ABSTRAK

Pada masa berkembangnya jaringan komputer saat ini. Dirancanglah sebuah perangkat lunak untuk membangun infrastruktur jaringan yaitu Software Defined network (SDN). Software Defined Network (SDN) adalah Konsep dasar SDN adalah dengan melakukanpemisahan eksplisist antara control dan forwarding plane, serta kemudian melakukan abstraksi sistem dan mengisolasi kompleksitas yang ada padakomponen atau sub-sistem dengan mendefinisikan antar-muka (interface) yang standar. Pada jaringan konvensional administrator jaringan diharuskan menangani puluhan, ratusan atau babkan ribuan perangkat jaringan didalam sebuah organisasi. Permasalahan ini sering ditemukan dalam dunia industri. Disinilah Software Defined Network (SDN) menyediakan arsitektur yang menjanjikan untuk jaringan masa depan dan dapat memberikan keuntungan dengan programabilitas pada controller untuk mengatur seluruh trafik pada jaringan. Terlepas dari keuntungan yang dimiliki SDN, terdapat tantangan pada keamanan jaringan SDN. Yaitu akan kerentanannya terhadap serangan Distributed Denial of Service (DDoS). Distributed Denial of Service (DDoS) adalah salah satu serangan yang dapat menyerang komponen yang ada pada arsitektur SDN. Pada penelitian ini sistem deteksi dan mitigasi serangan DDoS dibangun untuk mendeteksi dan memitigasi serangan DDoS pada arsitektur SDN dengan menggunakan algoritma SOM. SOM diterapkan pada model machine learning untuk mengklasifikasikan trafik normal dan trafik serangan DDoS berdasarkan fitur yang diambil dari dataset yaitu *speed of flow entries* dan *speed of source IP*. Dari hasil pengujian yang telah dilakukan sistem mampu mendeteksi dan memitigasi serangan DDoS. Dengan pengukuran akurasi mendapatkan hasil terbaik sebesar 76,33333% dengan menggunakan learning rate 0,50 dan test size 0,30 .

Kata kunci : Software Defined Network (SDN), Self-organizing Map (SOM), Machine Learning, Distributed Denial Of Service (DDoS)