Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2016, 3(5):92-94**

ISSN: 2394-2630
CODEN(USA): JSERBR

Research Article

Software-Defined Networking Concepts

Matthew N O Sadiku, Mahamadou Tembely, Sarhan M Musa

Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446

Abstract Software-defined networking (SDN) is a new computer networking architecture that uses standardized application programming interface. Traditional networking architectures have limitations which must be overcome to meet today's requirements. SDN promises to remove the limitations on current network infrastructure. This paper briefly introduces SDN as the next wave of networking.

Keywords Software-defined networking, OpenFlow protocol

Introduction

The needs of business have surpassed the network's ability to provide service. The rising demands for cloud-based mobility, social media, server virtualization, and big data services require a new approach. Software-defined networking (SDN) provides that approach. SDN addresses the failure of the traditional networks to support the dynamic, scalable computing and storage needs of today's applications. SDN achieves this by separating or decoupling network control from data forwarding. SDN is complemented by virtualization technologies such as network function virtualization (NFV).

The term software-defined networking was first used by Open Networking Foundation (ONF), which is a non-profit industry consortium founded in March 2011. The goal of ONF is to transform networking industry to software industry through SDN and promote standard development. ONF promotes the use of OpenFlow protocol. The OpenFlow is a standard interface between the control and data planes. Major commercial switch vendors such as IBM, HP, and Cisco have launched switching products that support the OpenFlow protocol. Google has deployed SDN in its data centers across the globe.

SDN features

The SDN simplifies the traditional networking in two ways. First, the network now consists of uniform switching hardware with standard interfaces. Second, network control is not distributed but centralized and restricted to the controller. The basic SDN architecture [1] is shown in Figure 1. SDN has the following key features.

Separation: There is a separation of the control plane from the data plane. This separation of the control and data planes allows one to experiment with network protocols. The data plane is responsible for the packet forwarding and the control plane performs other functions. In other words, the control plane makes decisions about where traffic is sent, while the data plane forwards traffic to the desired destination. The network switches/routers forward packets by following the flow table rules determined by the control plane. The control plane is programmable and is implemented in a centralized mode. Various applications may run on top of the centralized controller. It is felt that the shift to a pure software model brings flexibility, efficiency, and agility unknown in traditional networks.

*Programmability***:** SDN makes the network more programmable in that it allows various network functionalities to be implemented in software. This way it makes the network fully adaptable to the changing needs of the

users, network operators, and the applications. Programmability and automation of network resources enables service providers unlock new revenue opportunities, adapt to real time changes and reduce network complexity [2].

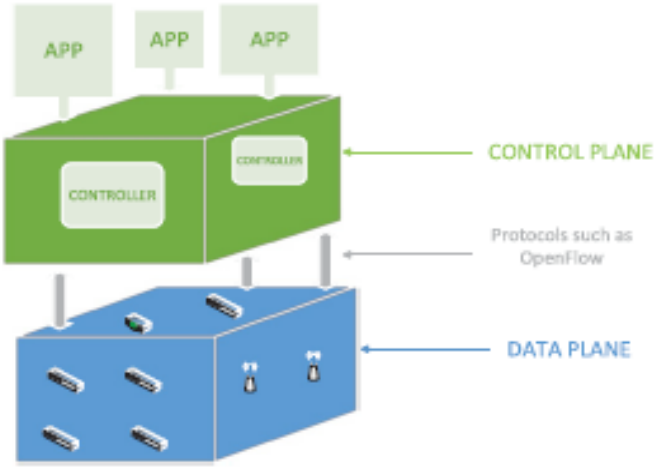

Figure 1: Basic SDN architecture [1].

SDN Security

Security is a major concern for SDN. SDN can be used to secure data offloading from mobile and handheld devices. While SDN can be leveraged to secure greater security for networks, it faces some major challenges securing itself. Due to the distinctive features of SDN, traditional network security approaches cannot be applied directly to it. The ability to programmatically control network behavior opens up possibilities for network security. Although it improves network performance, SDN creates some peculiar problems. The centralized control and programmability features of SDN introduce some new security challenges. For example, there is an increased potential for denial-of-service (DoS) attacks due to the centralized controller. OpenFlow is vulnerable to man-in-the-middle attacks when Transport Layer Security is not used. Network breaches may result when network controllers are shared by different users or applications [3]. It is important that SDN should be designed with security in mind right from the start. That implies that security issues should be identified and resolved to enable reliable wide area SDN deployment.

SDN Applications

SDN has been shown to be valuable in many applications. It has attracted a lot of attention in fields such as 5G mobile networks, cloud computing, wireless networks, data centers, optical networks, and Internet of Things (IoT).

Wireless networks: Most SDN solutions are based on wired networks. Recently, attempts have been made to adapt SDN to wireless networks. SDN provides a global centralized control of access points. An SDN controller can usually manage thousands of access points simultaneously. Several SDN controllers can be deployed when there is a large number of access points. Network administration in WiFi is mostly centralized. SDN concepts have been used to improve cellular networks. For example, the hidden terminal problem in wireless networks ceases to be an issue if transmission is centrally controlled.

Wireless sensor networks: Wireless sensor networks (WSNs) have benefited from the SDN approach. A typical WSN consists of a BS, which has the SDN controller, and sensor nodes. The control plane is decoupled from the data plane which runs the sensor nodes. A centralized controller uses OpenFlow to interact with the nodes. The nodes are often low powered and small. They are autonomous and adaptive to their environment.

Internet of Things: Everything in the world is being connected by the Internet of Things (IoT). SDN can be used in creating an IoT, which comprises of a large number of devices. SDN and network virtualization are the two key technologies that will enable IoT networks [4].

Optical Networks: Optical networks either maintain signals in the optical domain or use transmission channels that carry signals in the optical domain. Software-defined optical transceivers can be flexibly configured by

SDN [5]. SDN can be extended to the optical transport networks that interconnect data centers. Transport SDN enables efficient load balancing among widely dispersed data centers through a centralized controller.

Conclusion

As new technologies, such as IoT, cloud computing, and content delivery networks, emerge, the traditional network architecture becomes a handicap. Software-defined networking is the next wave of networking. It represents the next generation of infrastructure automation that is completely programmable and application-aware. It has generated a lot of interest from academia and industry.

Despite the proven benefits of SDN, there is significant reluctance in adopting it. Like any new technology, SDN has some disadvantages. These include controller redundancy and interoperability between devices from multiple vendors. Many organizations do not have the resources to invest in a new networking architecture. Comprehensive surveys on SDN can be found in [1,4-8].

References

[1]. N. A. Jagadeesan and B. Krishnamachari, "Software-defined networking paradigms in wireless networks: a survey," *ACM Computing Surveys*, vol. 47, no. 2, Nov. 2014, pp. 27:1-27:11.

[2]. S. Benington, "From embryonic to tectonic: SDN and the path toward industry transformation," *Lightwave*, May/June 2014, pp. 19-22.

[3]. S. T. Ali et al., "A survey of securing networks using software defined networking," *IEEE Transactions on Reliability*, vol. 64, no. 3, Sept. 2015, pp. 1086-1097.

[4]. N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of things: a survey," IEEE Access, vol. 4, 2016, pp. 5591-5606.

[5]. A. Thyagaturu et al., "Software defined optical networks (SDONs): a comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2016, pp. 1-49.

[6]. F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and OpenFlow: from concept to implementation," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, 2014, pp. 2181-2206.

[7]. Y. Jarraya, T, Madi, and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, 2014, pp. 1955-1980.

[8]. D. Kreutz et al., "Software-defined networking: a comprehensive survey," *Proceedings of IEEE*, vol. 103, no.1, January 2015, pp. 14-76.

About the Authors

Matthew N.O. Sadiku is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Mahamadou Tembely is a Ph.D. student at Prairie View A&M University, Texas. He received the 2014 Outstanding MS Graduated Student award for the department of electrical and computer engineering. He is the author of several papers.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.