Chapter 23
A Survey on Intrusion Detection System for Software Defined Networks (SDN)

Yogita Hande
GITAM University, Andhra Pradesh, India

Akkalashmi Muddana
GITAM University, Andhra Pradesh, India

ABSTRACT

Presently, the advances of the internet towards a wide-spread growth and the static nature of traditional networks has limited capacity to cope with organizational business needs. The new network architecture software defined networking (SDN) appeared to address these challenges and provides distinctive features. However, these programmable and centralized approaches of SDN face new security challenges which demand innovative security mechanisms like intrusion detection systems (IDS's). The IDS of SDN are designed currently with a machine learning approach; however, a deep learning approach is also being explored to achieve better efficiency and accuracy. In this article, an overview of the SDN with its security concern and IDS as a security solution is explained. A survey of existing security solutions designed to secure the SDN, and a comparative study of various IDS approaches based on a deep learning model and machine learning methods are discussed in the article. Finally, we describe future directions for SDN security.

1. INTRODUCTION

With the fast development in computer system and the boost in the network, demand requires more network systems deployment. The huge number of system deployment may lead to many complex attacks over the network and raises the need for powerful security mechanisms. Many researchers and industries have expressed interest in designing efficient security solutions to the network (Mukherjee et al., 1994). The modern approach of networking such as SDN abolishes static and distributed nature

DOI: 10.4018/978-1-7998-7705-9.ch023

of the legacy network. The centralization characteristics of SDN can result in an efficient and reliable network, but security is a major concern. To secure the network from unauthorized access, groups deployed a firewall, antivirus software, and an intrusion detection system (Aburomman & Reza, 2017). A firewall blocks outside attacks on the network and are not enough to secure network completely from attacks. This is where the Intrusion Detection System (IDS) comes into the picture (Aydin et al., 2009). Currently, machine learning approach is applied to IDS, however, deep learning approach have also been implemented in IDS field. This paper describes the various Intrusion Detection System designed for SDN. The paper is ordered in the following behavior. Section 2 offers a brief overview of SDN. Section 3 covers various network attacks and IDS security mechanism and also parameters essential for IDS performance evaluation. Section 4 provides a brief on the ML/DL approach. Section 5 gives a survey on different security solutions applied to the SDN environment, and, comparative study of various ML/DL based SDN IDS with their operational functionality and performances. Section 6 represents research implication carried out from the survey.

2. SOFTWARE DEFINED NETWORKING

The network is comprised of a number of devices which are connected to share the information from one place to another. One good example of a network is the internet. The Internet-based, business organizations and industries need to change their network configurations dynamically according to their business requirements. To achieve these changes over the traditional network is the one biggest challenge. The complex traditional network creates a barrier for data centers to innovate new services, interconnect different data centers, interconnection with enterprises, etc. A new approach needs to be looked at to overcome these issues. This is where software defined network (SDN) comes to manage and configure the network as per industry business needs from a central location through programming.

In a traditional network, the main components of a device are data, management, and control plane. However, the control plane is responsible for routing, i.e. to identify the path to transfer the data towards the destination using routing algorithms. The data plane may also be referred as the forwarding plane, as it is accountable to send the network traffic to the next node along the path selected by the control plane for the respective destination. The management plane helps to manage both the control and the data plane. However, in such traditional network, the data and the control plane is combined in a single physical device (router). The control plane will be effectively separated from data plane in the SDN network (Kreutz et al., 2015) and acts as a centralized software controller. Therefore, the controller provides programming functionality that allows a supervisor to organize and manage the network as per needs. SDN network having centralized control plane provides a global view, such that the flows are planned based on defined network policies to support traffic engineering, security, load balancing, etc. (Hayward et al., 2015). The following Figure 1 illustrates the architecture of SDN.

The typical SDN architecture consists of Infrastructure layer, as control layer and application layer. SDN uses different interfaces such as Northbound Interface and Southbound Interface to communicate amongst the planes. The Northbound Interface (NBI) is used among the application and the control layer, whereas the south bound interface (SBI) allows the control layer to communicate with the data layer and vice a versa. One of the popular Northbound Interface is REST API and Southbound Interface is openflow. Moreover, openflow protocol allows the SDN implementation in hardware and software environment. The controller is a vital part of the SDN network, which is otherwise referred as the net-