ABSTRACT

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infra-structure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple network hops are needed for one node to exchange data with another across the network. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets to other mobile nodes in the network that may not be within the direct reach wireless transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi hop paths through the network to any other node. The concept of an ad hoc network is sometimes called as infrastructure-less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

The wireless ad hoc nature of Mobile Ad hoc Networks brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks. During passive attacks, an attacker just listens to the channel in order to discover valuable information. This type of attack is usually impossible to detect, as it does not produce any new traffic in the
network. On the other hand, during active attacks an attacker actively participates in disrupting normal operation of the network. This type of attack involves deletion, modification, replication, redirection and fabrication of protocol control packets or data packets. Securing ad hoc networks against malicious attacks is difficult to achieve. Preventive mechanisms include among others authentication of message sources, data integrity and protection of message sequencing, and using intrusion detection systems to identify and prevent the malicious nodes to perform attacks. Incorporating cryptographic mechanisms like authentication is challenging, as there is no centralised key distribution centre or trusted certification authority. These preventive mechanisms need to be sustained by detection techniques that can discover attempts to penetrate or attack the network.

The work is concentrated primarily on the provision of security in the On-demand routing protocols like Ad hoc On Demand Vector (AODV) and Dynamic Source Routing (DSR) since they are efficient for routing in large ad hoc networks and they initiate and maintain the routes that are currently needed. The work proposes the application of Dual Hash Authentication Technique (DHT) in association with Self-Healing and Optimizing Routing Technique (SHORT) in AODV. In Dual Hash Authentication, one hash function is used to authenticate the received routing packets and the other one is used to prevent the current nodes modifying the routing information themselves. SHORT helps all the neighbouring nodes to monitor the route and try to optimize it, if and when a better local sub-path is available.
The work also proposes Triple Hash Authentication Technique (THT) which is almost similar to DHT but included HMAC authentication for the third one between the source node and destination node. This THT is also applied to both the on-demand routing protocols as mentioned above. In addition to the above techniques, Digital Signature mechanism is applied to the routing protocol DSR and its performance is compared with DSR and AODV. The work further proposes the application of intrusion detection system (IDS) and GeOmetric DOMinated set algorithm (GODOM). The IDS is used to check every packet using some threshold value in order to identify the malicious packets. GODOM algorithm is used to find out the number of active nodes in which the IDS can be installed. This work is also applied to both AODV and DSR.

The performance of the protocols with the above security mechanisms is evaluated using the Network Simulator (NS2). The performance is analysed based on the metrics Packet Delivery Ratio, Control Overhead and Packet loss in the case of authentication based security mechanisms. In the case of IDS based security mechanisms, the performance is analysed based on the parameters Selecting active nodes, Packets sent, Malicious Packets detected and Packet Delivery Ratio. In both the cases, the results show that DSR protocol is performing better than AODV protocol.