iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VII **Month of publication:** July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7111

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

SDN Networks Qualities, Application and Security Issues: A Survey

Meghna Gupta[1], Shivam Agarwal[2]
[1]*I.T. Department, IMS Ghaziabad (University Courses Campus), Ghaziabad, Uttar Pradesh*
[2]*Department of Information technology, Jims Engineering Management Technical Campus, Greater Noida, Uttar Pradesh*

Abstract: SDN (Software Defined Network) is the new technology in the networking which is used in various technologies which are used in now a days and in future references. Basically there is a need for a new network which gives better utilization, scalability, security and reliability. SDN network is used to control over the network in offline mode as well as online mode. In this paper we discuss the SDN qualities, application and its security.

I. INTRODUCTION

Conventional networking used the special algorithms which are implemented on hardware devices to control the data flow in the network and managing the routing paths. It also determines the how different devices are interconnected in the network. But in this conventional network all the routing paths and the algorithm are also defined before the packet is traverse in the network. A problem in this conventional methodology if the traffic is high then it poses severe limitations on the network. So there is a demand for security, scalability, network speed and reliability in the network, which gives better performance in increasing network traffic. Current network does not provide full flexibility due to routing rules which are hardwired implement. So there is a need to
Maintain the network in terms of hardware and software. So basically to maintain the networks form software SDN gives us a technique known as Open Flow which is helpful in maintaining the networks on online as well as offline. Open Flow is software on which the administrator can manage the packets of the network and decide the paths according to the situation or according to the available band width of the networks. Basically SDN will work on the cognitive radio. The cognitive radio is the technique in which the secondary users use the available band width which is available in the spectrum so that the data is transferred. So the utilization of band width is done and the through put of the spectrum is increases. So in this paper we first of all we know the quality and applications of SDN in section second. And in the third section we will study about the security of SDN networks.

II. SDN QUALITIES AND APPLICATIONS

So first of all we know about the SDN network qualities. So as we told you the description about the SDN network. Basically SDN works on two techniques first is Open Flow and second is Data flow. So the Open Flow is the platform where an administrative gives the commands and set the path of the network dynamically and Data Flow is the place on which these commands which are decided by the administrative are executed. So on open flow we set the network paths and data flow obeys the commands of the open flow. Now the qualities of SDN network will be discussed below.

A. Qualities of SDN Networks

1) *Intelligence and Speed:* SDN have a power to optimize the work load by the distribution of workload by powerful control panel. So when the work load is distributed then this is directly increased in the speed of the networks and the resource utilization is also increased.
2) *Easy Network Management:* in this we know that administrators have remote control over the SDN network so they can change the characteristics of the network such as connectivity and services of the network based on the work load which is present on the network. This makes the network more reliable and to maintain the quality of the network.
3) *Multi Tenancy:* The SDN can be expanded across multiple partitions of the networks such as data clouds and data centre. SDN can use decoupled control/data planes and resource visualization to well support cross-tenant data centre optimization.
4) *Virtual Application Networks:* In SDN if the administrator sees that there is a high work load on the network then the administrator implemented the virtual application network by using the distributed overlay virtual network (DOVE). This helps in better mobility and automation of the loads of the networks that have been virtualized.

©IJRASET: All Rights are Reserved

B. SDN applications

There are various applications on which the SDN networks use. Some of them are listed below.

1) *Internet Research:* We are using internet in our daily life, but the updating in the internet brings many challenges as it is constantly being used; so to solve the problem it is difficult to test new ideas and strategies on the existing network. But an SDN technology gives the features to testing ideas without changing the current network. In SDN the open flow help in distributing the control and data traffic to be separated. So it is very easy to spate hard ware and software. So due to this separation the SDN allow to experimenting with new addressing schemes so that new internet architecture schemes can be tested.
2) *Rural Connections:* SDN provides rural connections; SDN simplifies enterprise networks and complex data centres, so it can further be utilized to simplify rural Wi-Fi networks. The main issues in rural are sparse population, small profit margins and resource constraints, and others. SDN we can separate the configuration and constraints of a network by placing the control functionality in the central controller. So SDN makes the rural internet is more efficient than the other networks.
3) *Mobile Device Offloading:* SDN provides the privacy for business applications. Privacy is very important for the business application because people often work on data need to be kept secure. So SDN provides the privacy mechanism on which you can give access to only those devices which you want. And we can also restrict the data so that the data is also being kept secure.

III. SECURITY OF SDN NETWORKS:

The basic properties of a secure communication networks are: confidentiality, integrity, availability of information non-repudiation and authentication. So all these parameters are to be fulfilled for provide the security mechanism of any communication network. So if we want to secure the data which is in the network so first of all we have to secure the network so that no attacker can breach the network security.

For providing the security of SDN network first of all we have to know about the SDN framework. So the SDN framework is shown in the diagram. The SDN framework is made up of three layers, application layer, control layer and data plane layers.

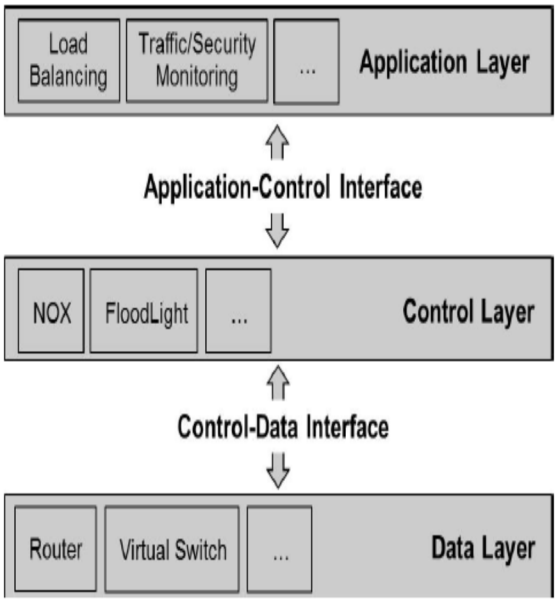


Fig.1. SDN Framework

So for showing the security challenges in every layer we describe these in a tabular format. In that table we see that which attack is done on which layer. So he table is shown below which shows the challenges of every layer in the SDN framework and the interfaces between the layers.

©IJRASET: All Rights are Reserved

Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
Unauthorized Controller Access			√	√	√
Unauthenticated Application	√	√	√		
Data Leakage e.g.					
Flow Rule Discovery (Side Channel Attack on Input Buffer)					√
Forwarding Policy Discovery (Packet Processing Timing Analysis)					√
Data Modification e.g.					
Flow Rule Modification to Modify Packets			√	√	√
Malicious Applications e.g.					
Fraudulent Rule Insertion	√	√	√		
Controller Hijacking			√	√	√
Denial of Service e.g.					
Controller-Switch Communication Flood			√	√	√
Switch Flow Table Flooding					√
Configuration Issues e.g.					
Lack of TLS (or other Authentication Technique) Adoption			√	√	√
Policy Enforcement	√	√	√		

The table shows the security issues on the layers of SDN framework and the interfaces between layers.
So in this we see that there are so many security issues on every layer of the SDN framework so we have to make the mitigation techniques to counter these attacks.

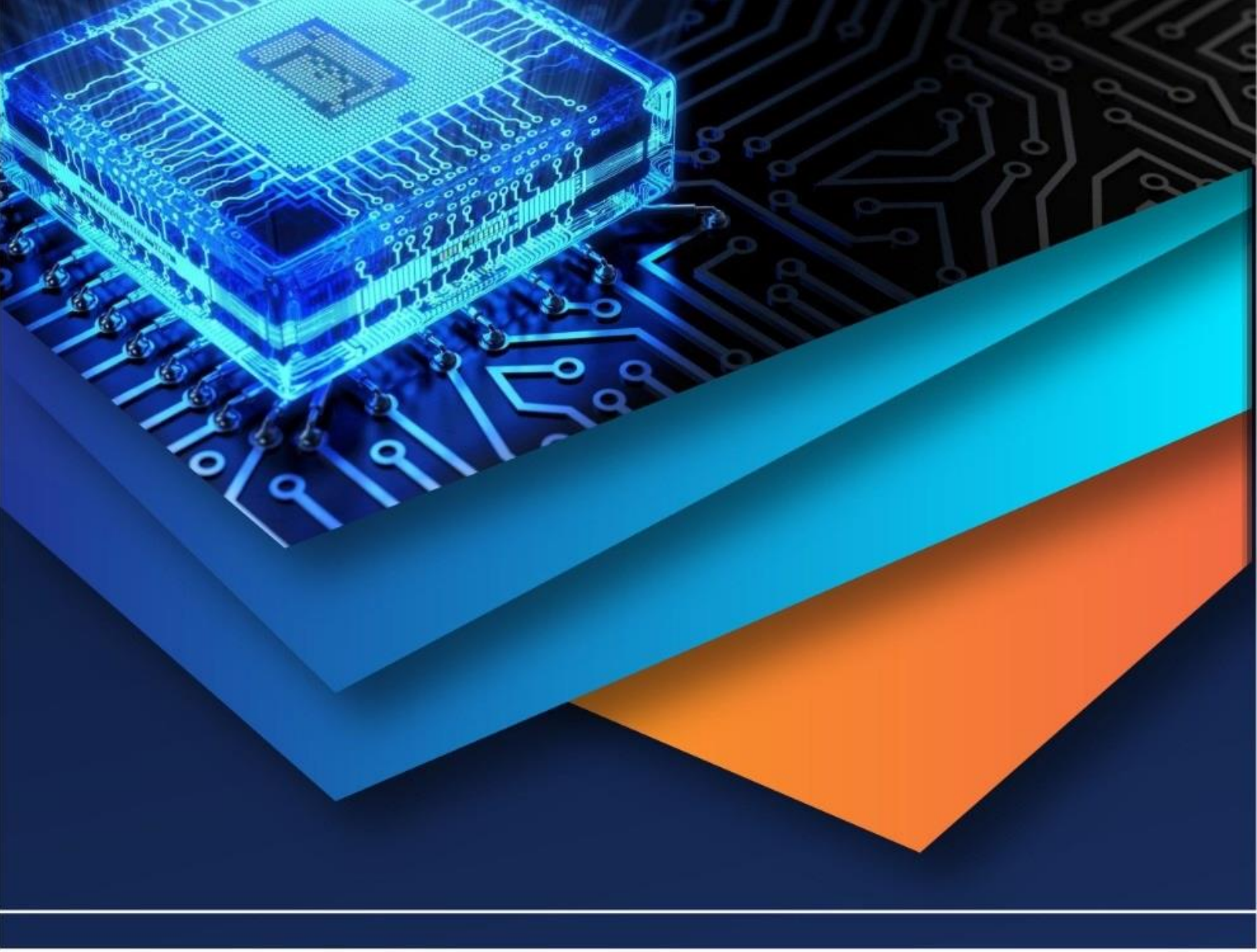
IV. CONCLUSION AND FUTURE WORK

In this paper first we know about the SDN networks and then the qualities of the SDN networks and some of the applications of SDN networks. Security issues of the SDN framework are also given in this paper.
In this we see that there are so many security issues which are on layers of SDN framework and the interfaces between the layers, so to mitigate these issues is a future work. Because SDN is widely used in coming days so we have to implement some security strategy to counter these attacks.

REFERENCES

[1] S. Ortiz, "Software-defined networking: On the verge of a breakthrough?" Computer, vol. 46, no. 7, pp. 10– 12, Jul. 2013.
[2] H. Kim and N. Feamster, "Improving network management with software defined networking," IEEE Commun. Mag., vol. 51, no. 2, pp. 114–119, Feb. 2013.
[3] K. Bakshi, "Considerations for software defined networking (SDN): Approaches and use cases," in Proc. IEEE Aerosp. Conf., Mar. 2013, pp. 1–9.
[4] S. Agarwal, M. Kodialam, and T. V. Lakshman, "Traffic engineering in software defined networks," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2211–2219.
[5] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, and M. Zhu, "B4: Experience with a globally-deployed software defined wan," in Proceedings
[6] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," Communications Magazine, IEEE, vol. 51, no. 7, 2013.
[7] "Network Functions Virtualization - Introductory White Paper," October, 2012. [Online]. Available: http://portal.etsi.org/NFV NFV White Paper.pdf
[8] C. Douligeris and D. N. Serpanos, Network security: current status and future directions. Wiley. com, 2007..

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)