The Internet has experienced a tremendous expansion in its size and complexity since its commercialization. Internet hosts are threatened by large-scale Distributed Denial-of-Service (DDoS) attacks in the network. DDoS attacks typically rely on compromising a large number of hosts to generate traffic to a single destination node. Thus the severity of DDoS attacks will likely increase to the possible extend, as greater numbers of poorly secured hosts are connected to high-bandwidth Internet connections. To detect and coordinate DDoS attacks in the network usually an Intrusion Detection System (IDS) is used but, this method consumes most of the resources and thereby degrades the network performance. Moreover, the memory-less feature of the routing mechanism makes the operation hard to traceback the source of the DDoS attacks. This paper analyzed the performance of an Ant Colony Optimization (ACO)-based IP traceback method to identify the origin of the attack in the network. The ACO-based IP traceback approach uses flow level information to identify the origin of a DDoS attack. The ACO-based IP traceback method is implemented using NS-2 simulation on various network scenarios consisting of 8 nodes, 10 nodes, and 14 nodes. The results of the experimental and simulation studies demonstrate the effectiveness and efficiency of the proposed system.
Performance Analysis of ACO-based IP Traceback

References

Performance Analysis of ACO-based IP Traceback


Index Terms

Computer Science
Network Security
Keywords
Ant Colony Optimization  attacks  DDoS  Internet  IP traceback  pheromone