A DDoS (Distributed Denial-of-Service) attack is a distributed large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc., the victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. There are many proposed methods in the literature which aim to alleviate this problem; such as hop-count filtering, rate-limiting and statistical filtering. However, most of these solutions are meant for the wired Internet and there is little research efforts on mechanisms against DDoS attacks in wireless networks such as MANETs, IDS and ICMP. In this paper, we study the vulnerability of MANETs to DDoS flooding attacks and provide an overview of the commonly used security mechanism against DDoS attacks in wireless networks. The defense schemes proposed are statistical filtering, detection of RTS/CTS packets, signal interference frequency and retransmission time and response stage with ECN marking mechanism.
Reference

- Q. Li, E-C. Chang and M. C. Chan, On the Effectiveness of DDoS Attacks on Statistical Filtering,

Index Terms

Computer Science
Networks

Keywords

DDos
IDS
MANETs

wireless network

attack system