


Flow-Based Anomaly Detection Using BNN for Attack Mitigation on SDN

Nang May Phu Lwin, University of Computer Studies, Mandalay, Myanmar*

 <https://orcid.org/0000-0002-7425-2767>

Su Thawda Win, University of Computer Studies, Mandalay, Myanmar

ABSTRACT

Distributed denial of service (DDoS) attack remains one of the major issues that compromises the resources and services of the components in software defined network (SDN) environments. The implementation of intrusion prevention system (IPS) in OpenFlow-based SDN architecture has emerged to strengthen the security mechanisms by exploiting the concepts of SDN and OpenFlow protocols. This article provides the anomaly detection of the live traffic flow with backpropagation neural network (BNN) for the online detection and mitigation of DDoS attacks. The dataset from the testbed is used to emulate the efficiency of the proposed method. The results achieve more than 90% detection accuracy with less than 6% false alarm rate. CPU utilization on the centralized controller is also measured by means of SYN and UDP flooding to calculate the effect of malicious traffic on the resources of the system.

KEYWORDS

Backpropagation Neural Network, Distributed Denial of Service, Intrusion Prevention System, Network Security, OpenFlow, Software-Defined Networking

INTRODUCTION

The public and private cloud have gain popularity in recent years. The complexity of network infrastructure is rapidly increasing in deployment. The existing traditional networks, on the other hand, have become very slow and too complex. This would make it harder for network administrators to manage and maintain the network, in the context of modification for rapid innovation and cost-efficient development. Open Network Foundation (ONF) developed a new approach called Software-Defined Networking (SDN) in 2011. SDN is an innovative network architecture in which the control planes are decoupled from the data planes of every network device within the network. The control logic of every networking device shifts to the centralized control units that are located at the control plane within the network. The data plane consists of the simple packet forwarding devices that execute the instructions from the control plane and traffic forwarding. The most widely used protocol in SDNs is OpenFlow. SDN enables the programmability to directly control the networks, centrally manageable that make more flexible and simpler troubleshooting. SDN becomes popular in both academic and industrial research. SDN enables dynamic and scalable ways to manage the networks.

Although SDN can have many advantages, it still has certain challenges to overcome, such as scalability, performance, and security. The most challenging issue is security. According to Kreutz et

DOI: 10.4018/IJSST.304072

*Corresponding Author

al., (2013), seven kinds of threat vectors target SDN components and the communication between them. The DDoS attack is one of the utmost challenges and has the highest impact in SDN environments for its centralized control nature. CAIDA, DARPA, KDD, and NSLKDD are the standard datasets used by the researchers for Intrusion Detection System (IDS) in both SDN and traditional networks. The features in these datasets are generalized traffics collected from network simulation or laboratory. Therefore, specific features are essential to improving classification accuracy. For traffic generation, normal, DDoS, LAND, and Smurf attacks, traffic are generated in their previous work (Lwin et al.,2021). Due to the flow-based nature of SDN, the authors proposed hybrid IPS, Snort with the flow-based anomaly approach. Six specific features are extracted from the flow and stored as a labeled dataset. The authors used the error backpropagation algorithm to train and evaluate their model by accuracy, false alarm rate, and detection rate. For real-time DDoS prediction, the controller will collect flow statistics from switches suspected of that on the attacker's pathways.

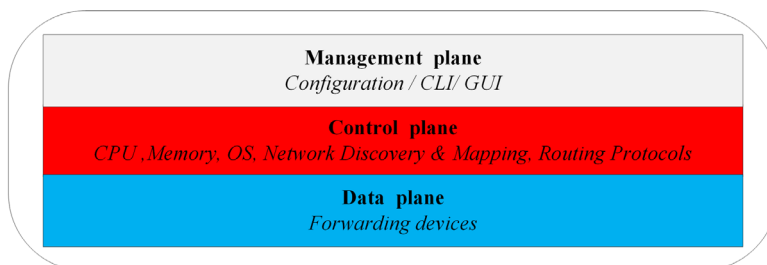
This article provides flow-based anomaly detection using Backpropagation Neural Network (BNN) on SDN environments. The rest of the paper is organized as follows. The theoretical background is introduced in the second section. Related works are presented in the third section. This article gives the design and evaluation of flow-based anomaly detection in the fourth section. The conclusion is done in the final section.

BACKGROUNDS

Software-Defined Networking

The traditional networks are built on proprietary devices with embedded software to manually configure for high-level policy by using lower layer controls and vendor-specific configuration. The functions are segregated into three discrete categories: the management plane, the control plane, and the data plane, which are bundled inside of devices vertically, as in figure 1. As the control and data planes are tightly coupled, the existing traditional networks have become very slow and the development of new functionality is costly. In 2011, ONF addressed this problem with an approach, Software-Defined Networking (SDN).

Figure 1. Structure of the traditional network devices



SDN is a network paradigm that separates the control plane from the network devices. It also supports the logical centralization and programmability of the network services. SDN is directly programmable, centrally manageable, and vendor-neutral. SDN is comprised of application, control, and infrastructure layers, as shown in figure 2. The first one implements the network functionalities such as routing algorithms, security, network policy management via programmable interfaces and communicates with the SDN controllers via northbound Application Programming Interface (API). The second layer maintains the global map of the entire network. The network operating system usually runs on the controllers within the control plane. Due to its logically centralized nature, SDN provides abstractions for the application layer and communicates with the forwarding devices of the infrastructure layer via southbound APIs. The standard southbound protocol is OpenFlow. The third layer is also known as the data plane, where traffic data are

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/flow-based-anomaly-detection-using-bnn-for-attack-mitigation-on-sdn/304072

Related Content

Linear Discriminant Analysis

David Zhang, Xiao-Yuan Jing and Jian Yang (2006). *Biometric Image Discrimination Technologies: Computational Intelligence and its Applications Series* (pp. 41-64). www.irma-international.org/chapter/linear-discriminant-analysis/5919

Integration of Gaussian Processes and Particle Swarm Optimization for Very-Short Term Wind Speed Forecasting in Smart Power

Miltiadis Alamaniotis and Georgios Karagiannis (2017). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 1-14). www.irma-international.org/article/integration-of-gaussian-processes-and-particle-swarm-optimization-for-very-short-term-wind-speed-forecasting-in-smart-power/205541

Privacy in Identity and Access Management Systems

Andreas Pashalidis and Chris J. Mitchell (2012). *Digital Identity and Access Management: Technologies and Frameworks* (pp. 316-328). www.irma-international.org/chapter/privacy-identity-access-management-systems/61542

Before Smart Phones and Social Media: Exploring Camera Phones and User-Generated Images in the 2000s

Bilge Yesil (2017). *Biometrics: Concepts, Methodologies, Tools, and Applications* (pp. 480-500). www.irma-international.org/chapter/before-smart-phones-and-social-media/164616

An Enhanced Computational Fusion Technique for Security of Authentication of Electronic Voting System

Adewale Olumide Sunday, Boyinbode Olutayo and Salako E. Adekunle (2020). *International Journal of Smart Security Technologies* (pp. 22-37). www.irma-international.org/article/an-enhanced-computational-fusion-technique-for-security-of-authentication-of-electronic-voting-system/259322