ABSTRACT

Distributed Denial of Service (DDoS) attacks are a significant threat to network security, particularly in the context of Software-Defined Networking (SDN). This study develops a DDoS detection system for SDN networks using a deep learning model, specifically Long Short-Term Memory (LSTM). The centralized architecture of SDN makes it vulnerable to attacks that can disrupt the entire network by targeting the controller. To address this issue, we used Mininet for network simulation, Ryu Controller for traffic management, and tools like hping3 and Wireshark to generate and analyze data. The generated dataset was trained using LSTM to distinguish normal traffic from DDoS attacks. Testing results demonstrate that the LSTM model achieved an accuracy of 98.40%, proving its effectiveness in detecting DDoS attacks with minimal error. This research highlights the significant potential of LSTM in enhancing the security of SDN networks..

Keywords— ***Network Security, Distributed Denial of Service, Software Defined Network (SDN), Long Short-Term Memory (LSTM)***