International Journal of Engineering &Technology, 7 (3.12) (2018) 330-332

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Intrusion Detection on Software Defined Networking

Tella Nagarjuna Reddy[1], K.Annapurani Panaiyappan[2]

SRM Institute of Science & Technology, SRM Nagar
**Corresponding Author Email: [1]nagarjunatella22@gmail.com*

Abstract

Software Defined Networking and programmability on network have established themselves as current trends in IT by bringing autonomous operation with dynamic flow to network. Networks must be programmable, and it must be aware of the application in order to operate autonomously. Networks need to evolve to catch up with the current trends without losing their current status and operation, reliability, robustness, or security, and without distorting current investments. SDN is a transpiring network architecture where network control plane is distinguished from data plane and by that the network is directly programmable. This control, was initially bound in every network devices, enabled in the network to be abstracted for applications and services. Security is a major challenge for organizational and campus networks. The future of Internet depends on virtualization which is to provide numerous networks hosted the same physical hardware. This proposal takes a great advantage of the programmability provided by SDN to utilize Intrusion Detection System.

1. Introduction

The Implemented system is basically an Intrusion detection system in campus networks using SDN (Software Defined Networking). The potential to separate networks on basis software defined networking (SDN) has raised the bar. If in real world the campus network is intruded then how will SDN prevent it? SDN will deduce this condition with the help of Openflow. Currently, Openflow is a new network protocol. It is a standard for SDN in which the control plane and data plane of routing devices are separated. Therefore, Openflow provides a protocol to forward the information to different switches and routers. Anyone using the network can describe their respective routing table and utilize the network as per requirements.

Currently, there aren**'**t any practical experiments to conduct on novice network protocols (e.g.: routing protocols) with realistic scenario to obtain a satisfactory result that are required standardization. Every new idea within the networking community must be tested but with lack of resources they are not tried and tested. The need of virtual programmable network is rising. Virtual programmable networks can create the flow of new ideas, and innovation in the network. Current switches and routers are not based on open source platform, the only way is to either use virtual hardware or software.

This system will contain virtual network with few virtual hosts and virtual switches the hosts will be LINUX based Personal Computers. And with an Openflow controller to centralize the virtual network. Later this system can detect the malicious packets which are generated with help of Packet generator. The packets will be seized and analyzed with help of Wireshark which is Open source packet and protocol analyzer.

2. Existing System

Currently, there aren't any practical experiments to conduct on novice network protocols (e.g.: routing protocols) with realistic scenario to obtain a satisfactory result that are required standardization. Every new idea within the networking community must be tested but with lack of resources they are not tried and tested; thus it is believed that the networks are **"**fossilized**"**. The current network switches and routers have built-in resource intensive protocols. If the requirements need to change the performance and protocol then the switch or router has to be changed. And changing the hardware is very expensive and integrating it to the existing network is another mammoth task as all the hardware requirements are needed to be replaced accordingly to satisfy the requirements.

3. Proposed System

A. Why SDN: In established networks within corporate and government use network devices that consists of combination of control plane and data plane functions into the network hardware, mostly a switch or router. The control plane is a component of the router or switch which states how the network device communicate with other devices in the network. Illustration of control plane protocols can be shown by routing protocols, such as Open Shortest Path First, Border Gateway Protocol, and Spanning Tree Protocol. These protocols consists of the routing tables and port which lead to the data plane. These control plane protocols may work very well, and provide some network flexibility, but the limitations they pose are vital drawbacks.

Similarly, control plane protocols do not have any knowledge of the applications processing on the network, or how the application performance is effecting the network. Data plane functions consists of features like quality of service, encryption, Network Address Translation, and access control lists. These features directly affect data forwarding, and communication failures (packet dropping). Many of these features are static and they are determined by the configuration of the network devices. There is no way to convert the static features on basis dynamic conditions of the network and applications. The configuration of features is done on network topology, which limits the application of required functionality.

4. System Architecture

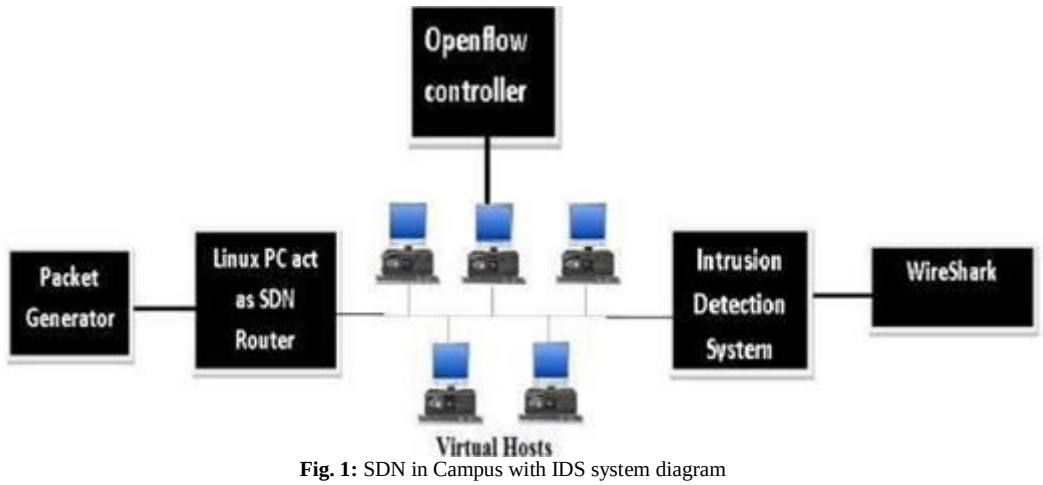

Fig. 1: SDN in Campus with IDS system diagram

5. Overall Description

The conventional Network architecture is a two layer architecture but with the help of SDN there is a separation between the control plane and data plane which introduces the third layer that is Abstraction layer. Thus with SDN it is a three layer architecture: Application Layer, Control Layer, and Infrastructure Layer.

A. Infrastructure Layer: The Infrastructure layer (data plane) is a segment of network that handles all the user traffic. The Infrastructure layer enables data transfer which handles multiple transactions through various protocols, and handles connections with help of remote peers. The conventional networks and SDN networks are unique in a way that in conventional networks all the layers and protocols are present in the firmware and the hardware present in the network but in SDN the control plane and data plane are separated which makes network administration becomes more easy and centralized.

B. Control Layer: The control layer is the part of a network that forms the network topology and is responsible for formation of routing tables. One of the main Function of control plane is to configure and manage the system. In SDN control layer is shifted on from hardware to software which enables the network programmability. With the help of network programmability the network administrator can configure the traffic through a centralized control accessing each and every switch or router present in the network. The administrator can set the priority on the routing which improves the performance on a whole.

C. Application Layer: The application layer is the part of SDN network architecture this layer mainly hosts the several network and business applications that are utilized by the organizations and campuses for the day-to-day operations.

D. SDN: Software-defined networking is an advance to computer networking which permits the network admins to manage network through abstraction of certain functionalities. An SDN differentiates the control and data planes which are present in the networking devices with the help of well-defined Application Programming Interface.

E. IDS: An intrusion detection system is a software application which monitors network and system activities to detect hostile activities or protocol contravention and formulates detailed reports to a management panel. The function of this system is to detect the intrusion in the network which will be virtually created with the

help of packet generator, then with the help of the system we will try to capture a hostile packet and review it.

F. OpenFlow controller: An OpenFlow controller is an SDN controller which operates on the basis of Openflow protocol. Its main function is to manage flow control in a SDN domain. The SDN controller portrays itself as an operating system (OS) of the network. All communications have to go through the controller. The controller uses the OpenFlow protocol to configure network devices and choose the best path for application traffic. The OpenFlow protocol established the basic communication in SDN that's why it is considered as a standard in a SDN network.

6. System Features

Software-Defined Networking focuses on the following key features:

1. Network control and Routing planes are Clearly decoupled.
2. Routing decisions are flow-based instead of destination-based.
3. The network forwarding logic is abstracted from hardware to a programmable software layer.
4. An element, called a controller, is introduced to coordinate network-wide forwarding decisions [4] Intrusion detection is one of the main issue for the network security. In this system we will test the system by generating the favorable and hostile packets. The user will be able to detect the hostile packets with other packets that are being reviewed by the IDS.

7. Future Scope

SDN can be a reliable for implementing an Intrusion Prevention System with Intrusion Detection System. For future work, we will study1 the reliability, robustness and efficiency of system, allowing various applications and IDS running on the network. A detail study on different types and nature of malware will improve the system with various defensive measures.

8. Advantages

1. Flexibility: SDN has shown us the flexibility it can provide by showing its operations and centralization. Users can program their own network according to their requirements.

2. Management: Managed Service Providers can use a single toolset to handle the network and its resources.

3. Planning: Visibility into network and its resources imply that organizations can utilize network more effectively for their business.

9. Conclusion

SDN promoted network virtualization, enabling network administrators to manage their networks with a centralized approach. May it be a real time situation or campus or organizational use, SDN advocacy can refine network statistics and properties. A detailed interface is available via the SDN controller, lending a hand in superior amalgamation and gradation among them. The fate of networking will lean on software. SDNs commitment is towards transforming current days invariable networks into adaptable, programmable rostrum with the insight to grant resources in a dynamic fashion, the robustness to support humongous data centers can only be done with the help of virtualization. With its many edge cutting features and staggering fabricating drive, SDN is going to be the new standard in vast domain of networks.

References

[1] "The Internet Protocol Journal" Volume 16, Number 1, March 2013.
[2] SDN reference website, "www.sdn.ieee.org", 2018.
[3] Richard Heady, George Luger, Arthur Maccabe, Mark Servilla, "The Architecture of a Network Level Intrusion Detection System", 1990.
[4] Seungwon Shin, Lei Xu, Sungmin Hong-Enhancing Network Security through Software Defined Networking (SDN) 2016
[5] Isolani PH, Wickboldt JA, Both CB, Rochol J, Granville LZ. Interactive monitoring, visualization, and configuration of OpenFlow-based SDN 2015
[6] SDX Central. Understanding the SDN Architecture"https: //www.sdxcentral.com/resources/sdn/i nside-sdn-archi-tecture/" 2016
[7] Mohd Abuzar Sayeed, Mohd Asim Sayeed and Sharad Saxena – " Intrusion Detection based on Software Define Network Firewall"- 2015