Abstract

Denial of Service (DoS) attacks or Distributed Denial of Service (DDoS) attacks are on the rise and have gained in frequency and complexity. Earlier most DDoS attacks targeted the network layer (Layer 3) and transport layer (Layer 4) of the communication system. But this network and transport layer attacks can often be filtered or detected using specialized DDoS protection equipment or using detection approaches. To dodge this detection the attackers have now moved up the stack and are focusing on the application layer (Layer 7) thus increasing the complexity of the DDoS attacks.

Application layer attacks aim is to overload specific components of an application infrastructure which is done by creating Hypertext Transfer Protocol (HTTP) or Domain Name System (DNS) traffic. These HTTP or DNS traffic are allowed by the firewalls and are legitimate to Intrusion Prevention System (IPS) devices since IPS provides security by inspecting packets for known threats only.

Application layer attacks can be detected using statistical, knowledge-based, soft computing and data mining and machine learning approaches. In this project focus was given on detection of attacks using machine learning approach. Here a sample of 1998 world cup semi-final dataset is used as training dataset and another sample dataset is used as the test dataset and detection is done using machine learning techniques such as decision trees. The objective of this project is to make a fast, dynamic and incremental detection tool.

Keywords:- *Application layer attack, Machine Learning approach, DDoS, Detection Tool*