Chapter 2

Literature Review

2.1 Introduction

Ad hoc wireless networks are self creating, self organizing and self administering [18]. In addition to this, each node in the network must be able to take care of routing of the data; these networks have the ability to form anywhere, anytime as long as two or more wireless users are willing to communicate [31]. In adhoc networks, routing is a critical issue. In adhoc networks, whole scenario is related with issues like medium access, routing, multicasting, transport layer, QoS, self organization, security, energy management, mobility management, addressing & service discovery, constrained bandwidth, scalability, random scenario, battery life & processing activity and pricing schemes.

Thesis work emphasizes on four out of above mentioned issues which are mobility management, random scenarios, security and battery life & processing activity. Keeping these four issues in view, objective of the thesis, exhaustive literature review has been done. In this chapter, comprehensive review on routing protocols is discussed in section 2.2. Section 2.3 presents issues of routing protocol and section 2.4 concludes the chapter.

2.2 Comprehensive review on existing routing protocols

There has been a rapid development in ad hoc networks making routing an active research topic. In ad hoc routing protocols, each node can discover multi-hop paths through network to any other node in the network. It can be classified into several kinds such as (i) Routing information update (ii) Temporal information for routing (iii)Routing topology[32] (iv)Utilization of specific resources. In this chapter, we review routing protocols based on topology. These protocols can be divided into three types as follows: (i) Proactive (ii) Reactive and (iii) Hybrid Routing.
In table-driven routing protocols (proactive routing) [33], information is periodically advertised to all nodes. So, all nodes have an up-to-date view of the network. Each node maintains information of other nodes in the routing tables and regularly updates information when node moves. And these protocols are also not suitable for large networks.

On the other hand, on-demand routing protocols (reactive routing) only discovers a new route when it is required. It has been found that table-driven schemes are more expensive in terms of energy consumption as compared to on demand schemes because of the large routing overhead incurred in the former. Thus, on-demand approach is preferable for designing minimum energy routing protocols. Fig 2.1 presents the detailed classification of routing protocols in mobile adhoc networks which mainly focuses on security feature for improving the performance of network.

2.2.1 Table Driven Routing Protocols

Table driven routing protocols are based on periodic exchange of control messages which are sent locally or throughout in the network. Thus, a route is frequently available when required. Various protocols such as DSDV, R-DSDV (Randomized Version of DSDV), FSR (Fish State Routing), CGSR (Cluster head Gateway Search Routing), OLSR (Optimized Link State Routing), TBRPF(Topology Based Reverse Path Forwarding), DREAM(Distance Routing Effect Algorithm for Mobility) etc. are examples of table driven routing protocols which as summarized as follows.

i. **DSDV (Destination sequenced distance-vector routing protocol):** DSDV [12][13] is an enhancement of Bellman Ford algorithm. Updation in table and sequence number leads to prevent problem like routing loops and count to infinity problem. In this mechanism, routes to all destinations are readily available at every node at all times. The tables are exchanged [5] between neighbors at regular intervals to keep up-to-date view of the network. Neighbor nodes use missing transmissions to detect broken links in the topology. When a broken link is found, it is assigned a metric value equal to
ii. **R-DSDV**: It is an enhancement of DSDV and known as randomized version of Destination Sequence Distance Vector [34]. It uses congestion control mechanism [29] using probabilistic model. This protocol enables each node to decide whether or not to forward/drop a packet and what type of packet to forward/drop. This process is known as randomized decision of node. The decision process is based on congestion value. This value is maintained by each node. At the arrival of packet, if congestion level is high then packet is dropped otherwise not.

iii. **FSR (Fish State Routing)**: This protocol [35] refers multilevel scope. This protocol is applicable for large networks where high mobility and low bandwidth is required. FSR was designed to reduce message overhead in dynamic environment. Each node stores link status for destination in the network. It broadcasts link state updates of a destination to its neighbors. From such updates, topology of entire network is formed by a node. This node computes efficient routes. This approach follows fisheye concept which maintains accurate and optimal path information about immediate neighborhood of a node. In this process, node rapidly shares information with its nearest neighborhoods and less frequently with distant nodes. Thus it alleviates problem of message overhead but it increases bandwidth issue when node density increases.

iv. **CGSR (Cluster head Gateway Search Routing)**: This protocol [36] is designed to provide effective membership and traffic management. It is based on distance vector routing protocol. In this protocol, the whole network can be partitioned into clusters. And each cluster maintains one cluster head and at least one gateway node. By using the concept of cluster, it reduces the size of table as compared to distance vector protocol. But the maintenance of cluster structure is very difficult in CGSR.
v. **OLSR (Optimized Link State Routing):** This protocol is an enhancement [5][37] of LSR and follows the concept of multi point relays(MPR). Nodes selected as relay can forward the data and are defined as one hop neighbors. Nodes regularly broadcast beacon messages to its one hop neighbors, which include the list of neighbors to which a link exists. Selecting multi point relay nodes as the forwarding stations reduces the link state information which reduces overhead of OLSR protocol.

vi. **TBRPF (Topology Based Reverse Path Forwarding):** TBRPF [38] is based on link state algorithm. It uses tree topology and dijkstra algorithm concepts to minimize overhead and increase robustness. In TBRPF, each node forwards each update along a minimum hop tree and also provides more information than it requires. It reduces communication cost. It uses reverse path forwarding process which is applicable to large networks and as a result it greatly decreases collision and traffic.

vii. **DREAM (Distance Routing Effect Algorithm for Mobility):** It is a proactive [39] and location based routing protocol that follows the concept of directional flooding to forward data packets. In this approach, routing table stored at each node contains location information for any other node in the network. When node N1 wants to send a packet to node N2, it uses the location information for N1 to obtain N1’s direction and then transmits msg to all its one hop neighbors in the direction of node N2. Each neighbor node repeats this process, until B is eventually reached. Thus there will be multiple copies of each packet at the same time. The probability of finding N2 in the computed direction relies on how the location information is disseminated through the network.

### 2.2.2 Reactive (On demand) Routing Protocols:

Such protocols are superior to proactive routing protocols and are reactive in nature, known as dynamic routing protocols. These protocols are based on on-demand route discoveries. Thus route are determined only when they are required by the source node.
i. **DSR**: It is known [14][5] as source routing protocol. This protocol is particularly designed for use in multihop wireless adhoc networks. It maintains two mechanisms:

a) **Route Discovery**: When a source node S (initiator) sends a packet to destination node (target node) D, it searches a possible route in its route cache. In this process, it stores discovered routes in route cache. Route discovery requires 7 fields during this process such as sourceid, destid, ReqID, Addresslist, Hoplimit, NetworkInterfaceList, Acknowledgment list. Initially source node contains address list as empty and RREQ message contains 3 fields as source ID, destination ID, Unique RREQ ID. Then source node broadcasts the message within its transmission range. And source node also maintains a replica of send message in its buffer, known as send buffer. Time frame plays major important factor. Packets can be dropped (i) if buffer is overflow or (ii) route is not discovered within specified time. When a node receives a RREQ message then reverse process generated otherwise it searches its own route cache for a route to the target. And node id is added in the address list and again RREQ is broadcasted.

b) **Route Maintenance**: To maintain this process, it is essential to maintain the routes that are stored in the route cache.

ii. **AODV (Ad hoc On Demand Distance Vector Routing)**: This protocol [15] is combination of DSR and DSDV routing protocol. It uses route discovery process same as DSR make use of hop by hop routing like DSDV. In DSDV, each node knows its neighbors and costs. And node maintains its own routing table, storing all nodes in the network, the distance and next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors periodically its whole routing table. Thus node can verify efficient route to another node using this neighbor as next hop. Count to infinity problem arises, incase of link breakage. After finding a route with other neighbor nodes, it broadcasts a Route Request (RREQ) to all its neighbors. The RREQ propagates through the network until it reaches the destination or a node with fresh enough route to the destination. Then availability of route is unicast by a RREP back to source. Nodes use hello messages for local
iii. **FORP (Flow Oriented Routing Protocol):** FORP \[5\][18][40] is an on-demand routing protocol and it is based on pure flooding mechanism. Moreover, it maintains prediction based multi-hop handoff mechanism. This attempt is used to reduce the effect of communication failure. Its route request process is same as DSR. Additionally, each node that receives flow_req calculates link expiration time (LET). Due to this, destination could easily know when route is about to expire. If it expires, destination node generates a handoff message and propagates it by flooding. When source node receives this message, it can easily identify the optimal path to handoff. Then the source send flow_setup message along the newly chosen route. This protocol generates scalability problem in large networks.

iv. **TORA:** TORA \[5\][31][40] is distributed, dynamic and multihop routing protocol. This protocol is also known as source initiated protocol. TORA is based on the directed link reversal algorithms and provide loop free multiple path routes to a destination node. In this protocol, each node maintains local topology and can detect partitioning of the network easily. This protocol is better than FORP in terms of efficiency, adaptability, scalability for large, dense mobile networks. This protocol is designed to minimize reaction to topological changes at a very low rate.

v. **ABR (Associativity based routing protocol):** This protocol \[5\][18][31][40] is based on distributed source initiated on demand routing. It selects routes based on the stability of wireless links. It is also known as beacon based routing. In this algorithm, each node maintains the count of its neighbors’ beacons and verifies stability of the link. Due to this feature, this protocols results higher attainable throughput. Also, this protocol deals with fault tolerance when base station fails.
vi. SSA (Signal Stability Based Adaptive Routing Protocol): It is an on-demand routing protocol and consider signal stability as a prime factor. In SSA, signal strength is used to rectify a link as stable or unstable. SSA provides more stable routes as compared with shortest path routing protocols such as DSR and AODV. This protocol provides good link stability as compared to other protocols.

vii. PLBR (Preferred Link Based Protocol): This protocol maintains preferred list. This list contains subset of nodes from its neighbors. Selection of node in preferred list is based on link connectivity and node feature. All nodes present in the network receive route request packets due to its broadcast nature. But node present in the preferred list can forward that data. So, this approach minimizes control overhead by using subset of preferred list.

![Classification of Routing Protocol](image)

**Fig 2.1:** Classification of Routing Protocol

### 2.2.3 Hybrid Routing Protocol

Hybrid routing protocols also exist and they try to achieve an efficient balance between both categories of protocols [5][18][31][40]. Nodes within a certain distance
from the node concerned, or with in a particular geographical region, are said to be
with in the routing zone of the given node. For routing within this zone, a table driven
approach is used. For nodes that are located beyond this zone, an on demand approach
is used.

i. **ZRP (Zone Routing Protocol):** It is known as hybrid proactive/reactive scheme.
[31][40]. In ZRP, a node proactively maintains routes destinations within a local
neighborhood, which is considered as a routing zone. Node routing zone is a
collection of nodes whose minimum distance hop from the node is no greater than
a parameter referred to as the zone radius. In ZRP, two types of routing protocols
are used (i) Intrazone routing protocol is used for routing within a zone and (ii)
Interzone routing protocol(IERP) is used for routing outside the zone. Such
protocols are suitable for large area networks by adjusting the transmission range
of nodes.

ii. **CEDAR (Core Extraction Distributed Adhoc Routing Protocol):** It supports
QoS [5][18][31][40] reliable mechanism and based on extracting core nodes in the
network. It employs a distributed algorithm to select core nodes. This algorithm
follows three steps: (i) the establishment and maintenance of the core of the
network for performing the route computations (ii) Propagation, bandwidth
utilization and stability information of links (iii) efficient routing computation
algorithm for QoS provisioning. CEDAR provides robustness and low overhead
infrastructure.

It has been analyzed that each existing routing protocol emphasizes on particular
characteristics of the network and tries to improve things in a certain direction. It is
challenging issue for critical real life applications in which wired networks are not
approachable. Thus, there is need to monitor issues of routing protocols to increase
the performance of routing protocol.
2.3 Issues of Routing Protocols

2.3.1 In Simulation Scenario

Ad hoc routing [5][18][31][42] is still a very challenging issue in mobile ad hoc networks. Various researchers have put their effort in surveys of ad hoc networks and also discussed about the routing efficiency in ad hoc routing protocol. And it has been concluded that there should be an effective criteria to evaluate the performance of routing protocol in ad hoc networks. Simulation is one criterion in which routing protocol relies for testing, validation and performance evaluation. This method is most appropriate in case of high complexity. This technique emphasizes on the behavior of nodes in large network scenario. There are number of simulation tools to accomplish these results like ns2[43], GloMoSim[44], OMNet++[46], OPNET[45], AnSim [47] and QualNet [48][49].

While exploring the possibilities of network simulators [43-39][182-183], two kinds of simulators are available in market.(i) Commercial (ii) Open Source.

i. Commercial based simulator, such as OPNET and QualNet which are not available for the general users without license and have a effective license cost. There is specialized team to maintain the documentation and general updation of these two simulators.

ii. In open source, There is no specialized team for maintaining the documentation and general updation. So, any user (individual or organization team) can put efforts to fix the bugs. Examples are NS2, NS3, OMNET++, JSim, AnSim, GloMoSim etc.

Among all the explored simulators[182-186] it has been analyzed that NS2 has good documentation as well as user support where as incomplete and poor written documentation are important pitfalls of GloMoSim. Network Simulators NS2, NS3 OMNET++ are based on object oriented methodology and GloMoSim is based on procedural concepts. Further, JSim and AnSim are based on object oriented concepts but are limited to traffic and mobility scenarios as well as both simulators do not provide functionality to add any modification in existing or new protocol. In
comparison with NS2, JSim can support up to 500 nodes with maximum execution time. OMNET++ is GUI based simulator and provide efficient results in Wireless sensor networks but it has limitation in context to available protocols, individual models and energy consumption in mobile ad hoc networks. This drawback causes numbers of bugs in reports.

In dynamic environment, large number of mobility scenario is required. For this, mobility scenarios can be generated by changing in parameter such as pause time and speed. In [50] [51], authors have proposed behavior of ad hoc routing protocols in wireless adhoc networks. And it has been concluded that there is need to check efficiency of routing protocol by using different trace files. Suresh Kumar et. al. have designed [52][53] an ad hoc network model for disaster recovery scenario using DSR, AODV and DSDV. From simulation results, authors [50-53] have observed that table driven routing like DSDV provides better results as compared with reactive routing protocols (AODV and DSR) in terms of delay. But in case of high mobility, performance of table driven protocol deteriorates. Further, they have also compared the performance of DSR and AODV. It has been found that AODV provide good results in high load scenarios and DSR is suitable in scenario where paths are limited to few hops and there is a requirement of less number of control overheads. In [54] [55], it is analyzed that AODV routing protocol produces a very consistent throughput with minimal latency in large network scenario while DSR provides varying results in the same scenario. This approach provides limited results with parameters like throughput.

Ad hoc networks exacerbate the perception of that risk because of complex security challenges arising due to increased degree of openness and dynamic scenario. These network usually change due to high mobility, catastrophic failures and break in connectivity of networks. At this time, other nodes may try to establish communication among nodes for data transmission in network. So, it is very difficult to decide whom to trust in discovered nodes. Consequently, some nodes may exhibit a malign behavior and deny their cooperation which degrades network performance and functions. In this scenario, it is very complex to identify roles of nodes throughout in the network.
Thus, network scenario poses critical issues to manage trust in the network. And there is need to develop a model to evaluate authenticate node for efficient data transmission in adhoc environment. For effective results, numbers of scenario results are required and energy consumption can be minimized by turning off unnecessary nodes.

2.3.2 Mobility Management
In ad hoc networks, routing protocol is the basic requirement of mobility management scheme. The mobility management [56] provides packet delivery without delay to their destinations. Both schemes location management and handoff management are incorporated in mobility management schemes. Handoff management [57] focuses on rerouting concept where location management routing protocol use location of a node for enhancing the performance of the underlined protocol routing protocol. In adhoc networks, searching efficient path in adhoc routing is a challenging research issue due to rapid changes in dynamic node mobility.

Node mobility [57] in mobile adhoc routing can be easily addressed through multihop routing discovery. Megha bhatt et. al. [58], have analyzed impact of node mobility for evaluating the performance of adhoc wireless networks. Further, they have incorporated this approach with real life situations like speed calculation of pedestrian.

Theus Hossman [30] has concluded that there are two possibilities to model the mobility of the nodes in a simulation. The first is that node trajectories are measured in a real network, for instance, node positions can be measured with a GPS device, and then can be used as input for driving the simulations.

The second possibility is to use mobility model, which maintains set of rules of how nodes behave. But mobility model reflects behavior of nodes only to a certain degree. So, these approaches are not sufficient enough to solve these problems and there is a need to model the mobility of nodes in simulation [10] by taking care of above discussed problems.
2.3.2.1 Mobility Models Overview

In ad hoc networks, mobility models depict [59] movement pattern of mobile users and how their location, velocity, speed, direction and acceleration change over time. Mobile nodes communicate directly with each other. Due to limited transmission range and battery life, communications between two nodes does not produce effective results where nodes are not in same transmission range. This problem can be violated by using intermediate nodes with routing. Thus routing is very important in mobile adhoc networks where mobility models must be evaluated with respect to end to end delay and efficient data transmission.

Mobility models are intended to focus on individual movement patterns due to point to point communication in cellular networks [54][60-62] whereas adhoc networks are designed for group communication. In adhoc networks, these models [63] are designed to maintain movement, and efficient transmission among nodes in real life applications.

In addition to this, these models focus on the individual motion behavior between mobility era with minimum simulation time in which a mobile node moves with constant speed and direction. These models represent the features of the mobile nodes in an adhoc network like speed, direction, distance and node movement. Mobility models [64] can be categorized based on the following criteria which are based on dimension, scale of mobility, randomness, geographical constraints, destination oriented and by changing other parameters. Generally, there are two types of mobility models (i) Trace based mobility models and (ii) Synthetic mobility models. Trace models provide mobility patterns based on deterministic approach whereas synthetic mobility models present movements of mobile nodes in realistic manner.

2.3.2.1.1 Trace Models

For predicting stability of the nodes, movement patterns history and monitoring on periodic movements is required. Movement pattern of nodes provide path of a mobile node which maintains the degree of stability in the network. In [30][63][65], authors have concluded that stability of the nodes can be enhanced by predicting future positions of the nodes.
2.3.2.1.2 Synthetic Models

Such type of models is very close to real life situations. Synthetic mobility models are categorized in two types (i) Entity based group mobility model and (ii) Group Based Mobility Model. Entity and group mobility movement models maintain mobile’s traversing pattern from one place to another in a given time. Each type of models is further categorized as constrained based or statistical based mobility model [66-67]. In Constrained topology based mobility models, mobile nodes have only partial randomness where the movement of nodes is restricted by obstacles, pathways, speed etc. In Statistical mobility model, mobile nodes have total randomness where nodes are allowed to move anywhere in the area and the speed and direction are allowed to choose.

<table>
<thead>
<tr>
<th>Mobility Models</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traces and Synthetic Models</td>
<td>Mobility generation</td>
</tr>
<tr>
<td>Group based and entity based models</td>
<td>Social behavior</td>
</tr>
<tr>
<td>Statistical Mobility model and constrained topology</td>
<td>Randomness (Total/Partial)</td>
</tr>
</tbody>
</table>

Table 2.1: Criteria for classification of mobility model [68]

2.3.2.1.2.1 Entity based mobility model

i. Random Walk Mobility Model

Initially, it was used by Johnson et. al and Lee et. al [56][64][66][68-75] which is based on Brownian motion. It is a simple entity mobility model and also known as memory less mobility model where each node moves in a straight line at a constant speed throughout the simulation time. In this model, changes in terms of direction and speed are monitored by considering pause time. If time expires then mobile node chooses a random destination as well as a speed that is uniformly distributed between interval 0 and maxspeed.

ii. Random Waypoint Mobility Model

This model [56] [67][69][76-77] is widely used by researchers. It generates non homogenous spatial distribution of nodes. In simulated area, mobile node selects a
random position and velocity v which lies in the range from maxspeed and minspeed. It contains the features of both entity and statistical models. As mobile node starts movement for choosing destination at selected speed, it then pauses for a time interval and start the process again. It then rests for a certain pause time and repeats this process till the simulation continues. Velocity and pause time are two important parameters used in this model. Topology of adhoc network is stable in low velocity and long pause time where as topology is highly dynamic if velocity is high and pause time is short. So, by varying these parameters, we can generate various mobility scenarios with different levels of node speed. This model is most approachable in the applications like at airport.

### iii. Random Direction Mobility Model

It is an entity mobility model and is similar to [56][78-79] random walk mobility model.. In this model, a mobile node selects a direction and speed from uniform distribution of (0,360°) and interval between maxspeed and minspeed. A node moves in the direction of (0,360°) until edge boundary is found. After reaching at boundary, mobile node selects another direction between (0,180°), destination along with direction and then continues the process. This model avoids center clustering of Random Waypoint Model.

### iv. Gauss Markov Mobility Model

This model [56][67][80] was designed to maintain different levels of randomness by using one varying parameter alpha in mobility pattern. This pattern is based on statistical mobility pattern ,and overcomes the problem of sudden changes in random waypoint mobility model. At each fixed intervals of time, n a movement occurs by modifying the speed and direction of a node. If value of alpha is zero then, Brownian motion is obtained and if alpha is equal to 1, then linear motion is obtained. By varying the value of alpha [0, 1], intermediate levels of randomness could be obtained. Value of the next location is calculated based on the current location.
Fig. 2.2 (a): Types of Mobility Model in adhoc networks

v. **Boundless simulation area**

In this model [30][56][64][67][70][77], speed and direction of each node is changing rapidly. At every regular time, node adjusts its direction and speed by making changes in the current values of these two parameters. In this model, nodes move in
unobstructed way in the simulation boundary. As a result, it converts 2D rectangular area into torous shaped simulated area.

![Simulated Area Diagram]

**Fig 2.3:** Boundless mobility model in simulated area

vi. **Probabilistic version of Random Walk**

It is based [30][56][67][70][77] on markov chain model. It maintains 3x3 probability matrix which represents three states with respect to x direction as well as y direction. State 0 symbolizes Node Stays, State 1 shows movement of a node in backward direction whereas state 2 illustrates node’s movement in forward direction.

vii. **City Section Mobility Model**

In this model [66], simulation area represents streets within a city. By using map, mobile node can move along the grid of streets on the map. Such models [56] [64] [67] [70] [77] are placed in real or imaginary city map. This model has certain limitations in terms of speed and unidirectional.

viii. **Brownian motion Mobility Model**

It maintains continuous time stochastic process in which node moves with brownian motion in two dimensional planes. In this model, there is no correlation among the nodes present in the network.

2.3.2.1.2.2 **Group Based Mobility Model**

In this model, nodes coordinate in the same group. Apart from group communication, behavior of node is also considered. In real life situations, there is need to check the behavior of nodes by their neighbors. In [64], author has discussed various real life examples for group model. “For example, a mobile user is willing to know the route from his home to office. When hearing on FM radio that there is an accident on the way to work, then he can take an alternate path. Another example is if a group of
people are searching for a missing object. Then there is need of proper coordination among nodes for identifying the missing object”.

**Fig 2.4 Group Mobility Overview [81]**

i. **Reference Point Group Mobility Model (RPGM)**

RPGM model is based on reference velocity in mobile adhoc network. In this model, each [77][79][81-83] node moves in the group. It divides movement of entire group and movement of each node in the group. Each group has group leader which determines group’s movement behavior. Mobility group of the node is represented by actual positions of the nodes.

However, it is hard to evaluate actual positions of the nodes as well topology changes of each node in the group. In addition to this, velocity and coverage of a group is considered. Monitoring of behavior is important in real life applications like military deployment where number of soldiers may move together in a group.

ii. **Column Mobility Model**

In this model [81], center movement is defined as movement of group behavior in terms of velocity, speed, position, direction and acceleration.

iii. **Pursue Mobility Model**

This model is used for tracking the targets. For e.g. police want to catch the thief. Consequently, mobile nodes track a particular target. The current position of mobile node is evaluated by adding old position of node and accelerated value of old position with random vector. The value of random vector is calculated by an entity mobility
model. Initially, location of target node is stored at position \((x_1, y_1)\). Then verify all the number of nodes and register location of pursuing node \(P(x_2, y_2)\). If distance of pursuing node is less than distance of target node then evaluate current position of the node otherwise target node is being tracked by pursuing node.

iv. Nomadic Community Model

It is a [66] group mobility model where group of mobile nodes move from one position to another. Such models are beneficial in various real life applications like conference management, military, agriculture etc. Rigid movement among the nodes is required when group travels from one location to another. In this model, reference point of each node is determined based on the general movement of the group. As compared [84] with column based mobility model, this model shares same reference grid whereas column based model uses one reference point w.r.t. each column.

Dynamic topology [70] and random mobility nature among mobile nodes increase vulnerabilities of adhoc networks. Adhoc random mobility patterns of node in adhoc network make it hard to detect anomaly behavior of a node. It is desirable [85] for adhoc network policy to be robust and secure to different node position and node velocities. So, there is need to authenticate nodes in mobile adhoc networks due to frequent changes in nodes mobility.

2.3.3 Battery life Management and processing

In mobile adhoc networks, energy consumed by mobile devices is significant factor that limits the battery life. Each node has limited transmission energy and far nodes use multi hop approach for data transmission. Rapid topology change, limited bandwidth, limited battery and low transmission power are major challenges for mobile ad hoc routing. Initially, energy is assigned to each node in adhoc environment for initiating battery life of node. Such scenario demands for network partitioning into logical group, so that these issues could be met easily.

Thus, proper utilization of node energy is very important. Transmission power control mechanism provides an optimum solution to overcome this problem. Also, there is need to concentrate on optimum approach for saving battery life of nodes. P.R.
Kumaret. Al and Krunz et. al have suggested transmission power control scheme. In this algorithm, each node transmits low energy and interference by adjusting transmission power in the network [87-89].

In [90], authors have discussed an adaptive transmission power control scheme based on autonomous clustering. Suggested scheme adjusts the transmission power of each node by estimating distance between the node and neighboring nodes. In addition to this, it removes the occurrences of unidirectional links to adjust transmission power and packet loss due to interference. In [91], author has proposed protocol in which node energy is based on the condition of routing control. Additionally, author has highlighted energy balancing between nodes by omitting low energy nodes in routing. This protocol provides insufficient results in terms of overhead. In continuation with this approach, Dheeraj et. al.[92] has discussed energy consumption of proactive and reactive routing protocol based on exponential source traffic rather than CBR source traffic. And this work can be enhanced by using Pareto traffic source approach. In [93], authors have suggested that topology control is another technique to improve the multihop routing. By this concept, transmit power of each node can be adjusted by optimizing performance measures such as throughput, connectivity, lifespan of networks of battery powered nodes, simplifying the routing algorithms. Further, impact of topology control algorithm is evaluated by considering statistical properties into an account. This approach provides good results in large networks.

Ramanathan et. al [94] proposed topology control mechanism which are designed to minimize transmit power of each node (saving battery life and maintain connectivity) in mobile adhoc networks. Energy optimization by transmission range adjustment in mobile adhoc networks is suggested by Erdun Zhao et. al[95]. Authors compared hop by hop transmission protocol, direct hop transmission protocol and Energy Balanced transmission protocol. In addition to this, a novel scheme Energy Optimized and balanced by transmission range adjustment (EOBTRA) is proposed. For this, iterative algorithms are used to select optimal route nodes and their transmission ranges. Further this approach can be beneficial for other protocols. From survey results, it is concluded that efficient path maintenance in routing by using mobility parameter is very complex task. Consequently, [96] has proposed PARO protocol maintains route using route maintenance by electing redirectors.
Further, distributive adaptive topology algorithm is proposed that maintains local information by their nodes for the formation of clusters. This approach entails long network lifetime.

To maintain connectivity and stability [97], authors have developed topology control protocol that amends the transmission range of mobile nodes with in the clusters. This algorithm improves stability and reduces number of global reelections for the cluster heads. But this approach increases number of members in clusters.

### 2.3.4 Real Life Applications

Real world system [98] requires adhoc network issues to be addressed effeminately. High mobility of nodes is generated due to rapid changes in topology and there is need of efficient routing protocol to monitor these dynamic changes. Thus routing plays a very important role in adhoc networks due to its characteristics. Jan. et. al [98] used grid environment to evaluate routing protocol’s behavior in mobile ad hoc network. Authors have used adhoc health grid system in emergency situation for performance evaluation. Performance of adhoc routing protocol is evaluated by considering two scenarios i.e. small network with low mobility and large network with high mobility. They have found that performance of protocol can be judged with different scenarios whereas performance of protocol can be evaluated based on range of conditions [99]. Thus, there is need to monitor the mobility and traffic pattern by considering variety of different scenarios.

### 2.3.5 Security

The security-sensitive applications of ad hoc networks [19][29] require high degree of security because of high probability of attacks due to change in position of the nodes, and frequent deactivation and reactivation of malicious nodes. Attacks on adhoc wireless networks can be classified into two broad categories namely passive and active attacks. In passive attacks, attacker only listens the message, it does not send or update message whereas active attacks may disrupt the information of a node and
degrades the performance of complete adhoc network. Security of routing in adhoc network is challenging issue due to active and passive attacks.

2.3.5.1 Existing Attacks in Adhoc Networks

i. **Man in Middle Attack:** An attacker site between the sender and the receiver and snuffle any information being sent between two host terminals.

ii. **Interceptions:** Attackers might initiate interception attacks to get an illicit access to the routing messages that are not intentionally sent to them. This attack jeopardizes integrity and confidentiality of the packets. Wormhole attacks, Black hole attacks, and Routing packet analysis attacks are examples of interception attacks.

iii. **Eavesdropping:** Due to absence of centralized administration, Source and destination nodes rely on intermediate node to relay their data. This makes the nodes more susceptible to attacks based on information contained in the eavesdropped packets.

iv. **Jamming:** it is most traditional [100] technique to prevent communication in network. Jamming of radio signals causes messages to be lost or corrupt.

v. **Link Withholding Attack:** In this, a malicious node ignores link information of other nodes.

vi. **Traffic Analysis:** A malign node can send many DAD/fake messages to its neighbors which augments traffic overload.

vii. **Routing Disruption:** In this [101], a malicious node intentionally drops control packets, misroutes data or circulates irrelevant information to its neighbors.

viii. **Wormhole Attacks:** In this, two attacker nodes are linked via a private network connection. It is very sophisticated and severe attack.
ix. **Black Hole Attacks:** In a black hole [102] attack, a malicious node advertises misleading information, claiming that it has an optimum route and causes other good nodes to route data packet through malicious one. On receiving the data, malicious node drops the packet.

x. **Byzantine Attacks:** It [103] creates routing loops, forwarding packets through non optimal paths, or selectively dropping packets.

xi. **Resource Consumption:** An Attacker [104] can consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to other nodes present in the network.

xii. **Routing Table Poisoning Attack:** An attacker [105] could broadcast spoofed packets with source route to node via itself. In this situation, neighbors can store fake information. Another option is injecting a RREQ packet with a high sequence number; this will cause that all other legitimate RREQ packets with lower sequence number to be deleted [106].

xiii. **Location Disclosure Attack:** It gathers [107] the node location information, such as route map and then plan to do mischievous behavior. In traffic analysis techniques, an attacker can easily discover the location of a node, and the overall information and structure of the network.

xiv. **Flooding Attack:** In this attack [108], attacker can consume network resources unnecessary. This causes severe degradation in network performance.

xv. **Session Hijacking:** In this, attacker impersonates the victim node and continues the session with the target.

xvi. **SYN Flooding:** It is commonly used attacks and it exploits [109] the TCP’s three hand shake mechanism.
xvii. **Denial of Service (DoS):** A “denial-of-service” (DoS) [110-115] is an attack with the purpose of preventing legitimate users from using a specified network resource for which they have authorization. For e.g., malicious node can alter MAC or IP address.

xviii. **Repudiation Attack:** it makes data or information appear to be invalid or misleading.

xix. **DDoS (Distributed Denial of Service):** DDoS is coordinated attack [115] on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems.

### 2.3.5.2 Classification of Existing Secure Routing Protocols

To meet the recent and rapidly increasing demand in decentralized environments like mobile ad hoc networks (MANETS) [16] the need for a secure routing protocol becomes inevitable so that the attacks such as malicious routing misdirection, black hole, gray hole, denial of service etc. can be averted[116].

i. **SLSP (Secure Link State Protocol):** This protocol [117] provides secure proactive topology discovery which is beneficial for network operation. It is known as stand alone and self contained link state discovery protocol. It is responsible for securing the route discovery and distribution of link state information. This protocol is robust against Dos and Byzantine adversaries. But this protocol is still vulnerable to colluding attackers and other attackers.

ii. **SEAD (Secure Efficient Adhoc Distance Vector Routing Protocol):** It is [118] based on DSDV routing protocol. This protocol is used to guard against Denial of Service by using one way hash functions. It provides limited CPU processing capability. Long lived routing loops can be reduced by using destination sequence numbers. These destination sequence numbers provide replay protection of routing update messages in SEAD.

iii. **SAODV (Secure Ad hoc On Demand Distance Vector):** It is an enhancement over version of AODV [5][119] routing protocol that utilizes
iv. **CONFIDANT (Cooperation of nodes fairness in dynamic adhoc network):**

   It [120] is an enhancement of DSR routing and based on selection of selfish and unselfish nodes. Trust and routing calculation process is evaluated by experience, observation and behavior of other nodes, present in the network. It identifies routing misbehavior and maintains the provision of correct forwarding and traffic diversion.

v. **ARAN (Authenticated Routing for Ad-Hoc Networks):** ARAN [121] is an on demand secure routing protocol and it relies on digital certificates. By using certificate process, it provides authentication, message integrity and non repudiation. Thus, it ensures end to end message delivery between source and destination. ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. This protocol does not perform well when it is itself authenticated by selfish node and this also leads to wastage of bandwidth.

vi. **ARIADNE:** It is a secure on [122] demand routing protocol and it is based on TESLA concept. TESLA is an efficient authentication scheme that requires loose time synchronization. Firstly, it verifies route authenticity and secondly, it also checks that no node is missing on RREQ message. It is vulnerable to an attacker that happens to be along the discovered route. This routing can authenticate any three schemes: (i) Shared secrets between each pair of nodes (ii) Shared secrets between communicating nodes combined with broadcast authentication or (iii) digital signatures. Ariadne needs the security association between the initiator and every node including intermediate node and the source node. ARIADNE prevents attackers with uncompromised routes and
vii. **ENDAIRA**: It is an improved version [123] of ARIADNE and provides solution where ARIADNE fails. It is based on provision on public key system concept. But it does not provide any solution against man in middle attack. So, there is need to generate enhanced version of ENDAIRA known as ENDIARA Loc.

viii. **ENDAIRALoc**: This protocol [123] provides solution over man in the middle attack as well as the wormhole attack. It uses location information of a node to resist this attack. It uses pair wise secret keys i.e. symmetric key mechanism rather than public key mechanism. As a result, energy consumption reduces effectively.

ix. **PrAODV**: It is an enhancement of an AODV [124] routing protocol. It uses prediction based routing to reduce route breakages which improves the performance of the network. It maintains two additional parameters in RREP message of AODV such as velocity and location information. These parameters help to calculate predicted link value by which source node can easily predict lifetime of a node.

x. **CORE**: Michiardi and Molva introduced an approach[125] which suggests an algorithm that relies on DSR routing. It follows reputation mechanism for monitoring the cooperativeness of nodes. This mechanism uses the nodes’ reputation to forward packets through reliable nodes.

xi. **SAR**: It is an extension of AODV [126] routing protocol. This protocol uses trust level mechanism to make efficient and secure routing decision. In this, a node can find a path through nodes with a particular shared key. It shares symmetric encryption key concept among the nodes. SAR increases overhead due to calculation of encryption and decryption process at each node. It can be implemented using any routing protocol.
xii. **BISS (Building Secure Routing out of an Incomplete Set of Security Associations):** In this [5][127], only the destination has security associations established with all nodes on the selected route. The sender will authenticate route nodes directly through security associations and indirectly the nodes which it does not have security associations. The suggested algorithm reduces length ratio. Authentication process can be done by using message authentication codes and digital signatures. It follows RREQ process as in Ariadne.

xiii. **TIARA (Techniques for Intrusion-resistant, Ad Hoc Routing Algorithms):** This protocol [128] is used to protect against Resource depletion attack, Flow disruption attack and Route hijacking. This algorithm can be used with any other existing routing protocol.

xiv. **SRP (Secure Routing Protocol):** It is an on demand [129] routing protocol. It can discover all possible paths between two nodes. The sole assumption of the protocol is that all the nodes share a group key K and can be trusted from the beginning. This algorithm is suitable for various applications like military and emergency situations.

xv. **SPREAD (Security Protocol for Reliable data delivery):** It provides data confidentiality [130] security service in routing protocols. It uses secret sharing scheme between neighboring nodes to strengthen data confidentiality. It overcomes the problem of eavesdropping and colluded attacks.

xvi. **AODV-SEC:** It is an improved version [131] of SAODV and extension of AODV routing protocol. It uses PKI as a trust anchor for node identification using X.509 certificates. X.509 version of AODV-SEC does not scale well in case traffic load increases. It may be due to the cryptographic mechanisms.

Although researchers [133-135][57-59] have designed security extensions for several existing protocols, many of which remove performance optimizations.

It has been found that there does not exist any particular protocol available in the literature which can manage both internal and external attacks. Thus, designing
efficient routing protocols that provide both high security and high network performance is still a focus of recent research in this field.

2.3.5.3 Intrusion Detection Schemes

Intrusion detection is a process of monitoring activities in a system which can be an adhoc network. The provision of maintaining and conducting this task is called an Intrusion Detection System (IDS) [139][140][141]. Naseer et. al [142] has focused on a certain limitations of watchdog[143] and path rater[144] and proposed a novel algorithm Ex Watchdog IDS. Ex Watchdog identifies malicious nodes which divide the whole network by sending fake/misbehaving information to other nodes. Watchdog and pathrater approach is based on direct trust mechanism. In addition to this mechanism, proposed approach also maintains Route guard for response. This algorithm fails if malicious node tampers the packet. Also suggested approach is not applicable for real life applications.

Further, Rajeshwari et. al has proposed EIDAN (Enhancement on Intrusion Detection Systems For Ad hoc Networks)[145] a new architecture that uses intrusion detection techniques. The novelties of the system lie between the detection of active attacks. It has been designed to detect resource consumption attack, packet dropping attack and fabrication attacks. Rafsanjani et. al[139] did not found any suitable application to remove intrusions for mobile adhoc network. Thus researchers have classified architecture for intrusion detection systems and also compared with existing intrusion detection systems. Zhang and Lee [146] put forward an intrusion detection system in MANET. This approach is distributed and dependent on nodes cooperation. Each node maintains IDS agent which is responsible for intrusions detection. This approach is more suitable for flat network infrastructure. Bachrgger et al [147] has developed a similar protocol as discussed in [144] for DSR, called CONFIDANT. This protocol is also designed to overcome the problem as discussed in [143]. In this protocol, behavior of neighbor nodes can be evaluated by each node having in the same transmission range. After malicious node detection, intermediate node circulates information about its misbehave to all other neighbor nodes, present in the network. Process to handle node observation and information gathered by trusted node is also
identified. Prevention of false report i.e. CORE protocol is proposed by [147] which is an effective solution of DoS [148].

Subsequently, extension of DSR known as OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) was proposed by Baker et. al [148]. This protocol evaluates behavior of a node based on ranking. Ranking of a node degrades gradually if its threshold value is lower than faulty thresholds. Further, Cluster based intrusion detection system was proposed by Huang and Lee [149]. This protocol identifies attacks as well as type of attacks.

In [150], authors have discussed honest rate based collaborative intrusion detection system (HIDS). This algorithm was based on rating and decision making process based on multiple threshold values. Ranking node of index is initialized by 1. Node is punished, if it is not forwarding packets otherwise rewarded.

In work [151], we have focused on all the limitations of watchdog and AODV vulnerabilities and proposed a solution to find good neighbor nodes with in transmission range for data transmission and also evaluate trust of each node. This protocol is beneficial in small as well as large network in the presence of varying number of malicious nodes. Bahareh et. al [152] has designed an Intrusion Detection System based on protocol by including host based and network based intrusion detection system into an account. Efficiency of an algorithm was evaluated based on detection rate, CPU usage and accuracy.

Zhang et al [153] has focused on intrusion detection approach by changing behavior of a node. After considering this approach, Trang et. al [154] has proposed a solution by using IDS agent to detect the intrusions without changing the normal activities of the protocol. This approach was implemented in the presence of one malicious node. Also it does not deal with impersonation attacks and its performance deteriorates which mobility of network is high. [155] has discussed solution against wormhole attack for end to end node detection. Chaki et. al [156] has proposed scheme by taking heterogeneous IDS into an account. This algorithm resolves the problem of phantom intrusion detection and also discards a suspected intruder.
In [157], an agent-based Intrusion Detection Model of Mobile Ad Hoc Network is proposed. Suggested approach prefers decision mode concept that forms a cluster-head-centered backbone network as well as partial cluster heads to execute total network intrusion detection.

2.3.5.4 Malicious Node Detection Schemes

Oscar et. al [25] has suggested a scheme to detect misbehaviour in packet forwarding approach in mobile adhoc networks. In this algorithm, misbehavior node is easily identified if it drops packets. But Packet may be lost due to high mobility and noisy channels in the presence of correctly behaving nodes. Probability of malicious node detection is only 50% which is limitation of this algorithm. [158] has enhanced packet forwarding operations by proposing multipath reliable routing algorithm. This algorithm considers detection of malicious nodes by the destination node. Also, remove the entire path where malicious nodes reside. Path Removal and Data Packet prevention is formed by using dispersion techniques.

Trust propagation model as well as trust calculation process was proposed by Yan Lindsay et. al[159]. This approach has used four axioms and evaluates the validity of axioms on probability based model and entropy based model. Two concepts are used for axioms development i.e. concatenation propagation and multipath propagation. This proposed algorithm highlights trust propagation problems in adhoc network. Here, coordinated malicious nodes can reduce good nodes’ recommendation trust by attacking on small number of users or creating conflicting views for good nodes, present in the network. So, this paper does not investigate all possible attacks in this paper. The focus of this paper is only based on trust evaluation process with good metrics.

In [160], author has proposed reputation based model by using beta distribution approach. The reputation based model is composed of two parameters reputation parameters and reputation management. Reputation parameter table maintains all the information of related parameters. And reputation management involves manipulation, updation, calculation of this parameters and also evaluate credit values of these nodes. Direct reputation was observed through the direct observation of the
behavior of nodes. Whereas, Indirect reputation is evaluated by exchanging the information. But this approach was not efficient in case of third party approach. Further, indirect reliability of third party node is introduced by Guisheng Yin et. al. In this approach, there is need to consider, nodes which have limited resources.

Raja and Khan [161] has discussed seven methods for black hole attack detection in AODV. Probability distribution function, time finite state machines concept, neighbors advise, statistical model, data mining approach are main focusing concept of this paper. Anomaly detection based on markov chain model and dynamic training technique for malicious node (having black hole characteristics) is discussed. Here, Khan et. al has highlighted on black hole nodes only. Kanthakumar et. al[612] has discussed Camouflagge Event Based Malicious node detection architecture(CENDA) to detect malicious nodes while identifying the type of attack. This system can be used as admiration of an existing system which is controlled and monitored by base station in the sensor network systems. In this algorithm, repeated query for a node is generated about its different neighbors. Also there is loss of anonymity and it may provide complicated results in military like applications.

In [163], author has divided an algorithm based on FSM detection process. If a node misbehaves like mismatching between IP and MAC address of a node, source node and hop count are unreachable, forwarded RREQ messages were not heard, RREQ/hello forwarding rate is beyond the threshold, then respective alarm with respect to attack will be generated. These techniques are based on direct trust metrics, So Chi Zhang et. al [164] has discussed an approach by considering routing algebra concept. They have developed abstract framework for trust based routing. This routing involves two phases such as direct trust inference and indirect trust inference. These inference axioms can be used in trust based routing by using QoS metrics. Indirect trust inference axioms is evaluated with direct trust and based on transitive trust evaluation scheme. But this approach is not suitable for real life applications.

In [165], author has proposed improved neighbor detection algorithm for AODV routing protocol by using concept signal to noise ratio. In this approach, there is wastage of wireless resources and eventually deteriorates the network performance. Sridhar et. al [166] has discussed hop count based routing for providing life time link
stability for residual lifetime of a link. [167] has suggested a method to decide to number of necessary nodes by considering size and transmission range of a network. Moreover, [168] [169] has proposed that probability of a network connectivity goes to zero if $r(|V|) \leq \sqrt{(1-\epsilon) A \log |V| / \Pi|V|}$, for any $\epsilon > 0$. Otherwise if $r(|V|) \geq \sqrt{A(\log |V| + \gamma |V|) / \Pi|V|}$, is connected with probability converging to 1. [170] has analyzed that frequent interrupting of neighbour nodes can produce transmission delay and low quality in terms of data transfer. In [23], malicious node detection is proposed by using bayesian game approach. Further, post detection game is used between malicious node and regular node.

Gong et. al [171] has suggested trust vector model for malicious node detection. But this approach provides solution against black hole attacks only. In [172], has proposed packet forwarding scheme and CBC-Xmode approach for malicious node detection. This approach uses a cryptographic scheme which is not suitable for large networks. Fei Xing et. al[173] has focused on the survivability of ad hoc networks with node misbehaviors and failures. In this approach, semi markov process model is proposed to characterize two cases: (i) the evolution of node behavior and (ii) probabilistic connectivity of individual node. Author has evaluated these two cases to solve node isolation related problems. Here authors, have highlighted all the problems against denial of service attack and isolate the node if attack is detected. This algorithm has limited solution against DoS.

2.4 Summary

This chapter presented a review of literature for ad hoc routing protocols. This chapter gives a clear view on issues of routing protocols in the presence of attacks. Solution of this problem against each routing protocol has been discussed in this chapter. The problem with ad hoc routing protocol is that it is difficult to maintain secure data among large number of trustworthy or untrustworthy nodes. Thus they lack flexibility and are even not suitable for real life environment. Ad hoc routing protocols do not support all of the ad hoc features. As such, deriving a precise routing algorithm could become a difficult undertaking in real time environment. The following chapter presents the methodology used in the present research work and comparative analysis of existing routing protocols based on metrics is discussed. So, the present work proposes solving the ad hoc routing protocol problem in untrustworthy environment.
This chapter presents the comparative analysis of ad hoc routing protocols and their comparisons with algorithm namely Enhanced AODV.