ABSTRACT

Denial of Service (DoS) is a phenomenon which is becoming a hot topic lately. The intensity of DoS attacks is increasing every day with the discovery of a new type of attack with the same type which is Distributed Denial of Service (DDoS). Both attack the victims by flooding with a lot of traffic channels packet at a time. This makes the flow of packets to the victims computer becomes choked and victim don't get the desired package because the density of traffic on its network.

LRD and self-similarity methods is suitable to the network traffic behavior which is variability and burstiness. In LRD method stated that network traffic shows a long-term memory in which behavior is correlated through time apart. This shows that every packet sent and received has a particular relationship although correlation and inter-arival time is quite far apart. In DDoS possibility of correlation and the relationship is not going to happen in the near future though. It makes use of DDoS detection using LRD be one of the best method. Self-similarity is a scale of invariant which is always have the same, so when self-similarity used into traffic modeling, it will show a plot of the traffic will have in common, even though it has a different time.

The result of this research shows that self-similarity analysis have good performance. This can be seen from hurst eksponen value corresponding to existing theory where the estimated hurst eksponen value between 0,5 and 1 for normal dataset testing and out of that range for anomali datset testing. Otherwise it can be seen from mahalanobis distance value for every self-similarity behavior. From testing of each step, mahalanobis distance value for DDoS testing always have a biger value than normal testing. While mahalanobis distance from flashcrowd testing have smaller value then normal testing.

Keywords : DDoS, LRD, Self-similarity, burstiness, mahalanobis