Abstract

An Ad-hoc Network is a self configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. Each node or mobile device is equipped with a transmission and receiver. They are said to be purpose-specific, autonomous and dynamic. Ad-hoc networking is a concept in computer communication, which means that users wanted to communicate with each other from a temporary network, without any form of central administration.

Term Ad-hoc means a network which can take different forms in terms of topologies and in terms of devices used. Ad-hoc devices can be mobile standalone or networked. A mobile Ad-hoc Network (MANET) is an autonomous system of mobile hosts which are free to move around randomly and organize themselves arbitrarily. MANET is viewed as suitable system which can support some specific applications as virtual classrooms military communications, emergency search and rescue operations, data acquisition in hostile environment communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc. In Ad-hoc Network nodes can change position quite frequently. The nodes in an Ad-hoc network can be laptops, PDA (personal digital assistant) or palm tops etc. These are often limited in resources such as CPU capacity, storage capacity, battery power and bandwidth. Each node participating in the network acts as both as a router and as a host and must therefore be willing transfer packets to other nodes. For this purpose a routing protocol is needed. Ad-hoc network has a certain characteristics which impose new demands on routing protocols. The most important characteristic is dynamic topology, which is a consequence of node mobility.
The Internet Engineering Task Force currently has working group named Mobile Ad-hoc Networks (MANET) that is working on routing specifications for Ad-hoc Networks. This thesis evaluates some of the existing protocol and suggests a new protocol. To accomplish this task several routing protocol for Ad-hoc Networks have been studied such as Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA) and Ad-hoc on Demand Distance Vector Routing (AODV). In all the protocols major emphasis has been on stable and shortest routes, while ignoring major issue of security. Performance of protocols suffers due to Malicious Nodes but there is no effective mechanism to detect these Malicious Nodes. Whenever break occurs most of the protocols proposed require knowledge of the network topology for routing. These protocols involve communication overheads of route maintenance and route discovery. Taking into account all these parameters, in this study, a new routing protocol Reverse On-Demand Distance Vector Routing Protocol (RAODV) has been proposed. This protocol uses the concept of Node Status to check whether the Node is Malicious or not. The scheme is designed for a secure and stable path for communication.

RAODV establishes a stable and secure route using various phases. Every phase performs a specified task.

RAODV has the following phases:

(I) Route Request (RREQ)
(II) Route Reply (RREP)
(III) Data transmission (DTRAM)
(IV) Detection of Malicious Nodes (DMALN)
(V) Route Error (RERR)
(VI) Route Repair (RREPR)
(VII) Establishing New Path (ESTNP)
RREQ phase set status of each Node, participate in the routing process. Node status has been set with the help of Source and Destination Node Sequence Number. Status of all Nodes set as ‘TRUE’ whose Sequence Number in between the ‘Source Node Sequence Number’ and ‘Destination Node Sequence Number’ and Node status is set as FALSE whose Sequence number does not match with the given condition. Nodes have TRUE status enters in to Non_Malicious Array and Node have FALSE status enters into the Malicious Array.

RREP phase sent available RREP to the Source Node. If multiple RREPs are received by the Source, it selects the path on the basis of shortest path algorithm.

DTRAM after selecting the path, transmission starts between the Source Node and Destination Node.

DMLAN phase checks status of every Node in the active route. If it finds any Node in the current route that does not belong to Non_Malicious Array it declares this Node as Malicious Node.

RERR phase generates a RERR after the detection of Malicious Node. As the RERR propagates towards the Source, each intermediate Node invalidates routes to any unreachable Destinations.

RREPR phase tries to repair the route locally by releasing a RREQ to find a new route to the Destination and if it is not able to repair the route it release RERR to the Source.

ESTNP phase invalidates the route and reinitiates route discovery. If more then one routes are available it selects the shortest route and establishes a path between Source and Destination.

RAODV again verifies status of each Node in the new Route. This process repeats until RAODV establishes a stable and secure path for data transmission between Source and Destination.
The proposed protocol was designed to provide better security in efficient manner. Modified schemes introduced here is effective for active attacker. It identifies the active attacker and keeps them away from the route for further communication. The work carried out contributes in terms of proposed new protocol modification to the existing protocol and gives a new secure authentication scheme in routing to enhance security.

The Organization of the thesis is as follows:

**Chapter 1** contains a short description of Infrastructured Wireless Network, Infrastructure-less Wireless Network, Mobile Ad-hoc Network (MANET), History of MANET, Characteristics of MANET, Applications of MANET, Advantages of MANET, Disadvantages of MANET and Objectives of the work. **Chapter 2** is about research motivation and problem statement. Various security issues have been discussed in detail. **Chapter 3** introduces an extensive literature survey in the field of security in ad-hoc networks and also about the existing secured protocols in MANET. **Chapter 4** is the crux of the thesis which describes proposed scheme with detailed algorithms and its implementation using various scripts and scenarios. Simulation tools are investigated, and results of the various metrics applied on various protocols and summarized in **Chapter 5**. Last, Conclusions and the future scope of the research is discussed (and discuss future research topics) in **Chapter 6**.