Abstract

Mobile ad hoc network is based upon multi-hop communication wherein the nodes themselves act as routers as well as source. The inherent characteristics of a MANET make it vulnerable to a variety of insider as well as outsider attacks. Most of the secure routing protocols do not focus on the insider attacks wherein certain adversarial nodes may launch a number of attacks on the routing protocol as well as on the data transmission by simply dropping the packets without forwarding them. We propose a secure hybrid routing protocol which combats the packet dropping attack carried on by an individual / colluding adversaries. It forms routes based upon a metric assigned to each node called weight / cost which indicates its good / bad behaviour. A least cost route has to be formed by including those nodes with least weight representing good packet forwarding behaviour. The protocol monitors the ongoing data transmission in the form of acknowledgements from destination, detects the adversarial nodes on the path through a mechanism based upon bloom filters used as node behavioural proofs, adjusts the weight of the adversarial nodes and propagates the information so that the proactive routing tables involving the adversarial node update their appropriate routing table entries. The result of these activities is the establishment of a route including those nodes with good packet forwarding behaviour.
A Secure Hybrid Routing Protocol to Combat Malicious Packet Dropping in a MANET

References

- Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002


Index Terms

Computer Science
Mobile Networks

Keywords

Colluding adversaries  Packet Drop Attack  Bloom filters  Secure Hybrid Routing Protocol