ABSTRACT

A Mobile Ad hoc NETwork (MANET) is a group of mobile nodes. The supportive contribution of all nodes is the basis for routing function in MANET. The MANET can exist and perform well only when the MANET nodes behave cooperatively during the data forwarding. The conventional routing protocol, such as Adhoc On-Demand Distance Vector (AODV) routing protocol in MANETs assumes that all the mobile nodes follow the prescribed procedure without deviation. It is highly vulnerable to the black hole attacks due to the open nature of the network. In this attack, a black hole attacker advertises that it has the shortest path to the destination node with the highest sequence number and it is selected as the shortest path to the destination. When the source node receives the fake reply packet, it presumes that the route discovery process is complete and ignores all other reply messages. As a result, the source node sends all the packets to the malicious node. In this way, the malicious node can easily drop the data packets and possibly cause damage to the network resources. Eliminating those attackers from the network becomes a significant issue in MANET. Detecting such malicious node is the primary function of an active Intrusion Detection Systems (IDS). The proposed research offers two noteworthy contributions.
The initial approach evaluates the black hole attack impact on the performance of the AODV routing protocol. The effect of the attack on AODV is measured through simulation under various scenarios. This work creates different scenarios by varying the number of connections, the number of nodes, and node speed. The AODV with black hole attack suppresses the route rediscovery process due to the fake reply of the attacker and continuously drops the packets. It reduces the packet delivery ratio, throughput, as well as routing overhead, compared to the AODV routing protocol. To reduce the hazards from such attackers and enhance the security of the network, this research work extends an AODV routing protocol, named as Node Trust Path Trust Secure AODV routing protocol (NTPTSAODV) for MANET.

Finally, the proposed research work provides a secure NTPTSAODV routing protocol that aims at identifying and isolating the black hole attacks in MANET. The proposed NTPTSAODV routing protocol integrates the data routing behavior with the relative speed in trust measurement to improve the security and reliability of packet forwarding over MANETs in the presence of black hole nodes. The weighted trust measurement along with the node mobility improves the performance of NTPTSAODV routing under dynamic network topology. The trust, which is a measure of faith in the routing behavior of a node, is calculated by maintaining the two counters to count the failure rate of control and data packet
transmissions. The simulation results show that the NTPTSAODV improves the throughput by 41.4% and 58.3% compared to the BDAODV and AODV respectively. The NTPTSAODV provides better performance and capable of delivering packets to the destinations even in the presence of increasing number of malicious nodes with high delivery ratio and overhead, low end-to-end delay and packet loss ratio. Also detect single as well as multiple black hole attacks under MANETs.