Abstract

In the networking world, a denial of service (DoS) attack is an incident in which a user is deprived of the services of a resource they would normally expect to have. Intrusion Detection System (IDS) is the tool that is able to detect occurrences of intrusion at host, the network and application in the system. One of the most common network attacks is Denial of Service (DoS) attack. In DoS attack of the computer system an individual host will send huge number of packets to one machine so it make the operating of the network and host slow. In this paper, signature of selected attacks such as Smurf, Ping-of-Death which are based on network flow is considered and Mail-Bomb. The system uses MCA based system for detection of the DoS attack. The proposed system monitors the network path to detect attacks and the results show less false negative error during monitoring of the system. Specially, signature based IDS which use fuzzy decision tree for monitoring network path observes that there are great improvements on speed of detection as well as performance of system in the organization.


Index Terms

Computer Science

Fuzzy Systems

Keywords

Denial-of-Service attack, IDS, Multivariate correlations, fuzzy logic