ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are decentralized wireless networks where nodes communicate without pre-established infrastructure. These networks are susceptible to a variety of security threats, one of which is the Black Hole Attack, where a malicious node falsely advertises the shortest path to a destination and drops all received packets.To mitigate this, a Black Hole Protected AODV (Ad hoc On-Demand Distance Vector) Routing Protocol is proposed, which incorporates additional security mechanisms into the standard AODV protocol. Use cryptographic techniques (e.g., digital signatures, hash functions) to verify the authenticity of RREQ and RREP messages.Nodes maintain a Trust Table to record the behavior of neighboring nodes.Trust scores are updated based on successful packet delivery or anomalies.Implement a delay timer for RREP messages.The source node waits for multiple RREPs and verifies their legitimacy based on route consistency or trust values.Cross-check received RREPs with alternate routes to identify anomalies.Discard suspicious or inconsistent replies.Nodes monitor the behavior of their neighbors to detect packet forwarding anomalies.If a node consistently drops packets, it is flagged as malicious.The source node broadcasts an RREQ message to find a route to the destination. Nodes replying to the RREQ must attach cryptographic proof (e.g., signed hashes) to the RREP.The source node verifies the RREP messages for authenticity and trustworthiness. If a node fails to forward packets or consistently sends fake RREPs, it is marked as malicious and excluded from the route table.This information is shared with neighboring nodes.