ABSTRACT

The rapid development of information technology and especially the Internet today triggers phenomena traffic anomalies (attacks) or threats to a computer or server. Flash crowd is a phenomenon of increasing access / traffic is high to a server for a particular event. Denial of Service (DoS) and Distributed Denial of Service (DDoS) is an attack that occurred with flood the network with a lot of data (traffic flooding) or flood the network with a lot of requests to a host or service (request flooding) that can not be accessed by registered users (legitimate users). Therefore, we need a system of detection by clustering the traffic anomalies.

This final project research used a technique to detect the traffic anomaly which is clustering based. CURE algorithm is a hierarchical based clustering algorithm which has ability in terms of handling outliers. Then, the focus of this final project research is in terms of handling the outliers points from the dataset. Outliers eliminated by removing a point that was considered as an outlier with outlier removal technique clustering (ORC).

The results from this study, CURE algorithm has a good performance in detecting anomalous traffic. It show with the tests performed by DARPA 1998 dataset, where the average value of 98.4588 % detection rate, 0.2325 % false positive rate, and 94.7323 % accuracy. The test results of elimination of outliers with threshold value 0.1 - 1, ORC technique successfully found and remove the points that are considered as an outlier.

Keywords : traffic anomaly, ddos, *flash crowd*, *preprocessing*, *clustering*, cure algorithm