MLKD 2024
The First International Conference on
Machine Learning and Knowledge Discovery
Amirkabir University of Technology, December 18-19, 2024

Using Deep Reinforcement Learning Technique for Distributed Denial of Service Attack Detection in Software Defined Networks

Khashayar Delavari[*] Mehran Shetabi[†] Sayed Alireza Sadrossadat[‡]

Abstract

The rapid advancement of Software Defined Networking (SDN) has introduced significant benefits in terms of network flexibility, management, and scalability. However, the centralization of control in SDN also brings substantial security challenges, particularly from Distributed Denial of Service (DDoS) attacks. Traditional detection mechanisms often fall short due to the evolving and sophisticated nature of these attacks. This paper proposes an innovative Deep Reinforcement Learning (DRL)-based technique to enhance the detection and mitigation of DDoS attacks in SDN environments. By leveraging the adaptive learning capabilities of DRL, the proposed model continuously learns and adapts to new attack patterns, providing a robust defense mechanism. The model utilizes a combination of Autoencoder (AE) and Bidirectional Gated Recurrent Unit (BGRU) to effectively analyze traffic patterns and detect anomalies. Experimental results, conducted using a comprehensive dataset from real network traffic, demonstrate the superior accuracy, higher detection rate, and reduced false-positive rates of our approach compared to existing methods. Furthermore, the proposed technique includes a trust value mechanism to mitigate the effects of detected attacks, ensuring enhanced security and reliability for SDN networks.

Keywords: Software Defined Networking, DDoS attack detection, Deep Reinforcement Learning, Autoencoder, Bidirectional Gated Recurrent Unit

[*] Yazd University, khashayardelavarii@gmail.com
[†] Yazd University, mshetabi@yazd.ac.ir
[‡] Yazd University, alireza.sadr@yazd.ac.ir