ABSTRAK

Pada masa sekarang ini jaringan telah menjadi infrastruktur yang sangat penting bagi bisnis, perkantoran maupun kampus. Oleh karena itu, sangat penting sekali untuk memiliki sistem infrastruktur jaringan yang mudah dikelola namun memiliki kemampuan kerja yang optimal dan juga fleksibel. *Software Defined Network* (SDN) merupakan teknologi baru dalam konsep jaringan, dimana SDN memisahkan *control plane* dan *data plane*. *Controller* sebagai otak yang mengatur *forwarding* paket dari suatu jaringan SDN, sehingga dapat melakukan kontrol terpusat pada jaringan yang banyak dalam sebuah *controller*. *Controller* belum memiliki sistem keamanan yang cukup baik untuk melindungi dari serangan. Terdapat beberapa kasus serangan seperti *Distributed Denial of Service* (DDoS) yang menjadi suatu permasalahan serius pada keamanan jaringan. Untuk dapat menunjang teknologi yang semakin maju maka perlu diterapkan konsep jaringan yang memadai juga. Pada penelitian ini akan membangun sebuah konsep jaringan SDN dan melakukan pengembangan pada *controller* dengan menerapkan *machine learning K-Nearest Neighbors* (KNN). Fungsi dari *machine learning* KNN sendiri yaitu untuk dapat melakukan klasifikasi pada trafik yang dijalankan. Trafik yang dijalankan nantinya akan terdapat trafik serangan yang dapat di deteksi dan mitigasi oleh *controller* yang sudah dikembangkan. *Controller* yang digunakan pada penelitian ini adalah ryu *controller*. Tujuan dari penelitian ini adalah membangun sistem deteksi dan mitigasi serangan DDoS dengan menggunakan *machine learning* model algoritma KNN. Dalam penelitian ini terbukti bahwa kinerja *machine learning* KNN yang dikembangkan pada *controller* dapat melakukan deteksi dan mitigasi serangan DDoS. Pada pengujian pengukuran akurasi mendapatkan nilai 82% dengan menggunakan nilai K = 5 dan data test yang digunakan sebesar 30%.

Kata Kunci: ***Software Defined Network (SDN), Distributed Denial of Service (DDoS), K-Nearest Neighbors (KNN), Controller.***