ABSTRACT

DDoS (Distributed Denial of Service) is one of the cyber-attacks that make the network service unavailable. SDN (Software Defined Network) has tools to defeat the DDoS, because SDN has good features in defeating DDoS such as logically centralized controller, separation control plan, and programmability network. There are many defense mechanisms in SDN against DDoS attack, source-based Defense mechanism is one of the defense mechanisms in which the defense mechanism is deployed in the source.

This thesis offers the SVM (Support Vector Machine) that combined with Ryu controller that can predict the incoming packet based on the learned traffic, whether it is a normal packet or DDoS packet, and blocking the packet if the packet indicating the DDoS traffic. The simulation is done by sending the normal TCP traffic from the server to the client and attacking the server in order to make the service unavailable.

The purpose of this simulation is to evaluate the capability of the SVM controller in handling the various size packet size and number of attackers of DDoS attack. The result of the simulation the smallest attack damage that DDoS does is at the 300 PPS rate with 1,2,3, and 4 attackers with an average throughput 9 Mbps. The maximum attack damage that DDoS does is in 3000 PPS with 4 and 5 attackers with a throughput below 4 Mbps. However, the damage can be mitigated by the SVM mitigation, proven by the throughput is increased after the SVM mitigating the DDoS attack which for 3000 PPS with 4 attackers become 6.9 Mbps and for 3000 PPS with 5 attackers become 5.3 Mbps. Moreover, the higher accuracy of the SVM is 87% and the lowest accuracy is 67%

Keywords: Software Defined Networking (SDN), Support Vector Machine (SVM), Distributed Denial of Service Attacks (DDoS), Source-based defense mechanism.