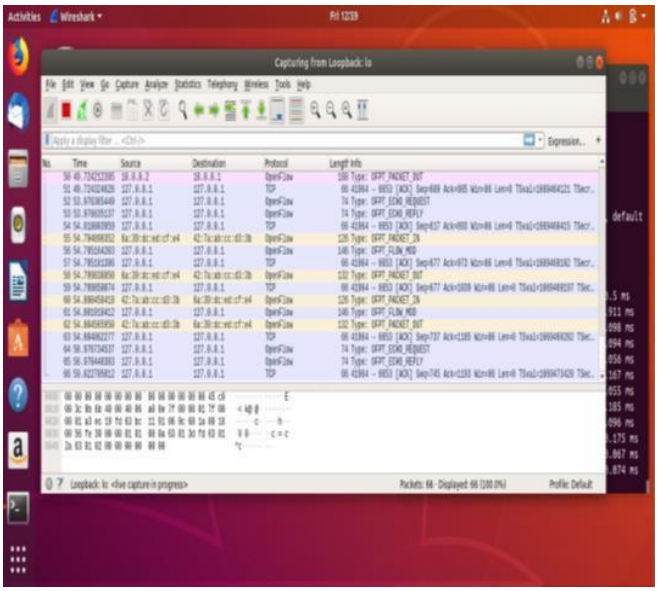

Fig 7.3 Output Of Terminal Window

From the figure 7.3, it can be clearly said that the connection has been established correctly and the reply has been sent from the user 2(server) also. This says that there is a secured connection between the openflow switch and the computers connected to it. It gives the statistics between the host and the server that the packet is encrypted and then decrypted in the server side and vice versa.

7.4 Output Of Wireshark Window:

Figure 7.4, shows that the packets have been transmitted using the openflow protocol and the information has received by the destination and it sends an acknowledgement to the host so that it clearly said that the packets has received safely to the destinated server and the reply is also got from it. This request and reply reveals the correct connection between the source and destination and there is no delay between them and no retransmission has occurred between them.

Figure 7.5, shows that the connection establishment have done correctly this shows the protocol which is done using open flow protocol and the packet have been sent request and reply comes from the destination correctly. The packet comes in and comes out from the destination port and vice versa. The MAC address from the source and destination of the encryption has been corrected properly.

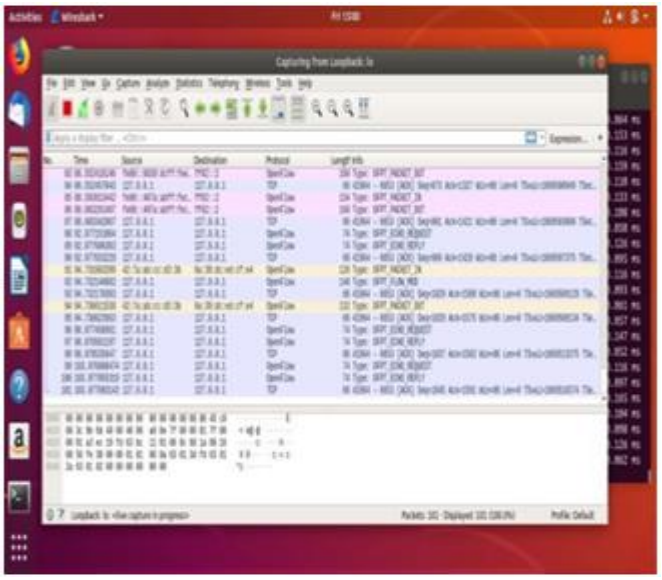

Fig 7.5 Output Of Wireshark Window.

VII. CONCLUSION:

A more testful issue is the barriers provided by the business challenges. The new technology threatens the existing conditions and also the best invention does not always win [h]. The networking hardware industry is immense – and for many decades its been growing which has built up using the same business model. On disaggregating software has been presented as the main concept in networking has turned out to be quite demanding for those to see this as a reason to delay. On the startup side, startup fundings can be very hard. To create a startup SDN ecosystem billions of dollars are required. This is the reason for the office-holders to win their game. The service providers revealed despondency that main commercial salesperson were not more communal to usher an answer to the market. So, OpenFlow remains at a critical point. The evolution in the community of open source is possible and it will be mastered by some rising new ventures. Service providers and large management are using this to bring their own results. Yet, prime networking trader will test, demonstrate, and document OpenFlow compatibility in their products.

REFERENCES:

1. D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, and G. Minden, “A survey of active network research,” IEEE Commun. Mag., vol. 35, no. 1, pp. 80–86, 1997.
2. B. Pfaff et al., “Extending networking into the virtualization layer,” in Proc. Workshop Hot Topics Netw., pp. 1–6, 2009.
3. N. McKeown et al., “OpenFlow: Enabling innovation in campus networks,” SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008.
4. K. Sood, S. Yu and Y. Xiang, “Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review,” IEEE Internet of Things Journal, vol. 3, no. 4, pp. 453-463, 2016.
5. H. Kobo, A. Abu-Mahfouz and G. Hancke, “A Survey on Software-Defined Wireless Sensor Network: Challenges and Design Requirements,” IEEE Access, vol. 5, pp. 1872-1899, 2017.
6. H. Zubaydi, M. Anbar and C. Wey, “Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller,” in Proceedings of PICICT, pp. 10-16, 2017.
7. Neghabi, N. Navimipour, M. Hosseinzadeh and A. Rezaee, “Load Balancing Mechanisms in the Software Defined Networks: A Systematic
8. and Comprehensive Review of the Literature,” IEEE Access, vol. 6, pp. 14159-14178, 2018.
9. D. Kreutz et al., “Software Defined Networking: A Comprehensive Survey,” in Proceedings of IEEE, vol. 103, no. 1, pp. 14-76, 2015.

AUTHORS PROFILE

Anshath Nisha P,Who is pursuing Final Year ECE in National Engineering College,Kovilpatti.

Jessica Priyadharshini P, Who is pursuing Final Year ECE in National Engineering College,Kovilpatti.