98. AN AUTHENTICATED SECURE ROUTING IN MOBILE AD-HOC AND WIRELESS NETWORK

InfantLithiya.K M.E-Student,Sivasundari.A Assistant Professor MNM Jain Engineering College Chennai, India.

Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. A major requirement on the network is to provide unidentifiability and unlinkability for mobile nodes and their traffics.The existing protocols are vulnerable to the attacks of fake routing packets or denial-of-service (DoS) broad-casting, even the node identities are protected by pseudonyms. In this paper, we propose a new routing protocol, i.e., authenticated anonymous secure routing (AASR), to overcome the pre-mentioned problems.We adopt a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.Extensive simulations are used to compare the performance of AASR to that of AODV, a representative on-demand anonymous routing protocol provides more throughput than AODV under the packet-dropping attacks, although AASR experiences more cryptographic operation delay.

Keywords—Unindentifiability and Unlinkability; Group Signature; Authenticated Anonymous secure Routhig.

ISBN 978-81-904760-6-5