Abstract

Mobile Ad-hoc Network (MANET) is an open loop infrastructure, having independent movement of each node without any decentralized control. Due to dynamic nature, MANET has many security issues than conventional networks. In this paper Ad-Hoc on Demand Distance Vector (AODV) is used as a routing protocol in MANET. Many types of attacks are introduced in MANET such as blackhole attack, wormhole attack, routing table overflow attack, routing cache poisoning attack etc., which occur due to the malicious node and degrade the achievement of AODV. In this paper, blackhole attack is taken into consideration which is more dangerous than other attacks. To maintain a secure route selection under blackhole attack, it is necessary to make a strong security proposal, which maintain the performance of network. This paper introduces a new security scheme which deals with MAODV (Modified Ad-Hoc on Demand Distance Vector) which enlarges the performance of network and eliminates the risk of blackhole attack in the presence of malicious node.
- M. Tamilarasi and T. Sundararajan, Secure enhancement scheme for detecting sel_sh nodes in manet, "pp. 1{5, 2012
- S. Singh, P. Jain, P. Bindra, and C. Goel, Opnet based simulation and performance analysis of aodv and grp by varying number of misbehavior nodes. "
- A. Ajina, G. R. shaktidhrma, study of energy efficient, power aware routing algorithm and their applications. 2010 second international conference on machine learning and computing.
- S. Usha, S. Radha a collective network arbitration protocol to detect mac misbehavior in manets 2010
MAODV: To Identify a Secure Route Selection in MANET under Blackhole

- P. Joshi Security issues in routing protocols in MANETs at network layer Procedia Computer Science 3 (2011) 954–960

Index Terms

Computer Science Wireless

Keywords

MANET  AODV  MAODV  Malicious node  Security  Blackhole attack