ABSTRACT

As the development of Internet technology today, a growing number of emerging types of attacks or threats against a computer or a server in a network, one example in the form of traffic anomalies. Some types of anomaly traffic on a computer in an internet network such as Denial of Service (DoS), Distributed Denial of Service (DDoS) or flashcrowd. Therefore, it is necessary to have a detection system to detect and recognize each traffic anomalies.

At this final project research develop statistics-based detection system using Multivariate Correlation Analysis (MCA). MCA using representation techniques Triangle-Area-Map (TAM) to describe the relationship between each feature traffic by calculating the distance of a single feature value to the value of other features for each feature extraction results. The results of data processing were analyzed using the Mahalanobis Distance to be used as reference or observation data.

The detection process of the observed data based on threshold of the reference data and anomaly classification process using Mahalanobis Distance and Cosine Distance to calculate the distance between values of the TAM observed traffic features with the TAM reference traffic. System testing is made by measuring the level of accuracy of the algorithm, based on the output of system with parameters Detection Rate (DR), False Positive Rate (FPR) and Accuracy (ACC).

Keywords: *traffic anomalies, DDoS, flashcrowd, multivariate correlation analysis, triangle-area-map, mahalanobis distance, cosine distance*