IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Software Defined Networking (SDN) Challenges, issues and Solution

Deepak Singh Rana[1*], Shiv Ashish Dhondiyal[2], Sushil Kumar Chamoli[3]

[1]Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India
[2]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India
[3]Department of Computer Science, Uttarakhand Sanskrit University, Haridwar, India

[*]*Corresponding Author: deepakranageu@gmail.com Tel.: +91-9719924551*

Available online at: www.ijcseonline.org

Accepted: 10/Dec/2018, Published: 31/Jan/2019

Abstract— IT infrastructure and its maintenance processes are changing in different organizations by the advent of cloud computing and may be able to eliminate their existing hardware. In traditional way of configuring a switch or routers may error-prone and cannot fully utilize the capability of existing network infrastructure. SDN is a way of providing programmability for network application development by its distinguished features decoupling the control plane from the data plane. In this paper we focused on the new concept in computer networking field, software defined network (SDN) and its challenges, issues, solutions. First, we provided and cover its basic model and software used to build a computer network with the help of software defined network mechanism then software tools used are listed, challenges and issues are described.

Keywords— SDN, OPENFLOW, Performance, Security, CDDA**.**

I. INTRODUCTION

As the name suggest software defined networking (SDN), it is a computer network which implemented, manage and made by a software (programmatically). It is a technology that implements the functionality of a computer network by specific software like OPEN-FLOW, CDDA etc. It is an approach in networking era/field where network is implemented, maintained programmatically with less number of physical components to facilitate the network requirement of any organization. Network troubleshooting and its performance is controlled and configured by this software which is defined for various purposes. Due to slow to change, expensive, limitations and variable IT requirements of traditional computer networks prevents many organizations form innovating the full value of their IT investments [1] software defined networking offers numerous benefits including on-demand provisioning, automated load balancing, streamlined physical infrastructure and the ability to scale network resources in lockstep with application and data needs [2].

Legacy network infrastructure is typically a mix of vendor solutions, platforms and protocol solutions making the ultimate goal of an integrated network ecosystem a difficult process for many organizations. According to Enterprise Networking Planet, it is feasible, though perhaps not optimal to implement software defined networking on existing physical infrastructure. Today the enterprise and large customers look to build new SDN infrastructure from the ground up [2].

SDN suggests centralizing network intelligence in one network component by disassociating the forwarding process of network packets (data plane) from the routing process (control plane).

The control plane consists of one or more controllers which are considered as the brain of SDN network where the whole intelligence is incorporated. However, the intelligence centralization has its own drawbacks when it comes to security [2][5] scalability and elasticity [3] and this is the main issue of SDN.

II. NEED OF SDN

In traditional networking system dedicated hardware devices like switch, router, firewall and any other devices like hub are configured manually by the IT system managers/administrators and are fully responsible for ensuring each device is updated with the latest configuration settings.

Traditional networking solutions are in steady decline because of new technology like cloud computing and virtualization in the market, by which we can have centralized data and operations to take place to give high availability and operations to end users.

SDN is new perspectives on how networks are managed, is rapidly becoming the go to solution for those who are having trouble overcoming the limitations of traditional networking, It is by decoupling hardware from software i.e. separating the control plane (which determines where to send traffic) from the data plane (which carries out these decisions and forwards traffic), SDN enables the hardware to be controlled/managed from a centralized software application that is separated from the hardware itself. Following are the three main focused need of SDN.

- Layered architecture with standard open standard Interface.
- It is more efficient since software can be easily developed by different vendors.
- Facilitate innovation in computer Networking, More flexibility with programmability.

III. BENEFITS OF SDN

1) Future ready infrastructure

Technology innovation moves fast. A flexible and scalable IT platform can mean the difference between keeping pace and just trying to keep up. SDN has the agility to use the latest cloud resources effectively and provides a framework to support data-intensive, real-time applications.

2) Reduced hardware costs

SDN uses the concept of software to build a network with minimum required hardware, it eliminates the need from manual support and configuration costs by using administrative efficiency and utilization of network is improved by using the concept of virtualization.

3) Centralized networking management

SDN has the capabilities to handle entire network form a single unit called central point, simplify the management, security of a network and allows distributing security and policy information consistently across any organization.

IV. DEVELOPMENT OF SDN

SDN software is continuously progressing Google, CISCO and different companies are focusing on the development of the SDN architecture and implementing in their different business locations. CISCO APIC-EM is an SDN controller or policy-based management and security through a single controller. Table below gives the development of SDN software based on the requirement.

Table1. Development of SDN

Year	Technology	Description
2011	SDN	Movement to decouple control and forwarding planes to enable innovation.
2012	OPEN FLOW	This is First standard interface for separating the network control and data planes.
2014	ONOS	Leading Open Source SDN Controller for Operators.
2017	CORD	Edge Cloud solution, with 70% of operators planning to deploy CORD to transform their networks.

V. ARCHITECTURE OF SDN

Architecture of the SDN describes how SDN works [5] in its various levels and how it maintains the software security and reliability. There are mainly three layers in software defined networking: Control, Data and Application.

1) Control plane: The powerful plane of an SDN network that carries signalling traffic and responsible for routing in the network. Packets are originated and destined for a router. Centralized configuration and management are the function of control plane of SDN. It is a logical entity in software defined network that receives commands/instructions from the application layer and transmits them to the networking components of SDN. The task of the controller is to extract useful information from the hardware devices and communicates back to the SDN applications with an abstract view of the network, including various activities happening in the network. Usually a software solution, the SDN controller resides here to provide centralized control of the router and switched that populates the data plane, removing the control plane from the individual devices. Different types of routing protocols like OSPF, EIGRP, RIP and BGP are managed by the control plane with IPv4, IPV6 and ARP.

2) Data Plane: It is like the physical layer of OSI model, consist of network elements like physical and virtual devices that deals with the data traffic. It is referred as the forwarding plane of SDN and is physically responsible for forwarding frames of packets from its ingress to egress interface using the protocols used by control plane.

3) Application Plane: Different application which are being used in a business to tell the network what to do based on the need of the business, controller use the APIs to pass the commands on router SDN switches etc. to perform the required task.

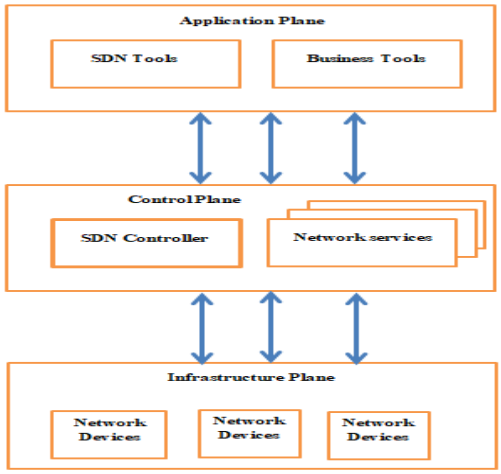

Figure 1: SDN architecture

VI. SOFTWARE USED IN SDN

To monitor and implement SDN various tools and language are used below the summary of software used is given.

Table 2. Various software tools used in SDN

Software	Type of tool	Brief working
ONIX	SDN initiatives, forming platform.	For distributed system for flexible computer network management.
VERIFLOW	Networking debugging tool.	Discovering the faults in SDN.
Routeflow	Routing architecture provide links between source and commercial product.	Inspired by SDN concept.
MININET	Virtual emulator provides environment for prototyping any SDN Idea.	Poor performance for higher level.
Frenetic	High level language for programming open flow architecture.	Consist query language SQL Syntax based, Stream Processing, Specification language.
Nettle	Function reactive programming.	Facilitate network management and support event driven networking.

EXAMPLE OF SDN USING MININET

Mininet is a simulation tool/software for the software defined networking (SDN) developed by Bob Lantz and Brian O'Connor, use the python API for network creation and very much suitable for designing a SDN for an organization. It is a network emulator which creates a network of virtual hosts, switches, controllers, and links, hosts run standard Linux network software, and its switches support OpenFlow for highly flexible custom routing and Software-Defined Networking. Mininet supports research, development, learning, prototyping, testing, debugging, and any other tasks that could benefit from having a complete experimental network on a laptop or other PC, provides a virtual test bed and development environment for software-defined networks (SDN).

Mininet mainly consist of:

a) **Isolated Hosts-** A group of user-level processes moved into a network namespace that provide exclusive ownership of interfaces, ports and routing tables.

b) **Emulated Links-** Linux Traffic Control (tc) enforces the data rate of each link to shape traffic to a configured rate. Each emulated host has its own virtual Ethernet interface(s).

c) **Emulated Switches-** The default Linux Bridge or the Open vSwitch running in kernel mode is used to switch packets across interfaces. Switches and routers can run in the kernel or in the user space.

Example:

root@mail:/home/gehumailserver#mn

mininet>nodes

available nodes are:

CONTROLLER-0 CONTROLLER-1 CONTROLLER-2 GEHU1 GEHU2 GEHU3 GEHU4 GEHU5 GEHU6 GEHU7 GEHU8 GEHU9 GEHU10 GEHU11 GEHU12 GEHU13 GEHU14 GEHU15 GEHU16 LAB1SWITCH LAB2-SWITCH LAB3-SWITCH LAB4-SWITCH SWITCH-L1 SWITCH-L2 SWITCH-L3

mininet> links

GEHU1-eth0<->LAB1SWITCH-eth1 (OK OK)
.....
GEHU5-eth0<->LAB2-SWITCH-eth1 (OK OK)
.....
GEHU9-eth0<->LAB3-SWITCH-eth1 (OK OK)

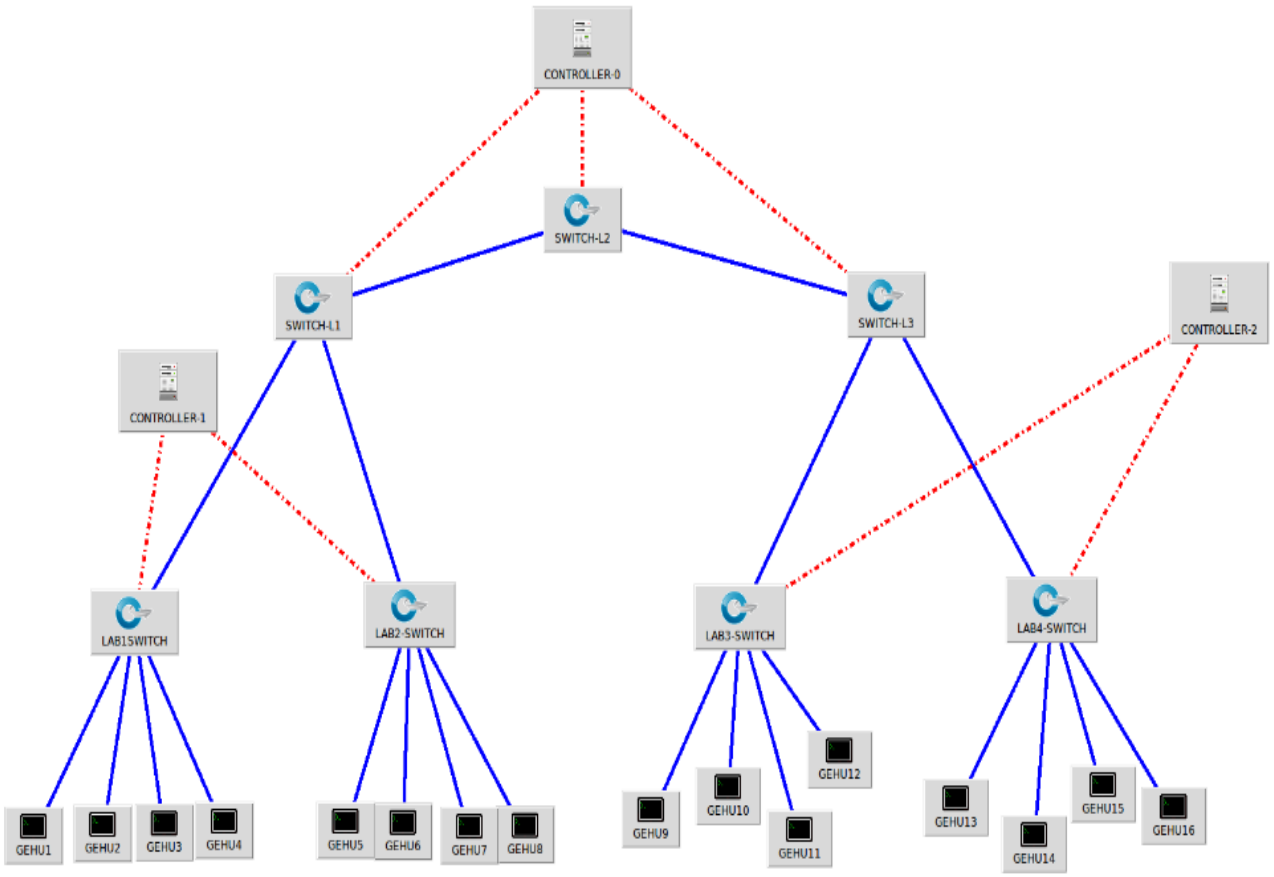

Figure 2: SDN setup in Mininet

.....
GEHU13-eth0<->LAB4-SWITCH-eth1 (OK OK)
.....
LAB1SWITCH-eth3<->SWITCH-L1-eth3 (OK OK)
.....
mininet> net
GEHU1 GEHU1-eth0:LAB1SWITCH-eth3
.....
GEHU13 GEHU13-eth0:LAB4-SWITCH-eth3
…….....

VII. RELATED WORK

State of the art research challenges: In [6] state of the art research challenges are given the aim of the research is to describe the benefits of using SDN in a multitude of environments such as in data centres, data centre networks, and network as service offerings, present the various challenges facing SDN, like scalability, reliability and security. **A Comprehensive Survey:** Authors in [7] present comprehensive survey on SDN in which they describe things from introduction to motivation for SDN, describe how SDN is differs from traditional networking and its roots. Analysis of the hardware infrastructure, southbound and northbound APIs, network virtualization layers, network operating systems (SDN controllers), network programming languages, and network applications is described in the research.

A Survey on Software-Defined Networking: Authors in [8] surveys latest developments in this active research area of SDN, present a generally accepted definition for SDN with the two-characteristic decoupling the control plane from the data plane and providing programmability for network application development and presents potential benefits of

SDN. A three-layer architecture, including an infrastructure layer, a control layer, and an application layer, and substantiate each layer with existing research efforts and its related research areas finally suggested open research challenges. **A Network in a laptop:** in this paper rapid prototyping for software defined networks is describe, creation of SDN [9] is done with the help of Mininet, interact with another network and customization of the network is done. **A Survey of Software-Defined Networking Past, Present, and Future of Programmable Networks:** Because of the evolution of SDN it is necessary to focus on programmable networks that simplify management of the network and enable innovation by adding the features in network programmatically. In [10] authors provide historic perspective of programmable network to recent developments, discuss current alternatives for implementation and testing of SDN-based protocols and services, examine current and future SDN applications, and explore promising research directions based on the SDN paradigm. SDN may be developed with the help of software like MININET, Nettle with proper software development life cycle, in [13] criteria and working structure of open source software is presented, different advantages and disadvantages are listed by the authors.

VIII. SDN CHALLENGES

Reliability: Reliability plays a major role in any software development, if any failure occurs in a system, its users should be informed, and solution must perform automatically. Reliability of software is the probability that it will work properly in a specified environment and for a specific amount of time. The configuration of SDN controller must intelligent and validate the network management to increase the availability of the network [3] so that errors can be prevented and handle. Authors in [4] studied the reliability of ONOS, a production-grade SDN controller, find a fault reports and found fairly consistent behaviour across the releases, in terms of number of bugs, fault detection and resolution time. When devices fail or stop working in legacy networks, network traffic is routed through alternative nearby path/nodes to maintain flow control and continuity. In SDN only central controller is in charge of whole network, if central network fails than whole network may stop working or collapse. To increase the network reliability vendors/developers of the software should concentrate on exploiting the main controller functions.

Scalability: The traditional LAN is deployed in a multi-tiered architecture in which Layer 3 routing functionality is used to connect multiple Layer 2 networks. These traditional LANs do not scale very well when supporting east-west traffic because at least one Layer 3 device, and most likely multiple Layer 3 devices, are in the end-to-end path. The traditional LAN is Scalability is an attribute that describes the ability of a process, network, software or organization to grow and manage increased demand. An SDN controller should be able to support a minimum of 100 switches. It must also be able to mitigate the impact of network broadcast overhead and the proliferation of flow table entries [3]. Scalability is the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged to accommodate that growth.

Low level interface: The control applications of SDN for network management, network policy should be developed, SDN framework needs to translate these developed network policies into low-level configurations of the switch used. The programming interface of the framework of the SDN must coordinate the multiple asynchronous events at the switches to perform even simple tasks.

Performance and Security: Open interfaces of the SDN network may bring new type of network attacks that may reduce the performance of the SDN. Security in cloud computing is described and different security issues and challenges are briefly discussed by the authors in [12].

Various D-DOS attack may down the working of networks. In [15] authors describe the SYN flood attack, which may down the server of any organization by exhausting the queue of the TCP protocol. To manage and solutions must be in SDN framework should be developed for the software integrity, remote access management, network threat detection and mitigation, authentication and authorization of the users.

ACKNOWLEDGEMENT

The authors would like to thank the reviewers for their careful examination of the research paper and valuable comments and suggestions which helped to considerably improve the quality of the paper. We are also thankful to the Management of Graphic Era Educational Society for always being supportive and for providing such a commendable research-oriented platform to us.

References

[1] https://www.ibm.com/services/network/software-defined.

[2] https://www.webopedia.com/TERM/S/software_defined_networking.html.

[3] Ashton, Metzler, and Associates, Ten Things to Look for in an SDN Controller, Technical Report, 2013.

[4] P. Vizarreta, K. Trivedi, B. Helvik, P. Heegaard, W. Kellerer and C. M. Machuca, "An empirical study of software reliability in SDN controllers," *2017 13th International Conference on Network and Service Management (CNSM)*, Tokyo, 2017, pp. 1-9.

[5] https://cdn.ttgtmedia.com/rms/editorial/HowSDNWorks-SoftwareDefinedNetworks-Ch4.pdf S. Willium, "Network

Security and Communication", IEEE Transaction, Vol.31, Issue.4, pp.123-141, 2012.

[6] Manar Jammala1, TaranpreetSingha, AbdallahShamia, RasoolAsalb, and YimingLic," Software-Defined Networking. State of the Art and Research Challenges," In Computer Networks, vol. 72, pp. 74–98, 2014.

[7] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015.R. Solanki, "Principle of Data Mining", McGraw-Hill Publication, India, pp. 386-398, 1998.

[8] W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, "A Survey on Software-Defined Networking," in IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 27-51, First quarter 2015.M. Mohammad, "Performance Impact of Addressing Modes on Encryption Algorithms", In the Proceedings of the 2001 IEEE International Conference on Computer Design (ICCD 2001), Indore, USA, pp.542-545, 2001.

[9] Bob Lantz, Brandon Heller, Nick McKeown, "A Network in a Laptop: Rapid Prototyping for Software-Defined Networks," in Hotnets-IX Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks Article No. 19.

[10] Bruno NunesAstuto, Marc Mendonça, Xuan Nam Nguyen, Katia Obraczka, ThierryTurletti, " A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks,"Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers, 2014, 16 (3), pp.1617 - 1634.

[11] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," IEEE Communications Magazine, vol. 55, pp. 80-87, 2017.

[12] Vishal Kadam1, Makhan Kumbhkar , Security in Cloud Environment, International Journal of Scientific Research in Computer Science and Engineering uter Science and Engineering uter Science and Engineering, vol-2,issue-3, June-2014

[13] Seema Rani, Kumari. (2018). Open Source Software: A Prominent Requirement of Information Technology. International Journal of Scientific Research in Network Security and Communication. 6. 24-29. 10.26438/ijsrnsc/v6i2.2429.

[14] Ashish Dhondiyal, Shiv & Singh Rana, Deeepak. (2018). Sleeping Mode MODLEACH Protocol for WSN. IJARCCE. 7. 112-116. 10.17148/IJARCCE.2018.7823.

[15] Rana, Deepak & Garg, Naveen & Chamoli, Sushil. (2012). A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations. International Journal of Computer Technology and Applications. Vol 3 (4), 1476-1480

Authors Profile

Mr. Deepak Singh Rana has done M.Tech (Computer science and Engineering), from Graphic Era University Dehradun, Uttarakhand, currently working as Assistant Professor in Department of Computer Science and Engineering, Graphic Era Hill University Dehradun, Uttarakhand, India. His research interest includes computer networks, Numerical Computation, Cyber Security, Malware Analysis and Design, Open Source Technology & ICT applications in Education. He has published various research papers and technical reports in International and national journals, he can be reached at deepakranageu@gmail.com.

Mr. Shiv Ashish Dhondiyal has done M.Tech (Computer science and Engineering), from Uttarakhand Technical University, He is Gold madelist in Mtech (CSE) 2016 batch. He is working as Assistant professor in Department of Computer Science and Engineering, Graphic Era Deemed to be University Dehradun, Uttarakhand, India. His research interests includes computer networks, Data Structure, Cyber Security, and Wireless Sencor Network. He has published various research papers in International and national journals. He can be reached at shivashis1234@gmail.com.

Mr. Sushil Kumar Chamoli has done M.Tech (Computer Science and Engineering), Currently working as assistant Professor, Department of Computer Science, Uttarakhand Sanskrit University, Haridwar, Uttarakhnad India. He is UGC-NET and GATE Qualified in Computer Science. His research interests are mobile adhoc network, operating system, Cloud computing. He can be reached at sushilchamoli@gmail.com.

