ABSTRACT

In recent years, the phenomenon of anomaly traffic on a computer network traffic attracted much attention of research. According to [1] a Distributed Denial of Service (DDoS) is a type of attack that could harm the network traffic that is being used, both againts the target of attacks and all users. While flashcrowd event is a huge spike in network traffic because of the number of internet users who access the server up significantly and put heavy pressure on the network link that leads to the server.

In this final project used statistical techniques covariance matric is not ignore the feature with other features, can be made anomaly detection system by changing the original data into feature space covariance. No attack can be classified by using SVM. Accuracy, detection rate and false positive rate is the testing parameters used in the study.

Results from this study, SVM algorithm has the performance average value in classifying the data detection rate of 99% on a homogenous dataset KDDCUP 99 and an accuracy of 90.5%. For heterogeneous data performance decreased with increasing FPR value at which the data in the test with an average of 22.6% due to the data given in the attack *noise* preprocessing process.

Keyword : Anomaly detection, covariance matrix, landmark window, SVM, DDoS, flashcrowd, detection rate, false positive rate.