ABSTRACT

Internet technology at this time growing rapidly, as well as the threat of attacks to internet users are increasingly. One of the emerging threats is Distributed Denial of Service (DDoS), DDoS is a type of Anomaly Traffic that causes users can not access the internet as it should.

In detecting anomaly attacks, there are two methods: signature method and anomaly based method. In this study the method used is an anomaly based method that does not use the database to detect anomalous attacks, this method works with pattern recognition as where the characteristics of anomalies that can change the pattern so as to enable detect the types of new attacks. However, anomaly based weaknesses have high false detection when not well made.

In this Final Project has been built anomaly detection system using anomaly based traffic method. Mahalanobis distance and CART algorithm are used for anomaly detection and revision function belief on BDI concept. In this study used poison distribution as a grouping of data during system testing, this is done so that the system built later can be applied in real life. Using the DR, FPR, and ACC parameters for each test, the average results generated for each test were μDR = 80.36%, μFPR = 0.0008%, and μACC = 99.89%.

Keywords: Anomaly detection, Mahalanobis, CART, revision function belief, poisson distribution, BDI