ABSTRACT

Traffic anomaly detection system based on network security is a system that serves to determine the peculiarities or disturbances in a computer network. There are some examples of the types of traffic anomalies include Denial of Service (DoS), Distributed Denial of Service (DDoS) and so on. Where any anomalies having different characteristics traits that will lead to an anomalous pattern. Hence the need for traffic anomaly detection system that can handle and catch the pattern which is formed by the traffic anomalies.

At this final project research used a technique in which traffic anomaly detection based *cluster*ing algorithm using Denstream. Denstream algorithm is one of the density-based *cluster*ing algorithm which is used for the processing of Data Stream. In the final project research has focused on modifying the micro-*cluster* update process.

Results from this study, Denstream algorithm has good performance in detecting anomalous traffic. It can be demonstrated by tests performed by DARPA 1998 dataset, where the average value of *Purity* is 97.07%.

Keywords : traffic anomaly, ddos, *clustering*, algoritma Denstream, *update micro-cluster*