An Approach to Increase Bandwidth Utilization under Suspected Flood Attack

Abstract

Bandwidth is very crucial and limited resource available, so it should be properly utilized. Network congestion occurs when a link or node is carrying large amount of data in case of flood attack and quality of service deteriorates. Effects of flood attack include queuing delay, packet loss or the blocking of new connections. As a consequence incremental increases in offered load leads to either small increase in network throughput, or to an actual reduction in network throughput. Modern networks use congestion control and avoidance techniques to avoid such congestion collapses. One of widely used queuing algorithm is Drop Tail which is used in most
of the routers to avoid congestion and to encourage smooth flow of packets. In this paper we propose a technique to better utilize bandwidth under flood attack. Simulations of the proposed technique have been carried out to compare it with the DropTail. Ns-2 is used as the simulation tool. In this simulation experiment, different types of traffic like tcp, udp are considered. Routers are attacked with different attack intensities to determine the effect of proposed method under various circumstances.

References

- Yi Zhang and Qiang Liu, "A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), July 9-11, 2010, Chengdu, China, pp 163-167
- S.H.C. Haris, R.B. Ahmad and M.A.H.A. Ghani, "Detecting TCP SYN Flood Attack based on Anomaly Detection", 2nd International Conference on Network Applications Protocols and
Index Terms

Computer Science

Keywords
Network Congestion  Bandwidth Management  Drop Tail Queue  Queuing Algorithms