ABSTRACT

The development of modern networking technology, particularly through the implementation of Software-Defined Networking (SDN), offers high flexibility in managing data traffic through centralized control. However, this architecture also introduces new security challenges, especially against volumetric attacks such as Internet Control Message Protocol (ICMP) Flood, which can overload the controller and significantly degrade network performance. This study aims to analyze the application of the Support Vector Machine (SVM) algorithm for anomaly traffic detection, as well as the implementation of rate limiting techniques as a mitigation effort to reduce the impact of ICMP Flood attacks on SDN based on the POX Controller. Simulations were carried out using the Mininet emulator under both normal and attack traffic conditions, with and without mitigation, while measuring performance parameters including packet length, ICMP count, packet loss, and round-trip time (RTT). The testing covered five attack scenarios (two attackers without mitigation, three to five attackers with mitigation) with an attack intensity of up to 100,000 ICMP packets sized 5,000 bytes at intervals of 1–2.5 ms. The results show that without mitigation, communication disruption lasted up to 1,323 seconds, with False Positive (FP) values reaching 23,134, indicating the system failed to distinguish legitimate traffic from flood traffic. In contrast, with the implementation of rate limiting, delay spike durations were reduced to 45–94 seconds, and FP values dropped significantly to the range of 1,396–2,589. Additionally, packet loss remained under 72%, and SVM detection accuracy ranged from 93.48% to 95.82%, indicating that the system was able to maintain communication stability even under flood pressure. The application of rate limiting proved effective in reducing attack rates and maintaining normal traffic flow, even with packet loss rates between 45% and 72%. These findings confirm that the integration of SVM detection and rate limiting on the POX Controller is effective in mitigating ICMP Flood attacks without disrupting normal traffic.

Keywords — **Software-Defined Network, ICMP Flood, DDoS, POX Controller, Rate Limiting, Network Security**