ABSTRACT

Distributed Denial of Service (DDoS) attacks, such as ICMP Flood and SYN Flood, pose a significant challenge in maintaining the availability and stability of network services. Software-Defined Networking (SDN) offers centralized and flexible network control, but lacks built-in security mechanisms to automatically detect and mitigate such attacks. To address this limitation, an integrated system is required that can monitor network traffic and perform mitigation when threats are detected. This study designs a network security system by integrating SDN using OpenDayLight as the controller, Suricata for intrusion detection and mitigation, and Open vSwitch for traffic management. The system is tested and evaluated based on Quality of Service (QoS) parameters, including throughput, packet loss, delay, and jitter. The results show that the system successfully detects and mitigates DDoS attacks automatically. During the ICMP Flood attack, throughput decreased from 234,254 bit/s to 117,743 bit/s, delay increased from 1.746 ms to 4.904 ms, jitter from 1.158 ms to 3.298 ms, while packet loss remained at 0%. In the SYN Flood scenario, throughput dropped from 410,315 bit/s to 165,172 bit/s, delay and jitter both increased from 1.159 ms and 1.158 ms to 3.298 ms, and packet loss decreased from 0.00262% to 0%. These results demonstrate that the system maintains network stability and preserves QoS during attack conditions.

Keywords: SDN, IDPS, DDoS, Quality of Service, Network Security