Abstract

Most of the existing security mechanisms for detecting the packet droppers in a mobile ad hoc network generally detect the adversarial nodes performing the packet drop individually wherein false accusations upon an honest node by an adversarial node are also possible. In this paper, we propose a security mechanism to detect those nodes performing packet dropping either on their own individually or in collusion such that they cannot evade detection and no false accusations are possible. The detection of adversarial nodes is done by the source node through the analysis of the reports submitted by all the intermediate nodes on the source to destination paths. The composition of the report from each of the intermediate nodes involves certain pre-computed hash values which act as acknowledgments from each receiver node (successor) to the forwarder node (predecessor) and also a secure proof through which each intermediate node claims the packets which have been received within a communication session. The proposed mechanism has minimum communication and computational overhead since the secure proof is based upon a hash computation and report submission is secured through symmetric cryptographic primitives. The report analysis process ensures that evading the detection is not possible even in collusive adversarial model.


Index Terms

Computer Science

Security

Keywords

Packet droppers  Colluding adversaries  Reports  Secure proof  Onion hash.