Mobile Ad-hoc networks are those networks which have no physical links between the nodes. In MANET mobile nodes dynamically forming a network topology without the use of any existing network infrastructure or centralized administration. Routing in a MANET is challenging because of the dynamic topology and the lack of an existing fixed infrastructure. In most of their
specifications it is assumed that all the nodes in the network are friendly. But in the open, collaborative MANET environment practically any node can maliciously or selfishly disrupt and deny communication of other nodes. Security in MANET is a very difficult problem to incorporate without degrading the performance of the protocol. There are various security issues associated with OLSR and STAR routing protocols among which one is packet dropping by malicious node. In this paper we have proposed one approach to minimize the packet dropping by malicious nodes in the network by applying IPSec in OLSR and STAR routing protocols and compared the results with existing without IPSec protocols. The simulation results demonstrate the success of the proposed approach and maximize the overall performance of MANET in presence of malicious nodes.

References

- BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOUSHIKI NEMOTO AND NEI KATO.”A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOc NETWORKS”, IEEE Wireless Communications, October 2007.
Securing OLSR and STAR Routing Protocols Against Packet Dropping by Malicious Nodes


Index Terms

Computer Science

Wireless

Keywords

IPSec
OLSR
STAR
MANET
Malicious node
Securing OLSR and STAR Routing Protocols Against Packet Dropping by Malicious Nodes