ABSTRACT

the development of technology and information currently very rapid. Internet technology the most important part of community life in the world. now technology of internet has easier acces to find a information by public. With the ease of access to the technology of internet triggers the traffic anomalous phenomenon . Traffic anomalous phenomena in the form of a Distributed Denial of Service (DDoS) and flash crowd. Distributed Denial of Service (DDoS) is a type of attack on a computer or server with one way traffic flooding the network with lots of requests (request flooding) that can not be accessed by real users. Flash crowd is the situation of a very high increase in traffic in a network and so can not be accessed within a certain time frame.

Considering the negative impact of the phenomenon that received the traffic anomalies, considered important to build detection method that can distinguish DDoS attacks and flash crowd. In this final project will be constructed a method Intrusion Detection System (IDS) with unsupervised learning clustering technique that uses algorithms ISODATA with euclidean distance as well as modifications to the handling of attacks dataset using windowing on the application so that it can work well in the detection and distinguish between normal traffic and anomalies.

Results from this study, the algorithm Isodata has good performation at detecting anomalous traffic. It can be demonstrated by tests performed by DARPA 1998 dataset, average value of DR is 95.9587%, FPR is 0.829782%, ACC is 93.9086%. The test results take less than 5 minutes to process one million data by using the euclidean distance.

Keyword : Traffic Anomaly, Ddos, *Flash Crowd*, *Clustering*, Isodata, *Euclidean Distance*, Windowing.