# ABSTRACT

Distributed Denial of service (DDoS) is a prevelant threat in todays networks because effective DDoS attacks are now easy to launch with IRC channels and easy availability of vulnerable hosts. At the same time defending a network resource against them is disproportionately difficult. Despite the extensive research in recent years, DDoS attacks continue to harm, as the attackers try to adapt to the newer protection and attack mechanisms. DDoS attacks may come as flooding attacks or low rate attacks which are difficult to detect. For this reason, we provided a method which will help differentiate between the predictable DDoS attack and non predictable DDoS attacks. In this method, the pearson correlation coefficients of the packets along with the time interval helped to detect the same. The execution time for each 5 sec window was found to be 0.22044 sec which is way lesser than the actual time window. Again DDoS attacks may be caused by many IPs but a single IP is mostly the culprit and is responsible for the flooding. Our second method provides a mechanism to deal with that and segregate the culprit IP. Flooding can be caused by bogus traffic of TCP/UDP/ICMP protocol packets. We can only detect such type of attack if they cross a specific threshold. In this project, we could detect them by setting a threshold for each type of protocol. We have done all this is offline mode and will be done in real time in our future work.