Conceptual Review of DoS Attacks in Software Defined Networks

Najmun Nisa
Faculty of Computer Science & IT
University Malaysia Sarawak
Sarawak, Malaysia
najam_nisa@comsats.edu.pk

Adnan Shahid Khan
Faculty of Computer Science & IT
University Malaysia Sarawak
Sarawak, Malaysia
skadnan@unimas.my

Zeeshan Ahmad[1,2]
[1]*Faculty of Computer Science & IT*
University Malaysia Sarawak
Sarawak, Malaysia
[2]*King Khalid University*
Abha, Saudi Arabia
zayshan@kku.edu.sa

Sehrish Aqeel
Faculty of Computer Science & IT
University Malaysia Sarawak
Sarawak, Malaysia
20010206@unimas.my

Jamil Asim
Faculty of Computer Science & IT
University Malaysia Sarawak
Sarawak, Malaysia
jamil.asim@uo.edu.pk

Shehroz Afzal
Faculty of Computer Science & IT
University Malaysia Sarawak
Sarawak, Malaysia
shehrozafzal347@gmail.com

2022 Applied Informatics International Conference (AiIC) | 978-1-7281-8428-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/AiIC54368.2022.9914598

Abstract— ***Software-defined networking (SDN) is a new developing technology that has been widely adopted by businesses because of its low cost and greater innovation in networks specially Scaling or manually configuring physical infrastructure. This makes it easier to design networks and manage huge networks. Scaling or manually configuring physical infrastructure is a problem for older networks, which cannot keep up with today's rapid technological advancements. Another important issue is the lack of information and the absence of a skill set or experienced experts required with technological expertise, which is very much concerned about the current situation. For this reason, a software-defined network architecture has been developed that allows for a more flexible network that can be reconfigured to meet changing needs. However, there are also other security concerns to consider especially the controller's security. In this paper, we examine the impact of Denial of Service (DoS) attacks on the SDN controller and different mitigation techniques to overcome these attacks. The research effort also points out possible future research on this topic, as well as its limitations.***

Keywords— Denial of Service (DoS), Flexible network, Security attacks, Software-defined Networking (SDN),

I. INTRODUCTION

In the near future, the globe will experience a new technological revolution. The Internet is only a few years away from connecting billions of "things" that can communicate with one other from anywhere. As most devices are proprietary, it is impossible to change or improve their functions. As networks grow in size, these characteristics make it difficult for cloud service providers to tailor and optimize network resources to meet specific customer demands [1]-[3].

The unique network design known as SDN (software-defined network) allows networks to be virtualized. By decoupling data and control planes, new network applications may be developed and deployed more quickly, as well as equipment upgrades can be made independently. In comparison, the network switch is just responsible for transmitting data, and the centralized controller is only responsible for controlling that data. Network programmability, which makes it easier to roll out new services, is another benefit of this type of network design. As a drawback, it gives rise to new ways of attacks on the network. [4]-[6].

II. BACKGROUND: OVERVIEW OF SDN ARCHITECTURE AND ITS LAYERS

Managing and controlling a network is a difficult challenge for network administrators. To maintain a secure network with a high degree of functionality, network devices must provide low-level configurations that enable the execution of complex tasks. In addition, we are unable to implement many earlier suggestions and improvements because of our inability to alter the operation of the underlying architecture. Network administrators in the early 1990s studied traditional networks and incorporated programmability, which led to active networks. When central network control learned that present networks lacked the applications that powered them, they redesigned their functions, and SDN architecture was developed because of the need for rapid network updates, cloud computing, virtualization, and device configuration. Since data forwarding and control logic are separated in SDN, network control and applications may be programmed independently [7]-[8].

Flow table management, load balancing, routing options, attack and virus detection, and other network functions are made possible by the cooperation between both the control and data planes. OpenFlow is the protocol that is used to communicate between the two planes. The control plane comprises all of the logic and devices that govern how and where data from the data plane should be transferred.

The data-plane of a network oversees everything that has to do with data, from how it is handled to how it moves around the system. Security is supplied at the node level through the use of software-defined networking (SDN), which replaces firewall policies with flow rules created at the individual switch level. Controllers can maintain a global perspective of the network as network devices degrade to the level of packet-forwarding devices under the supervision of SDN technology. To offer a comprehensive picture of the network, OpenFlow, a defined protocol, is employed [10]-[20]. With the Open Flow protocol, a server may identify the