Malicious packet drop attack over the data plane in a MANET involves malicious nodes dropping the data packets after the route formation. In this paper, a security mechanism has been proposed to detect those nodes which exhibit the malicious behavior by dropping the data packets during the data transmission phase after participating in the route establishment phase without exhibiting any malicious behavior. The detection is done based upon a trust management framework employing the Dempster Shafer Theory to represent the trust. The design of the trust management framework has been covered in earlier works and the current work focuses upon its application for the design of a novel security mechanism. Trust is computed based upon the forwarding behavior represented by acknowledgement reports submitted to the source node. The composition of the report ensures that the source node can verify its authenticity. Trust updates upon intermediate nodes are done by the source node at the end of a session which facilitates the secure route formation through the proposed mechanism. The efficiency and accuracy of the proposed security mechanism is validated using the network simulator ns2 and the experimental results show that the proposed mechanism
outperforms the other schemes.

References


Index Terms

Computer Science Wireless

Keywords

Acknowledgement Reports, Packet Droppers, Trust Management Framework, Reward Factor, Punishment Factor.