ABSTRACT

Traffic anomaly is an event which an Internet user can not access the Internet as it should, it could be because of the increased traffic drastically (Flash Crwod) or actual attack (DoS or DDoS) by those who do not want the user to access the internet. DDoS is an attack in which attack by flooding the target traffic using the message " PING " so that the target can not be connected properly. While Flash Crowd is where the state of a traffic increase but gradually (unlike DDoS) due to natural disasters, product promotion, and others.

There are two methods for performing anomaly detection, the signature and anomaly based. Signature method using the database in the introduction of an anomaly, so if there is a new anomaly maybe cannot be detected. Meanwhile, Anomaly does not use a database but use the learning patterns occur, so that if there is a new anomaly be detected. So that the final project, using method anomaly-based as detection methods .

In this final project applying methods Clustering using K -Means Algorithm Modified by Timestamp Initialization on Sliding Window. The results obtained in the form of a traffic anomaly detection with best detection rate is 96.06% and false positive rate is 0.75% from testing with any dataset.

Keyword : Anomaly, Clustering, K-Means, Timestamp Initialization, Sliding Window.