The ad-hoc networks are the temporarily established wireless networks which does not require fixed infrastructure it is also called as infrastructure less network. There is no central control authority in ad-hoc network. Because of some flaws of ad-hoc network such as shared wireless medium and lack of any central coordination makes them more prone to attacks in comparison with the wired network. It is peer to peer network. Among all the attacks wormhole attack is the most severe attack. In this attack an attacker capture the packets at one location in the network and send it to another attacker at a distant location through tunnels which is established through different ways like packet encapsulation, using high power transmission or by using direct antennas. This tunnel between two colluding attackers is virtual and it is called as a wormhole. The wormhole attack is possible even if the attacker has not comprised any hosts, and all
communication provides authenticity and confidentiality. By using the various approaches for finding the solution over wormhole attack, the dynamic information of the packets could still be modified. So in order to give more robust protection in some special scenario like battlefields, which requires highly secured information, there is need of developing some secured mechanism for wormhole detection. Taking into consideration this problem the proposed scheme is developed. This paper discusses proposed works on wormhole attack along with comparison of different wormhole detection techniques in ad-hoc wireless network.

References

- D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless

Index Terms

Computer Science

Wireless

Keywords

ad-hoc Networks
Worm Hole Attack
Wired & Wireless Networks
Tunnel