A Comparative Study on Conventional Network and Software Defined Network

** K. Khavya*
*** T. Vairam*

Abstract

Software Defined Networking (SDN) is the next big technology in networking. It decouples the network control plane from the forwarding plane and it has the central controller that is programmatic. The entire network is controlled by the central controller. SDN is automated, reliable, cost –efficient, agile, and dynamic in nature. This paper reviews the study on traditional network and SDN. The comparison is based on the different protocols used, firewalls, control plane, and few other basic parameters such as reliability, vulnerability, error control, architecture, and cost parameters. As a result of comparison, it is evident that SDN is more efficient than the traditional network architecture.

Keywords : Agile, central controller, control plane, dynamic, error control, firewall, forwarding plane, reliability, SDN, networking, vulnerability

I. INTRODUCTION

This review paper does a comparative study on traditional network and SDN and finds SDN to be the best suited technology in today's networking world because of reasons such as reliability, automation, cost effectiveness, high availability, more efficiency, and support for multi-tenancy in data centers.

II. TRADITIONAL NETWORK ARCHITECTURE

The traditional network architecture [1] is a static network design and it has the layered architecture approach called Open Systems Interconnection (OSI) that comprises of eight layers such as physical, data link, network, transport, session, application, and presentation, in which Layer 2 Data link and Layer 3 Network layer correspond to the networking functionality in the conventional network setup. The conventional network [2] has data plane (for data related task), management plane (for management and monitoring activities), and control plane (for co-ordination among the devices) on a single plane. The control plane is device-driven in nature since it uses protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Address Resolution Protocol (ARP), and Spanning Tree Protocol (STP). This led to a limitation in the technical and management plane. The network is monitored and controlled by network administrators. Any small updation in the network will be done manually by the administrators irrespective of the network size [3]. Organizations can deploy any of the topologies such as star, bus, ring, mesh, and based on basis of the need of the organization. Firewalls can be deployed on the network for security.

III. SDN ARCHITECTURE

SDN is an emerging architecture [4] that is automated, dynamic, manageable, and a cost efficient approach that decouples the forwarding functions, and the network control. SDN has the central controller that is programmable using APIs and essential software such that the controller controls the entire network via the program. It needs no or very less human intervention and it is cost

Manuscript Received: October 12, 2019; Revised: October 26, 2019; Accepted: November 7, 2019. Date of Publication: December 5, 2019.
* K. Khavya is PG Student at Department of Information Technology, PSG College of Technology, Coimbatore - 641 004, Tamil Nadu, India.(email id : khavyakannappan97@gmail.com)
** T. Vairam is Assistant Professor (Sl.Gr) with Technology, Department of Information Technology, PSG College of Technology, Coimbatore - 641 004, Tamil Nadu, India. (email id : tvairam@gmail.com)
DOI : 10.17010/ijcs/2019/v4/i6/150423

efficient [5]. The most prominent protocol used in SDN is Open flow. It is agile as it abstracts the control plane from the forwarding plane and it adjusts to the changing needs of the network. SDN is built on open standards such that it is vendor neutral and protocol independent [6]. The main advantage in choosing SDN is that it reduces the packet overhead as in a traditional network. Every packet is transmitted along with control information but in SDN only data is transmitted via data plane and the control information remains in the control plane. Link failures can also be easily identified in SDN but not in traditional network. So, there is a greater chance of packet failure in traditional systems. Fig. 1. Shows the comparison of conventional network vs. SDN architecture.

IV. RELATED RESEARCH WORKS

A. A Survey and a Comparative study on Software Defined Networking

Dawood et al. [7] reviewed the SDN architecture, different simulators, and performed a comparative study on conventional networks, and SDN architecture. They surveyed tools like NS3 and Mininet, where NS3 is used only for simulation and has the extension of Multi-Protocol Label Switching (MPLS) so that it can be deployed with various switches on open flow framework, whereas mininet can be used for research purposes. It is used to create virtual networks, hosts, and switches on computer/virtual machine/cloud. The parameters used in comparing conventional network and SDN are resource management, energy consumption, storage, security, programming and interfacing, and performance valuation. With this study, it is evident that SDN can be replaced with the existing conventional architecture for better results.

B. Comparative Analysis of SDN and Conventional Networks Using Routing Protocols

Gopi et al. [8] analyzed the working of routing protocols in SDN and traditional networks. The conventional network uses protocols like OSPF, BGP, and

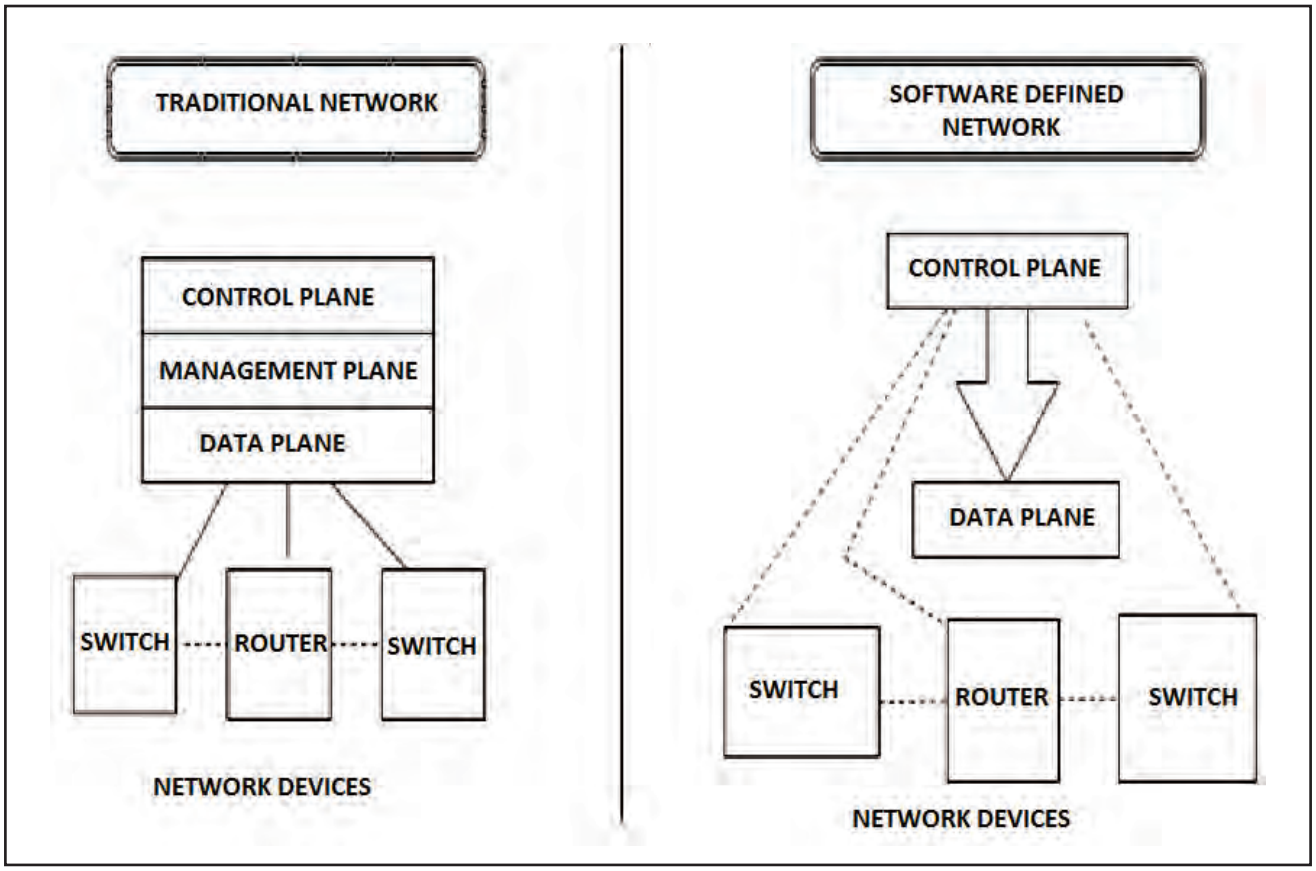

Fig. 1. Comparison of Conventional Network vs SDN Architecture

Routing Information Protocol (RIP) for routing the information, whereas SDN uses the forwarding mechanism of the SDN controller. In this work, the performance measures include calculating the convergence time during link failure irrespective of the topology and found that SDN produces good throughput compared to traditional network. Traditional networks are influenced by the type of network topology used. The experiments are carried out on mininet framework using Floodlight controller in SDN and in conventional networks packet tracer is deployed. This setup initially had the bandwidth of 10 Mbps with 0 link delay and the node size is scaled up from 8 to 80 and in all cases. The convergence time of SDN was minimal compared to conventional networks. Since the native network setup is influenced by topology, there was a delay in convergence time, but in SDN, it is dynamic. The routing table updation and topology updation is carried automatically in no time.

C. Comparative Analysis of Control Plane Security of SDN and Conventional Networks

Abdou et al. [9] compared the security of control plane in conventional network and traditional network. The comparison is given as follows. The control functions in layer 2 and layer 3 includes Address Resolution Protocol (ARP), whereas SDN uses host location learning for basic forwarding mechanism. The major attacks possible in conventional network are MAC table and ARP table poisoning and can be prevented by using Ticket-based ARP and voting based protocols, whereas in SDN, the major attacks can be host profile poisoning, link fabrication, spoofed link-manipulation messages, and Border Gateway Protocol (BGP), and it can be overcome by using MAC binding, host location validation, UNI filtering of control messages, and improving authentication and integrity. The results show that both conventional network and SDN are prone to attacks but in SDN it is easier to predict the chances of attacks and it can be recovered.

D. Bandwidth Management Using Software Defined Network and Comparison of the Throughput Performance with Traditional Network

Jimson et al. [10] correlated the bandwidth performance of conventional networks and SDN. The experimental setup in traditional network includes two simulations such as 11 nodes and 15 nodes respectively. In SDN, the experimental setup, Ryu controllers are used and it has two simulations that involve 13 and 17 nodes respectively. Both the setups include testing at sensitive traffic and non-sensitive traffic modes. The results prove that low bandwidth is used to carry sensitive data traffic. Moreover, in conventional network, the output is obtained as uneven bandwidth value and in SDN, the steady bandwidth is obtained for all topology, traffic, and network size. Table I shows the comparative study on traditional network and SDN.

TABLE I.
COMPARATIVE STUDY ON TRADITIONAL NETWORK AND SDN

FEATURES	REFERENCE NUMBER	TRADITIONAL NETWORK	SOFTWARE DEFINED NETWORK
Architecture	[12]	It is the static architecture and it pertains to traditional network setup with networking components like hub, switch, routers, gateway etc. which are employed for traditional Open Services Architecture (OSI) layers.	It has the traditional architecture setup. It has the central programmatic controller which manages the whole network, and data plane that takes care of the data that has been transmitted on the network.
Transfer of message	[12]	When the message has been transmitted from sender to destination, the message will be divided into chunks of packets. Each packet will be transmitted separately from initial sender to the destination. The shortest distance will be computed and on the basis of the algorithm adopted and routing table information, it will be updated by sending the message to the next nearest hop along with control information, and original data to be sent. This process repeats iteratively until all the packets reach the destination.	Similar approach is carried in SDN but the SDN controller will take charge of monitoring the packet flow. Once the message has been transmitted from the sender, the shortest distance is computed by the controller, and the packet is transmitted to the destination. This also involves the process of updating the routing table information for every packet that is transmitted. Here the packet does not contain the control information, so the transmission is faster.

Updation done	[12]	Any updation performed such as adding a node, assigning the IP address for the node, changing the router information, etc. is done manually by the administrator.	All the updations are carried automatically by the programmed controller.
Network management	[12]	Mostly all the work is carried out by the network administrator.	It involves less human intervention.
Cost of maintenance	[12] [13]	Initial installation cost is lower than SDN's cost but maintenance cost is higher than that of SDN.	Initial installation cost is higher but maintenance cost is much lower than SDN.
Payload cost	[12]	Every time the message is transferred, both the control messages and original messages are transmitted which increases the payload cost at every instance.	It has the controller for monitoring and maintaining the network, so only the original messages are transferred to the destination excluding the payload cost. So, the payload cost is reduced in this case.
Error control	[12] [13]	It takes a lot of time to check the error on the network manually.	It is much easier to check the error because of the programmatic central controller.
Reliability	[12]	Here, the shortest route is computed on the basis of the algorithm but it is not sure that the path chosen will have working nodes and links that function properly. The issues will be found only when the packet passes the defected node or link. Now, the path will be altered and there are a lot of chances that the packet may drop due to the Time To Live (TTL) field. Here, it involves human intervention to correct this issue when noted by the administrator.	The central controller is responsible for monitoring and managing every node in the network. If any deformed node is found on the network, the controller automatically repairs the node. While the data is being transmitted, the controller checks for the correctness of the nodes and links in path of transmission, and forwards the packet on a particular route. So, there is no chance of packet loss.
Vulnerability	[12]	Though firewalls are installed over the network, these are vulnerable since they require human intervention.	It has very less chance of being attacked since it is an automated process and machine does most of the task.
Authentication	[12]	It involves low authentication.	It has higher levels of authentication, and authorization to access every element on the network.
Presence of controller	[12]	It does not require the administrator to monitor the network every time. Periodic monitoring can be efficient.	It involves the availability of controller 24*7.
Coordination among network elements	[12] [13]	It is important that the elements participating in the communication interact with each other.	It is important that elements participating in the communication interact with each other and with the central controller.
Viewabilty	[12] [13]	It is difficult to have the entire view of the network.	It is much easier to view the entire network via the central controller.
Multi-Tenancy	[12] [13]	Traditional network may or may not use the multi-tenant approach but it involves Network Flow Virtualization (NFV).	SDN data centres support a lot of multi-tenancy so that they are more helpful for smaller work groups.

V. CONCLUSION

Thus, this survey work depicts the comparison between traditional network architecture and SDN. As per the discussion, SDN is found to be a better technology compared to traditional networking setup [6]. In SDN, automation is done using programmatic approach and the whole network is controlled by the programmed central controller. The disadvantage is that the whole network will collapse if the controller fails but there is a low chance that the controller will fail. The maintenance cost is lowered in SDN and it involves less human intervention. Small companies and orgaizations can bear the fruit of SDN via the multi-tenant approach with data center [10]. Hence, SDN as a booming technology can be used as an alternative to the existing traditional network system [11].

REFERENCES

[1]Wikipedia, *"Network architecture."* [Online]. Available: https://en.wikipedia.org/wiki/Network_architecture

[2] *"Traditional network versus SDN."*[Online]. Available: https://www.rfwirelessworld.com/Terminology/traditional-networking-vs-software-defined-networking.html

[3] "From static networks to software-driven networks - An evolution in process." 2016. [Online].Available: https://www.isaca.org/Journal/archives/2016/volume-4/Pages/from-static-networks-to software-driven-networks-an-evolution-in-process.aspx

[4] ONF, "Software Define Networking - SDN Definition." [Online]. Available: https://www.opennetworking.org/sdn-definition/

[5] CISCO, "SDN Definition by Cisco." [Online]. Available: https://www.cisco.com/c/en_in/solutions/software-defined-networking/overview.html#~stickynav=4

[6] Networklessons.com, "Introduction to SDN (Software Defined Networking)." [Online]. Available: https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-to-sdn-software-defined-networking

[7] M. A. Salam and A. S. Dawood, "A survey and a comparative study on software-defined networking," *Int. Res. J. of Comput. Sci*., vol. *177*, no. *6*, pp. 1-10, 2014.

[8] D. Gopi, S. Cheng, and R. Huck, "Comparative analysis of SDN and conventional networks using routing protocols," in *2017 Int. Conf. on Comput., Inform. and Telecommunication Syst. (CITS)*, pp. 108-112, 2017. Doi: 10.1109/CITS.2017.8035305

[9] A. R. Abdou, P. C. van Oorschot, and T. Wan, "Comparative analysis of control plane security of SDN and conventional networks," *IEEE Commun. Surveys & Tutorials*, vol. *20*, no. *4*, pp. 3542-3559, 2018. DOI: 10.1109/COMST.2018.2839348

[10] E. R. Jimson, K. Nisar, and M. H. B. A. Hijazi, "Bandwidth management using software defined network and comparison of the throughput performance with traditional network," in *2017 International Conference on Computer and Drone Applications*, pp. 71-76. Doi: 10.1109/ICONDA.2017.8270402

[11] Y. Hu, H. Li, and Y. Peng, "NVLAN: A novel VLAN technology for scalable multi-tenant data center networks," in *2014 Second International Conference on Advanced Cloud and Big Data*, pp. 190-195. Doi: 10.1109/CBD.2014.32.

[12] T. D. Nadeau and K. Gray, *SDN: Software Defined Networks: An authoritative review of network programmability technologies*. O'Reilly Media Inc., 2013.

[13] P. A. Morreale and J. M. Anderson, *Software defined networking: Design and deployment*. CRC Press, 2014.

About the Authors

K. Khavya is pursuing M.Tech (Information Technology) from PSG College of technology, Coimbatore. She completed B. E. (Computer Science and Engineering) in 2018. Her areas of interest include Cloud computing and networking.

Dr. T. Vairam is Assistant Professor with PSG College of technology. Her areas of interests are Internet of Things, wireless sensor networks, and SDN.