Chapter 45
The Usage Analysis of Machine Learning Methods for Intrusion Detection in Software-Defined Networks

Derya Yiltas-Kaplan
Istanbul University – Cerrahpaşa, Turkey

ABSTRACT

This chapter focuses on the process of the machine learning with considering the architecture of software-defined networks (SDNs) and their security mechanisms. In general, machine learning has been studied widely in traditional network problems, but recently there have been a limited number of studies in the literature that connect SDN security and machine learning approaches. The main reason of this situation is that the structure of SDN has emerged newly and become different from the traditional networks. These structural variances are also summarized and compared in this chapter. After the main properties of the network architectures, several intrusion detection studies on SDN are introduced and analyzed according to their advantages and disadvantages. Upon this schedule, this chapter also aims to be the first organized guide that presents the referenced studies on the SDN security and artificial intelligence together.

INTRODUCTION

Software Defined Network (SDN) architecture is one of the most recently emerging technologies. SDN is described in 2004 by various researchers in the universities of Princeton, Carnegie Mellon, Stanford, and California as its current concept. Its standards have been designed in the last few years.

Inside the traditional computer networks, each device such as router or switch is responsible from the routing and forwarding operations nearby their packet traffic controls. By this way, a traditional network covers the data, control, and management planes in each device. Here the data plane manages the incoming data, the control plane covers the protocols which construct the routing tables, and the management

DOI: 10.4018/978-1-7998-7705-9.ch045

plane follows and changes the functions of the control plane. On the other hand, an SDN diversifies the control and data planes by embedding the control part inside a central element called controller. In this architecture, router/switch devices do not make any process between each other. Instead, each router/switch is connected to the controller and sometimes gets a decision from this controller device. Such centralized structure provides SDN with the advantages of flexibility, high programmability, security, and fast configuration.

The controller in an SDN structure is the main part that manages the network operations. This part is programmable and can be constructed by different software tools. A controller is related with some designations of new services and obtainment of the functions. Some present controller software can be listed as Beacon, Floodlight, NOX, ONOS, POX, and Pyretic. The most widespread one is the Floodlight. The controller software can be implemented for deciding the routes for the packet flows, realizing the network monitoring, managing the flows and other network processes. The researchers say that SDN provides all networking operations by the help of the centralized software part—controller without any requirement of some configurations on other network devices.

Several network operations such as intrusion detection, routing, firewall filtering, and flow forwarding are examples of the tasks of an SDN controller. This chapter is related to the intrusion detection part and analyzes this task based on the studies including machine learning methods. In the literature there is quite limited number of papers that present SDN and machine learning collaborations, of which only some of them give attention to the SDN security issues. The collaboration between SDN and machine learning has only been used for proposing some methods in the security area. This chapter is the first analysis report on the referenced studies with defining the methods by giving their computational success rates as a strong capability.

As a summary of this chapter, the main definitions about SDN structure are given. It is because, without understanding the SDN, one cannot investigate the literature deeply. Nearby SDN, the background about intrusion detection systems and machine learning methods is also explained. After that part, several current studies that give a connection between SDN and machine learning methods are analyzed. The main objective of this chapter is to give a literature review based on comparing the merits and demerits of different methods used in the machine learning phases. At the end, this chapter gives some deficiencies as unsolved problems in the literature of the SDN studies including the machine learning methods.

BACKGROUND

Software Defined Network

SDN is one of the most recent technologies in the area of computer networks. The main parts in an SDN cover the same devices as in traditional networks with a diversity in the functions of the recent devices and an additional controller part inside the new structure. The difference between switch connections on the architecture of a traditional network and that of an SDN can be easily observed from Figures 1-2.

Figure 1 shows that the switches in a traditional network communicate with each other. There are also data and control functions together inside each switch. This means that the switches have several abilities such as giving route directions to the packets and changing some packet transmission rules.