

ABSTRAK

Software Defined Network (SDN) adalah sebuah paradigma jaringan baru yang memisahkan *control plane* dan *data plane*. SDN memiliki control terpusat yang memungkinkan administrator dapat mengendalikan data flow. SDN menggunakan protokol Open Flow yang memungkinkan pelaksanaan konsep SDN di kedua perangkat keras dan perangkat lunak. Dalam SDN, ada *software* bernama controller yang mengelola switch untuk kontrol trafik. Controller berkomunikasi dengan OpenFlow switch dan mengelola switch melalui protokol OpenFlow.

Karena SDN merupakan jaringan yang dapat diprogram secara terbuka oleh siapa saja hal itu membuat jaringan SDN rentan terhadap serangan, khususnya pada bagian *control plane* dan *data plane*. Hal ini menjadikan sistem SDN mengalami ancaman besar dalam sisi keamanannya.

Dalam tugas akhir ini disimulasikan serangan DDoS pada sebuah jaringan SDN. POX digunakan sebagai *control plane* dan Mininet sebagai *data plane*. Entropi digunakan sebagai metoda deteksi adanya serangan DDoS dalam sebuah jaringan dengan konsep SDN. Analisis kinerja jaringan juga dilakukan pada proses simulasi untuk mengetahui nilai parameter *network convergence time* dan *quality of service* (*Delay, Throughput, Jitter, dan Packet Loss Ratio*). Sehingga dapat diketahui bagaimana performansi jaringan SDN saat terjadi serangan *Distributed Denial of Service* (DDoS) menggunakan entropi sebagai detektor.

Kata kunci: Software Defined Network, SDN Security, QoS, DDoS attacks, Entropy, Threshold, Randomness