ABSTRACT

Internet has grown so fast that made positive and negative effect for it's user. It same as threat that can be happen to computer or server in a network, one of them is about anomaly traffic, for example is flashcrowd that happen when the demand of traffic in a network is increase significally. It's happen because too many user that access the same network and cause traffic density to increase.There are so many research about traffic anomaly but the data that used in the research still in damped mode or we call it offline, it means the data not real and determine by the researcher.Therefore, a system detection is needed to detect and identify traffic anomaly based on streaming traffic.

In this Final Task, anomali detection will be research with BIRCH (*Balanced Iterative Reducing and Clustering Using Hierarchies*) algorithm. This system can detect and identify anomaly that happen in the network with cluster based system to make anomaly cluster and normal cluster traffic.Then, it will continued with DBSCAN (Density Based Spatial Clustering of Applications with Noise) clustering algorithm for labeling traffic packet.

Result from this study, BIRCH and DBSCAN algorithm has good performance in detecting anomalous traffic. It can be demonstrated by tests the accuracy of detecting datastream, where the average value of accuracy is 98.4% and it takes about 600 seconds or 10 minute for one process from 30.000 data.

Keyword : BIRCH, DBSCAN, flashcrowd, streaming traffic