ABSTRACT

The Attack detection system based on anomaly traffic with Denstream algorithm clustering method is a computer network security system which serves to detect disturbances on computer networks by detecting based on pattern generated by anomaly traffic. Distributed Denial of Service (DDoS) is one example of the types attacks that can disrupt traffic on computer networks, this kind of attack have a characteristic, which in each of its attacks will send a number of data packets continuously to the target. By using anomaly detection, DDoS attacks can be detected by identifying patterns caused by anomalies.

This final project research used a technique to detect the traffic anomaly which is clustering based. Denstream algorithm is one of the Density-based clustering algorithm that can be used in the Data Stream Then, the research focus of this final project is Denstream algorithm Adjusting the cluster generating process periodically..

The results from this study, Denstream algorithm has a good performance in detecting anomalous traffic. It show with the tests performed by DARPA 1998 dataset, where the average value of 98.02% Purity.

Keywords : traffic anomaly, ddos, *clustering*, Denstream algorithm, *Density*, *generating cluster*