A COMBINED PROTETION FOR ENTIRE NETWORK BASED ON IMMUNE INSPIRED THEORIES

P.S. Thumilvannan, M.E.,A.P/CSE Dept., S. Hirutiha,(M.E),
Arulmigu Meenakshi Amman College of Engg
Thiruvannamalai Dt, Near Kanchipuram.

Abstract—The combined protection for entire network identifies the traffic anomalies by monitoring the header information. Some attacks like denial of service led to develop the techniques for identifying the network traffic. The possibilities of traffic-analysis based mechanisms for attack and anomaly detection is also being studied. The motivation for this work came from a need to reduce the likelihood that an attacker may hijack the position machines to stage an attack on a third party. A position may want to prevent or limit misuse of its machines in staging attacks, and possibly limit the liability from such attacks. In particular, the utility of observing packet header data of outgoing traffic, such as destination addresses, port numbers and the number of flows, in order to detect attacks/anomalies originating from the position at the edge of a position is also dealt with. Detecting anomalies/attacks close to the source allows us to limit the potential damage close to the attacking machines. Project approach passively monitors network traffic at regular intervals and analyzes it to find any abnormalities in the aggregated traffic.

Keywords-Network Traffic; Traffic anomalies; anomaly Detection.