The 3rd International Multidisciplinary Information Technology and Engineering Conference 2021, Windhoek, Namibia, 23 - 25 November 2021

A review of intrusion detection techniques in the SDN environment

Sebopelo, R; Isong, B; Gasela, N; Abu-Mahfouz, Adnan MI

Abstract:

Despite the advantages of Software-defined networking (SDN) over the traditional networks, SDN is facing several challenges such as security threats and attacks, dominated by a distributed denial of service (DDoS) attacks that target the controller. In recent years, the SDN has witnessed several research attentions leading to proposals and the development of countermeasures such as intrusion detection systems (IDS). IDS plays a critical role in detecting and preventing malicious activities on the networks. Several detection techniques have been exploited for the effectiveness of the IDS such as pattern matching, anomaly-based and specification-based. With the nature of SDN architecture, flow-based anomaly detection has been effective and commendable. Therefore, this paper conducted a review of some of the IDS schemes in the SDN environment. It was aimed to identify the solution offers, techniques, challenges and provide research directions. The findings show that IDS in the SDN is an active research area and several techniques exist and are dominated by machine learning (ML) which exploits the network traffic flow to detect abnormal behaviours. Intrusion detection on the SDN is still at large and more ML techniques needs to be explored, considering the critically of the SDN controller.