A Novel Technique for Sybil Attack Detection and Prevention in MANET

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 130

Number 9

Year of Publication: 2015

Authors:

Priya Jain, Rashmi Nigoti

10.5120/ijca2015907083

Abstract

The attacker quickly affected the routing performance and drops the all packets that contain some data for receiver. This research proposed the Sybil Detection and Prevention (SDP) against Sybil attack. The property of this attack is to reply with every neighbors through multiple recognition (MR) value of itself i.e. fake identity, fake generated specification of itself in dynamic network. Routing protocols for MANET must handle obsolete routing information to hold the dynamically changeable topology. Incorrect routing information accomplished by malicious nodes to extent drop of packets, be considered malicious information. Whereas there are adequately many correct nodes, the SDP is able to find routes that deviates from these compromise nodes and provides secure path in between source to designation. The SDP has detected the malicious nodes and capture the malicious information of MR value generated in MANET. The SDP has immobilized the malicious functioning of Sybil attacker and enhance routing performance in presence of attacker. The better routing performance is devalued through performance parameters such as throughput and packets drop. The proposed scheme is improves throughput, minimizes data loss and provides secure routing.
References

19. Network Simulator-ns-2 Tutorial Available on link,

**Index Terms**

Computer Science

Wireless

**Keywords**

Security, MANET, SDP, Routing, Sybil attacker