Abstract

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes that can has no fixed or predetermined topology, with mobile nodes and dynamic membership changes. A self-organizing network is a network that can automatically extend, change, configure and optimize its topology, coverage, capacity, cell size, and channel allocation, based on changes in location, traffic pattern, interference, and the situation or environment. MANETs due to complete autonomy of the member nodes and lack of any centralized infrastructure are particularly vulnerable to different types of attacks and security threats. Packet drop attack is one of them. In this paper mechanism has been proposed to detect and defend against packet drop attacks. Simulation has been done using ns 2. 34 to evaluate the conventional AODV and proposed algorithm when packet drop attack is injected in network. The Result indicates that our proposed solution gives significant better performance then AODV in concern of Packet delivery ratio & Throughput with tolerable increase in routing overhead, End to End delay.

References

- C. E. Perkins, E. M. B. Royer and S. R. Das, "Ad-hoc On-Demand Distance
An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks


- Shah Vrutik, Modi N, Patani A; aodvgap-an acknowledgment based approach to mitigate selective forwarding attacks in manet; in international journal of computer engineering & technology (IJCET) ISSN 0976 – 6367(P) ISSN 0976 – 6375(Online) Volume 3,
An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks

Issue 2, July- September (2012), pp. 458-469


Index Terms

Computer Science

Wireless

Keywords

Black hole attack   AODV   Routing Security   MANETs   Packet drop attacks