DDoS attacks are launched with the intention of depleting the network and server resources. The proposed work identifies that the malice behavior of the nodes requesting service and the malice nature of the traffic are the two major issues to be addressed. Accordingly, the defense framework employs attack avoidance methods, attack prevention model and attack detection strategies to be deployed in each autonomous system (AS). A way of avoiding attacks is to ensure that attacks may not exploit the vulnerabilities. This is achieved in this work through enhanced anti-spoofing techniques that resolve insider attacks, and a differentiated routing based on traffic classification.

References


Index Terms

Computer Science

Networks

Keywords

DDoS, Attack detection, Autonomous system, anti-spoofing.