Abstract

It is an adhoc network which is set up by wireless mobile computers (or nodes) which moves randomly in the places that have no network infrastructure or hard to reach location. Since the nodes communicate with each other to gather network information. They cooperate by forwarding data packets to other nodes in the network. In wireless adhoc networks, cooperation between nodes takes place so that they route each other's packet till it reaches destination. Hence they are exposed to a wide range of security attacks. Also because the vulnerability of routing protocols, the wireless ad-hoc networks have to face several security risks. One of these attacks is the Blackhole Attack against network integrity which absorbs all data packets in the network. Since the data packets do not reach the destination node due to Blackhole attack. As a result data loss will occur. In this paper, we simulated the Black hole attack in various wireless ad-hoc network scenarios: with Blackhole attack and without Blackhole attack and comparison of existing TCP variants: TCP, FullTCP, Reno, Reno/Asym, New Reno, New Reno/Asym, Asym, Sack, Fack and Vegas. The impact of Blackhole attack on the performance of MANET is evaluated on the basis of those two scenarios. The measurements were taken to analyze network performance are Throughput, Packet Delivery.
Mobile Adhoc Network under the Adaptive TCP Variants Techniques for Maximization of Throughput Ratio and Total Dropped Packet. The simulation was done by using network simulator (NS-2.34).

References

Mobile Adhoc Network under the Adaptive TCP Variants Techniques for Maximization of Throughput


Index Terms

Computer Science

Wireless Networks

Keywords

Mobile ad-hoc network (MANET)  TCP variants  routing protocol  network security  Blackhole attack  NS-2.