An Enhanced Detection Technique for Blackhole Attack in MANET

Abstract

A mobile ad-hoc network (MANET) is a self-optimizing infrastructure-less network. AODV (Ad-hoc On-demand Distance Vector) routing protocol is a loop free protocol used in ad-hoc networks. It is designed such that it can self-start in an environment where all the nodes are mobile in nature. It can also resist a variety of network behaviors such as mobility, failure of links and much more. The ad-hoc network is susceptible to black-hole attack. In a black hole attack, the router drops the packets instead relaying them and is a type of denial-of-service attack.

The proposed work enhances the AODV routing protocol for detecting a black hole attack more efficiently and hence reducing the delay and communication overhead in the MANET. In the proposed work, the behavior of the source node is modified by broadcasting the pirated RREQ which includes its own sequence number instead of destination sequence number and preprocess RREP () function is also added which makes it more secure than the existing solutions. For this the network simulation 2.35 is used. The results obtained from the proposed
methodology shows that the end-to-end delay has been decreased; packet delivery ratio and throughput have been increased.

References

New York 2016

Index Terms

Computer Science Wireless

Keywords

MANET, AODV, Black hole Attack, NS-2