ABSTRACT

Distributed Denial of Service (DDoS) attacks, particularly UDP Flood, pose a serious threat to Software Defined Networking (SDN) architecture due to its centralized management. This centralized nature makes SDN vulnerable, as it becomes an easy target for attacks that can disrupt the control function of the network, which relies on a single controller. This research implements a mitigation system against UDP Flood attacks by combining Rate Limiting using the Ryu Controller and detection based on Support Vector Machine (SVM). The simulation was conducted on a tree topology using Mininet. The results show that the system is capable of detecting and limiting attacks adaptively and in real-time. Evaluation using a confusion matrix indicates that the system achieves an average detection accuracy of 87.62% with 0% false positives, meaning that normal traffic was never misclassified as an attack. Specifically, detection accuracy reached 90% in the two-attacker scenario and slightly decreased to around 82% in the seven-attacker scenario. Regarding network recovery, a recurring pattern was observed: normal → unreachable → normal → unreachable → normal, indicating that connections were intermittently disrupted due to the mitigation mechanism before finally stabilizing. The estimated average recovery times for normal traffic based on the number of attacking hosts were as follows: 5.19 minutes (2 attackers), 2.30 minutes (3 attackers), 2.00 minutes (5 attackers), and 1.48 minutes (7 attackers). However, under certain conditions, recovery time could exceed 15 minutes. Normal traffic only fully recovers once all attack processes have been stopped and no suspicious traffic is present in the network. The system is also equipped with a visual dashboard for real-time monitoring of attack status and mitigation progress.

Keywords **— SDN, DDoS, *UDP Flood*, *RYU Controller*, *Rate Limting*, SVM**