Abstract

ABSTRACT

Mobile Ad-hoc Networks (MANET) are gaining popularity as they allow independent mobile nodes to communicate with each other through radio waves. The dynamic nature of MANET demands that network topology changes frequently, requiring frequent updates to achieve efficient data routing. Ad-hoc On-demand Distance Vector (AODV) is the most efficient ad hoc routing protocol for MANET, which discovers neighbors by broadcasting a Hello message and uses a Route Request (RREQ) message to multicast to the neighbors of the source node. However, AODV is not suitable for dense networks due to issues like the constant route cache timer expiring before receiving replies from all neighbors, inadequate route management, and high network overhead introduced during route discovery. AODV may be suitable for sparse networks, but it affects the network's throughput performance and Quality of Service (QoS) overall.

The present research has developed the security mechanism against attacks with the help of protocols to address the security threats occurring during data transmission in MANET environment. Several protocols like Ad-hoc Network Management Protocol (ANMP) and Internet routing protocol for efficient attack detection have been reported in literature. Those protocols enable accommodating the sheer number and node heterogeneity of both independent as well as survivable for adapting to network dynamics. However, the limitations exist in terms of poor attack detection, lower energy efficiency, higher packet drop ratios, and bandwidth consumption. As a result, the security of the network in question cannot be guaranteed due to decreased performance and a substantial decrease in overall efficiency.

The most of the existing protocols have been developed to identify either black-hole or gray-hole attacks during the route discovery stage. There are only a few unified

protocols to identify both types of attacks. In addition, the attacks during data transmission can degrade the transmission efficiency by dropping data packets, which affects the network throughput. Therefore, it is necessary to identify the attacks during the data transmission stage.

An insufficient dynamic structure of a MANET makes it particularly vulnerable to various routing attacks. Black-hole attacks are suspected nodes that emerge in the system and surreptitiously reject data transmitted or received. The discovery and avoidance of this attack are made more difficult by the constant denial of information during the exchange. The black-hole node is a node that joins the AODV protocol by declaring itself as a legitimate route for the target. It builds a new route to the target node via the source node and rejects packets from any other nodes, preventing valuable data from being exchanged. Gray-hole nodes forward data in the same way as regular nodes do. However, it may reject packets selectively without confidence and realize suspected behaviors based on rejecting or broadcasting packets from other nodes. Sequence number assaults are another name for black-hole and gray-hole attacks.

In the recent trends, Mobile Ad-hoc Network (MANET) have yielded tremendous opportunity and popularity, which insisted on many kinds of research to focus on it. This highly flexible nature of the MANET also creates many networks performance-related and security related issues. Various security vulnerabilities threaten the process in MANET in various ways. Sequence number attacks such as grey hole and black hole attacks are such dangerous attacks that significantly weaken the functioning and performance of the network in different situations. However, it is necessary to authenticate the nodes during data transmission since the gray-hole nodes broadcast an accurate Target Sequence Number (TSN) during the route discovery, whereas it becomes malicious and drops the

packets during the data forwarding. In addition, different kinds of attacks such as black-hole, grey-hole, and sink-hole, bogus, modification attacks, and route fabrication attacks, etc. influence the network lifetime and data transmission efficiency.

The proposed framework is to protect the mobile ad-hoc network from distinct attacks. This work contains four phases: (i) Secure Route Discovery (ii)Attack Discovery based on Energy and Trust (iii) Distinct Attack Identification (iv) Protecting MANET's from distinct Attacks. In the first phase of this work, developed a hybrid framework with secure neighbor discovery, node authentication using MECDHA and malicious node detection and isolation process. The hybrid framework is incorporated with the AODV protocol and changed as SRD-AODV. The proposed work achieves good attack detection rated and improves the packet delivery. In the second phase of this work, black hole and grey hole attacks are identified and minimized energy consumption. Hence, the data packet dropping was mitigated and the routing overhead was reduced. In the third phase of this work, the SIIDAI protocol was developed to identify various types of attacks based on their SAP number. In the fourth phase of this work the SIIDAI protocol with DPI used to prevent the packets from various attacks, the simulation results showed that the proposed SIIDAI protocol with DPI has an average end-to-end delay of 3.46 seconds, a PDR of 91.98%, and a throughput of 87.84 kbps. In the final phase of this work, the proposed methodology protected packets from sequential attacks based on their DPI number. The SIIDAI protocol based on DPI number protected the MANET from six different attacks namely black-hole, grey-hole sink-hole, bogus, modification attacks, and route fabrication. The SIIDAI protocol is simulated by the Network Simulator and its efficiency is compared with the existing protocols.