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 algorism 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
- J. D. Brutlag. Aberrant behavior detection in time series for network monitoring. In LISA '00: Proceedings of the 14th USENIX conference on System administration, pages 139–146, Berkeley, CA, USA, 2000
Index Terms
Computer Science
Network Security

Keywords
DDoS Impact  Anomaly Detection Method  ?-Stable Model