Abstract

Ad-hoc networks establish communication in improvised environments without requiring any fixed infrastructure. These networks are inherently prone to security attacks, with node mobility being the primary cause in allowing security breaches. Therefore, it is required that the nodes cooperate for the integrity of network operation. However, nodes may refuse to cooperate by not forwarding packets to others for selfish reasons and/or not wanting to exhaust their resources. Due to high mobility of nodes in the network, detecting misbehavior is a complex problem. Nodes have to share routing information in order for each to find the route to the destination. This requires nodes to trust each other. Thus we can state that trust is a key concept in secure routing mechanisms. A number of secure routing protocols based on trust have recently been proposed. However, all these protocols use the traditional route discovery model, where a node drops RREQ packet if its own ID is in the source route of the packet, or if it has previously processed the packet. A misbehaving node takes advantage of this vulnerability and forwards the RREQ fast, so that the RREQ received from other nodes are dropped and the path discovered includes itself (the misbehaving node). In this paper, we present a unique trust based method which is not vulnerable to this behavior. In our method,
each node broadcasts a RREQ packet if it is received from different neighbors. A secure and efficient route to the destination is calculated as a weighted average of the trust value of the nodes in the route, with respect to its behavior observed by its neighboring nodes and the number of nodes in the route. We evaluate the misbehaving node detection rate and the efficiency of our method along a number of parameters. Results show that our method increases the throughput of the network while discovering a secure route.

**Reference**


- QUALNET simulator, Available from: .


Trust Enhanced Secure Multi-Path DSR Routing


Index Terms

Computer Science Network Security

Key words

Trust Misbehaving nodes Dynamic Source Routing Path Trust