

Security Scheme for Malicious Node Detection in Mobile Ad Hoc Networks

Punit Rathod¹, Nirali Mody¹, Dhaval Gada¹, Rajat Gogri¹, Zalak Dedhia¹,
Sugata Sanyal², and Ajith Abraham³

¹ Mumbai University, India

{punit_r,nirali_mody, dhavalgada, rajatgogri, zalakdedhia}@rediffmail.com

² School of Technology and Computer Science,
Tata Institute of Fundamental Research, India
sanyal@tifr.res.in

³ School of Computer Science and Engineering, Chung-Ang University, Korea
ajith.abraham@ieee.org

In Ad hoc On Demand Vector (AODV) routing protocol for Mobile Ad hoc Networks (MANET), malicious nodes can easily disrupt the communication. A malicious node that is not part of any route may launch Denial of Service (DoS) Attack. Also once a route is formed, any node in the route may turn malicious and may refrain from forwarding packets, modify them before forwarding or may even forward to an incorrect intermediate node. Such malicious activities by a misbehaving node cannot be checked for in pure AODV protocol. In this paper, a proactive scheme is proposed to detect the above-mentioned malicious activities.

A malicious node flooding the network with fake control packets, such as RREQs (Route Requests) causes congestion in the network. The processing of RREQ by the nodes in the network leads to further degradation in performance of the network. This abnormal behaviour is handled in our scheme by ensuring a fair distribution of resources among all contending neighbours. Incoming RREQs are processed only if number of RREQs from the said neighbour are below RREQ_ACCEPT_LIMIT. This parameter specifies a value that ensures uniform usage of a node's resources by its neighbors. Another threshold RREQ_BLACKLIST_LIMIT determines whether a node is acting malicious or not. If the number of RREQs go beyond RREQ_BLACKLIST_LIMIT then the node is blacklisted and all requests from it are blocked temporarily. Thus, isolating the malicious node.

Tampering of packets by a Malicious node in the route can be detected by promiscuous listening by the other nodes that are part of the route. This type of moral policing, done by the nodes, ensures detection of any malicious activity taking place. To facilitate detection, extra information regarding route is exchanged while route formation. This information contains the next-to-next-hop (NTNH) information in addition to the usual next-hop information. This information is used by a node to verify whether the next-hop node is forwarding the packets to the correct NTNH. This NTNH exchange is critical. To

provide security to it, promiscuous listening is proposed during the route formation also.

The series of simulations reveal that the proposed scheme provides a secured AODV routing protocol with minimal extra overhead as compared to pure AODV protocol.