ABSTRACT

Software Defined Network (SDN) is a new network paradigm that separate control plane and data plane. SDN has centralized control that allows administrators to control data flow. SDN using Open Flow protocol that allows the implementation of the concept of SDN in both hardware and software. In SDN, there is a software called controller that manages the switches to control traffic. Controller communicates with OpenFlow switches and manage the switches via OpenFlow protocol.

Because SDN is a network that can be programmed openly by anyone it makes SDN network vulnerable to attack, particularly in the control plane and data plane. It makes SDN system experiencing a major threat in the side of security.

In this paper, DDoS attacks simulated on a network SDN. POX used as a control plane and Mininet as a data plane. Entropy is used as a method of detection of DDoS attacks on a network with the concept of SDN. Network performance analysis was also performed on the simulation process to determine the value of the parameter network convergence time and quality of service (Delay, Throughput, Jitter and Packet Loss Ratio). So that it can be seen how the SDN network performance during the attack Distributed Denial of Service (DDoS) using entropy as a detector.

***Keywords**: Software Defined Network, SDN Security, QoS, DDoS attacks, Entropy, Threshold, Randomness*