Abstract

A Denial of Service (DoS) attack is a malicious effort to keep endorsed users of a website or web service from accessing it, or limiting their ability to do so. A Distributed Denial of Service (DDoS) attack is a type of DoS attack in which many computers are used to cripple a web page, website or web-based service. Fault either in users’ implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched of the type of network attacks, denial-of-service flood attacks have reason the most severe impact. This analysis study on flood attacks and Flash Crowd their improvement, classifying such attacks as either high-rate flood or low-rate flood. Finally, the attacks are appraised against principle related to their characteristics, technique and collision. This paper discusses a statistical approach to analysis the distribution of network traffic to recognize the normal network traffic behavior. The EM algorithm is discussed to approximate the distribution parameter of Gaussian mixture distribution model. Another time series analysis method is studied. This paper also discusses a method to recognize anomalies in network traffic, based on a non restricted ?-stable first-order model and statistical hypothesis testing.
References

- http://www.cert.com


- Huang Kai, Qi Zhengwei, Liu Bo” Network Anomaly Detection Based on Statistical Approach and Time Series Analysis” 2009 International Conference on Advanced Information Networking and Applications Workshops

- Federico Simmross, Juan Ignacio, Pablo Cassia-de-la-Higuera, Ioannis A. Dimitriadis" Anomaly Detection in Network Traffic Based on Statistical Inference and ?-Stable Modeling” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 4, JULY/AUGUST 2011


- Monika sachdeva, gurvinder singh, Krishan Kumar, Kuldeep Singh”DDoS Incident and their Impact”IAJIT2010”

- Khadijah Wan, Mohd Ghazali Rosilah Hassan” Flooding Distributed Denial of Service Attacks-A Review “


**Index Terms**

Computer Science

Network Security

**Keywords**

DDoS Impact   Anomaly Detection Method   ?-Stable Model