ABSTRACT

With the growth of the Internet in today's world, network security has become a serious problem to cope with. Of special mention are the DoS (Denial of service) and DDoS (Distributed DoS) attacks which poses a big threat to any electronic society. The DDoS attacks take advantage of the functional architecture of the Internet, which makes them all the more lethal. While majority of research literature has focused on using various fundamental classifier models for detecting DDoS attacks, the unavailability of larger sets of training data and the lack of accuracy in the existing sets render these mechanisms ineffective in the long run.

In this project we have designed a practical, carefully engineered and adaptive anomaly based detection system to detect DDoS attacks using a Naïve Bayesian Classifier. It is configured to work with small sets of training data and unlike signature detection based systems; it can detect unknown (zero- day) attacks. The system is designed to be near the target and focuses primarily on the TCP layer protocol. The classifier consists of two phases of operation. During the *training phase*, the input traffic is divided into traffic subsets which fit into logical entities called windows. The probability distribution of the different TCP packets in these windows is estimated based on observation of a large number of normal packets. These probability distribution values act as input to the next phase, which is the *deployment phase*. During the deployment phase, the probability of a window (function of probabilities of individual packets) is determined. If this probability is found to be lesser than a threshold probability, then the particular sequence is said to be abnormal. At any point in the course of deployment, if the number of abnormal windows goes beyond a particular number (user defined parameter called Abnormal Window Count (AWC)), then the system flags an attack.

Keywords: Denial of Service(DoS), Distributed DoS(DDoS), Naïve Bayesian, TCP, Abnormal Window Count(AWC), Cross Validation, Windowing, Smoothing, Bands.