Anomaly based DDoS Attack Detection

Abstract

Distributed denial-of-service (DDoS) attack poses a serious threat to network security. Several methods have been introduced to reduce the damage. However, most of the methods have been found unable to detect the attack in real-time with high detection accuracy. This paper presents a simple yet effective method to detect DDoS attack for all possible attack scenarios given by Mirkovic [1] viz constant rate, pulsing rate, increasing rate and sub-group. The proposed method is validated using well known CAIDA dataset.

References

Anomaly based DDoS Attack Detection

and Distributed Computing Systems.


Symposium on Recent Advances in Intrusion Detection.


Index Terms

Computer Science Security

Keywords

Denial of Service (DOS) Attack, Distributed Denial of Service (DDoS) Attack, Information Gain (IG), Attack Rate, Protocol, Feature Selector (FS)