ABSTRACT

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve (1) efficient detection with a small number of false alarms and (2) real-time transfer of packets. Here we introduce a method for effective detection of DDoS attacks. We classified the network status into 3 parts viz. normal, pre-attack and attack states. These network status are utilized in the detection stage of the developed model anti-DDoS framework. Here we bypass the normal state packets, dropped the attack state packets and send the pre-attack state packets into the prevention stage of anti-DDoS framework. Initially, we analyze the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select the specific features of packet transfer viz. entropy of source and destination IP address, port number, number of packet etc.

After that we studied about different classifiers viz. KNN, Naïve Bayes, C4.5, Decision Tree, etc. We also studied about ensemble classifiers and its different methods used for it. Then we implement KNN classifier in C and test it with different datasets. We tested the KNN Classifier with different UCI and NSL dataset. KNN classifier classifies the attack state of the instances of the dataset provided and it has provided us good results.

We have also tested Naïve Bayes, C4.5 and Decision Table classifiers for different datasets. We have also tested Adaboost ensemble method using the above mentioned classifiers for various datasets. Adaboost ensemble method has very good accuracy of correctly classified instances.

Keywords: Denial of Service, Distributed Denial of Service, Low rate DDoS attack, ensemble classifier, anti-DDoS framework, KNN, Naïve Bayes. C4.5, Decision Table