Abstract

Communication in a Mobile ad hoc network is accomplished in a multi-hop fashion wherein the nodes themselves act as routers as well as source. MANET is vulnerable to a variety of insider as well as outsider attacks because of its inherent characteristics like dynamically changing topology, limited power and no centralized authority to monitor the behaviour of the nodes. Most of the secure routing protocols focus on the control plane attacks targeting the different elements of the routing protocol but data plane attacks are more difficult to handle for which we need to ensure secure data forwarding since certain adversarial nodes may launch a number of attacks on the data transmission by simply dropping the packets without forwarding them. The current paper is an extension to our earlier work where we addressed one of the most difficult data plane attacks namely, the packet dropping attack. In our earlier work, we had proposed a secure hybrid routing protocol which combats the packet dropping attack carried on by an individual / colluding adversaries and elaborated upon the first two phases of Secure Least Cost route establishment and Detection of individual node / colluding nodes maliciously dropping packets. Once a node has been identified as an adversary, we need to work upon the remedial action to prevent the future routes from involving adversarial nodes. In the current paper, we elaborate upon the last two phases namely: Punishing the adversarial nodes upon misbehaviour detection and Propagation of information about node misbehaviour and good
An Extension to Secure Hybrid Routing Protocol to Combat Malicious Packet Dropping in a MANET

behave. The current paper extends our earlier work by considering an additional colluding adversarial model consisting of consecutive nodes on the route from source to destination acting as colluding adversaries. Finally the protocol results in the establishment of a route including those nodes with good packet forwarding behaviour.

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