ABSTRACT

This research is a result of the analysis of the attacks that Mobile Ad Hoc NETworkS (MANETS) face in routing, service and resource consumption. This research is done on the principle that there could be a layering of protocols for MANETS that would show impressive characteristics in the defense of the different types of attacks. Four protocols are proposed to defend against DoS (Denial of Service) attack.

MANETS are multi-hop wireless networks and are ever expanding to take up the centre stage in communication industry. The problem of unsecured MANETS i.e., those that have no permanent infrastructure is totally different from the wire topography or fixed structures. The performance of routing protocols in MANETS is affected by the mobile nature of the nodes. Hence, the fundamental problem is the designing of appropriate protocols which supports greater node mobility for MANETS. The security threats in MANETS include DoS, intrusion and tampering. This research work addresses DoS attack, which is one of the major security threats in MANETS. DoS attack is an attempt to make a computer resource unavailable to its intended users, which aim to destroy the functionality of a network. The attacks on DoS can be categorized into three types (Routing Disruption Attacks, Resource Consumption Attacks and Selective Forwarding Attacks), which are taken into consideration for the proposed system. This research is aimed at securing MANETS from these attacks by proposing new protocols.

In Routing Disruption Attacks, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. The Routing Disruption Attacks are addressed by ESARP (Efficient Secure Authenticated Routing Protocol) and SEARP (Secure Enhanced Authenticated Routing Protocol) to detect routing misbehavior of the nodes. The aim of the proposed protocols is to detect the malicious nodes, which cause problems in routing and account of faulty behavior of the nodes.

The ESARP is proposed to detect the malicious nodes using a digital signature mechanism with the help of route discovery process. It provides a credit based incentive scheme to identify well behaved and misbehaved nodes. With the help of a credit counter, it reduces the unnecessary overhead of verifying the intermediate node signature for each time during a data transfer process. The credit counter increments the credit for a positive routing and decrements for negativity. It is proposed to identify the misbehaving nodes by proposing a new algorithm for updating the routing table entry. Thus the need for route maintenance is eliminated. Experiments involving this new algorithm show the effectiveness of the route discovery process with a routing table updated periodically. The SEARP is proposed to avoid link breakage using congestion avoidance and load balancing. Based on time factor, it proposes a route cache mechanism to provide better network performance for data transfer.

In Resource Consumption Attacks, the attacker injects packets into the network to consume valuable network resources such as energy. These attacks are addressed by the EESARP (Energy Efficient Secure Authenticated

Routing Protocol) to provide a balanced selection of fast paths and better use of network resources. This protocol is proposed to find best nodes in terms of residual energy and end-to-end delay. It increases path availability and reduces travel time of packets.

In Selective Forwarding Attacks, the neighboring nodes will faithfully forward their messages to the base station. However, a malicious node that has included itself in the path of data flow can refuse to forward certain messages. The Selective Forwarding Attacks are addressed by the RARARP (Reliable Attack Resistant Authenticated Routing Protocol) to achieve high reliability with increase in delivery ratio and decrease in delay. This attack can potentially drop the throughput of a host to zero. The proposed protocol provides resistance against these attacks by preventing the nodes from getting overloaded. By selecting non attacked routes for data passing, it achieves reliability in routing by punishing the link to its parent as defective or finding a new route to the destination.

The positive results have encouraged these four protocols to create a very effective mechanism that can ward off all the three types of attacks (Routing Disruption Attacks, Resource Consumption Attacks and the Selective Forwarding Attacks) faced by MANETS. The proposed protocols take ad hoc reactive protocols (Secure Ad hoc On-demand Distance Vector routing protocol, Ad hoc On-demand Resilient Path routing protocol and Secure Dynamic Source Routing protocol) as their base protocols to carry out this research work.