ABSTRACT

Mobile Ad hoc Network (MANET) is the assortment of cooperative wireless nodes without physical existence of any access network point or infrastructure. This thesis addresses issues pertaining to mobile adhoc networks due to lack of infrastructure and dynamic mobility. MANETs are gaining attention in the increasing real life applications such as military, conference management system, search and rescue applications. Consequently, these are beneficial in classrooms, conventions where students share their views dynamically through mobile devices. In these networks, each node in the network must be able to take care of routing of the data and this is the domain of ad-hoc routing. Requirement of efficient routing algorithm is a major requirement in mobile adhoc networks. Fulfillment of this requirement has been a complex problem due to lack of fixed infrastructure and rapid movement of nodes.

The mobility of these nodes imposes issues in terms of mobility management, energy consumption, battery life and security. The main contributions of the thesis are in the areas of mobility management, random scenarios, battery life & processing activity and security. In the thesis, comprehensive review of existing routing protocols and their issues have been studied in detail. To provide secure routing in adhoc networks, it is essential to authenticate each node. The presence of malicious nodes in an adhoc network deteriorates the network performance. In this thesis, two new algorithms have been proposed by enhancing the AODV (Adhoc On Demand Distance Vector). Enhanced AODV provides a solution against threatening attacks in mobile adhoc network. Enhanced AODV method requests its next hop to send a confirmation message to originating node by maintaining ECC (Elliptic Curve Cryptography) table. After acquiring Route Reply (RREP) and confirmation message, the source node determines the validity of paths.

Further, another algorithm EIDS-AODV (Enhanced Intrusion Detection System in Adhoc On demand Distance Vector) modifies AODV protocol and defends against malicious nodes without using cryptographic algorithms. It has been assumed that all benevolent nodes are regular and well behaved in nature. A node is considered suspicious if it is moving out of transmission range after route discovery, or if communication breakage occurs during data transmission and also sequence number
of rebroadcast RREQ (Route Request) is not equal to the same RREQs already exists in the routing table.

Further work, analyzed the nature of identified suspicious nodes by calculating their confidence value and node capacity. If analytical results moves towards negative effects with respect to confidence value and node capacity then a suspicious node will become a malicious node. Enabling and disabiling of power factor minimize energy conservation and requires minimum overhead. Analytical results are computed through RUP (Rational Unified Process: Rational Application Development Tool). Algorithm is improved and extended by adding more realistic strategies such as varying node position, movement, speed and traffic scenarios. Apart from identification of malicious node, it has been observed that this approach leads to less conservation and less communication breakage in adhoc routing. The experimental results demonstrate that proposed approach can effectively detect malicious nodes in ns2 (Network Simulator). This approach has been found beneficial for identifying malicious nodes in network layer attacks for large network scenario.

Proposed work not only identifies the malicious nodes but also removes malicious nodes from the network. In this thesis, it has been assumed that transitive trust calculation process is not applicable in real life scenarios. It has been accentuated that proposed work is most appropriate for adhoc networks and can be established on the fly without requiring a dedicated trust infrastructure or pre-configuration of nodes.